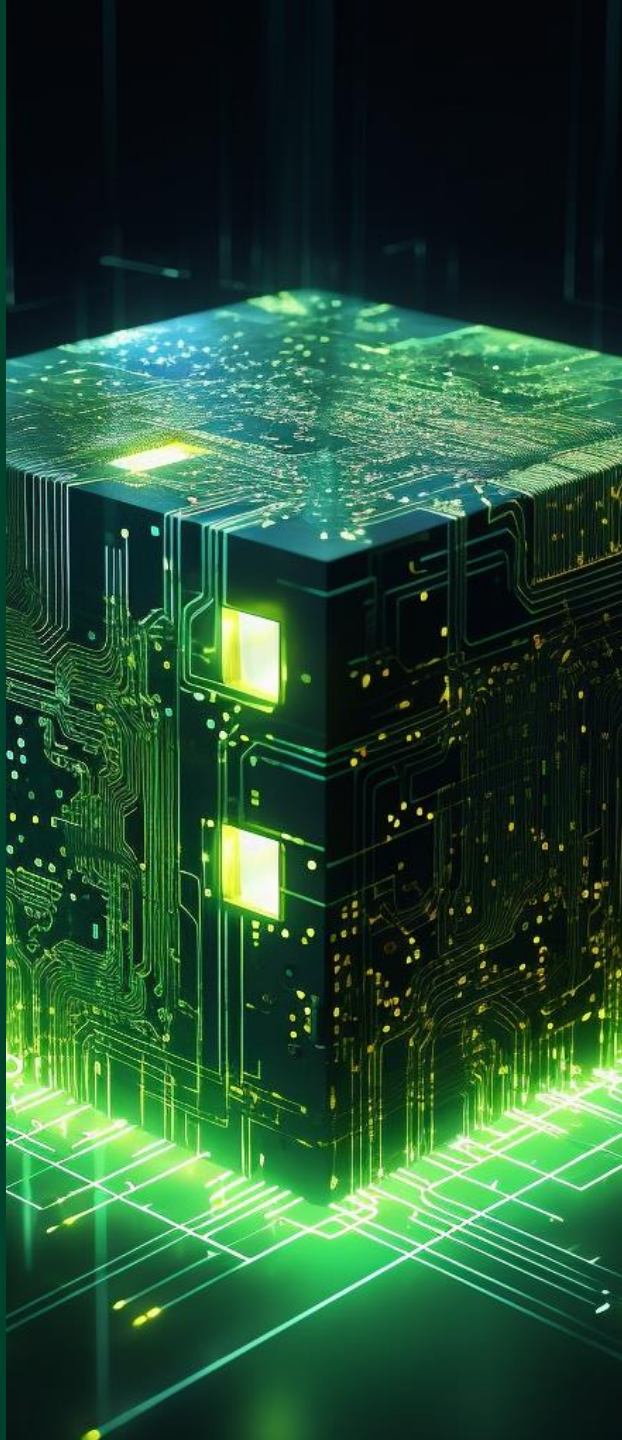
The One Step Most Organizations Miss with Active Directory

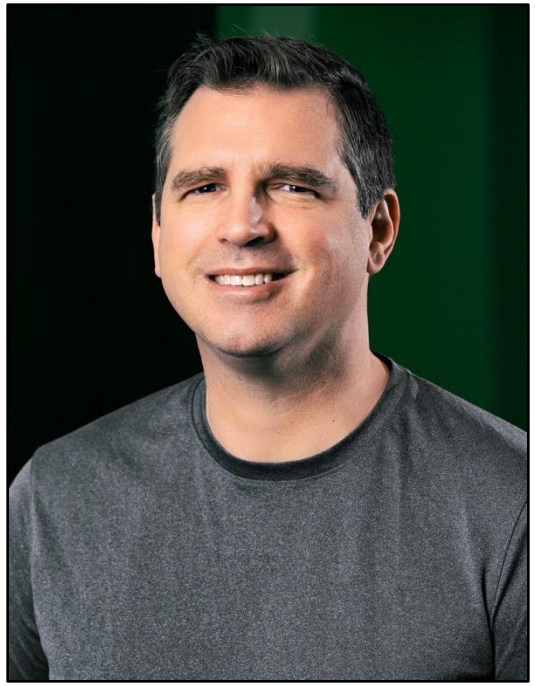
Presented by: Sean Metcalf & Paul Sems

TRUSTEDSEC



TRUSTEDSEC

Presenting Today



Sean Metcalf
Identity Security Architect

Paul Sems
Managing Director of Remediation Services

Agenda

- Storytime with Paul
  - 3 Stories describing real world issues
- Key Security Configuration Issues Presented by Sean
- Wrap-up & Conclusion

Storytime #1

Administrative Hygiene & Excessive Delegation

Story #1 – Key Takeaways

- **Administrative hygiene**
  - Default domain Administrator account
  - Active Directory Admins membership
  - Active Directory built-in groups membership
- **Delegation at the domain root**
  - Groups delegated full control permissions on the domain

Administrative Hygiene: Default Domain Administrator

- The password should be current
- Any logons should be known and logged
- Account should be reserved as an emergency account (“break glass)
- There should be no Kerberos Service Principal Name associated
- Renaming the account doesn’t provide additional security but can reduce unsuccessful logon false positives

```
Name          Enabled Created              PasswordLastSet      LastLogonDate        ServicePrincipalName
----          ------- -------              ---------------      -------------        --------------------
Administrator    True 11/10/2019 3:36:51 PM 5/19/2020 4:32:44 PM 5/11/2020 1:16:56 PM {MSSQLSvc/GammaDB23:1434, MSSQLSvc/
```


https://github.com/PyroTek3/Misc/blob/main/Get-ADDefaultAdministrator.ps1

Administrative Hygiene: Active Directory Admins

- Passwords should be current
- Any inactive accounts should be disabled & removed
- There should be no computer accounts listed
- Kerberos pre-authentication should always be required
- Question whether service account members should have full Active Directory privileges
- There should be no Kerberos Service Principal Name associated with admin accounts associated with people

SamAccountName	ObjectClass	PasswordLastSet	LastLogonDate	Enabled	DoesNotRequirePreAuth	UseDESKeyOnly	PasswordNeverExpires	ServicePrincipalName
AdminBriella	user	8/2/2025 10:13:20 PM	8/12/2025 5:22:27 PM	False	False	False	False	{}
AdminCarsonR	user	8/12/2025 2:18:17 PM		True	False	False	True	{}
AdminClaireM	user	8/12/2025 2:18:17 PM	8/12/2025 5:22:28 PM	False	False	False	False	{}
AdminCristian	user	8/2/2025 10:13:20 PM	8/12/2025 5:22:27 PM	True	False	True	False	{MSSQLSvc/Iota78:1433}
AdminDreamR	user	8/12/2025 2:18:17 PM		True	False	False	False	{}
AdminEmilioG	user	8/12/2025 2:18:17 PM	8/12/2025 5:22:27 PM	True	True	False	True	{}
Administrator	user	7/15/2025 11:20:23 AM	8/12/2025 5:22:17 PM	True	False	False	True	{}
AdminMichael	user	8/2/2025 10:13:20 PM	8/12/2025 5:22:27 PM	True	False	False	True	{}
AdminOakleyA	user	8/12/2025 2:18:16 PM	8/12/2025 5:22:29 PM	False	False	False	False	{}
AdminSaintW	user	8/12/2025 2:18:17 PM		True	True	True	False	{}
adminSean	user	7/15/2025 3:09:36 PM	9/2/2025 11:21:50 AM	True	False	False	True	{}
AdminSergio	user	8/2/2025 10:13:20 PM	8/12/2025 5:22:29 PM	True	True	False	False	{}
AdminTanner	user	8/2/2025 10:13:21 PM	8/12/2025 5:22:27 PM	True	False	False	False	{}
GammaDB33$	computer	8/12/2025 3:55:35 PM		True	False	False	False	{}
svc-CiscoUnity	user	8/20/2025 11:06:21 AM	8/12/2025 5:22:26 PM	True	False	False	False	{}
svc-Cognos	user	8/12/2025 2:18:09 PM	8/12/2025 5:22:23 PM	True	False	False	False	{}
svc-Kafka	user	8/12/2025 2:17:23 PM	8/12/2025 5:27:15 PM	False	False	False	False	{}
svc-OpenAccess	user	8/12/2025 2:17:59 PM	8/12/2025 5:27:13 PM	True	False	False	True	{}
svc-SharePoint	user	8/12/2025 2:17:28 PM	8/12/2025 5:22:28 PM	True	False	False	True	{}

https://github.com/PyroTek3/Misc/blob/main/Get-ADAdmins.ps1

Administrative Hygiene: Default AD Groups

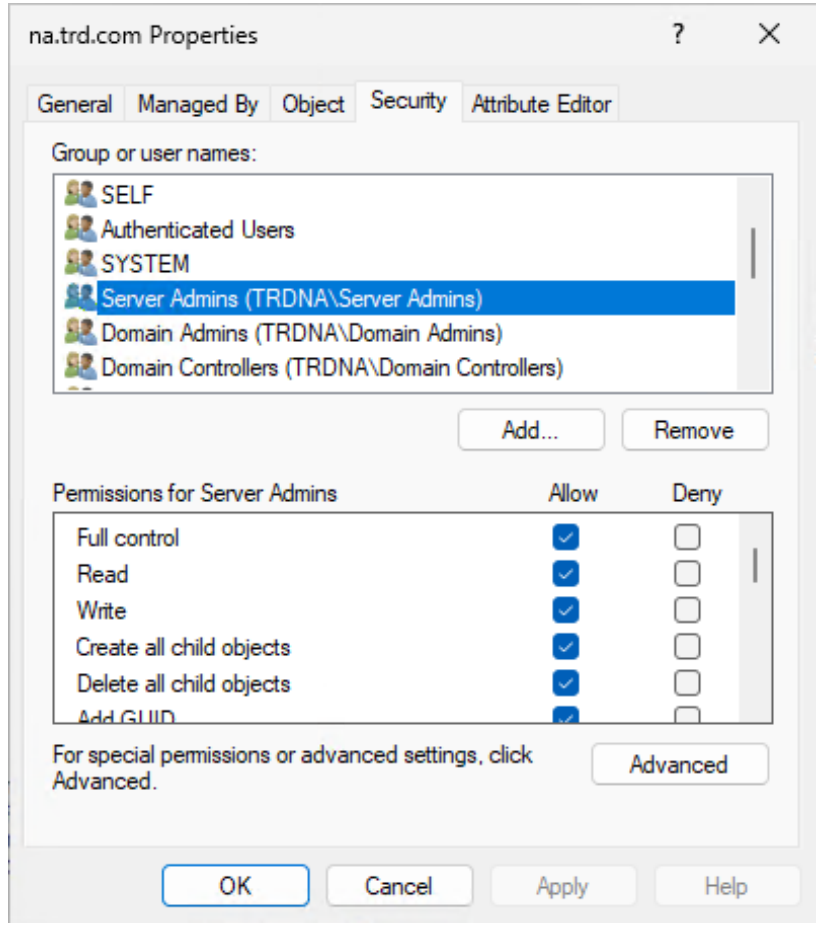
- The following groups should be empty:
  Account Operators, Group Policy Creator Owners, Print Operators, & Schema Admins
- Backup Operators membership should be limited to service accounts that require the ability to AD backup/restore
- DNSAdmins should be limited to only those that require DNS administrative rights
- Server Operators are effectively Domain Controller admins & should be limited

GroupName	MemberCount	Members
Account Operators	6	AdminEmilioG,AdminDreamR,AdminOakleyA,svc-Cloudera,svc-CiscoUnity,svc-PaloAlto
Backup Operators	7	svc-CommVault,SVC-VMWARE,AdminEmilioG,AdminSaintW,svc-CiscoUnity,svc-SharePoint,AdminSergio
DNSAdmins	7	AdminEmilioG,AdminSaintW,AdminAuroraM,AdminOakleyA,svc-Cognos,svc-OpenAccess,AdminTanner
Enterprise Key Admins	5	AdminCarsonR,AdminClaireM,AdminAuroraM,AdminMichael,AdminSergio
Event Log Readers	4	svc-PKI1,SVC-VMWARE,AdminSaintW,AdminDreamR
Group Policy Creator Owners	5	Administrator,AdminOakleyA,AdminSaintW,AdminEmilioG,AdminCarsonR
Print Operators	6	AdminOakleyA,svc-OpenAccess,svc-Oracle,svc-Cloudera,AdminMichael,AdminSergio
Server Operators	6	AdminCarsonR,AdminNavyM,svc-Oracle,svc-PaloAlto,AdminMichael,AdminBriella
Schema Admins	4	AdminCarsonR,AdminOakleyA,AdminMichael,Administrator

https://github.com/PyroTek3/Misc/blob/main/Get-ADBuiltInAdmins.ps1

Domain Level Permission Issues

- Often implemented to solve something now
- Potential impact in the future
- Permissions delegated at the domain root typically have more permissions than intended
- Should be configured to be more granular



Workstation Admins (TRDNA\Workstation Admins) Allow Full control None Descendant Computer objects

Immediate Actions: Improving AD Admin Account Security

- Limit accounts in privileged AD admin groups
- Ensure AD admin accounts have current passwords – no passwords should be 15 years old
- Assume no service accounts need to be in AD admin groups
- Ensure no AD admin accounts associated with people have Kerberos Service Principal Names (SPNs)
- Ensure all AD admin accounts associated with people have “sensitive” bit set and are members of the Protected Users group (eventually)
- Disable accounts that are no longer in use (and eventually remove from privileged groups)

Immediate Actions: Domain Level Permissions

- Review security permissions configured at the domain root
- Scrutinize the following permissions:
  - GenericAll (Full Control), WriteDACL (Change Permissions), WriteOwner (Change Owner), and DS-Replication-Get-Changes-All
- Ensure that granular permissions are delegated at the OU level where it makes sense

Storytime #2

Virtual Infrastructure

Story #2 – Key Takeaways

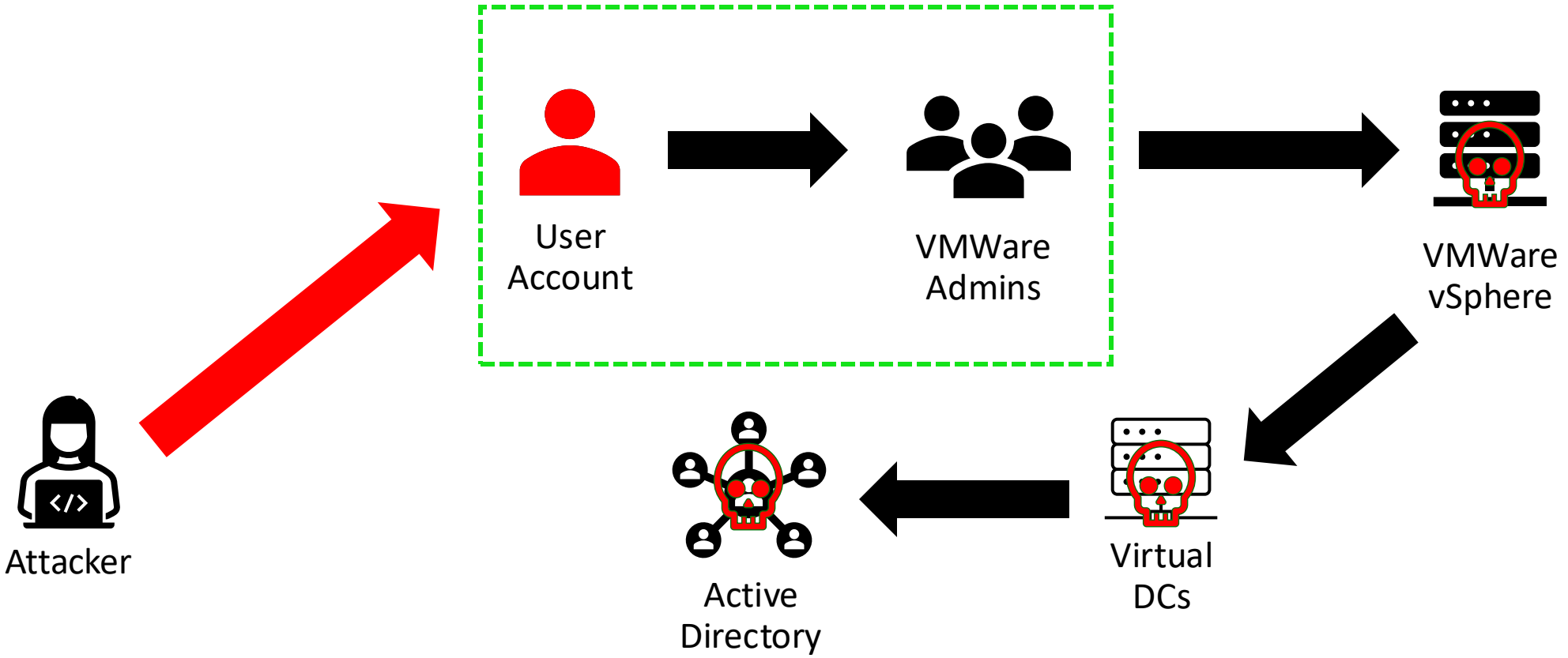
- Adversary compromises non-admin account that is a member of VMware admins group
- VMware environment compromised
- Captured virtual disk associated with virtual Domain Controller
- Extracts sensitive information such as password hashes from Active Directory database file (ntds.dit)

Note: VMware is used in this section since it is an extremely popular solution. Most of the virtual platforms have the same capability.

User in the VMware Admins Group

```
PS C:\users\Sean> Get-ADGroupMember 'VMware Admins'


distinguishedName : CN=AdminSylasT,OU=Accounts,OU=AD Administration,DC=na,DC=trd,DC=com
name              : AdminSylasT
objectClass       : user
objectGUID        : 8de7efaa-7a25-4b12-9823-7854714b1174
SamAccountName    : AdminSylasT
SID               : S-1-5-21-3414064619-3552714665-383130355-2334

distinguishedName : CN=AdminTheoW,OU=Accounts,OU=AD Administration,DC=na,DC=trd,DC=com
name              : AdminTheoW
objectClass       : user
objectGUID        : c0b8582d-72e7-4820-95fc-1ab74a210389
SamAccountName    : AdminTheoW
SID               : S-1-5-21-3414064619-3552714665-383130355-2337

distinguishedName : CN=AdminBellaC,OU=Accounts,OU=AD Administration,DC=na,DC=trd,DC=com
name              : AdminBellaC
objectClass       : user
objectGUID        : ef86a0d2-4080-4c8c-a9fb-72a4657bcc52
SamAccountName    : AdminBellaC
SID               : S-1-5-21-3414064619-3552714665-383130355-2342

distinguishedName : CN=AdminErikG,OU=Accounts,OU=AD Administration,DC=na,DC=trd,DC=com
name              : AdminErikG
objectClass       : user
objectGUID        : ab14a310-3607-4a5f-bdfb-97f06cb8c6f3
SamAccountName    : AdminErikG
SID               : S-1-5-21-3414064619-3552714665-383130355-2346

distinguishedName : CN=Angela.Mitchell,OU=Domain Users,DC=na,DC=trd,DC=com
name              : Angela.Mitchell
objectClass       : user
objectGUID        : 751477db-ced8-4f1d-9f17-64d6a916f0f7
SamAccountName    : Angela.Mitchell
SID               : S-1-5-21-3414064619-3552714665-383130355-2490
```

VMware to Active Directory



ESX Admins group gets Full VMware rights

- When a ESXi server is domain-joined, it assumes any "ESX Admins" group in Active Directory & its members should have full VMware admin rights
- Anyone who can create & manage a group in AD (if the group doesn't exist), can get full admin rights to the VMware ESX hypervisors joined to AD
- Storm-0506, Storm-1175, Octo Tempest, & Manatee Tempest leveraged this configuration to compromise Domain Controllers
- Tracked as CVE-2024-37085 for ESXi 7.0 & 8.0

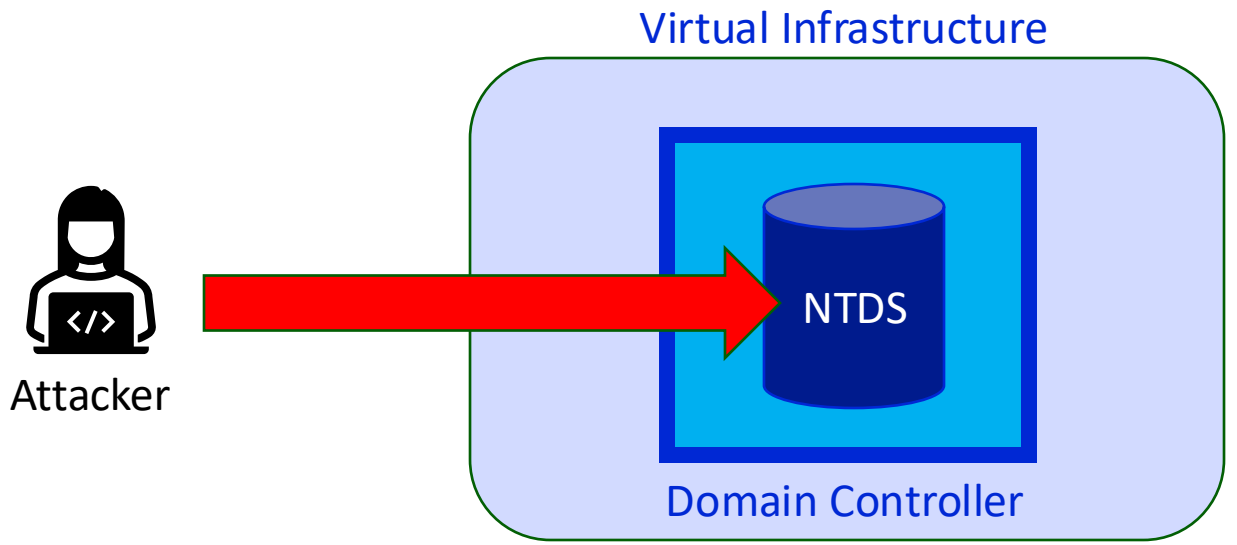
By default, an ESXi host joined to an AD domain queries the domain for the ESX Admins group, and this behavior is not configurable. If the group exists in AD, it is granted the Administrator role on the host, and any user accounts in that group receive full administrative privileges on the host and can log in to the host through SSH. https://knowledge.broadcom.com/external/article?legacyId=1025569

TRUSTEDSEC

https://www.microsoft.com/en-us/security/blog/2024/07/29/ransomware-operators-exploit-esxi-hypervisor-vulnerability-for-mass-encryption/ July 29, 2024

Attacker Capability

- Snapshot the existing virtual hard drive associated with the virtual Domain Controller then extract data
- Create a clone of the virtual Domain Controller and capture the Active Directory database file (ntds.dit)
- Shutdown the virtual Domain Controller and edit the Active Directory database file directly on disk then restart the DC



Immediate Actions

- Don’t domain join ESXi hosts
- Evaluate disconnecting vCenter from Active Directory
- Review VMware admins groups (including ESX Admins) and ensure only appropriate admin accounts are members
- Ensure vCenter is limited to an admin network and not accessible from the main corporate network
- Longer term: Leverage Domain Controller disk encryption (BitLocker) to prevent offline attacks

Storytime #3

Active Directory Certificate Services (ADCS)

Story #3 – Key Takeaways

- Active Directory Certificate Services (ADCS) enabled AD compromise
- No auditing is configured in ADCS by default
- Default ADCS settings are not secure
- Dangerous configurations with ADCS templates are easy to create

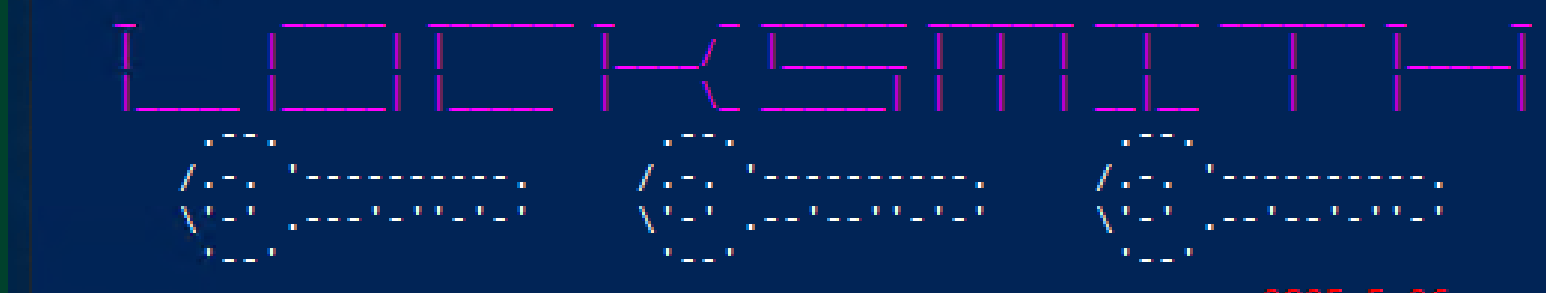
Templates with Dangerous Configs

- **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****.*
- ***TrustedSec has found at least one certificate that matches this description in ~95% of the environments we've assessed.***

Immediate Actions: Locksmith

```
PS C:\users\sean> invoke-locksmith
```



```
                                                    v2025.5.26
Gathering AD CS Objects from trd.com...
Identifying auditing issues...
Identifying AD CS templates with dangerous ESC1 configurations...
Identifying AD CS templates with dangerous ESC2 configurations...
Identifying AD CS templates with dangerous ESC3 configurations...
Identifying AD CS templates with poor access control (ESC4)...
Identifying AD CS objects with poor access control (ESC5)...
Identifying Certificate Authorities with EDITF_ATTRIBUTESUBJECTALTNAME2 enabled (ESC6)...
Identifying Certificate Authorities with Non-Standard Admins (ESC7)...
Identifying HTTP-based certificate enrollment interfaces (ESC8)...
Identifying AD CS templates with szOID_NTDS_CA_SECURITY_EXT disabled (ESC9)...
Identifying Certificate Authorities with IF_ENFORCEENCRYPTICERTREQUEST disabled (ESC11)...
Identifying AD CS templates with dangerous ESC13 configurations...
Identifying AD CS templates with dangerous ESC15 configurations...
Identifying Certificate Authorities with szOID_NTDS_CA_SECURITY_EXT disabled (ESC16)...
```


https://github.com/jakehildreth/Locksmith

Immediate Actions: Locksmith

```
-------------------------------------------------------------
     ESC15 - Vulnerable Certificate Template - Schema V1
-------------------------------------------------------------

Technique   Template Name Risk Enabled Issue
---------   ------------- ---- ------- -----
ESC15/EKUwu User          High    True User uses AD CS Template Schema Version 1, and TRDRoot\Domain Users
                                       is allowed to enroll in this template.

                                       If patches for CVE-2024-49019 have not been applied it may be possible to include
                                       arbitrary Application Policies while enrolling in this template, including
                                       Application Policies that permit Client Authentication or allow the creation
                                       of Subordinate CAs.

                                       More info:
                                         - https://trustedsec.com/blog/ekuwu-not-just-another-ad-cs-esc
                                         - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49019

ESC15/EKUwu EFS           High    True EFS uses AD CS Template Schema Version 1, and TRDRoot\Domain Users
                                       is allowed to enroll in this template.

                                       If patches for CVE-2024-49019 have not been applied it may be possible to include
                                       arbitrary Application Policies while enrolling in this template, including
                                       Application Policies that permit Client Authentication or allow the creation
                                       of Subordinate CAs.

                                       More info:
                                         - https://trustedsec.com/blog/ekuwu-not-just-another-ad-cs-esc
                                         - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49019

ESC15/EKUwu Machine       High    True Machine uses AD CS Template Schema Version 1, and TRDRoot\Domain Computers
                                       is allowed to enroll in this template.

                                       If patches for CVE-2024-49019 have not been applied it may be possible to include
                                       arbitrary Application Policies while enrolling in this template, including
                                       Application Policies that permit Client Authentication or allow the creation
                                       of Subordinate CAs.

                                       More info:
                                         - https://trustedsec.com/blog/ekuwu-not-just-another-ad-cs-esc
                                         - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49019
```


https://github.com/jakehildreth/Locksmith

Immediate Actions: Run Locksmith in Mode 1

```
---------------------------------
    Auditing Not Fully Enabled
---------------------------------


Technique          : DETECT
CA Name            : trd-TRD-ROOT-ADCS1-CA
Risk               : Medium
DistinguishedName  : CN=trd-TRD-ROOT-ADCS1-CA,CN=Enrollment Servic
Issue              : Auditing is not fully enabled on TRD-Root-ADC
Fix                : certutil.exe -config 'TRD-Root-ADCS1.trd.com\
                     Invoke-Command -ComputerName 'TRD-Root-ADCS1.
                         Get-Service -Name 'certsvc' | Restart-Ser
                     }
Risk Score         : 3
Risk Score Detail  : Base Score: 3
```

```
-----------------------------------------------------
    ESC5 - Vulnerable Access Control - PKI Object
-----------------------------------------------------


Technique          : ESC5
Object Name        : TRD-ROOT-ADCS1
Risk               : High
DistinguishedName  : CN=TRD-ROOT-ADCS1,CN=Computers,DC=trd,DC=com
objectClass        : computer
Issue              : BUILTIN\Account Operators has GenericAll elevated rights
                     on this computer object.

                     This computer is hosting a Certification Authority (CA). It is likely
                     BUILTIN\Account Operators can take control of this object.

                     There is little reason for anyone other than AD Admins to have elevated rights
                     to this CA host.

Fix                : $ACL = Get-Acl -Path 'AD:CN=TRD-ROOT-ADCS1,CN=Computers,DC=trd,DC=com'
                     foreach ( $ace in $ACL.access ) {
                         if ( ($ace.IdentityReference.Value -like 'BUILTIN\Account Operators' ) -and
                             ( $ace.ActiveDirectoryRights -notmatch '^ExtendedRight$') ) {
                             $ACL.RemoveAccessRule($ace) | Out-Null
                         }
                     }
                     Set-Acl -Path 'AD:CN=TRD-ROOT-ADCS1,CN=Computers,DC=trd,DC=com' -AclObject $ACL
Risk Score         : 4
Risk Score Detail  : Base Score: 0
                     Unprivileged Principal: +1
                     Unprivileged Principal: +1
                     Certification Authority Host Computer: +2
```

TRUSTEDSEC

https://github.com/jakehildreth/Locksmith

So, What Is The One Step Most Organizations Miss with Active Directory?

Proactive Security Assessment

- Perform a proactive security assessment before a penetration test or Red Team engagement
- Prioritize High priority issues and identify quick wins
- Remediate the high priority issues that can be resolved more quickly
- You can perform your own security review, though a more comprehensive audit is highly recommended

https://www.hub.trimarcsecurity.com/post/securing-active-directory-performing-an-active-directory-security-review

TrustedSec Proactive Security Assessments

- Active Directory Security Assessment (ADSA)
- Microsoft 365 Cloud Security Assessment (MCSA)
- Certificate Services
- Endpoints & Intune
- Backup Infrastructure
- Azure Infrastructure
- AWS Infrastructure
- Professional Services

https://trustedsec.com/services/harden

Conclusion

- It is critical to identify security issues Active Directory environment before the attackers.
- Perform a proactive AD security assessment
- After this assessment, build a project plan to fix the high priority issues with the lowest level of effort.
- Resolve the quick wins.

New Article: Password Spray Detection

Password-spray detection typically relies on correlating failed logins over time, but this often leads to false positives. In our latest blog, Identity Security Architect Sean Metcalf shares how to detect password-spraying more accurately by leveraging a honeypot account.

https://trustedsec.com/blog/detecting-password-spraying-with-a-honeypot-account

REFERENCES AND ADDITIONAL READING

- **Locksmith**
  https://github.com/jakehildreth/Locksmith
- **PowerPUG – for moving AD Admins into Protected Users group**
  https://github.com/jakehildreth/PowerPUG
- **Misc PowerShell Scripts**
  https://github.com/PyroTek3/Misc
- **Password Spray Detection**
  https://trustedsec.com/blog/detecting-password-spraying-with-a-honeypot-account
- **Perform your own Active Directory security review**
  https://www.hub.trimarcsecurity.com/post/securing-active-directory-performing-an-active-directory-security-review

TRUSTEDSEC

FOLLOW US @TRUSTEDSEC

The information security industry is constantly evolving – keep up by following TrustedSec's active social media, blogs, podcasts and webinars.

TrustedSec.com

TRUSTEDSEC

THANK YOU!