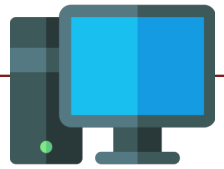
To remember



Artefacts

- **CA database** : C:\Windows\System32\CertLog\<CA-NAME>.edb
- **Hive – *SYSTEM***
  CA config : Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc
- **Hive – SOFTWARE**
  Template cache HKU\.DEFAULT\Software\Microsoft\Cryptography\CertificateTemplateCache
- **IIS logs** : *C:\inetpub\logs\LogsFiles*
- **Windows event logs** : 4882, 4885, 4886, 4887, 4888, 4890, 4891, 4892, 4896, 4897, 4898, 4899, 4900
- **NTDS database** : *Services\Public Key Services\Certificate Templates*

Tools

- **Collect** : *FastIR, Velociraptor, Certutil, Dissect*
- **Analysis** : *Certify, PSPKIAudit, Python, ESEDatabaseView, Dissect, Log2Timeline*

Detect

CVE-2022-26923

Hunt for :

- Event logs :
  - 4887 : "*RequesterName*" =/= "*Subject*"
  - 4741 : Computer account creation event
- CA database : "*RequesterName*" =/= "*Subject*"

ESC1

Hunt for :

- CA database : "*RequesterName*" != "*SAN*"

ESC3

Hunt for :

- Event logs :
  - 4887 : "*RequesterName*" =/= "*Subject*"
- CA database : "*RequesterName*" =/= "*Subject*"

ESC4

Hunt for :

- Event logs :
  - 4899 : "*NewTemplateContent*"
- AD object :
  - "*whenChanged*" attribute