Secure Ideas
professionally evil®

Active Directory Hacking

3 "New" Techniques

January 31, 2024

Eric Kuehn

Principal Security Consultant
Secure Ideas, LLC

- Based out of Charlotte, NC
- Been with Secure Ideas for over 7 years

Over 25 Years of Industry Experience

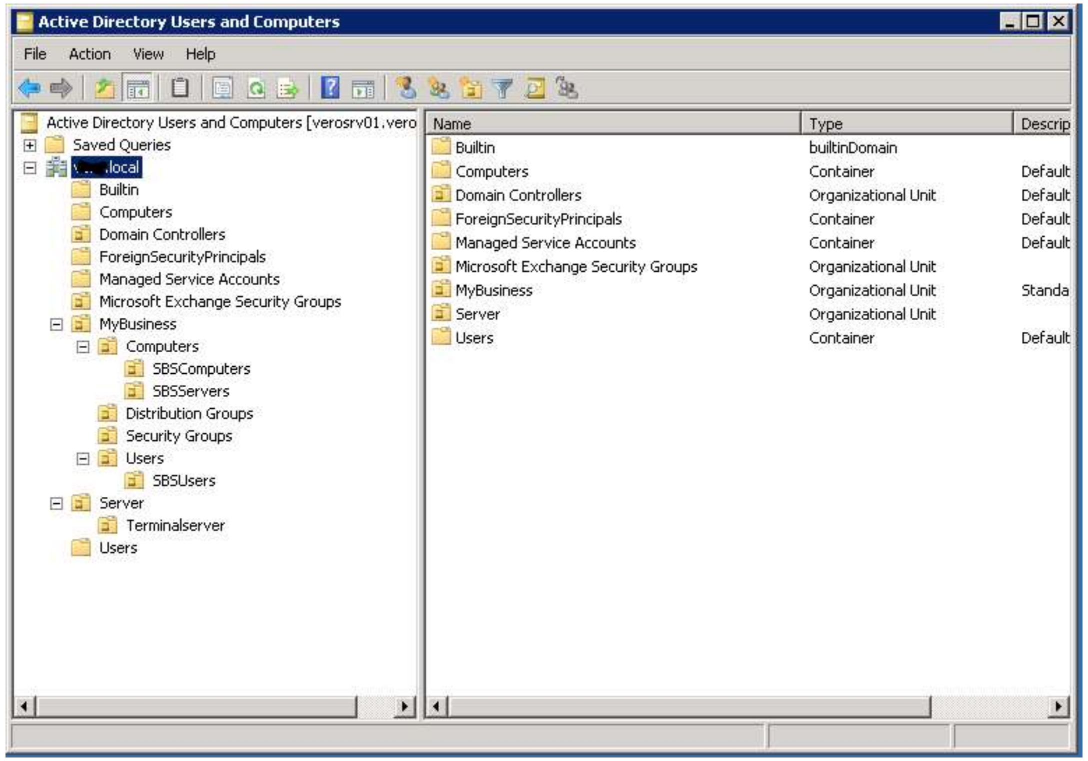
- Active Directory
- Windows Systems and Applications
- System Architecture
- Penetration Testing, Security Consulting, & Training
- MITRE ATT&CK Framework Contributor

Other Interesting Facts

- Movie Enthusiast
- Gamer
- Father of Four

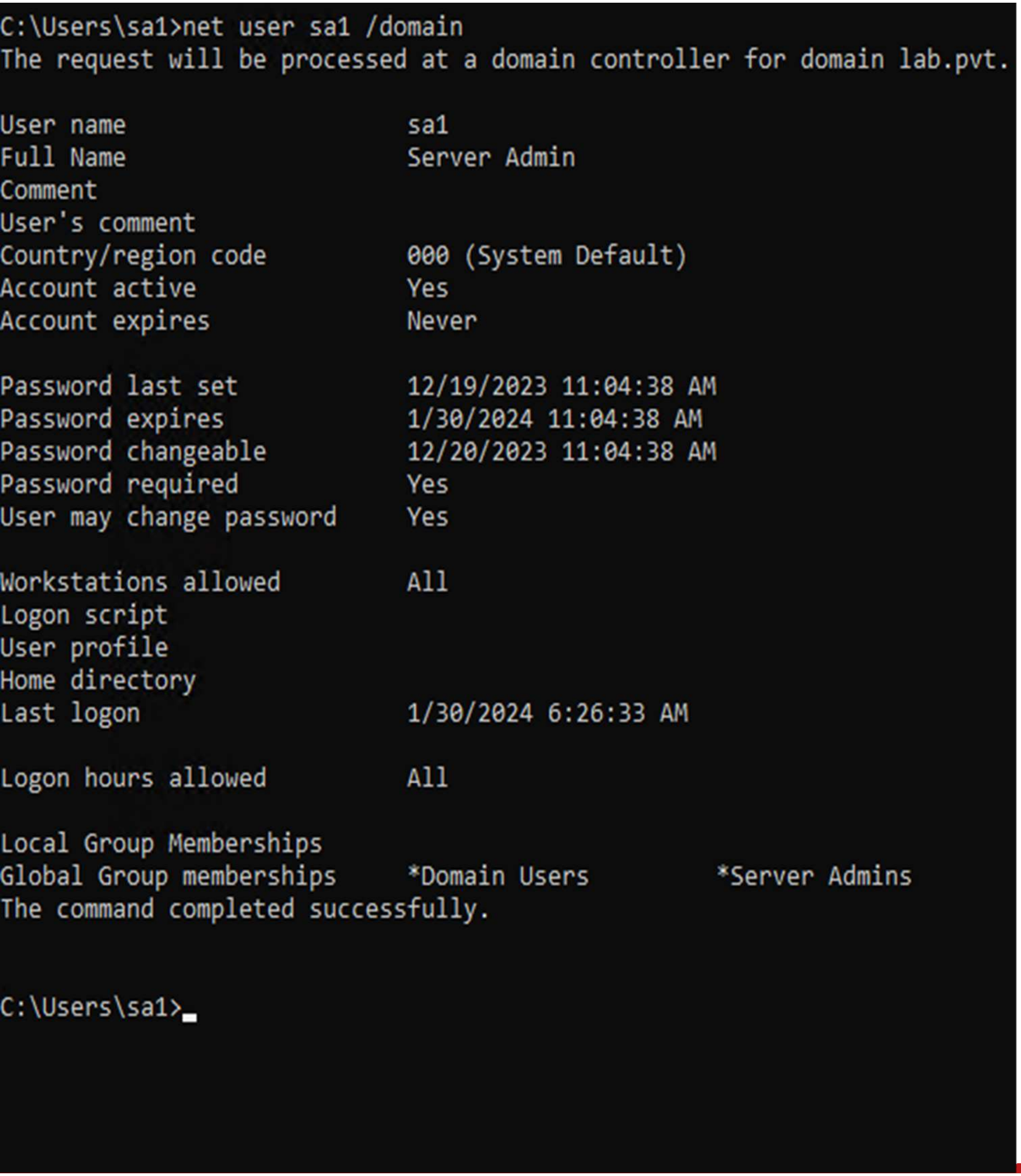
What is Active Directory / Why Do I Care?

- It's everywhere
- Provides centralized authentication and authorization in Windows networks
- Holds a significant amount of information
- Compromising it grants full control over the network



```
Active Directory Users and Computers [verosrv01.vero
⊞ Saved Queries
⊟ [redacted].local
    Builtin
    Computers
    Domain Controllers
    ForeignSecurityPrincipals
    Managed Service Accounts
    Microsoft Exchange Security Groups
  ⊟ MyBusiness
    ⊟ Computers
        SBSComputers
        SBSServers
      Distribution Groups
      Security Groups
    ⊟ Users
        SBSUsers
  ⊟ Server
      Terminalserver
    Users
```

Name	Type	Descrip
Builtin	builtinDomain	
Computers	Container	Default
Domain Controllers	Organizational Unit	Default
ForeignSecurityPrincipals	Container	Default
Managed Service Accounts	Container	Default
Microsoft Exchange Security Groups	Organizational Unit	
MyBusiness	Organizational Unit	Standa
Server	Organizational Unit	
Users	Container	Default



```
C:\Users\sa1>net user sa1 /domain
The request will be processed at a domain controller for domain lab.pvt.

User name                    sa1
Full Name                    Server Admin
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            12/19/2023 11:04:38 AM
Password expires             1/30/2024 11:04:38 AM
Password changeable          12/20/2023 11:04:38 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   1/30/2024 6:26:33 AM

Logon hours allowed          All

Local Group Memberships
Global Group memberships     *Domain Users         *Server Admins
The command completed successfully.


C:\Users\sa1>_
```

Utility 1: net.exe

- accounts
- group
- localgroup
- user

Pros

- Built-in to every version of Windows
- Easy to use to make changes

Cons

- Device must be part of the Domain you want to make the changes to
- Not the best for getting information
- Probably flagged you as suspect by EDR

Tip

- Don’t forget the /domain flag!

net.exe Examples

List members of the Domain Admins group

```
net group "Domain Admins" /domain
```

Add a member to the Domain Admins group

```
net group "Domain Admins" user1 /domain /add
```

Remove a member from the Domain Admins group

```
net group "Domain Admins" user1 /domain /delete
```

Create a new group in the domain named New Group

```
net group "New Group" /domain
```

List members of the builtin administrators group in the domain

```
net localgroup administrators /domain
```

List password policy for the domain

```
net accounts /domain
```

Get properties of a user account (sa1 in the example below) in the domain

```
net user sa1 /domain
```

Utility 2: Straight LDAP

Pros

- No extra ports needed
- Device can be in a remote domain or not in the domain at all
- Loads of tools and programs
- Not Windows specific

Cons

- Need to understand LDAP syntax
- May not return all results for a query
- Values may not be human readable
- Bad queries can kill busy DCs

Sample LDAP Filters

Return the Domain Admins group	`(&(objectclass=group)(cn=Domain Admins))`
Get properties of a user account (sa1 in the example below) in the domain	`(&(objectCategory=person)(objectClass=user)(SamAccountName=sa1))`
Return all members of the builtin administrators group	`(memberOf:1.2.840.113556.1.4.1941:=CN=Administrators,CN=Builtin,DC=lab,DC=pvt)`
Find all enabled user accounts	`(&(objectCategory=person)(objectClass=user)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))`

Modifying AD with LDP

Step One

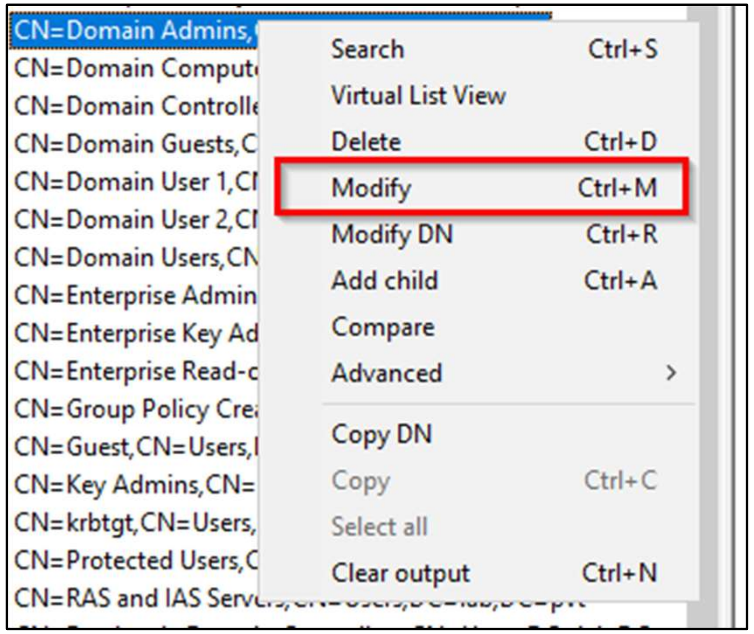
- Find the object you want to modify
- Right Click it and select Modify

Step Two

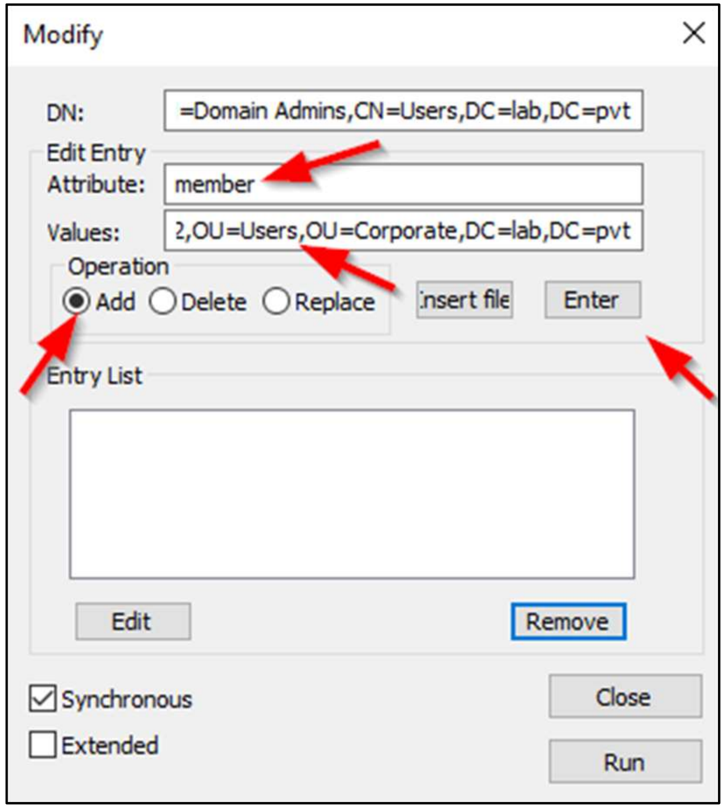
- Enter the attribute you want to update in the *Edit Entry Attribute* box
- Enter the new value you want to put in the attribute
- Select the operation you want to do to the attribute
- Click on Enter

Step Three

- Verify the value you want is in the Entry List
- Click on Run



```
CN=Domain Admins,
CN=Domain Comput
CN=Domain Controlle
CN=Domain Guests,C
CN=Domain User 1,CI
CN=Domain User 2,CI
CN=Domain Users,CN
CN=Enterprise Admin
CN=Enterprise Key Ad
CN=Enterprise Read-c
CN=Group Policy Cre
CN=Guest,CN=Users,I
CN=Key Admins,CN=
CN=krbtgt,CN=Users,
CN=Protected Users,C
CN=RAS and IAS Serv
```



DN: =Domain Admins,CN=Users,DC=lab,DC=pvt

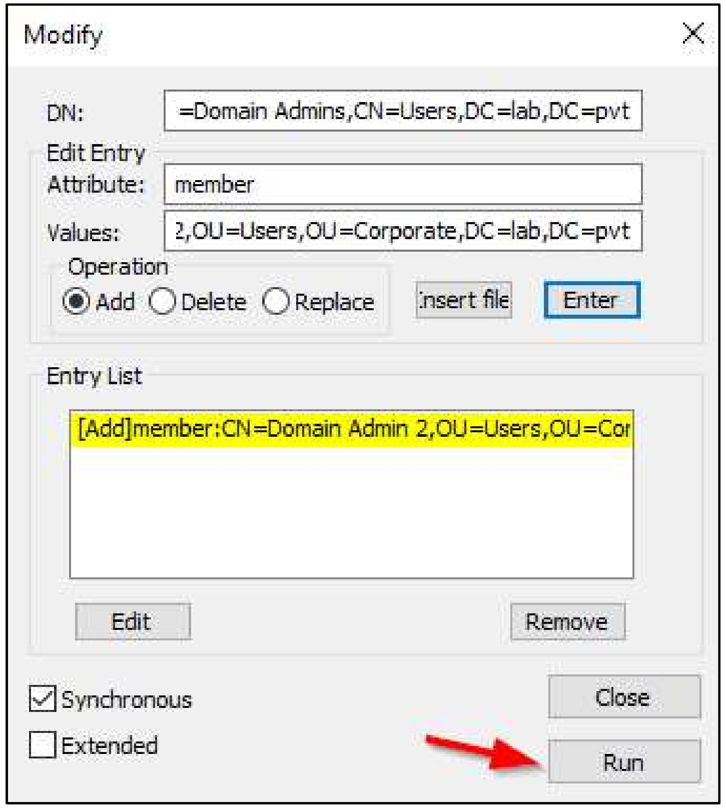
Edit Entry Attribute: member

Values: 2,OU=Users,OU=Corporate,DC=lab,DC=pvt

Operation: ● Add ○ Delete ○ Replace

☑ Synchronous

□ Extended



DN: =Domain Admins,CN=Users,DC=lab,DC=pvt

Edit Entry Attribute: member

Values: 2,OU=Users,OU=Corporate,DC=lab,DC=pvt

Operation: ● Add ○ Delete ○ Replace

Entry List

```
[Add]member:CN=Domain Admin 2,OU=Users,OU=Cor
```

☑ Synchronous

□ Extended

Utility 3: PowerShell cmdlets

Pros

- Finding objects is easy
- AD objects are returned as PowerShell objects
- Most attributes are converted to a human readable format
- Returns all objects and not just a subset
- Device can be in a remote domain or not in the domain at all

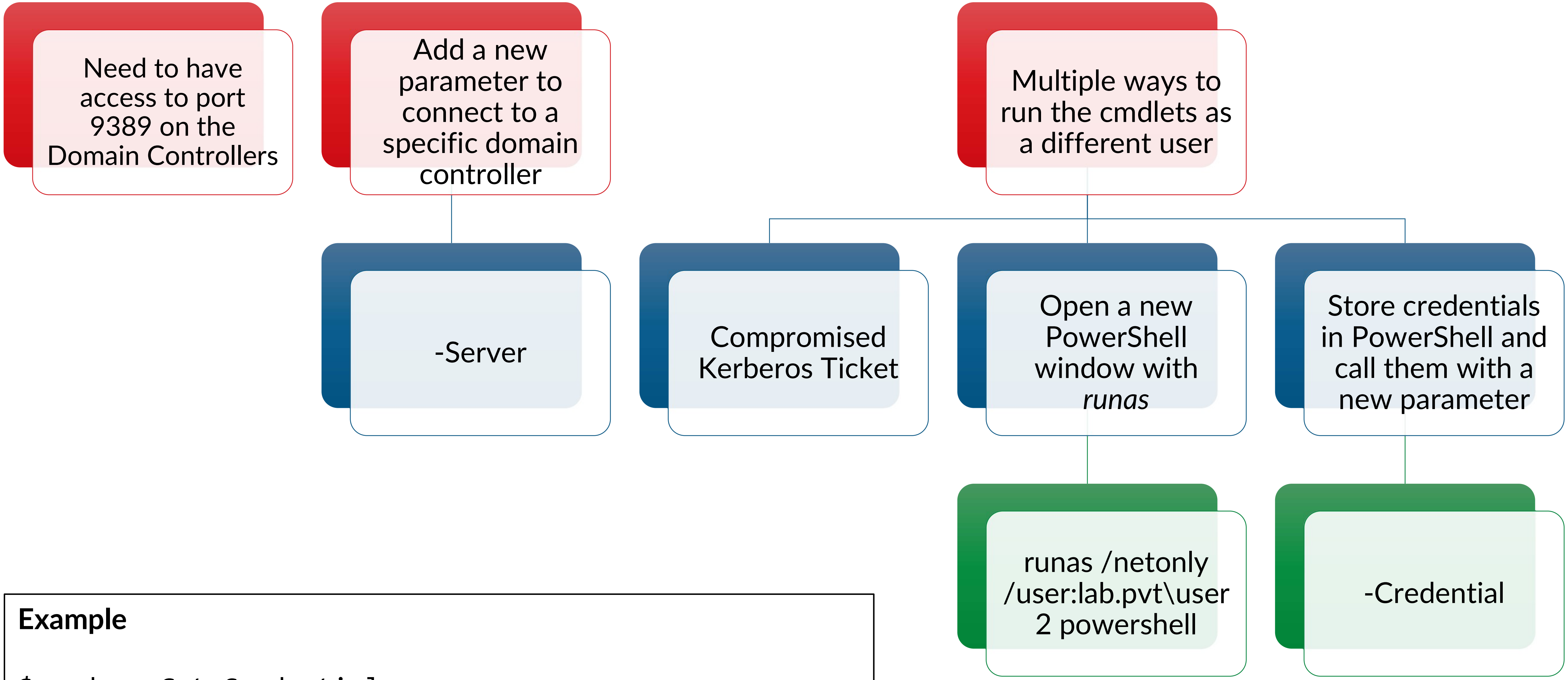
Cons

- Requires AD Web Services (port 9389) be open to device
- Most likely not on a compromised windows host
- PowerShell is verbose

PowerShell Examples

List members of the Domain Admins group	`Get-ADGroupMember "Domain Admins" –Recursive | select SamAccountName |ft`
Add a member to the Domain Admins group	`Add-ADGroupMember -Identity "Domain Admins" -Members "pt1"`
Remove a member from the Domain Admins group	`Remove-ADGroupMember -Identity "Domain Admins" -Members "pt1"`
Create a new group in the domain named New Group	`New-ADGroup "New Group" -GroupCategory Security -GroupScope Global`
List password policy for the domain	`Get-ADDefaultDomainPasswordPolicy`
Get properties of a user account (sa1 in the example below) in the domain	`Get-ADUser sa1 -Properties *`

Using AD cmdlets Remotely



Need to have access to port 9389 on the Domain Controllers

Add a new parameter to connect to a specific domain controller

-Server

Multiple ways to run the cmdlets as a different user

Compromised Kerberos Ticket

Open a new PowerShell window with *runas*

runas /netonly /user:lab.pvt\user 2 powershell

Store credentials in PowerShell and call them with a new parameter

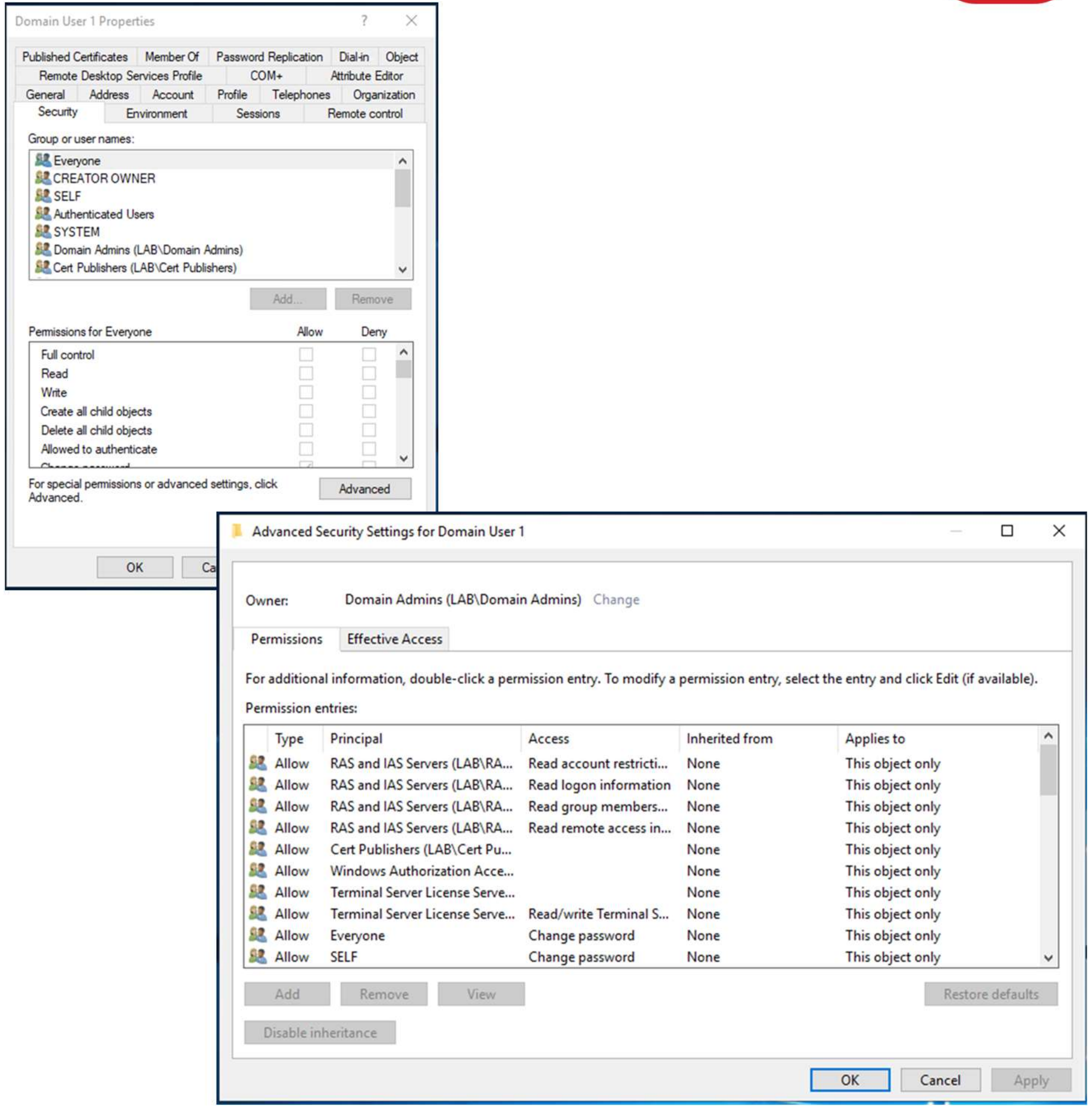
-Credential

Example

```
$creds = Get-Credential
Get-ADDomain -Server 172.27.120.92 -Credential $creds
```

Utility 4: Active Directory Users and Computers

- Pros
  - Easy to use
  - Visual representation
  - Best way to see ACLs on individual objects
- Cons
  - Can only view properties of one object at a time
  - Can't use complex queries
  - Doesn't work well unless part of the forest
  - Most likely not on a compromised windows host



Group or user names:

- Everyone
- CREATOR OWNER
- SELF
- Authenticated Users
- SYSTEM
- Domain Admins (LAB\Domain Admins)
- Cert Publishers (LAB\Cert Publishers)

Permissions for Everyone	Allow	Deny
Full control	□	□
Read	□	□
Write	□	□
Create all child objects	□	□
Delete all child objects	□	□
Allowed to authenticate	□	□

For special permissions or advanced settings, click Advanced.

Owner: Domain Admins (LAB\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	RAS and IAS Servers (LAB\RA...	Read account restricti...	None	This object only
Allow	RAS and IAS Servers (LAB\RA...	Read logon information	None	This object only
Allow	RAS and IAS Servers (LAB\RA...	Read group members...	None	This object only
Allow	RAS and IAS Servers (LAB\RA...	Read remote access in...	None	This object only
Allow	Cert Publishers (LAB\Cert Pu...		None	This object only
Allow	Windows Authorization Acce...		None	This object only
Allow	Terminal Server License Serve...		None	This object only
Allow	Terminal Server License Serve...	Read/write Terminal S...	None	This object only
Allow	Everyone	Change password	None	This object only
Allow	SELF	Change password	None	This object only

Secure Ideas professionally evil®

Questions?

Active Directory Hacking: "New" Techniques