# A Hitch-hacker's Guide to DACL-Based Detections (Part 1A)

trustedsec.com/blog/a-hitchhackers-guide-to-dacl-based-detections-part-1-a

This blog series was co-authored by Security Consultant Megan Nilsen and TAC Practice Lead Andrew Schwartz.

## 1 Introduction

If you were to collectively ask any Windows penetration tester or “red teamer” to recount their most common “attack paths,” there is no doubt that many, if not all of them, will include Active Directory (AD) based attacks. It’s easy to understand both why AD has been commonly dubbed the “attacker’s playground” and why a defender could become overwhelmed by the vast AD attack surface.

The goal of this post is to provide the “blue team” with a greater level of understanding on how these attacks “may” operate, but also help identify where an adversary may be hiding. As such, this post will strive to collectively identify those AD attributes that an attacker or adversary may modify within a target environment to lead into further access.

It is important to note that this blog is assuming that the adversary already has a foothold within the domain and has acquired the appropriate access they need to make modifications to the objects we will discuss. This post also does not examine any post exploitation (i.e., forged Kerberos tickets, etc.). We are only addressing the modifications given that the primary purpose of this exercise is to build detections to identify when changes are made. Furthermore, a level of “intelligence” (i.e., providing an attribution of attack to adversary) has not been incorporated. While “attribution matters,” for time purposes, intelligence has not been mapped to each attack.

Lastly, this post will, in a series of three (3) parts, provide classic Splunk SPL queries for detecting the attacks outlined, using only Windows Event IDs as described. Furthermore, this blog post only examines a subset of the Windows Event logging data source, and not all possible telemetry within this data set have been analyzed.

## 2 Using a Visual Roadmap - Object/Attribute Overview

The following chart, from The Hacker Recipes, provides a visual roadmap and serves as a basis to the AD Objects and Attributes that we will be working with throughout this three (3) part series. We will step through this roadmap in order to try to provide as much detection coverage as possible.

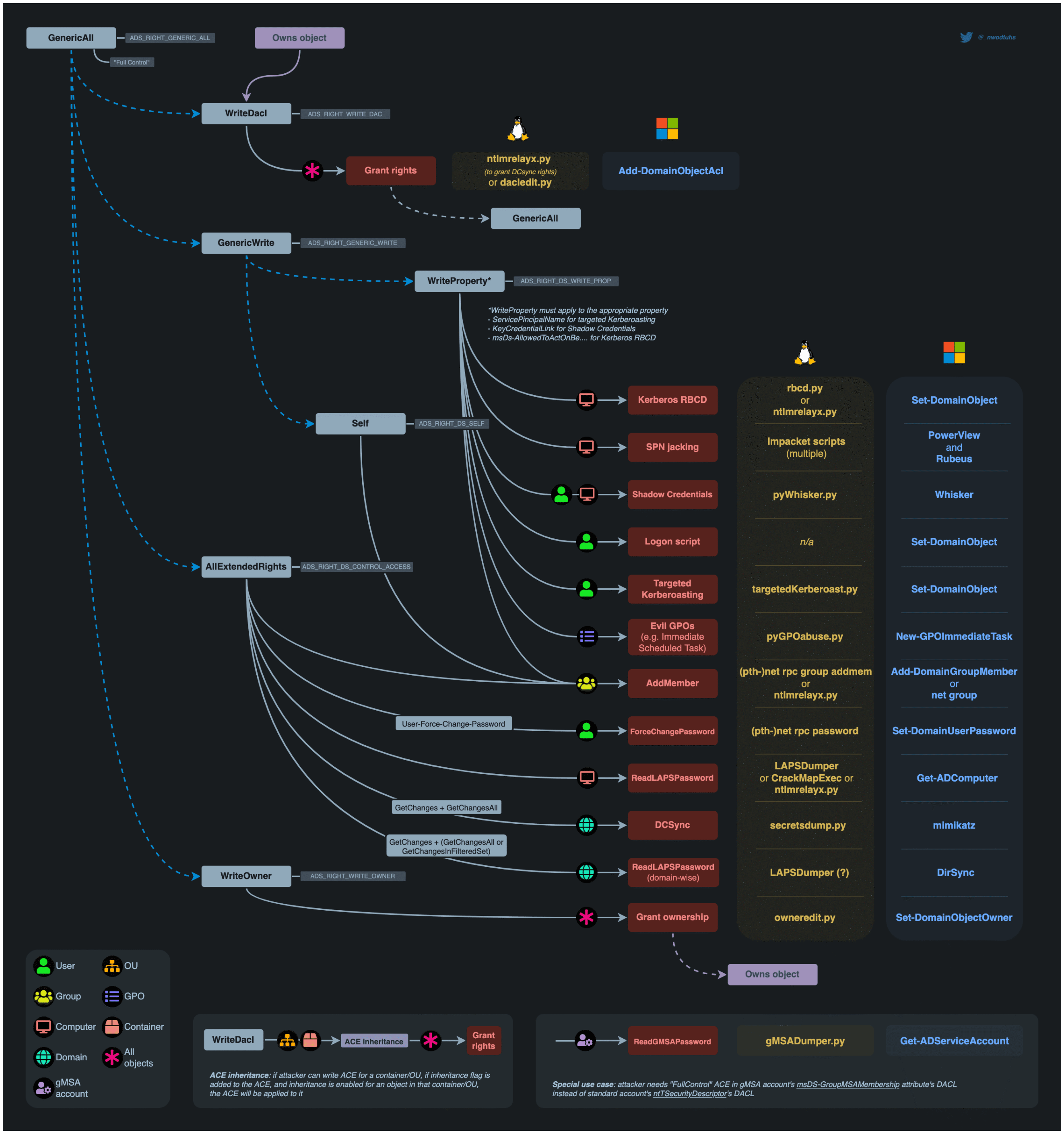


Figure 1 - Object Review Flow Chart From the Hacker Recipes

# 3 Logging Setup

## 3.1 Windows Events

It should be noted that Event ID 5136 is not enabled by default and can be configured by enabling:

***Advanced Audit Policy Configuration > Audit Polices > DS Access > Audit Directory Service Changes.***

However, there are some limitations with Event ID 5136, namely that it does not provide much contextual data for us to quickly identify what we would need to respond to a potential attack.

Enter correlation…and Windows Event IDs 4662 and 4624. Both events are part of the Advanced Auditing policies and may not be enabled by default. If we combine the data from all three (3) Event IDs, we can essentially build a template to build detections for the various modifications/changes to provide greater contextual representation.

Event 4662 is configured via by enabling:

***Advanced Audit Policy Configuration > Audit Polices > DS Access > Audit Directory Service Access.***

Event 4624 is frequently enabled by default but can be configured by enabling:

***Advanced Audit Policy Configuration > Audit Polices > Logon/Logoff > Audit Logon***

If we combine the data from all three (3) Event IDs, we can essentially build a query that provides a greater contextual representation of the attack.

In addition, for some detections, we may use other Events such as:

Event 5145, which can be configured by enabling:

***Advanced Audit Policy Configuration > Audit Polices > Detailed Tracking > Audit Detailed File Share***

Event 4742, which can be configured by enabling:

***Advanced Audit Policy Configuration > Audit Polices > Audit Computer Account Management***

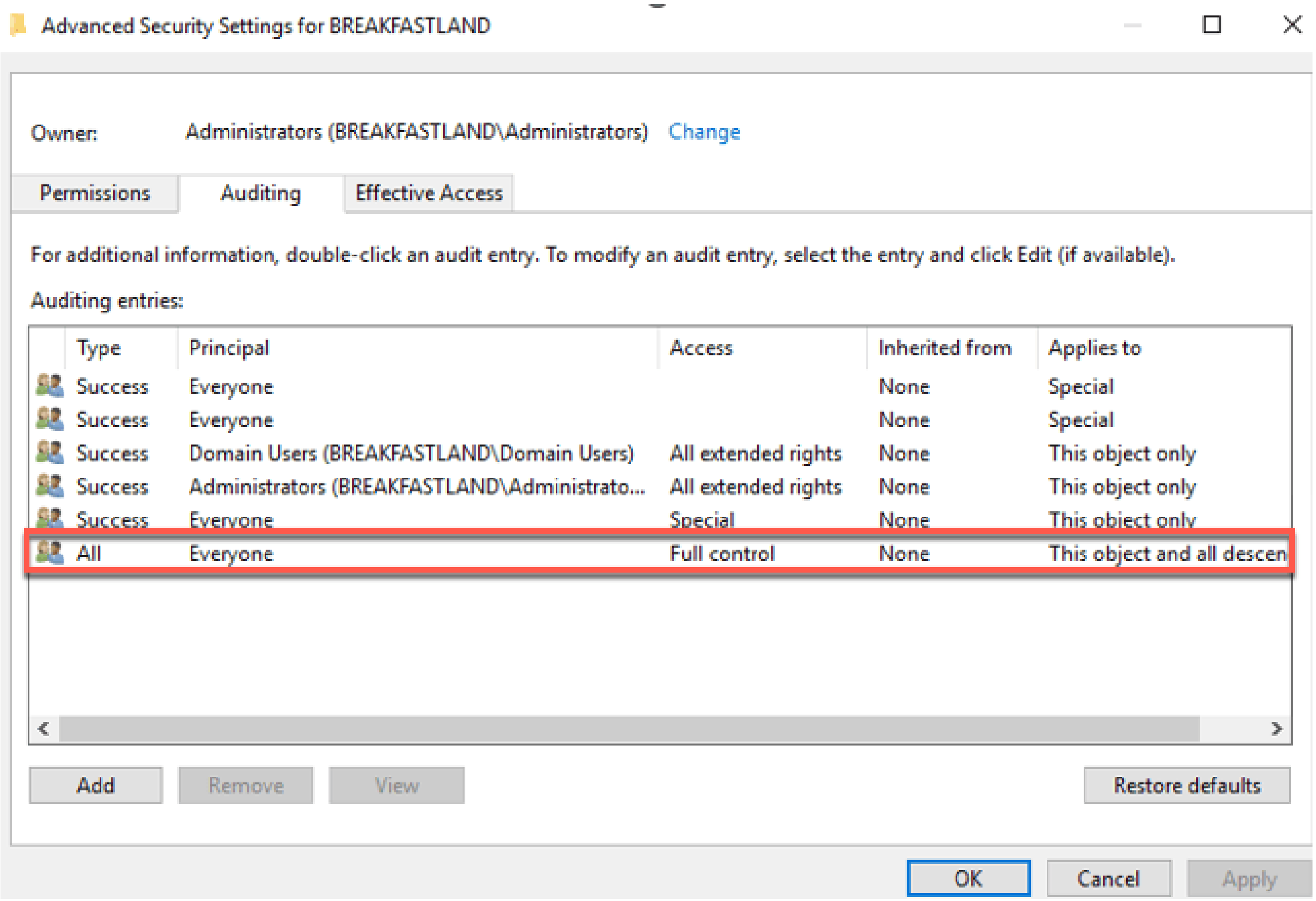
Event 4738, which can be configured by enabling:

***Advanced Audit Policy Configuration > Audit Polices > Audit User Account Management***

## 3.2 SACL

*Configuring a SACL is an* ***additional step*** *that must be taken even if the above listed Windows Events are currently being ingested.*

For the purpose of this blog post, we have created a SACL entry on the root of our Domain to audit all objects; however, this can be done more granularly if logging volume is a concern.



Advanced Security Settings for BREAKFASTLAND

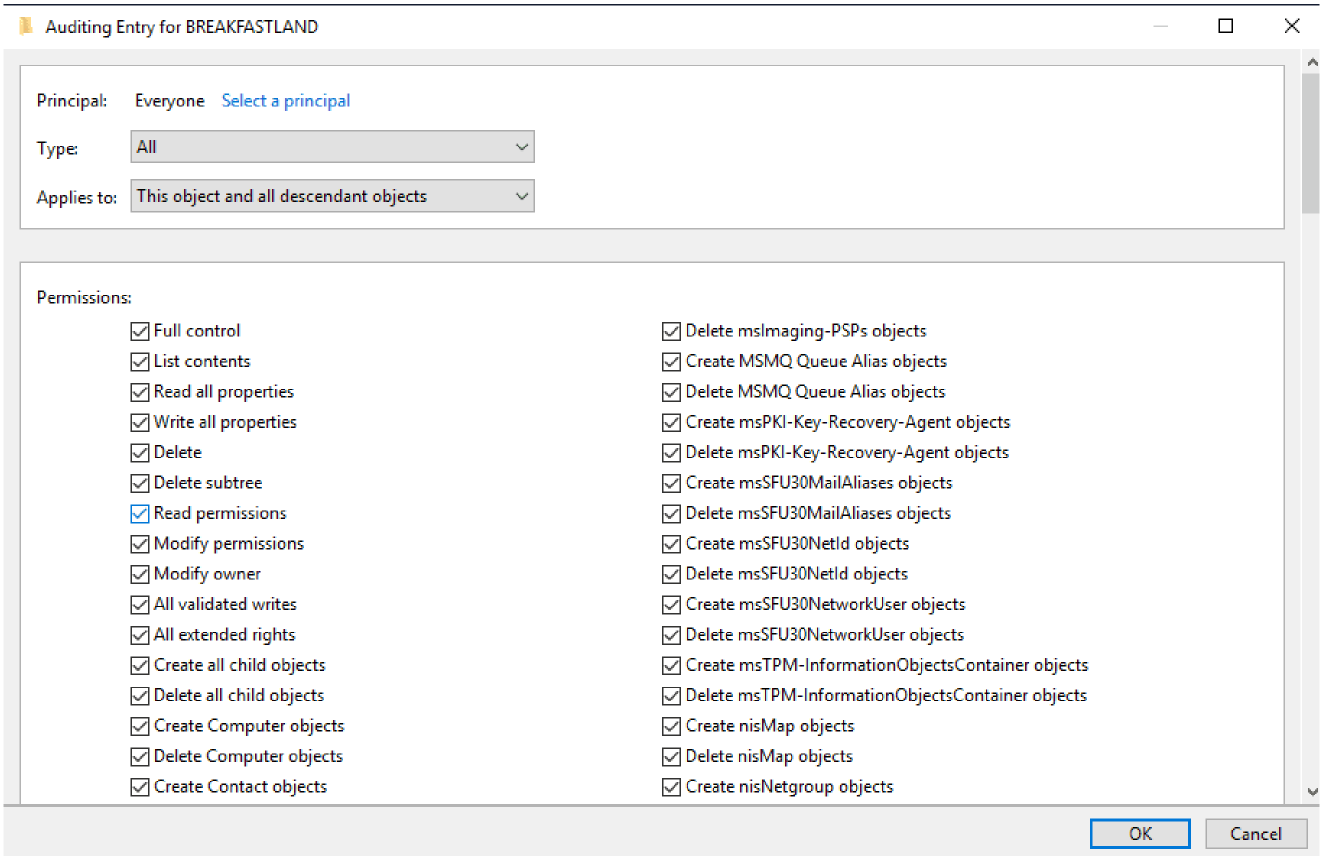
Owner: Administrators (BREAKFASTLAND\Administrators) Change

For additional information, double-click an audit entry. To modify an audit entry, select the entry and click Edit (if available).

Auditing entries:

| Type | Principal | Access | Inherited from | Applies to |
|---|---|---|---|---|
| Success | Everyone | | None | Special |
| Success | Everyone | | None | Special |
| Success | Domain Users (BREAKFASTLAND\Domain Users) | All extended rights | None | This object only |
| Success | Administrators (BREAKFASTLAND\Administrato... | All extended rights | None | This object only |
| Success | Everyone | Special | None | This object only |
| All | Everyone | Full control | None | This object and all descen |

Figure 2 - SACL Configuration for BREAKFASTLAND.LOCAL



Auditing Entry for BREAKFASTLAND

Principal: Everyone Select a principal

Type: All

Applies to: This object and all descendant objects

Permissions:

- ☑ Full control
- ☑ List contents
- ☑ Read all properties
- ☑ Write all properties
- ☑ Delete
- ☑ Delete subtree
- ☑ Read permissions
- ☑ Modify permissions
- ☑ Modify owner
- ☑ All validated writes
- ☑ All extended rights
- ☑ Create all child objects
- ☑ Delete all child objects
- ☑ Create Computer objects
- ☑ Delete Computer objects
- ☑ Create Contact objects
- ☑ Delete msImaging-PSPs objects
- ☑ Create MSMQ Queue Alias objects
- ☑ Delete MSMQ Queue Alias objects
- ☑ Create msPKI-Key-Recovery-Agent objects
- ☑ Delete msPKI-Key-Recovery-Agent objects
- ☑ Create msSFU30MailAliases objects
- ☑ Delete msSFU30MailAliases objects
- ☑ Create msSFU30NetId objects
- ☑ Delete msSFU30NetId objects
- ☑ Create msSFU30NetworkUser objects
- ☑ Delete msSFU30NetworkUser objects
- ☑ Create msTPM-InformationObjectsContainer objects
- ☑ Delete msTPM-InformationObjectsContainer objects
- ☑ Create nisMap objects
- ☑ Delete nisMap objects
- ☑ Create nisNetgroup objects

Figure 3 - SACL Configuration

In addition, you may need to enable auditing for specific User or Computer objects. We will attempt to call these items out specifically as we run through each detection; however, if you find you are not receiving the logging for the object that is being modified, be sure to check your SACL for the object as that is likely to be the issue.

## 4 Blog Format

Due to the length of this blog series and the number of attributes covered, it is important to do a quick overview of the format and what to expect.

Each section will contain the following headings:

- Name of the Attribute (CN of the attribute)
- Background

  Will cover a brief overview of what the attribute (LDAP-Display-Name) is and the relevant links to Microsoft documentation

- Modifying the Attribute (Attack)
    - Will cover how the “attack” was performed, including relevant setup for modifying the attribute in question, screenshots/commands, and tools used
    - If additional auditing was enabled for building the detection, it will also likely be covered here—or, if additional setup was more complex, will be broken out into a preceding or subsequent heading
- Building the Detections
    - Will cover a variety of detections that will include a range of complexity
    - As was stated in the introduction, not all the possible telemetry data points within this data set have been analyzed. However, we have tried our best to cover the Event IDs that are most accessible and prominent for building out detections
    - Where necessary, we will provide a flow of logic for detections that involve more complexity or additional information to interpret what is being shown. However, most detections will follow a similar format and will not be explained in further detail

# 5 Object Modifications & Detections

## 5.1 Writing to msDS-Allowed-to-Act-On-Behalf-Of-Other-Identity

Beginning at the top of the Hacker Recipes flow chart, the first attribute modification on our list is regarding Resource Based Constrained Delegation (RBCD), whereby the attack may be writing to the attribute msDS-AllowedtoActOnBehalfOfOtherIdentity. This attribute was previously examined by Andrew, Jonathan Johnson, and Charlie Clark in this post.

As this has already been covered in detail, we will not be addressing this attribute within this post.

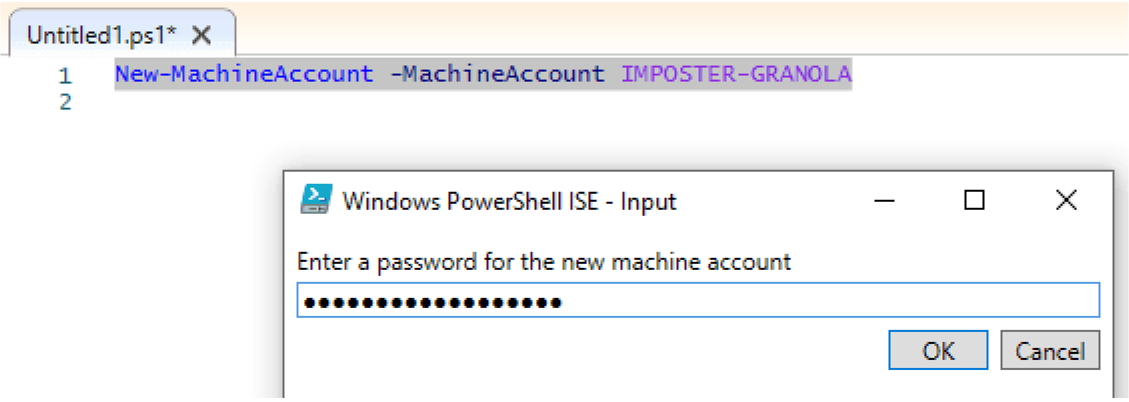
## 5.2 Writing to Service-Principal-Name (SPN)

### 5.2.1 Background

The Service Principal Name (SPN) of an object is a unique identifier that can be used by Kerberos to associate a “service instance” with an authentication attempt. SPNs are frequently abused by attackers using Impacket Modules such as GetUsersSPN.py or other hacker toolsets that exist to exploit existing SPNs or to create new ones that can be leveraged to bypass other authentication mechanisms.

### 5.2.2 Creating a Machine Account Using PowerMad

Before we can modify our SPN attribute, we are going to create a new machine account to use as our “victim” computer. This “victim” computer account will be used for many of the attribute modifications we will make with PowerMad and other tools moving forward through this blog series.



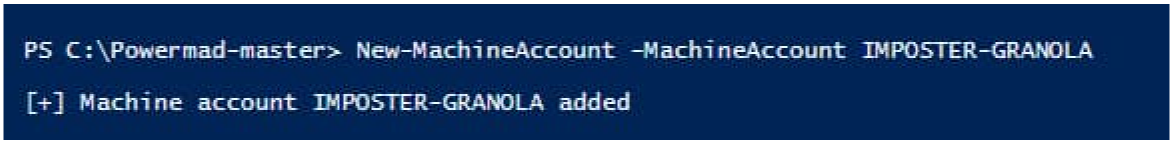
```
New-MachineAccount -MachineAccount IMPOSTER-GRANOLA
```

Windows PowerShell ISE - Input

Enter a password for the new machine account

••••••••••••••••••

Figure 4 - Creating a New Computer Account



```
PS C:\Powermad-master> New-MachineAccount -MachineAccount IMPOSTER-GRANOLA
[+] Machine account IMPOSTER-GRANOLA added
```

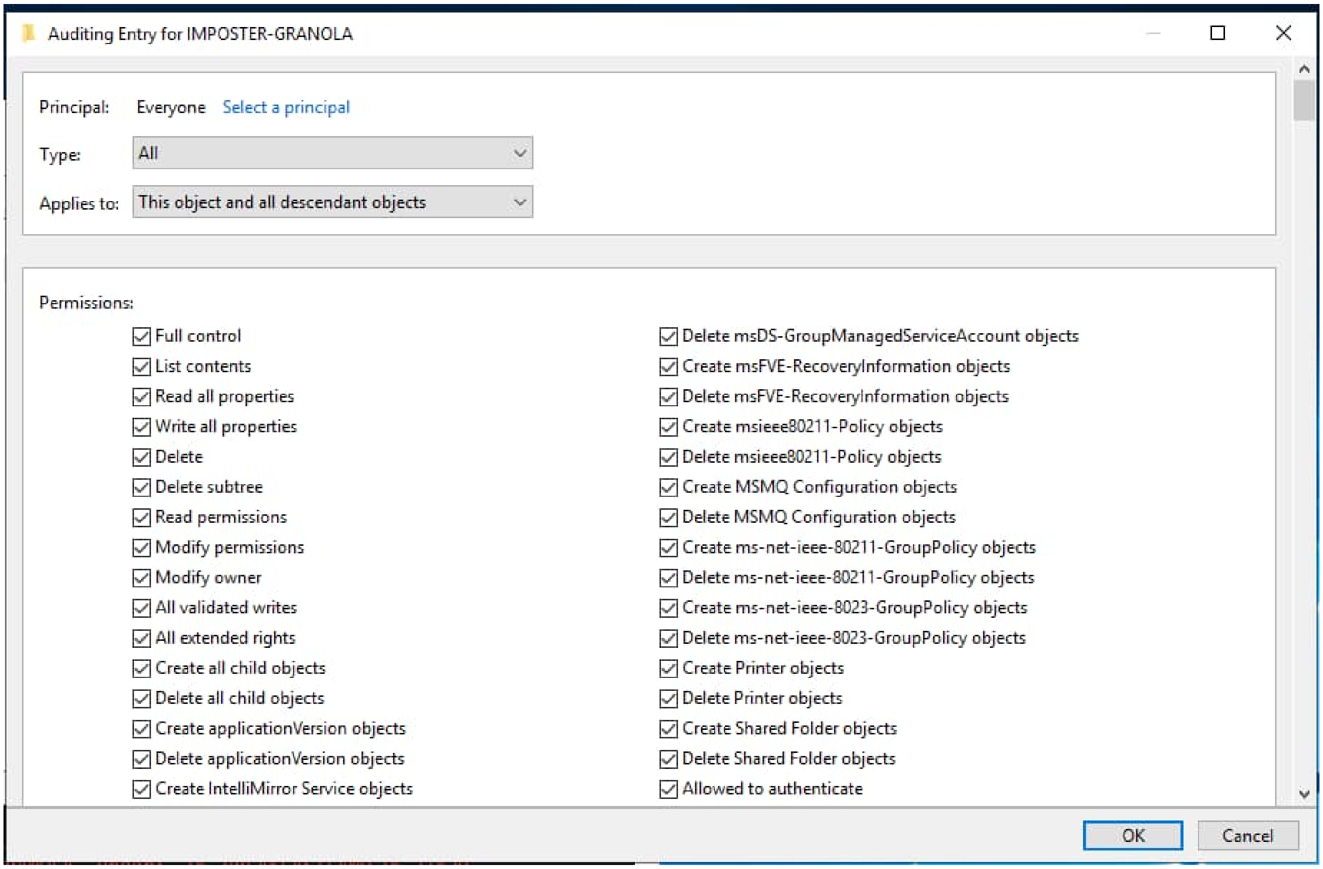
Figure 5 - Computer Account Creation with PowerMad

Before changing any attributes, this is what the **IMPOSTER-GRANOLA$** machine account we created looks like as a freshly created object.

```
PS C:\Users\head.chef> Get-ADComputer -Identity "IMPOSTER-GRANOLA" -Properties *


AccountExpirationDate               :
accountExpires                             : 9223372036854775807
AccountLockoutTime                   :
AccountNotDelegated                  : False
AllowReversiblePasswordEncryption    : False
AuthenticationPolicy                 : {}
AuthenticationPolicySilo             : {}
BadLogonCount                        : 0
badPasswordTime                      : 0
badPwdCount                          : 0
CannotChangePassword                 : False
CanonicalName                        : BREAKFASTLAND.LOCAL/Computers/IMPOSTER-GRANOLA
Certificates                         : {}
CN                                   : IMPOSTER-GRANOLA
codePage                             : 0
CompoundIdentitySupported            : {}
countryCode                          : 0
Created                              : 5/30/2023 11:59:24 AM
createTimeStamp                      : 5/30/2023 11:59:24 AM
Deleted                              :
Description                          :
DisplayName                          :
DistinguishedName                    : CN=IMPOSTER-
GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL
DNSHostName                          : IMPOSTER-GRANOLA.breakfastland.local
DoesNotRequirePreAuth                : False
dSCorePropagationData                : {12/31/1600 4:00:00 PM}
Enabled                              : True
HomedirRequired                      : False
HomePage                             :
instanceType                         : 4
IPv4Address                          :
IPv6Address                          :
isCriticalSystemObject               : False
isDeleted                            :
KerberosEncryptionType               : {}
LastBadPasswordAttempt               :
LastKnownParent                      :
lastLogoff                           : 0
lastLogon                            : 0
LastLogonDate                        :
localPolicyFlags                     : 0
Location                             :
LockedOut                            : False
logonCount                           : 0
ManagedBy                            :
MemberOf                             : {}
MNSLogonAccount                      : False
Modified                             : 5/30/2023 11:59:24 AM
```

```
modifyTimeStamp                      : 5/30/2023 11:59:24 AM
msDS-User-Account-Control-Computed   : 0
Name                                 : IMPOSTER-GRANOLA
nTSecurityDescriptor                 :
System.DirectoryServices.ActiveDirectorySecurity
ObjectCategory                       :
CN=Computer,CN=Schema,CN=Configuration,DC=BREAKFASTLAND,DC=LOCAL
ObjectClass                          : computer
ObjectGUID                           : 863169ce-25a7-468d-a147-3e193587df4f
objectSid                            : S-1-5-21-1865600711-3446354287-3882071624-1113
OperatingSystem                      :
OperatingSystemHotfix                :
OperatingSystemServicePack           :
OperatingSystemVersion               :
PasswordExpired                      : False
PasswordLastSet                      : 5/30/2023 11:59:24 AM
PasswordNeverExpires                 : False
PasswordNotRequired                  : False
PrimaryGroup                         : CN=Domain
Computers,CN=Users,DC=BREAKFASTLAND,DC=LOCAL
primaryGroupID                       : 515
PrincipalsAllowedToDelegateToAccount : {}
ProtectedFromAccidentalDeletion      : False
pwdLastSet                           : 133299467648286422
SamAccountName                       : IMPOSTER-GRANOLA$
sAMAccountType                       : 805306369
sDRightsEffective                    : 15
ServiceAccount                       : {}
servicePrincipalName                 : {RestrictedKrbHost/IMPOSTER-GRANOLA,
HOST/IMPOSTER-GRANOLA,
                                       RestrictedKrbHost/IMPOSTER-
GRANOLA.breakfastland.local,
                                       HOST/IMPOSTER-GRANOLA.breakfastland.local}
ServicePrincipalNames                : {RestrictedKrbHost/IMPOSTER-GRANOLA,
HOST/IMPOSTER-GRANOLA,
                                       RestrictedKrbHost/IMPOSTER-
GRANOLA.breakfastland.local,
                                       HOST/IMPOSTER-GRANOLA.breakfastland.local}
SID                                  : S-1-5-21-1865600711-3446354287-3882071624-1113
SIDHistory                           : {}
TrustedForDelegation                 : False
TrustedToAuthForDelegation           : False
UseDESKeyOnly                        : False
userAccountControl                   : 4096
userCertificate                      : {}
UserPrincipalName                    :
uSNChanged                           : 376938
uSNCreated                           : 376936
whenChanged                          : 5/30/2023 11:59:24 AM
whenCreated                          : 5/30/2023 11:59:24 AM
```

We will also need to build a SACL for the **IMPOSTER-GRANOLA$** computer object in order to receive the appropriate logging within our SIEM. In this case I have enabled full auditing for this object.



Auditing Entry for IMPOSTER-GRANOLA

Principal: Everyone Select a principal

Type: All

Applies to: This object and all descendant objects

Permissions:

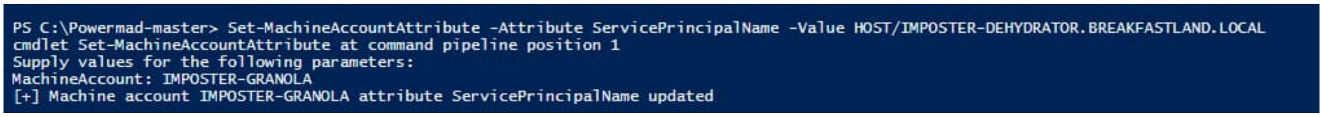
- ☑ Full control
- ☑ List contents
- ☑ Read all properties
- ☑ Write all properties
- ☑ Delete
- ☑ Delete subtree
- ☑ Read permissions
- ☑ Modify permissions
- ☑ Modify owner
- ☑ All validated writes
- ☑ All extended rights
- ☑ Create all child objects
- ☑ Delete all child objects
- ☑ Create applicationVersion objects
- ☑ Delete applicationVersion objects
- ☑ Create IntelliMirror Service objects
- ☑ Delete msDS-GroupManagedServiceAccount objects
- ☑ Create msFVE-RecoveryInformation objects
- ☑ Delete msFVE-RecoveryInformation objects
- ☑ Create msieee80211-Policy objects
- ☑ Delete msieee80211-Policy objects
- ☑ Create MSMQ Configuration objects
- ☑ Delete MSMQ Configuration objects
- ☑ Create ms-net-ieee-80211-GroupPolicy objects
- ☑ Delete ms-net-ieee-80211-GroupPolicy objects
- ☑ Create ms-net-ieee-8023-GroupPolicy objects
- ☑ Delete ms-net-ieee-8023-GroupPolicy objects
- ☑ Create Printer objects
- ☑ Delete Printer objects
- ☑ Create Shared Folder objects
- ☑ Delete Shared Folder objects
- ☑ Allowed to authenticate

Figure 6 - Adding Auditing for **IMPOSTER-GRANOLA**

### 5.2.3 Modifying the Attribute (Attack)

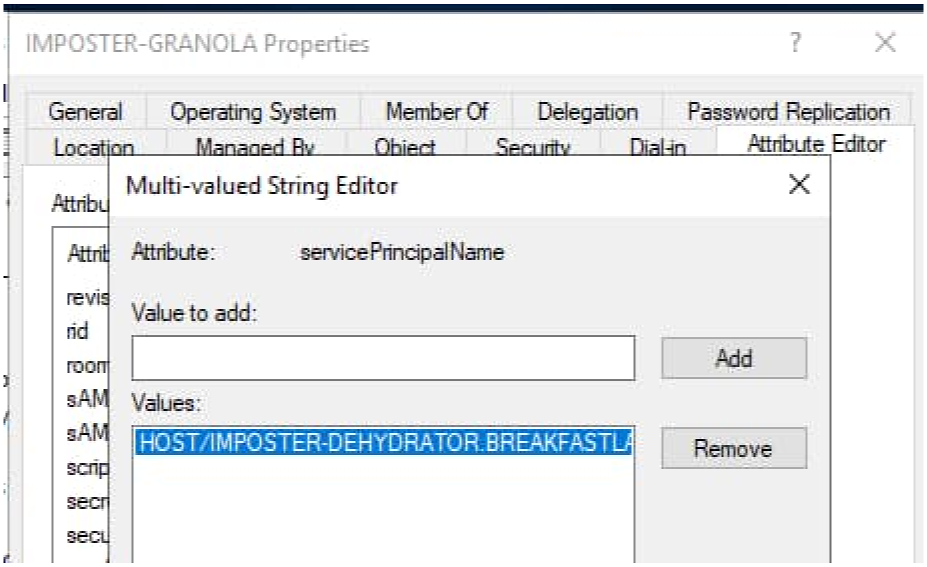
To modify the SPN attribute directly, we will use the PowerMad toolset, leveraging the `Set-MachineAccountAttribute` cmdlet:

```
Set-MachineAccountAttribute -Attribute ServicePrincipalName -Value ‘HOST/IMPOSTER-DEHYDRATOR.BREAKFASTLAND.LOCAL’
```



```
PS C:\Powermad-master> Set-MachineAccountAttribute -Attribute ServicePrincipalName -Value HOST/IMPOSTER-DEHYDRATOR.BREAKFASTLAND.LOCAL
cmdlet Set-MachineAccountAttribute at command pipeline position 1
Supply values for the following parameters:
MachineAccount: IMPOSTER-GRANOLA
[+] Machine account IMPOSTER-GRANOLA attribute ServicePrincipalName updated
```

Figure 7 - Modifying SPN Attribute



Attribute: servicePrincipalName

Value to add:

Values:

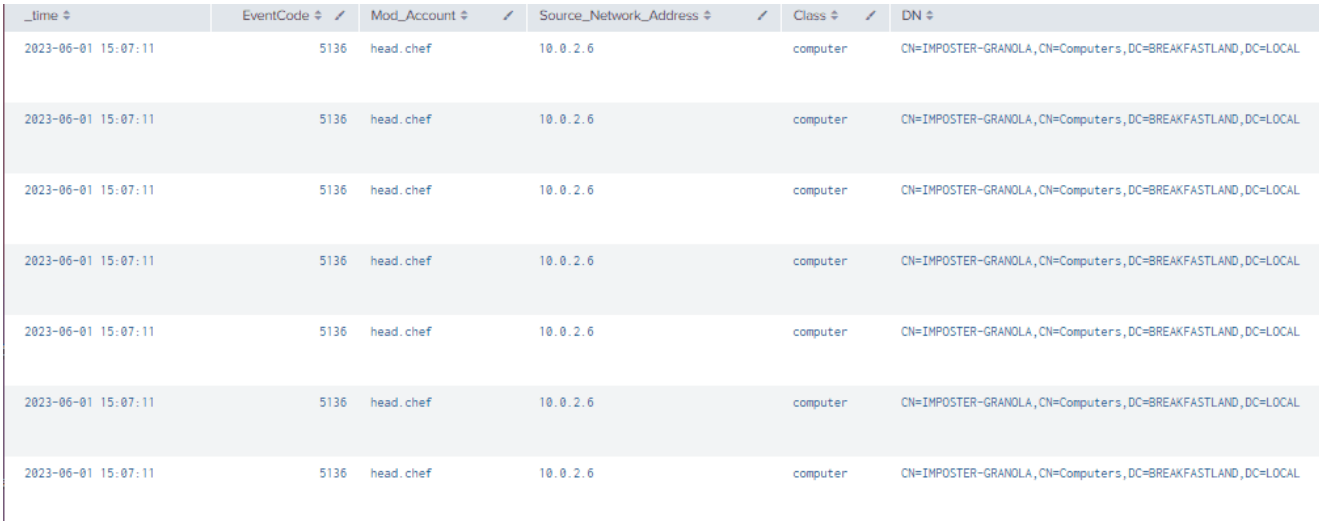
HOST/IMPOSTER-DEHYDRATOR.BREAKFASTLA

Figure 8 - ServicePrincipalName Attribute Post Modification

## 5.2.4 Building the Detections

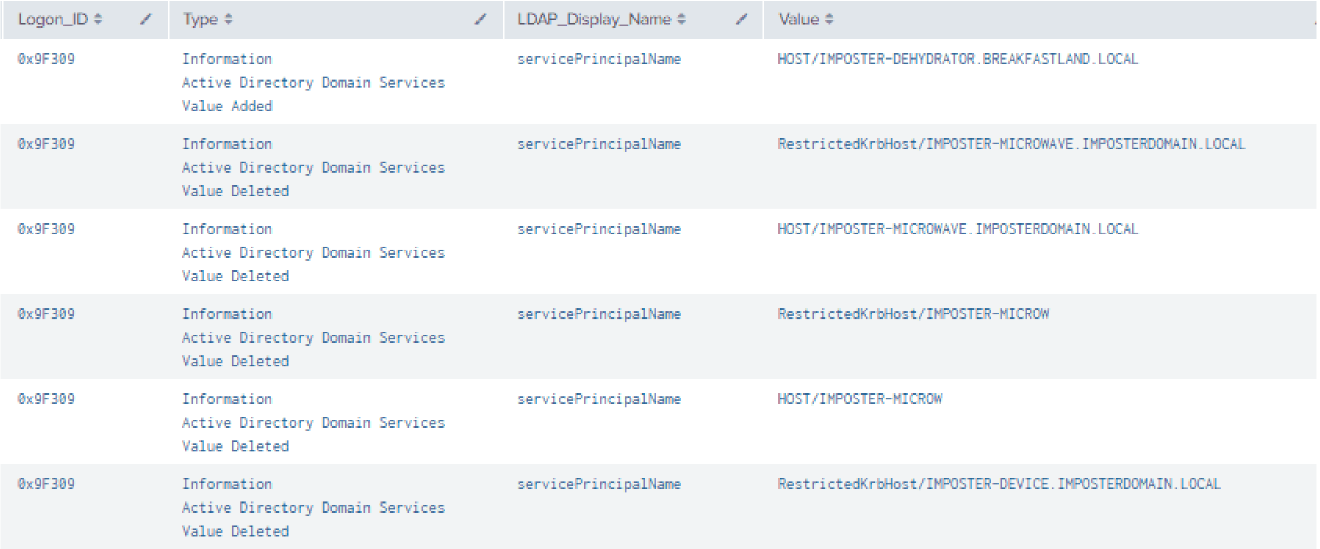
### 5.2.4.1 Detection With Event IDs 5136 and 4662

```
index=main ((EventCode=5136 AND LDAP_Display_Name=servicePrincipalName)  OR
(EventCode=4624 AND Account_Name!="*$" AND Account_Name!="ANONYMOUS LOGON" AND
Account_Name!="SYSTEM"))
| eval Logon_ID=if(EventCode==4624,mvindex(Logon_ID,-1), mvindex(Logon_ID,-1))
| eval Mod_Account=if(EventCode==4624,mvindex(Account_Name,-1),
mvindex(Account_Name,-1))
| join type=outer Logon_ID
        [ search (EventCode=5136) OR (EventCode=4624)
        | stats count by Logon_ID, Account_Name, Source_Network_Address
        | table Account_Name,Logon_ID, Source_Network_Address]
| table _time, EventCode, Mod_Account, Source_Network_Address, Class, DN, Logon_ID,
Type, LDAP_Display_Name, Value
| where  len(Class)>0
```



| _time ⇕ | EventCode ⇕ | Mod_Account ⇕ | Source_Network_Address ⇕ | Class ⇕ | DN ⇕ |
|---|---|---|---|---|---|
| 2023-06-01 15:07:11 | 5136 | head.chef | 10.0.2.6 | computer | CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL |
| 2023-06-01 15:07:11 | 5136 | head.chef | 10.0.2.6 | computer | CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL |
| 2023-06-01 15:07:11 | 5136 | head.chef | 10.0.2.6 | computer | CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL |
| 2023-06-01 15:07:11 | 5136 | head.chef | 10.0.2.6 | computer | CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL |
| 2023-06-01 15:07:11 | 5136 | head.chef | 10.0.2.6 | computer | CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL |
| 2023-06-01 15:07:11 | 5136 | head.chef | 10.0.2.6 | computer | CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL |
| 2023-06-01 15:07:11 | 5136 | head.chef | 10.0.2.6 | computer | CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL |

Figure 9 - Detection with Event IDs 5136 and 4624 (1)

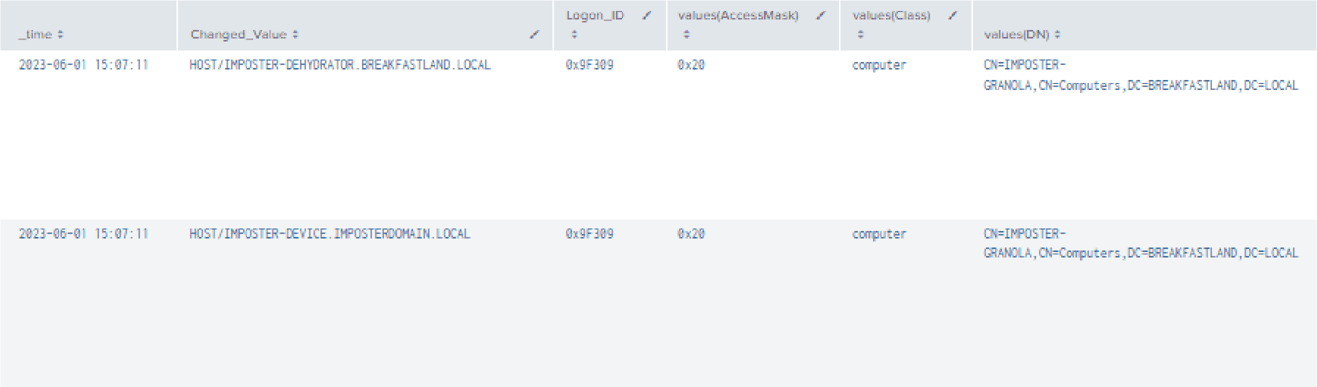


| Logon_ID | Type | LDAP_Display_Name | Value |
|---|---|---|---|
| 0x9F309 | Information<br>Active Directory Domain Services<br>Value Added | servicePrincipalName | HOST/IMPOSTER-DEHYDRATOR.BREAKFASTLAND.LOCAL |
| 0x9F309 | Information<br>Active Directory Domain Services<br>Value Deleted | servicePrincipalName | RestrictedKrbHost/IMPOSTER-MICROWAVE.IMPOSTERDOMAIN.LOCAL |
| 0x9F309 | Information<br>Active Directory Domain Services<br>Value Deleted | servicePrincipalName | HOST/IMPOSTER-MICROWAVE.IMPOSTERDOMAIN.LOCAL |
| 0x9F309 | Information<br>Active Directory Domain Services<br>Value Deleted | servicePrincipalName | RestrictedKrbHost/IMPOSTER-MICROW |
| 0x9F309 | Information<br>Active Directory Domain Services<br>Value Deleted | servicePrincipalName | HOST/IMPOSTER-MICROW |
| 0x9F309 | Information<br>Active Directory Domain Services<br>Value Deleted | servicePrincipalName | RestrictedKrbHost/IMPOSTER-DEVICE.IMPOSTERDOMAIN.LOCAL |

Figure 10 - Detection with Event IDs 5136 and 4624 (2)

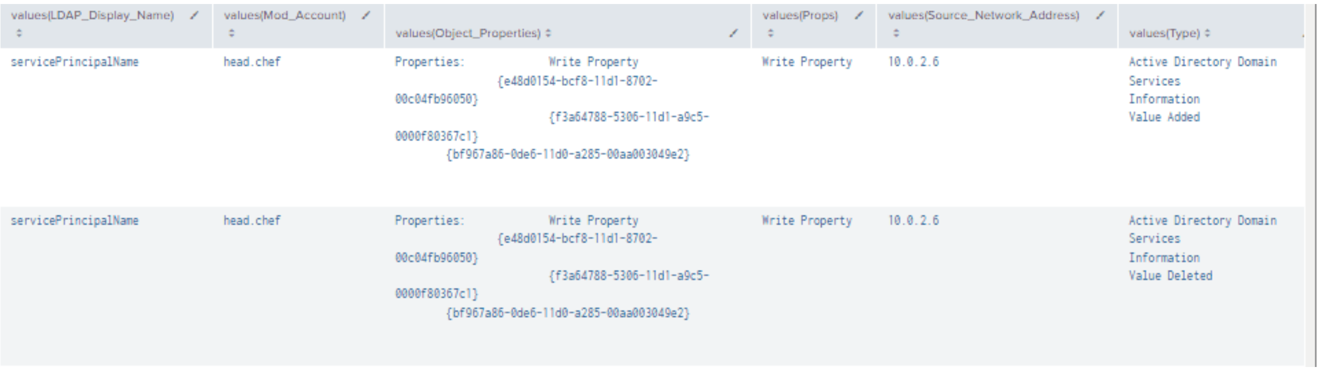
### 5.2.4.2 Detection With Event IDs 5136, 4624, and 4662

```
index=main ((EventCode=5136 AND LDAP_Display_Name=servicePrincipalName)  OR
(EventCode=4624 AND Account_Name!="*$" AND Account_Name!="ANONYMOUS LOGON" AND
Account_Name!="SYSTEM") OR (EventCode=4662 AND Access_Mask=0x20))
| eval Logon_ID=if(EventCode==4624,mvindex(Logon_ID,-1), mvindex(Logon_ID,-1))
| eval Mod_Account=if(EventCode==4624,mvindex(Account_Name,-1),
mvindex(Account_Name,-1))
| eval Changed_Value=if(EventCode==5136,mvindex(Value,-1), mvindex(Value,-1)) | join
type=outer Logon_ID
        [ search (EventCode=5136) OR (EventCode=4624)
        | stats count by Logon_ID, Account_Name, Source_Network_Address
        | table Account_Name,Logon_ID, Source_Network_Address ]
| join type=outer Logon_ID
    [ search index=main Account_Name!=*$  EventCode=4662 Access_Mask = 0x20
    | eval Props=Properties
    | eval AccessMask=Access_Mask
    | eval ObjectType=Object_Type
    | eval ObjectName=Object_Name
    | rex field=Message "(?<Object_Properties>(?ms)(?<=)Properties:(.*?)(?
=Additional\s+))"
    |table Account_Name,Logon_ID,Props,AccessMask,ObjectType, ObjectName,
Object_Properties]
| table _time, Mod_Account, Source_Network_Address , Class, DN, Logon_ID, Type,
LDAP_Display_Name, Changed_Value, AccessMask, Props, Object_Properties
| where  len(Class)>0
| stats values by _time, Changed_Value, Logon_ID
```



| _time | Changed_Value | Logon_ID | values(AccessMask) | values(Class) | values(DN) |
|---|---|---|---|---|---|
| 2023-06-01 15:07:11 | HOST/IMPOSTER-DEHYDRATOR.BREAKFASTLAND.LOCAL | 0x9F309 | 0x20 | computer | CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL |
| 2023-06-01 15:07:11 | HOST/IMPOSTER-DEVICE.IMPOSTERDOMAIN.LOCAL | 0x9F309 | 0x20 | computer | CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL |

Figure 11 – Detection with Event IDs 5136, 4662, 4624 (1)

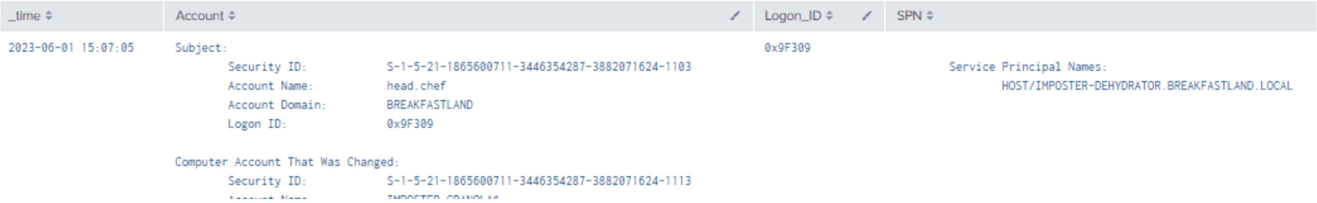


| values(LDAP_Display_Name) | values(Mod_Account) | values(Object_Properties) | values(Props) | values(Source_Network_Address) | values(Type) |
|---|---|---|---|---|---|
| servicePrincipalName | head.chef | Properties: Write Property<br>{e48d0154-bcf8-11d1-8702-00c04fb96050}<br>{f3a64788-5306-11d1-a9c5-0000f80367c1}<br>{bf967a86-0de6-11d0-a285-00aa003049e2} | Write Property | 10.0.2.6 | Active Directory Domain Services Information Value Added |
| servicePrincipalName | head.chef | Properties: Write Property<br>{e48d0154-bcf8-11d1-8702-00c04fb96050}<br>{f3a64788-5306-11d1-a9c5-0000f80367c1}<br>{bf967a86-0de6-11d0-a285-00aa003049e2} | Write Property | 10.0.2.6 | Active Directory Domain Services Information Value Deleted |

Figure 12 - Detection with Event IDs 5136, 4662, 4624 (2)

5.2.4.3 Detection With Event ID 4742

```
index=main EventCode=4742   | rex field=Message "(?<Account>(?
ms)..........................................................................Account\
s+Name.*?(Account\s+Name:\s+)(\w+..........))"    | rex field=Message "(?<SPN>(?
ms)\s+Service\s+Principal\s+Name(.*).+?(?=Additional\s+))"    | search SPN!="*Service
Principal Names: -*" | table  _time, Account,
 Logon_ID, SPN
```



| _time | Account | Logon_ID | SPN |
|---|---|---|---|
| 2023-06-01 15:07:05 | Subject:<br>Security ID: S-1-5-21-1865600711-3446354287-3882071624-1103<br>Account Name: head.chef<br>Account Domain: BREAKFASTLAND<br>Logon ID: 0x9F309<br>Computer Account That Was Changed:<br>Security ID: S-1-5-21-1865600711-3446354287-3882071624-1113 | 0x9F309 | Service Principal Names:<br>HOST/IMPOSTER-DEHYDRATOR.BREAKFASTLAND.LOCAL |

Figure 13 - Detection With Event ID 4742

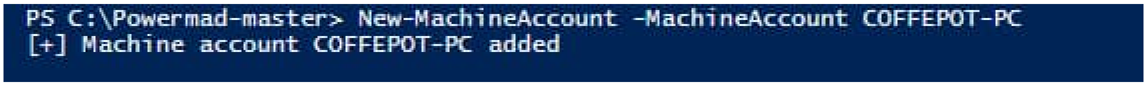
## 5.3 Writing to msDS-Allowed-to-Delegate-To

### 5.3.1 Background

The msDS-AllowedToDelegateTo attribute contains a list of Service Principal Names that are used to configure services so they can obtain Kerberos Tickets used for “Constrained Delegation” for the targeted account.

### 5.3.2 Modifying the Attribute (Attack)

For this particular attack/attribute modification, we will first create a second new machine account with PowerMad.

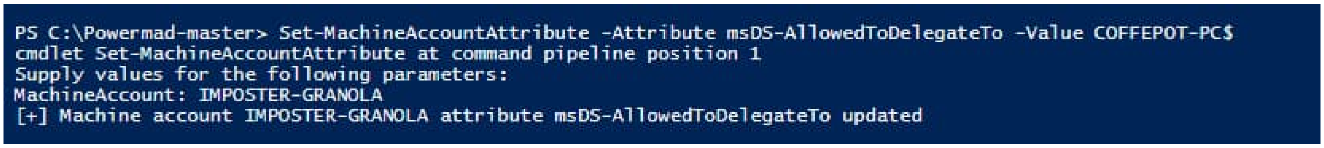


```
PS C:\Powermad-master> New-MachineAccount -MachineAccount COFFEPOT-PC
[+] Machine account COFFEPOT-PC added
```

Figure 14 - New Machine Account Creation

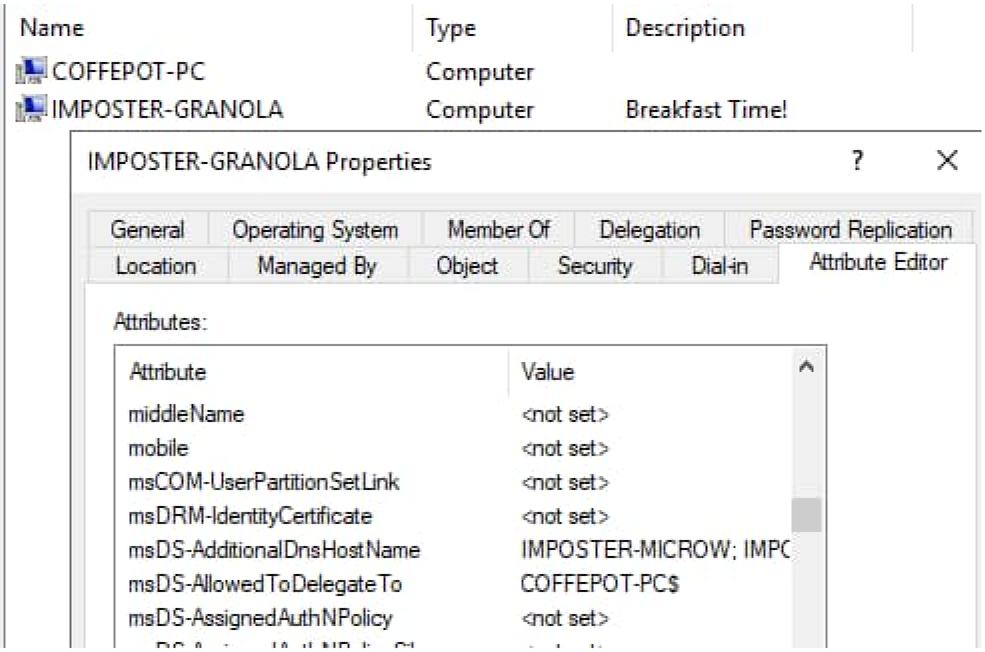
One thing to note with this attribute is that it cannot be modified unless the user making the change has the ***SeEnableDelegationPrivilege***. This article discusses the requirements in more detail and is an excellent read.

Because we are running these commands with a Domain Administrator account, I was able to modify the attribute.



```
PS C:\Powermad-master> Set-MachineAccountAttribute -Attribute msDS-AllowedToDelegateTo -Value COFFEPOT-PC$
cmdlet Set-MachineAccountAttribute at command pipeline position 1
Supply values for the following parameters:
MachineAccount: IMPOSTER-GRANOLA
[+] Machine account IMPOSTER-GRANOLA attribute msDS-AllowedToDelegateTo updated
```

Figure 15 - Modifying msDS-AllowedToDelegateTo Attribute



| Name | Type | Description |
|---|---|---|
| COFFEPOT-PC | Computer | |
| IMPOSTER-GRANOLA | Computer | Breakfast Time! |

IMPOSTER-GRANOLA Properties

Attributes:

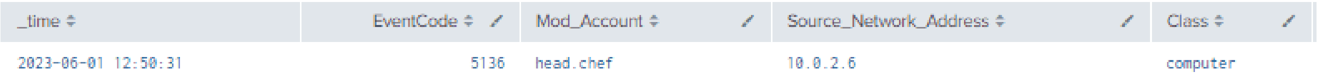
| Attribute | Value |
|---|---|
| middleName | <not set> |
| mobile | <not set> |
| msCOM-UserPartitionSetLink | <not set> |
| msDRM-IdentityCertificate | <not set> |
| msDS-AdditionalDnsHostName | IMPOSTER-MICROW; IMPC |
| msDS-AllowedToDelegateTo | COFFEPOT-PC$ |
| msDS-AssignedAuthNPolicy | <not set> |

Figure 16 - Attribute Post Modification

### 5.3.3 Building the Detections

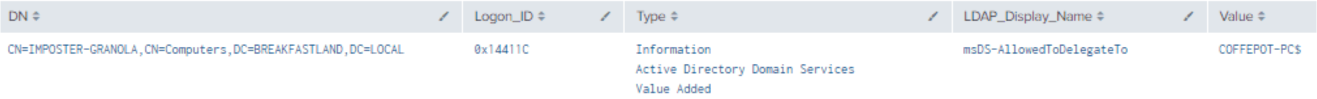
### 5.3.3.1 Detection With Event IDs 5136 and 4624

```
index=main ((EventCode=5136 AND LDAP_Display_Name=msDS-AllowedToDelegateTo)  OR
(EventCode=4624 AND Account_Name!="*$" AND Account_Name!="ANONYMOUS LOGON" AND
Account_Name!="SYSTEM"))
| eval Logon_ID=if(EventCode==4624,mvindex(Logon_ID,-1), mvindex(Logon_ID,-1))
| eval Mod_Account=if(EventCode==4624,mvindex(Account_Name,-1),
mvindex(Account_Name,-1))
| join type=outer Logon_ID
        [ search (EventCode=5136) OR (EventCode=4624)
        | stats count by Logon_ID, Account_Name, Source_Network_Address
        | table Account_Name,Logon_ID, Source_Network_Address]
| table _time, EventCode, Mod_Account, Source_Network_Address, Class, DN, Logon_ID,
Type, LDAP_Display_Name, Value
| where  len(Class)>0
```



| _time | EventCode | Mod_Account | Source_Network_Address | Class |
|---|---|---|---|---|
| 2023-06-01 12:50:31 | 5136 | head.chef | 10.0.2.6 | computer |

Figure 17 - Detection With Event IDs 5136 and 4624 (1)

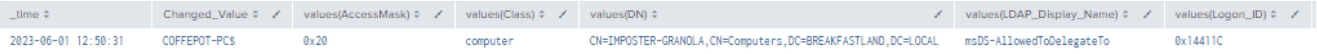


| DN | Logon_ID | Type | LDAP_Display_Name | Value |
|---|---|---|---|---|
| CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL | 0x14411C | Information<br>Active Directory Domain Services<br>Value Added | msDS-AllowedToDelegateTo | COFFEPOT-PC$ |

Figure 18 - Detection With Event IDs 5136 and 4624 (2)

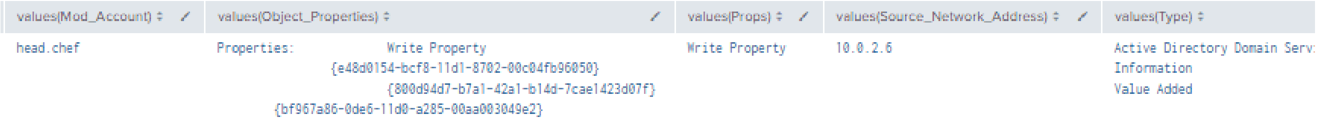
### 5.3.3.2 Detection With Event IDs 5136, 4624, and 4662

```
index=main ((EventCode=5136 AND LDAP_Display_Name=msDS-AllowedToDelegateTo)  OR
(EventCode=4624 AND Account_Name!="*$" AND Account_Name!="ANONYMOUS LOGON" AND
Account_Name!="SYSTEM") OR (EventCode=4662 AND Access_Mask=0x20))
| eval Logon_ID=if(EventCode==4624,mvindex(Logon_ID,-1), mvindex(Logon_ID,-1))
| eval Mod_Account=if(EventCode==4624,mvindex(Account_Name,-1),
mvindex(Account_Name,-1))
| eval Changed_Value=if(EventCode==5136,mvindex(Value,-1), mvindex(Value,-1))
| join type=outer Logon_ID
        [ search (EventCode=5136) OR (EventCode=4624)
        | stats count by Logon_ID, Account_Name, Source_Network_Address
        | table Account_Name,Logon_ID, Source_Network_Address ]
| join type=outer Logon_ID
    [ search index=main Account_Name!=*$  EventCode=4662 Access_Mask = 0x20
    | eval Props=Properties
    | eval AccessMask=Access_Mask
    | eval ObjectType=Object_Type
    | eval ObjectName=Object_Name
    | rex field=Message "(?<Object_Properties>(?ms)(?<=)Properties:(.*?)(?
=Additional\s+))"
    |table Account_Name,Logon_ID,Props,AccessMask,ObjectType, ObjectName,
Object_Properties]
| table _time, Mod_Account, Source_Network_Address , Class, DN, Logon_ID, Type,
LDAP_Display_Name, Changed_Value, AccessMask, Props, Object_Properties
| where  len(Class)>0
| stats values by _time, Changed_Value
```



| _time | Changed_Value | values(AccessMask) | values(Class) | values(DN) | values(LDAP_Display_Name) | values(Logon_ID) |
|---|---|---|---|---|---|---|
| 2023-06-01 12:50:31 | COFFEPOT-PC$ | 0x20 | computer | CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL | msDS-AllowedToDelegateTo | 0x14411C |

Figure 19 - Detection With Event IDs 5136, 4662, 4624 (1)

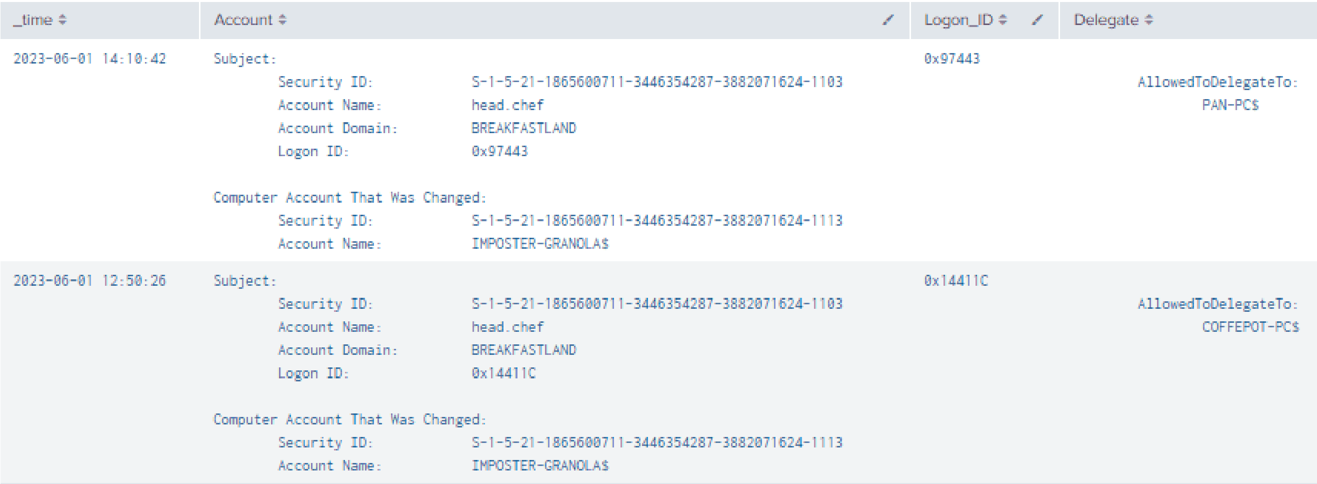


| values(Mod_Account) | values(Object_Properties) | values(Props) | values(Source_Network_Address) | values(Type) |
|---|---|---|---|---|
| head.chef | Properties: Write Property<br>{e48d0154-bcf8-11d1-8702-00c04fb96050}<br>{800d94d7-b7a1-42a1-b14d-7cae1423d07f}<br>{bf967a86-0de6-11d0-a285-00aa003049e2} | Write Property | 10.0.2.6 | Active Directory Domain Serv<br>Information<br>Value Added |

Figure 20 - Detection With Event IDs 5136, 4662, 4624 (2)

### 5.3.3.3 Detection With Event ID 4742

```
index=main EventCode=4742
| rex field=Message "(?<Account>(?
ms).........................................................................Account\
s+Name.*?(Account\s+Name:\s+)(\w+..........))"
| rex field=Message "(?<Delegate>(?ms)\s+AllowedToDelegateTo(.*).+?(?=Old\s+))"
| search Delegate!="*AllowedToDelegateTo: -*"
| table  _time, Account, Logon_ID, Delegate
```



| _time | Account | Logon_ID | Delegate |
|---|---|---|---|
| 2023-06-01 14:10:42 | Subject:<br>Security ID: S-1-5-21-1865600711-3446354287-3882071624-1103<br>Account Name: head.chef<br>Account Domain: BREAKFASTLAND<br>Logon ID: 0x97443<br><br>Computer Account That Was Changed:<br>Security ID: S-1-5-21-1865600711-3446354287-3882071624-1113<br>Account Name: IMPOSTER-GRANOLA$ | 0x97443 | AllowedToDelegateTo:<br>PAN-PC$ |
| 2023-06-01 12:50:26 | Subject:<br>Security ID: S-1-5-21-1865600711-3446354287-3882071624-1103<br>Account Name: head.chef<br>Account Domain: BREAKFASTLAND<br>Logon ID: 0x14411C<br><br>Computer Account That Was Changed:<br>Security ID: S-1-5-21-1865600711-3446354287-3882071624-1113<br>Account Name: IMPOSTER-GRANOLA$ | 0x14411C | AllowedToDelegateTo:<br>COFFEPOT-PC$ |

Figure 21 - Detection With Event ID 4742

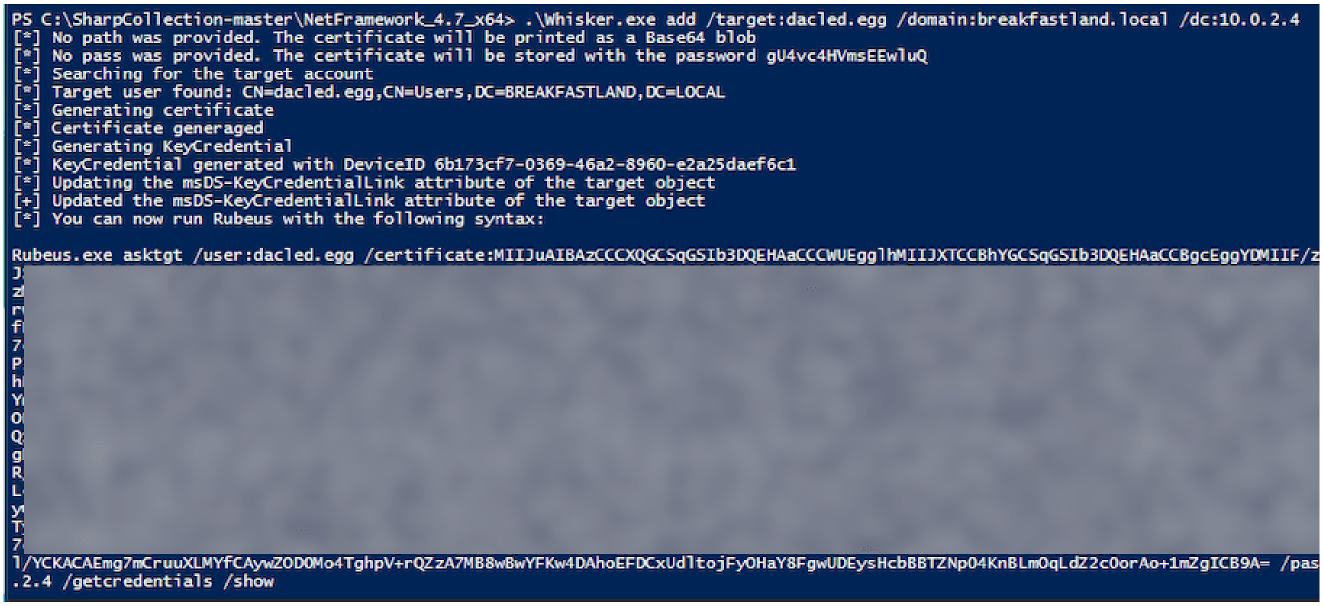
## 5.4 Shadow Credentials - Writing to msDS-Key-Credential-Link

### 5.4.1 Background

The msDS-KeyCredentialLink attribute can be used to store a key-based alternate set of credentials for a given user object—in this case, our victim account **dacled.egg**.

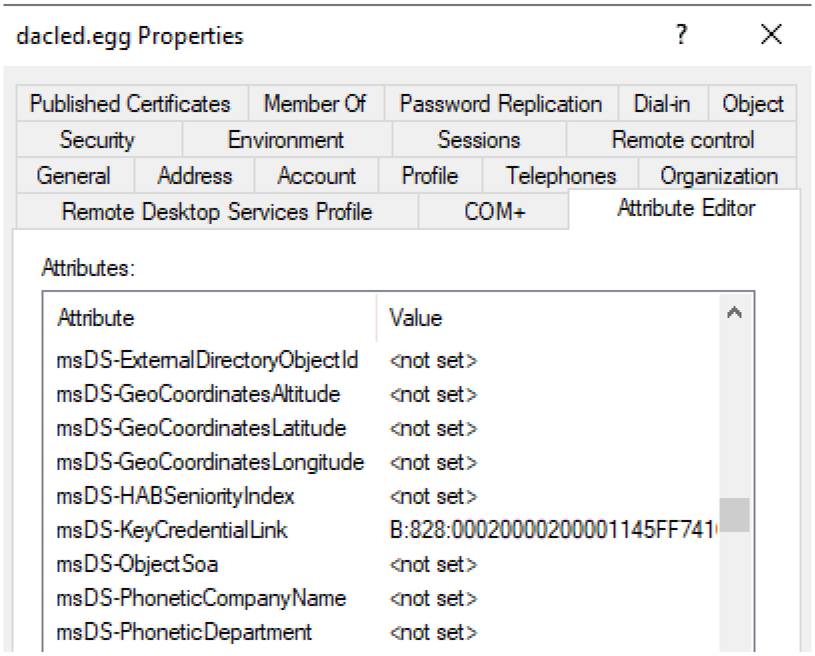
### 5.4.2 Modifying the Attribute (Attack)

To modify the **msDS-KeyCredentialLink**attribute, we will be primarily following the attack walkthrough here.



```
PS C:\SharpCollection-master\NetFramework_4.7_x64> .\Whisker.exe add /target:dacled.egg /domain:breakfastland.local /dc:10.0.2.4
[*] No path was provided. The certificate will be printed as a Base64 blob
[*] No pass was provided. The certificate will be stored with the password gU4vc4HVmsEEwluQ
[*] Searching for the target account
[*] Target user found: CN=dacled.egg,CN=Users,DC=BREAKFASTLAND,DC=LOCAL
[*] Generating certificate
[*] Certificate generaged
[*] Generating KeyCredential
[*] KeyCredential generated with DeviceID 6b173cf7-0369-46a2-8960-e2a25daef6c1
[*] Updating the msDS-KeyCredentialLink attribute of the target object
[+] Updated the msDS-KeyCredentialLink attribute of the target object
[*] You can now run Rubeus with the following syntax:

Rubeus.exe asktgt /user:dacled.egg /certificate:MIIJuAIBAzCCCXQGCSqGSIb3DQEHAaCCCWUEgglhMIIJXTCCBhYGCSqGSIb3DQEHAaCCBgcEggYDMIIF/z
[redacted]
1/YCKACAEmg7mCruuXLMYfCAywZODOMo4TghpV+rQZzA7MB8wBwYFKw4DAhoEFDCxUdltojFyOHaY8FgwUDEysHcbBBTZNpO4KnBLmOqLdZ2cOorAo+1mZgICB9A= /pas
.2.4 /getcredentials /show
```

Figure 22 - Executing Shadow Credentials Attack With Whisker



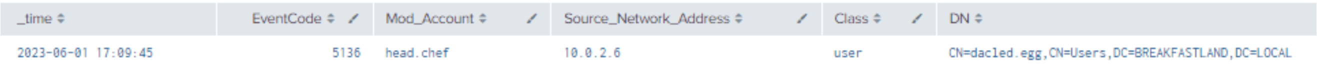
| Attribute | Value |
|---|---|
| msDS-ExternalDirectoryObjectId | <not set> |
| msDS-GeoCoordinatesAltitude | <not set> |
| msDS-GeoCoordinatesLatitude | <not set> |
| msDS-GeoCoordinatesLongitude | <not set> |
| msDS-HABSeniorityIndex | <not set> |
| msDS-KeyCredentialLink | B:828:00020000200001145FF741 |
| msDS-ObjectSoa | <not set> |
| msDS-PhoneticCompanyName | <not set> |
| msDS-PhoneticDepartment | <not set> |

Figure 23 - Change in Object Post Attack

## 5.4.3 Building the Detections

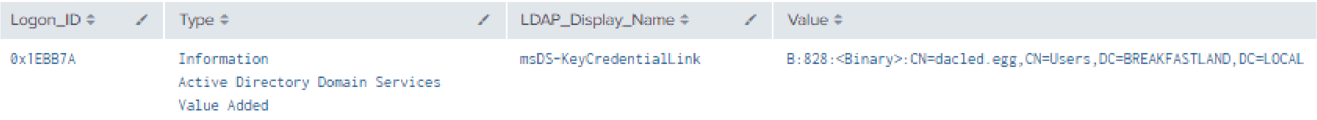
### 5.4.3.1 Detection With Event IDs 5136 and 4624

```
index=main ((EventCode=5136 AND LDAP_Display_Name=msDS-KeyCredentialLink)  OR
(EventCode=4624 AND Account_Name!="*$" AND Account_Name!="ANONYMOUS LOGON" AND
Account_Name!="SYSTEM"))
| eval Logon_ID=if(EventCode==4624,mvindex(Logon_ID,-1), mvindex(Logon_ID,-1))
| eval Mod_Account=if(EventCode==4624,mvindex(Account_Name,-1),
mvindex(Account_Name,-1))
| join type=outer Logon_ID
        [ search (EventCode=5136) OR (EventCode=4624)
        | stats count by Logon_ID, Account_Name, Source_Network_Address
        | table Account_Name,Logon_ID, Source_Network_Address]
| table _time, EventCode, Mod_Account, Source_Network_Address, Class, DN, Logon_ID,
Type, LDAP_Display_Name, Value
| where  len(Class)>0
```



| _time | EventCode | Mod_Account | Source_Network_Address | Class | DN |
|---|---|---|---|---|---|
| 2023-06-01 17:09:45 | 5136 | head.chef | 10.0.2.6 | user | CN=dacled.egg,CN=Users,DC=BREAKFASTLAND,DC=LOCAL |

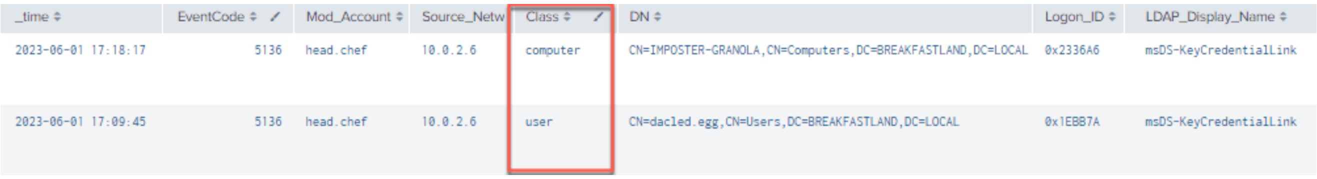
Figure 24 - Detection of Modification for msKeyCredentialLink (1)



| Logon_ID | Type | LDAP_Display_Name | Value |
|---|---|---|---|
| 0x1EBB7A | Information<br>Active Directory Domain Services<br>Value Added | msDS-KeyCredentialLink | B:828:<Binary>:CN=dacled.egg,CN=Users,DC=BREAKFASTLAND,DC=LOCAL |

Figure 25 - Detection of Modification for msKeyCredentialLink (2)

As a quick note, because we have not specified a class for this query—and for other queries—you do not need to write a separate query to pick up modifications to computer objects, as they will be picked up automatically.



| _time | EventCode | Mod_Account | Source_Netw | Class | DN | Logon_ID | LDAP_Display_Name |
|---|---|---|---|---|---|---|---|
| 2023-06-01 17:18:17 | 5136 | head.chef | 10.0.2.6 | computer | CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL | 0x2336A6 | msDS-KeyCredentialLink |
| 2023-06-01 17:09:45 | 5136 | head.chef | 10.0.2.6 | user | CN=dacled.egg,CN=Users,DC=BREAKFASTLAND,DC=LOCAL | 0x1EBB7A | msDS-KeyCredentialLink |

Figure 26 - msKeyCredentialLink Modification Showing Changes to User and Computer Objects

## 5.5 Logon Script (Script-Path)

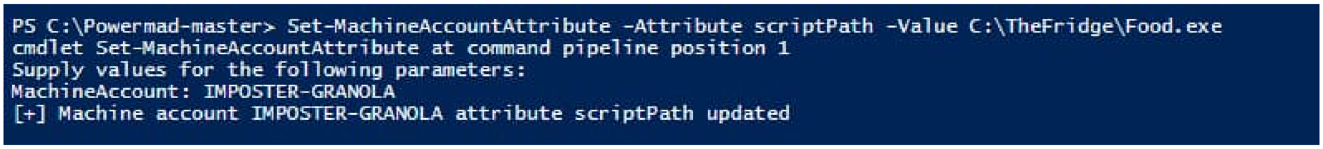
### 5.5.1 Background

The scriptPath attribute specifies the path designated for a user or computer object's logon script.

### 5.5.2 Modifying the Attribute (Attack)

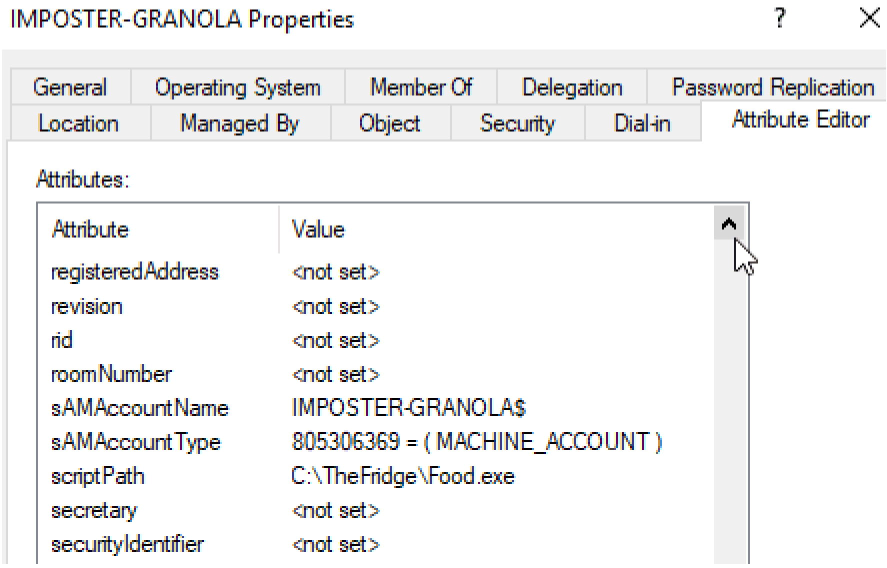
As previously, we will modify the ***scriptPath*** attribute with the following PowerMad Command:

```
Set-MachineAccountAttribute -Attribute scriptPath -Value ‘C:\TheFridge\Food.exe’
```



```
PS C:\Powermad-master> Set-MachineAccountAttribute -Attribute scriptPath -Value C:\TheFridge\Food.exe
cmdlet Set-MachineAccountAttribute at command pipeline position 1
Supply values for the following parameters:
MachineAccount: IMPOSTER-GRANOLA
[+] Machine account IMPOSTER-GRANOLA attribute scriptPath updated
```

Figure 27 - Modifying scriptPath Attribute



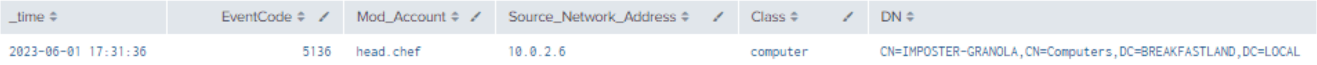
| Attribute | Value |
|---|---|
| registeredAddress | <not set> |
| revision | <not set> |
| rid | <not set> |
| roomNumber | <not set> |
| sAMAccountName | IMPOSTER-GRANOLA$ |
| sAMAccountType | 805306369 = ( MACHINE_ACCOUNT ) |
| scriptPath | C:\TheFridge\Food.exe |
| secretary | <not set> |
| securityIdentifier | <not set> |

Figure 28 - scriptPath Attribute Post Modification

### 5.5.3 Building the Detections

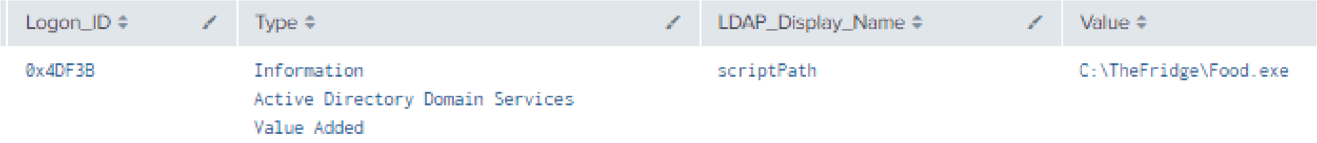
5.5.3.1 Detection with Event IDs 5136 and 4624

```
index=main ((EventCode=5136 AND LDAP_Display_Name=scriptPath)  OR (EventCode=4624 AND
Account_Name!="*$" AND Account_Name!="ANONYMOUS LOGON" AND Account_Name!="SYSTEM"))
| eval Logon_ID=if(EventCode==4624,mvindex(Logon_ID,-1), mvindex(Logon_ID,-1))
| eval Mod_Account=if(EventCode==4624,mvindex(Account_Name,-1),
mvindex(Account_Name,-1))
| join type=outer Logon_ID
        [ search (EventCode=5136) OR (EventCode=4624)
        | stats count by Logon_ID, Account_Name, Source_Network_Address
        | table Account_Name,Logon_ID, Source_Network_Address]
| table _time, EventCode, Mod_Account, Source_Network_Address, Class, DN, Logon_ID,
Type, LDAP_Display_Name, Value
| where  len(Class)>0
```



| _time | EventCode | Mod_Account | Source_Network_Address | Class | DN |
|---|---|---|---|---|---|
| 2023-06-01 17:31:36 | 5136 | head.chef | 10.0.2.6 | computer | CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL |

Figure 29 - Detection With Event IDs 5136 and 4624 (1)

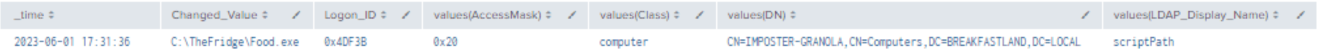


| Logon_ID | Type | LDAP_Display_Name | Value |
|---|---|---|---|
| 0x4DF3B | Information<br>Active Directory Domain Services<br>Value Added | scriptPath | C:\TheFridge\Food.exe |

Figure 30 - Detection With Event IDs 5136 and 4624 (2)

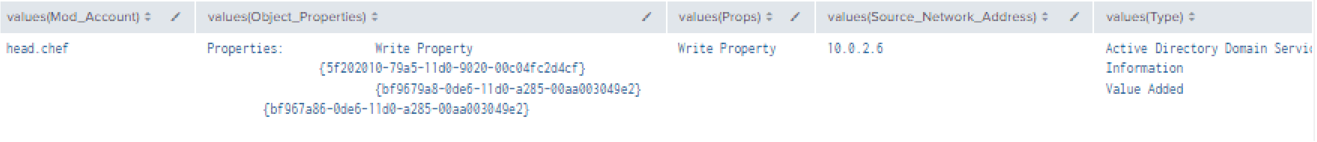
5.5.3.2 Detection With Event IDs 5136, 4624, and 4662

```
index=main ((EventCode=5136 AND LDAP_Display_Name=scriptPath)  OR (EventCode=4624 AND
Account_Name!="*$" AND Account_Name!="ANONYMOUS LOGON" AND Account_Name!="SYSTEM") OR
(EventCode=4662 AND Access_Mask=0x20))
| eval Logon_ID=if(EventCode==4624,mvindex(Logon_ID,-1), mvindex(Logon_ID,-1))
| eval Mod_Account=if(EventCode==4624,mvindex(Account_Name,-1),
mvindex(Account_Name,-1))
| eval Changed_Value=if(EventCode==5136,mvindex(Value,-1), mvindex(Value,-1))
| join type=outer Logon_ID
        [ search (EventCode=5136) OR (EventCode=4624)
        | stats count by Logon_ID, Account_Name, Source_Network_Address
        | table Account_Name,Logon_ID, Source_Network_Address ]
| join type=outer Logon_ID
    [ search index=main Account_Name!=*$  EventCode=4662 Access_Mask = 0x20
    | eval Props=Properties
    | eval AccessMask=Access_Mask
    | eval ObjectType=Object_Type
    | eval ObjectName=Object_Name
    | rex field=Message "(?<Object_Properties>(?ms)(?<=)Properties:(.*?)(?
=Additional\s+))"
    |table Account_Name,Logon_ID,Props,AccessMask,ObjectType, ObjectName,
Object_Properties]
| table _time, Mod_Account, Source_Network_Address , Class, DN, Logon_ID, Type,
LDAP_Display_Name, Changed_Value, AccessMask, Props, Object_Properties
| where  len(Class)>0
| stats values by _time, Changed_Value, Logon_ID
```



| _time | Changed_Value | Logon_ID | values(AccessMask) | values(Class) | values(DN) | values(LDAP_Display_Name) |
|---|---|---|---|---|---|---|
| 2023-06-01 17:31:36 | C:\TheFridge\Food.exe | 0x4DF3B | 0x20 | computer | CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL | scriptPath |

Figure 31 - Detection With Event IDs 5136, 4662, 4624 (1)

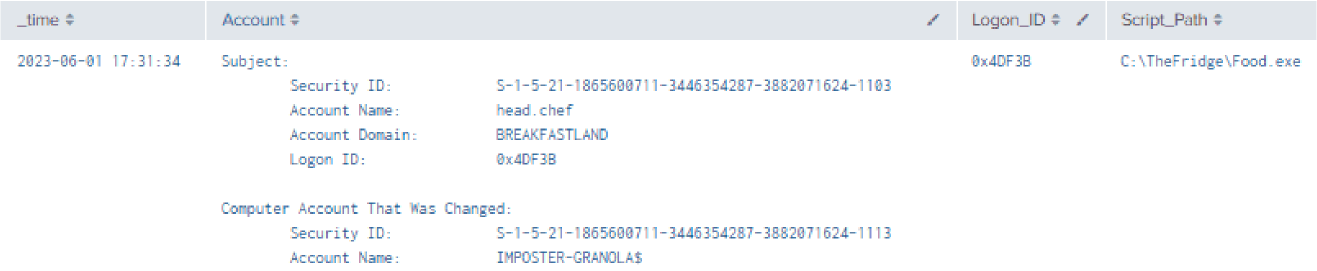


| values(Mod_Account) | values(Object_Properties) | values(Props) | values(Source_Network_Address) | values(Type) |
|---|---|---|---|---|
| head.chef | Properties:            Write Property<br>{5f202010-79a5-11d0-9020-00c04fc2d4cf}<br>{bf9679a8-0de6-11d0-a285-00aa003049e2}<br>{bf967a86-0de6-11d0-a285-00aa003049e2} | Write Property | 10.0.2.6 | Active Directory Domain Servi<br>Information<br>Value Added |

Figure 32 - Detection With Event IDs 5136, 4662, 4624 (2)

### 5.5.3.3 Detection with Event ID 4742

```
index=main EventCode=4742 Script_Path!="*-*"
| rex field=Message "(?<Account>(?
ms)...........................................................................Account\
s+Name.*?(Account\s+Name:\s+)(\w+..........))"
| table  _time, Account, Logon_ID, Script_Path
```



| _time | Account | Logon_ID | Script_Path |
|---|---|---|---|
| 2023-06-01 17:31:34 | Subject:<br>Security ID: S-1-5-21-1865600711-3446354287-3882071624-1103<br>Account Name: head.chef<br>Account Domain: BREAKFASTLAND<br>Logon ID: 0x4DF3B<br><br>Computer Account That Was Changed:<br>Security ID: S-1-5-21-1865600711-3446354287-3882071624-1113<br>Account Name: IMPOSTER-GRANOLA$ | 0x4DF3B | C:\TheFridge\Food.exe |

Figure 33 - Detection With Event ID 4742

## 5.6 ms-TS-Inital-Program

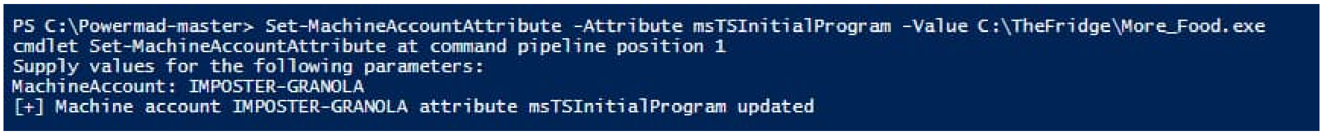
### 5.6.1 Background

The msTSInitialProgram attribute stores data for applications that should be started upon initial logon. This information will include the path and file name of the application(s).

### 5.6.2 Modifying the Attribute (Attack)

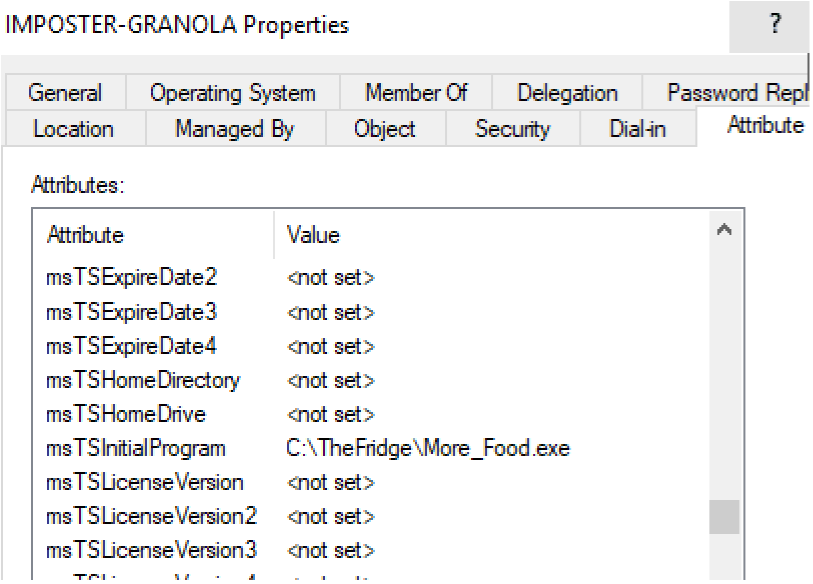
As previously, we will modify the ***msTSInitialProgram*** attribute with the following PowerMad Command:

```
Set-MachineAccountAttribute -Attribute msTSInitialProgram -Value
‘C:\TheFridge\More_Food.exe’
```



```
PS C:\Powermad-master> Set-MachineAccountAttribute -Attribute msTSInitialProgram -Value C:\TheFridge\More_Food.exe
cmdlet Set-MachineAccountAttribute at command pipeline position 1
Supply values for the following parameters:
MachineAccount: IMPOSTER-GRANOLA
[+] Machine account IMPOSTER-GRANOLA attribute msTSInitialProgram updated
```

Figure 34 - Modifying msTSInitialProgram



Attributes:

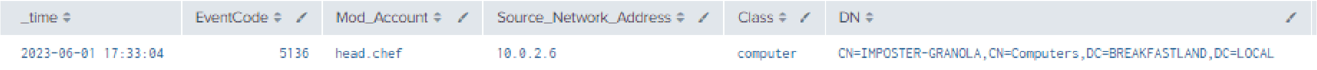
| Attribute | Value |
|---|---|
| msTSExpireDate2 | <not set> |
| msTSExpireDate3 | <not set> |
| msTSExpireDate4 | <not set> |
| msTSHomeDirectory | <not set> |
| msTSHomeDrive | <not set> |
| msTSInitialProgram | C:\TheFridge\More_Food.exe |
| msTSLicenseVersion | <not set> |
| msTSLicenseVersion2 | <not set> |
| msTSLicenseVersion3 | <not set> |

Figure 35 - msTSInitialProgram Post Modification

### 5.6.3 Building the Detections

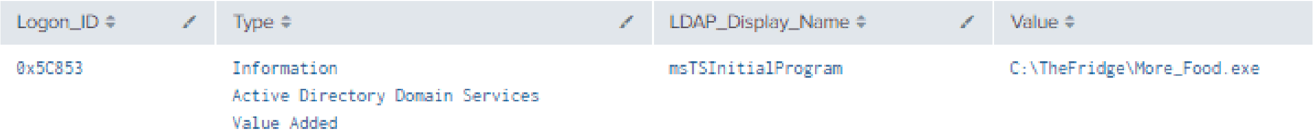
#### 5.6.3.1 Detection With Event IDs 5136 and 4624

```
index=main ((EventCode=5136 AND LDAP_Display_Name=msTSInitialProgram)  OR
(EventCode=4624 AND Account_Name!="*$" AND Account_Name!="ANONYMOUS LOGON" AND
Account_Name!="SYSTEM"))
| eval Logon_ID=if(EventCode==4624,mvindex(Logon_ID,-1), mvindex(Logon_ID,-1))
| eval Mod_Account=if(EventCode==4624,mvindex(Account_Name,-1),
mvindex(Account_Name,-1))
| join type=outer Logon_ID
        [ search (EventCode=5136) OR (EventCode=4624)
        | stats count by Logon_ID, Account_Name, Source_Network_Address
        | table Account_Name,Logon_ID, Source_Network_Address]
| table _time, EventCode, Mod_Account, Source_Network_Address, Class, DN, Logon_ID,
Type, LDAP_Display_Name, Value
| where  len(Class)>0
```



| _time | EventCode | Mod_Account | Source_Network_Address | Class | DN |
|---|---|---|---|---|---|
| 2023-06-01 17:33:04 | 5136 | head.chef | 10.0.2.6 | computer | CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL |

Figure 36 - Detection With Event IDs 5136 and 4624 (1)

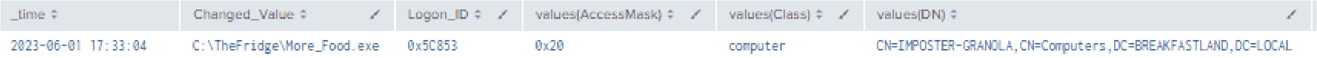


| Logon_ID | Type | LDAP_Display_Name | Value |
|---|---|---|---|
| 0x5C853 | Information<br>Active Directory Domain Services<br>Value Added | msTSInitialProgram | C:\TheFridge\More_Food.exe |

Figure 37 - Detection With Event IDs 5136 and 4624 (2)

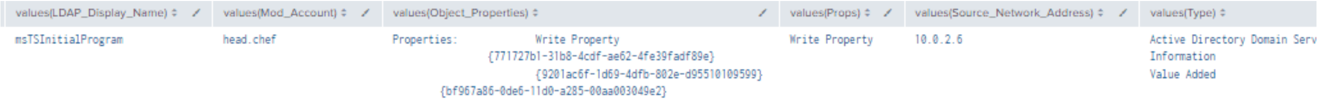
#### 5.6.3.2 Detection With Event IDs 5136, 4624, and 4662

```
index=main ((EventCode=5136 AND LDAP_Display_Name=msTSInitialProgram)  OR
(EventCode=4624 AND Account_Name!="*$" AND Account_Name!="ANONYMOUS LOGON" AND
Account_Name!="SYSTEM") OR (EventCode=4662 AND Access_Mask=0x20))
| eval Logon_ID=if(EventCode==4624,mvindex(Logon_ID,-1), mvindex(Logon_ID,-1))
| eval Mod_Account=if(EventCode==4624,mvindex(Account_Name,-1),
mvindex(Account_Name,-1))
| eval Changed_Value=if(EventCode==5136,mvindex(Value,-1), mvindex(Value,-1))
| join type=outer Logon_ID
        [ search (EventCode=5136) OR (EventCode=4624)
        | stats count by Logon_ID, Account_Name, Source_Network_Address
        | table Account_Name,Logon_ID, Source_Network_Address ]
| join type=outer Logon_ID
    [ search index=main Account_Name!=*$  EventCode=4662 Access_Mask = 0x20
    | eval Props=Properties
    | eval AccessMask=Access_Mask
    | eval ObjectType=Object_Type
    | eval ObjectName=Object_Name
    | rex field=Message "(?<Object_Properties>(?ms)(?<=)Properties:(.*?)(?
=Additional\s+))"
    |table Account_Name,Logon_ID,Props,AccessMask,ObjectType, ObjectName,
Object_Properties]
| table _time, Mod_Account, Source_Network_Address , Class, DN, Logon_ID, Type,
LDAP_Display_Name, Changed_Value, AccessMask, Props, Object_Properties
| where  len(Class)>0
| stats values by _time, Changed_Value, Logon_ID
```



| _time | Changed_Value | Logon_ID | values(AccessMask) | values(Class) | values(DN) |
|---|---|---|---|---|---|
| 2023-06-01 17:33:04 | C:\TheFridge\More_Food.exe | 0x5C853 | 0x20 | computer | CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL |

Figure 38 - Detection With Event IDs 5136, 4662, 4624 (1)



| values(LDAP_Display_Name) | values(Mod_Account) | values(Object_Properties) | values(Props) | values(Source_Network_Address) | values(Type) |
|---|---|---|---|---|---|
| msTSInitialProgram | head.chef | Properties: Write Property<br>{771727b1-31b8-4cdf-ae62-4fe39fadf89e}<br>{9201ac6f-1d69-4dfb-802e-d95510109599}<br>{bf967a86-0de6-11d0-a285-00aa003049e2} | Write Property | 10.0.2.6 | Active Directory Domain Serv<br>Information<br>Value Added |

Figure 39 - Detection With Event IDs 5136, 4662, 4624 (2)

## 5.7 GPO Abuse - Group-Policy-Container Class

### 5.7.1 Background

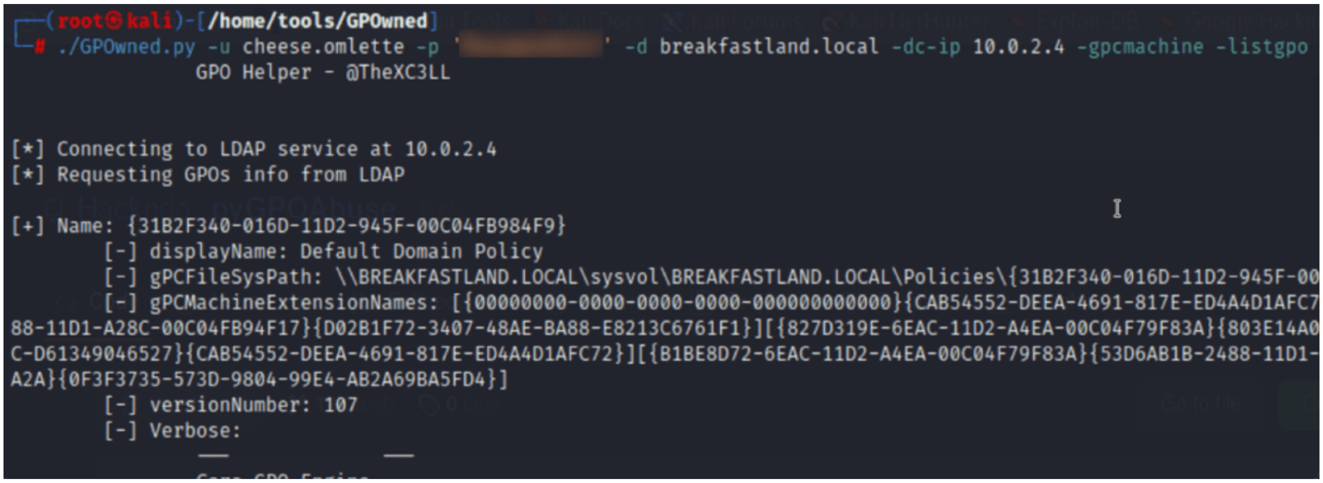
groupPolicyContainer is an AD Schema class that is modified when a GPO is updated through the Group Policy Editor. While modifying GPOs is a normal administrative task, it can also be abused by attackers who may use scheduled tasks or other GPO features to establish persistence or move laterally through the network.

### 5.7.2 Modifying the Attribute (Attack)

While GPO can be modified through the GUI, we are going to leverage the tools mentioned in the Hacker Recipes to remotely modify a GPO from a machine connected to the network.

Using GPOwned.py, we first need to procure the “unique ID/Name” of the GPO we are going to be attacking. The syntax is simple:

```
python3 GPOwned.py -u cheese.omlette -p password -d breakfastland.local -dc-ip
10.0.2.4 -gpcmachine -listhpo
```

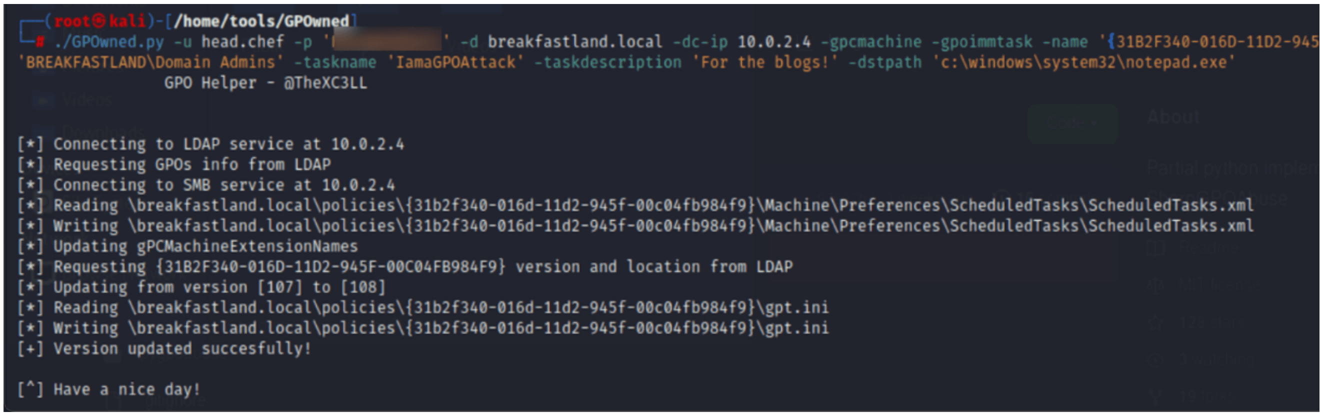


```
┌──(root㉿kali)-[/home/tools/GPOwned]
└─# ./GPOwned.py -u cheese.omlette -p '[redacted]' -d breakfastland.local -dc-ip 10.0.2.4 -gpcmachine -listgpo
                GPO Helper - @TheXC3LL


[*] Connecting to LDAP service at 10.0.2.4
[*] Requesting GPOs info from LDAP

[+] Name: {31B2F340-016D-11D2-945F-00C04FB984F9}
        [-] displayName: Default Domain Policy
        [-] gPCFileSysPath: \\BREAKFASTLAND.LOCAL\sysvol\BREAKFASTLAND.LOCAL\Policies\{31B2F340-016D-11D2-945F-00
        [-] gPCMachineExtensionNames: [{00000000-0000-0000-0000-000000000000}{CAB54552-DEEA-4691-817E-ED4A4D1AFC7
88-11D1-A28C-00C04FB94F17}{D02B1F72-3407-48AE-BA88-E8213C6761F1}][{827D319E-6EAC-11D2-A4EA-00C04F79F83A}{803E14A0
C-D61349046527}{CAB54552-DEEA-4691-817E-ED4A4D1AFC72}][{B1BE8D72-6EAC-11D2-A4EA-00C04F79F83A}{53D6AB1B-2488-11D1-
A2A}{0F3F3735-573D-9804-99E4-AB2A69BA5FD4}]
        [-] versionNumber: 107
        [-] Verbose:
```

Figure 40 - GPOwned Output

Once you’ve enumerated a list of GPOs on the domain, you can identify the “Name” —in our case the Default Domain Policy GPO— of the GPO you wish to modify, and then you can run the following command:

```
python3 GPOwned.py -u head.chef -p <password> -d breakfastland.local -dc-ip 10.0.2.4
-gpcmachine -gpoimmtask -name '{31B2F340-016D-11D2-945F-00C04FB98}' -author
'BREAKFASTLAND\Domain Admins' -taskname 'ImaGPOAttack' -taskdescription 'For the
blogs!' -dstpath 'c:\windows\system32\notepad.exe'
```



```
┌──(root㉿kali)-[/home/tools/GPOwned]
└─# ./GPOwned.py -u head.chef -p '[redacted]' -d breakfastland.local -dc-ip 10.0.2.4 -gpcmachine -gpoimmtask -name '{31B2F340-016D-11D2-945
'BREAKFASTLAND\Domain Admins' -taskname 'IamaGPOAttack' -taskdescription 'For the blogs!' -dstpath 'c:\windows\system32\notepad.exe'
                GPO Helper - @TheXC3LL


[*] Connecting to LDAP service at 10.0.2.4
[*] Requesting GPOs info from LDAP
[*] Connecting to SMB service at 10.0.2.4
[*] Reading \breakfastland.local\policies\{31b2f340-016d-11d2-945f-00c04fb984f9}\Machine\Preferences\ScheduledTasks\ScheduledTasks.xml
[*] Writing \breakfastland.local\policies\{31b2f340-016d-11d2-945f-00c04fb984f9}\Machine\Preferences\ScheduledTasks\ScheduledTasks.xml
[*] Updating gPCMachineExtensionNames
[*] Requesting {31B2F340-016D-11D2-945F-00C04FB984F9} version and location from LDAP
[*] Updating from version [107] to [108]
[*] Reading \breakfastland.local\policies\{31b2f340-016d-11d2-945f-00c04fb984f9}\gpt.ini
[*] Writing \breakfastland.local\policies\{31b2f340-016d-11d2-945f-00c04fb984f9}\gpt.ini
[+] Version updated succesfully!

[^] Have a nice day!
```

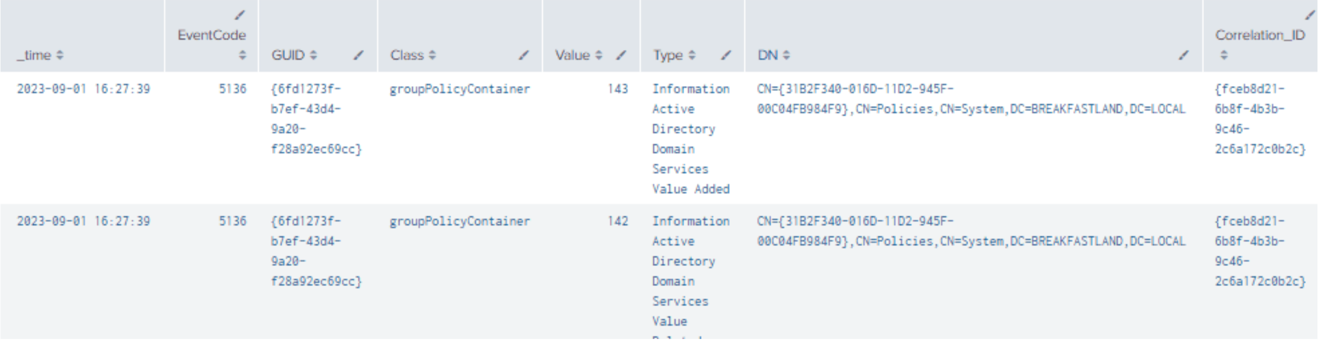
Figure 41 - GPOwned GPO Modification

*Note: This attack was run originally as a non-privileged user and was not successful. It was successful as a privileged user. Second, the author of this script notes that it can be a bit buggy and should be used with precaution in production environments. Specifically, the bug we encountered was that the script would not pick up or drop GPOs that were new or deleted. Thus, keep in mind that there may be removed GPOs that are listed but no longer exist.*

### 5.7.3 Building the Detections

At a very basic level, we can detect changes to the ***groupPolicyContainer*** "class" using Event ID 5136, as we have done with the majority of our previously built detections.

```
index=main EventCode=5136 Class=groupPolicyContainer
|table _time, EventCode, GUID, Class, Value, Type, DN, Correlation_ID
```



| _time | EventCode | GUID | Class | Value | Type | DN | Correlation_ID |
|---|---|---|---|---|---|---|---|
| 2023-09-01 16:27:39 | 5136 | {6fd1273f-b7ef-43d4-9a20-f28a92ec69cc} | groupPolicyContainer | 143 | Information Active Directory Domain Services Value Added | CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=BREAKFASTLAND,DC=LOCAL | {fceb8d21-6b8f-4b3b-9c46-2c6a172c0b2c} |
| 2023-09-01 16:27:39 | 5136 | {6fd1273f-b7ef-43d4-9a20-f28a92ec69cc} | groupPolicyContainer | 142 | Information Active Directory Domain Services Value | CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=BREAKFASTLAND,DC=LOCAL | {fceb8d21-6b8f-4b3b-9c46-2c6a172c0b2c} |

Figure 42 - Basic Query to Detect Changes to groupPolicyContainer

However, here we begin to run into some challenges with the limitations of Event ID 5136—namely, that while we can see evidence that the Group Policy GUID targeted in our attack was changed, we cannot see what exactly was changed or where it was changed from.

Given the breadth of function within GPO, this is critical to know in order to facilitate timely incident response and to assist analysts by adequately communicating information needs to AD/GPO Administrators.

To get the information we need, such a source IP address of the attacking host, as well as the change that was actually made to the GPO, we need to leverage Event ID 5145 and Event ID 4662.

*Note: See the "Windows Events" section under "Logging Setup" within this blog for specifics on how to enable this logging.*

In this case, the two (2) added events provide us with the following telemetry:

Event ID 5145:

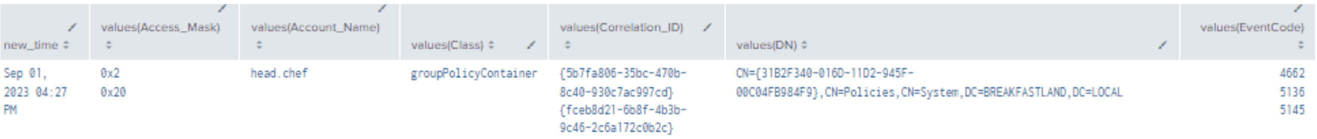
- The Relative Target Name contained within this Event ID provides us with additional specifics on the actual network share/file/object accessed within our targeted GPO.
- Provides a source IP address

Event ID 4662:

- Gives additional contextual data about the object/class/attributes involved
- Can be omitted if telemetry from Event IDs 5136 and 5145 is sufficient for organizational needs

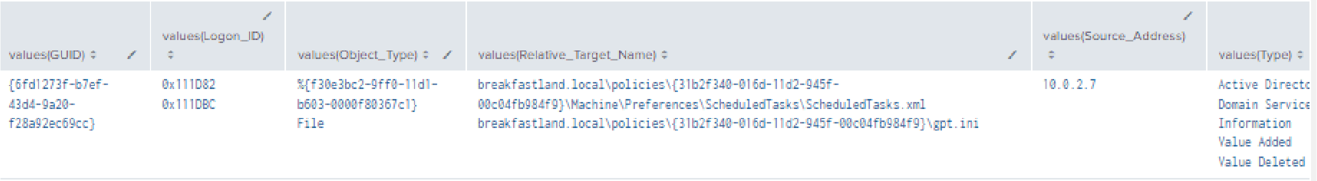
5.7.3.1 Detection With Event IDs 5136, 5145, and 4662

```
index=main ((EventCode=5136 AND  Class=groupPolicyContainer AND (Type="Value Added"
OR Type="Value Deleted"))  OR (EventCode=5145 AND Accesses="WriteData (or AddFile)")
OR (EventCode=4662 AND Access_Mask=0x20 AND Object_Type="%{f30e3bc2-9ff0-11d1-b603-
0000f80367c1}"))
| eval new_time =strftime(_time, "%b %d, %Y %I:%M %p")
| table  new_time, Source_Address, Logon_ID, Account_Name, EventCode, GUID, DN,
Correlation_ID, Type, Relative_Target_Name, Access_Mask, Object_Type, Class
| stats values by new_time
|sort by new_time
```



| new_time | values(Access_Mask) | values(Account_Name) | values(Class) | values(Correlation_ID) | values(DN) | values(EventCode) |
|---|---|---|---|---|---|---|
| Sep 01, 2023 04:27 PM | 0x2<br>0x20 | head.chef | groupPolicyContainer | {5b7fa806-35bc-470b-8c40-930c7ac997cd}<br>{fceb8d21-6b8f-4b3b-9c46-2c6a172c0b2c} | CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=BREAKFASTLAND,DC=LOCAL | 4662<br>5136<br>5145 |

Figure 43 - Detecting Modifications to groupPolicyContainer Object Complex (1)



| values(GUID) | values(Logon_ID) | values(Object_Type) | values(Relative_Target_Name) | values(Source_Address) | values(Type) |
|---|---|---|---|---|---|
| {6fd1273f-b7ef-43d4-9a20-f28a92ec69cc} | 0x111D82<br>0x111DBC | %{f30e3bc2-9ff0-11d1-b603-0000f80367c1}<br>File | breakfastland.local\policies\{31b2f340-016d-11d2-945f-00c04fb984f9}\Machine\Preferences\ScheduledTasks\ScheduledTasks.xml<br>breakfastland.local\policies\{31b2f340-016d-11d2-945f-00c04fb984f9}\gpt.ini | 10.0.2.7 | Active Directo<br>Domain Service<br>Information<br>Value Added<br>Value Deleted |

Figure 44 - Detecting Modifications to groupPolicyContainer Object Complex (2)

## 6 Conclusion of Part 1A

Due to the length, this post has been split into two sections (Part 1A and Part 1B). Please see this link for a total PDF version of Part 1.

Lastly, this blog would not have been possible without help from the following people:

Charlie Bromberg (@_nwodtuhs)

Jonathan Johnson (@jsecurity101)

Jim Sykora (@jimsycurity)

Kelsey Segrue (@KelseySegrue)

## 7 References:

https://www.thehacker.recipes/ad/movement/dacl

**Windows Events:**

https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4662

https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4624

https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-5145

https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4742

https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4738

**msDS-AllowedtoActOnBehalfOfOtherIdentity:**

https://learn.microsoft.com/en-us/windows/win32/adschema/a-msds-allowedtoactonbehalfofotheridentity

https://jsecurity101.medium.com/defending-the-three-headed-relay-17e1d6b6a339

**Service Principal Name (SPN):**

https://learn.microsoft.com/en-us/windows/win32/ad/service-principal-names

https://www.semperis.com/blog/spn-jacking-an-edge-case-in-writespn-abuse/
https://blog.harmj0y.net/activedirectory/targeted-kerberoasting/

https://learn.microsoft.com/en-us/windows/win32/ad/mutual-authentication-using-kerberos

https://github.com/fortra/impacket

https://github.com/fortra/impacket/blob/master/examples/GetUserSPNs.py

https://github.com/Kevin-Robertson/Powermad

**msDS-AllowedtoDelegateTo:**

https://learn.microsoft.com/en-us/windows/win32/adschema/a-msds-allowedtodelegateto

https://skyblue.team/posts/delegate-krbtgt/

https://csandker.io/2020/02/10/KerberosDelegationAWrapUp.html

**msDS-KeyCredentialLink:**

https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-ada2/45916e5b-d66f-444e-b1e5-5b0666ed4d66

https://posts.specterops.io/shadow-credentials-abusing-key-trust-account-mapping-for-takeover-8ee1a53566ab

https://cyberstoph.org/posts/2022/03/detecting-shadow-credentials/

**ScriptPath:**

https://learn.microsoft.com/en-us/windows/win32/adschema/a-scriptpath

**msTSInitalProgram:**

https://learn.microsoft.com/en-us/windows/win32/adschema/a-mstsinitialprogram

**GPO:**

https://learn.microsoft.com/en-us/windows/win32/adschema/c-grouppolicycontainer

https://github.com/Hackndo/pyGPOAbuse

https://github.com/X-C3LL/GPOwned

https://www.thehacker.recipes/ad/movement/group-policies

https://learn.microsoft.com/en-us/windows/win32/adschema/c-grouppolicycontainer

https://wald0.com/?p=179

https://serverfault.com/questions/692772/group-managed-service-accounts-principalsallowedtoretrievemanagedpassword

https://serverfault.com/questions/692772/group-managed-service-accounts-principalsallowedtoretrievemanagedpassword

https://labs.withsecure.com/tools/sharpgpoabuse

**AddMember:**

https://www.thehacker.recipes/ad/movement/dacl/addmember

https://github.com/PowerShellMafia/PowerSploit

https://learn.microsoft.com/en-us/windows/win32/adschema/r-self-membership

https://learn.microsoft.com/en-us/windows/win32/adschema/a-member

**ForceChangePassword:**

https://www.thehacker.recipes/ad/movement/dacl/forcechangepassword

https://learn.microsoft.com/en-us/windows/win32/adschema/r-user-force-change-password

**GrantOwnerShip:**

https://www.thehacker.recipes/ad/movement/dacl/grant-ownership

**LAPS/GMSA:**

https://www.trustedsec.com/blog/splunk-spl-queries-for-detecting-gmsa-attacks/

https://www.trustedsec.com/blog/a-lapse-in-judgement/

https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-ada2/60acc5e9-e6dc-481f-a3ff-2cb763ab2d33

https://learn.microsoft.com/en-us/powerquery-m/datetime-fromfiletime

https://adsecurity.org/?p=4367

https://learn.microsoft.com/en-us/powershell/module/activedirectory/?view=windowsserver2022-ps

**DCSync:**

https://github.com/fortra/impacket

https://www.alteredsecurity.com/post/a-primer-on-dcsync-attack-and-detection

https://www.thehacker.recipes/ad/movement/credentials/dumping/dcsync

https://itconnect.uw.edu/tools-services-support/it-systems-infrastructure/msinf/other-help/understanding-sddl-syntax/

**msDS-GroupManagedServiceAccount/msDS-ManagedServiceAccount References:**

https://woshub.com/group-managed-service-accounts-in-windows-server-2012/

https://blog.netwrix.com/2022/10/13/group-managed-service-accounts-gmsa/

**PowerMad/Set-MachineAcccountAttribute:**

https://github.com/Kevin-Robertson/Powermad https://stackoverflow.com/questions/39226518/filtering-only-second-account-name-in-windows-event-log-using-a-regex

https://learn.microsoft.com/en-us/troubleshoot/windows-server/identity/useraccountcontrol-manipulate-account-properties

https://skyblue.team/posts/delegate-krbtgt/

**Other:**

An ACE in the Hole Stealthy Host Persistence via Security Descriptors [Corrected Audio]

https://specterops.io/wp-content/uploads/sites/3/2022/06/an_ace_up_the_sleeve.pdf