

Audit et sécurisation (hardening) d'AD CS

Il est important que notre PKI soit sécurisée. Il existe différents outils permettant de l'auditer :

[Certipy](#), [Exegol](#), [PSPKIAudit](#) ou encore [Locksmith](#).

Exemple de Certify et Certipy :

```
C:\>certify find /vulnerable
```

```

  _____
 /  _  |      | | ( ) /  |
| |  _  _  _  | |  |  _  _
| |  /  _ \ '  | |  |  | | |
| |  _  _ /  | |  |  | | | |
 \___\___| |  \___| |  \___|
                                     _/ |
                                     |__./
```

v1.0.0

```
[*] Action: Find certificate templates
```

```
[*] Using the search base 'CN=Configuration,DC=ad,DC=khroners,DC=fr'
```

```
[*] Listing info about the Enterprise CA 'Khroners Labs Enterprise CA'
```

Enterprise CA Name	: Khroners Labs Enterprise CA
DNS Hostname	: SRV-CA35-01.ad.khroners.fr
FullName	: SRV-CA35-01.ad.khroners.fr\Khroners Labs Enterprise CA
Flags	: SUPPORTS_NT_AUTHENTICATION, CA_SERVERTYPE_ADVANCED
Cert SubjectName	: CN=Khroners Labs Enterprise CA, DC=ad, DC=khroners, DC=fr
Cert Thumbprint	: 8FD1AEAF57EE974EB726D884775133B4D4C9D270
Cert Serial	: 1500000004A03185E3D30CA7C300000000000004
Cert Start Date	: 02/10/2023 08:09:54
Cert End Date	: 02/10/2028 08:19:54
Cert Chain	: CN=KhronersLabsCertificateAuthority ->

CN=KhronersLabsEnterpriseCA, DC=ad, DC=khroners, DC=fr

UserSpecifiedSAN : Disabled

CA Permissions :

Owner: BUILTIN\Administrateurs S-1-5-32-544

Access Rights

Principal

Allow Enroll

AUTORITE NT\Utilisateurs

authentifiésS-1-5-11

Allow ManageCA, ManageCertificates

BUILTIN\Administrateurs

S-1-5-

32-544

Allow ManageCA, ManageCertificates

AD\Admins du domaine

S-1-5-

21-1812995439-3560927909-1751902240-512

Allow ManageCA, ManageCertificates

AD\Administrateurs de l'entrepriseS-1-

5-21-1812995439-3560927909-1751902240-519

Enrollment Agent Restrictions : None

[+] No Vulnerable Certificates Templates found!

Certify completed in 00:00:00.5455163

```
certipy find -u gilles.besson@ad.khroners.fr -password Password -scheme ldap
```

Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Finding certificate templates

[*] Found 36 certificate templates

[*] Finding certificate authorities

[*] Found 1 certificate authority

[*] Found 14 enabled certificate templates

[*] Trying to get CA configuration for 'Khroners Labs Enterprise CA' via CSRA

[!] Got error while trying to get CA configuration for 'Khroners Labs Enterprise CA' via CSRA:
CASSessionError: code: 0x80070005 - E_ACCESSDENIED - General access denied error.

[*] Trying to get CA configuration for 'Khroners Labs Enterprise CA' via RRP

[!] Failed to connect to remote registry. Service should be starting now. Trying again...

[*] Got CA configuration for 'Khroners Labs Enterprise CA'

[*] Saved BloodHound data to '20231007001536_Certipy.zip'. Drag and drop the file into the
BloodHound GUI from @ly4k

```
[*] Saved text output to '20231007001536_Certipy.txt'  
[*] Saved JSON output to '20231007001536_Certipy.json'
```

3 fichiers sont ensuite générés. On peut analyser nous même le txt ou importer dans BloodHound GUI le .zip.

Revision #1

Created 6 October 2023 22:02:49 by Khroners

Updated 6 October 2023 22:41:37 by Khroners