HERE TO STAY:
GAINING PERSISTENCE BY ABUSING ADVANCED AUTHENTICATION MECHANISMS

MARINA SIMAKOV
IGAL GOFMAN

Microsoft

> ABOUT US

Marina Simakov

Security Researcher @ Microsoft

- Holds an M.Sc. in computer science
- Special interest in graph theory
- Huge dog lover

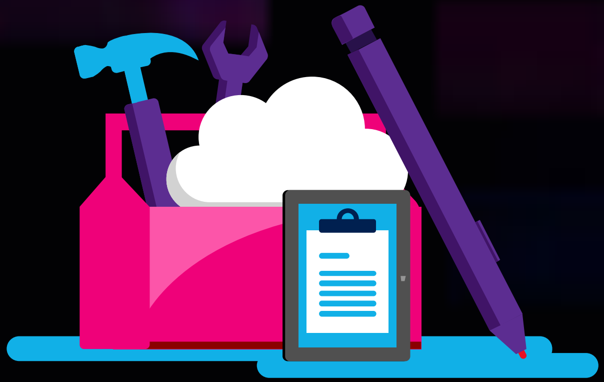
Igal Gofman

Security Researcher @ Microsoft

- Self taught security researcher & developer
- Loves Python
- Electronic music geek!

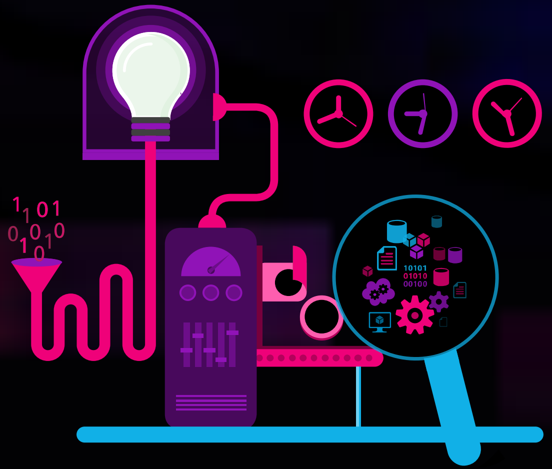
> WHY ARE WE HERE?

- **AWARENESS TO WEAK SPOTS**
  - Relatively Easy to Exploit
  - Easily Automated
  - Usually not monitored
- **DETECTION METHODS**
- **TALK TO US**



> AGENDA

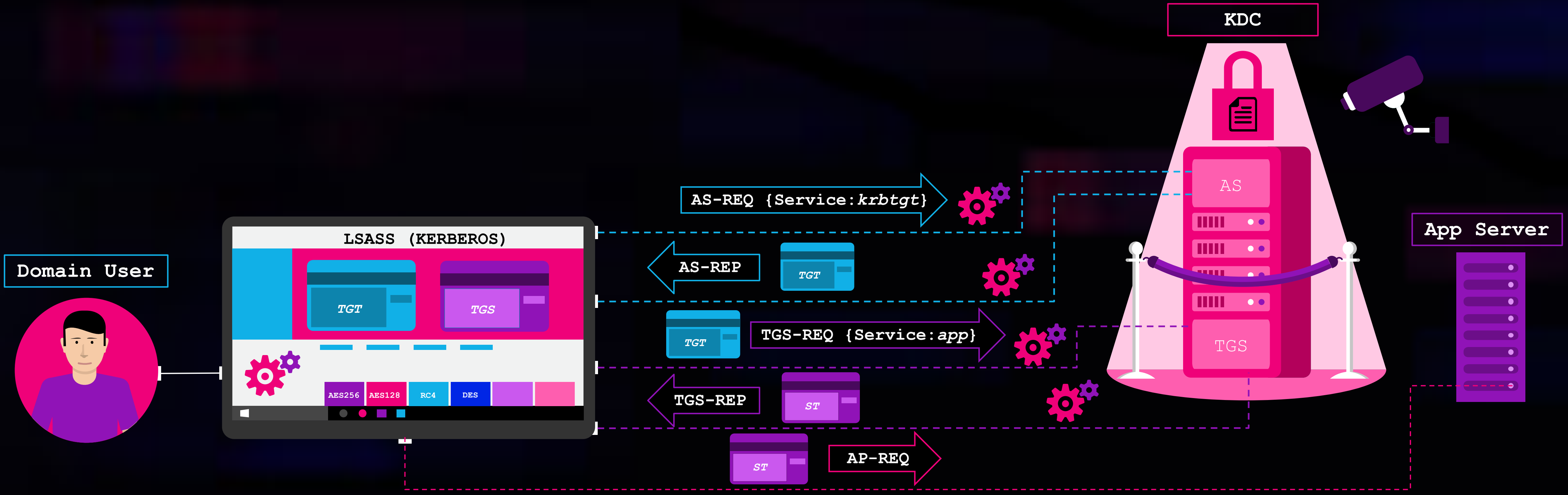
- INTRODUCTION TO KEY TERMS
  - Kerberos
  - Kerberos Delegation
- GAINING PERSISTENCE
  - Focus on High Privileges
  - Malicious JIT administration
- DEMO
- MITIGATIONS & TAKEAWAYS



> INTRODUCTION

▪ KERBEROS INTRO

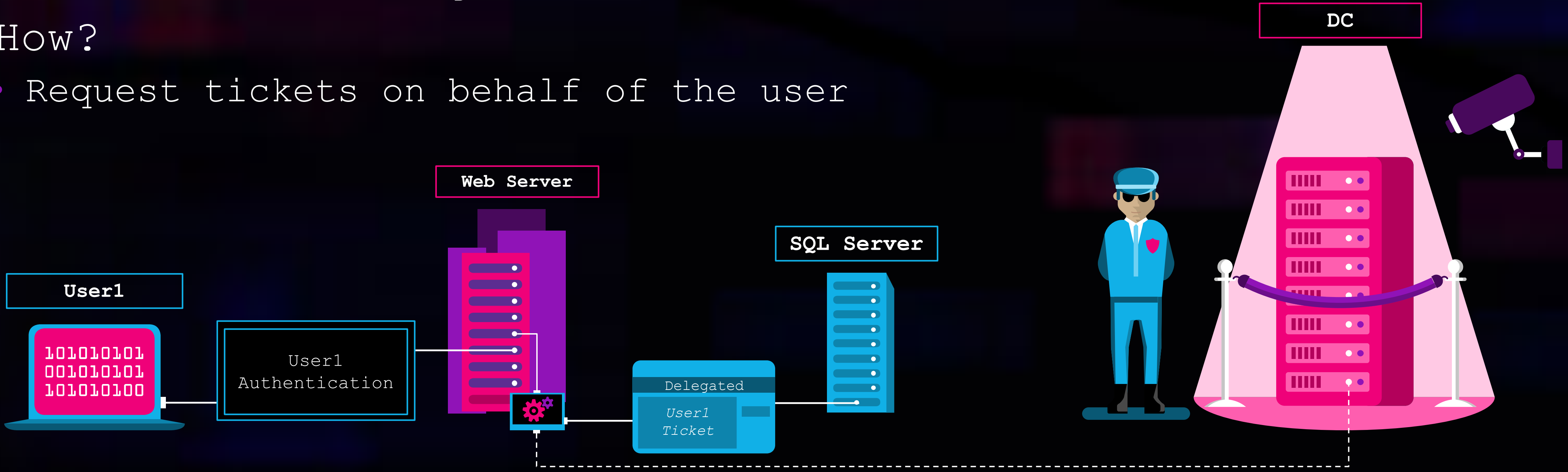
- Ticket based authentication protocol



> INTRODUCTION

▪ KERBEROS DELEGATION

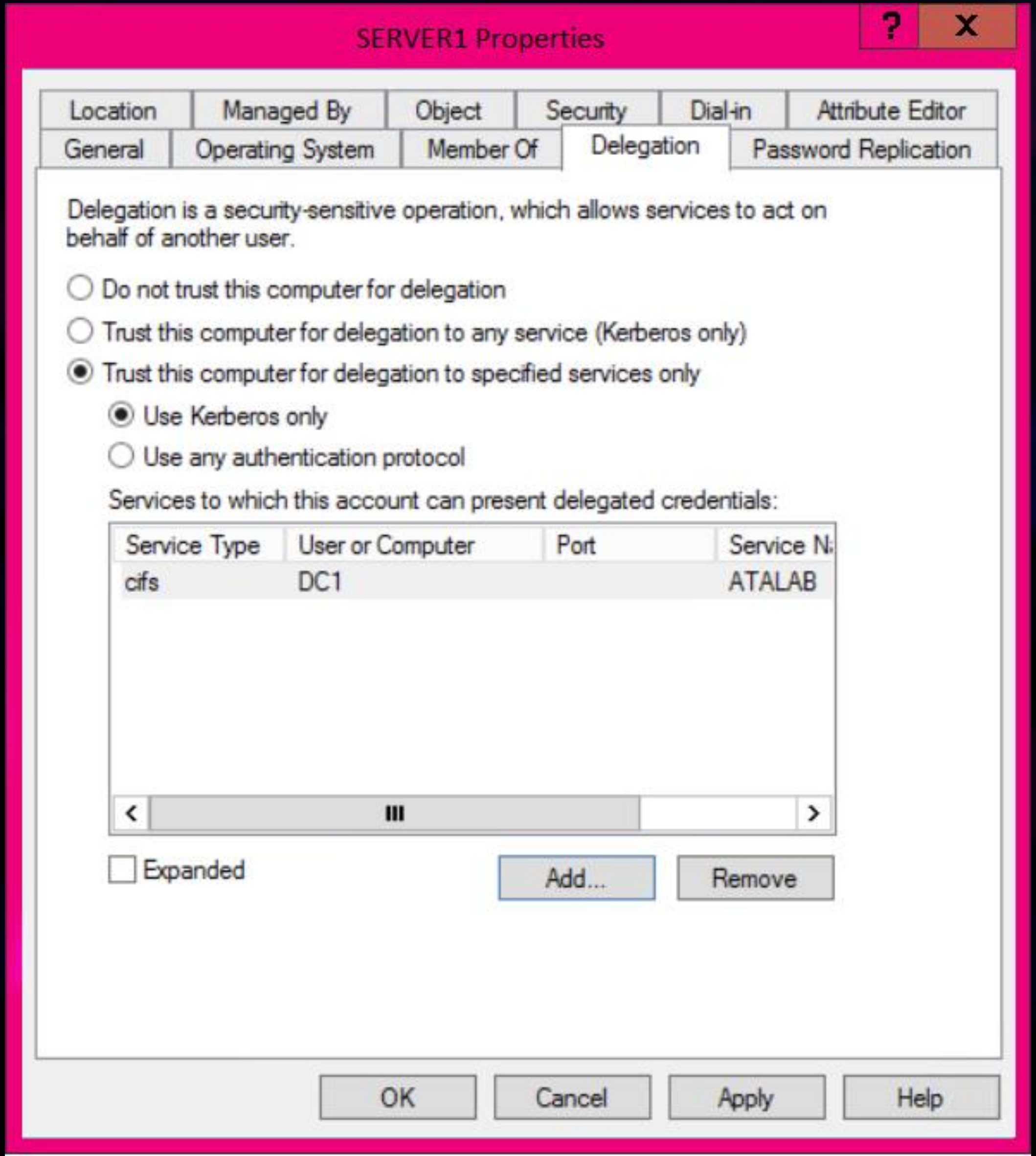
- Why?
  - An application reusing user credentials
  - Web server accessing a SQL DB
- How?
  - Request tickets on behalf of the user



> INTRODUCTION

▪ DELEGATION TAB

- **UNCONSTRAINED DELEGATION**
  - Delegation to any service
- **CONSTRAINED DELEGATION**
  - Kerberos Only (S4U2Proxy)
  - Protocol Transition (S4U2Self + S4U2Proxy)



SERVER1 Properties

Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this computer for delegation

○ Trust this computer for delegation to any service (Kerberos only)

● Trust this computer for delegation to specified services only

● Use Kerberos only

○ Use any authentication protocol

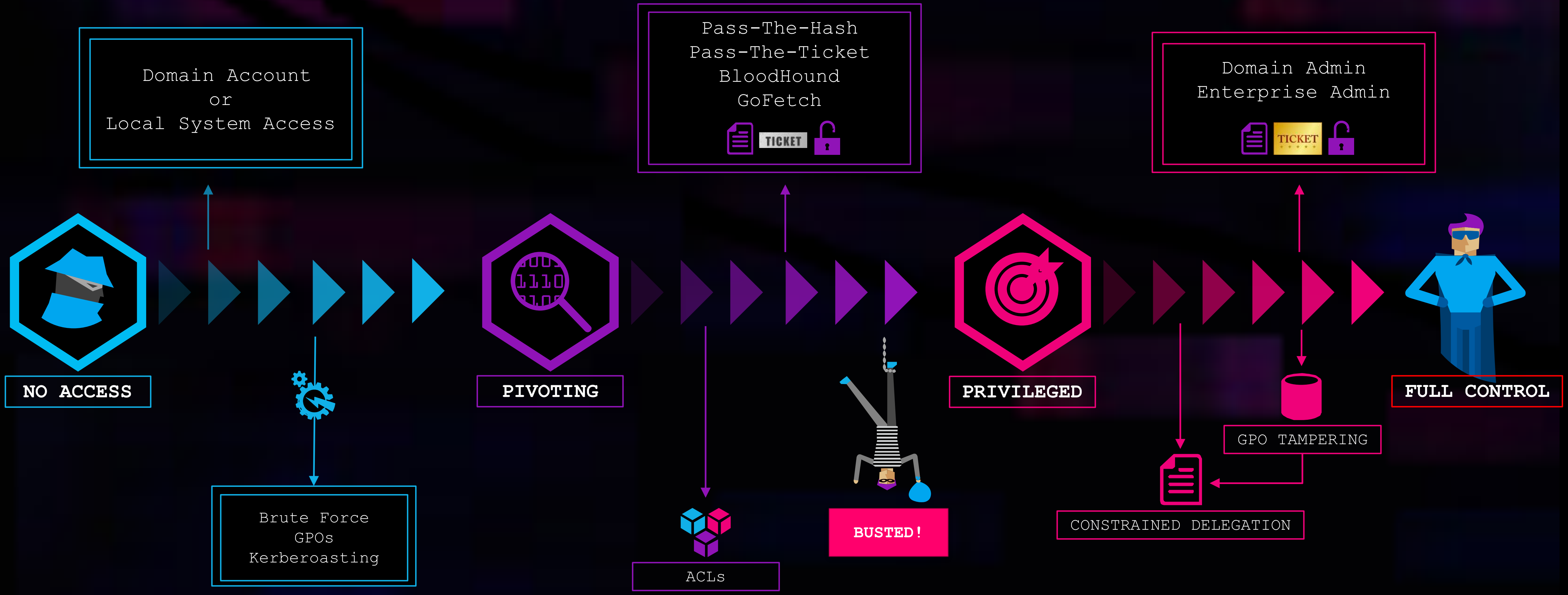
Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Service N:
cifs	DC1		ATALAB

□ Expanded

GAINING PERSISTENCE

FROM ZERO TO HERO



NO ACCESS

Domain Account
or
Local System Access

Brute Force
GPOs
Kerberoasting

PIVOTING

Pass-The-Hash
Pass-The-Ticket
BloodHound
GoFetch

ACLs

BUSTED!

PRIVILEGED

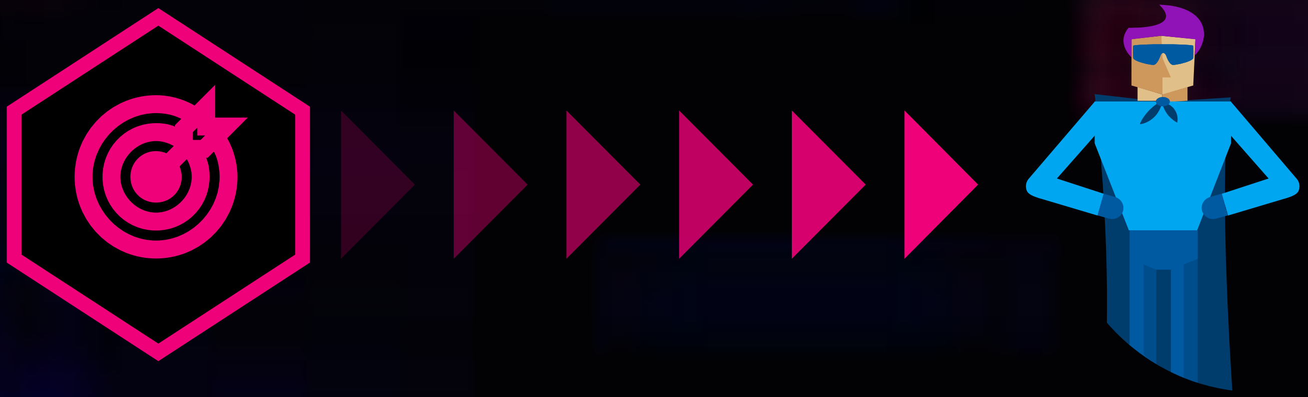
Domain Admin
Enterprise Admin

GPO TAMPERING

CONSTRAINED DELEGATION

FULL CONTROL

PERSISTENCE – PRIVILEGED



PERSISTENCE - PRIVILEGED

- **COMMON METHODS**
  - Dump NTDS.dit (VSS, DRSUAPI)
  - Golden ticket
  - Skeleton key

- **WEAKNESSES**
  - Replication requests from a non-DC machine
  - Detect crafted tickets
  - Encryption downgrade

JUST IN TIME ADMINISTRATION (JIT)

PERSISTENCE - PRIVILEGED

JIT (JUST-IN-TIME) ADMINISTRATION

- Accounts holding permanent high privileges serve as valuable targets for attackers
- JIT Administration
  - High privileges are required to perform an operation
  - Get the required privileges for a limited amount of time
  - When the time period expires, the high privileges are revoked
- Reduces the attack surface

PERSISTENCE - PRIVILEGED

- MAL-JIT (MALICIOUS-JUST-IN-TIME)
  - Get administrative access for a limited time
  - Perform malicious operations
  - Leave no traces behind to avoid detection

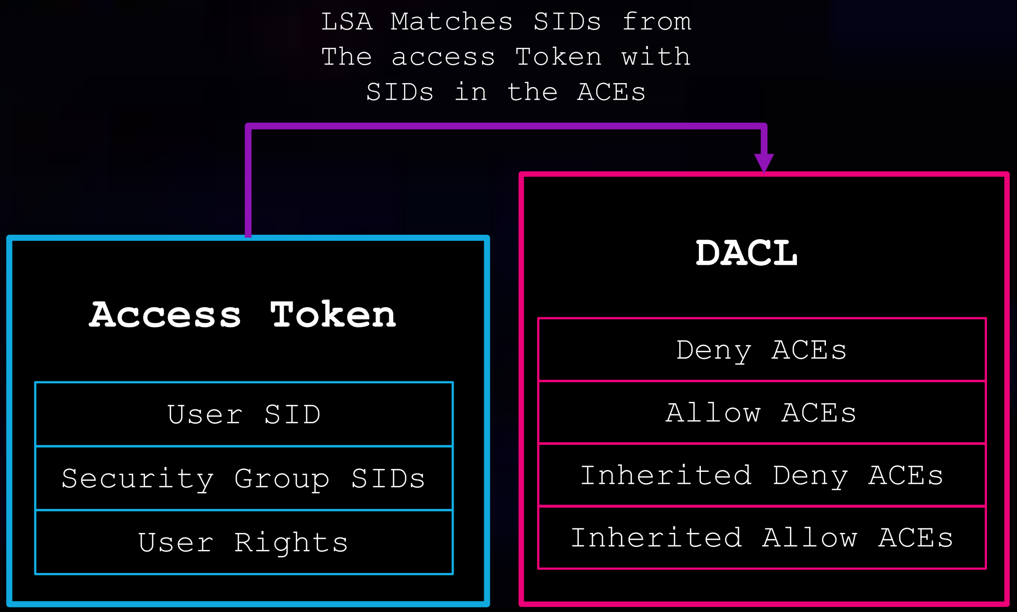
- SCENARIOS
  - Delegation scenario
  - AdminSDHolder scenario 1
  - AdminSDHolder scenario 2

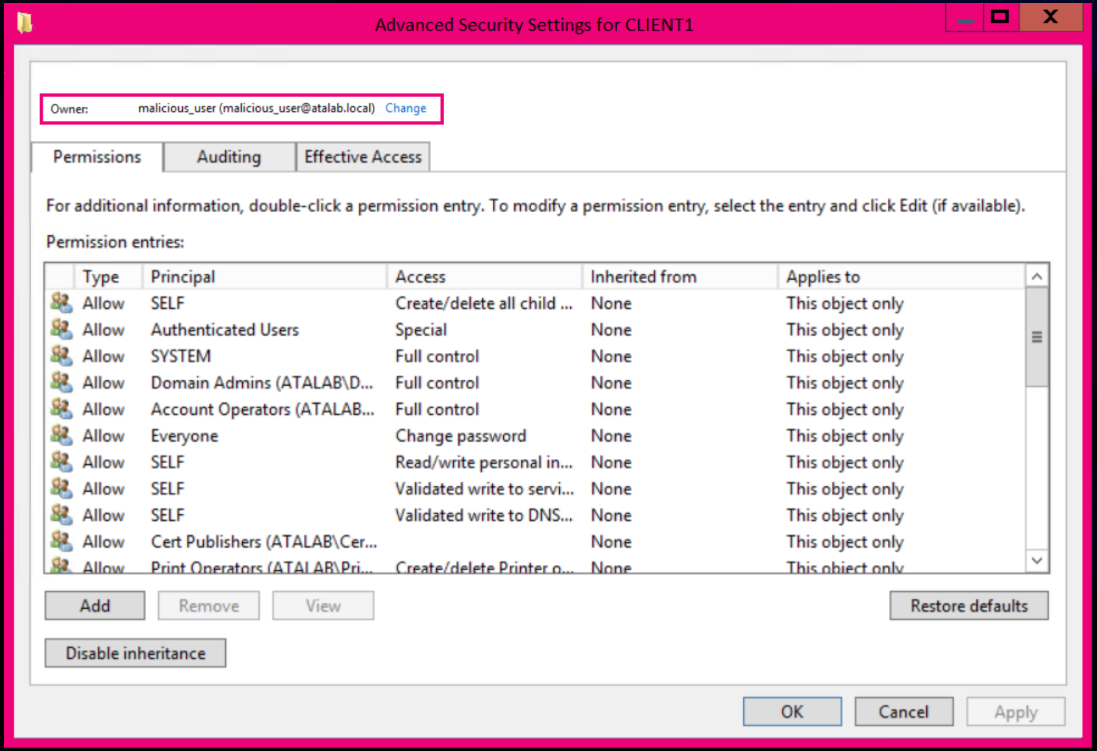
MALICIOUS JIT
DELEGATION SCENARIO

PERSISTENCE - PRIVILEGED

▪ OBJECTS INTRO

- Object Ownership
- Discretionary Access Control List (DACL)
- Access control entries (ACE)




Advanced Security Settings for CLIENT1

Owner: malicious_user (malicious_user@atalab.local) Change

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

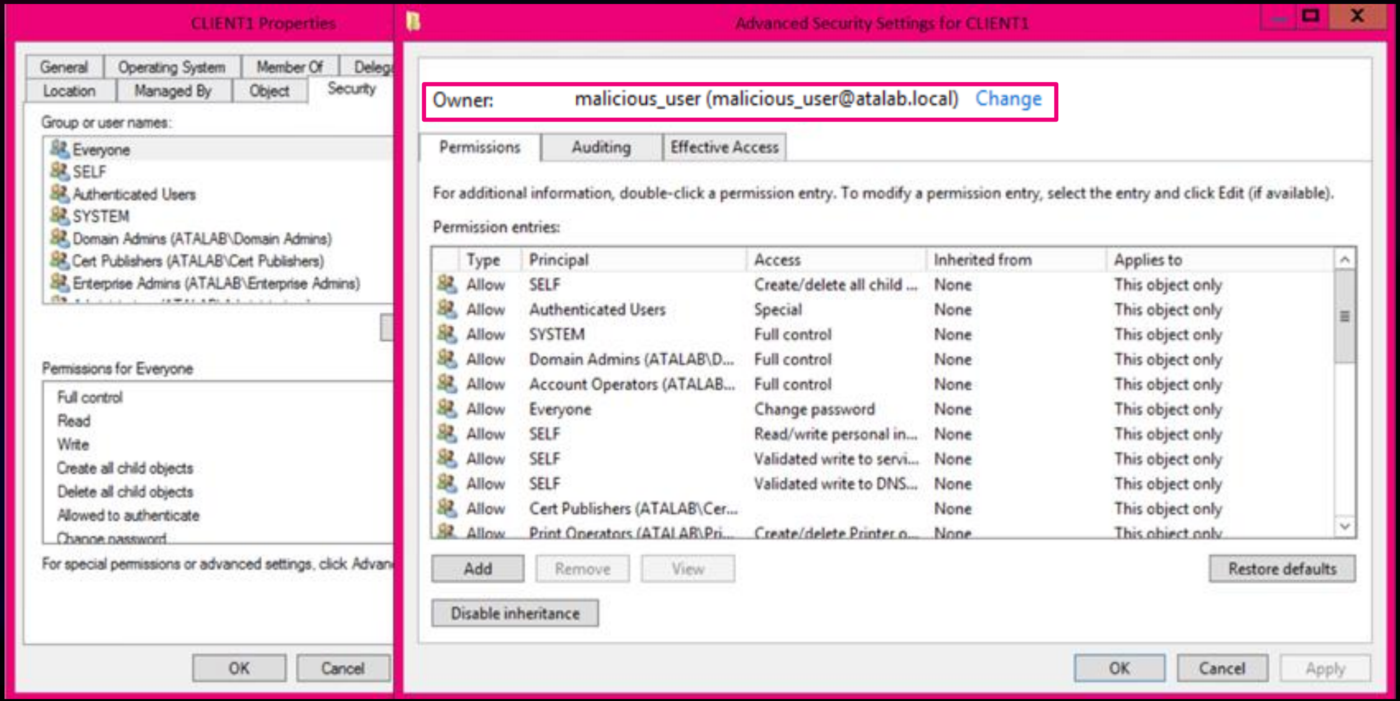
Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	SELF	Create/delete all child ...	None	This object only
Allow	Authenticated Users	Special	None	This object only
Allow	SYSTEM	Full control	None	This object only
Allow	Domain Admins (ATALAB\D...	Full control	None	This object only
Allow	Account Operators (ATALAB...	Full control	None	This object only
Allow	Everyone	Change password	None	This object only
Allow	SELF	Read/write personal in...	None	This object only
Allow	SELF	Validated write to servi...	None	This object only
Allow	SELF	Validated write to DNS...	None	This object only
Allow	Cert Publishers (ATALAB\Cer...		None	This object only
Allow	Print Operators (ATALAB\Pri...	Create/delete Printer o...	None	This object only

PERSISTENCE - PRIVILEGED

▪ DELEGATION SCENARIO

- Add a new machine account
- Set machine owner to a malicious account
  - Owner can edit the ACL of the object



Group or user names:

- Everyone
- SELF
- Authenticated Users
- SYSTEM
- Domain Admins (ATALAB\Domain Admins)
- Cert Publishers (ATALAB\Cert Publishers)
- Enterprise Admins (ATALAB\Enterprise Admins)

Permissions for Everyone

- Full control
- Read
- Write
- Create all child objects
- Delete all child objects
- Allowed to authenticate
- Change password

For special permissions or advanced settings, click Advan

Owner: malicious_user (malicious_user@atalab.local) Change

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

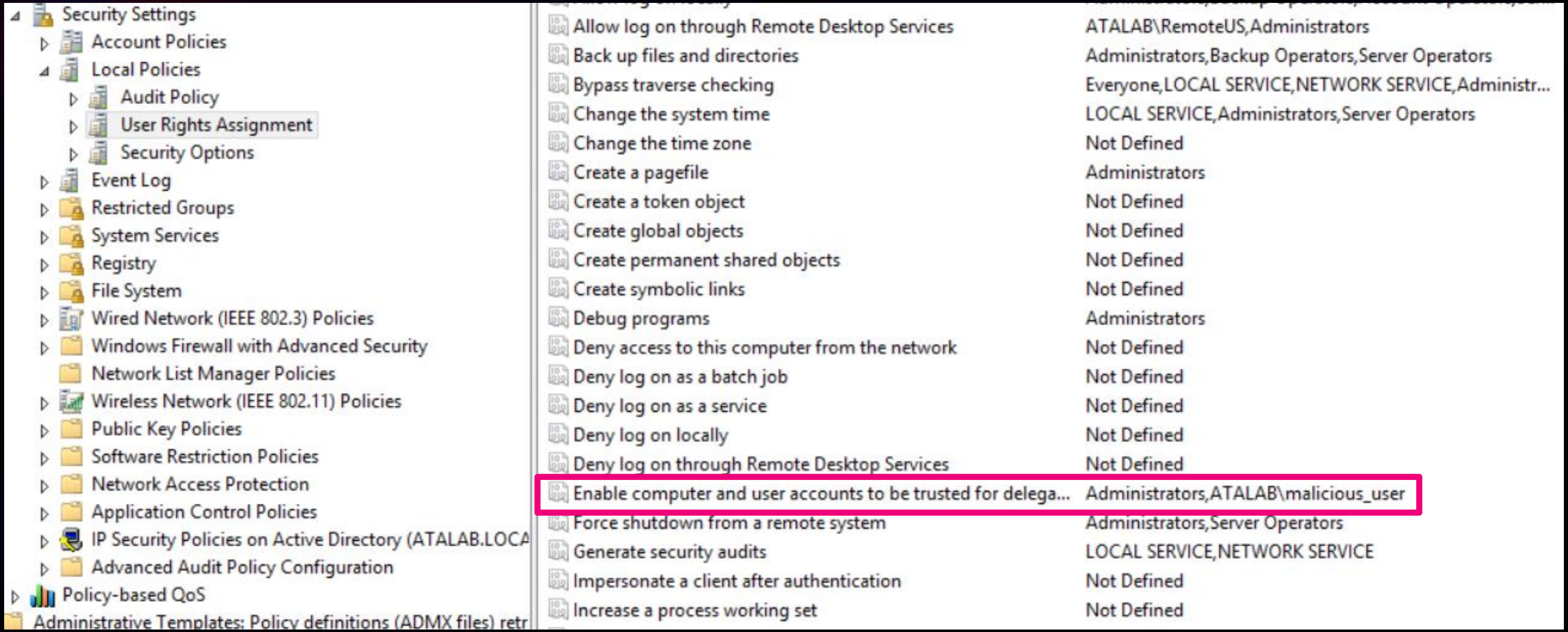
Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	SELF	Create/delete all child ...	None	This object only
Allow	Authenticated Users	Special	None	This object only
Allow	SYSTEM	Full control	None	This object only
Allow	Domain Admins (ATALAB\D...	Full control	None	This object only
Allow	Account Operators (ATALAB...	Full control	None	This object only
Allow	Everyone	Change password	None	This object only
Allow	SELF	Read/write personal in...	None	This object only
Allow	SELF	Validated write to servi...	None	This object only
Allow	SELF	Validated write to DNS...	None	This object only
Allow	Cert Publishers (ATALAB\Cer...		None	This object only
Allow	Print Operators (ATALAB\Pri...	Create/delete Printer o...	None	This object only

PERSISTENCE - PRIVILEGED

▪ DELEGATION SCENARIO

- GPO Tampering: “Enable accounts to be trusted for delegation”



- Security Settings
  - Account Policies
  - Local Policies
    - Audit Policy
    - User Rights Assignment
    - Security Options
  - Event Log
  - Restricted Groups
  - System Services
  - Registry
  - File System
  - Wired Network (IEEE 802.3) Policies
  - Windows Firewall with Advanced Security
  - Network List Manager Policies
  - Wireless Network (IEEE 802.11) Policies
  - Public Key Policies
  - Software Restriction Policies
  - Network Access Protection
  - Application Control Policies
  - IP Security Policies on Active Directory (ATALAB.LOCA
  - Advanced Audit Policy Configuration
- Policy-based QoS
- Administrative Templates: Policy definitions (ADMX files) retr

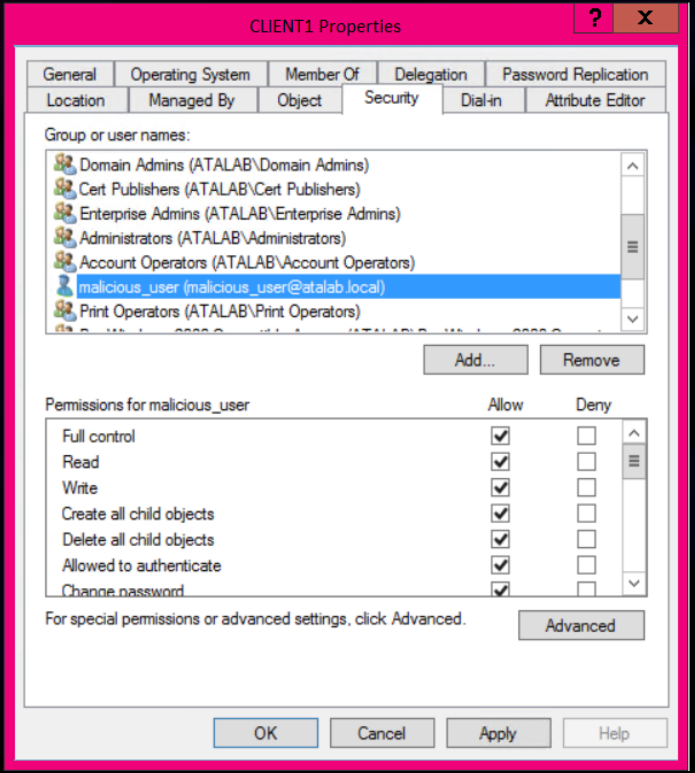
Allow log on through Remote Desktop Services	ATALAB\RemoteUS,Administrators
Back up files and directories	Administrators,Backup Operators,Server Operators
Bypass traverse checking	Everyone,LOCAL SERVICE,NETWORK SERVICE,Administr...
Change the system time	LOCAL SERVICE,Administrators,Server Operators
Change the time zone	Not Defined
Create a pagefile	Administrators
Create a token object	Not Defined
Create global objects	Not Defined
Create permanent shared objects	Not Defined
Create symbolic links	Not Defined
Debug programs	Administrators
Deny access to this computer from the network	Not Defined
Deny log on as a batch job	Not Defined
Deny log on as a service	Not Defined
Deny log on locally	Not Defined
Deny log on through Remote Desktop Services	Not Defined
Enable computer and user accounts to be trusted for delega...	Administrators,ATALAB\malicious_user
Force shutdown from a remote system	Administrators,Server Operators
Generate security audits	LOCAL SERVICE,NETWORK SERVICE
Impersonate a client after authentication	Not Defined
Increase a process working set	Not Defined

I lost all of my administrative rights

PERSISTENCE - PRIVILEGED

▪ DELEGATION SCENARIO – MAL-JIT

- DACL Modification:
  - Add ‘GenericAll’ ACE for malicious_user on new machine



CLIENT1 Properties

Group or user names:

- Domain Admins (ATALAB\Domain Admins)
- Cert Publishers (ATALAB\Cert Publishers)
- Enterprise Admins (ATALAB\Enterprise Admins)
- Administrators (ATALAB\Administrators)
- Account Operators (ATALAB\Account Operators)
- malicious_user (malicious_user@atalab.local)
- Print Operators (ATALAB\Print Operators)

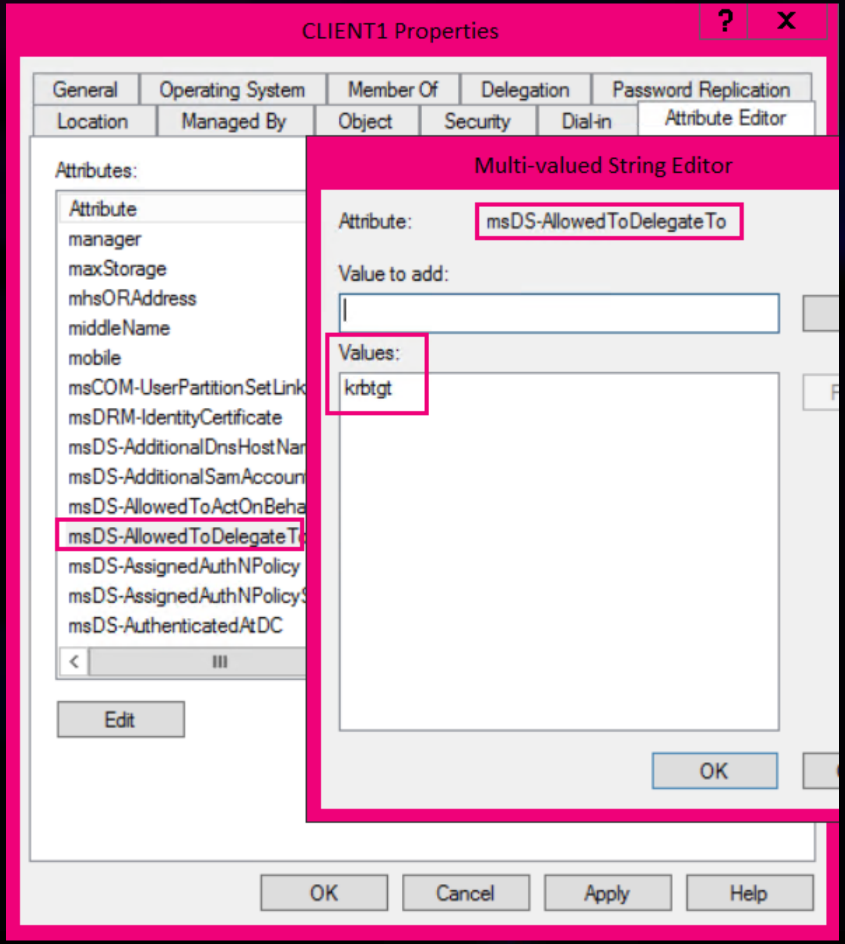
Permissions for malicious_user	Allow	Deny
Full control	☑	□
Read	☑	□
Write	☑	□
Create all child objects	☑	□
Delete all child objects	☑	□
Allowed to authenticate	☑	□
Change password	☑	□

For special permissions or advanced settings, click Advanced.

PERSISTENCE - PRIVILEGED

▪ DELEGATION SCENARIO – MAL-JIT

- Allow delegation to krbtgt
- Request 'Administrator' TGT
- Remove footprints:
  - Remove delegation
  - Revert ACL
- Perform malicious operations



CLIENT1 Properties

Multi-valued String Editor

Attribute: msDS-AllowedToDelegateTo

Value to add:

Values:
krbtgt

MAL-JIT SUCCESSFUL!

< DEMO 1 >

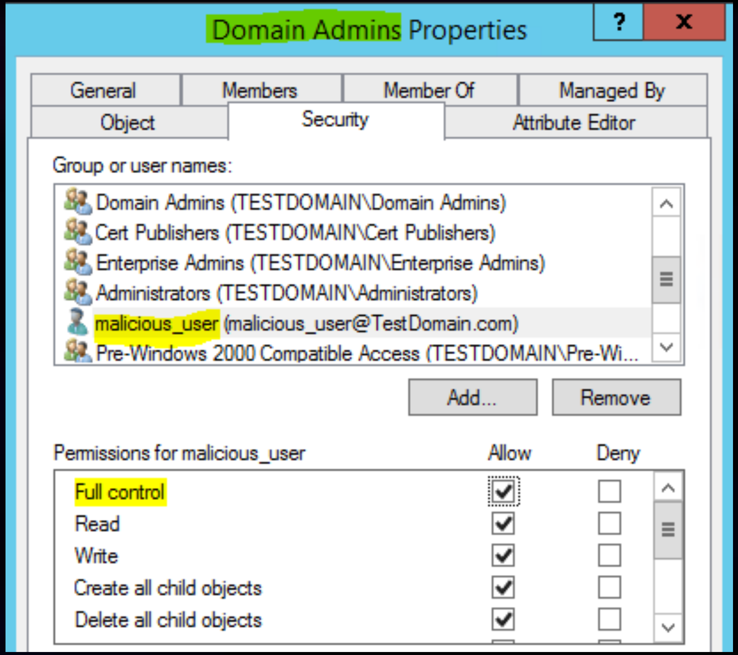
MALICIOUS JIT

ADMINSDHOLDER MANIPULATION 1

PERSISTENCE - PRIVILEGED

ADMINSDHOLDER MANIPULATION 1

- Persistence can be obtained by ACL modification of privileged groups – such as 'Domain Admins'



Group or user names:

- Domain Admins (TESTDOMAIN\Domain Admins)
- Cert Publishers (TESTDOMAIN\Cert Publishers)
- Enterprise Admins (TESTDOMAIN\Enterprise Admins)
- Administrators (TESTDOMAIN\Administrators)
- malicious_user (malicious_user@TestDomain.com)
- Pre-Windows 2000 Compatible Access (TESTDOMAIN\Pre-Wi...

Permissions for malicious_user	Allow	Deny
Full control	☑	☐
Read	☑	☐
Write	☑	☐
Create all child objects	☑	☐
Delete all child objects	☑	☐

- Problem: AdminSDHolder!

PERSISTENCE - PRIVILEGED

ADMINSDHOLDER MANIPULATION 1

- SDProp overrides the ACLs of protected groups & users with the AdminSDHolder ACL
- Runs periodically (default: 1 hour)
- Result: malicious_user loses his permission

- Protected accounts:
  - Enterprise Admins
  - Domain Admins
  - Administrators
  - …

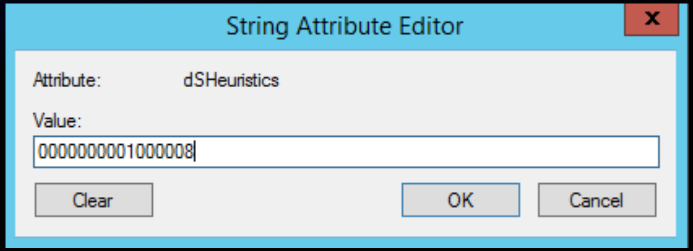
PERSISTENCE - PRIVILEGED

ADMINSDHOLDER MANIPULATION 1

- The following groups can be excluded from the AdminSDHolder protection:

Bit	Group to Exclude	Binary Value	Hexadecimal Value
0	Account Operators	0001	1
1	Server Operators	0010	2
2	Print Operators	0100	4
3	Backup Operators	1000	8

- Exclude groups by editing the ‘dsHeuristics’ attribute under the Configuration Container


String Attribute Editor

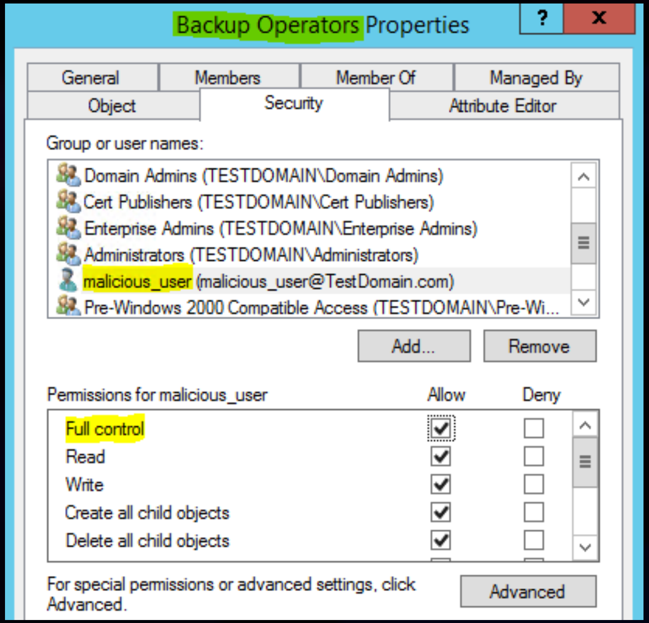
Attribute: dSHeuristics

Value: 0000000001000008

PERSISTENCE - PRIVILEGED

ADMINSDHOLDER MANIPULATION 1

- Add ACEs to excluded groups



Backup Operators Properties

Group or user names:

- Domain Admins (TESTDOMAIN\Domain Admins)
- Cert Publishers (TESTDOMAIN\Cert Publishers)
- Enterprise Admins (TESTDOMAIN\Enterprise Admins)
- Administrators (TESTDOMAIN\Administrators)
- malicious_user (malicious_user@TestDomain.com)
- Pre-Windows 2000 Compatible Access (TESTDOMAIN\Pre-Wi...

Permissions for malicious_user	Allow	Deny
Full control	☑	□
Read	☑	□
Write	☑	□
Create all child objects	☑	□
Delete all child objects	☑	□

For special permissions or advanced settings, click Advanced.

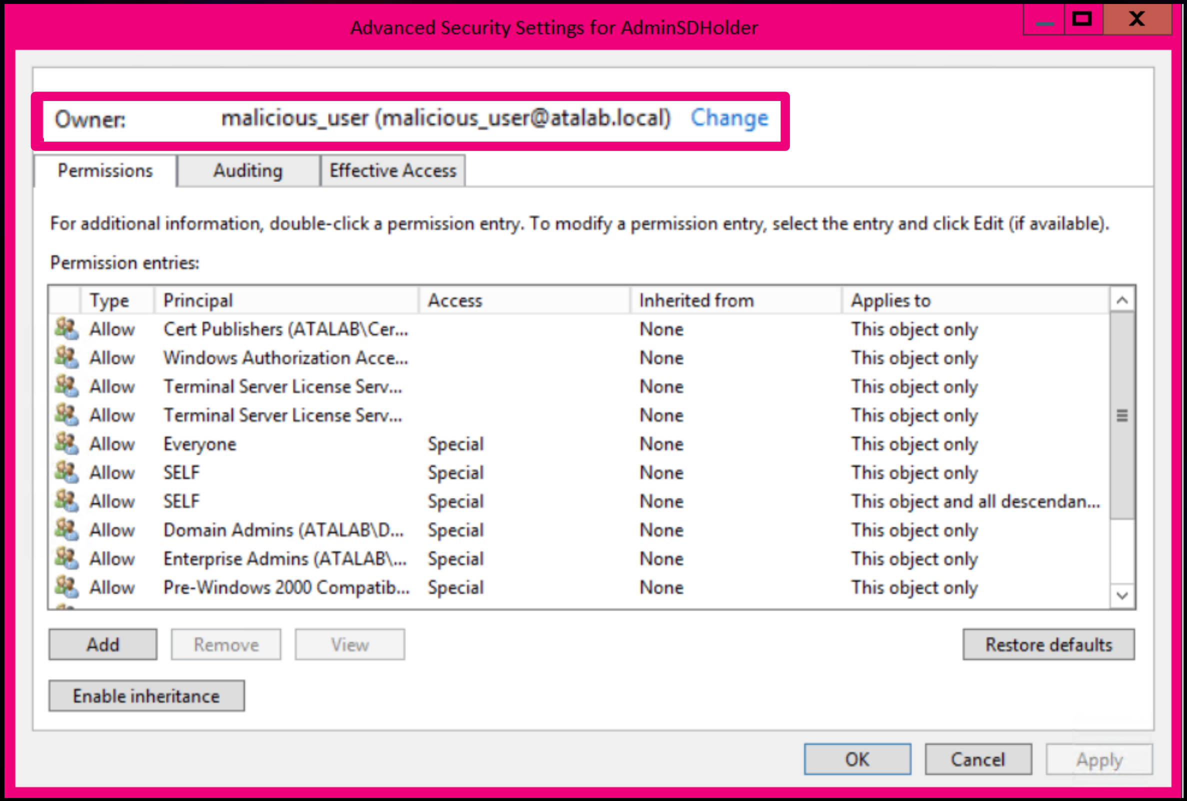
- SDProp will not affect the new ACL
- Malicious JIT at any time!

MALICIOUS JIT
ADMINSDHOLDER MANIPULATION 2

PERSISTENCE - PRIVILEGED

ADMINSDHOLDER MANIPULATION 2

- Change the owner of the AdminSDHolder object
- Still not allowed to modify group memberships



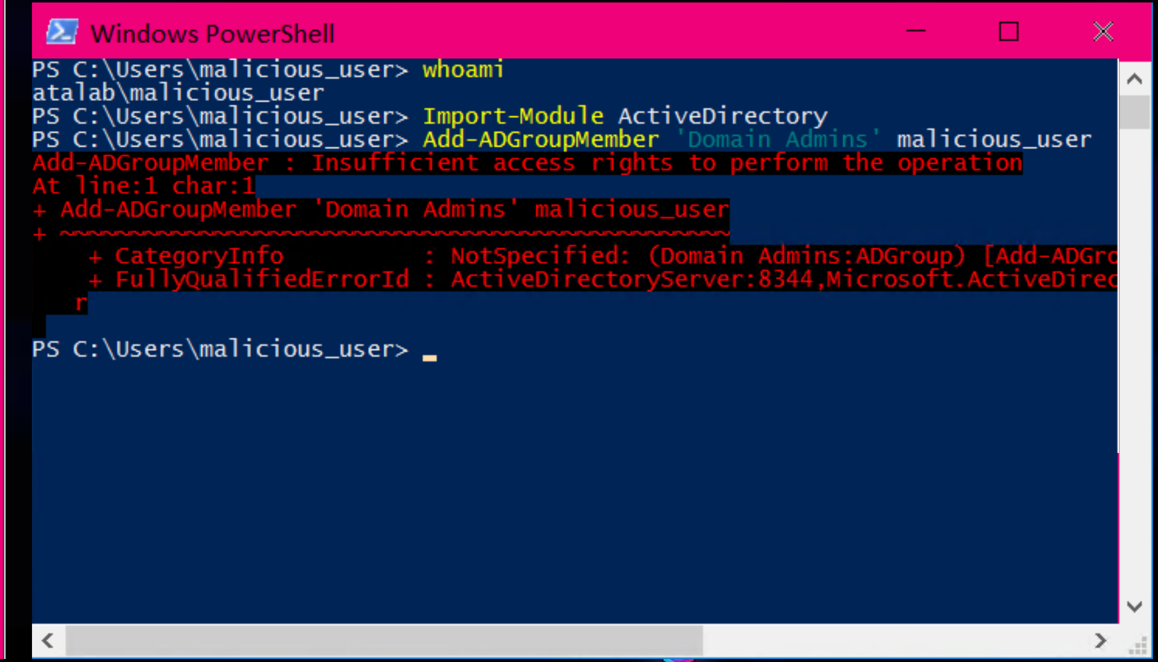
Advanced Security Settings for AdminSDHolder

Owner: malicious_user (malicious_user@atalab.local) Change

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

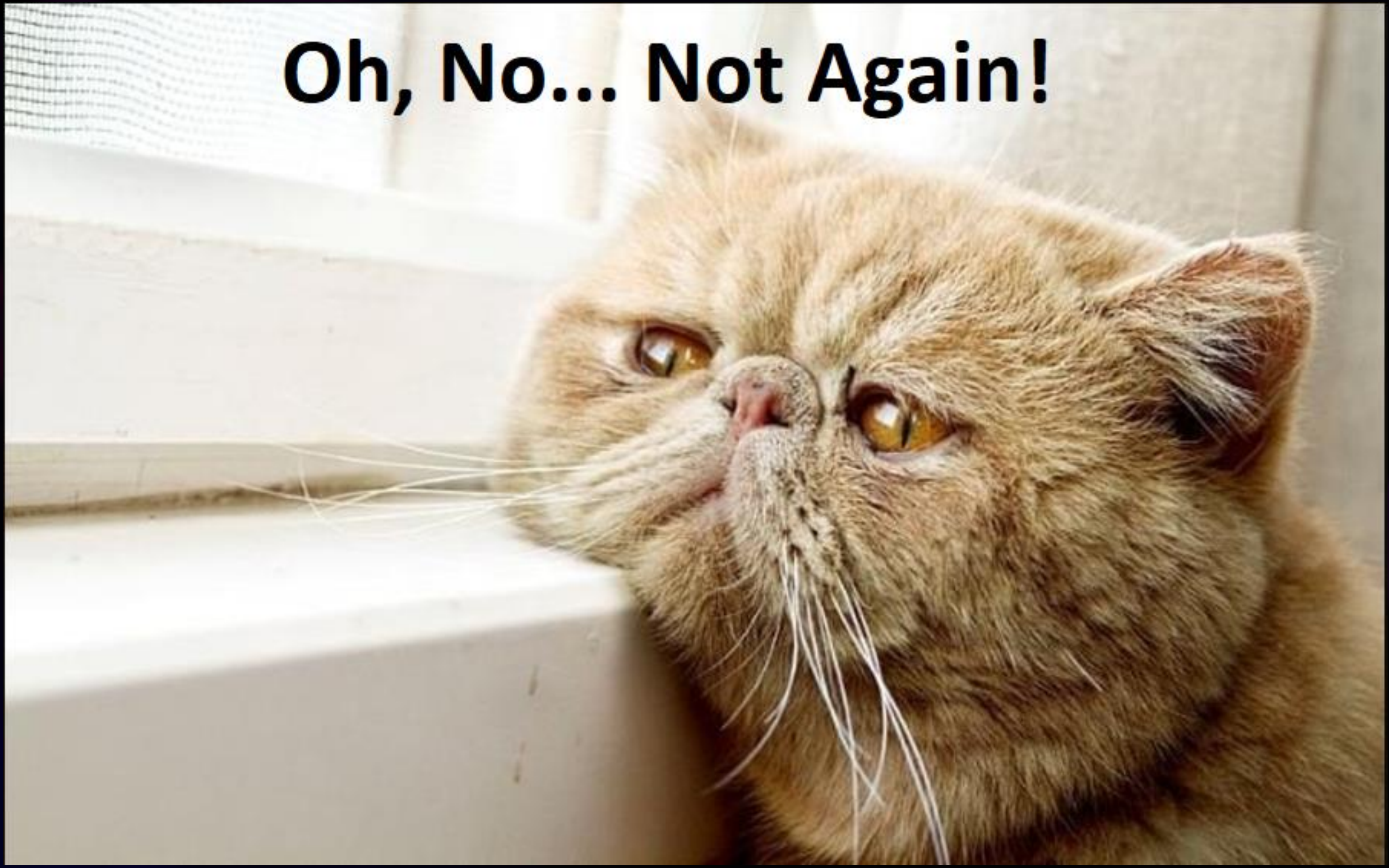
Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	Cert Publishers (ATALAB\Cer...		None	This object only
Allow	Windows Authorization Acce...		None	This object only
Allow	Terminal Server License Serv...		None	This object only
Allow	Terminal Server License Serv...		None	This object only
Allow	Everyone	Special	None	This object only
Allow	SELF	Special	None	This object only
Allow	SELF	Special	None	This object and all descendan...
Allow	Domain Admins (ATALAB\D...	Special	None	This object only
Allow	Enterprise Admins (ATALAB\...	Special	None	This object only
Allow	Pre-Windows 2000 Compatib...	Special	None	This object only



Windows PowerShell

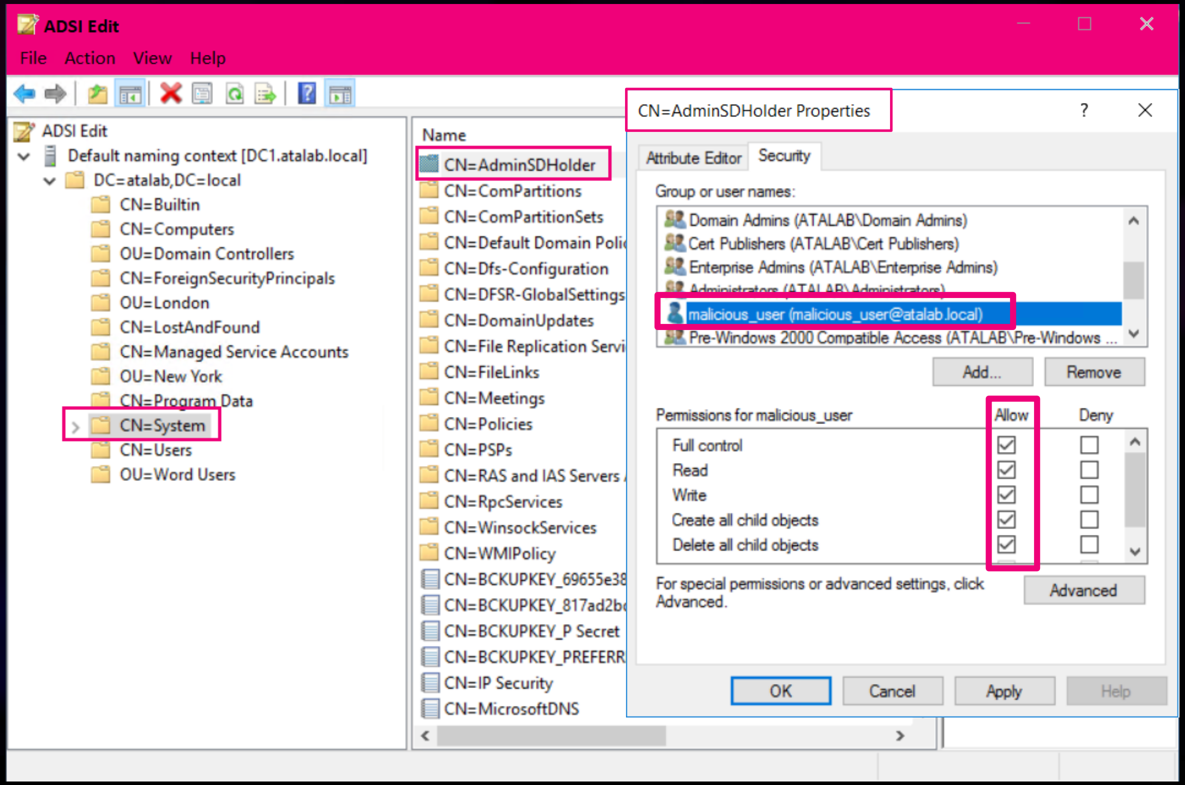
```
PS C:\Users\malicious_user> whoami
atalab\malicious_user
PS C:\Users\malicious_user> Import-Module ActiveDirectory
PS C:\Users\malicious_user> Add-ADGroupMember 'Domain Admins' malicious_user
Add-ADGroupMember : Insufficient access rights to perform the operation
At line:1 char:1
+ Add-ADGroupMember 'Domain Admins' malicious_user
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (Domain Admins:ADGroup) [Add-ADGro
    + FullyQualifiedErrorId : ActiveDirectoryServer:8344,Microsoft.ActiveDirec
   r

PS C:\Users\malicious_user> _
```


Oh, No… Not Again!

PERSISTENCE - PRIVILEGED

▪ ADMINSDHOLDER MANIPULATION 2 – MAL-JIT

- Just before SDProp is scheduled to run
  - Add malicious_user to the AdminSDHolder ACL



ADSI Edit
- Default naming context [DC1.atalab.local]
  - DC=atalab,DC=local
    - CN=Builtin
    - CN=Computers
    - OU=Domain Controllers
    - CN=ForeignSecurityPrincipals
    - OU=London
    - CN=LostAndFound
    - CN=Managed Service Accounts
    - OU=New York
    - CN=Program Data
    - CN=System
    - CN=Users
    - OU=Word Users

Name
- CN=AdminSDHolder
- CN=ComPartitions
- CN=ComPartitionSets
- CN=Default Domain Poli
- CN=Dfs-Configuration
- CN=DFSR-GlobalSettings
- CN=DomainUpdates
- CN=File Replication Servi
- CN=FileLinks
- CN=Meetings
- CN=Policies
- CN=PSPs
- CN=RAS and IAS Servers
- CN=RpcServices
- CN=WinsockServices
- CN=WMIPolicy
- CN=BCKUPKEY_69655e38
- CN=BCKUPKEY_817ad2b
- CN=BCKUPKEY_P Secret
- CN=BCKUPKEY_PREFERR
- CN=IP Security
- CN=MicrosoftDNS

CN=AdminSDHolder Properties

Attribute Editor | Security

Group or user names:
- Domain Admins (ATALAB\Domain Admins)
- Cert Publishers (ATALAB\Cert Publishers)
- Enterprise Admins (ATALAB\Enterprise Admins)
- Administrators (ATALAB\Administrators)
- malicious_user (malicious_user@atalab.local)
- Pre-Windows 2000 Compatible Access (ATALAB\Pre-Windows ...

Add... Remove

Permissions for malicious_user	Allow	Deny
Full control	☑	□
Read	☑	□
Write	☑	□
Create all child objects	☑	□
Delete all child objects	☑	□

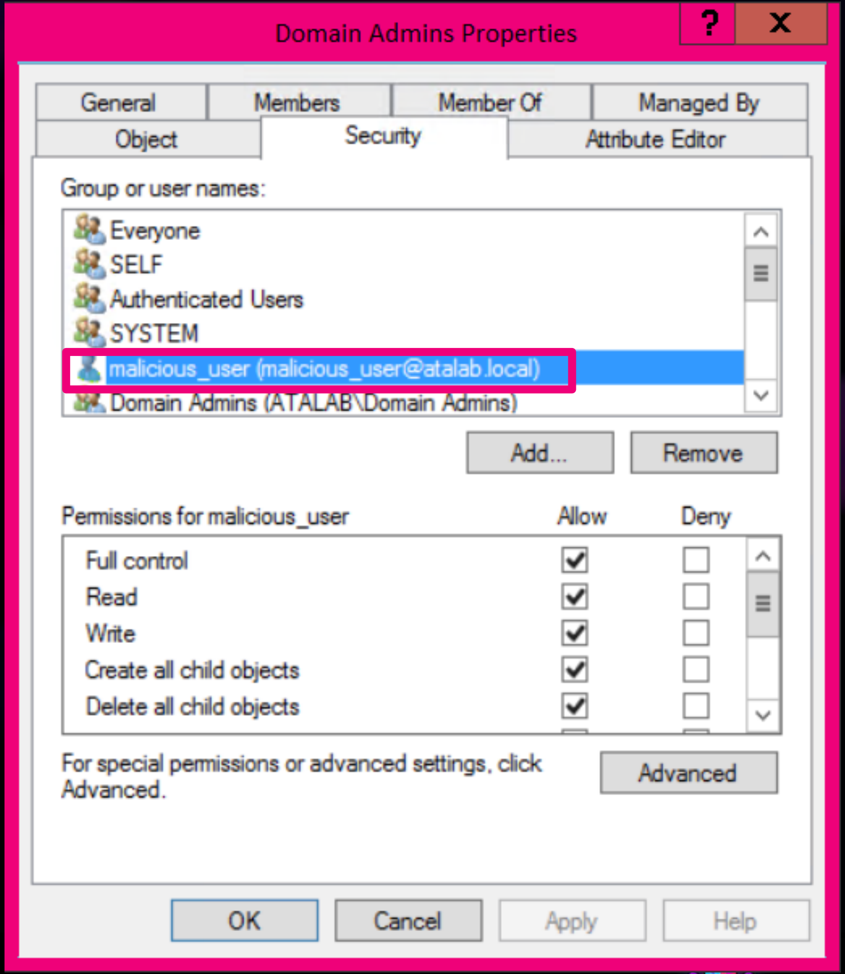
For special permissions or advanced settings, click Advanced.

Advanced

OK Cancel Apply Help

PERSISTENCE - PRIVILEGED

- ADMINSDHOLDER MANIPULATION 2 – MAL-JIT
  - SDProp adds malicious ACE to protected objects



Domain Admins Properties

Group or user names:

- Everyone
- SELF
- Authenticated Users
- SYSTEM
- malicious_user (malicious_user@atalab.local)
- Domain Admins (ATALAB\Domain Admins)

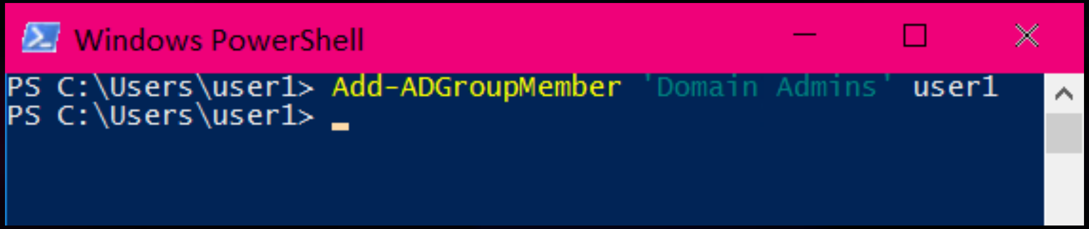
Permissions for malicious_user	Allow	Deny
Full control	☑	□
Read	☑	□
Write	☑	□
Create all child objects	☑	□
Delete all child objects	☑	□

For special permissions or advanced settings, click Advanced.

PERSISTENCE - PRIVILEGED

▪ ADMINSDHOLDER MANIPULATION 2 – MAL-JIT

- Add malicious_user to ‘Domain Admins’ group



```
PS C:\Users\user1> Add-ADGroupMember 'Domain Admins' user1
PS C:\Users\user1> _
```

- Obtain administrative TGT
- Revert (erase footprints)
  - Remove malicious_user from AdminSDHolder’s ACL
  - Force SDProp to run: removes malicious ACE from protected groups
  - Remove malicious_user from ‘Domain Admins’ group*

- **Entire operation can be automated to run in seconds!**

< DEMO 2 >

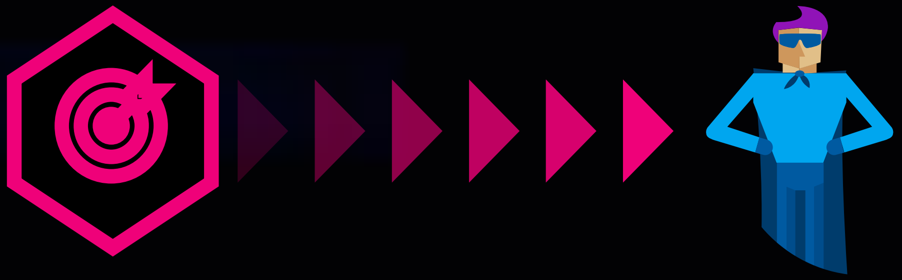
> MITIGATIONS

DETECT DELEGATION MISCONFIGURATIONS

- ‘Account is sensitive and cannot be delegated’
- GPO: ‘Enable accounts to be trusted for delegation’
- Monitor accounts trusted for delegation
- ‘AllowedToDelegateTo’ attribute

MONITOR ADMINSDHOLDER

- ACL
- Owner
- Excluded groups



QUESTIONS ?