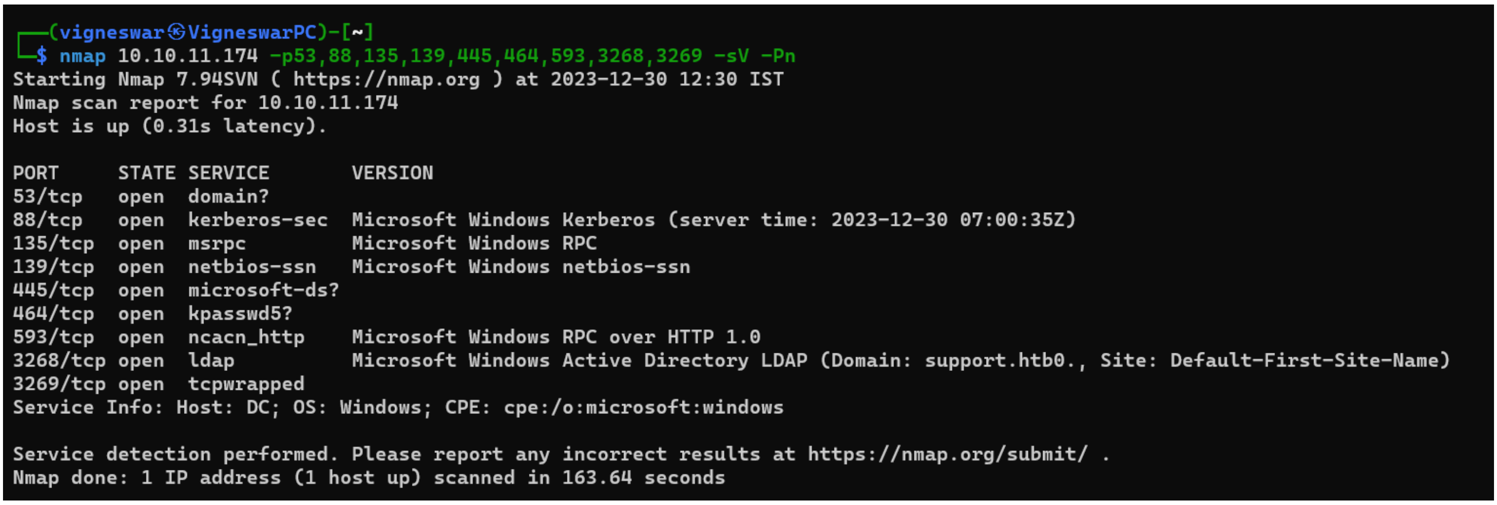
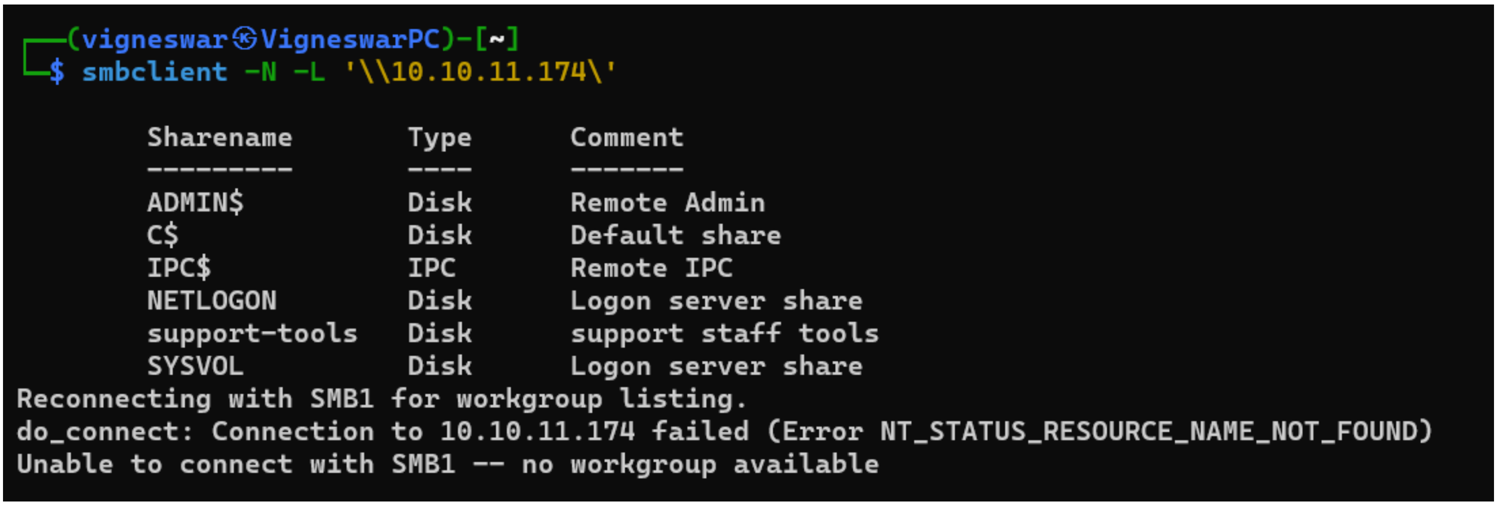
# *Information Gathering*

1) found open ports



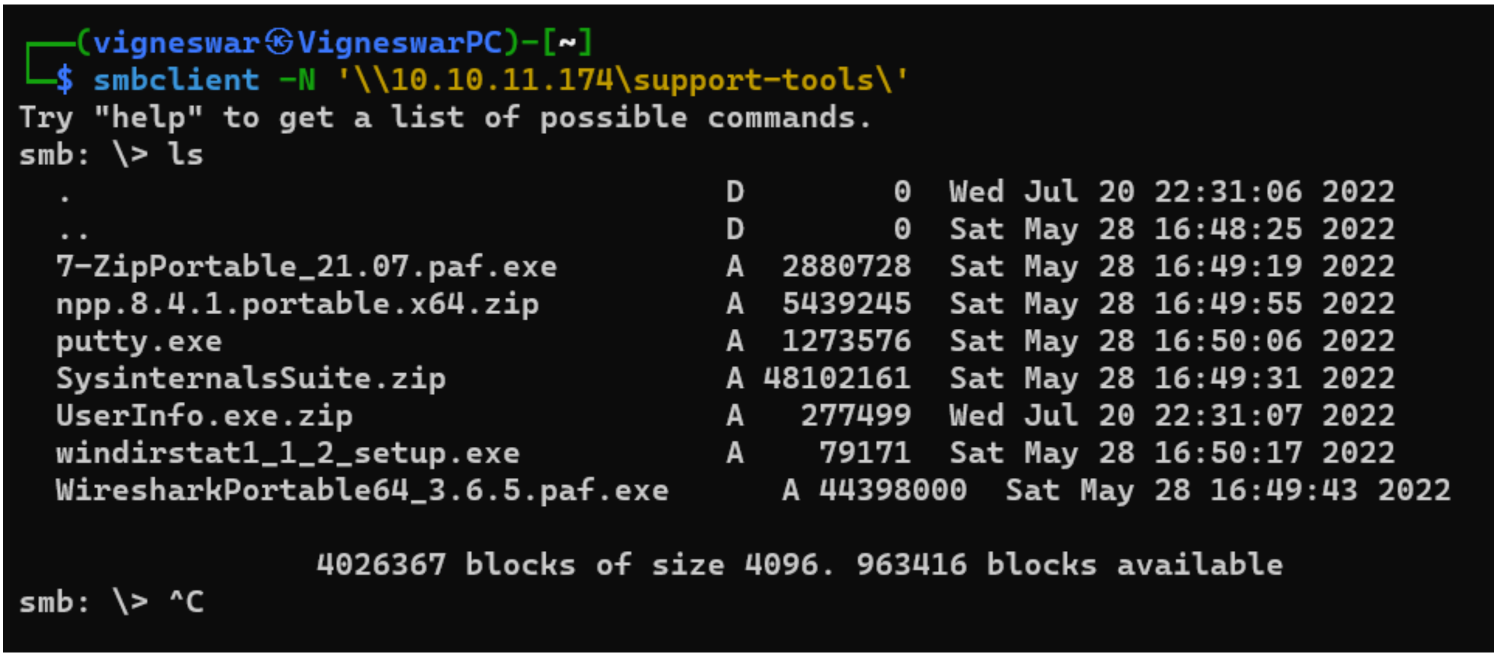
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nmap 10.10.11.174 -p53,88,135,139,445,464,593,3268,3269 -sV -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-30 12:30 IST
Nmap scan report for 10.10.11.174
Host is up (0.31s latency).

PORT     STATE SERVICE       VERSION
53/tcp   open  domain?
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2023-12-30 07:00:35Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: support.htb0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 163.64 seconds
```

2) found smb shares



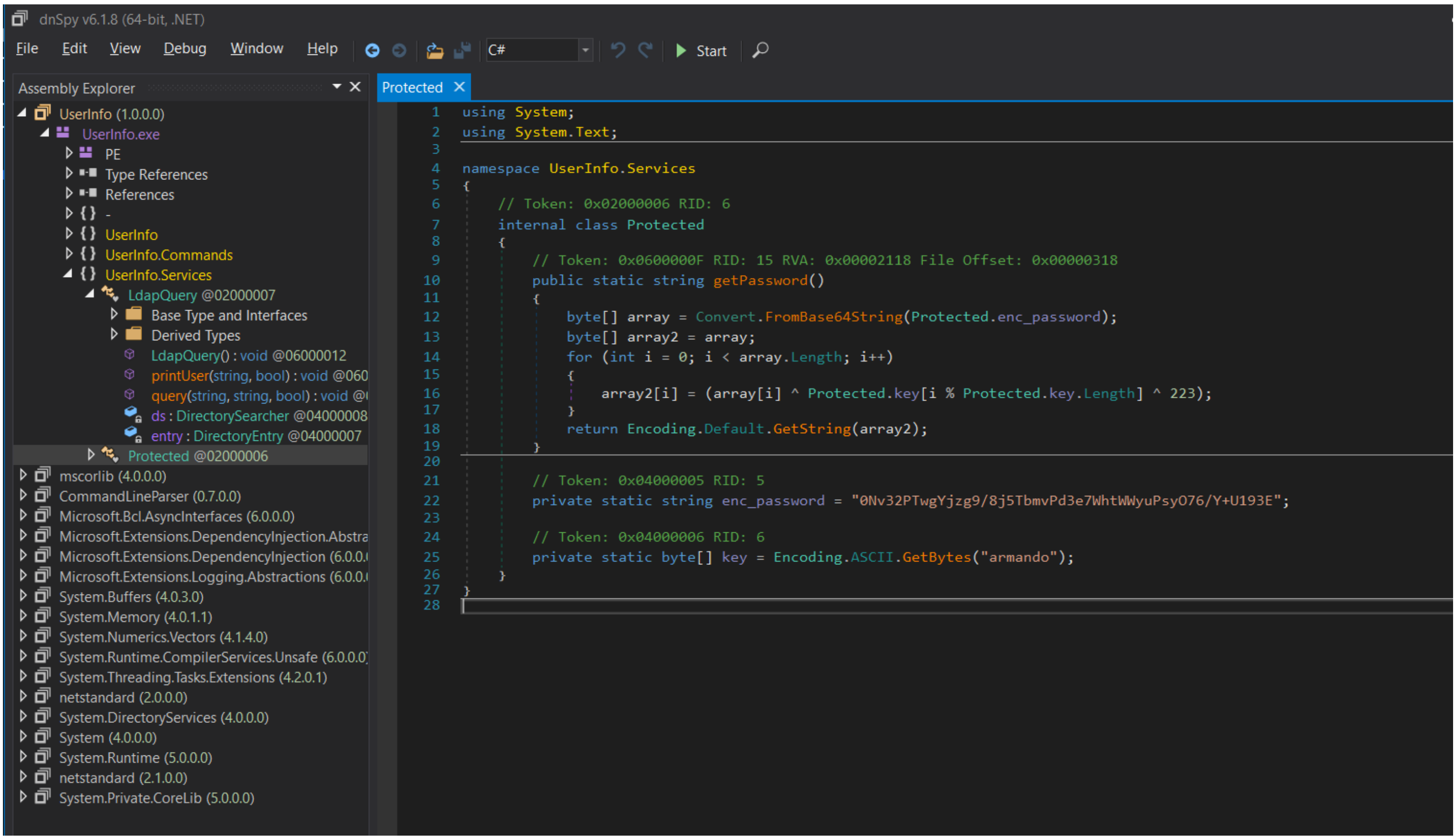
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ smbclient -N -L '\\10.10.11.174\'

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        support-tools   Disk      support staff tools
        SYSVOL          Disk      Logon server share
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.11.174 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

3) found a custom binary



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ smbclient -N '\\10.10.11.174\support-tools\'
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed Jul 20 22:31:06 2022
  ..                                  D        0  Sat May 28 16:48:25 2022
  7-ZipPortable_21.07.paf.exe         A  2880728  Sat May 28 16:49:19 2022
  npp.8.4.1.portable.x64.zip          A  5439245  Sat May 28 16:49:55 2022
  putty.exe                           A  1273576  Sat May 28 16:50:06 2022
  SysinternalsSuite.zip               A 48102161  Sat May 28 16:49:31 2022
  UserInfo.exe.zip                    A   277499  Wed Jul 20 22:31:07 2022
  windirstat1_1_2_setup.exe           A    79171  Sat May 28 16:50:17 2022
  WiresharkPortable64_3.6.5.paf.exe      A 44398000  Sat May 28 16:49:43 2022

                4026367 blocks of size 4096. 963416 blocks available
smb: \> ^C
```

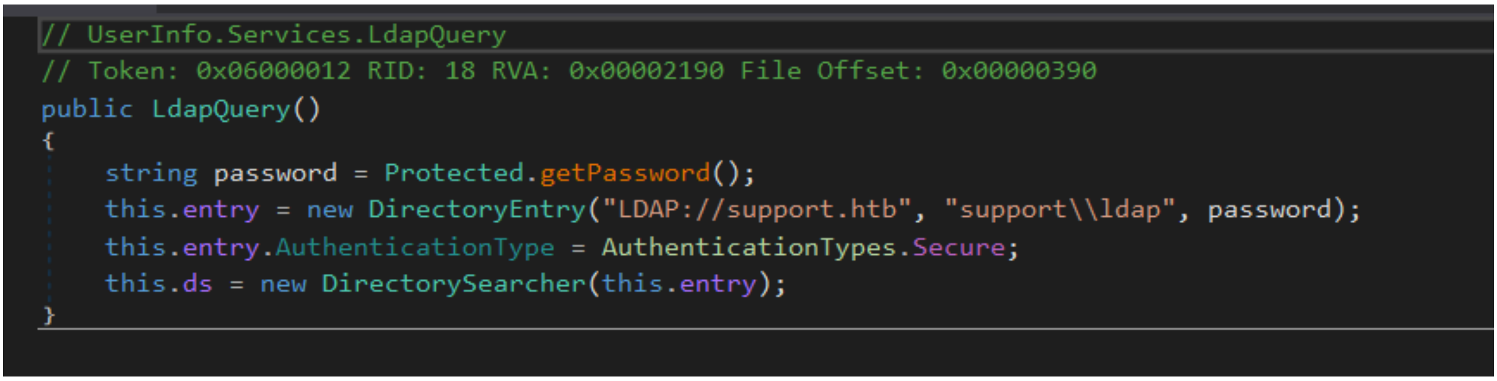
4) found credentials in the binary


dnSpy v6.1.8 (64-bit, .NET)
File
Edit
View
Debug
Window
Help
C#
Start
Assembly Explorer
Protected
UserInfo (1.0.0.0)
UserInfo.exe
PE
Type References
References
{ } -
UserInfo
UserInfo.Commands
UserInfo.Services
LdapQuery @02000007
Base Type and Interfaces
Derived Types
LdapQuery() : void @06000012
printUser(string, bool) : void @060
query(string, string, bool) : void @
ds : DirectorySearcher @04000008
entry : DirectoryEntry @04000007
Protected @02000006
mscorlib (4.0.0.0)
CommandLineParser (0.7.0.0)
Microsoft.Bcl.AsyncInterfaces (6.0.0.0)
Microsoft.Extensions.DependencyInjection.Abstra
Microsoft.Extensions.DependencyInjection (6.0.0.
Microsoft.Extensions.Logging.Abstractions (6.0.0.
System.Buffers (4.0.3.0)
System.Memory (4.0.1.1)
System.Numerics.Vectors (4.1.4.0)
System.Runtime.CompilerServices.Unsafe (6.0.0.0)
System.Threading.Tasks.Extensions (4.2.0.1)
netstandard (2.0.0.0)
System.DirectoryServices (4.0.0.0)
System (4.0.0.0)
System.Runtime (5.0.0.0)
netstandard (2.1.0.0)
System.Private.CoreLib (5.0.0.0)

```
using System;
using System.Text;

namespace UserInfo.Services
{
    // Token: 0x02000006 RID: 6
    internal class Protected
    {
        // Token: 0x0600000F RID: 15 RVA: 0x00002118 File Offset: 0x00000318
        public static string getPassword()
        {
            byte[] array = Convert.FromBase64String(Protected.enc_password);
            byte[] array2 = array;
            for (int i = 0; i < array.Length; i++)
            {
                array2[i] = (array[i] ^ Protected.key[i % Protected.key.Length] ^ 223);
            }
            return Encoding.Default.GetString(array2);
        }

        // Token: 0x04000005 RID: 5
        private static string enc_password = "0Nv32PTwgYjzg9/8j5TbmvPd3e7WhtWWyuPsyO76/Y+U193E";

        // Token: 0x04000006 RID: 6
        private static byte[] key = Encoding.ASCII.GetBytes("armando");
    }
}
```

nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz

4) found username - support



```
// UserInfo.Services.LdapQuery
// Token: 0x06000012 RID: 18 RVA: 0x00002190 File Offset: 0x00000390
public LdapQuery()
{
    string password = Protected.getPassword();
    this.entry = new DirectoryEntry("LDAP://support.htb", "support\\ldap", password);
    this.entry.AuthenticationType = AuthenticationTypes.Secure;
    this.ds = new DirectorySearcher(this.entry);
}
```