n|u DUBAI

nullDUBAI

JUNE 29 2018

Speaker

Pralhad Chaskar

Auditing ACLs on Active Directory

Auditing ACLs on Active Directory

by Pralhad Chaskar (@c0d3xpl0it)

Agenda

- Introduction
- What is ACL Background
- How to Audit ACL
- How to Abuse ACL
- Tools of Trade

What is Active Directory?

- Active Directory (AD) is a directory service that Microsoft developed for Windows domain networks.

Lets look at some ACL background...

Securable Objects

- A securable object is an object that can have a security descriptor. All named Windows objects are securable.

Object type	Security descriptor functions
Files or directories on an NTFS file system	GetNamedSecurityInfo, SetNamedSecurityInfo, GetSecurityInfo, SetSecurityInfo
Named pipes Anonymous pipes	GetSecurityInfo, SetSecurityInfo
Processes Threads	GetSecurityInfo, SetSecurityInfo
File-mapping objects	GetNamedSecurityInfo, SetNamedSecurityInfo, GetSecurityInfo, SetSecurityInfo
Access tokens	SetKernelObjectSecurity, GetKernelObjectSecurity
Window-management objects (window stations and desktops)	GetSecurityInfo, SetSecurityInfo
Registry keys	GetNamedSecurityInfo, SetNamedSecurityInfo, GetSecurityInfo, SetSecurityInfo
Windows services	GetNamedSecurityInfo, SetNamedSecurityInfo, GetSecurityInfo, SetSecurityInfo
Local or remote printers	GetNamedSecurityInfo, SetNamedSecurityInfo, GetSecurityInfo, SetSecurityInfo
Network shares	GetNamedSecurityInfo, SetNamedSecurityInfo, GetSecurityInfo, SetSecurityInfo
Interprocess synchronization objects (events, mutexes, semaphores, and waitable timers)	GetNamedSecurityInfo, SetNamedSecurityInfo, GetSecurityInfo, SetSecurityInfo

https://msdn.microsoft.com/en-us/library/windows/desktop/aa379557(v=vs.85).aspx

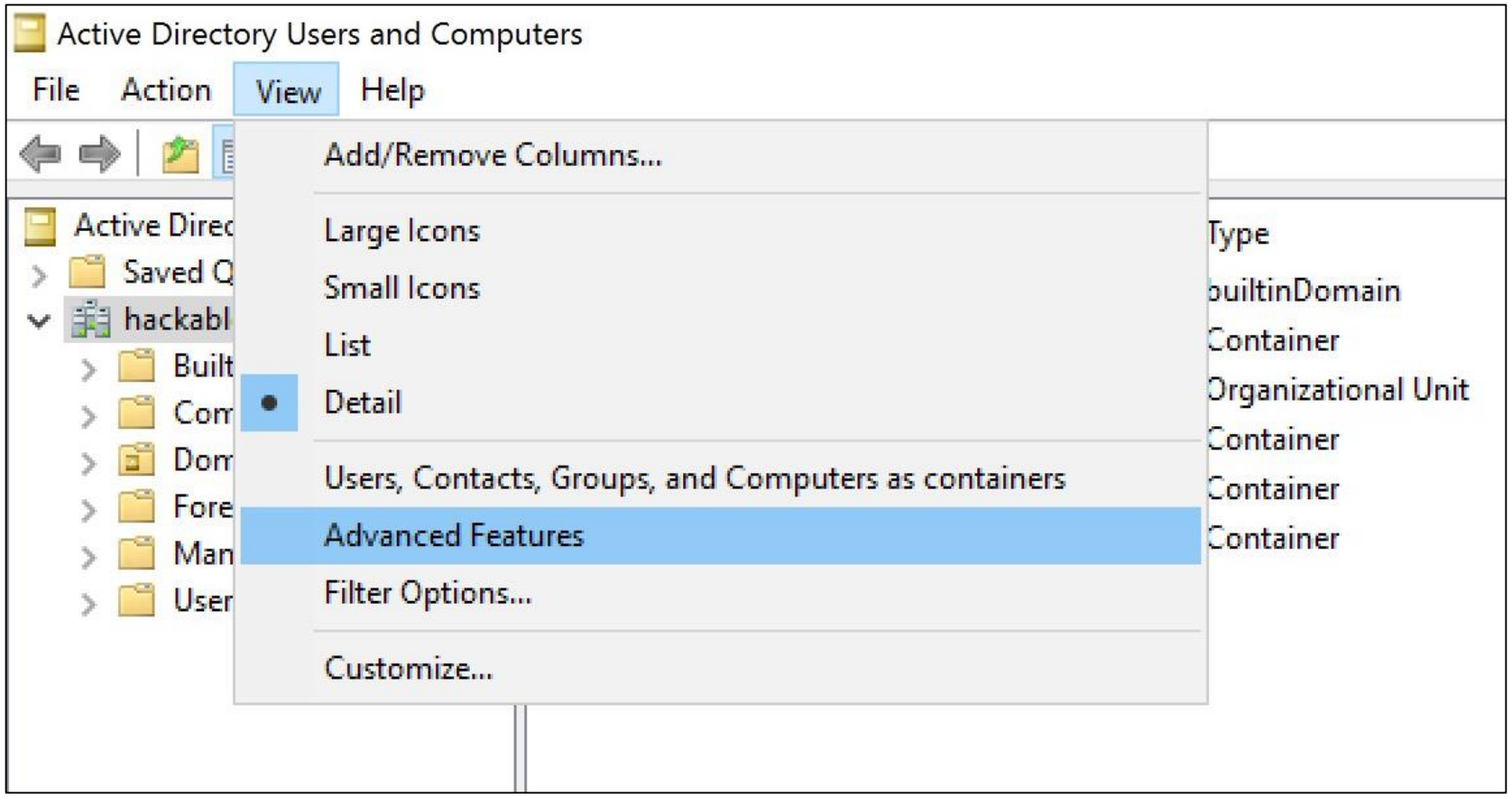
Security Descriptors

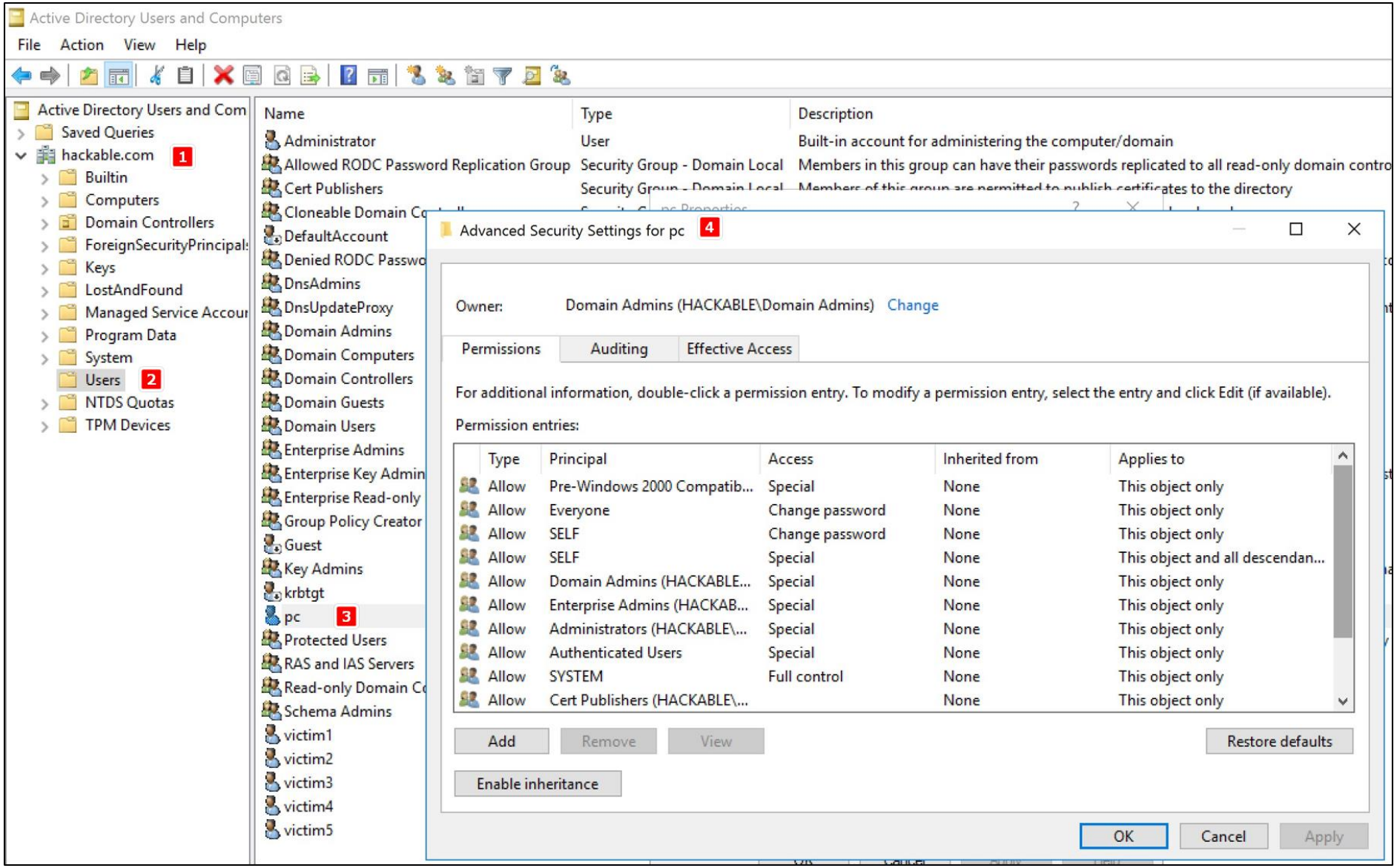
A *security descriptor* contains the security information associated with a securable object. A security descriptor consists of a **SECURITY_DESCRIPTOR** structure and its associated security information. A security descriptor can include the following security information:

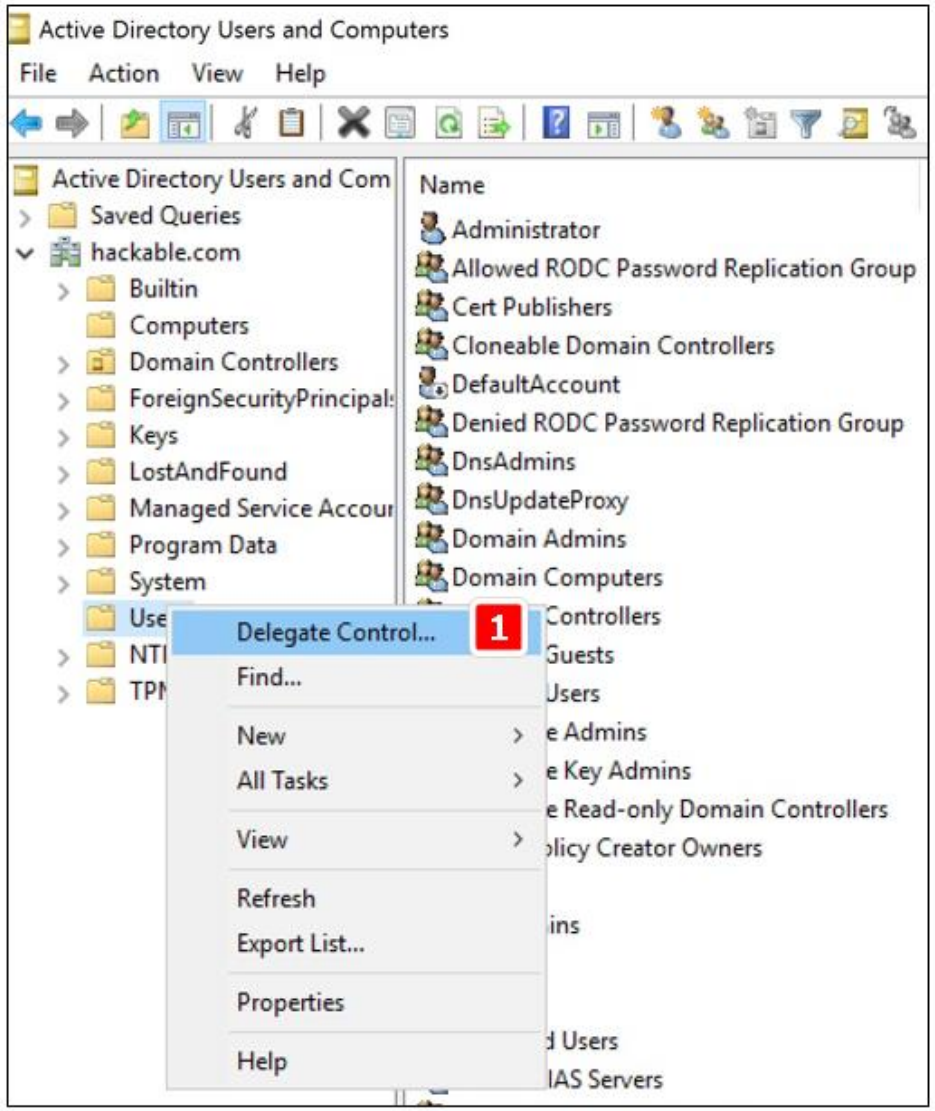
- Security identifiers (SIDs) for the owner and primary group of an object.
- A DACL that specifies the access rights allowed or denied to particular users or groups.
- A SACL that specifies the types of access attempts that generate audit records for the object.
- A set of control bits that qualify the meaning of a security descriptor or its individual members.

https://msdn.microsoft.com/en-us/library/windows/desktop/aa379563(v=vs.85).aspx

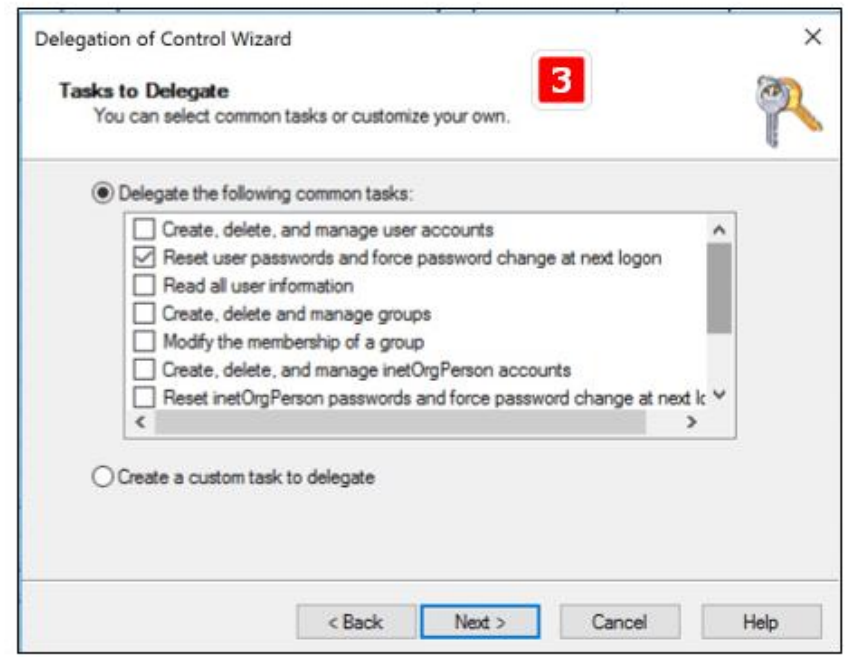
Advanced Feature in ADUC



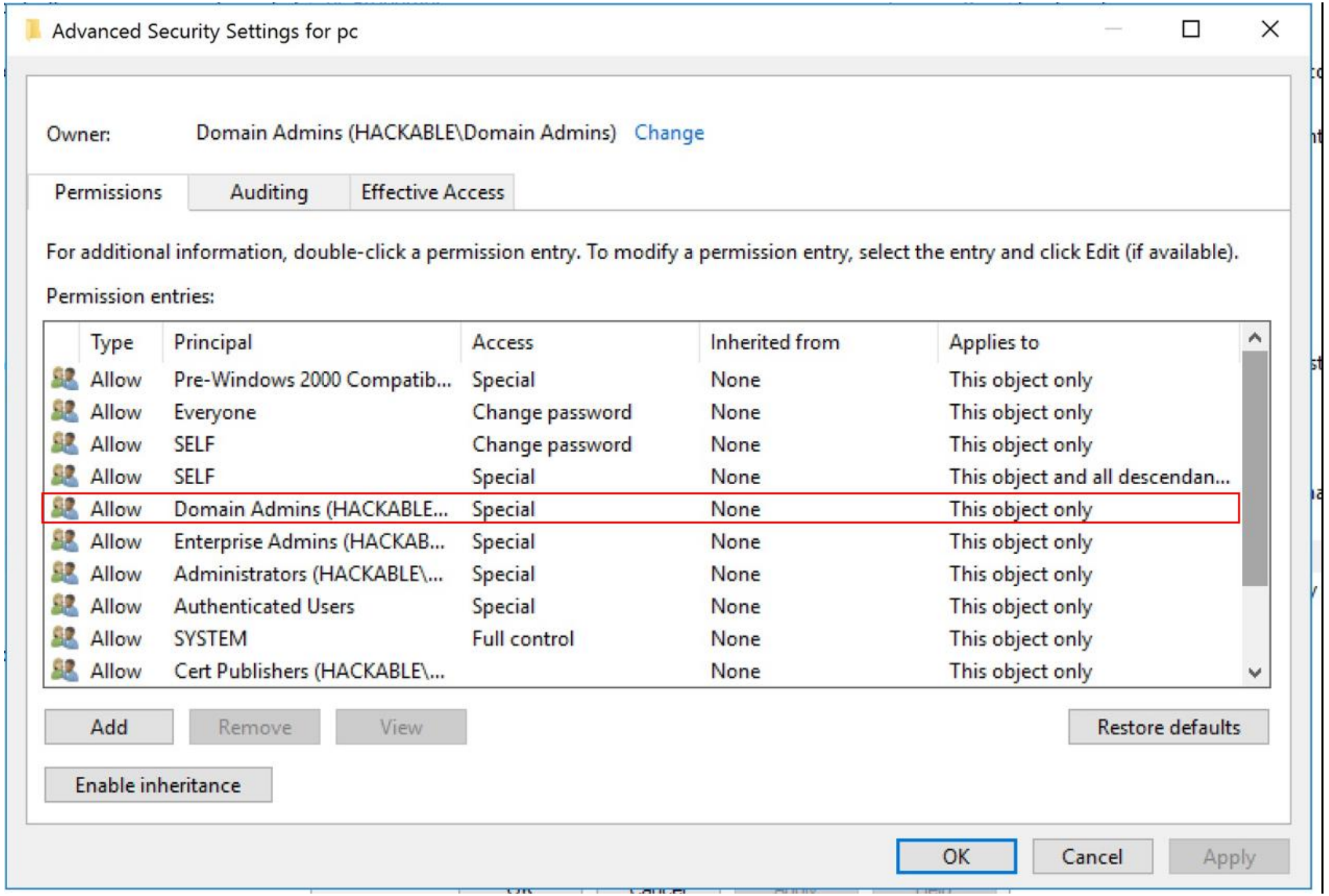

Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
hackable.com 1
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal
Keys
LostAndFound
Managed Service Accou
Program Data
System
Users 2
NTDS Quotas
TPM Devices
Name Type Description
Administrator User Built-in account for administering the computer/domain
Allowed RODC Password Replication Group Security Group - Domain Local Members in this group can have their passwords replicated to all read-only domain contro
Cert Publishers Security Group - Domain Local Members of this group are permitted to publish certificates to the directory
Cloneable Domain Co
DefaultAccount
Denied RODC Passwo
DnsAdmins
DnsUpdateProxy
Domain Admins
Domain Computers
Domain Controllers
Domain Guests
Domain Users
Enterprise Admins
Enterprise Key Admin
Enterprise Read-only
Group Policy Creator
Guest
Key Admins
krbtgt
pc 3
Protected Users
RAS and IAS Servers
Read-only Domain C
Schema Admins
victim1
victim2
victim3
victim4
victim5
Advanced Security Settings for pc 4
Owner: Domain Admins (HACKABLE\Domain Admins) Change
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 Pre-Windows 2000 Compatib... Special None This object only
Allow Everyone Change password None This object only
Allow SELF Change password None This object only
Allow SELF Special None This object and all descendan...
Allow Domain Admins (HACKABLE... Special None This object only
Allow Enterprise Admins (HACKAB... Special None This object only
Allow Administrators (HACKABLE\... Special None This object only
Allow Authenticated Users Special None This object only
Allow SYSTEM Full control None This object only
Allow Cert Publishers (HACKABLE\... None This object only
Add Remove View Restore defaults
Enable inheritance
OK Cancel Apply


Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
hackable.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Keys
LostAndFound
Managed Service Accour
Program Data
System
Use
NTI
TPM
Name
Administrator
Allowed RODC Password Replication Group
Cert Publishers
Cloneable Domain Controllers
DefaultAccount
Denied RODC Password Replication Group
DnsAdmins
DnsUpdateProxy
Domain Admins
Domain Computers
Controllers
Guests
Users
e Admins
e Key Admins
e Read-only Domain Controllers
licy Creator Owners
ins
d Users
IAS Servers
Delegate Control...
Find...
New
All Tasks
View
Refresh
Export List...
Properties
Help
1

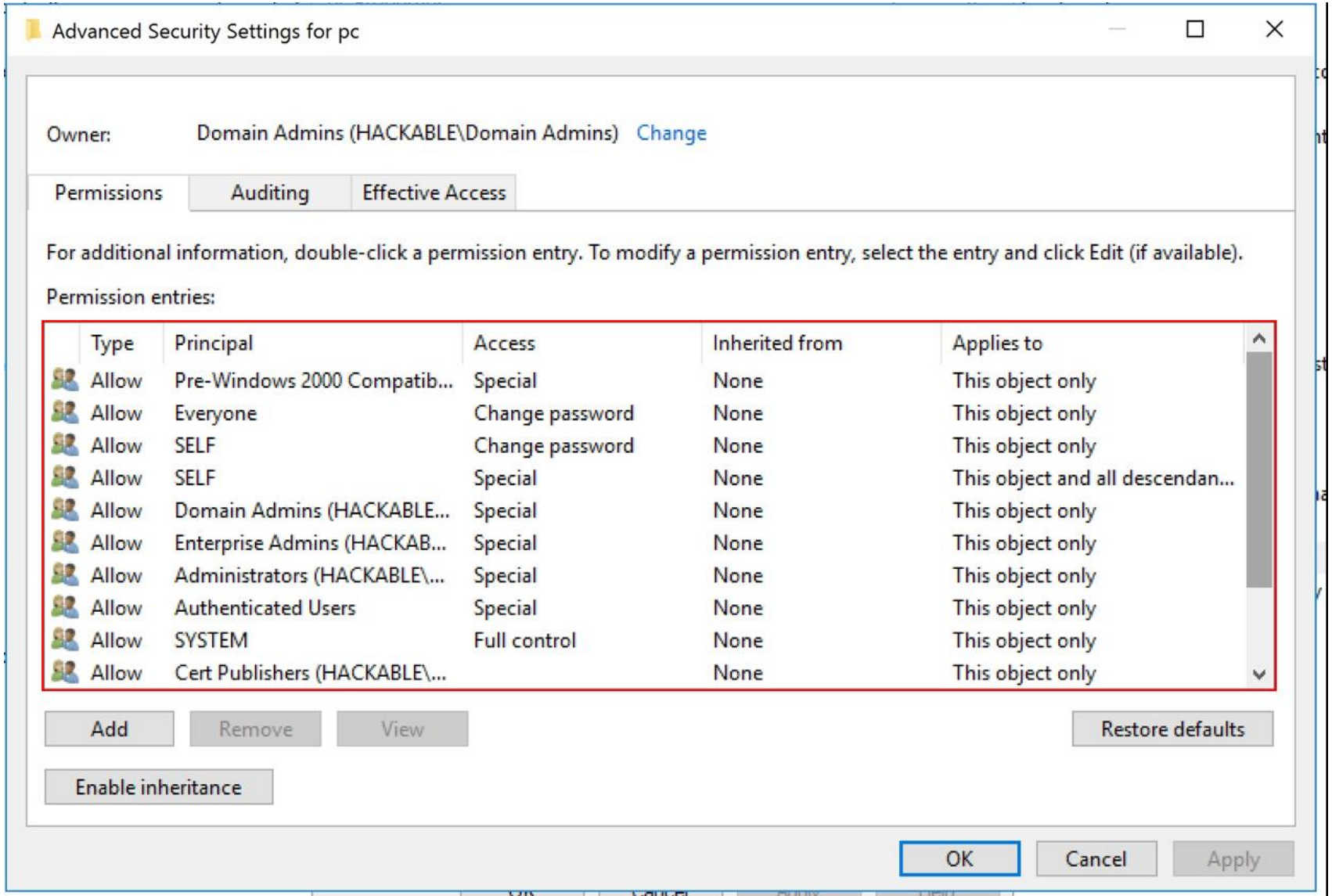

Delegation of Control Wizard
2
Users or Groups
Select one or more users or groups to whom you want to delegate control.
Selected users and groups:
pc (pc@hackable.com)
Add...
Remove
< Back
Next >
Cancel
Help


Delegation of Control Wizard
3
Tasks to Delegate
You can select common tasks or customize your own.
Delegate the following common tasks:
Create, delete, and manage user accounts
Reset user passwords and force password change at next logon
Read all user information
Create, delete and manage groups
Modify the membership of a group
Create, delete, and manage inetOrgPerson accounts
Reset inetOrgPerson passwords and force password change at next l
Create a custom task to delegate
< Back
Next >
Cancel
Help

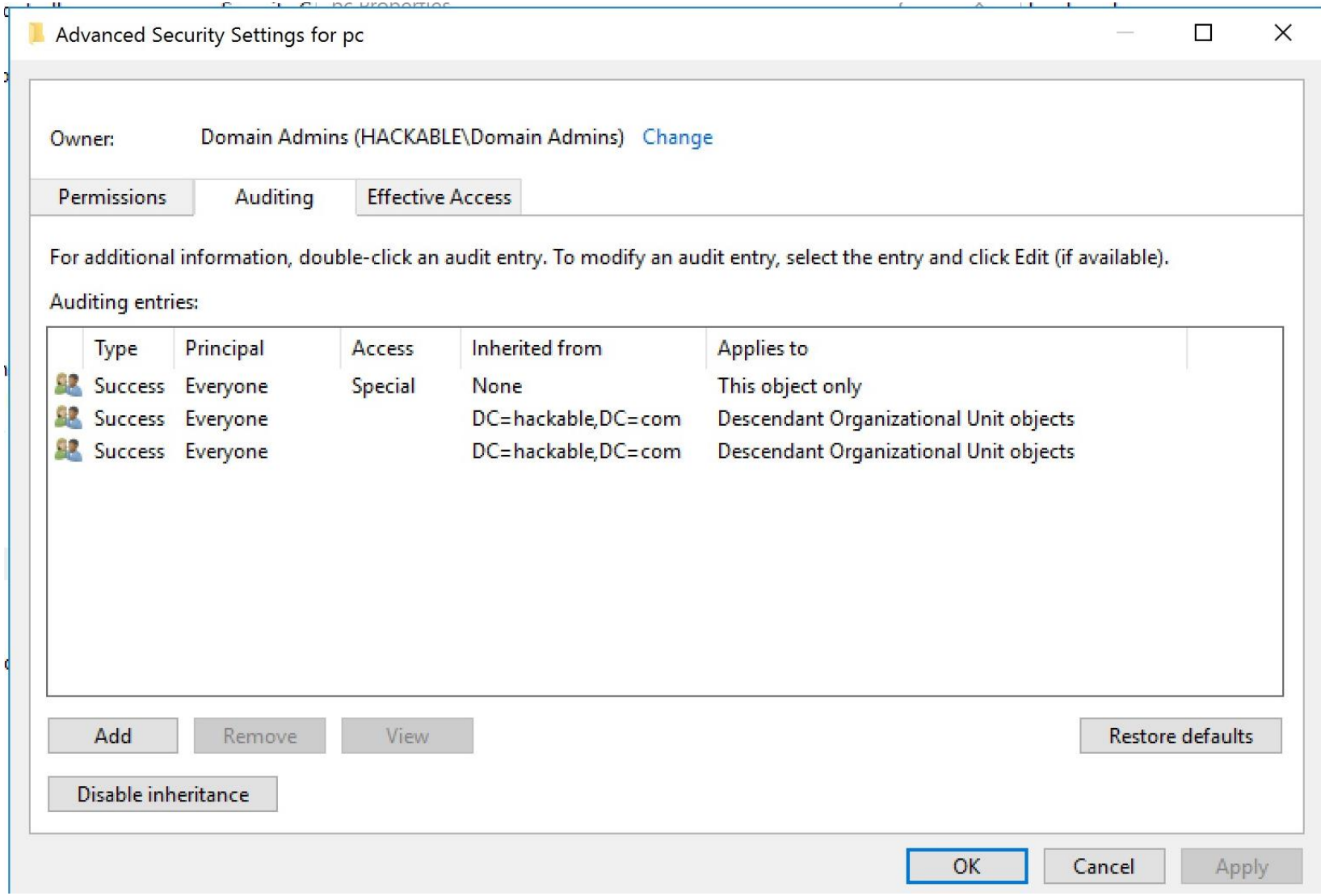
What is Access Control Entries (ACE)



What is Access Control List (ACL/DACL)



What is System Access Control List (SACL)



Example – ACL Abuse

Group	Permissions	OU
Helpdesk	Reset Passwords	OU=Users,OU=Corp,DC=Contoso,DC=Com
Helpdesk	Create/Modify Groups	OU=Groups,OU=Corp,DC=Contoso,DC=Com

Abusable ACEs

- **ForceChangePW** - Ability to change a users password without knowing the current password
- **AddMembers** - Ability to add any other user, group, or computer to a group
- **GenericAll** - Full object control over user and groups objects
- **GenericWrite** - Ability to write any object property value
- **WriteOwner** - Ability to grant object ownership to another principal
- **WriteDACL** - Ability to add a new ACE to the object's DACL
- **AllExtendedRights** - Ability to perform any "extended right" function

Disclaimer

All ACLS/ACE/DACL can be enumerated and read by Normal user. (No privilege required)

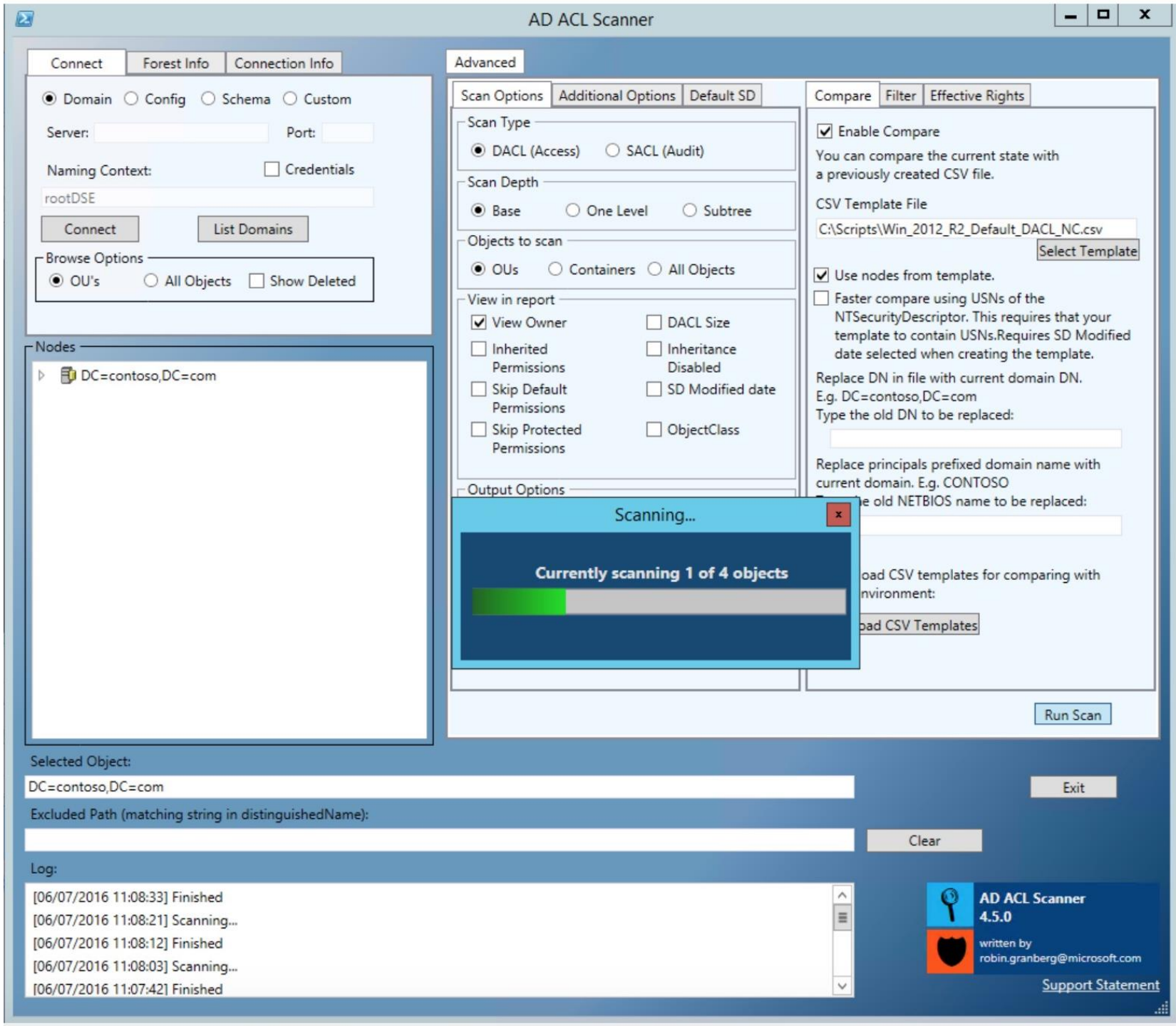
Tools of Trade

- ADACLScanner (https://github.com/canix1/ADACLScanner)
- Bloodhound (https://github.com/BloodHoundAD/BloodHound)
- Powerview (https://github.com/PowerShellMafia/PowerSploit/tree/master/Recon)

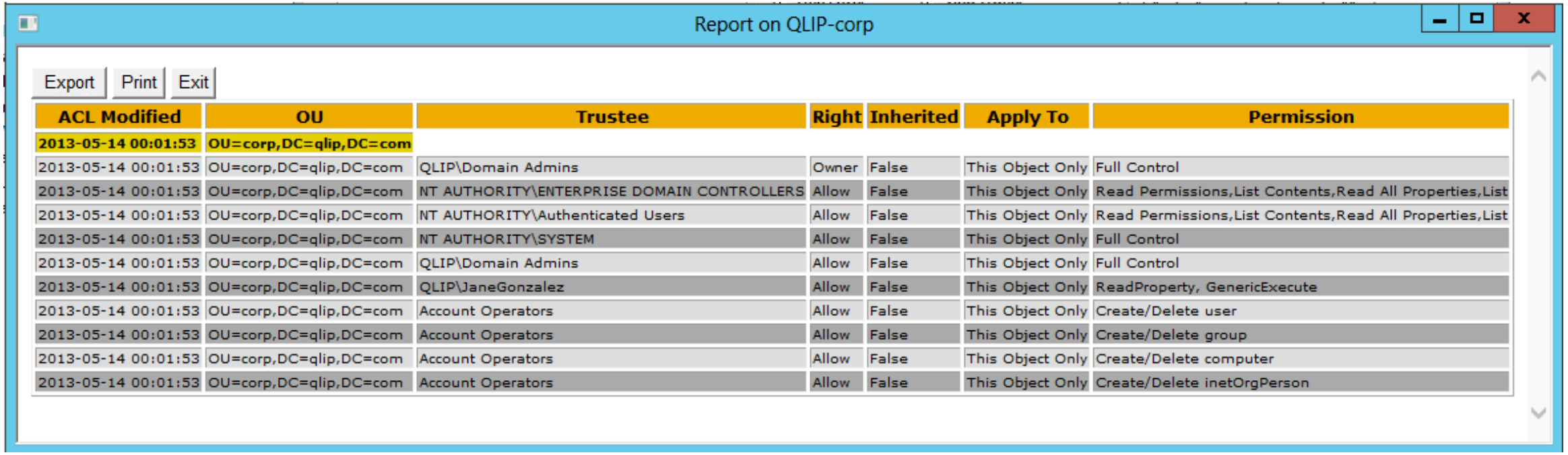
ADACLScanner

- This tool creates reports of the access control list for all of your Active Directory objects. With these reports you can see what/where and when permissions have been set.

https://github.com/canix1/ADACLScanner

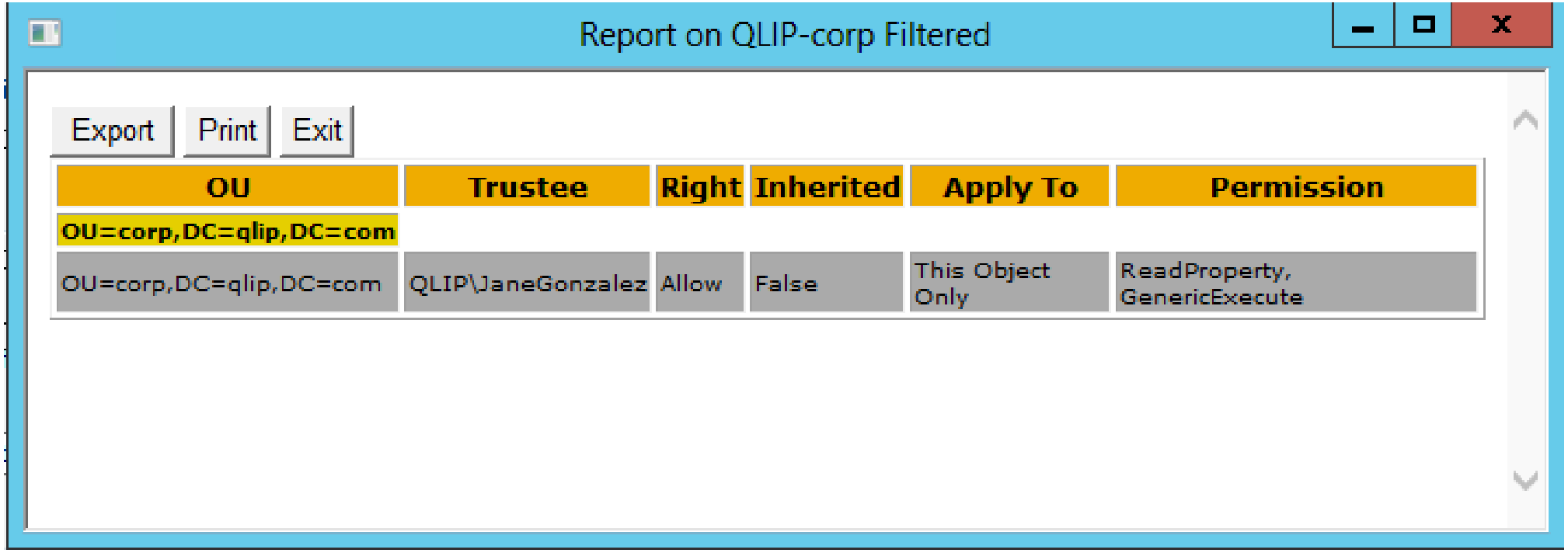


Report (HTML/CSV)



ACL Modified	OU	Trustee	Right	Inherited	Apply To	Permission
2013-05-14 00:01:53	**OU=corp,DC=qlip,DC=com**					
2013-05-14 00:01:53	OU=corp,DC=qlip,DC=com	QLIP\Domain Admins	Owner	False	This Object Only	Full Control
2013-05-14 00:01:53	OU=corp,DC=qlip,DC=com	NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Allow	False	This Object Only	Read Permissions,List Contents,Read All Properties,List
2013-05-14 00:01:53	OU=corp,DC=qlip,DC=com	NT AUTHORITY\Authenticated Users	Allow	False	This Object Only	Read Permissions,List Contents,Read All Properties,List
2013-05-14 00:01:53	OU=corp,DC=qlip,DC=com	NT AUTHORITY\SYSTEM	Allow	False	This Object Only	Full Control
2013-05-14 00:01:53	OU=corp,DC=qlip,DC=com	QLIP\Domain Admins	Allow	False	This Object Only	Full Control
2013-05-14 00:01:53	OU=corp,DC=qlip,DC=com	QLIP\JaneGonzalez	Allow	False	This Object Only	ReadProperty, GenericExecute
2013-05-14 00:01:53	OU=corp,DC=qlip,DC=com	Account Operators	Allow	False	This Object Only	Create/Delete user
2013-05-14 00:01:53	OU=corp,DC=qlip,DC=com	Account Operators	Allow	False	This Object Only	Create/Delete group
2013-05-14 00:01:53	OU=corp,DC=qlip,DC=com	Account Operators	Allow	False	This Object Only	Create/Delete computer
2013-05-14 00:01:53	OU=corp,DC=qlip,DC=com	Account Operators	Allow	False	This Object Only	Create/Delete inetOrgPerson

Filtering till user level



Full control on the domain level

					GenericRead, WriteDacl, WriteOwner	
DC=contoso,DC=com	CONTOSO\Enterprise Admins	Allow	False	This object and all child objects	Full Control	Match
DC=contoso,DC=com	CONTOSO\DelegationGoneBad	Allow	False	This Object Only	Full Control	New
DC=contoso,DC=com	CREATOR OWNER	Allow	False	computer	Validated write to computer attributes.	Match
DC=contoso,DC=com	NT AUTHORITY\ENTERPRISE	Allow	False	group	Read tokenGroups	Match

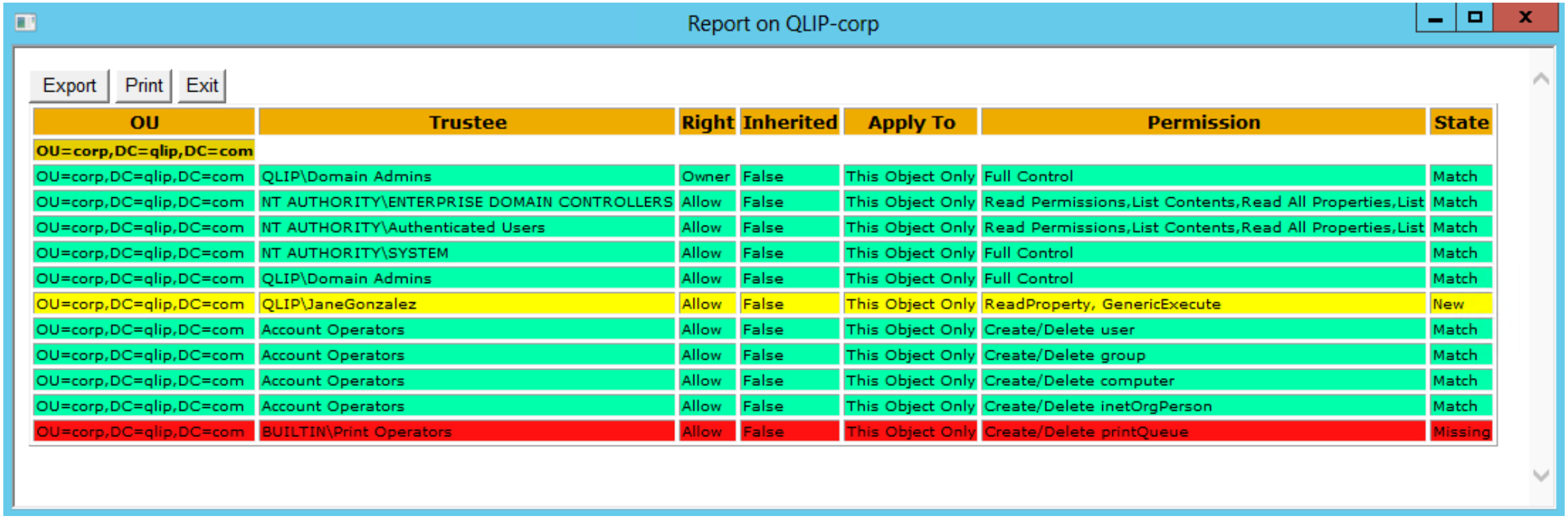
Full control granted on on domain level is not something you would delegate. The intension were probably to give someone full control on all OU's

Replicating Directory Changes All

DC=contoso,DC=com	CONTOSO\Enterprise Key Admins	Allow	False	This object and all child objects	Read All Properties;Write All Properties msDS-KeyCredentialLink	Match
DC=contoso,DC=com	CONTOSO\MaliciousUser	Allow	False	This object and all child objects	ExtendedRight Replicating Directory Changes All	New
DC=contoso,DC=com	CONTOSO\MaliciousUser	Allow	False	This object and all child objects	ExtendedRight Replicating Directory Changes	New

This permission should only be delegated to Administrators, Domain Admins and Domain Controllers unless you are using a product that does password sync using hashes,

Comparing current state and earlier



OU	Trustee	Right	Inherited	Apply To	Permission	State
OU=corp,DC=qlip,DC=com						
OU=corp,DC=qlip,DC=com	QLIP\Domain Admins	Owner	False	This Object Only	Full Control	Match
OU=corp,DC=qlip,DC=com	NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Allow	False	This Object Only	Read Permissions,List Contents,Read All Properties,List	Match
OU=corp,DC=qlip,DC=com	NT AUTHORITY\Authenticated Users	Allow	False	This Object Only	Read Permissions,List Contents,Read All Properties,List	Match
OU=corp,DC=qlip,DC=com	NT AUTHORITY\SYSTEM	Allow	False	This Object Only	Full Control	Match
OU=corp,DC=qlip,DC=com	QLIP\Domain Admins	Allow	False	This Object Only	Full Control	Match
OU=corp,DC=qlip,DC=com	QLIP\JaneGonzalez	Allow	False	This Object Only	ReadProperty, GenericExecute	New
OU=corp,DC=qlip,DC=com	Account Operators	Allow	False	This Object Only	Create/Delete user	Match
OU=corp,DC=qlip,DC=com	Account Operators	Allow	False	This Object Only	Create/Delete group	Match
OU=corp,DC=qlip,DC=com	Account Operators	Allow	False	This Object Only	Create/Delete computer	Match
OU=corp,DC=qlip,DC=com	Account Operators	Allow	False	This Object Only	Create/Delete inetOrgPerson	Match
OU=corp,DC=qlip,DC=com	BUILTIN\Print Operators	Allow	False	This Object Only	Create/Delete printQueue	Missing

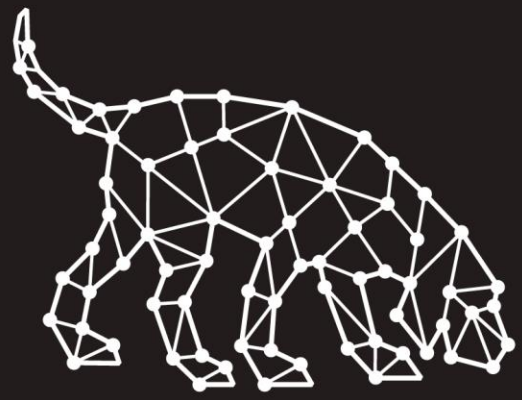
What kind of permissions are more of a risk than others?

Here's a couple of permissions that you should watch out for (This is not a compete list):

- **Full Control on all objects**
- **Create Child Objects**
  - Create new user accounts, groups etc.
  - Create dynamic objects, objects with a Time-To-Live and will disappear when TTL is meet.
- **All Extended Rights**
  - Password Resets
  - Replicating Directory Changes All
  - Potential access to all confidential attributes.
- **Extended Right: Replicating Directory Changes All**
  - This extended rights should ONLY be delegated to services that do password synchronization like the Azure AD Connect tool or other services using DSgetNCChanges for password sync.
  - FIM/MIM does not need this permissions see: https://support.microsoft.com/en-us/kb/303972
- **Reset Passwords**
- **Write Property to objects or sensitive attributes**
  - Modify group memberships.
  - Write userPrinicpalName.
  - Write altSecIdentities
  - Write userCertificate
  - Write userAccountControl.
  - Write servicePrincipalName.
- **Write Public Information**
  - Includes userPrincipalName.
- **Write Membership**
  - Includes member and memberOf.
- **Write User Account Restrictions**
  - Includes userAccountControl.
- **Write userPrincipalName**
  - Access to modify the userPrincipalName could let someone with a valid smart card to logon as someone else by having the SubjAltName field of the smart to match another Active Directory user account.
- **Write userAccountControl**
  - Allow blank password.
  - Downgrade Kerberos to DES only.
  - Enable/Disable accounts.

https://blogs.technet.microsoft.com/pfesweplat/2017/01/28/forensics-active-directory-acl-investigation/

Bloodhound



```
(a:Attackers)-[:Think_in]->(g:Graphs)
```

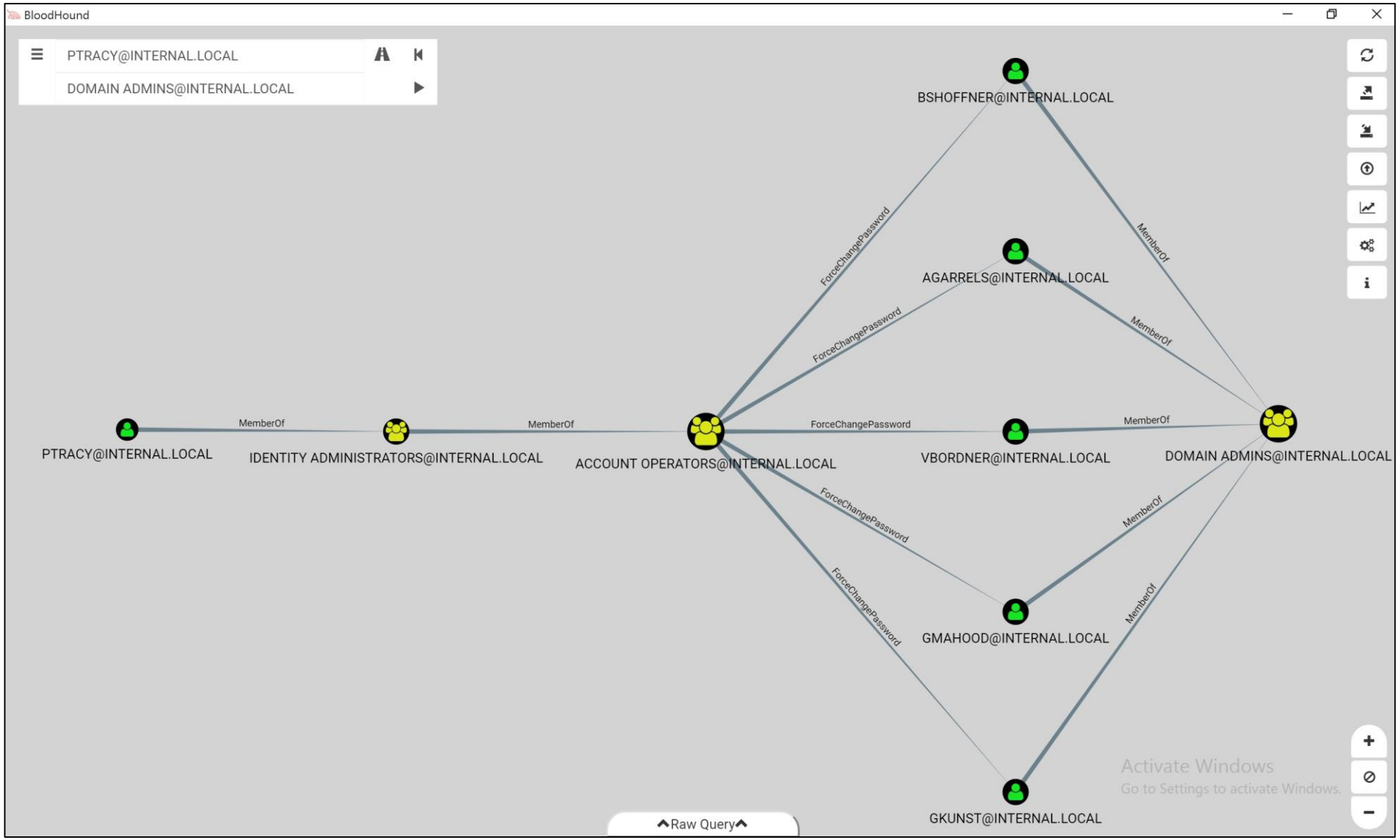
Bloodhound Options

```
C:\                                                    \Ingestors>SharpHound.exe -h
SharpHound v1.0.0
Usage: SharpHound.exe <options>

Enumeration Options:
    -c , --CollectionMethod (Default: Default)
        Default - Enumerate Trusts, Sessions, Local Admin, and Group Membership
        Group - Enumerate Group Membership
        LocalGroup - Enumerate Local Admin
        Session - Enumerate Sessions
        SessionLoop - Continuously Enumerate Sessions
        LoggedOn - Enumerate Sessions using Elevation
        ComputerOnly - Enumerate Sessions and Local Admin
        Trusts - Enumerate Domain Trusts
        ACL - Enumerate ACLs
        ObjectProps - Enumerate Object Properties for Users/Computers
        Container - Collects GPO/OU Structure
        All - Performs all enumeration methods

        This can be a list of comma seperated valued as well to run multiple collection methods!
```

```
C:\                                                                \Ingestors>SharpHound.exe --DomainController 192.168.50.11 -c All
Initializing BloodHound at 1:02 PM on 5/27/2018
Starting Default enumeration for      ae
Status: 786 objects enumerated (+786 26.2/s --- Using 50 MB RAM )
Status: 786 objects enumerated (+0 13.1/s --- Using 50 MB RAM )
Status: 786 objects enumerated (+0 8.733334/s --- Using 49 MB RAM )
Status: 787 objects enumerated (+1 8.37234/s --- Using 48 MB RAM )
Finished enumeration for      ae in 00:01:34.1815495
175 hosts failed ping. 0 hosts timedout.

Starting ACL enumeration for      .ae
Status: 821 objects enumerated (+821 821/s --- Using 63 MB RAM )
Finished enumeration for      .ae in 00:00:01.6698217
0 hosts failed ping. 0 hosts timedout.

Starting ObjectProps enumeration for      .ae
Status: 583 objects enumerated (+583 Infinity/s --- Using 61 MB RAM )
Finished enumeration for      .ae in 00:00:00.1506744
0 hosts failed ping. 0 hosts timedout.

Starting Container enumeration for      ae
Finished enumeration for      .ae in 00:00:02.8727424

Removed 1581 duplicate lines from .\group_membership.csv
Removed 78 duplicate lines from .\local_admins.csv
Removed 80 duplicate lines from .\sessions.csv
Removed 72 duplicate lines from .\acls.csv
```

Derivative Admin (without ACLs)

Derivative Admin (with ACLs)




DEMO

Powerview Supported cmdlets

Right	Abuse Function
GenericWrite/GenericAll	Set-DomainObject
WriteProperty to specific properties	Set-DomainObject
WriteDacl	Add-DomainObjectAcl
WriteOwner	Set-DomainObjectOwner
CreateChild	Add-DomainGroupMember
User-Force-Change-Password	Set-DomainUserPassword

Recommendations

- Remove dangerous ACLs
- Remove writeDACL permission for Exchange Enterprise Servers
- Monitor security groups
- Audit and monitor changes to the ACL
- Monitor Event logs for below Id
  - 4735: A security-enabled local group was changed
  - 4737: A security-enabled global group was changed
  - 4738: A user account was changed
  - 4755: A security-enabled universal group was changed

References

- https://wald0.com/?p=112
- https://www.blackhat.com/docs/us-17/wednesday/us-17-Robbins-An-ACE-Up-The-Sleeve-Designing-Active-Directory-DACL-Backdoors-wp.pdf
- https://blogs.technet.microsoft.com/pfesweplat/2013/05/13/take-control-over-ad-permissions-and-the-ad-acl-scanner-tool/
- https://blogs.technet.microsoft.com/pfesweplat/2017/01/28/forensics-active-directory-acl-investigation/
- https://www.youtube.com/watch?v=z8thoG7gPd0


ANY
QUESTIONS
?