



# Exploiting Relationship between Active Directory Objects

Boring security is smart security

@0xAJStrike



# Contents

- Red Team – Adversary simulation
- Why talk about Active Directory
- Active Directory Structure
- Active Directory Object Relationship
- Bloodhound Introduction
- Case studies!

# Whoami

```
PS C:\Users\Administrator>
```

```
PS C:\Users\Administrator> Get-ADUser Juned.Ansari
```

```
SamAccountname : Juned.Ansari
```

```
company : DarkMatter
```

```
title : Senior Consultant
```

```
Department : Computer Network Exploitation
```

```
initials : AJ
```

```
Employeeid : 1337
```

```
Description : Hacks for Work, Fun and Learn!, 10+ years of Field Experience, Started as System Admin, Played roles in both  
Defense and Offense, Primary area of focus is Advance Attack Simulation, Authored two books on Kali Linux
```

```
PS C:\Users\Administrator>
```



# Red Team Engagement vs Other Security Tests

- Vulnerability Assessment
  - Broad Scope, Breadth over depth
  - Automated
- Penetration Test
  - Varied scope, Balancing act between depth and breadth
  - Prioritized list of vulnerabilities
- Red Team Engagement
  - Goals
  - Measures impacts on an organization



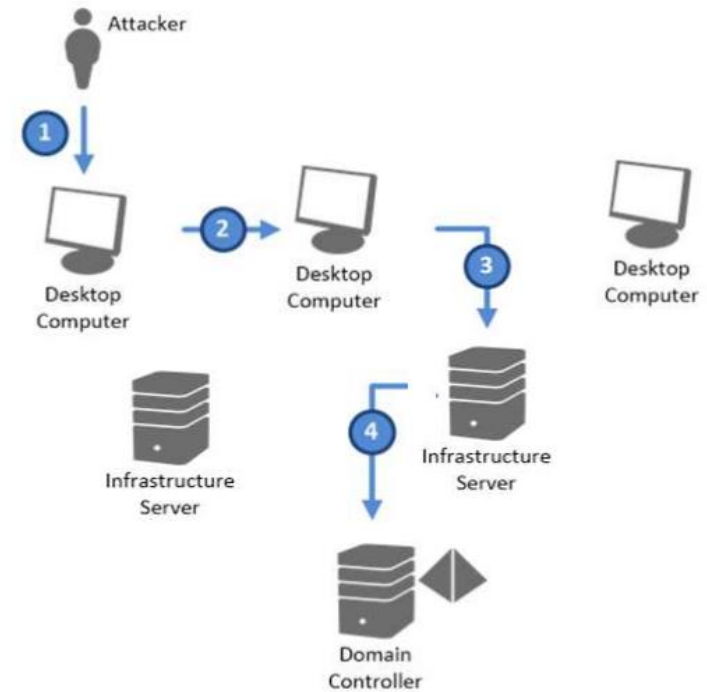
# Red Team Phases

- Get In: Gain access to network or System. This can be through a Compromised asset or through access granted as part of the scenario.  
Recon/Enumeration/Exploit
- Stay In: Establish persistence or permanent presence. Establish foothold in order to survive the duration of the engagement.  
Persistence/Lateral Movement/Continued Enumeration
- Act: Perform an operational impact, such as Exfiltrate data.



# Hunting for Targets

- Lateral Movement  
Moving across client computers  
Site A → Site B
- Vertical Movement  
Moving across server layers  
User VLAN → Server VLAN
- Collectively known in the cyber space as lateral Movement
- Critical piece in the attack chain as local compromise spreads and becomes global
- Increasing difficult for the Incident Response team to scope the breach and perform appropriate containment and remediation.

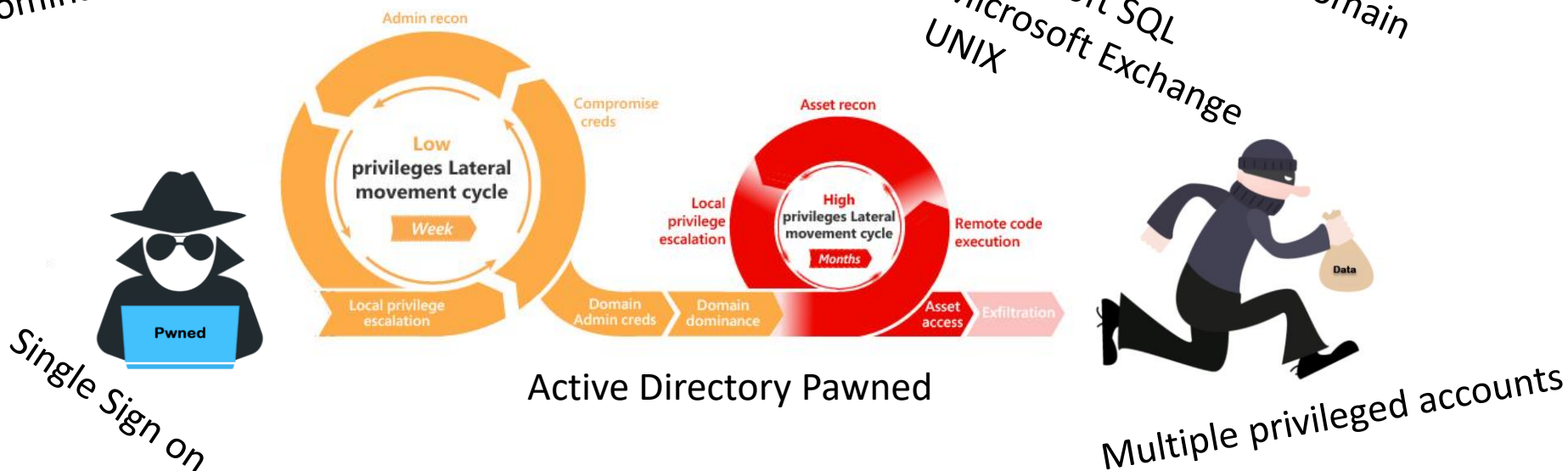




# The Cycle of Lateral movement

Windows Dominated Infrastructure

Applications Integrated with Domain  
Sharepoint  
Microsoft SQL  
Microsoft Exchange  
UNIX



# Security Solutions Era

- Enterprises have new security solutions integrated in their networks.
  - Security Information and Event Management
  - Vulnerability scanners
  - Next Generation Firewall
  - Endpoint Detection and Response solutions
  - Database Activity Monitors

**Response to every security issue is a new security solution!**





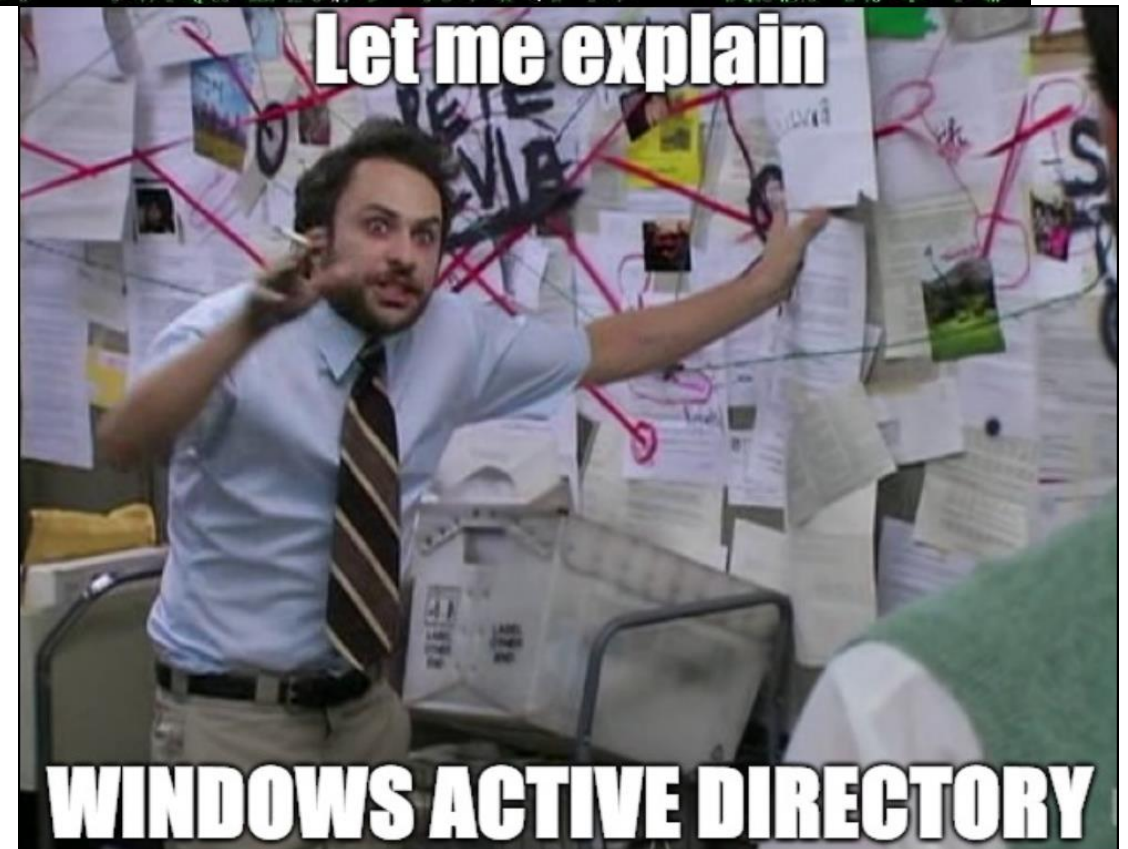


New security  
solutions

Strengthening  
Active  
Directory

# Reality about your AD infrastructure is...

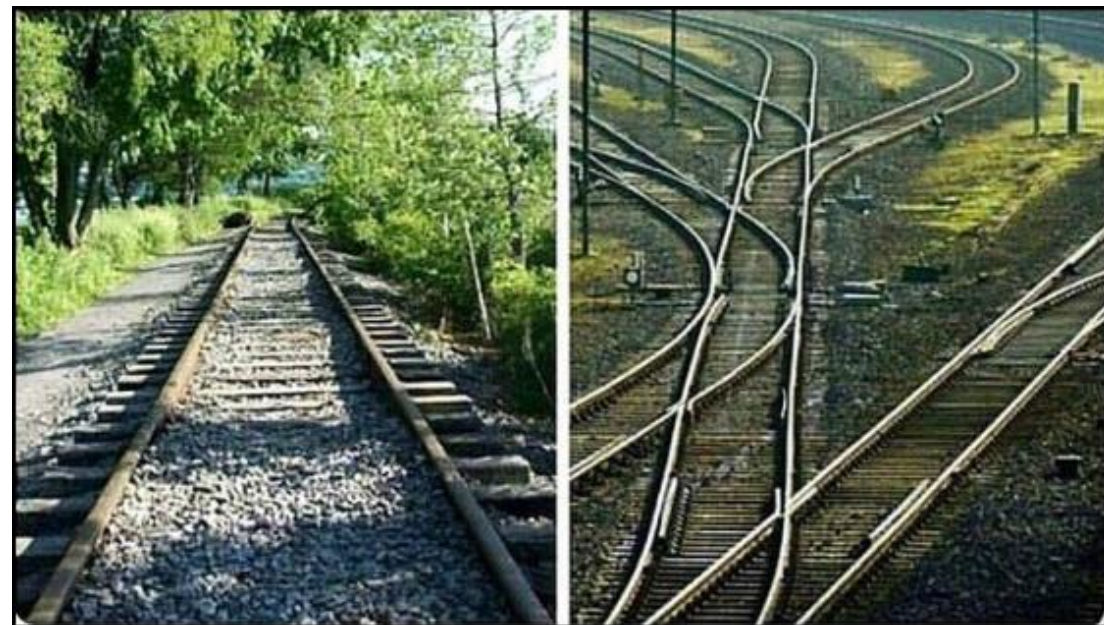
- Its there since a long time and its working... so leave it that way...
- Organizations have moved from couple of workstations to 1000s of Servers.





# Reality about your AD infrastructure is...

- Most Active Directory setups are rich with multiple paths to exploit.
- IT administration is mostly outsourced and contracted.
- Traditional methods of Administration used.





# Active Directory Structure

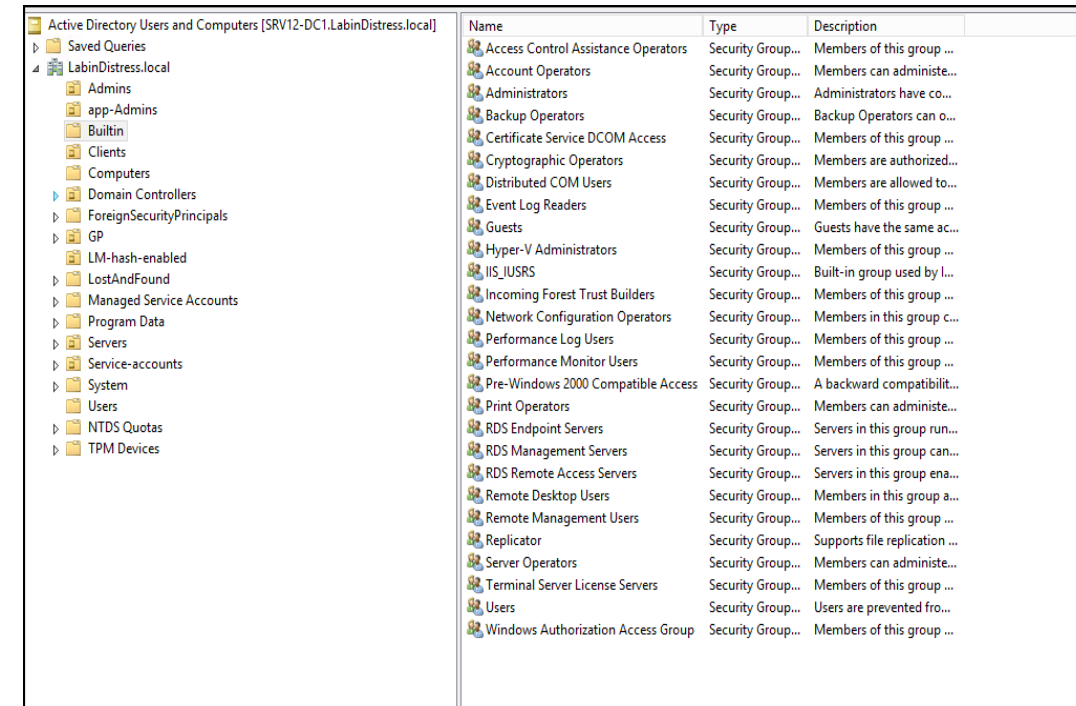


# Active Directory Structure

- In AD everything is an object.
  - Users, computers, domains, group, group policy, OU

- Every object has set of properties (attributes) permissions

- Domain Controller is heart of the AD
  - Provides Authentication
  - Stores all domain objects in a Database
  - Replicates Domain data



The screenshot shows the 'Active Directory Users and Computers' console for the domain 'LabinDistress.local'. The left pane displays a tree view of the domain structure, including 'Built-in' groups and 'Users'. The right pane shows a list of built-in security groups with their names, types, and descriptions.

Name	Type	Description
Access Control Assistance Operators	Security Group...	Members of this group ...
Account Operators	Security Group...	Members can administe...
Administrators	Security Group...	Administrators have co...
Backup Operators	Security Group...	Backup Operators can o...
Certificate Service DCOM Access	Security Group...	Members of this group ...
Cryptographic Operators	Security Group...	Members are authorized...
Distributed COM Users	Security Group...	Members are allowed to...
Event Log Readers	Security Group...	Members of this group ...
Guests	Security Group...	Guests have the same ac...
Hyper-V Administrators	Security Group...	Members of this group ...
IIS_IUSRS	Security Group...	Built-in group used by I...
Incoming Forest Trust Builders	Security Group...	Members of this group ...
Network Configuration Operators	Security Group...	Members in this group c...
Performance Log Users	Security Group...	Members of this group ...
Performance Monitor Users	Security Group...	Members of this group ...
Pre-Windows 2000 Compatible Access	Security Group...	A backward compatibilit...
Print Operators	Security Group...	Members can administe...
RDS Endpoint Servers	Security Group...	Servers in this group run...
RDS Management Servers	Security Group...	Servers in this group can...
RDS Remote Access Servers	Security Group...	Servers in this group ena...
Remote Desktop Users	Security Group...	Members in this group a...
Remote Management Users	Security Group...	Members of this group ...
Replicator	Security Group...	Supports file replication ...
Server Operators	Security Group...	Members can administe...
Terminal Server License Servers	Security Group...	Members of this group ...
Users	Security Group...	Users are prevented fro...
Windows Authorization Access Group	Security Group...	Members of this group ...

# Active Directory Objects – Attributes

- Each object has a set of attributes common across objects and attributes unique based on the functionality

The image displays two side-by-side screenshots of the Active Directory 'Attribute Editor' window, illustrating the attributes for different object types.

**Left Window: OU=Servers Properties**

Attribute	Value
desktopProfile	<not set>
destinationIndicator	<not set>
displayName	<not set>
displayNamePrintable	<not set>
distinguishedName	OU=Servers,DC=LabinDistress,DC=local
dSASignature	<not set>
dSCorePropagationD...	10/14/2018 9:49:21 PM Arabian Standard T
extensionName	<not set>
facsimileTelephoneN...	<not set>
flags	<not set>
fSMORoleOwner	<not set>
gPLink	[LDAP://cn={48D56F10-8C02-433B-B1D1-D
gPOptions	<not set>
instanceType	0x4 = ( WRITE )

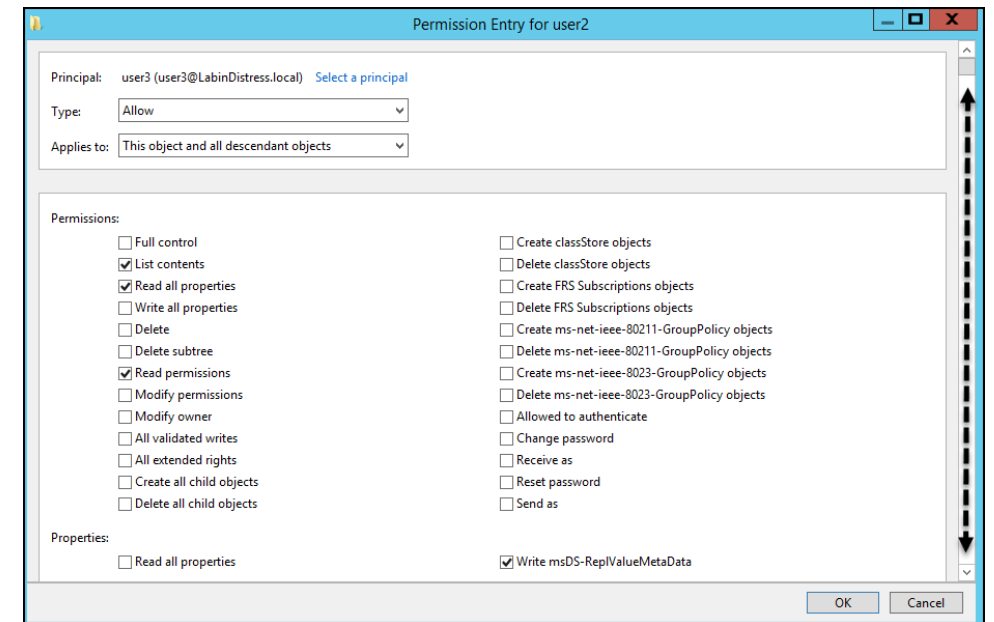
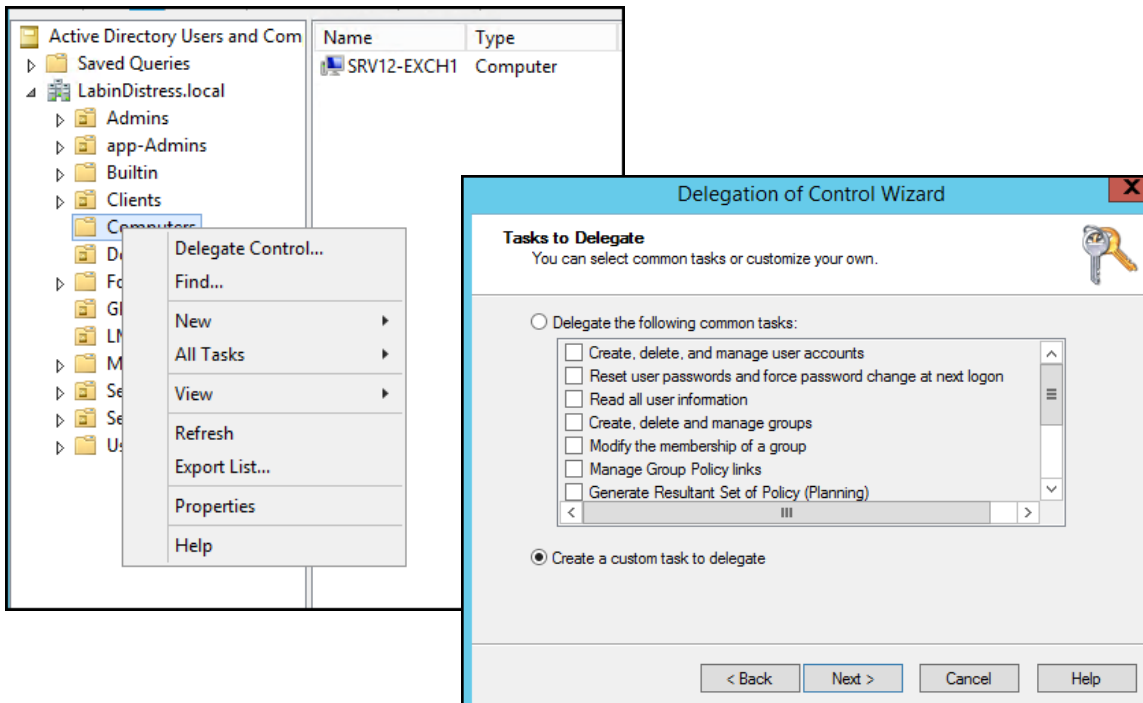
**Right Window: CN=user3 Properties**

Attribute	Value
audio	<not set>
badPasswordTime	(never)
badPwdCount	0
businessCategory	<not set>
c	<not set>
carLicense	<not set>
cn	user3
co	<not set>
codePage	0
comment	<not set>
company	<not set>
controlAccessRights	<not set>
countryCode	0
dBCSPwd	<not set>



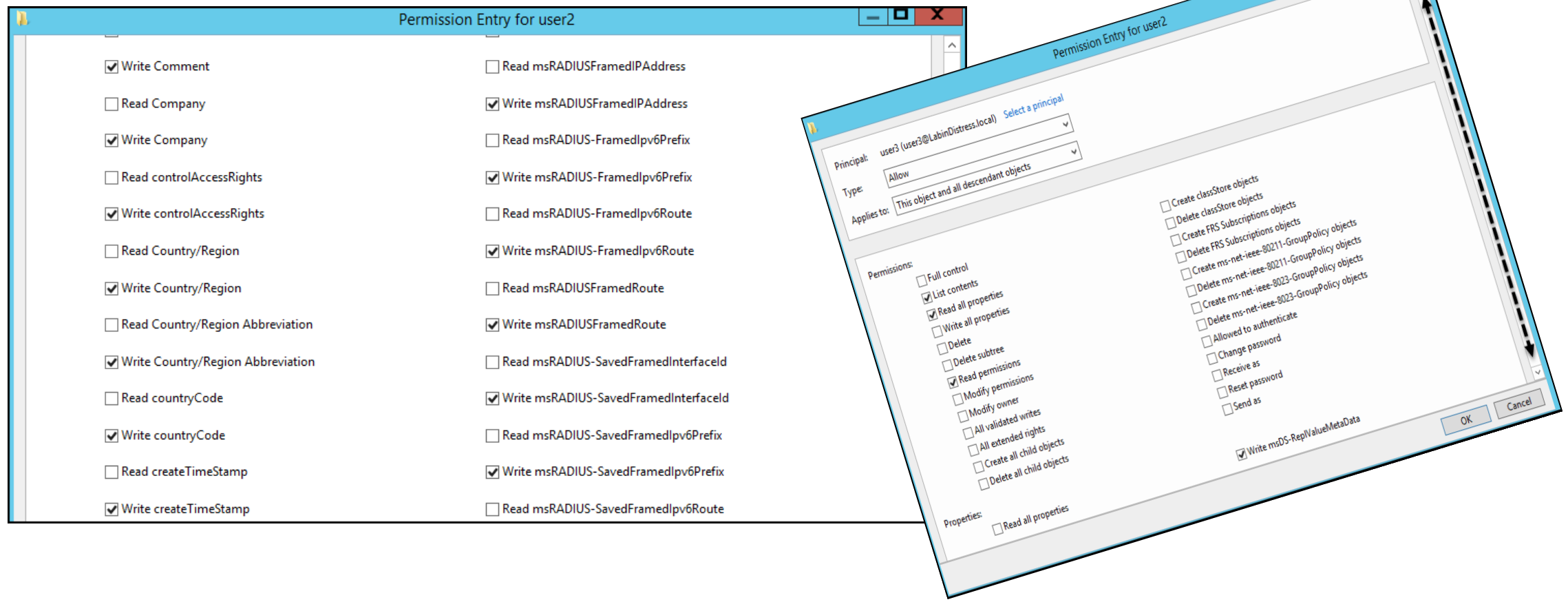
# AD Object Permissions

- Permissions on object can be assigned by OU Delegation
- Each object can have permissions set on it individually.



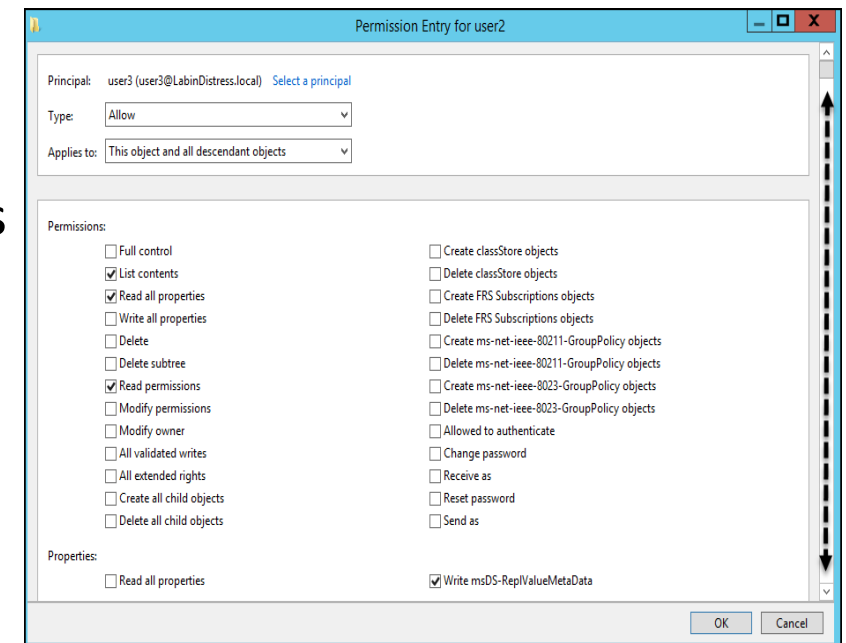
# AD Object Permissions

- Granular permissions to read and write individual attributes can also be assigned



# AD Object Permissions

- Domain administrators have permissions over all domain objects
- Enterprise Admins have rights over all domains in the forest
- IT Admins can assign permissions based on roles
  - Dev ops Team have permissions over their projects
  - IT helpdesk have rights over user machines and objects
  - Assistants have to operate their managers mailboxes
- Nested Permissions is integral to Active Directory

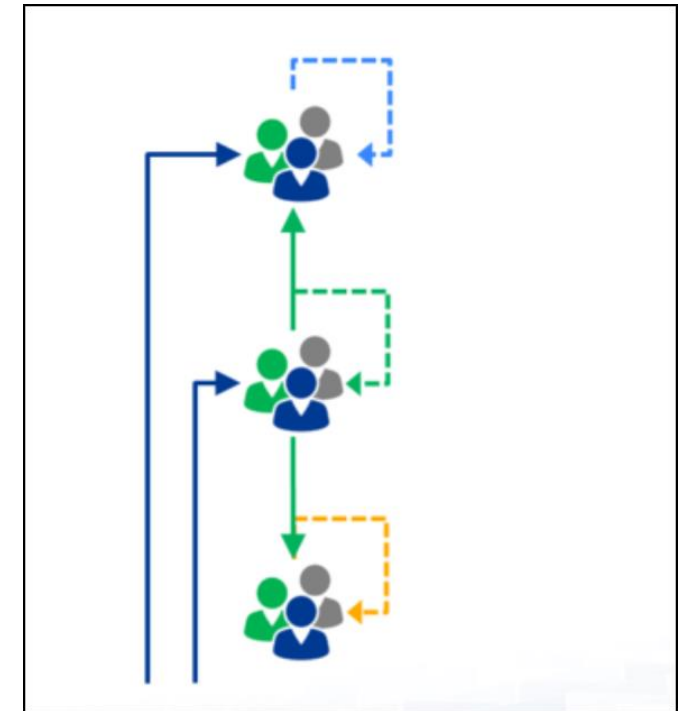




# AD Object- Nested Groups

- Nested Group is common in today's enterprises.
- Biggest Domain Group by default is the Domain Users group.
- Includes every new account created in the Domain

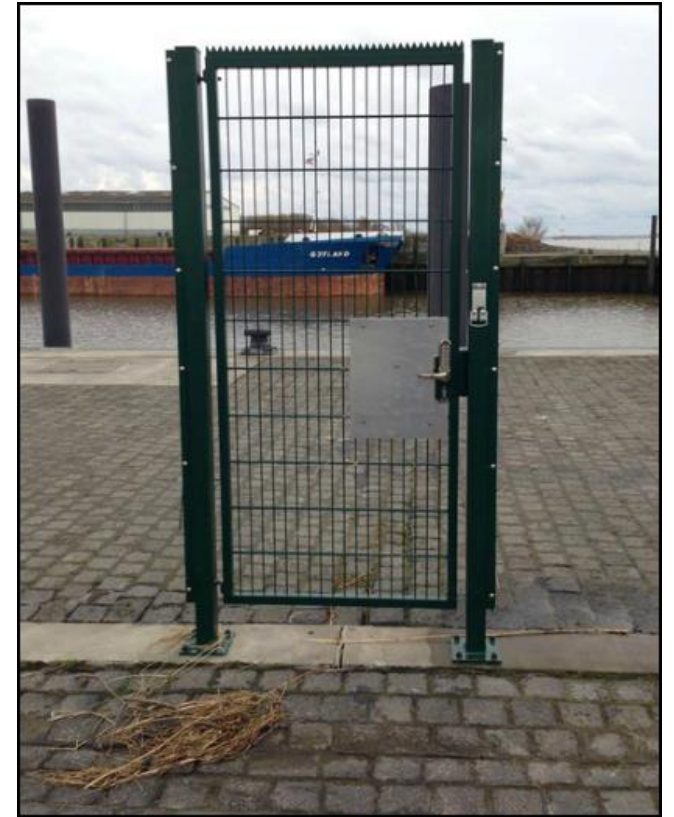
- User A → Group B → Group C → Group D
- Uncareful Group nesting leads to excessive Privileges.



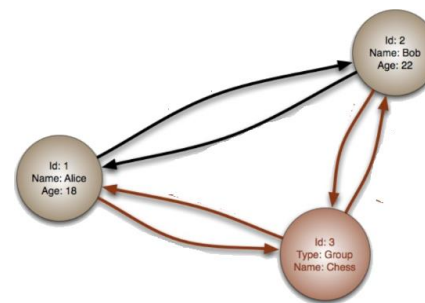
# Privileged Group Access

- Most accounts in AD domain are over-permissioned
- Service Accounts in Domain Admin Groups
- Service Accounts having permissions over privileged Users
- Domain accounts as Local Admins
- Computer accounts in Admin Groups
- Domain Admin accounts used on user machines
- Nested groups access

An attacker always on the hunt for such configurations



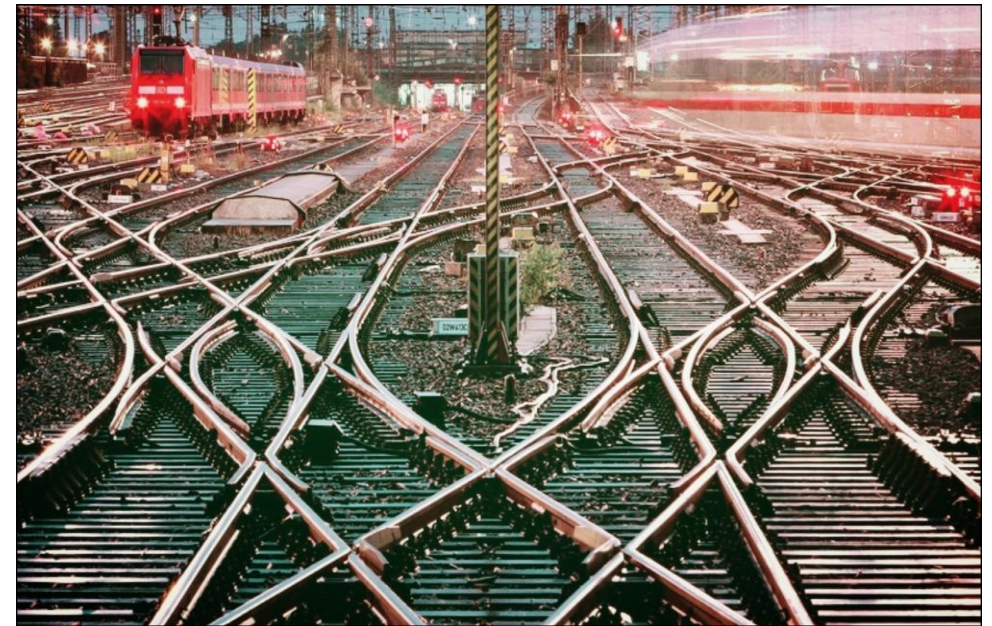
# Object Relationship Graphing





# Object Relationship Graphing

- During an adversary simulation we need to map the targeted environment and visualize possible attack path
  - Which domain admins are logged in to which machines
  - Does current domain user has admin privilege on any other machine
  - Which users have change password rights and full Access on which objects
- Home many hops is the Domain Admin workstation
- Are there any service accounts that can help me jump to any database server
- and lots more..... depends on what you are target it.
- Tedious manual way to tracing each permission across the domain
  - PowerShell module of Active Directory
  - Ge-ACL, Get-Netsession, Get-GPO etc



OR... automate and map the path to your target into a graph



# Manual Mapping of Access Control Entry

```
PS C:\Tools> Get-DomainObjectAcl -Identity "akhan" -ResolveGUIDs | where{$_.objectAceType -like "User-Force-Change-Password"}

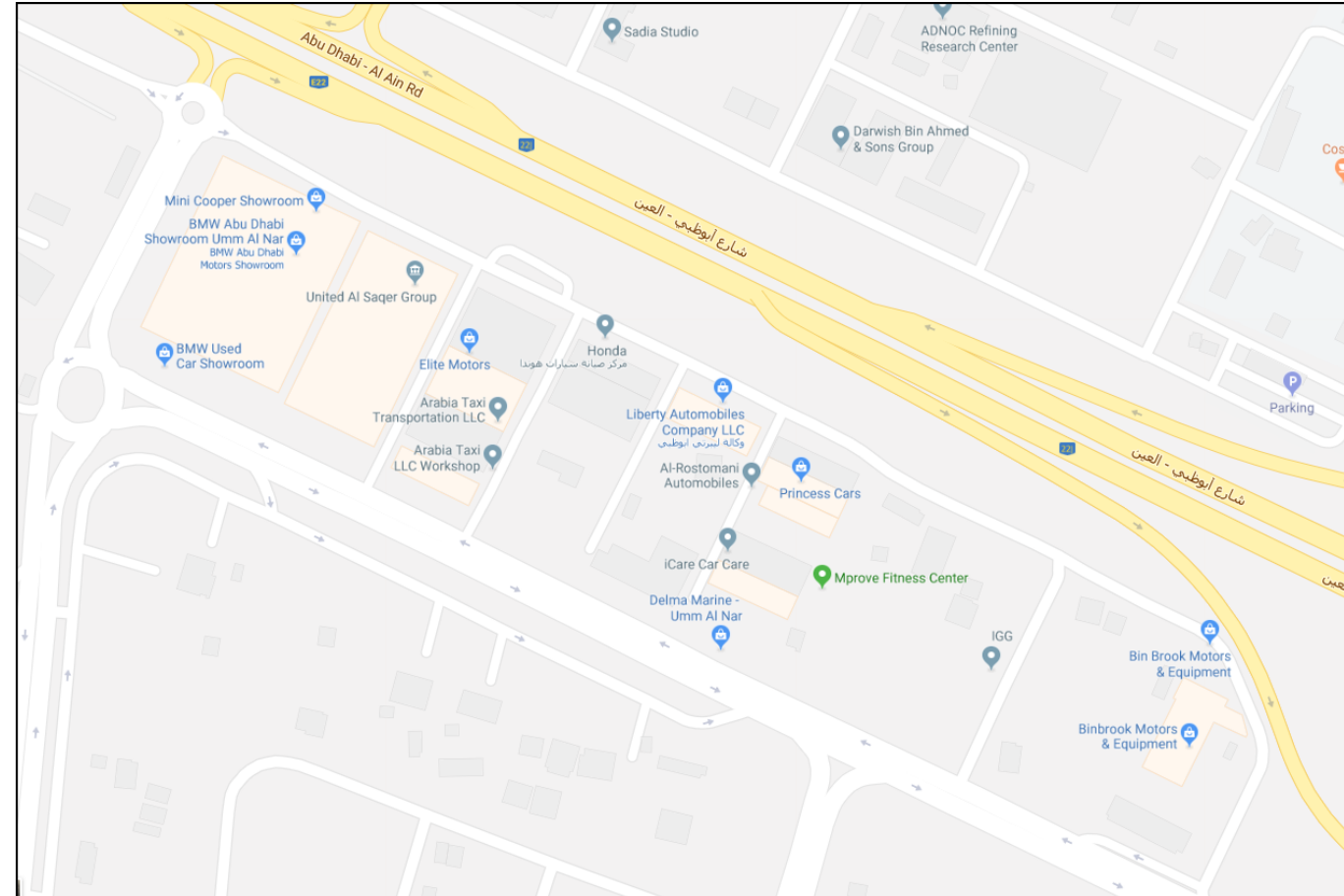
AceQualifier      : AccessAllowed
ObjectDN          : CN=Arman Khan,OU=HR,DC=LabinDistress,DC=local
ActiveDirectoryRights : ExtendedRight
ObjectAceType     : User-Force-Change-Password
ObjectSID         : S-1-5-21-3844510086-2928011428-106315059-1129
InheritanceFlags  : ContainerInherit
BinaryLength      : 72
AceType           : AccessAllowedObject
ObjectAceFlags    : ObjectAceTypePresent, InheritedObjectAceTypePresent
IsCallback        : False
PropagationFlags  : None
SecurityIdentifier : S-1-5-21-3844510086-2928011428-106315059-1128
AccessMask        : 256
AuditFlags        : None
IsInherited       : True
AceFlags          : ContainerInherit, Inherited
InheritedObjectAceType : User
OpaqueLength      : 0

PS C:\Tools> Get-DomainObject "S-1-5-21-3844510086-2928011428-106315059-1128"

userprincipalname : helpdesk@LabinDistress.local
countrycode       : 0
displayname       : helpdesk
samaccounttype    : USER_OBJECT
samaccountname    : helpdesk
objectsid         : S-1-5-21-3844510086-2928011428-106315059-1128
objectclass       : {top, person, organizationalPerson, user}
codepage          : 0
givenname        : helpdesk
cn               : helpdesk
primarygroupid    : 513
distinguishedname : CN=helpdesk,OU=Service-accounts,DC=LabinDistress,DC=local
name             : helpdesk
objectguid        : 0068a3c2-c818-4cf8-838f-69d4147ea3a5
objectcategory    : CN=Person,CN=Schema,CN=Configuration,DC=LabinDistress,DC=local
```

# Graph Theory

- Study of graphs, which are mathematical structures used to model pairwise relations between objects.
- A graph is made up of vertices (also called nodes or points) which are connected by edges
- The most basic form of graph that we use and see every day is Google Maps
- It's just one big graph! Where Edges represent streets and vertices represent crossings.







# BloodHound to our rescue

- Javascript web application that uses graph theory to reveal the hidden and often unintended relationships within an Active Directory environment.
- Heavily relies on the PowerShell based Domain reconnaissance tools called Powerview by harmjoy
- Retrieves Domain Object and ACE's data from Domain Controller using LDAP queries.
- Identifies session information and local Administrators from computers in the domain to find out currently logged on users.
- Massages the information and display the information in a graph format.
- Developed by @\_wald0, @CptJesus, and @harmj0y.



# Bloodhound terminology

- Nodes → Users, Computers, Groups and Domains
- Edges → Type of relationship between two AD objects.
  - MemberOf
  - HasSession
  - AdminTo
  - ACL – GenericAll
  - ACL – ForceChangePassword
  - ACL -- AddMember
- Paths → Series of Nodes connected by Edges which is the attack path. Each edge can be abused to reach the next node.



# Bloodhound Data Collection

## Group membership:

- Domain Security Group membership – Directly from Domain controller
- Group, user, domain and computer properties
- Local Admin and RDP Group membership – From each computer
- Session Information: Using the NetSessionEnum function against each computer
- Abusable ACEs from objects

Few more like GPO Links, DCOM, Domain trusts etc..



# Bloodhound Data Collection

```
PS C:\Tools> Import-Module .\SharpHound.ps1
PS C:\Tools>
PS C:\Tools> Invoke-BloodHound -CollectionMethod All
Initializing BloodHound at 9:37 PM on 4/2/2019
Resolved Collection Methods to Group, LocalAdmin, Session, Trusts, ACL, Container, RDP,
Starting Enumeration for LabinDistress.local
Status: 91 objects enumerated (+91 Infinity/s --- Using 157 MB RAM )
Finished enumeration for LabinDistress.local in 00:00:00.6656977
4 hosts failed ping. 0 hosts timedout.

Compressing data to C:\Tools\20190402213752_BloodHound.zip.
You can upload this file directly to the UI.
Finished compressing files!
PS C:\Tools> █
```



# Bloodhound Data Collection - ACL

Active Directory users, groups, and computers are securable objects.

Access Control Entries describe the allowed and denied permissions for other principals in Active Directory against the securable object.

Bloodhound hunts for 7 different Abusable ACEs

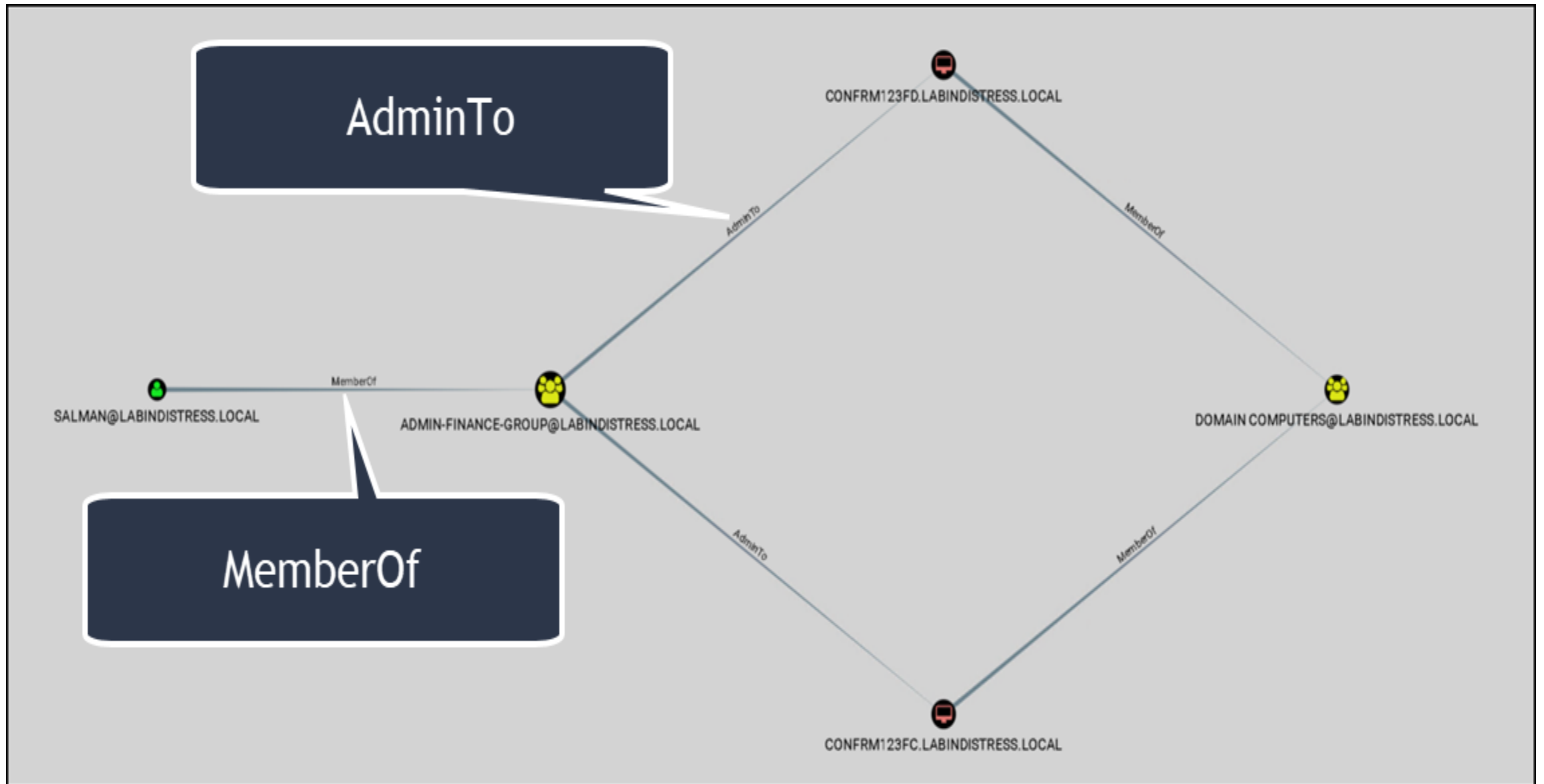
- ForceChangePassword
- AddMembers
- GenericAll
- GenericWrite
- WriteOwner
- WriteDACL
- AllExtendedRights

**By default, all authenticated users can read all ACEs on all objects!**

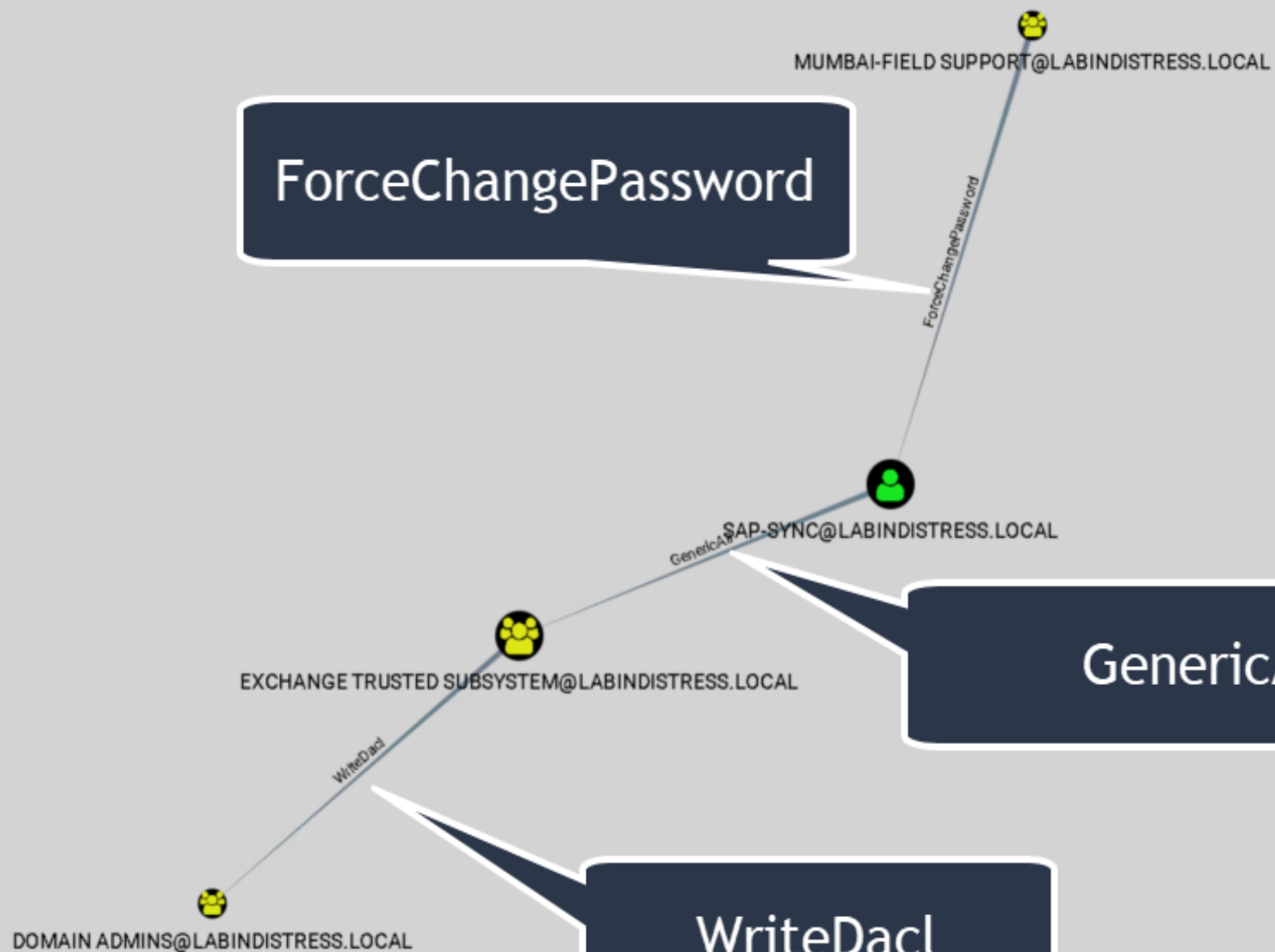
# Case Studies







**From unprivileged user to a local admin on 2 systems in the Domain!**



ForceChangePassword

GenericAll

WriteDacl

### User Info

Name	SAP-SYNC@LABINDISTRESS.LOCAL
Display Name	SAP-SYNC
Password Last Changed	Thu, 07 Jul 2011 00:53:20 GMT
Last Logon	Thu, 07 Jul 2011 00:53:20 GMT
Enabled	True

Sessions	0
Sibling Objects in the Same OU	0
Effective Inbound GPOs	0
<a href="#">See User within Domain/OU Tree</a>	

### Group Membership

First Degree Group Memberships	0
Unrolled Group Membership	0
Foreign Group Membership	0

### Local Admin Rights

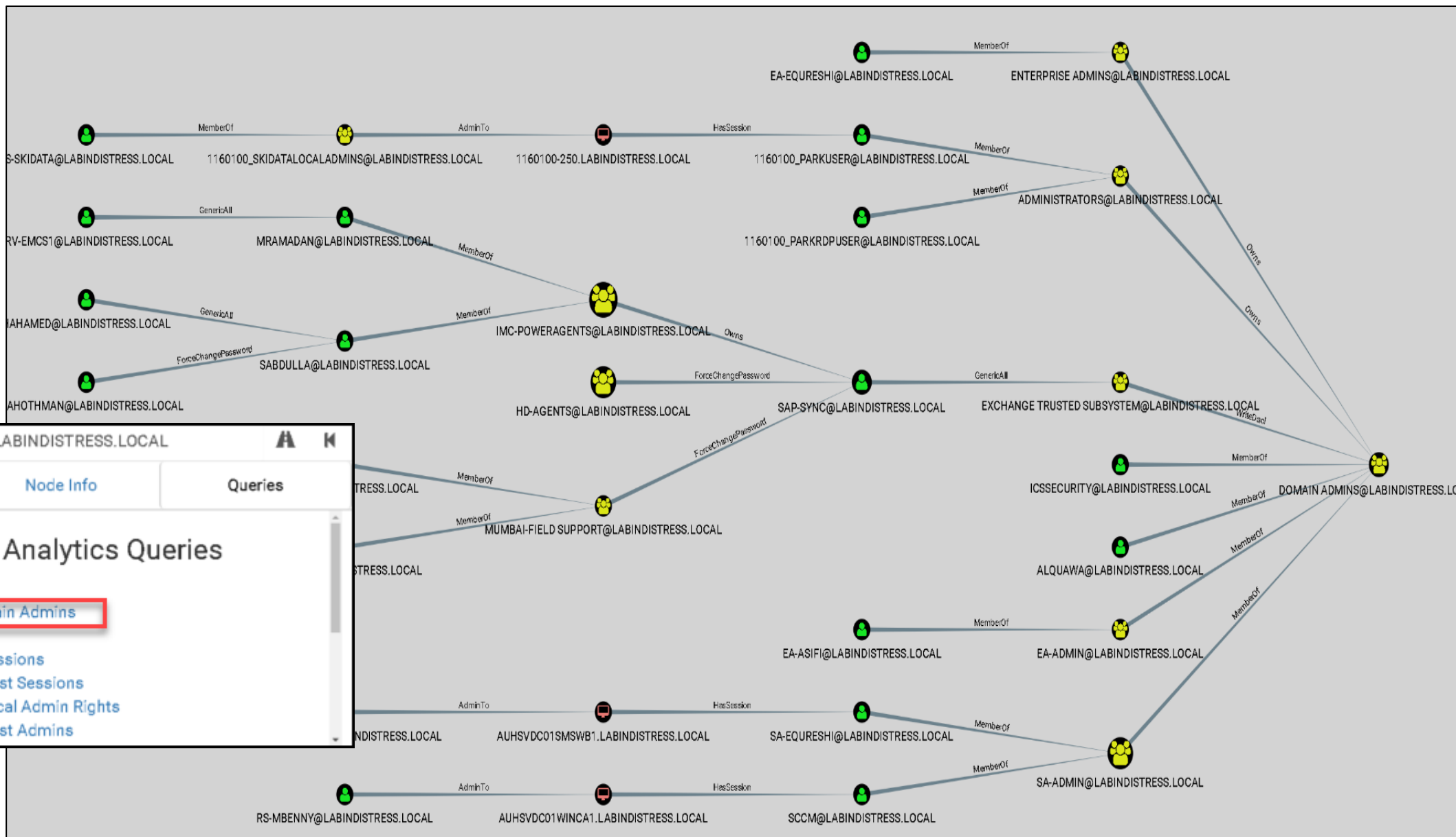
First Degree Local Admin	0
Group Delegated Local Admin Rights	0
Derivative Local Admin Rights	0

### Outbound Object Control

First Degree Object Control	12521
Group Delegated Object Control	0
Transitive Object Control	.

### Inbound Object Control

Explicit Object Controllers	9
Unrolled Object Controllers	53
Transitive Object Controllers	60



WS-FIELD SUPPORT@LABINDISTRESS.LOCAL

Database Info Node Info Queries

### Pre-Built Analytics Queries

- Find all Domain Admins
- Find Shortest Paths to Domain Admins
- Find logged in Admins
- Top Ten Users with Most Sessions
- Top Ten Computers with Most Sessions
- Top Ten Users with Most Local Admin Rights
- Top Ten Computers with Most Admins





- Bloodhound GitHub Repository

<https://github.com/BloodHoundAD/BloodHound>

- Injestor aka Data collection script/tool

<https://github.com/BloodHoundAD/BloodHound/tree/master/Ingestors>

- BloodHound User Interface

<https://github.com/BloodHoundAD/BloodHound/releases>

NOW WE'RE COMPLIANT!



**Boring security**  
**is**  
**Smart security**



Questions