
Cloud
Connect
Oslo Spektrum
November 7 - 9

When the Red Team/TA Goes Passwordless

Hasain ”The Wolf” Alshakarti

Principal Cyber Security Advisor @ TRUESEC

Passwordless

- Certificate Based Authentication
- Smart Card Logon
- Key Based Authentication (WHfB)

nic Cloud Connect

AD Certificate Services

- Often found misconfigured
- Great value for attackers
- No passwords needed!

Offensive Toolkit

- Since 2021 ADCS security awareness greatly increased with the release of Certify
- Certificate Templates attacks

https://github.com/GhostPack/Certify/
https://github.com/ly4k/Certipy

Vanilla persistency
“oob”

nic Cloud Connect

Vulnerable Templates

- ESC1 to ESC10 attacks
- CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT
  - Allows for impersonation!

https://specterops.io/wp-content/uploads/sites/3/2022/06/Certified_Pre-Owned.pdf
https://posts.specterops.io/certificates-and-pwnage-and-patches-oh-my-8ae0f4304c1d

Template Enumeration

Custom Subject Name

May 2022 Changes

- CVE-2022-34691
- CVE-2022-26931
- CVE-2022-26923

- Strong Mapping mechanism to address issue

https://support.microsoft.com/en-au/topic/kb5014754-certificate-based-authentication-changes-on-windows-domain-controllers-ad2c23b0-15d8-4340-a468-4d4f3b188f16

May 2022 Patch

- StrongCertificateBindingEnforcement
  - Disabled Mode
  - Compatibility Mode
  - Full Enforcement Mode

- Also Restrict Schannel (TLS Auth)
  - CertificateMappingMethods

StrongMapping “Bypass”

Disable SID Flag

```
PS C:\Users\causer> certutil -dstemplate HappyUser msPKI-Enrollment-Flag +0x80000
CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=corp,DC=local:
  HappyUser

Old Value:
  msPKI-Enrollment-Flag REG_DWORD = 9
    CT_FLAG_INCLUDE_SYMMETRIC_ALGORITHMS -- 1
    CT_FLAG_PUBLISH_TO_DS -- 8
New Value:
  msPKI-Enrollment-Flag REG_DWORD = 80009 (524297)
    CT_FLAG_INCLUDE_SYMMETRIC_ALGORITHMS -- 1
    CT_FLAG_PUBLISH_TO_DS -- 8
    0x80000 (524288)
CertUtil: -dsTemplate command completed successfully.
```

Disable Custom SID

LDAP TLS Authentication

- When Kerberos does not allow auth, LDAP might!

Shadow Credentials

- Key Trust: Public/Private key authentication with no certificates
- Stored in attribute msDS-KeyCredentialLink

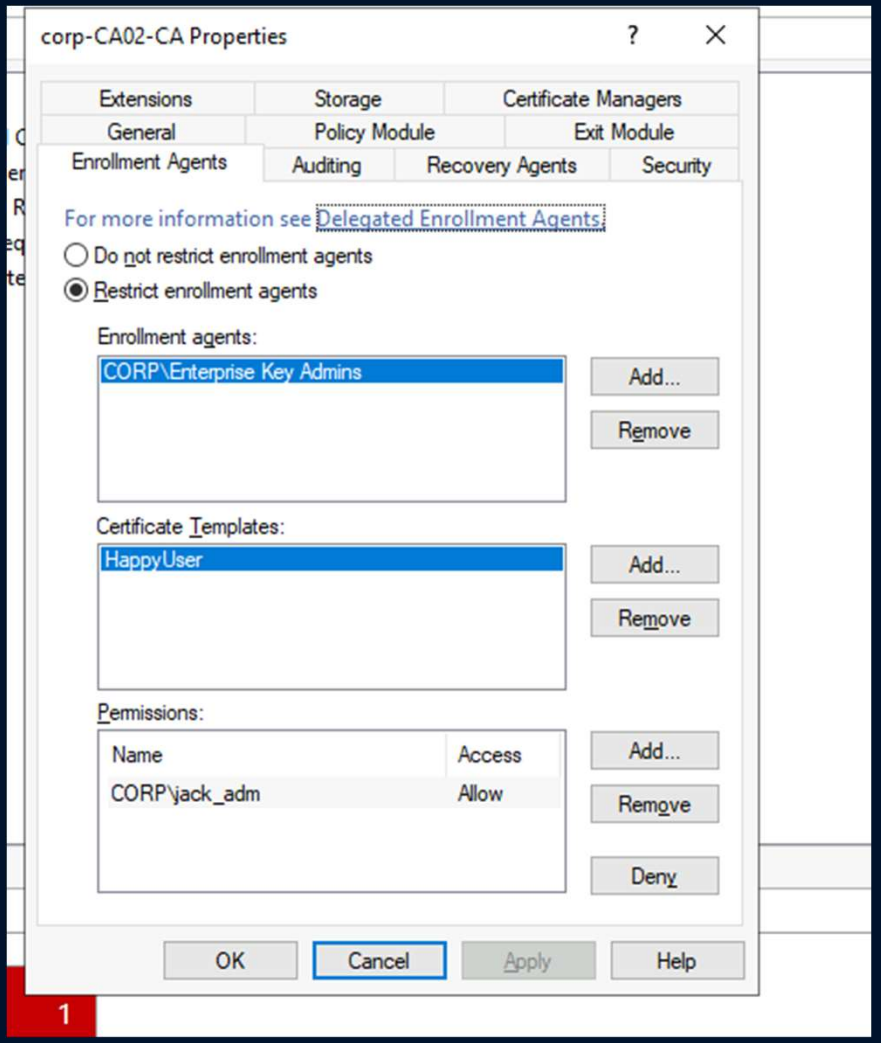
https://github.com/eladshamir/Whisker
https://github.com/Dec0ne/ShadowSpray/

Shadow Credentials

Enrollment Agent

- If a certificate is issued, it allows to act on behalf of any other user.
- Can be further limited to special users

Restricted Enrollment Agent



nic Cloud Connect

Key take aways

- Regular User/Computer certificates
- Template Configuration and Permissions
- StrongMapping vs "AltSecID"
- Shadow Credentials / msDS-KeyCredentialLink
- Enrollment Agent Restriction

Cloud Connect

Thank you!