Active Directory Tricks and Hidden Features

Pierre Audonnet

CSA - Microsoft Canada

QUIZ 1/2 Are those two commands doing the same thing?

- ping 10.0.0.10
- ping 10.0.0.010

SECTOR BRIEFINGS
October 25-26, 2023
METRO TORONTO CONVENTION CENTRE

QUIZ 2/2 Are those two commands doing the same thing?

- regedit.exe
- regedt32.exe

🎯 Objectives

0 Learn about quirks and oddities of the good old AD

1 Gain practical knowledge on features you can use today

2 Identify new points of control for defenders to better detect attacks

3 Identify new ways for attackers to hide or stay persistent

Pierre Audonnet

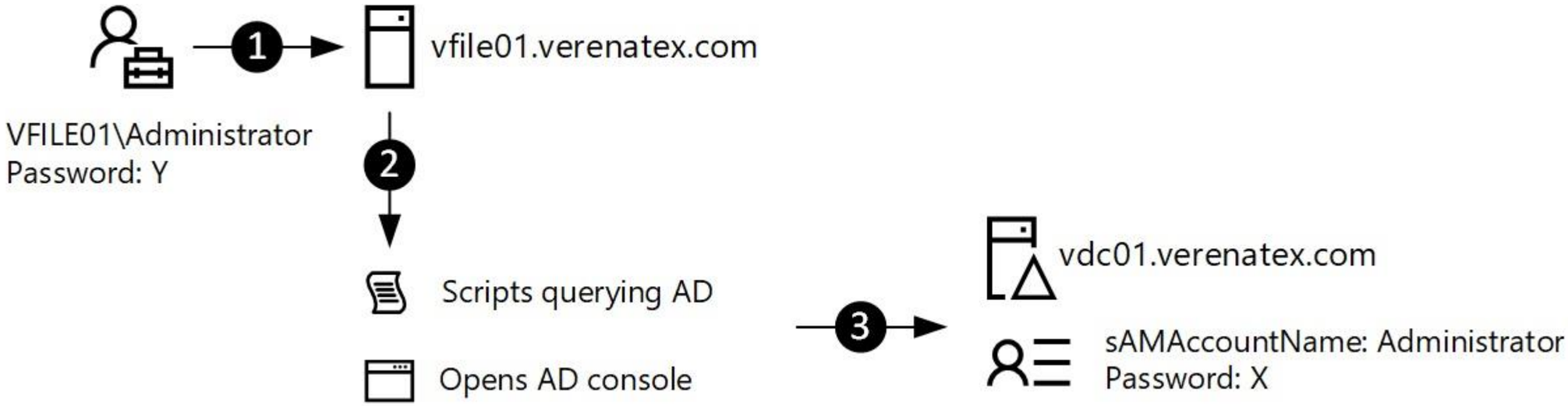
- PFE > CE > CSA-E > CSA
- ADRAP / Security Assessment
- Sentinel/Defender
- KQL, Logic Apps, wine

December 1999

Should I rename my admin account?

This doesn't seem to help to "hide" the account.

But it can help overall because of 🗀 **Q103390**



VFILE01\Administrator
Password: Y

Will that really lock out my account?

pwdProperties

- DOMAIN_LOCKOUT_ADMINS

Replication metadata is data too

Metadata is not here for auditing. It shows **WHAT** happened. Not **WHO** did it.

BUT it doesn't mean it doesn't have a value during investigations!

- The metadata was there before your SIEM
- Group membership tracking
- AES key generation
- …

SECTOR

```
C:\Users\administrator>repadmin /showobjmeta . "CN=Domain Admins,CN=Users,DC=contoso,DC=com"

Repadmin: running command /showobjmeta against full DC dc01.contoso.com

15 entries.
Loc.USN                          Originating DSA  Org.USN  Org.Time/Date        Ver Attribute
=======                          =============== ======== =============        === =========
  12545      9495099d-fc8f-4ab7-b29b-c18f3ee284ec     12341 2013-03-01 10:39:24    1 objectClass
[redacted]
LEGACY          member
        CN=svc_exchange,CN=Users,DC=contoso,DC=com
LEGACY          member
        CN=Administrator,CN=Users,DC=contoso,DC=com
PRESENT         member 2013-03-31 06:35:45   9495099d-fc8f-4ab7-b29b-c18f3ee284ec   12599   65051   1
        CN=DG,DC=contoso,DC=com
PRESENT         member 2013-03-11 03:01:35   9495099d-fc8f-4ab7-b29b-c18f3ee284ec   12601   46353   1
        CN=Lee Mendoza Adm,OU=_Admins,DC=contoso,DC=com
PRESENT         member 2013-03-11 03:01:35   9495099d-fc8f-4ab7-b29b-c18f3ee284ec   12603   46350   1
        CN=Katrina Mendoza adm,OU=_Admins,DC=contoso,DC=com
PRESENT         member 2013-03-11 03:01:22   9495099d-fc8f-4ab7-b29b-c18f3ee284ec   12605   46346   1
        CN=Connie Flores Adm,OU=_Admins,DC=contoso,DC=com
ABSENT          member 2023-10-24 15:40:32                                HQ\DC01  119034  119034   2
        CN=svc-sql,OU=Service Accounts,OU=_Admins,DC=contoso,DC=com
PRESENT         member 2017-05-03 19:34:17   5ecdf8e7-6e18-49b0-abeb-200bcfe45fec   21716   21716   1
        CN=PIerre,DC=contoso,DC=com
PRESENT         member 2018-11-02 06:47:12   ef65dd31-8b7f-4fe7-a57a-4678a9703674   94589   94589   1
        CN=Pierre Odonay,OU=_Admins,DC=contoso,DC=com
```

Replication metadata is data too

```
C:\>repadmin /showobjmeta . "<SID=S-1-5-21-1377293298-2038669548-2215429205-500>"

Repadmin: running command /showobjmeta against full DC localhost

Loc.USN                    Originating DSA  Org.USN  Org.Time/Date        Ver Attribute
=======                    =============== ========= =============        === =========
   8196                 Toronto\VERYOLDDC01      8196 2021-02-02 06:51:51    1 objectClass
…
32895                   Toronto\VERYOLDDC01     32895 2023-07-07 21:10:37 784118 lockoutTime
…
```

Time-limited group memberships

Were meant to be used in PAM trust.

But work for regular group memberships / JiT approach.

Require 2016 FFL.

```
Enable-ADOptionalFeature 'Privileged Access Management Feature' `
    -Scope ForestOrConfigurationSet -Target contoso.com

Add-ADGroupMember -Identity "Event Log Readers" -Members Bob `
    -MemberTimeToLive (New-TimeSpan -Minutes 45)
```

TGT lifetimes are adjusted to the lowest TTL.

Dynamic objects

Dynamic objects 101

Require low permissions. Can you create an object? You can create a dynamic version of it.

Default TTL is 1 day. Can be changed.

Disappear without traces (no metadata, no Deleted Objects container traces).

Can be easily detected.

Why can I still use my old password?

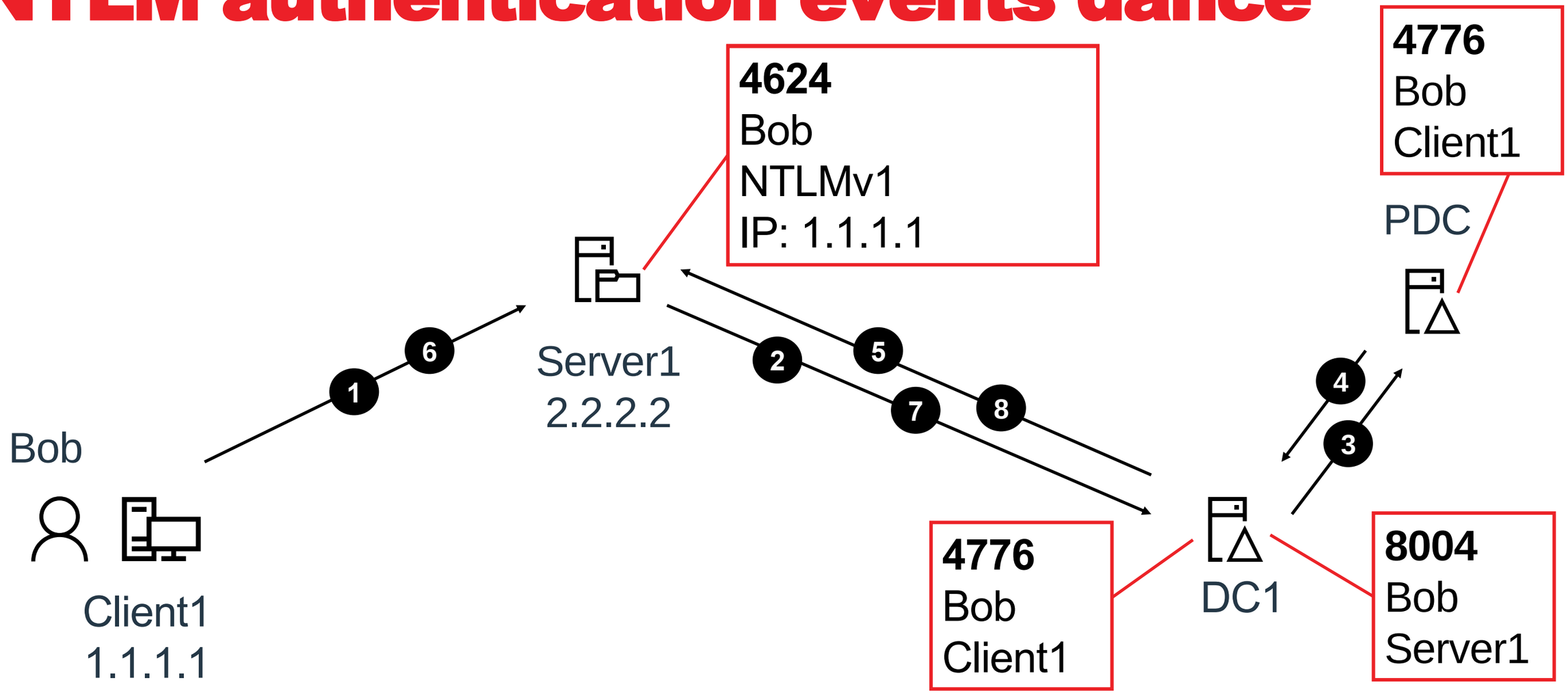
You just updated your password, but you can still access resources using the old one.

KB906305

Up to 60 minutes **OldPasswordAllowedPeriod**

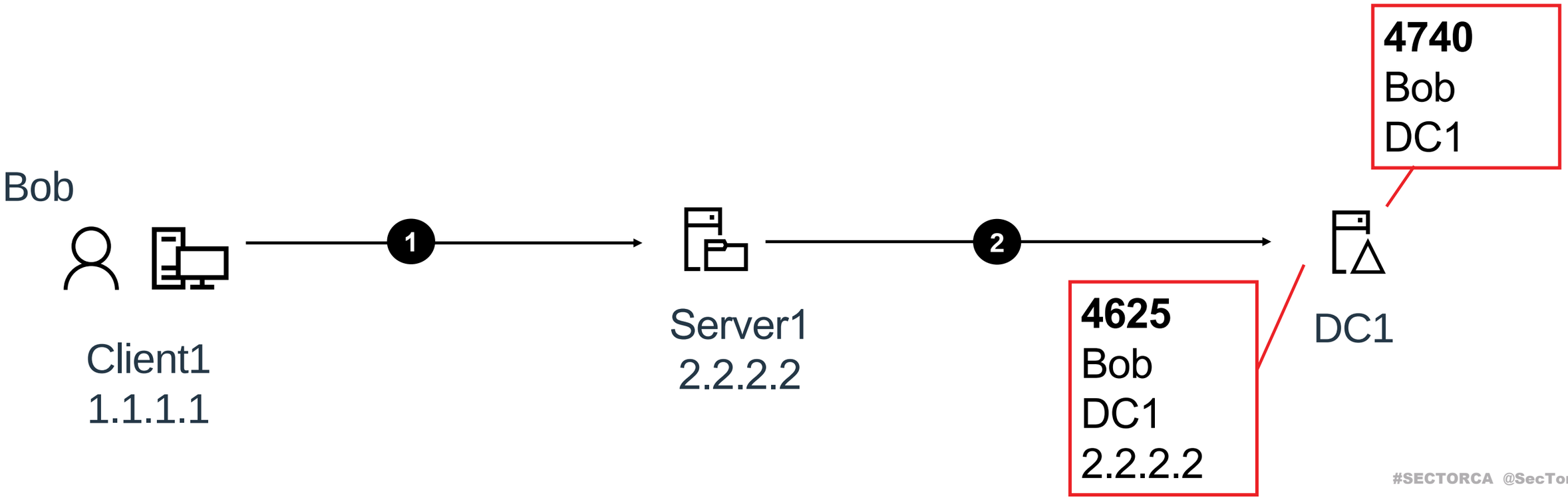
Double reset, or “User must change password at next logon”.

NTLM authentication events dance



What if I have a stupid application?

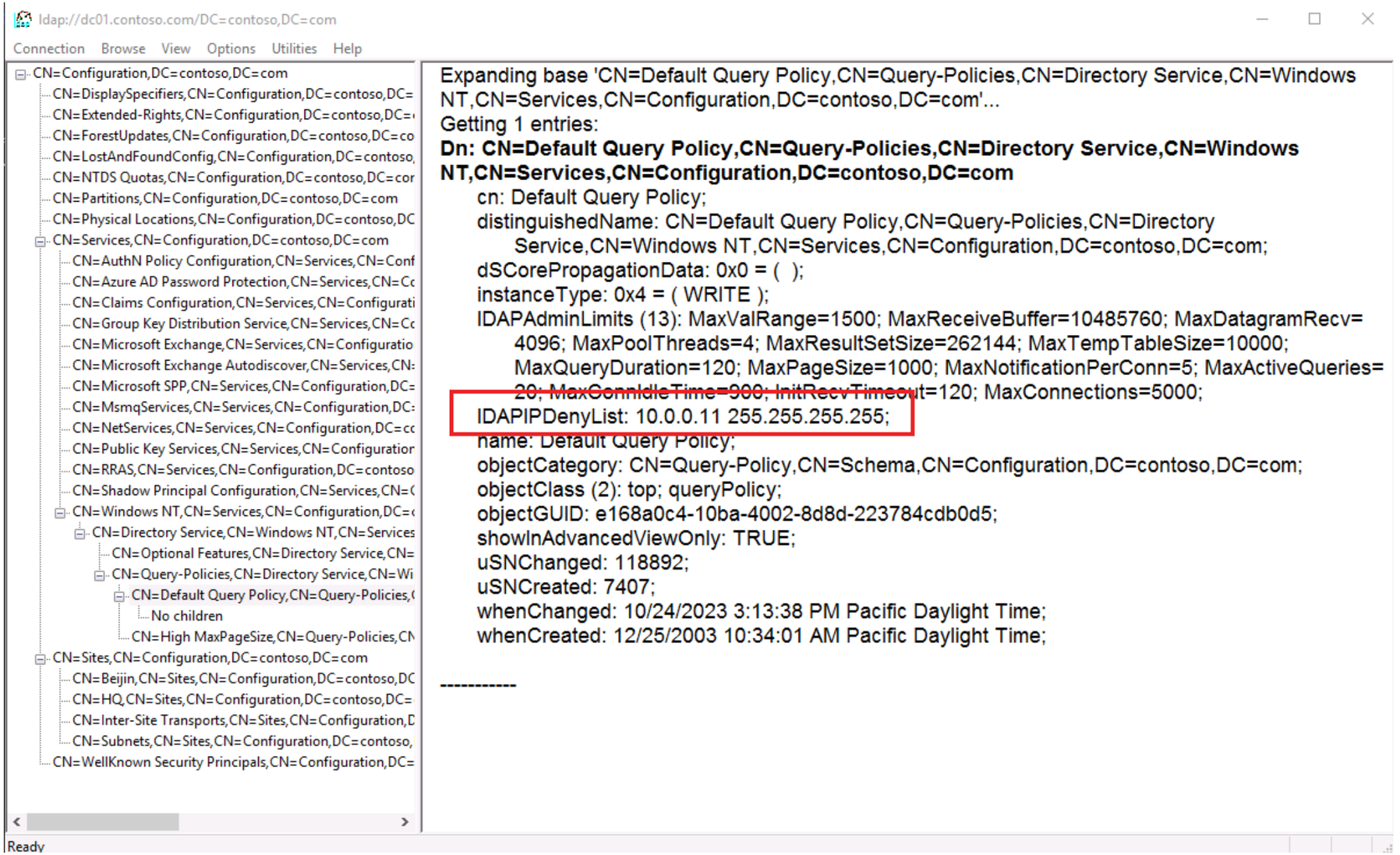
You mean an application that leverages LDAP as an authentication protocol?



Ban networks from making LDAP calls

IDAPIPDenyList is a property in LDAP policies that allows an administrator to ban an IPv4 subnets from making LDAP calls.

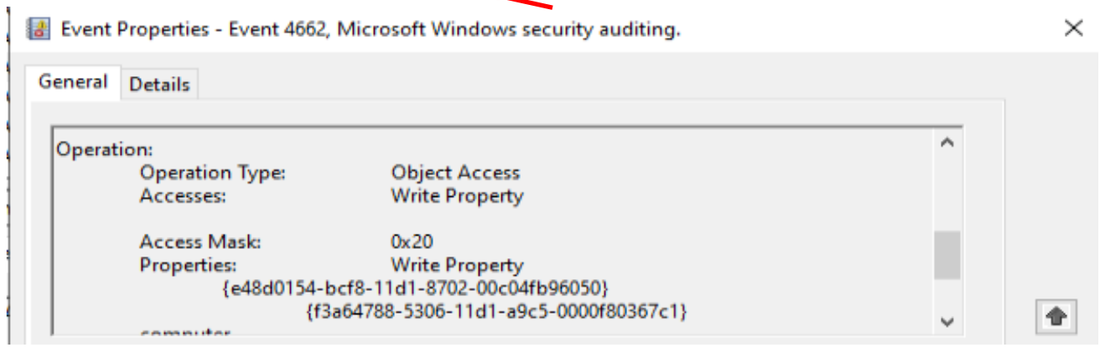
Replies matching clients with a TCP RST.

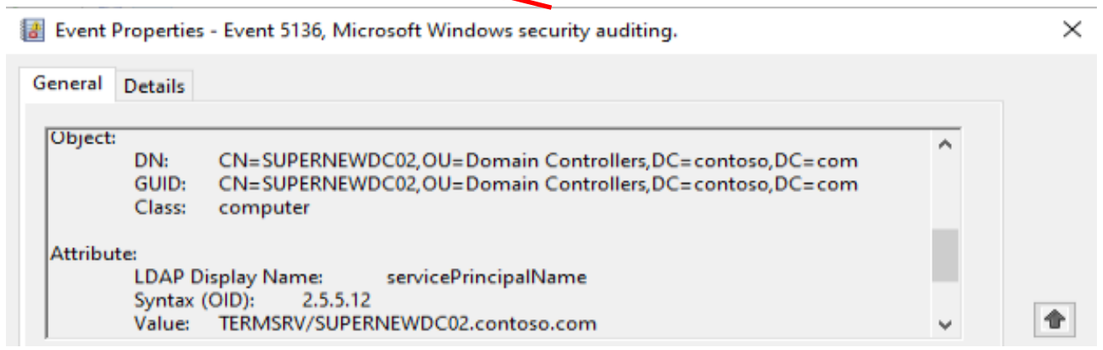

ldap://dc01.contoso.com/DC=contoso,DC=com
Connection Browse View Options Utilities Help
CN=Configuration,DC=contoso,DC=com
CN=DisplaySpecifiers,CN=Configuration,DC=contoso,DC=
CN=Extended-Rights,CN=Configuration,DC=contoso,DC=
CN=ForestUpdates,CN=Configuration,DC=contoso,DC=co
CN=LostAndFoundConfig,CN=Configuration,DC=contoso,
CN=NTDS Quotas,CN=Configuration,DC=contoso,DC=cor
CN=Partitions,CN=Configuration,DC=contoso,DC=com
CN=Physical Locations,CN=Configuration,DC=contoso,DC
CN=Services,CN=Configuration,DC=contoso,DC=com
CN=AuthN Policy Configuration,CN=Services,CN=Conf
CN=Azure AD Password Protection,CN=Services,CN=Cc
CN=Claims Configuration,CN=Services,CN=Configurati
CN=Group Key Distribution Service,CN=Services,CN=Cc
CN=Microsoft Exchange,CN=Services,CN=Configuratio
CN=Microsoft Exchange Autodiscover,CN=Services,CN:
CN=Microsoft SPP,CN=Services,CN=Configuration,DC=
CN=MsmqServices,CN=Services,CN=Configuration,DC:
CN=NetServices,CN=Services,CN=Configuration,DC=cc
CN=Public Key Services,CN=Services,CN=Configuratior
CN=RRAS,CN=Services,CN=Configuration,DC=contoso
CN=Shadow Principal Configuration,CN=Services,CN=(
CN=Windows NT,CN=Services,CN=Configuration,DC=(
CN=Directory Service,CN=Windows NT,CN=Services
CN=Optional Features,CN=Directory Service,CN=
CN=Query-Policies,CN=Directory Service,CN=Wi
CN=Default Query Policy,CN=Query-Policies,(
No children
CN=High MaxPageSize,CN=Query-Policies,CN
CN=Sites,CN=Configuration,DC=contoso,DC=com
CN=Beijin,CN=Sites,CN=Configuration,DC=contoso,DC
CN=HQ,CN=Sites,CN=Configuration,DC=contoso,DC=
CN=Inter-Site Transports,CN=Sites,CN=Configuration,D
CN=Subnets,CN=Sites,CN=Configuration,DC=contoso,
CN=WellKnown Security Principals,CN=Configuration,DC=
Expanding base 'CN=Default Query Policy,CN=Query-Policies,CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=contoso,DC=com'...
Getting 1 entries:
Dn: CN=Default Query Policy,CN=Query-Policies,CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=contoso,DC=com
cn: Default Query Policy;
distinguishedName: CN=Default Query Policy,CN=Query-Policies,CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=contoso,DC=com;
dSCorePropagationData: 0x0 = ( );
instanceType: 0x4 = (WRITE);
lDAPAdminLimits (13): MaxValRange=1500; MaxReceiveBuffer=10485760; MaxDatagramRecv=4096; MaxPoolThreads=4; MaxResultSetSize=262144; MaxTempTableSize=10000; MaxQueryDuration=120; MaxPageSize=1000; MaxNotificationPerConn=5; MaxActiveQueries=20; MaxConnIdleTime=900; InitRecvTimeout=120; MaxConnections=5000;
lDAPIPDenyList: 10.0.0.11 255.255.255.255;
name: Default Query Policy;
objectCategory: CN=Query-Policy,CN=Schema,CN=Configuration,DC=contoso,DC=com;
objectClass (2): top; queryPolicy;
objectGUID: e168a0c4-10ba-4002-8d8d-223784cdb0d5;
showInAdvancedViewOnly: TRUE;
uSNChanged: 118892;
uSNCreated: 7407;
whenChanged: 10/24/2023 3:13:38 PM Pacific Daylight Time;
whenCreated: 12/25/2003 10:34:01 AM Pacific Daylight Time;

Ready

Audit object modifications

```
C:\Windows\System32>auditpol /get /category:"DS Access"
System audit policy
Category/Subcategory                      Setting
DS Access
  Directory Service Changes               Success and Failure
  Directory Service Replication           No Auditing
  Detailed Directory Service Replication  No Auditing
  Directory Service Access                Success and Failure
```



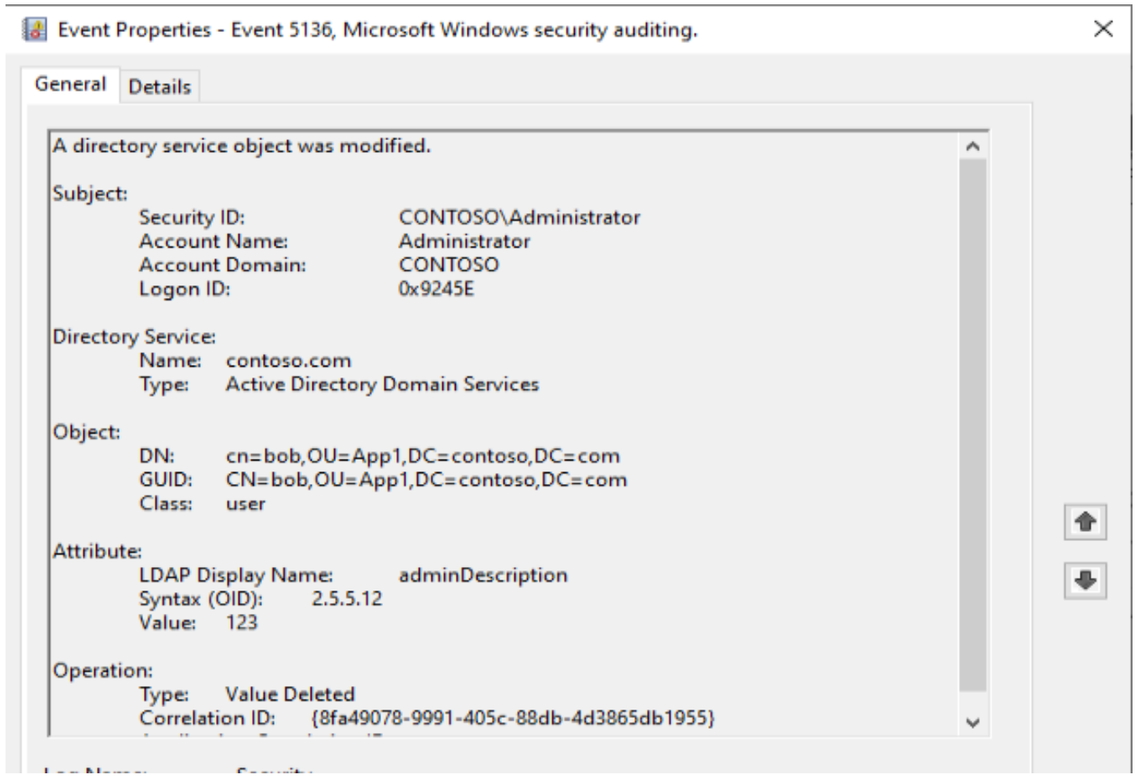


I didn’t see you there...

The flag **fNEVERVALUEAUDIT** allows an administrator to instruct the directory not to audit value changes on designated attributes.

fNEVERVALUEAUDIT

Before



After

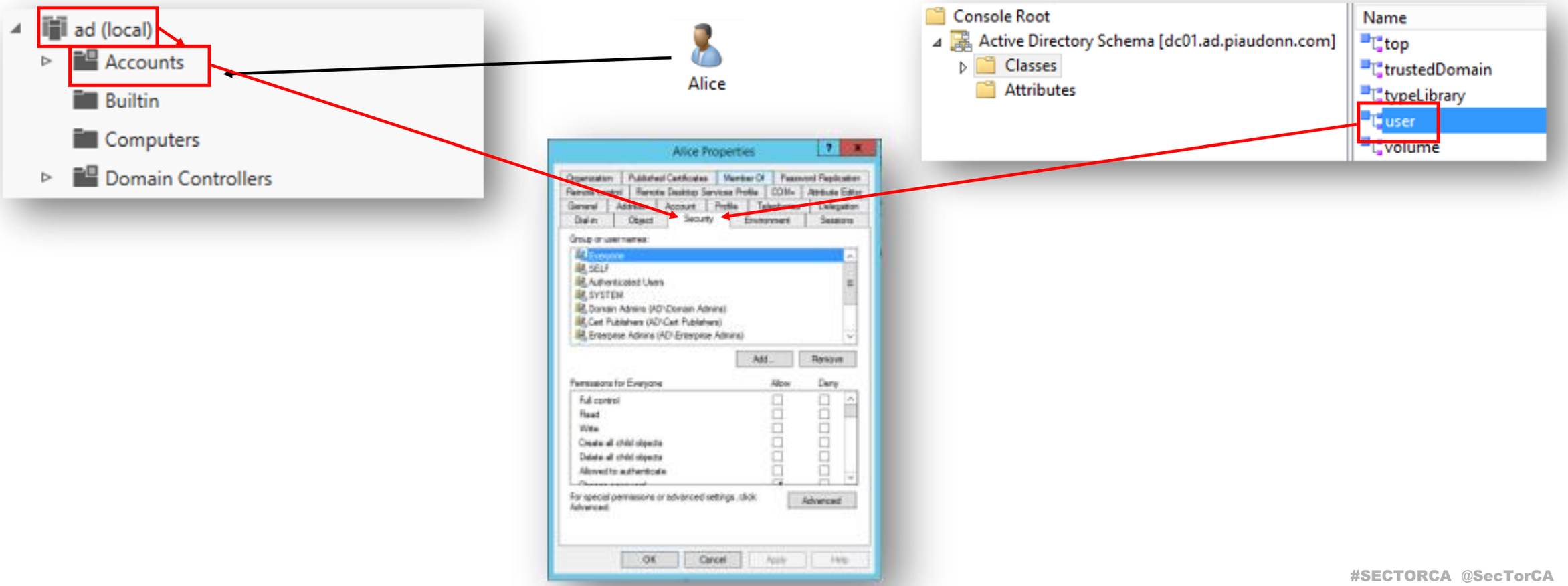
Wait a minute

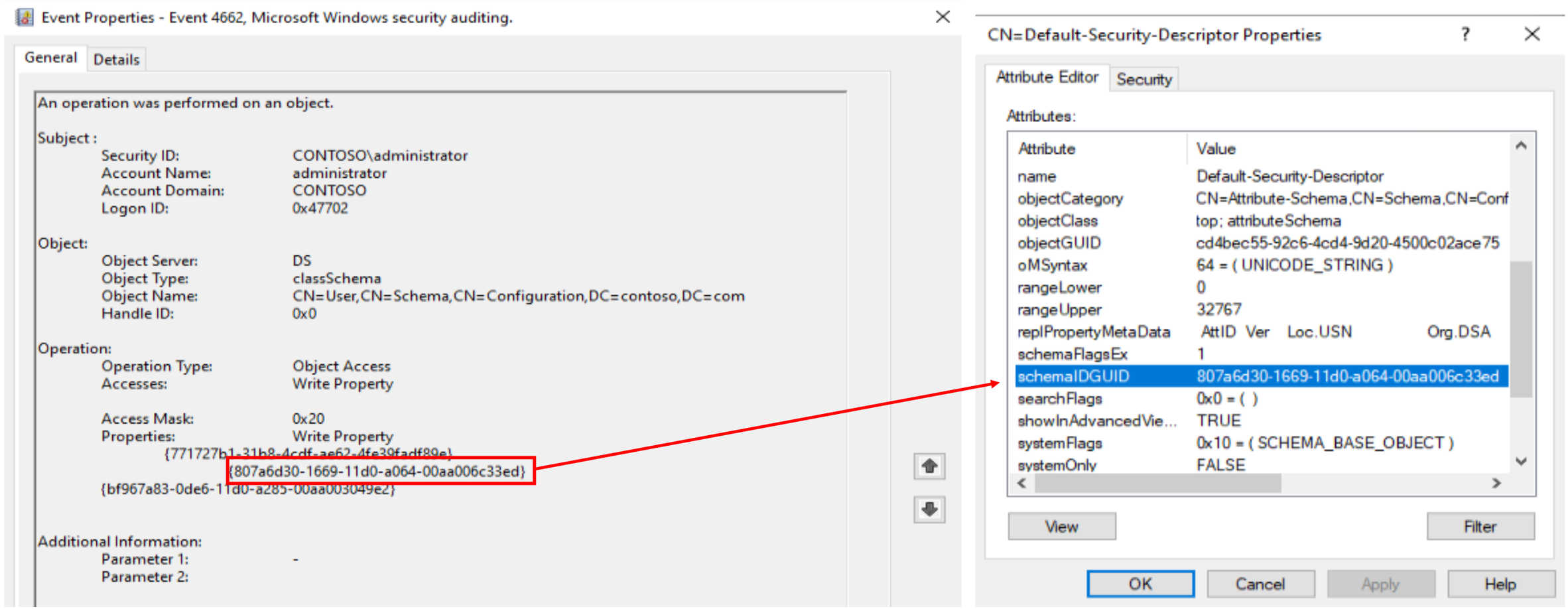
Post exploit stuff.

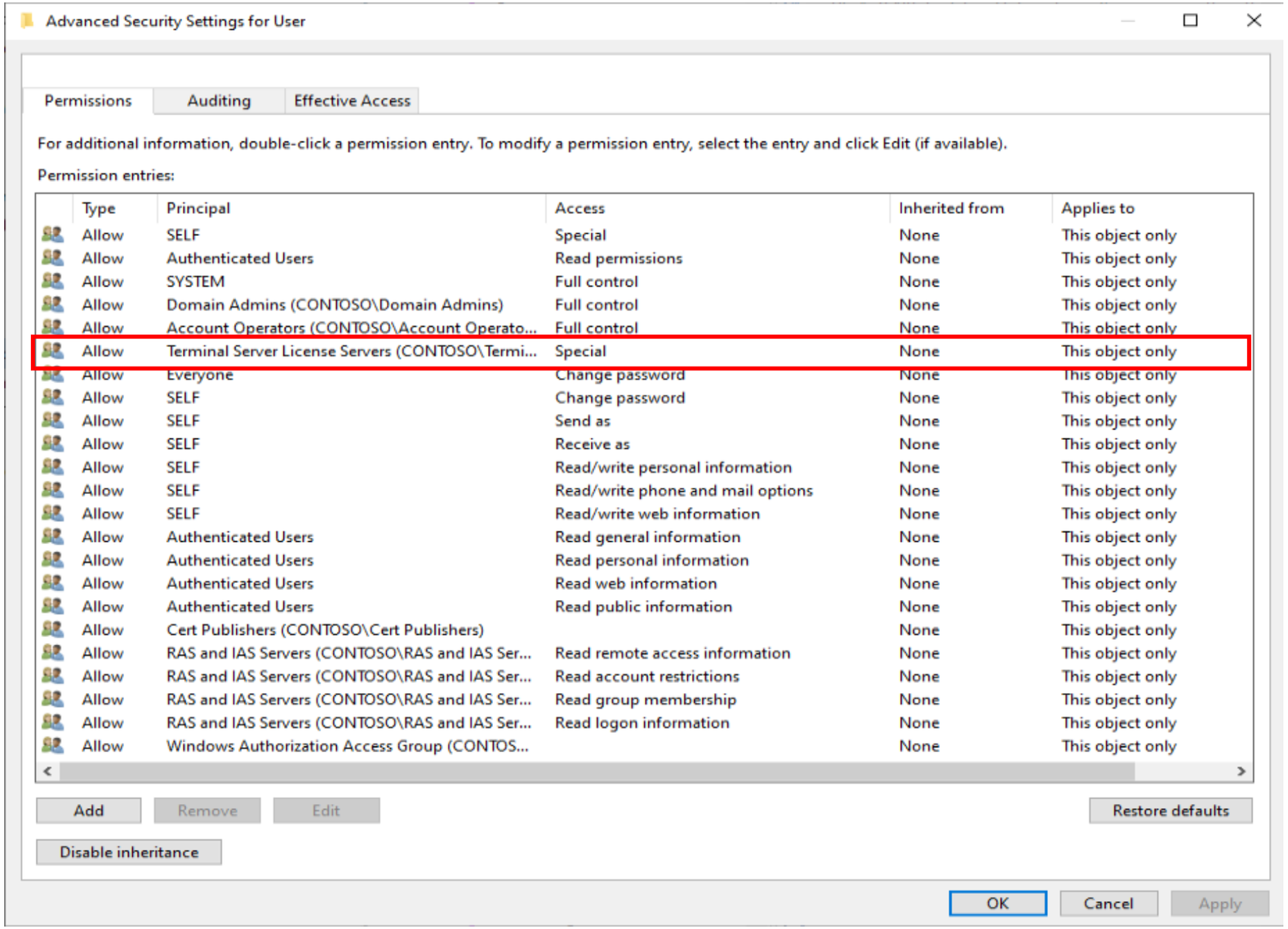
Evade detection? Do you really have use cases that detect schema changes?

SECTOR

defaultSecurityDescriptor

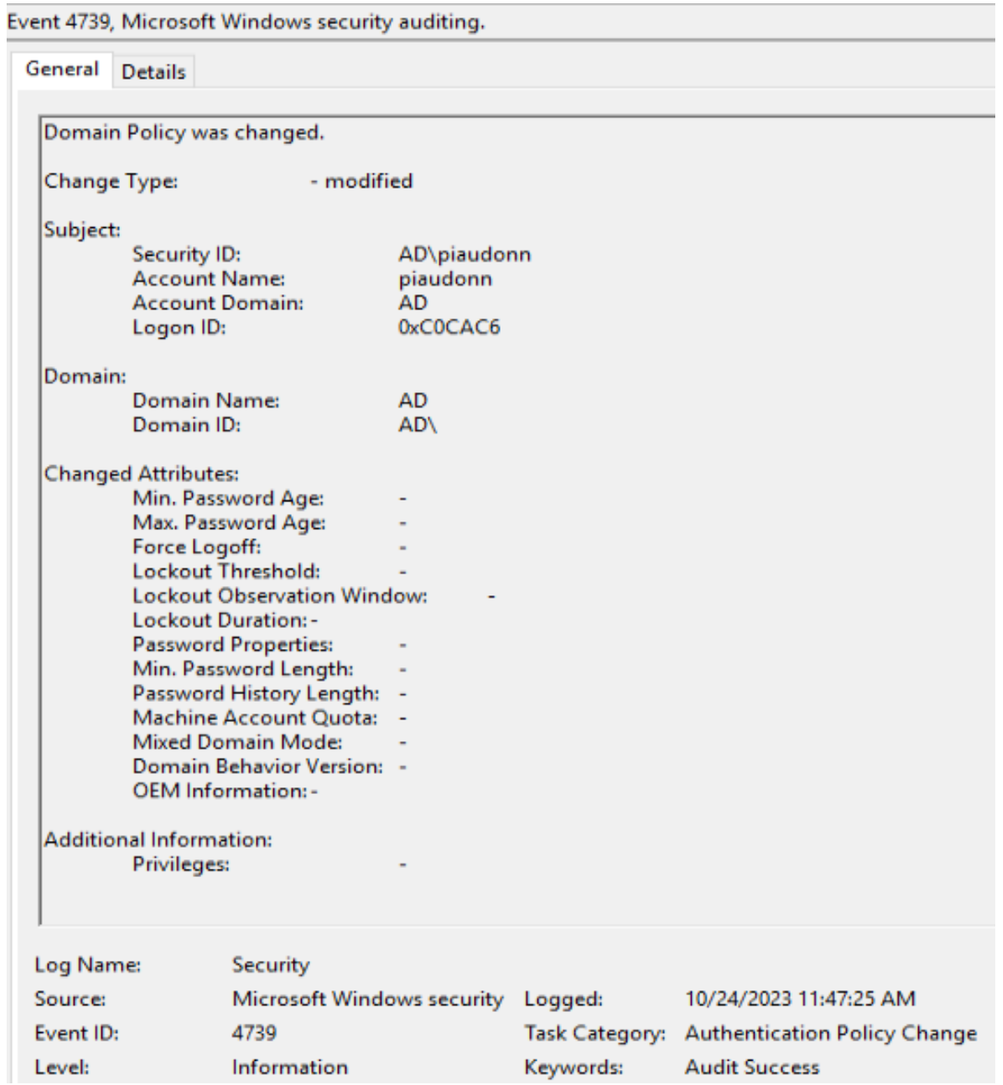



Event Properties - Event 4662, Microsoft Windows security auditing.
General
Details
An operation was performed on an object.
Subject :
Security ID: CONTOSO\administrator
Account Name: administrator
Account Domain: CONTOSO
Logon ID: 0x47702
Object:
Object Server: DS
Object Type: classSchema
Object Name: CN=User,CN=Schema,CN=Configuration,DC=contoso,DC=com
Handle ID: 0x0
Operation:
Operation Type: Object Access
Accesses: Write Property
Access Mask: 0x20
Properties: Write Property
{771727b1-31b8-4cdf-ae62-4fe39fadf89e}
{807a6d30-1669-11d0-a064-00aa006c33ed}
{bf967a83-0de6-11d0-a285-00aa003049e2}
Additional Information:
Parameter 1: -
Parameter 2:
CN=Default-Security-Descriptor Properties
Attribute Editor
Security
Attributes:
Attribute
Value
name Default-Security-Descriptor
objectCategory CN=Attribute-Schema,CN=Schema,CN=Conf
objectClass top; attributeSchema
objectGUID cd4bec55-92c6-4cd4-9d20-4500c02ace75
oMSyntax 64 = (UNICODE_STRING)
rangeLower 0
rangeUpper 32767
replPropertyMetaData AttID Ver Loc.USN Org.DSA
schemaFlagsEx 1
schemaIDGUID 807a6d30-1669-11d0-a064-00aa006c33ed
searchFlags 0x0 = ( )
showInAdvancedVie... TRUE
systemFlags 0x10 = (SCHEMA_BASE_OBJECT)
systemOnly FALSE
View
Filter
OK
Cancel
Apply
Help


Advanced Security Settings for User
Permissions
Auditing
Effective Access
For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).
Permission entries:
Type | Principal | Access | Inherited from | Applies to
Allow | SELF | Special | None | This object only
Allow | Authenticated Users | Read permissions | None | This object only
Allow | SYSTEM | Full control | None | This object only
Allow | Domain Admins (CONTOSO\Domain Admins) | Full control | None | This object only
Allow | Account Operators (CONTOSO\Account Operato... | Full control | None | This object only
Allow | Terminal Server License Servers (CONTOSO\Termi... | Special | None | This object only
Allow | Everyone | Change password | None | This object only
Allow | SELF | Change password | None | This object only
Allow | SELF | Send as | None | This object only
Allow | SELF | Receive as | None | This object only
Allow | SELF | Read/write personal information | None | This object only
Allow | SELF | Read/write phone and mail options | None | This object only
Allow | SELF | Read/write web information | None | This object only
Allow | Authenticated Users | Read general information | None | This object only
Allow | Authenticated Users | Read personal information | None | This object only
Allow | Authenticated Users | Read web information | None | This object only
Allow | Authenticated Users | Read public information | None | This object only
Allow | Cert Publishers (CONTOSO\Cert Publishers) | | None | This object only
Allow | RAS and IAS Servers (CONTOSO\RAS and IAS Ser... | Read remote access information | None | This object only
Allow | RAS and IAS Servers (CONTOSO\RAS and IAS Ser... | Read account restrictions | None | This object only
Allow | RAS and IAS Servers (CONTOSO\RAS and IAS Ser... | Read group membership | None | This object only
Allow | RAS and IAS Servers (CONTOSO\RAS and IAS Ser... | Read logon information | None | This object only
Allow | Windows Authorization Access Group (CONTOS... | | None | This object only
Add
Remove
Edit
Restore defaults
Disable inheritance
OK
Cancel
Apply

Post exploit stuff...

What about removing the SACL?


Event 4739, Microsoft Windows security auditing.
General
Details
Domain Policy was changed.
Change Type: - modified
Subject:
Security ID: AD\piaudonn
Account Name: piaudonn
Account Domain: AD
Logon ID: 0xC0CAC6
Domain:
Domain Name: AD
Domain ID: AD\
Changed Attributes:
Min. Password Age: -
Max. Password Age: -
Force Logoff: -
Lockout Threshold: -
Lockout Observation Window: -
Lockout Duration: -
Password Properties: -
Min. Password Length: -
Password History Length: -
Machine Account Quota: -
Mixed Domain Mode: -
Domain Behavior Version: -
OEM Information: -
Additional Information:
Privileges: -
Log Name: Security
Source: Microsoft Windows security
Logged: 10/24/2023 11:47:25 AM
Event ID: 4739
Task Category: Authentication Policy Change
Level: Information
Keywords: Audit Success

adminSDHolder RTFM

Protect DACL of privileged accounts, groups and its members*.

- ☑ Enterprise admins
  - ☑ Enterprise admins members
- ☑ Schema admins
  - ☑ Schema admins members
- ☑ Domain admins
  - ☑ Domain admins members

…

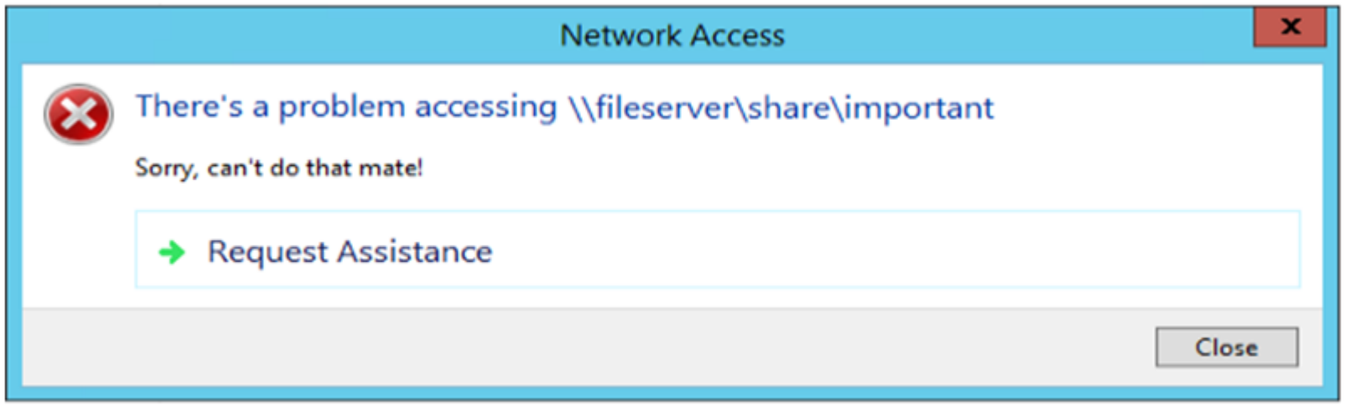
- ☑ Domain Controllers
  - ✗ Domain Controllers members

Direct consequences

Domain level ACL are applied to the domain controller objects (yes that delegation you set up at the top level on computer accounts…)

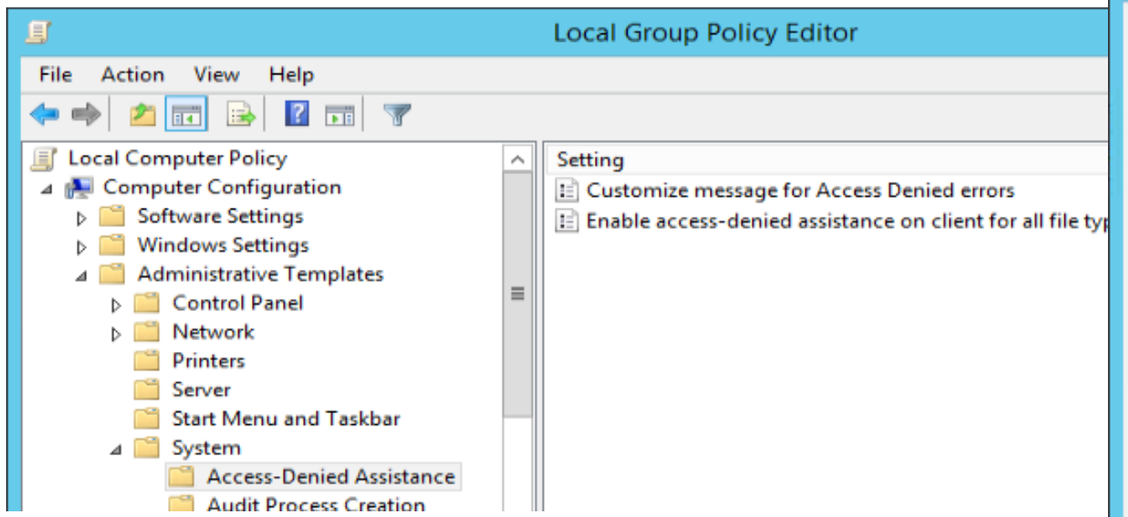
Objects aren't protected, sensitive attributes such as **altSecurityIdentities** or **msDS-KeyCredentialLink** are up for grabs!

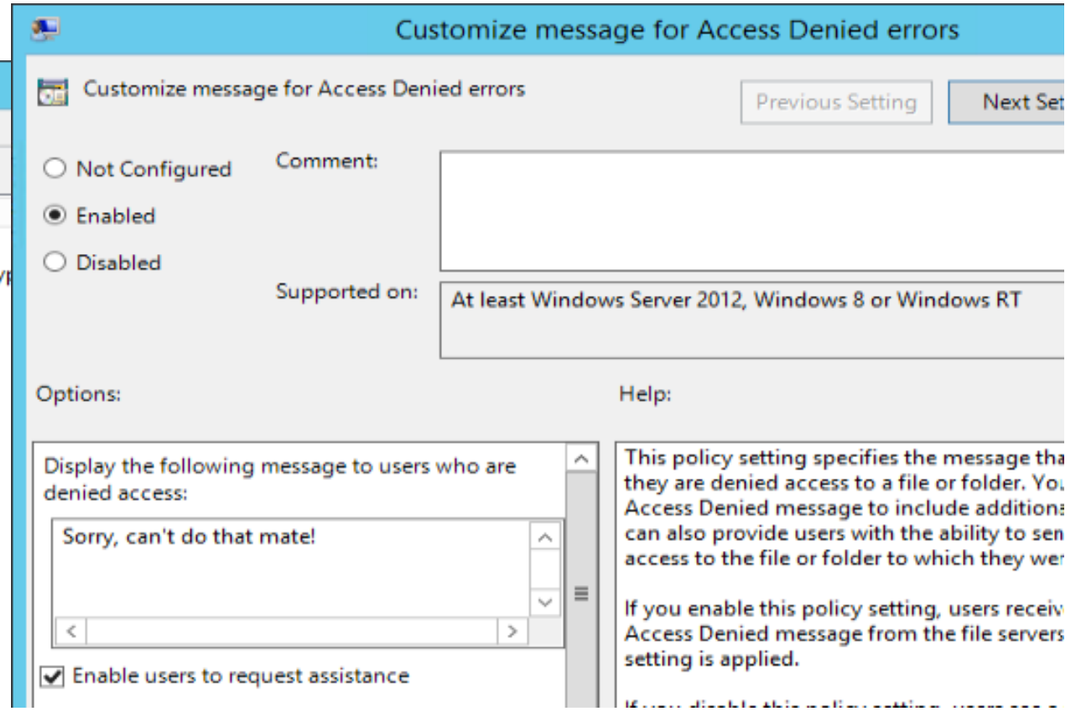
0x5


Network Access
There's a problem accessing \\fileserver\share\important
Sorry, can't do that mate!
Request Assistance
Close

Access-Denied Assistance

File server is a Windows box with File Server Resource Manager.





SECTOR

Access assistance requested from User: P\Bob to Path: \\FILESERVER\SHARE\IMPORTANT

Pierre Audonnet
To Pierre Audonnet

General

Please do not reply to this message as it is sent from an unmonitored account.

A user is requesting help accessing a shared folder or file. Review the user's permissions and then take the appropriate action.

User:	P\Bob
Path:	\\FILESERVER\SHARE\IMPORTANT
Justification from user:	Prettttyy pleeassse. I get you a beer. Promise!

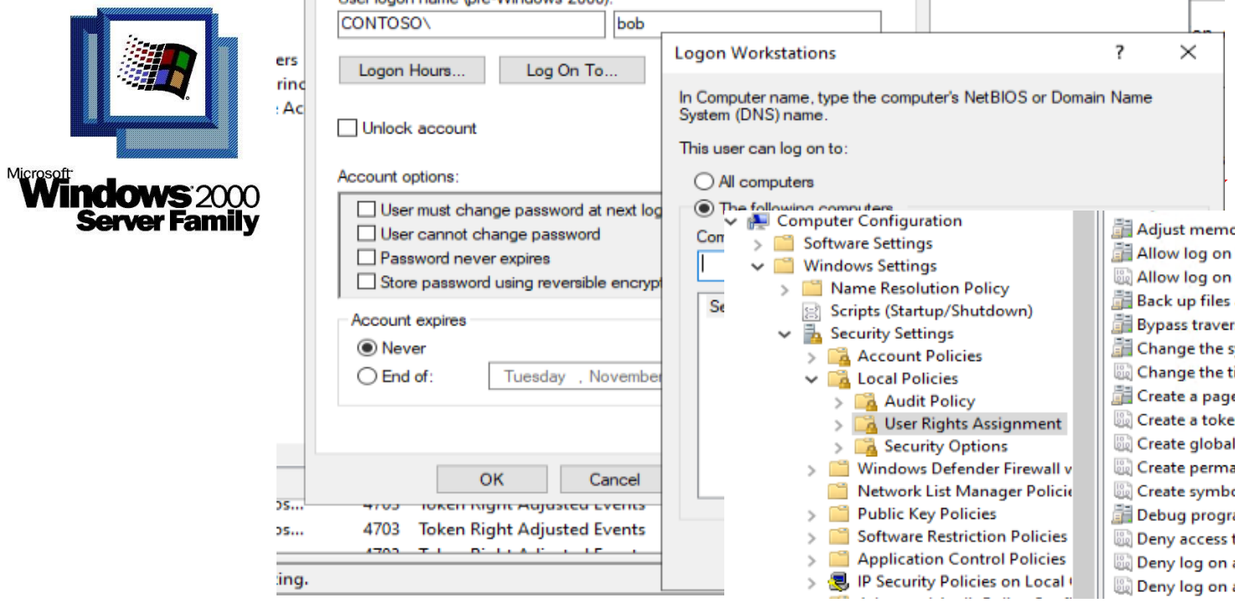
Current permissions for user (P\Bob):

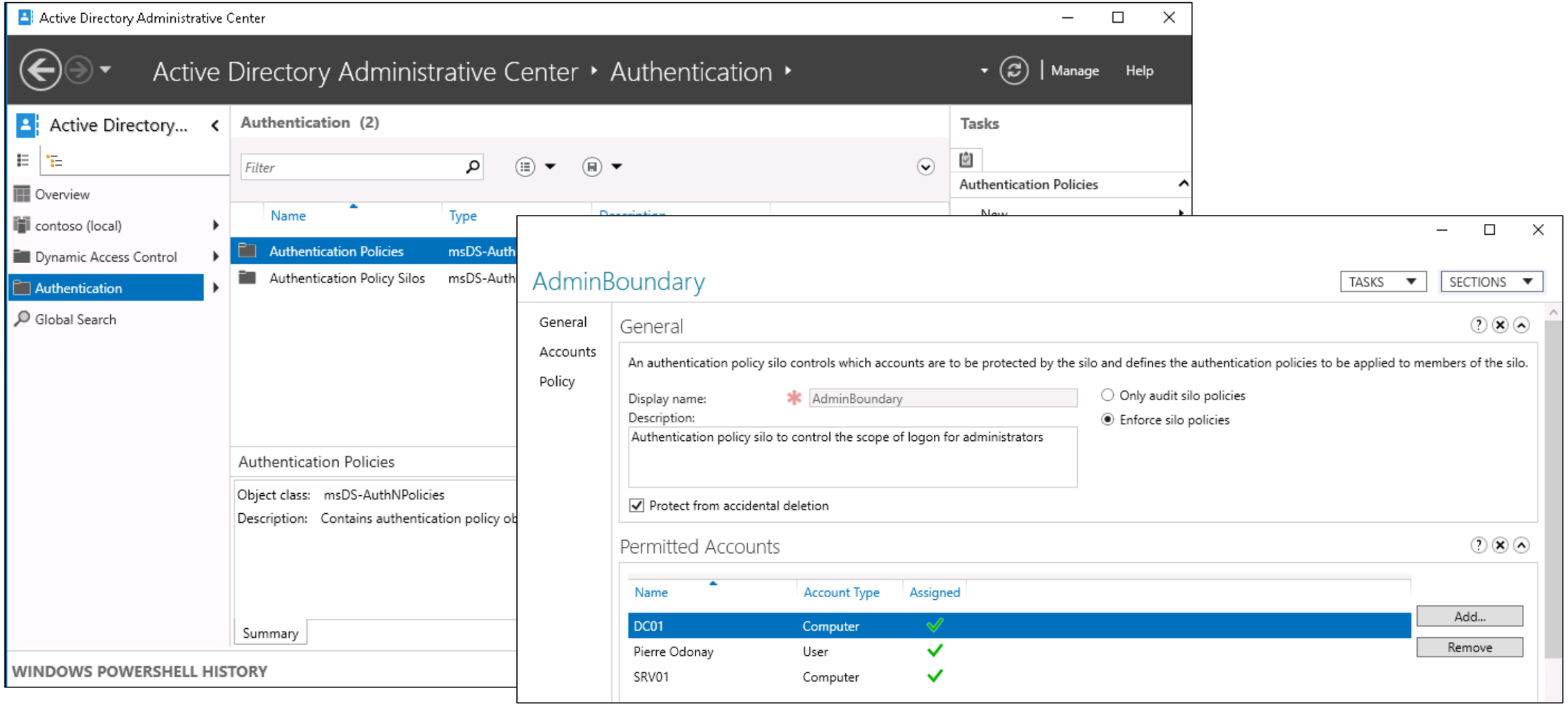
Permission	Effective Access	Access Limited By
Full Control	Blocked	File/Folder Permissions
Modify	Blocked	File/Folder Permissions
Read & Execute (or List Folder Contents)	Blocked	File/Folder Permissions
Read	Blocked	File/Folder Permissions
Write	Blocked	File/Folder Permissions

Help the User Obtain Access

Restricting logon locations

userWorkstations




Active Directory Administrative Center
Active Directory Administrative Center ▸ Authentication ▸
Manage
Help
Active Directory...
Overview
contoso (local)
Dynamic Access Control
Authentication
Global Search
Authentication (2)
Filter
Name
Type
Authentication Policies
msDS-Auth
Authentication Policy Silos
msDS-Auth
Tasks
Authentication Policies
New
Authentication Policies
Object class: msDS-AuthNPolicies
Description: Contains authentication policy ob
Summary
WINDOWS POWERSHELL HISTORY
AdminBoundary
TASKS
SECTIONS
General
Accounts
Policy
General
An authentication policy silo controls which accounts are to be protected by the silo and defines the authentication policies to be applied to members of the silo.
Display name:
AdminBoundary
Description:
Authentication policy silo to control the scope of logon for administrators
Only audit silo policies
Enforce silo policies
Protect from accidental deletion
Permitted Accounts
Name
Account Type
Assigned
DC01
Computer
Pierre Odonay
User
SRV01
Computer
Add...
Remove

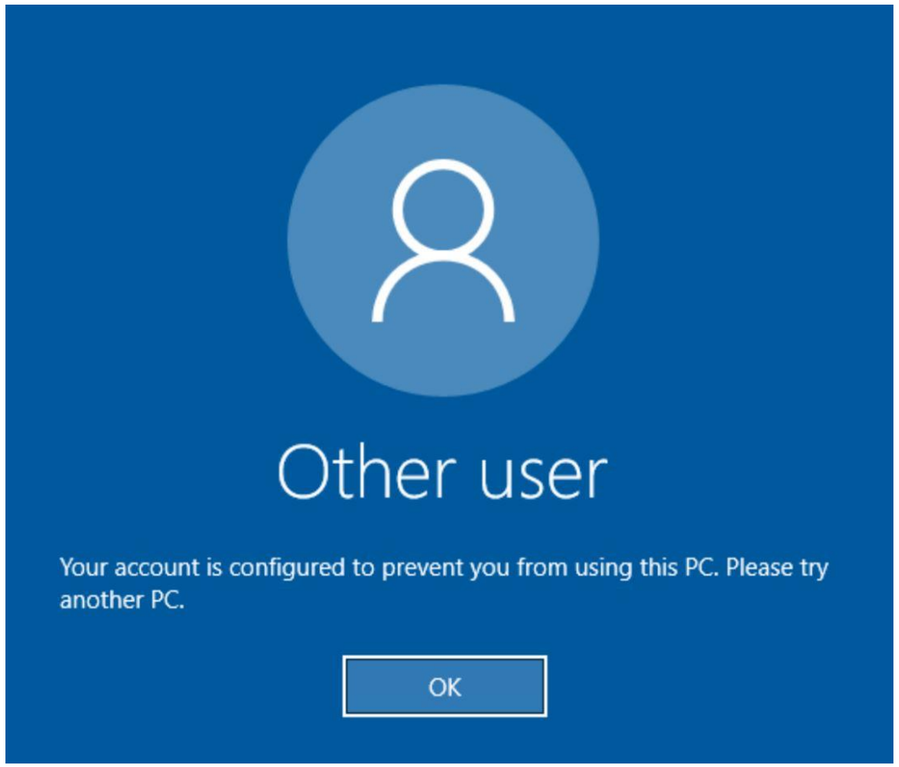
Authentication policies & silos

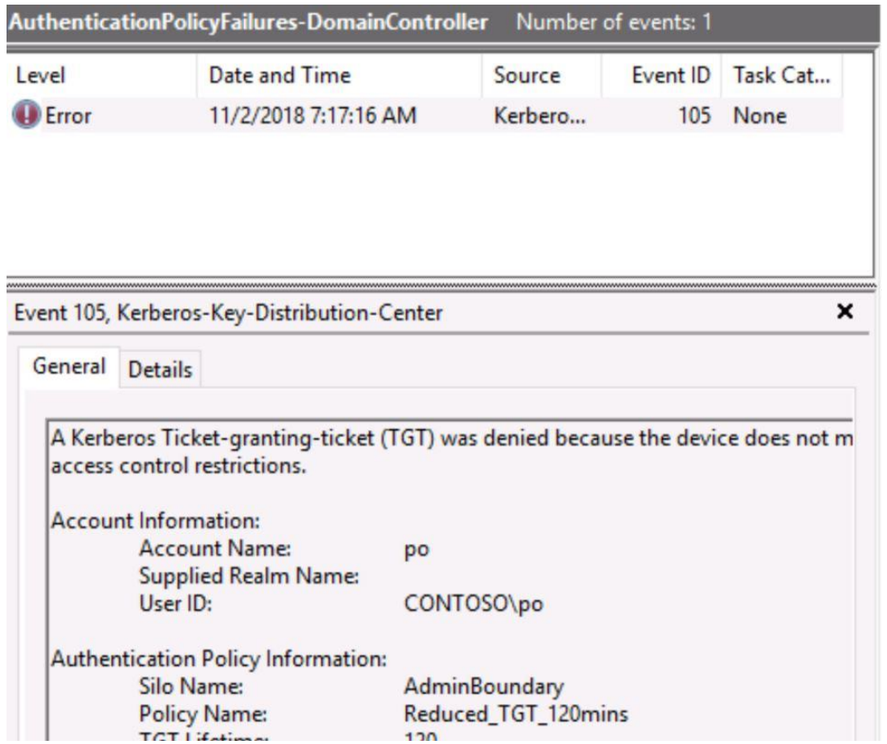
Requires:

- Windows Server 2012 R2 DFL
- Kerberos Armoring

Allows:

- Restricting accounts to specific hosts
- Customizing TGT lifetime
- When silos are used, enforcing Kerberos for user authentication


Other user
Your account is configured to prevent you from using this PC. Please try another PC.
OK


AuthenticationPolicyFailures-DomainController Number of events: 1
Level Date and Time Source Event ID Task Cat...
Error 11/2/2018 7:17:16 AM Kerbero... 105 None
Event 105, Kerberos-Key-Distribution-Center
General Details
A Kerberos Ticket-granting-ticket (TGT) was denied because the device does not m
access control restrictions.
Account Information:
Account Name: po
Supplied Realm Name:
User ID: CONTOSO\po
Authentication Policy Information:
Silo Name: AdminBoundary
Policy Name: Reduced_TGT_120mins

SECTOR

Are you still using RDP for admin stuff?

mstsc /RestrictedAdmin

```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::msv

Authentication Id : 0 ; 1022101 (00000000:000f9895)
Session           : RemoteInteractive from 1
User Name         : administrator
Domain            : CONTOSO
Logon Server      : DC01
Logon Time        : 10/30/2018 7:20:17 PM
SID               : S-1-5-21-1335734252-711511382-1358492552-500
        msv :
         [00000003] Primary
         * Username : Administrator
         * Domain   : CONTOSO
         * NTLM     : 92937945b518814341de3f726500d4ff
         * SHA1     : e99089abfd8d6af75c2c45dc4321ac7f28f7ed9d
         [00010000] CredentialKeys
         * NTLM     : 92937945b518814341de3f726500d4ff
         * SHA1     : e99089abfd8d6af75c2c45dc4321ac7f28f7ed9d
```

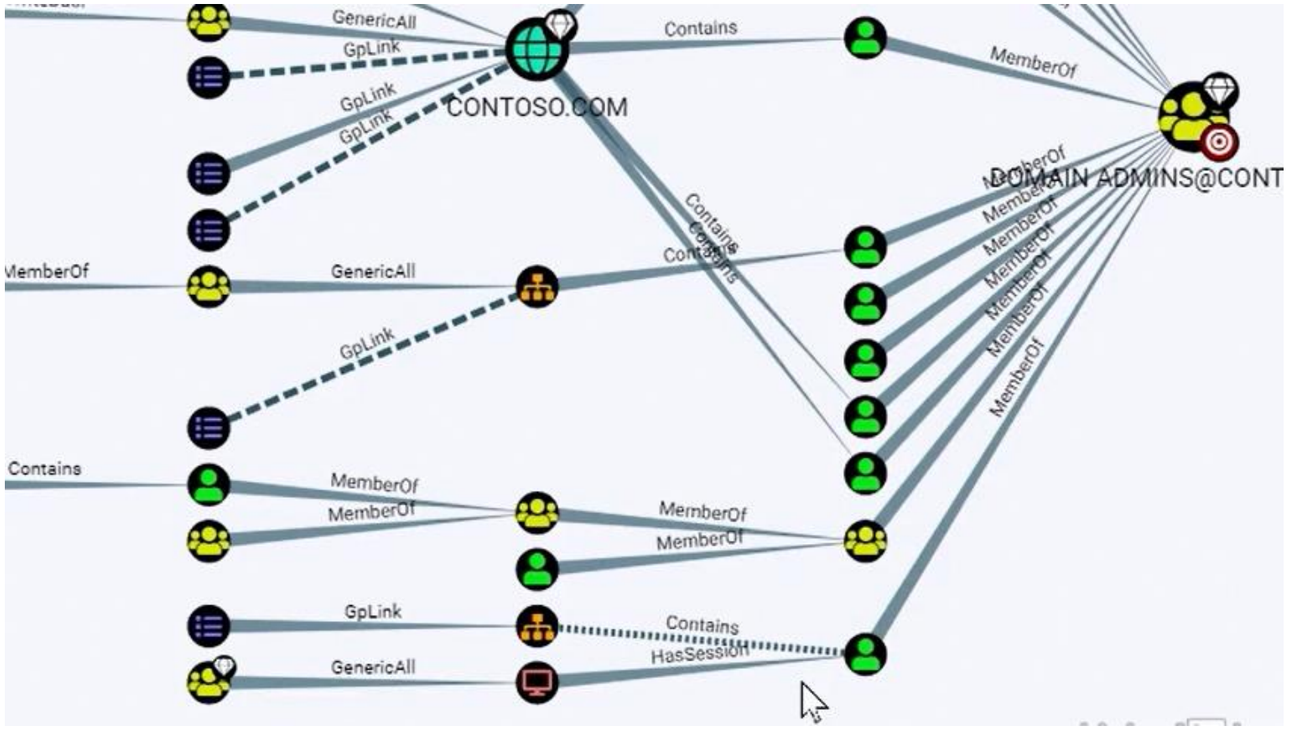
Are you still using RDP for admin stuff?

mstsc /RestrictedAdmin

DisableRestrictedAdmin DWORD 0x0

Do you still have SMB enumeration enabled?

Don’t make it too easy for your attackers.



```
C:\>nmap -p 445 --script smb-enum-sessions.nse --script-args smbuser=normaluser,smbpass=Pa$$w0rd 10.0.0.10
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-13 13:45 Pacifique (heure d?0t0)
Nmap scan report for dc01.contoso.com (10.0.0.10)
Host is up (0.00s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:15:5D:13:D3:31 (Microsoft)

Host script results:
| smb-enum-sessions:
|   Users logged in
|     CONTOSO\Administrator since <unknown>
|   Active SMB sessions
|     katrina.mendoza.adm is connected from \\192.168.1.127 for 11m17s, idle for 13s
|     SRV01$ is connected from \\192.168.1.11 for 11m15s, idle for 8s
|     Administrator is connected from \\192.168.1.11 for 11m15s, idle for 8s
|     EXCH1$ is connected from \\192.168.1.127 for 9m29s, idle for [not idle]
|     WIN10$ is connected from \\10.0.0.17 for 6m33s, idle for 1m45s
|     normaluser is connected from \\10.0.0.17 for 5m05s, idle for 4m51s
|     Administrator is connected from \\192.168.1.11 for 36s, idle for 8s
|     emea-admin is connected from \\10.0.0.27 for 18s, idle for 4s
|_    NORMALUSER is connected from \\10.0.0.17 for [just logged in, it's probably you], idle for [not idle]

Nmap done: 1 IP address (1 host up) scanned in 0.58 seconds
```

Do it today!

Just disable SMB enumeration:

```
Set-NetSessionEnumPermission
Restart-Service LanmanServer
```

Tribute to topics that did not make it

- **Prevent RDP and WinRM** – Use the Windows firewall to isolate your tier-0
- **NTDS Quota** – You have permissions to create an object, you just can't
- **DNS default permissions** – It's looser than you think it is
- **List object mode** – Everyone can read everything? It doesn't have to be this way
- **Last Interactive Logon Timestamp** – A LastLogonTimeStamp that is replicated
- **ADSI Schema Cache** – Or how your ADSI applications are DoS your branch offices
- **Guest lockout** – The noise that you can avoid instead of ignore
- **How admins are cheating with the password policy** – And that's easy to spot

Links, references, updates?

🔗 https://github.com/piaudonn/SecTor

This also contains the latest slides presented during the session.

Questions, feedback?

✉ piaudonn@microsoft.com

👤 Find me in the exhibition hall!