



AD CS means: Active Directory is Cheese (Swiss)

Jake Hildreth

Senior Security
Consultant @ Trimarc

Who is this guy?

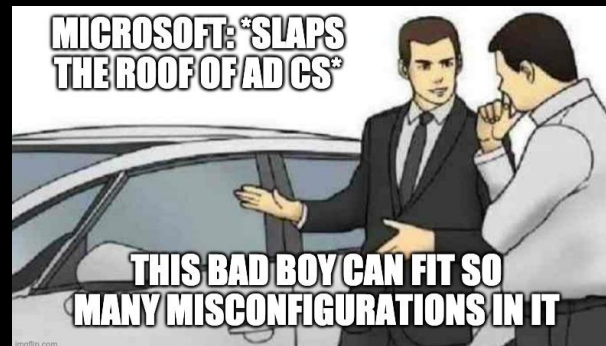
- Recovering systems administrator
- Over 20 years in Information Technology
- Active Directory Security Subject Matter Expert who performs AD security assessments for companies in the Fortune 500 and beyond
- Husband to Kari
- Dad of Kate

What are we talking about today?

- Very high-level overview of Public Key Infrastructure (PKI)
- Idiosyncrasies of Microsoft's PKI implementation
- Three of the most common misconfigurations found in the wild
- Three of the most dangerous misconfigurations
- Remediation guidance for these six issues
- Review!

Prior Research

- Primary Source: *Certified Pre-Owned*¹ - The bible of AD CS abuse from SpecterOps' Will Schroeder and Lee Christensen
 - Certificate Theft
 - Account Persistence
 - Domain Escalation
 - Domain Persistence
- Additional Info: Christoph Falta, Brian Komar, Pete Long, Vadims Podans, Ned Pyle, Elad Shamir, Carl Sörqvist



¹ posts.specterops.io/certified-pre-owned-d95910965cd2.

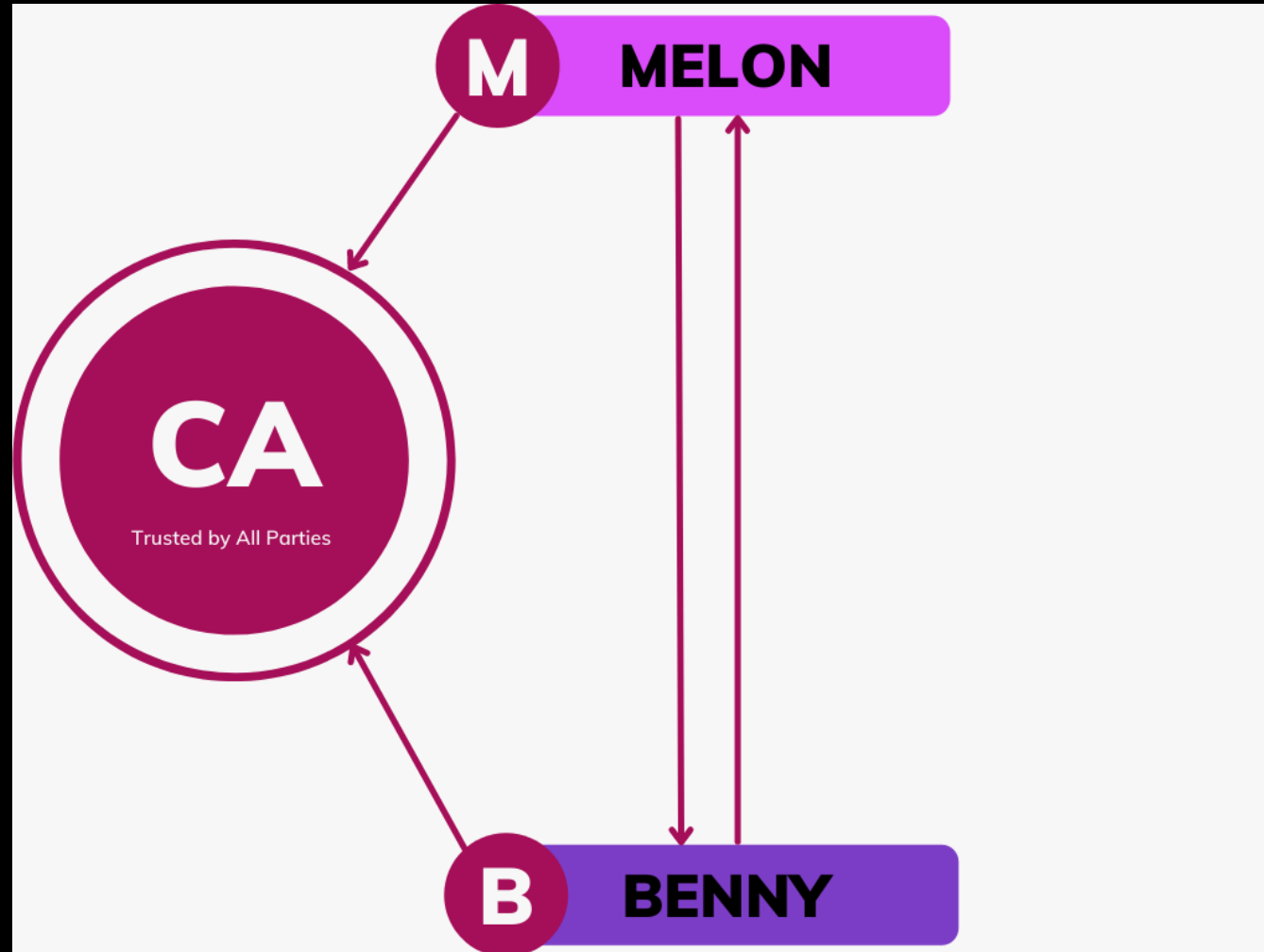
85,069 Foot Overview



Generic Public Key Infrastructure

- Primarily used to confirm authenticity and/or identity
- Can also be used to protect information via encryption
- Includes hardware, software, policies, and procedures
 - Each portion of the puzzle is its own animal
 - Interactions between elements create unexpected behaviors
- Requires at least three components. Bare bones example:
 - Certificate Authority (CA) – trusted by all parties
 - Party 1 – trusts the CA, but doesn't trust Party 2
 - Party 2 – trusts the CA, but doesn't trust Party 1

Generic Public Key Infrastructure



Benny (aka Mr. Mischief)



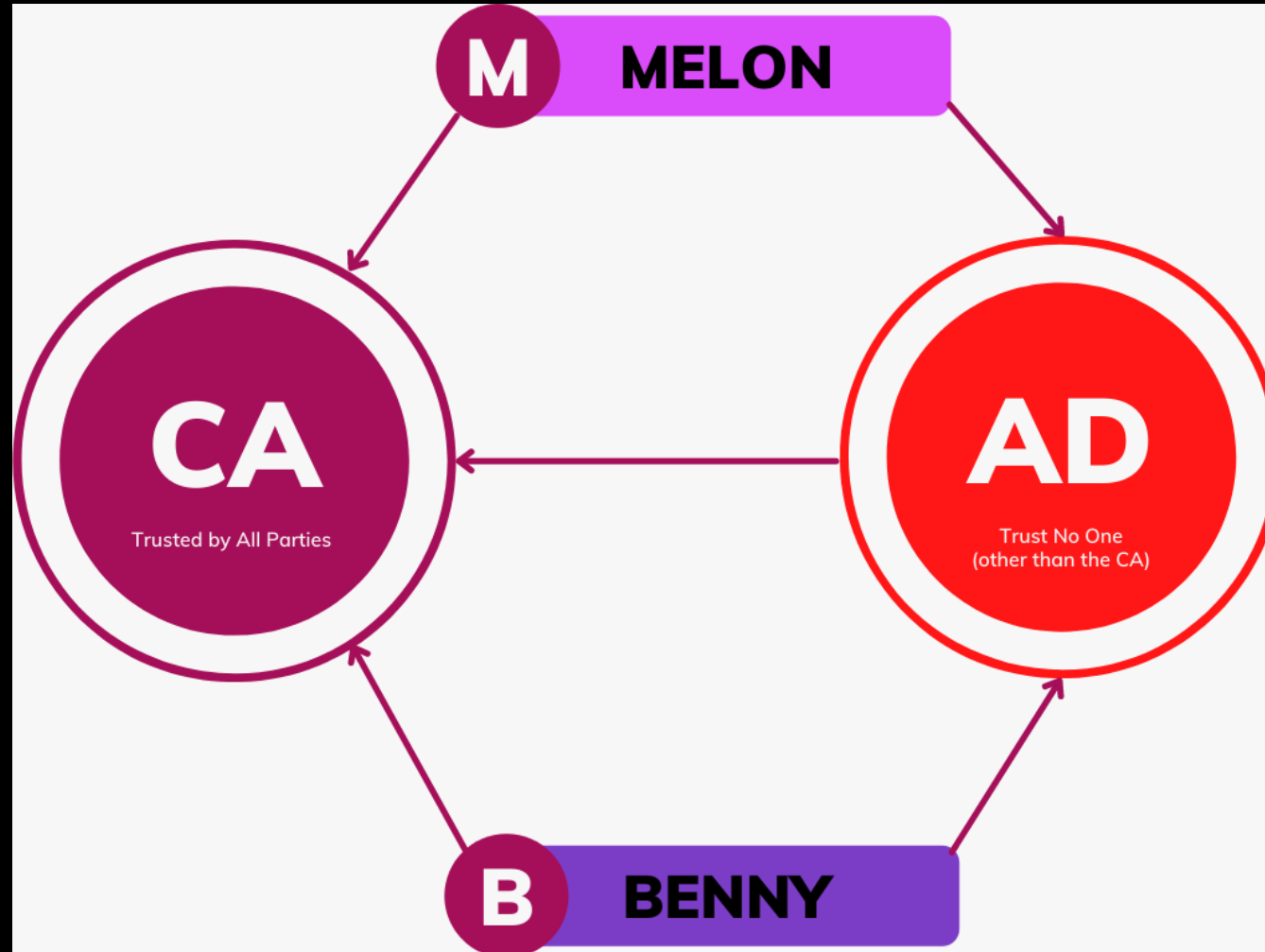
Melon (aka Mel-Mel)



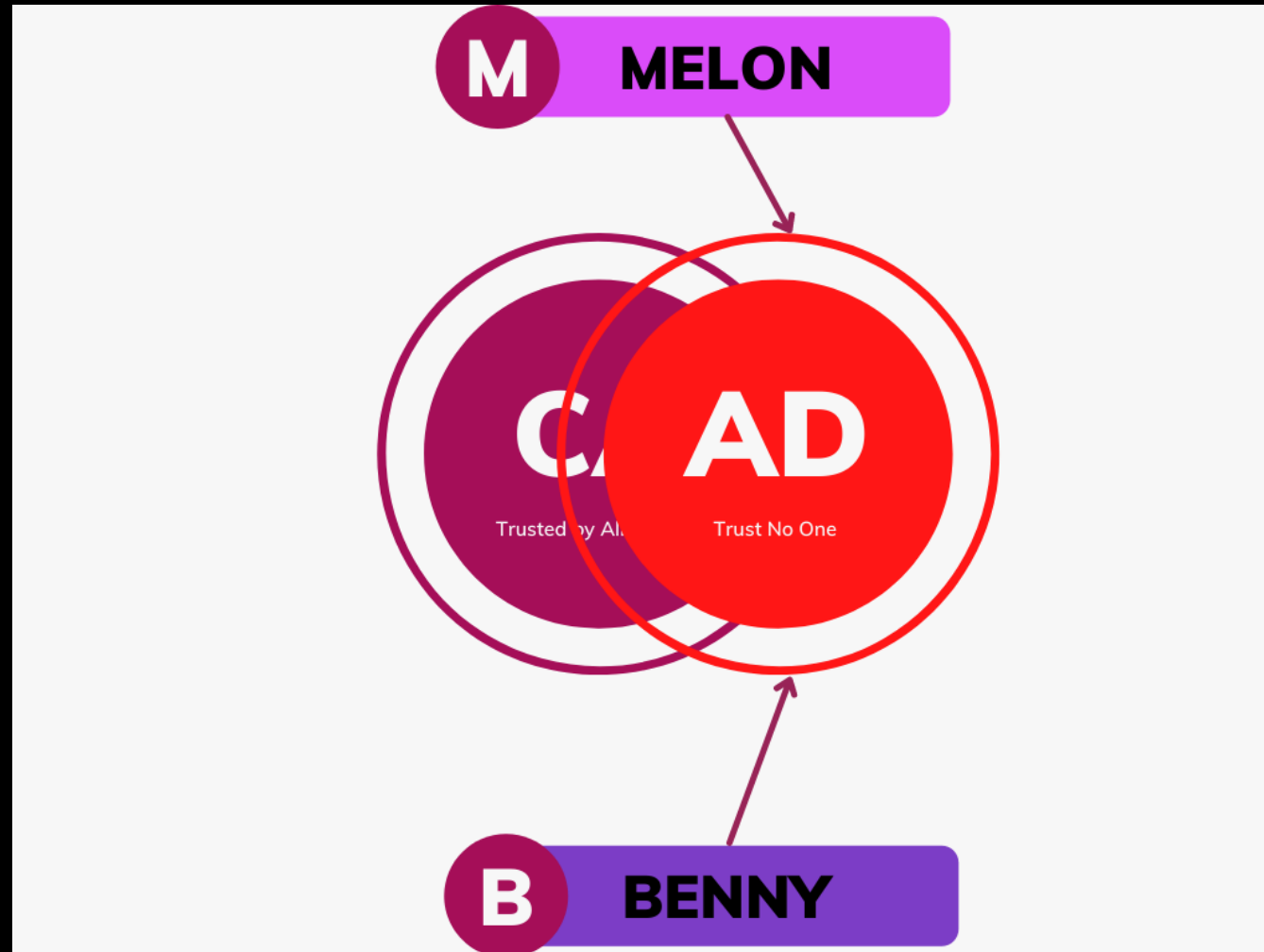
What Makes Active Directory Certificate Services (AD CS) Unique?

- Free and very easy to setup
- Almost no security guidance during deployment
- After installation, the user interface is as clear as mud
- Full impact of insecure configurations is rarely explained
- Out-of-box templates are secure, but insecure modifications are allowed
- Relies on Active Directory (AD) for user/computer authentication during certificate enrollment
- Almost all configuration is stored within Active Directory (AD)
- Certificates are not revoked when a password is changed
- It's EVERYWHERE

AD CS – The Expectation



AD CS – The Reality





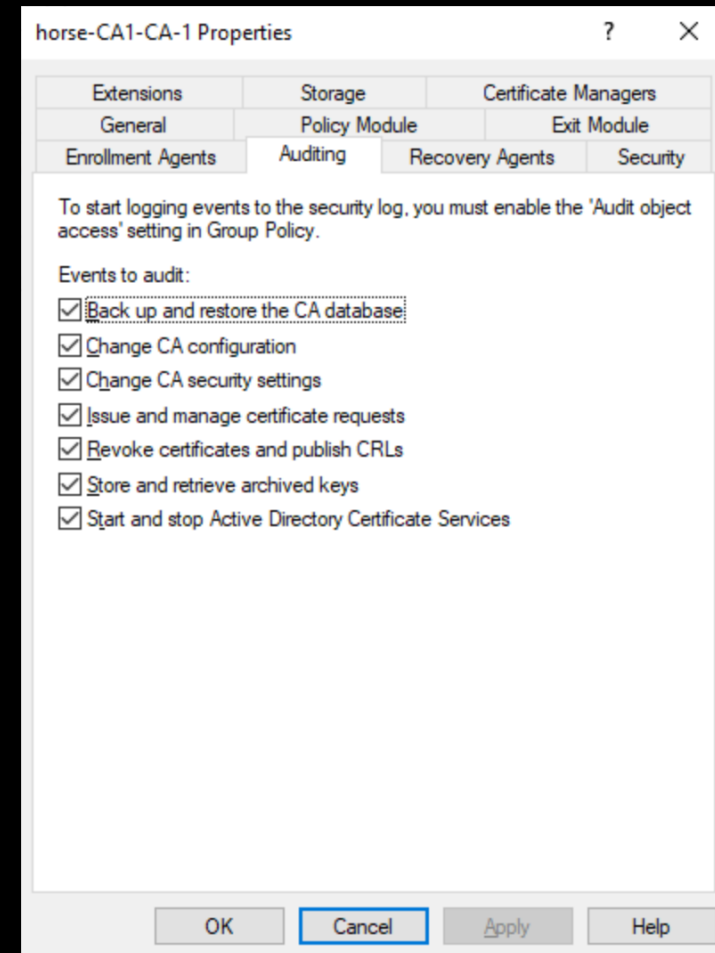
Common Misconfigurations

Common Misconfiguration #1: Insufficient Auditing

- AD CS auditing *is NOT enabled by default*
 - Why Microsoft?
 - Why would you do this?
 - Why would you do this to your loyal customers?
- Must be enabled on every CA individually
 - See above.
 - Thankfully can be enabled via certutil and easily scripted
- Can be very noisy depending on environment-specific Certificate Services usage.
- Not configured in most environments. Do not be ashamed.

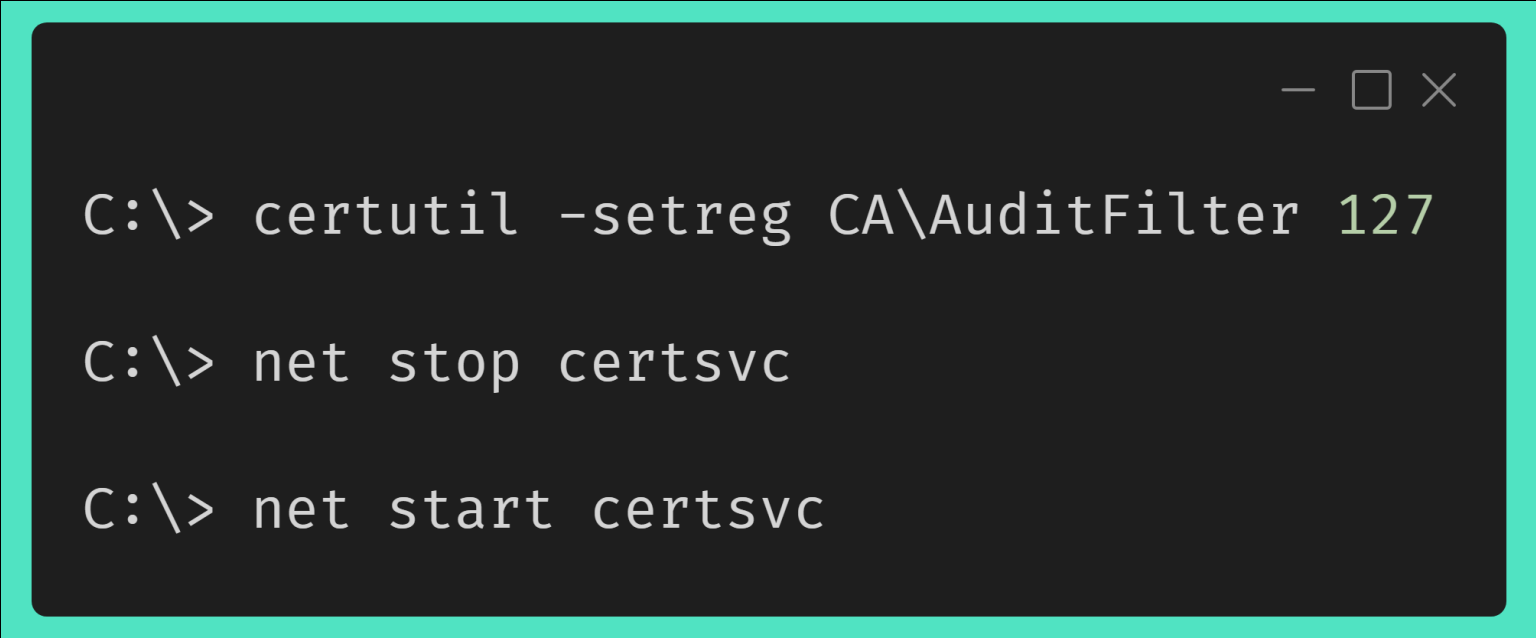
Remediation: Insufficient Auditing

- Step 1: Enable Auditing on the CA host (GUI Version)
 - Open the Certificate Authority MMC (certsrv.msc)
 - Right-click the CA name and select Properties
 - Click the Auditing tab and check all the boxes.
 - Click OK.
 - Restart the Certificate Services service
 - Repeat for every CA



Remediation: Insufficient Auditing

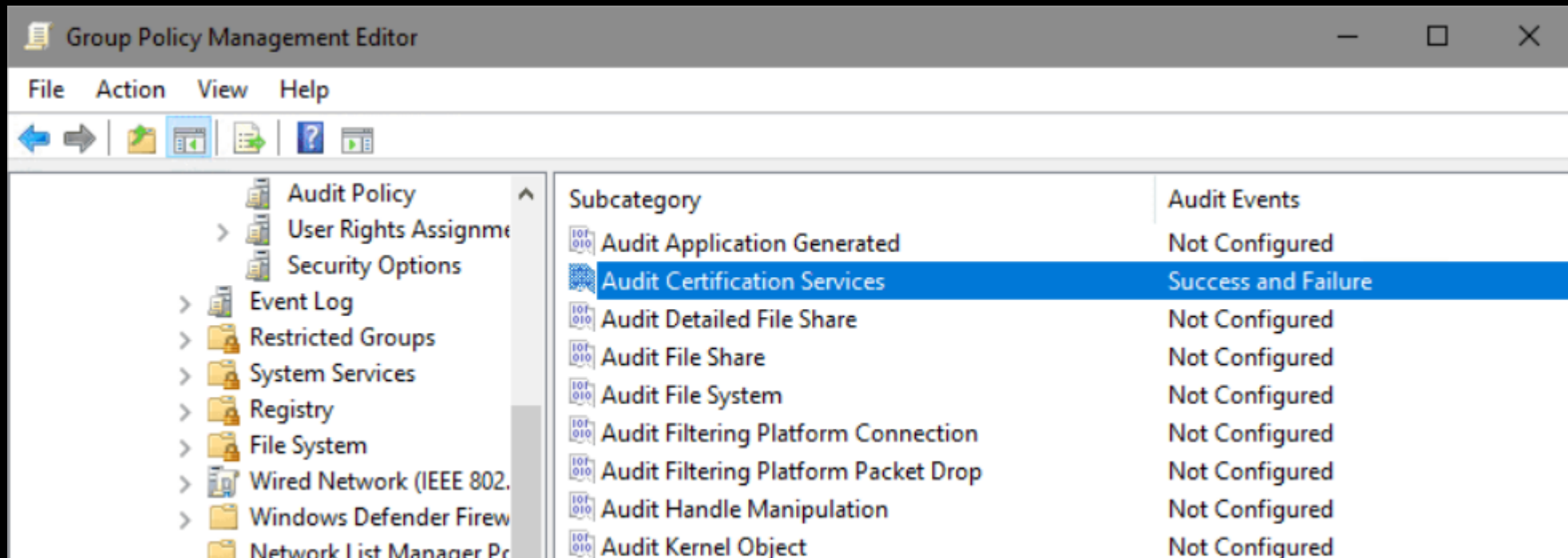
- Step 1: Enable Auditing on the CA host (Command Line Version)



```
C:\> certutil -setreg CA\AuditFilter 127  
  
C:\> net stop certsvc  
  
C:\> net start certsvc
```

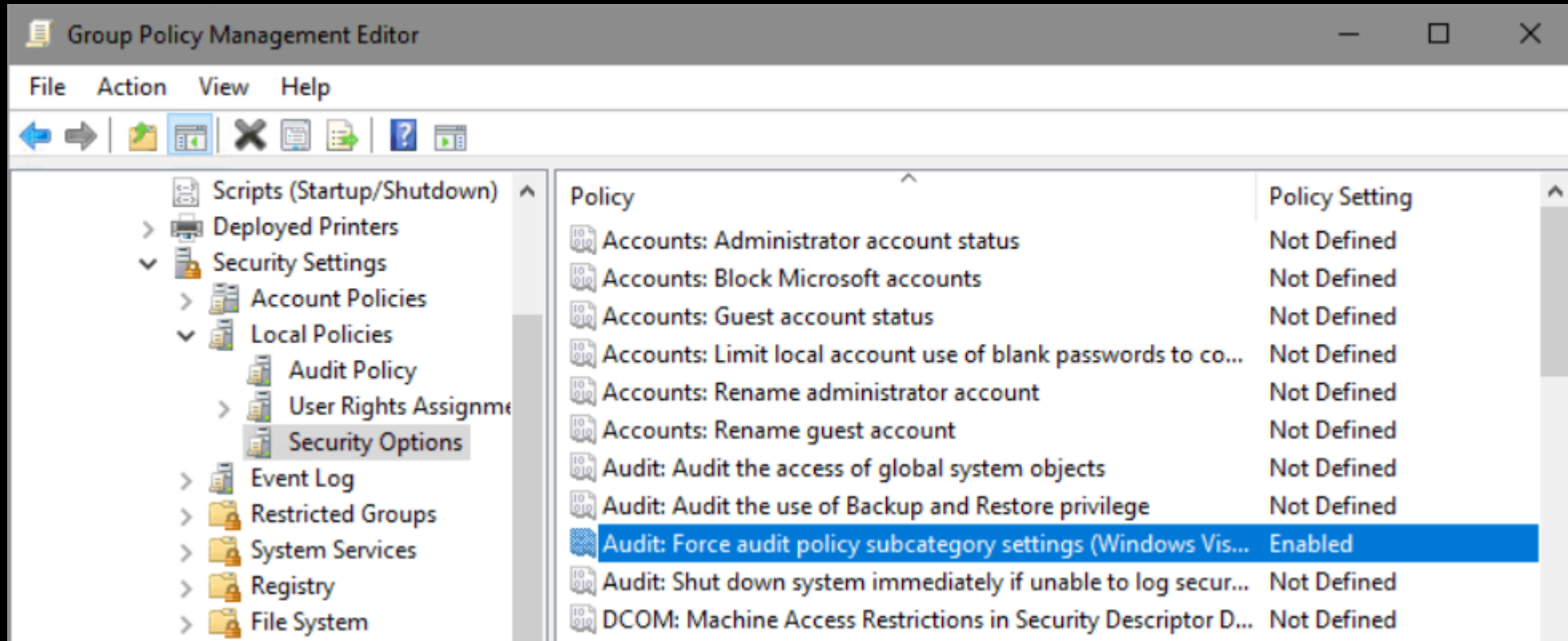

Remediation: Insufficient Auditing

- Step 2: Enable Certifications Services Auditing in Group Policy



Remediation: Insufficient Auditing

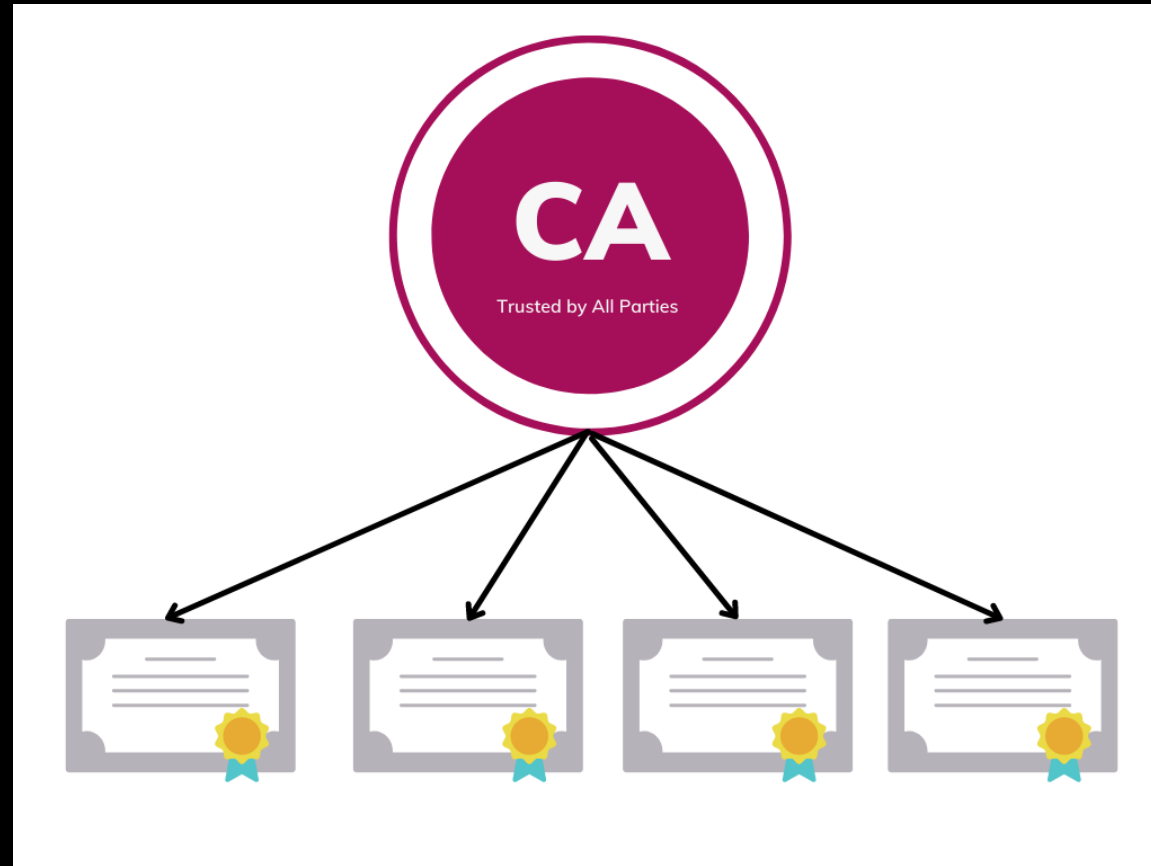
- Step 3: Enforce Advanced Auditing in Group Policy



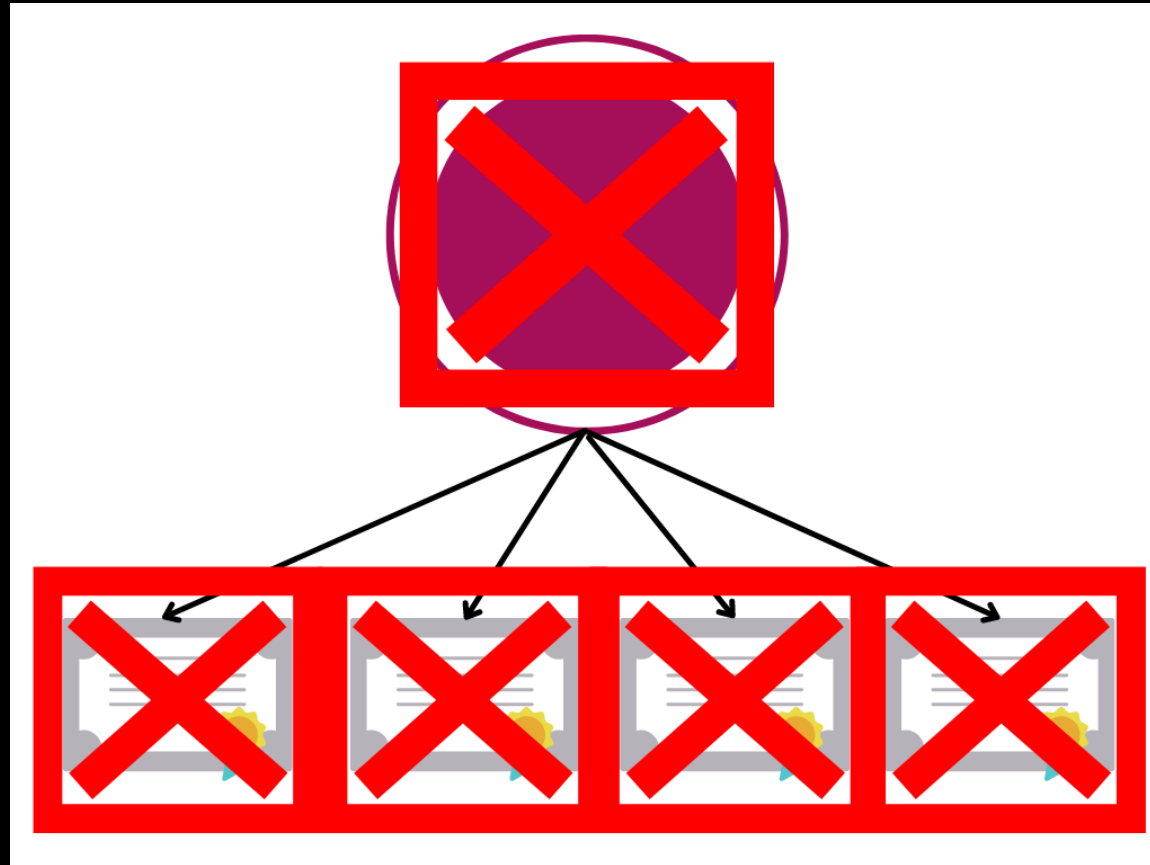
Common Misconfiguration #2: Single-Tier Architecture

- Default configuration
- Per Microsoft:
“This one-tier hierarchy **is not recommended for any production scenario** because with this hierarchy, a compromise of this single CA equates to a compromise of the entire PKI.”
- Little indication of implications of this configuration
- Mostly found in smaller networks with no dedicated security staff

Common Misconfiguration #2: Single-Tier Architecture



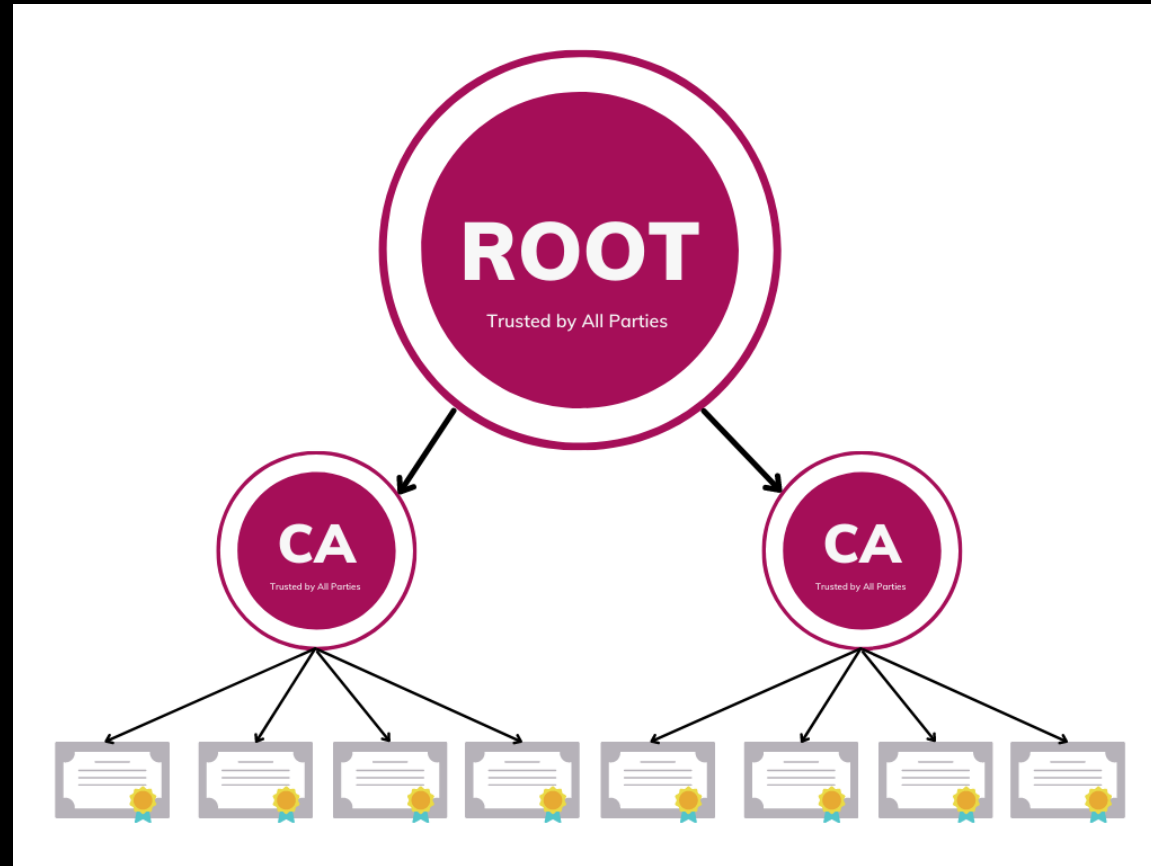
Common Misconfiguration #2: Single-Tier Architecture



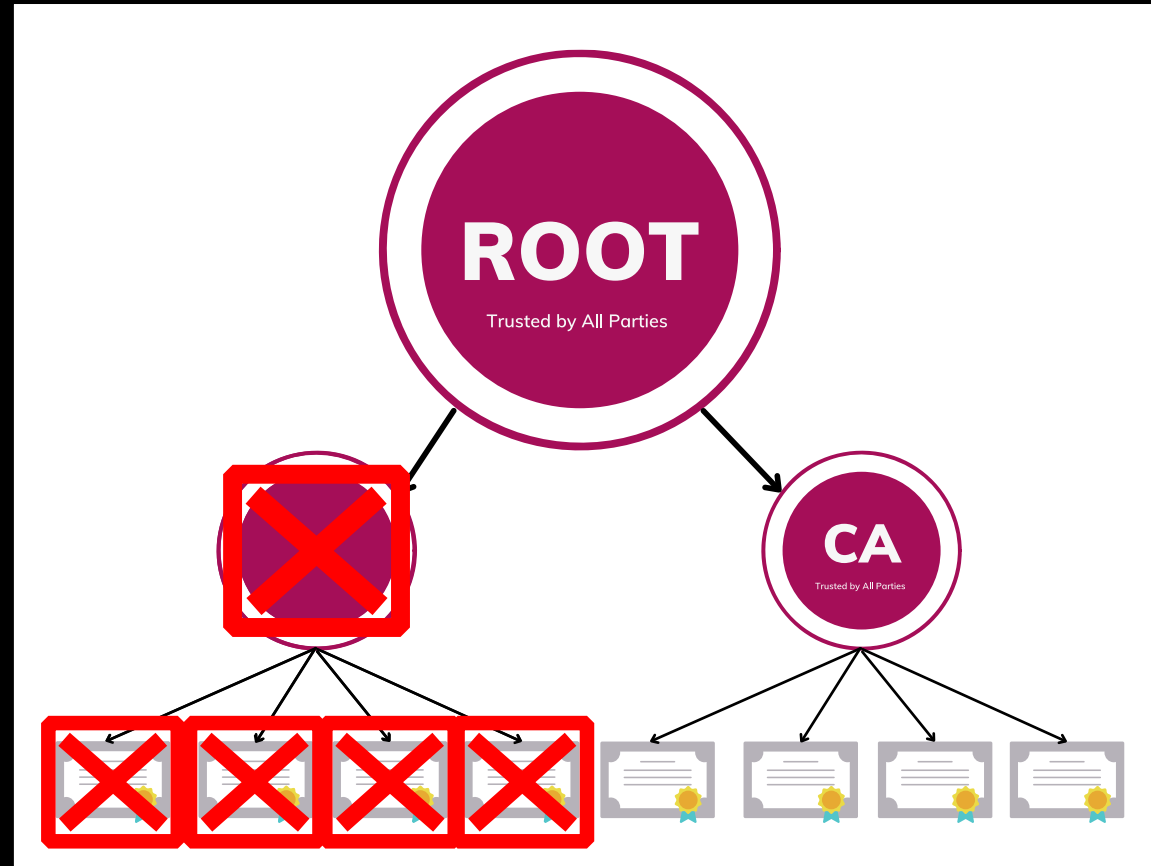
Remediation: Single-Tier Architecture

- Ask yourself if you *really* need your own AD-integrated PKI.
- If yes, a two-tier PKI is sufficient for most environments. In highly secure or highly distributed environments, a three-tier PKI may make more sense.
- Root CA **must** be built in Standalone mode.
 - Should remain offline unless issuing certificates for Intermediate/Issuing CAs or OS updates (much slower update cadence than usual)
 - Should utilize HSM, TPM, or vTPM to protect the CA's private keys
- Subordinate CAs should be built in Enterprise mode.
- Complete guide from PeteNetLive:
<https://www.petenetlive.com/KB/Article/0001309>

Remediation: Single-Tier Architecture



Remediation: Single-Tier Architecture



Common Misconfiguration #3: Non-Standard Object Ownership

- In general, when an AD object is created, its creator is the owner
- An object's owner can change all its settings regardless of configured permissions
- If... Correction... WHEN the owner of an object is compromised, the attacker can leverage that object to either escalate privileges or maintain persistence
- Often found in organizations with legacy installation(s) of AD CS where account tiering has been recently implemented

Common Misconfiguration #3: Non-Standard Object Ownership








Advanced Security Settings for horse-User

Owner: **Jake Hildreth (jhildreth1234)** [Change](#)

Permissions

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click the Modify button.

Permission entries:

Type	Principal	Access	Inherited from
 Allow	Authenticated Users	Special	None
 Allow	Administrator	Special	None
 Allow	Domain Admins (HORSE\Domain Admins)	Special	None
 Allow	Domain Users (HORSE\Domain Users)	Special	None
 Allow	Enterprise Admins (HORSE\Enterprise Admins)	Special	None
 Allow	Domain Admins (HORSE\Domain Admins)	Special	None
 Allow	Enterprise Admins (HORSE\Enterprise Admins)	Special	None

Remediation: Non-Standard Object Ownership

- Safe Owners include:
 - Well-Known Groups: Domain Admins, Enterprise Admins
 - Custom Groups: PKI Admins
- Enterprise Admins recommended



Remediation: Non-Standard Object Ownership

- Prerequisite: Active Directory PowerShell Module
- Find offending objects:

```
$ADRoot = (Get-ADRootDSE).rootDomainNamingContext
$Safe_Owners = "Enterprise Admins|Domain Admins|Administrators"

$ADCS_Objects = Get-ADObject -Filter * -SearchBase
                 "CN=Public Key Services,CN=Services,CN=Configuration,$ADRoot"
                 -SearchScope 2 -Properties *

$ADCS_Objects | Where-Object {
    $_.nTSecurityDescriptor.Owner -notmatch $Safe_Owners } |
Format-Table Name,DistinguishedName
```

<https://github.com/TrimarcJake/adcs-snippets>

Remediation: Non-Standard Object Ownership

- Results:

```
Administrator: Windows PowerShell

PS C:\Users\Administrator> $ADRoot = (Get-ADRootDSE).rootDomainNamingContext
PS C:\Users\Administrator> $Safe_Owners = "Enterprise Admins|Domain Admins|Administrators"
PS C:\Users\Administrator> $ADCS_Objects | Where-Object {
>>     $_.nTSecurityDescriptor.Owner -notmatch $Safe_Owners } |
>>     Format-Table Name,DistinguishedName
```

Name	DistinguishedName
NTAuthCertificates	CN=NTAuthCertificates,CN=Public Key Services,CN=Services,CN=Conf:
horse-User	CN=horse-User,CN=Certificate Templates,CN=Public Key Services,CN:
horse-WebServer	CN=horse-WebServer,CN=Certificate Templates,CN=Public Key Service
horse-Workstation Authentication	CN=horse-Workstation Authentication,CN=Certificate Templates,CN=f
horse-SubordinateCertificationAuthority	CN=horse-SubordinateCertificationAuthority,CN=Certificate Templat
horse-EnrollmentAgent	CN=horse-EnrollmentAgent,CN=Certificate Templates,CN=Public Key S

Remediation: Non-Standard Object Ownership

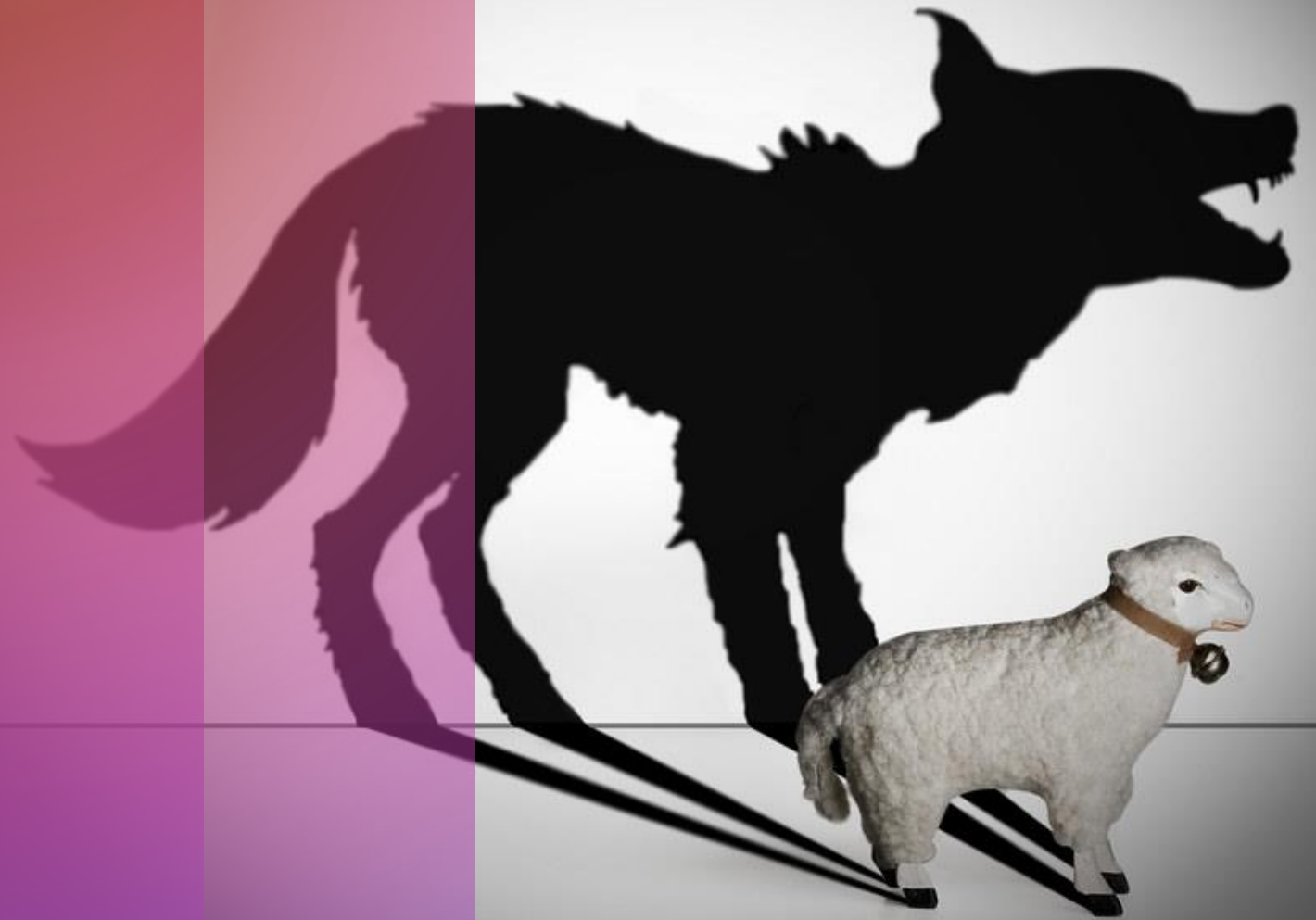
- Fix offending objects:

```
$DNSRoot = (Get-ADDomain).DNSRoot
$StandardOwner = New-Object System.Security.Principal.NTAccount($DNSRoot, "Enterprise Admins")

$ADCS_Objects_BadOwner = $ADCS_Objects | Where-Object {
    $_.nTSecurityDescriptor.Owner -notmatch $Safe_Owners
}

$ADCS_Objects_BadOwner | ForEach-Object {
    $ObjectPath = "AD:$($_.DistinguishedName)"
    $ObjectCN = $_.CanonicalName
    $ACL = Get-Acl -Path $ObjectPath
    $ACL.SetOwner($StandardOwner)
    Set-ACL -Path $ObjectPath -AclObject $ACL
}
```

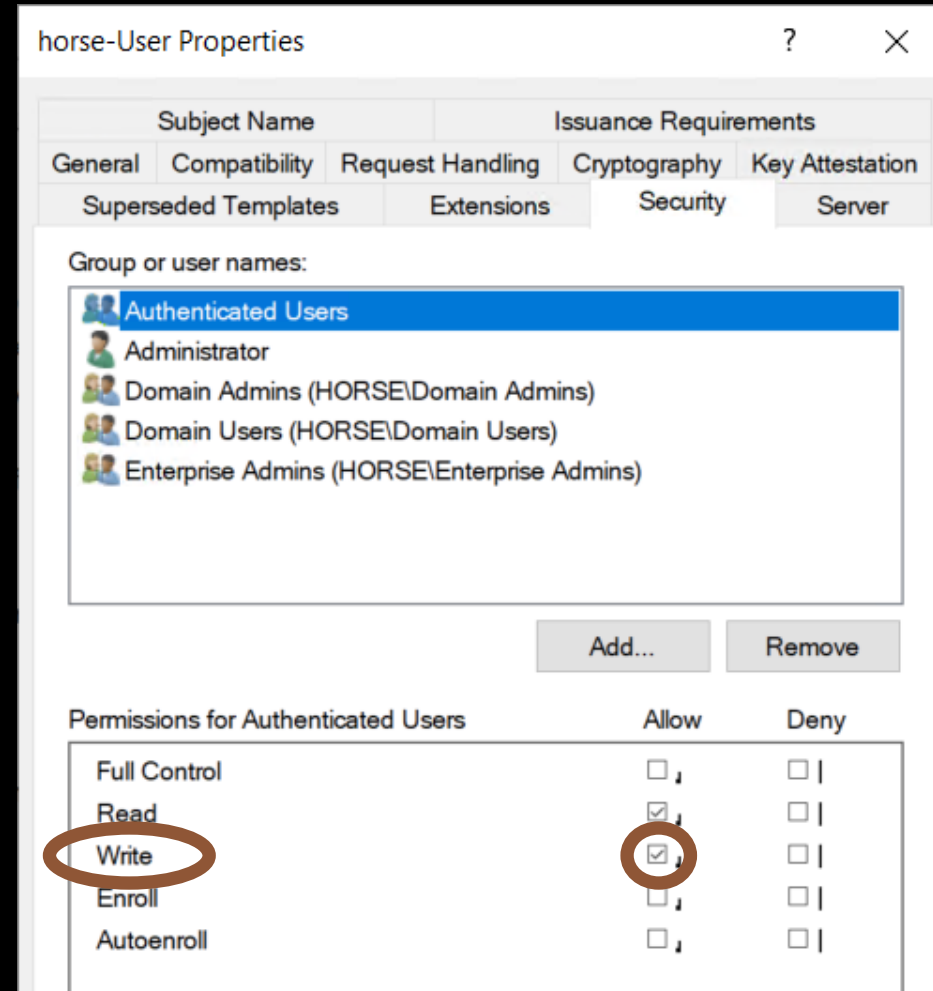
Dangerous Misconfigurations (The Fun Stuff!)



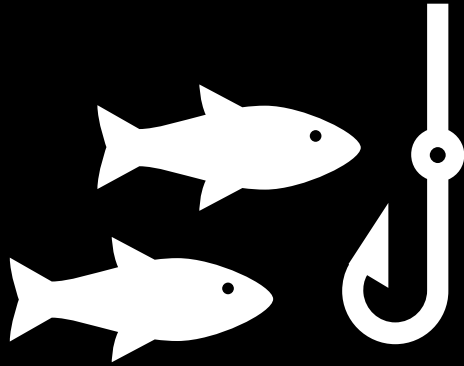
Dangerous Misconfiguration #1: Overly-permissive AD Object ACLs

- Low-privileged users should only be able to **read** objects in the AD “Public Key Services” (PKS) Container
- The “Everyone” group should never have rights on anything in the PKS Container
- Usually a template that was created for testing that was never removed after the test was complete.

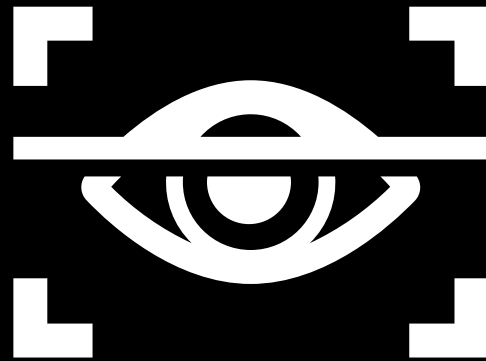
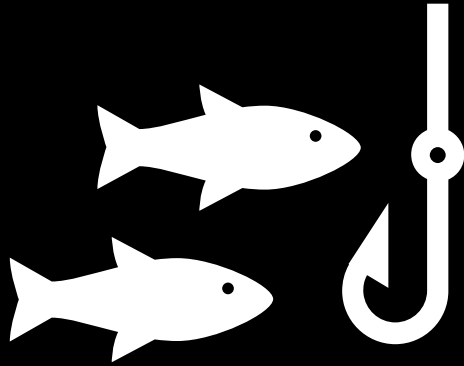
Dangerous Misconfiguration #1: Overly-permissive AD Object ACLs



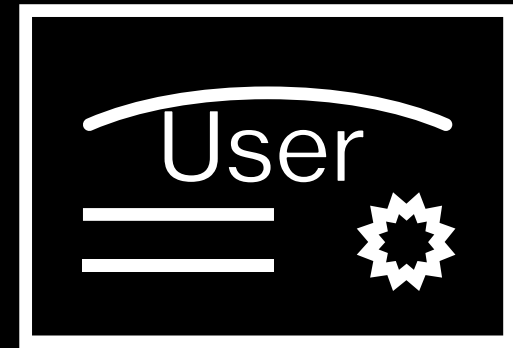
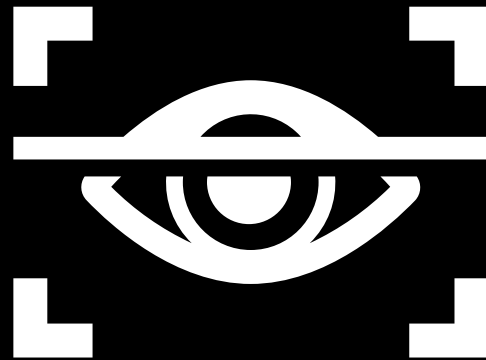
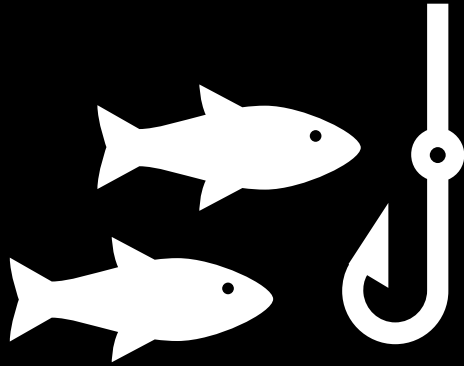
Example Attack: Overly-permissive AD Object ACLs



Example Attack: Overly-permissive AD Object ACLs

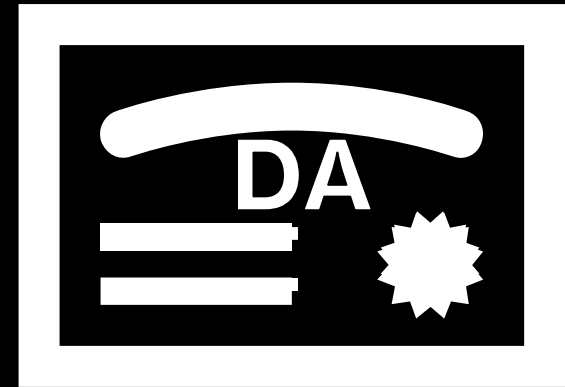
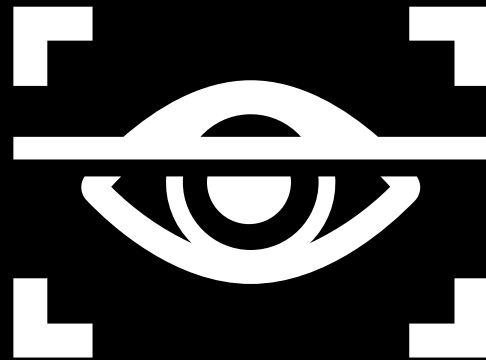
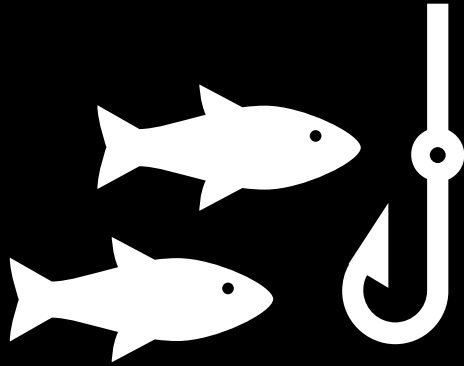


Example Attack: Overly-permissive AD Object ACLs



Example Attack:

Overly-permissive AD Object ACLs



Remediation:

Overly-permissive AD Object ACLs

- Safe configurations allow AD admins and PKI admins to modify objects in the PKS container but no one else.
- Identification:

```
$Safe_Users = "Domain Admins|Enterprise Admins|BUILTIN\Administrators|NT  
AUTHORITY\SYSTEM|$env:userdomain\Cert Publishers|$env:userdomain\Administrator"  
  
$DangerousRights = "GenericAll|WriteDacl|WriteOwner"  
  
foreach ( $object in $ADCS_Objects ) {  
    $BadACE = $object.nTSecurityDescriptor.Access | Where-Object {  
        ( $_.IdentityReference -notmatch $Safe_Users ) -and  
        ( $_.ActiveDirectoryRights -match $DangerousRights )  
    }  
    if ( $BadACE ) {  
        Write-Host "Object: $object" -ForegroundColor Red  
        $BadACE  
    }  
}
```


Remediation: Overly-permissive AD Object ACLs

- The results from this snippet will very likely include false positives. Consider this list a starting point for your own investigation!

```
Administrator: Windows PowerShell

PS C:\Users\Administrator> foreach ( $object in $ADCS_Objects ) {
>> $BadACE = $object.nTSecurityDescriptor.Access | Where-Object { ( $_.IdentityReference -notmatch $Safe_Users ) -and ( $_.ActiveD
irectoryRights -match $DangerousRights ) }
>> If ( $BadACE ) {
>> Write-Host "Object: $object" -ForegroundColor Red
>> $BadACE
>> }
>> }
Object: CN=horse-CA1-CA-1,CN=Enrollment Services,CN=Public Key Services,CN=Services,CN=Configuration,DC=horse,DC=local

ActiveDirectoryRights : CreateChild, DeleteChild, Self, WriteProperty, DeleteTree, Delete, GenericRead, WriteDacl, WriteOwner
InheritanceType       : All
ObjectType            : 00000000-0000-0000-0000-000000000000
InheritedObjectType   : 00000000-0000-0000-0000-000000000000
ObjectFlags           : None
AccessControlType      : Allow
IdentityReference      : HORSE\CA1$
IsInherited           : True
InheritanceFlags       : ContainerInherit, ObjectInherit
PropagationFlags       : None

Object: CN=NTAuthCertificates,CN=Public Key Services,CN=Services,CN=Configuration,DC=horse,DC=local
ActiveDirectoryRights : GenericAll
InheritanceType       : None
ObjectType            : 00000000-0000-0000-0000-000000000000
InheritedObjectType   : 00000000-0000-0000-0000-000000000000
ObjectFlags           : None
AccessControlType      : Allow
IdentityReference      : Everyone
IsInherited           : False
InheritanceFlags       : None
PropagationFlags       : None
```

<= False Positive!

Remediation: Overly-permissive AD Object ACLs

horse-User Properties

Subject Name Issuance Requirements

General Compatibility Request Handling Cryptography Key Attestation

Superseded Templates Extensions Security Server

Group or user names:

- Authenticated Users
- Administrator
- Domain Admins (HORSE\Domain Admins)
- Domain Users (HORSE\Domain Users)**
- Enterprise Admins (HORSE\Enterprise Admins)

Add... Remove

Permissions for Domain Users

	Allow	Deny
Full Control	<input type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Enroll	<input type="checkbox"/>	<input type="checkbox"/>
Autoenroll	<input type="checkbox"/>	<input type="checkbox"/>



horse-User Properties

Subject Name Issuance Requirements

General Compatibility Request Handling Cryptography Key Attestation

Superseded Templates Extensions Security Server

Group or user names:

- Authenticated Users
- Administrator
- Domain Admins (HORSE\Domain Admins)
- Domain Users (HORSE\Domain Users)**
- Enterprise Admins (HORSE\Enterprise Admins)

Add... Remove

Permissions for Domain Users

	Allow	Deny
Full Control	<input type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input type="checkbox"/>	<input type="checkbox"/>
Enroll	<input type="checkbox"/>	<input type="checkbox"/>
Autoenroll	<input type="checkbox"/>	<input type="checkbox"/>

Dangerous Misconfiguration #2: Templates with Bad Configs

- Templates options include:
 - Who can enroll/auto-enroll
 - Certificate purpose(s)/approved use(s)
 - Who is this certificate for?
 - Is approval required?
- If a normal user can specify the subject of the certificate, that *user can request a certificate on behalf of any other entity in the domain including a Domain Admin or Domain Controller.*
- *I've found at least one certificate that matches this description in nearly every environment I've assessed.*

Dangerous Misconfiguration #2: Templates with Bad Configs

horse-User Properties

Subject Name Issuance Requirements

General Compatibility Request Handling Cryptography Key Attestation

Superseded Templates Extensions Security Server

Group or user names:

- Authenticated Users
- Administrator
- Domain Admins (HORSE\Domain Admins)
- Domain Users (HORSE\Domain Users)**
- Enterprise Admins (HORSE\Enterprise Admins)

Add... Remove

Permissions for Domain Users

	Allow	Deny
Full Control	<input type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input type="checkbox"/>	<input type="checkbox"/>
Enroll	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Autoenroll	<input type="checkbox"/>	<input type="checkbox"/>

horse-User Properties

Subject Name Issuance Requirements

General Compatibility Request Handling Cryptography Key Attestation

Superseded Templates Extensions Security Server

To modify an extension, select it, and then click Edit.

Extensions included in this template:

- Application Policies**
- Basic Constraints
- Certificate Template Information
- Issuance Policies
- Key Usage

Edit...

Description of Application Policies:

- Client Authentication**
- Secure Email
- Encrypting File System

Dangerous Misconfiguration #2: Templates with Bad Configs

horse-User Properties

General Compatibility Request Handling Cryptography Key Attestation

Superseded Templates Extensions Security Server

Subject Name Issuance Requirements

☒ Supply in the request

☐ Use subject information from existing certificates for autoenrollment renewal requests

☐ Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format:

None

☐ Include e-mail name in subject name

Include this information in alternate subject name:

☐ E-mail name

☐ DNS name

☐ User principal name (UPN)

☐ Service principal name (SPN)

horse-User Properties

General Compatibility Request Handling Cryptography Key Attestation

Superseded Templates Extensions Security Server

Subject Name Issuance Requirements

Require the following for enrollment:

☐ CA certificate manager approval

☐ This number of authorized signatures: 0

If you require more than one signature, autoenrollment is not allowed.

Policy type required in signature:

Application policy:

Issuance policies:

Add...

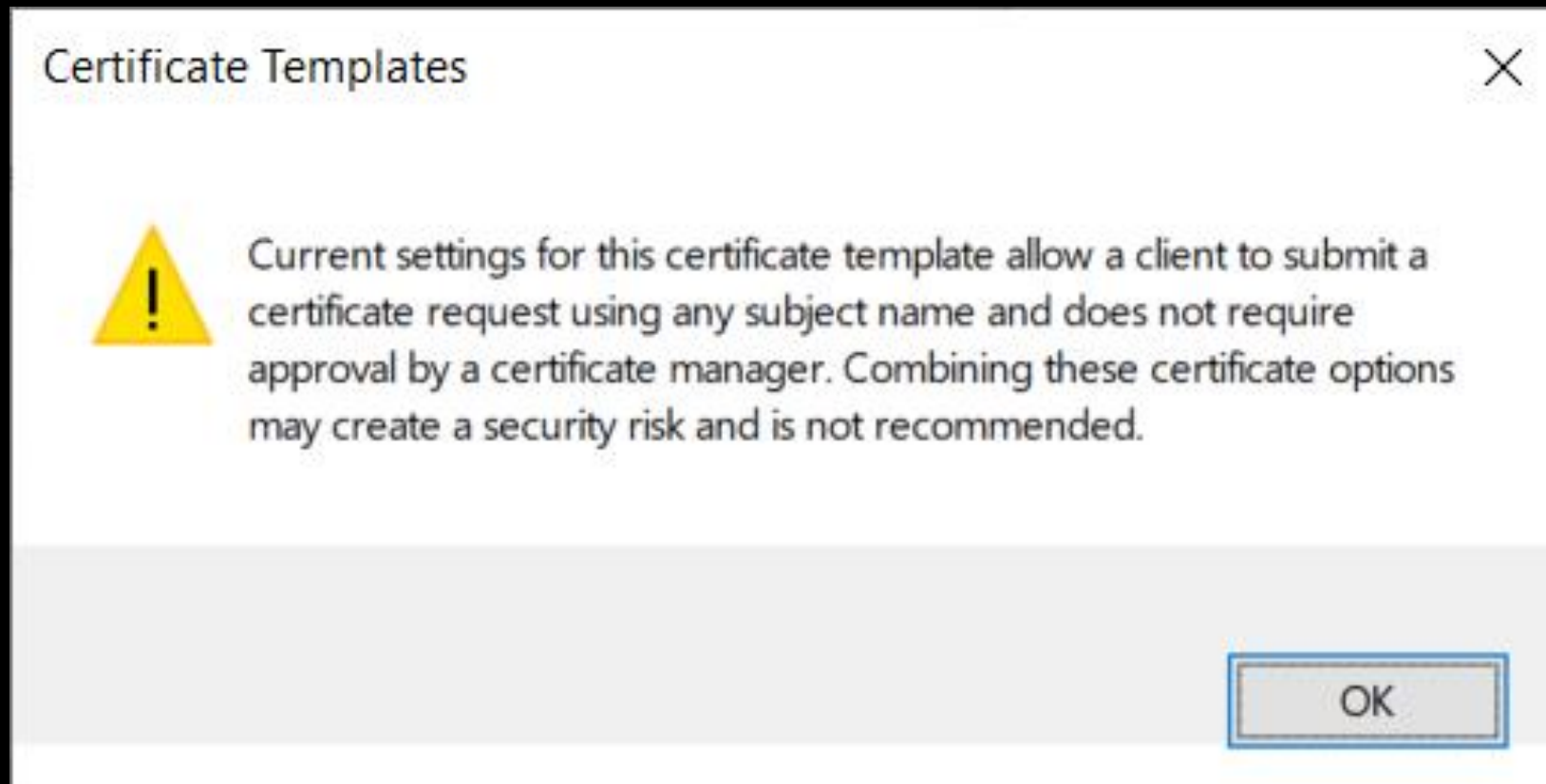
Remove

Require the following for reenrollment:

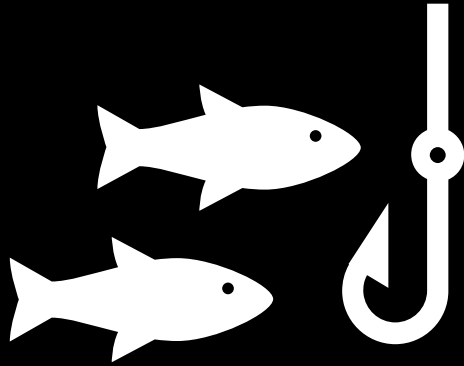
☒ Same criteria as for enrollment

☐ Valid existing certificate

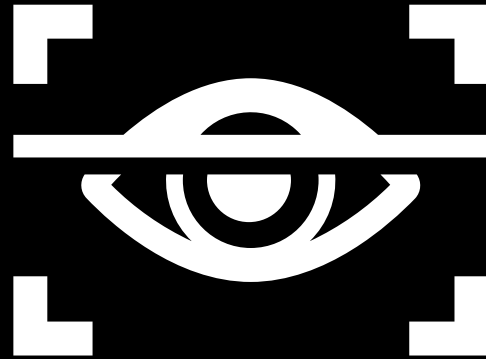
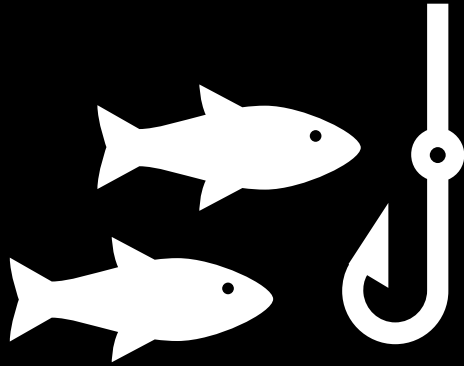
Dangerous Misconfiguration #2: Templates with Bad Configs



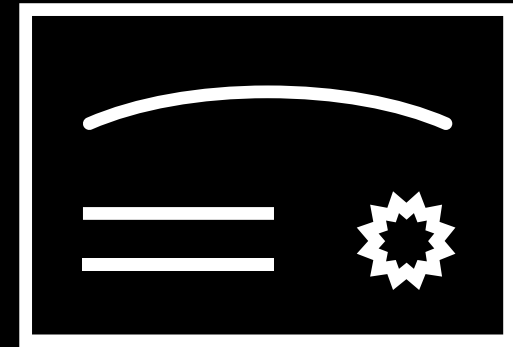
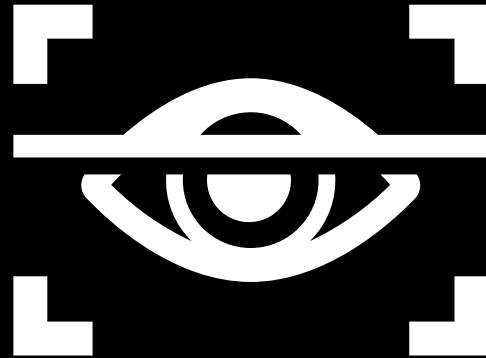
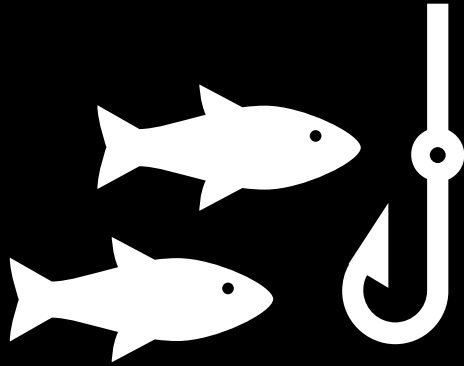
Example Attack: Templates with Bad Configs



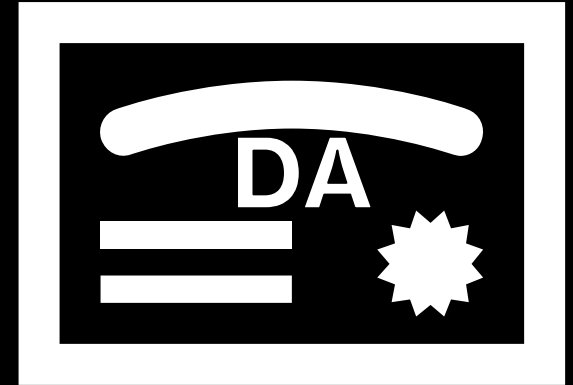
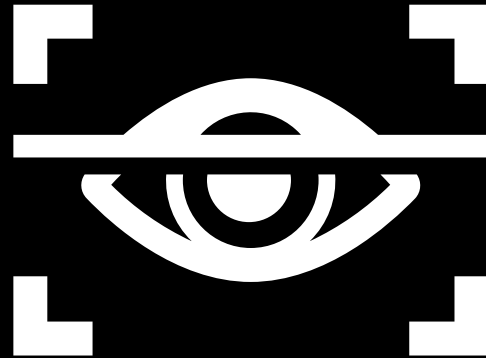
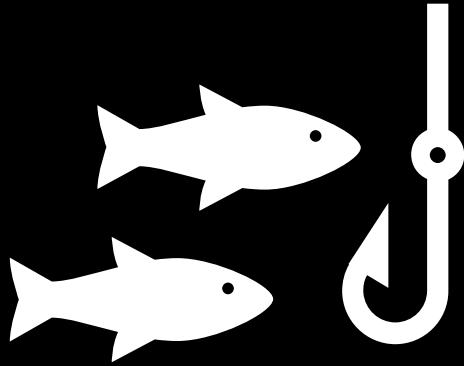
Example Attack: Templates with Bad Configs



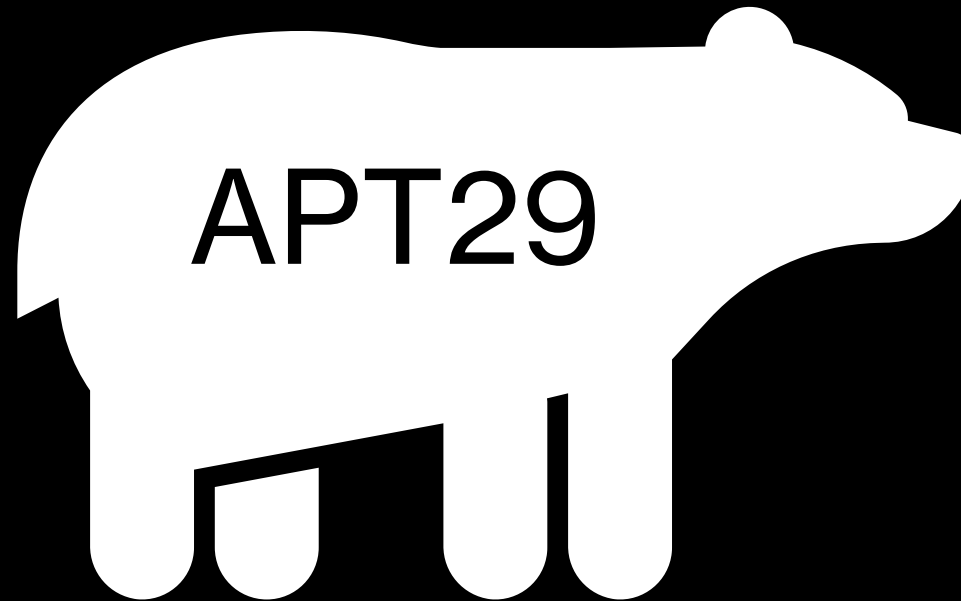
Example Attack: Templates with Bad Configs



Example Attack: Templates with Bad Configs



Example Attack: Templates with Bad Configs



<https://www.mandiant.com/resources/tracking-apt29-phishing-campaigns>

Remediation: Templates with Bad Configs

- Easy to find, slightly complex to fix
- Identification:

```
$ClientAuthEKUs = "1\3\6\1\5\5\7\3\2|  
1\3\6\1\5\2\3\4|  
1\3\6\1\4\1\311\20\2\2|  
2\5\29\37\0"  
  
$ADCS_Objects | Where-Object {  
    ($_.ObjectClass -eq "pKICertificateTemplate") -and  
    ($_.pkiExtendedKeyUsage -match $ClientAuthEKUs) -and  
    ($_.msPKI-Certificate-Name-Flag -eq 1) -and  
    ($_.msPKI-Enrollment-Flag -ne 2) -and  
    ( ($_.msPKI-RA-Signature -eq 0) -or ($null -eq $_.msPKI-RA-Signature) )  
} | Format-Table Name,DistinguishedName
```

Remediation: Templates with Bad Configs

- Results:

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> $ClientAuthEKUs = "1\3\6\1\5\5\7\3\2|1\3\6\1\5\2\3\4|1\3\6\1\4\1\311\20
\2\2|2\5\29\37\0"
>> $ADCS_Objects | Where-Object {
>> ($_.ObjectClass -eq "pKICertificateTemplate") -and
>> ($_.pkiExtendedKeyUsage -match $ClientAuthEKUs) -and
>> ($_.msPKI-Certificate-Name-Flag -eq 1) -and
>> ($_.msPKI-Enrollment-Flag -ne 2) -and
>> ( ($_.msPKI-RA-Signature" -eq 0) -or ($null -eq $_.msPKI-RA-Signature") )
>> } | Format-Table Name,DistinguishedName

Name                                     DistinguishedName
----
OfflineRouter                          CN=OfflineRouter,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Con...
horse-User                             CN=horse-User,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Config...
horse-Workstation Authentication       CN=horse-Workstation Authentication,CN=Certificate Templates,CN=Public Key Services...
```

Remediation:

Templates with Bad Configs

- Solution 1 – Prevent enrollee from self-assigning Subject Name

```
$ADCS_Objects_BadConfig = $ADCS_Objects | Where-Object {  
    ($_.ObjectClass -eq "pKICertificateTemplate") -and  
    ($_.pkiExtendedKeyUsage -match $ClientAuthEKUs) -and  
    ($_. "msPKI-Certificate-Name-Flag" -eq 1) -and  
    ($_. "msPKI-Enrollment-Flag" -ne 2) -and  
    ( ($_. "msPKI-RA-Signature" -eq 0) -or ($null -eq $_. "msPKI-RA-Signature") )  
}  
  
$ADCS_Objects_BadConfig | ForEach-Object {  
    $_. "msPKI-Certificate-Name-Flag" = 0  
}
```

Remediation: Templates with Bad Configs

horse-User Properties

Superseded Templates Extensions Security Server

General Compatibility Request Handling Cryptography Key Attestation

Subject Name Issuance Requirements

☒ Supply in the request

☐ Use subject information from existing certificates for autoenrollment renewal requests

☐ Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format:

None

☐ Include e-mail name in subject name

Include this information in alternate subject name:

☐ E-mail name

☐ DNS name

☐ User principal name (UPN)

☐ Service principal name (SPN)



horse-User Properties

Superseded Templates Extensions Security Server

General Compatibility Request Handling Cryptography Key Attestation

Subject Name Issuance Requirements

☐ Supply in the request

☐ Use subject information from existing certificates for autoenrollment renewal requests

☒ Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format:

Fully distinguished name

☐ Include e-mail name in subject name

Include this information in alternate subject name:

☐ E-mail name

☐ DNS name

☒ User principal name (UPN)

☐ Service principal name (SPN)

Remediation: Templates with Bad Configs

- Solution 2 – Require Manager Approval (lower chance of impact)

```
$ADCS_Objects_BadConfig = $ADCS_Objects | Where-Object {  
    ($_.ObjectClass -eq "pKICertificateTemplate") -and  
    ($_.pkiExtendedKeyUsage -match $ClientAuthEKUs) -and  
    ($_. "msPKI-Certificate-Name-Flag" -eq 1) -and  
    ($_. "msPKI-Enrollment-Flag" -ne 2) -and  
    ( ($_. "msPKI-RA-Signature" -eq 0) -or ($null -eq $_. "msPKI-RA-Signature") )  
}  
  
$ADCS_Objects_BadConfig | ForEach-Object {  
    $_. "msPKI-Enrollment-Flag" = 2  
}
```


Remediation: Templates with Bad Configs

horse-User Properties ? X

Superseded Templates Extensions Security Server

General Compatibility Request Handling Cryptography Key Attestation

Subject Name Issuance Requirements

Require the following for enrollment:

☐ A certificate manager approval

☐ This number of authorized signatures: 0

If you require more than one signature, autoenrollment is not allowed.

Policy type required in signature:

Application policy:

Issuance policies:

Add...

Remove



horse-User Properties ? X

Superseded Templates Extensions Security Server

General Compatibility Request Handling Cryptography Key Attestation

Subject Name Issuance Requirements

Require the following for enrollment:

☒ A certificate manager approval

☐ This number of authorized signatures: 0

If you require more than one signature, autoenrollment is not allowed.

Policy type required in signature:

Application policy:

Issuance policies:

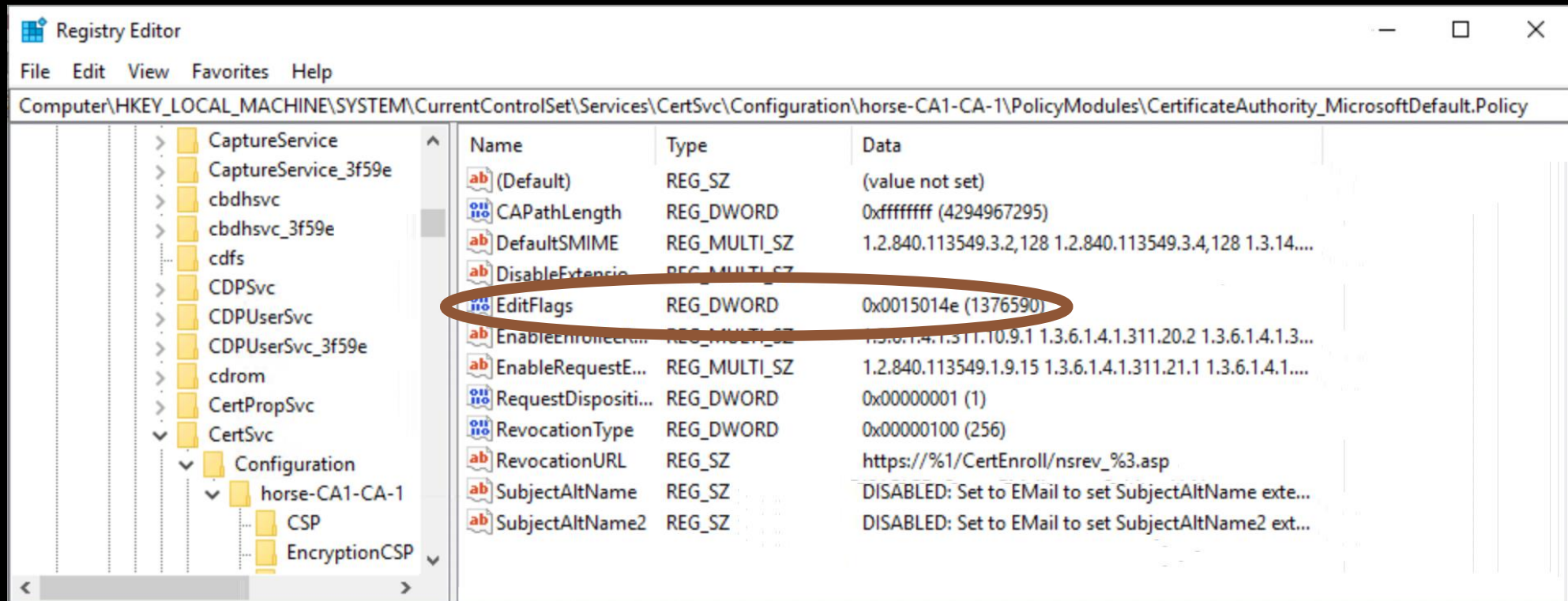
Add...

Remove

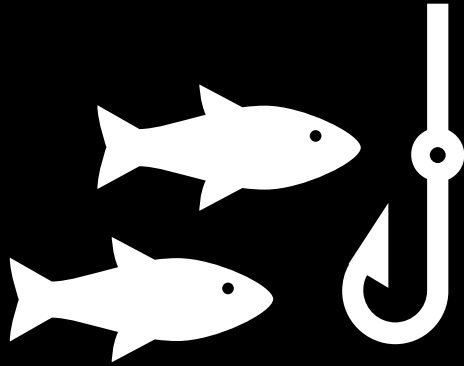
Dangerous Misconfiguration #3: Dangerous Flag on CA

- EDITF_ATTRIBUTESUBJECTALTNAME2 flag set on a CA
- Like previous issue, but worse. Much worse.
- This configuration allows a certificate requestor to specify an alternate subject on ANY template.
- Configured on each CA separately
- Found in environments where multiple PKIs exist or where cross-forest administration is being performed.

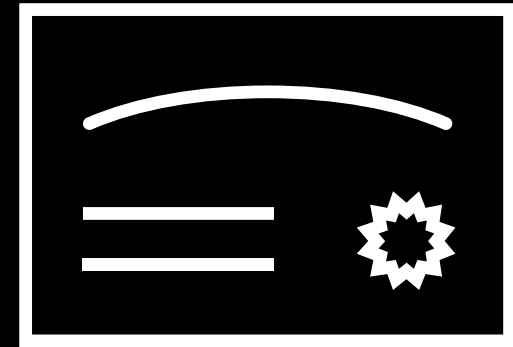
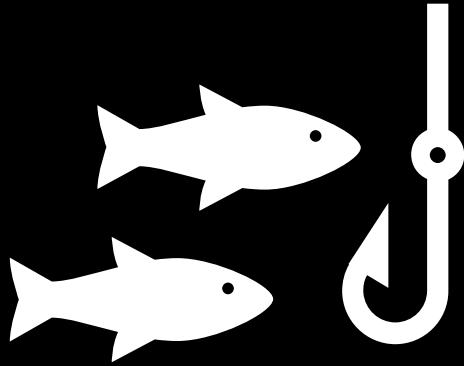
Dangerous Misconfiguration #3: Dangerous Flag on CA



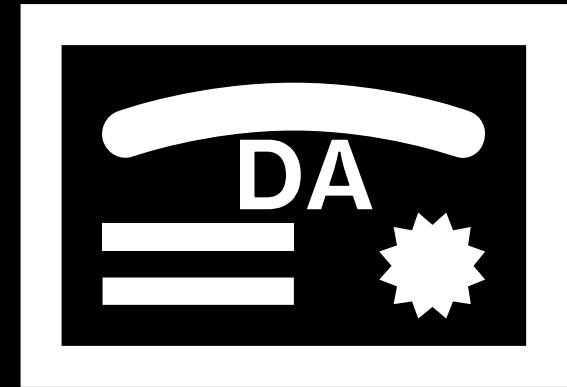
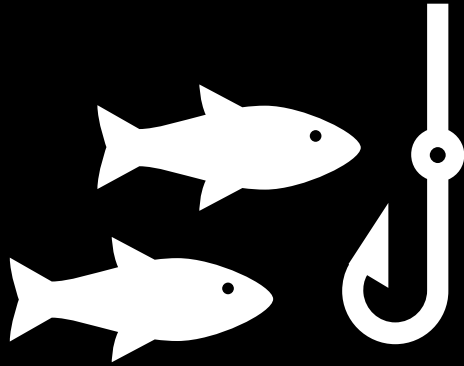
Example Attack: Dangerous Flag on CA



Example Attack: Dangerous Flag on CA



Example Attack: Dangerous Flag on CA



Remediation: Dangerous Flag on CA

- If this flag is set on all your CAs, remediating this issue will likely have operational impact depending on your exact PKI workflows.
- If the flag is only set on a subset of CAs, there *should* be no impact.



Remediation: Dangerous Flag on CA

- Identification

```
C:\>certutil -getreg policy\EditFlags
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\horse-CA1-
CA-1\PolicyModules\CertificateAuthority_MicrosoftDefault.Policy\EditFlags:

EditFlags REG_DWORD = 15014e (1376590)
  EDITF_REQUESTEXTENSIONLIST -- 2
  EDITF_DISABLEEXTENSIONLIST -- 4
  EDITF_ADDOLDKEYUSAGE -- 8
  EDITF_BASICCONSTRAINTSCRITICAL -- 40 (64)
  EDITF_ENABLEAKIKEYID -- 100 (256)
  EDITF_ENABLEDEFAULTSMIME -- 10000 (65536)
  EDITF_ATTRIBUTESUBJECTALTNAME2 -- 40000 (262144)
  EDITF_ENABLECHASECLIENTDC -- 100000 (1048576)
CertUtil: -getreg command completed successfully.
```

Remediation: Dangerous Flag on CA

- Unset the flag (output slightly edited for readability)

```
C:\>certutil -setreg policy\EditFlags -EDITF_ATTRIBUTESUBJECTALTNAME2  
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\horse-CA1-  
CA-1\PolicyModules\CertificateAuthority_MicrosoftDefault.Policy\EditFlags:
```

Old Value:

```
EditFlags REG_DWORD = 15014e (1376590)  
EDITF_ATTRIBUTESUBJECTALTNAME2 -- 40000 (262144)
```

New Value:

```
EditFlags REG_DWORD = 11014e (1114446)
```

CertUtil: -setreg command completed successfully.

The CertSvc service may need to be restarted **for** changes to take effect.



Let's Wrap This Up!

Quick Review!

- AD CS is incredibly easy to set up...
- ...And incredibly easy to screw up once it's deployed
- Remediation Plan:
 1. Do you really need AD CS? If yes, build or move to two-tier PKI if you aren't already there.
 2. Enable Auditing ASAP
 3. Remediate the most dangerous configurations
 4. Remediate overly permissive access controls and ownership
- Finally – protect CA hosts like the Tier 0 assets they are:
 - Limit local administrators to Domain Admins
 - Move CA computer objects to a top-level Organization Unit (OU)
 - Create separate Group Policy Objects for CAs OU
 - PKI Admins are Tier 0 too!

This seems like a lot of work.



- Tool in process: Locksmith
- Planned Features:
 - Check for any or all the misconfigurations
 - Create a report on each type of misconfiguration
 - Provide environment-specific code snippets to remediate any discovered issues
 - Easy button to just fix it!

If you'd like to assist with AD CS tooling development:

- GitHub: <https://github.com/TrimarcJake>
 - Code snippets shown in this presentation
 - Locksmith
- Email: jakehildreth (at) trimarcsecurity [dot] com
I would love to collaborate on AD security projects or assess your AD
- Twitter: <https://twitter.com/dotdotdotHorse>
Mostly weird humor with a smidge of infosec sprinkled in
- LinkedIn: <https://linkedin.com/jakehildreth>
Probably not the best way to contact me

Thanks!

- Will Schroeder and Lee Christensen, Christoph Falta, Brian Komar, Pete Long, Vadims Podans, Ned Pyle, Elad Shamir, Carl Sörqvist for providing the shoulders for me to stand on
- Sean Metcalf & Brandon Colley for reviewing these slides and providing feedback on overall presentation
- The rest of the Trimarc team for sitting through my dress rehearsal
- My wife for listening to me yammer on about this stuff
- My daughter for helping me get my explanations to a point where an 8y/o can (mostly) understand them

Resources

- Long, Pete. “Microsoft PKI Planning and Deploying Certificate Services.” *PeteNetLive*, 1 July 2020, www.petenetlive.com/KB/Article/0001309.
- Podāns, Vadims. “Enabling Active Directory Certificate Services (ADCS) Advanced Audit.” PKI Solutions Inc., 12 Aug. 2021, www.pkisolutions.com/enabling-active-directory-certificate-services-adcs-advanced-audit.
- Schroeder, Will. “Certified Pre-Owned - Posts By SpecterOps Team Members.” *Medium*, 6 Jan. 2022, posts.specterops.io/certified-pre-owned-d95910965cd2.
- “Securing PKI: Technical Controls for Securing PKI.” *Microsoft Docs*, 31 Aug. 2016, [docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn786426\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn786426(v=ws.11)).
- Wolfram, John, et al. “Trello From the Other Side: Tracking APT29 Phishing Campaigns.” *Mandiant*, 28 Apr. 2022, www.mandiant.com/resources/tracking-apt29-phishing-campaigns.