



**OUned**

**L'exploitation des Unités**

**Organisationnelles en environnement Active Directory**

**BARBHACK 2024**

**31/08/2024**

- Pentester @ Synacktiv depuis avril 2022
- Recherches Active Directory entre les missions
- Focus sur les Group Policy Objects



**Quentin Roland**

Pentester

# Introduction

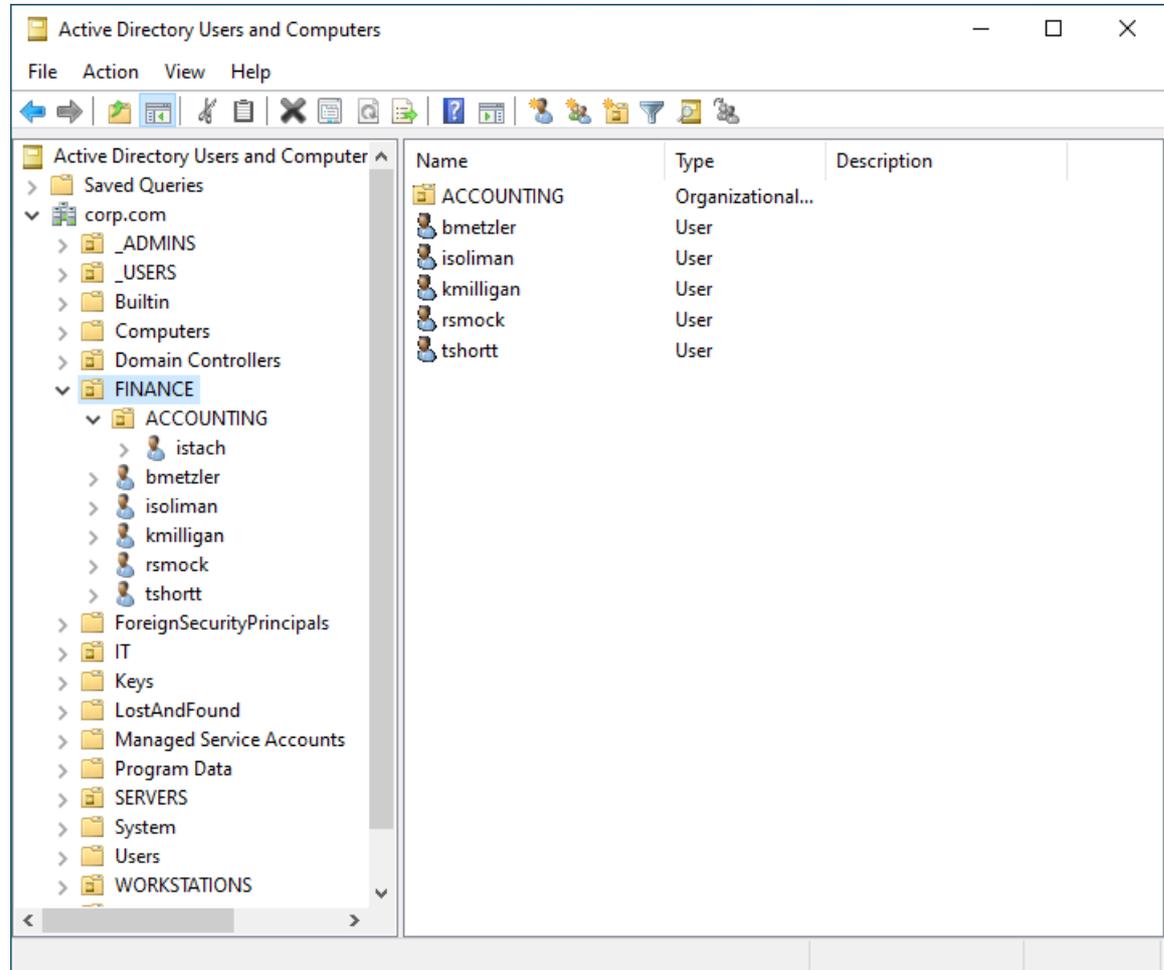
- **Vecteurs d'attaque portant sur les OUs relativement peu connus**
- **Découverte d'ACLs exploitables non-reportées par BloodHound, création d'un outil OUned.py**
- **Plus largement, la recherche de vecteurs d'attaque basés sur les permissions AD n'est probablement pas épuisée**

- **Unités Organisationnelles : définitions et ACLs**
- **Compromission d'OUs via héritage d'ACL : exploitation et limites**
- **Un vecteur d'attaque alternatif : empoisonnement de l'attribut gPLink**
- **Démonstration d'exploitation par OUned.py & vidéo**

# Unités Organisationnelles : définitions et ACLs

# Unités Organisationnelles : définitions et ACLs

*OUs : conteneurs logiques  
organisant les objets Active  
Directory en sous-ensembles*



# Unités Organisationnelles : définitions et ACLs

*Les OUs sont utilisées pour appliquer des configurations à des ensembles spécifiques d'objets Active Directory via GPO*

The screenshot shows the Group Policy Management console. On the left, the tree view shows the hierarchy: Forest: corp.com > Domains > corp.com > FINANCE. The right pane is titled 'FINANCE' and shows the 'Linked Group Policy Objects' tab. It contains a table with the following data:

Link Order	GPO	Enforced	Link Enabled	GPO Status
1	USER_HARDENING_ANY	No	Yes	Enabled
2	Empty	No	Yes	Enabled

- **Attribution de permissions sur les Unités Organisationnelles :**
  - Volontaire (permettre à un utilisateur de configurer des groupes d'objets via GPO).
  - Involontaire
- **ACLs régulières et intéressantes :**
  - GenericAll
  - GenericWrite
  - Manage Group Policy Links

# Unités Organisationnelles : définitions et ACLs

SERVERS Properties

General Managed By Object **Security** COM+ Attribute Editor

Group or user names:

- CREATOR OWNER
- SELF
- Authenticated Users
- SYSTEM
- Domain Admins (CORP\Domain Admins)
- Enterprise Admins (CORP\Enterprise Admins)

Permissions for CREATOR OWNER

	Allow	Deny
Full control	<input type="checkbox"/>	<input type="checkbox"/>
Read	<input type="checkbox"/>	<input type="checkbox"/>
Write	<input type="checkbox"/>	<input type="checkbox"/>
Create all child objects	<input type="checkbox"/>	<input type="checkbox"/>
Delete all child objects	<input type="checkbox"/>	<input type="checkbox"/>

For special permissions or advanced settings, click Advanced.

Delegation of Control Wizard

**Tasks to Delegate**  
You can select common tasks or customize your own.

Delegate the following common tasks:

- Create, delete, and manage user accounts
- Reset user passwords and force password change at next logon
- Read all user information
- Create, delete and manage groups
- Modify the membership of a group
- Manage Group Policy links**
- Generate Resultant Set of Policy (Planning)

Create a custom task to delegate

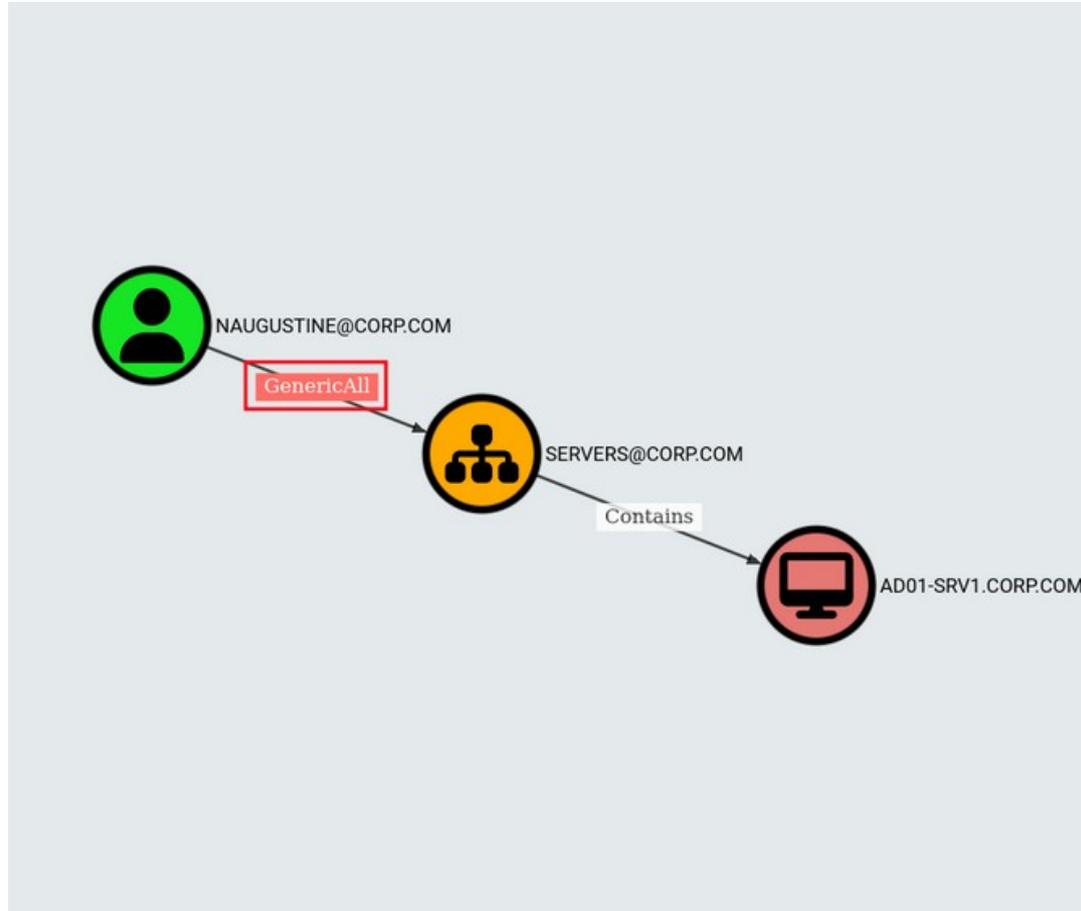
< Back Next > Cancel Help

- **L'attribution de droits sur les OUs n'est pas aussi inoffensive qu'elle n'en a l'air.**
- **Ces droits peuvent être exploités pour compromettre l'ensemble des objets enfants, y compris situés dans des OUs imbriquées.**

# Compromission d'OUs via héritage d'ACL : exploitation et limites

- **Vecteur d'attaque connu présent dans BloodHound, reposant sur le mécanisme d'héritage d'ACLs**
  - Possible de spécifier qu'une ACE définie sur un conteneur doit également s'appliquer à tous les objets enfants
  - Exploitation d'un droit **GenericAll** (comprenant **WriteDACL**) pour ajouter une ACE sur le conteneur

# Compromission d'OUs via héritage d'ACL : exploitation et limites



GenericAll

General

The user NAUGUSTINE@CORP.COM has GenericAll permissions to the OU SERVERS@CORP.COM.

This is also known as full control. This permission allows the trustee to manipulate the target object however they wish.

Windows Abuse

Linux Abuse

**Control of the Organization Unit**

With full control of the OU, you may add a new ACE on the OU that will inherit down to the objects under that OU. Below are two options depending on how targeted you choose to be in this step:

Generic Descendent Object Takeover

The simplest and most straight forward way to abuse control of the OU is to apply a GenericAll ACE on the OU that will inherit down to all object types. This can be done using Impacket's dacledit (cf. "grant rights" reference for the link).

```
dacledit.py -action 'write' -rights 'FullControl' -inheritance -principal 'JKHOLER' -target-dn 'OUDist' -ingushedName 'domain/' -user':'password'
```

Now, the "JKHOLER" user will have full control of all descendent objects of each type.

Targeted Descendent Object Takeover

If you want to be more targeted with your approach, it is possible to specify precisely what right you want to apply to precisely which kinds of descendent objects. Refer to the Windows Abuse info for this.

# Compromission d'OUs via héritage d'ACL : exploitation et limites

```
$ dactedit.py -action 'write' -rights 'FullControl' -inheritance -principal 'naugustine' -  
target-dn 'OU=SERVERS,DC=corp,DC=com' 'corp.com'/'naugustine': 'Password1'
```

```
[...]
```

```
[*] DACL modified successfully!
```

```
$ dactedit.py -action 'read' -principal 'naugustine' -target-dn 'CN=AD01-  
SRV1,OU=SERVERS,DC=corp,DC=com' 'corp.com'/'naugustine': 'Password1'
```

```
[...]
```

```
[*] Filtering results for SID (S-1-5-21-2015307081-2275635861-2347354195-1481)
```

```
[*] ACE[20] info
```

```
[*] ACE Type : ACCESS_ALLOWED_ACE
```

```
[*] ACE flags : CONTAINER_INHERIT_ACE, INHERITED_ACE, OBJECT_INHERIT_ACE
```

```
[*] Access mask : FullControl (0xf01ff)
```

```
[*] Trustee (SID) : naugustine (S-1-5-21-2015307081-2275635861-2347354195-1481)
```

## 1) Suppose un haut niveau de permission **WriteDACL/GenericAll**

- La possibilité d'ajouter une ACE nécessite **WriteDACL**
- Impossible à exploiter en cas de **GenericWrite** ou **Manage Group Policy Links**
- Par rapport à ces deux autres permissions, pas de chemin de compromission affiché par BloodHound

# Compromission d'OUs via héritage d'ACL : exploitation et limites

The screenshot shows the BloodHound Community Edition interface. At the top, there are navigation tabs for 'EXPLORE' and 'GROUP MANAGEMENT'. The main area is divided into a search bar with 'SEARCH', 'PATHFINDING', and 'CYPHER' options. Below the search bar, a list of entities is shown, with 'NAUGUSTINE@CORP.COM' and 'AD01-SRV1.CORP.COM' highlighted. On the right, the details for 'NAUGUSTINE@CORP.COM' are displayed, including fields for 'Password Never Expires', 'Password Not Required', 'SAM Account Name', and 'Trusted For Constrained Delegation'. Below these are expandable sections for 'Sessions', 'Member Of', 'Local Admin Privileges', 'Execution Privileges', 'Outbound Object Control', and 'Inbound Object Control'. A red box highlights the 'Outbound Object Control' section, which shows a count of 0. At the bottom left, a black error message box states 'Path not found.' with a close button and a 'Current Results' button.

Property	Value
Password Never Expires:	TRUE
Password Not Required:	FALSE
SAM Account Name:	naugustine
Trusted For Constrained Delegation:	FALSE
Sessions	0
Member Of	2
Local Admin Privileges	0
Execution Privileges	0
Outbound Object Control	0
Inbound Object Control	8

## 2) Inexploitable pour les objets présentant l'attribut **adminCount=1**

- Dans Active Directory, des objets fortement privilégiés (comptes et groupes) présentent l'attribut LDAP adminCount=1.
- Au vu de leur criticité, les ACLs de ces objets sont protégées par un processus automatique les restaurant à une valeur de référence
- **Le mécanisme d'héritage d'ACLs est désactivé pour ces objets**

# Compromission d'OUs via héritage d'ACL : exploitation et limites

Domain Admins	Domain Controllers
Enterprise Admins	Read-only Domain Controllers
Administrators	Administrator
Schema Admins	Replicator
Account Operators	Server Operators
Backup Operators	Print Operators
Krbtgt	

# Un vecteur d'attaque alternatif : empoisonnement de l'attribut gPLink

- **Un vecteur d'attaque moins connu existe, permettant :**
  - L'exploitation des OUs par le biais de permissions **GenericWrite** ou **Manage Group Policy Links**
  - L'exploitation des OUs contenant des objets présentant l'attribut **adminCount=1**
- Tiré du travail de **Petros Koutroumpis**, adapté pour réduire les pré-requis et l'automatiser

## ■ L'implémentation des GPOs dans Active Directory

- Group Policy Container (**objet LDAP** – métadonnées GPO, y compris path du Group Policy Template)

```
CN={46993522-7D77-4B59-9B77-F82082DE9D81},CN=Policies,CN=System,DC=corp,DC=com
```

- Group Policy Template (**SMB share** – fichiers du GPO, par défaut share SYSVOL du DC)

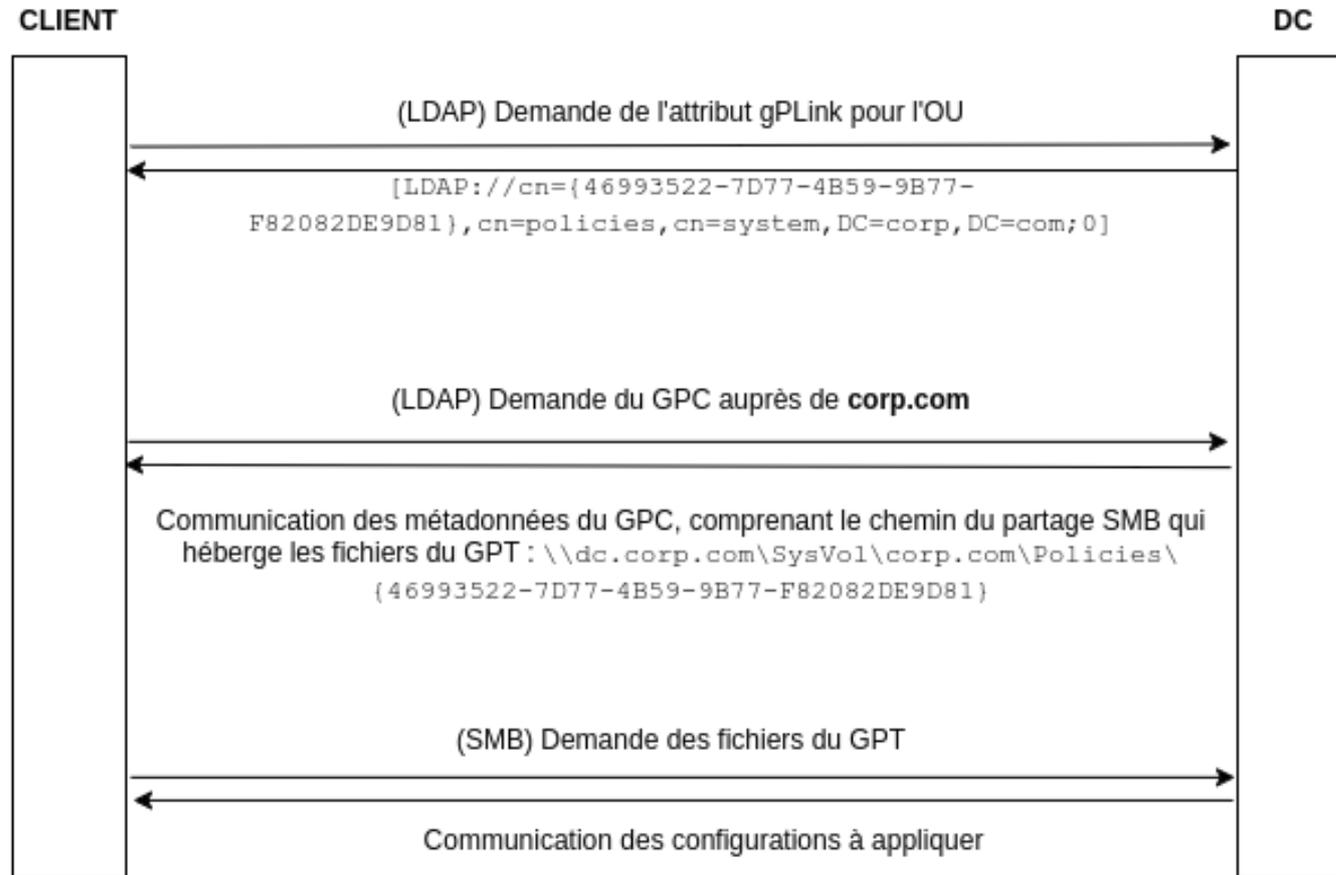
```
\\dc.corp.com\SysVol\corp.com\Policies\{46993522-7D77-4B59-9B77-F82082DE9D81}
```

## ■ L'attribut gPLink des Unités Organisationnelles

- Les GPOs sont appliquées aux OUs en spécifiant le CN du Group Policy Container dans l'attribut gPLink de l'OU.

```
[LDAP://cn={46993522-7D77-4B59-9B77-F82082DE9D81},cn=policies,cn=system,DC=corp,DC=com;0]
```

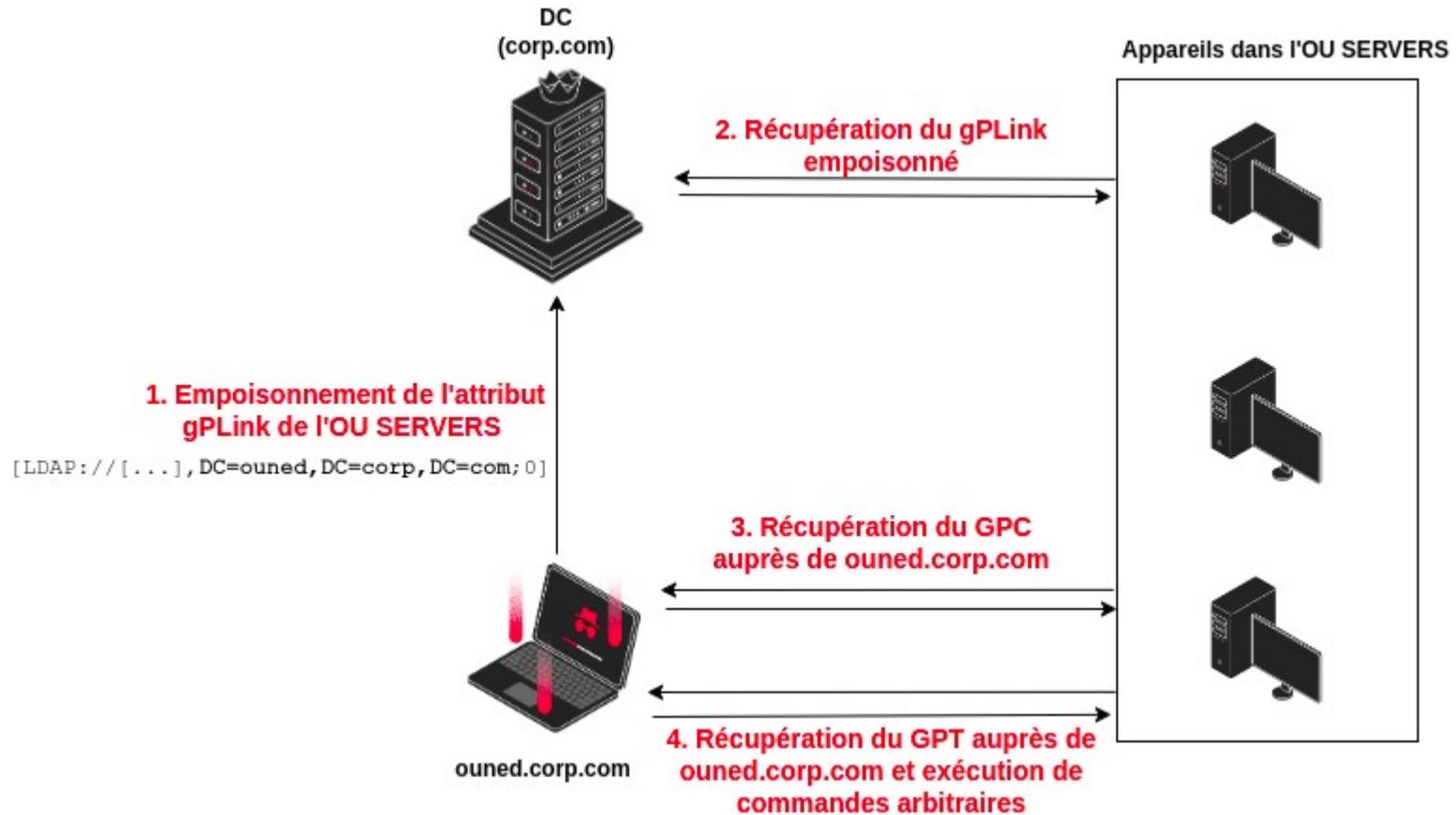
# Un vecteur d'attaque alternatif : empoisonnement de l'attribut gPLink



### ■ **Attaque par empoisonnement de l'attribut gPLink**

- 1) L'attaquant modifie l'attribut gPLink pour indiquer qu'une GPO est liée à l'OU, dont le GPC se trouve sur sa machine
- 2) L'attaquant héberge un serveur LDAP sur sa machine qui renvoie un GPC indiquant que le GPT se trouve également sur sa machine
- 3) L'attaquant héberge un serveur SMB renvoyant des fichiers de configuration malveillants au client

# Un vecteur d'attaque alternatif : empoisonnement de l'attribut gPLink



# Démonstration d'exploitation par OUned.py

- **Pré-requis à la réalisation de l'attaque (configuration AD par défaut) :**
  - Un compte machine disposant d'un SPN LDAP.
  - Un record DNS faisant pointer ce compte sur la machine de l'attaquant.
- **Pré-requis réseau : les objets cibles de l'OU doivent pouvoir joindre d'un point de vue réseau la machine de l'attaquant**

## ■ Détails d'implémentation pratique

- Utilisation d'un contrôleur de domaine factice pour simuler le serveur LDAP. Forward de l'ensemble du trafic LDAP.
- Ticket de service LDAP des clients : **LDAP@ouned.corp.com**. Pour que le DC puisse les déchiffrer :
  - Le nom de domaine du DC factice doit être synchronisé avec le nom du compte machine (**ouned.corp.com**)
  - Le mot de passe du compte machine doit être le même que celui du DC factice

**[VIDEO]**

# Conclusion

# Conclusion

The screenshot displays the BloodHound Community Edition interface. At the top, there are navigation options: "EXPLORE" and "GROUP MANAGEMENT". Below this, a search bar contains "NAUGUSTINE@CORP.COM" and "ADM-QROLAND@CORP.COM". The main area shows a pathfinding graph with three nodes: "NAUGUSTINE@CORP.COM" (green person icon), "\_ADMINS@CORP.COM" (yellow group icon), and "ADM-QROLAND@CORP.COM" (green person icon). A red box labeled "ManageGPLink" is positioned between the first and second nodes. An arrow labeled "Contains" points from the second node to the third. On the right, a detailed view for "ManageGPLink" is shown, including a "General" section with explanatory text and "Windows Abuse" and "Linux Abuse" sections with links to further information.

**ManageGPLink**

**General**

The user NAUGUSTINE@CORP.COM has the permissions to modify the gPLink attribute of the Organizational Unit \_ADMINS@CORP.COM.

The ability to alter the gPLink attribute of an Organizational Unit may allow an attacker to apply a malicious Group Policy Object to all of the OU's child items (including the ones included in nested sub-OUs). This can be exploited to make said child items execute arbitrary commands through an immediate scheduled task, thus compromising them.

Successful exploitation will require the possibility to add non-existing DNS records to the domain and to create machine accounts. Note that the attack vector implementation is not trivial and will require some setup.

**Windows Abuse**

From a domain-joined compromised Windows machine, the ManageGPLink permission may be abused through Powermad, PowerView and native Windows functionalities. For a detailed outline of exploit requirements and implementation, you can refer to [this article](#).

**Linux Abuse**

From a Linux machine, the ManageGPLink permission may be abused using the OUned.py exploitation tool. For a detailed outline of exploit requirements and implementation, you can refer to [the article associated to the OUned.py tool](#).

**OPSEC**

The present attack vector relies on the execution of a malicious Group Policy Object. In case some objects in the target Organizational Unit are unable to apply said Group Policy Object (for instance, because these objects cannot reach the attacker's machine in the internal network), events related to failed GPO application will be created. Furthermore, the execution of this attack will result in the modification of the gPLink property of the target Organizational Unit. The property should be reset to its original value after attack execution to avoid detection and ensure the OU child items can apply their legitimate Group Policy Objects again.



# Conclusion

The screenshot displays the BloodHound Community Edition interface. At the top, there are navigation tabs for 'EXPLORE' and 'GROUP MANAGEMENT'. Below this, a search bar and a 'PATHFINDING' tab are visible. The main area shows a pathfinding diagram with three nodes: NAUGUSTINE@CORP.COM (green person icon), SERVERS@CORP.COM (yellow server icon), and AD01-SRV1.CORP.COM (red server icon). Arrows indicate the path, with 'GenericWrite' labeled on the arrow from the user to the servers OU, and 'Contains' labeled on the arrow from the servers OU to the AD01-SRV1.CORP.COM server. On the right, a detailed view of the 'GenericWrite' permission is shown, including sections for 'General', 'Windows Abuse', 'Linux Abuse', and 'OPSEC'. Each abuse section contains text explaining the impact of the permission and provides links to related articles.

**GenericWrite**

**General**

**Windows Abuse**

With GenericWrite permissions over an Organizational Unit, you may make modifications to the gPLink attribute of the OU. The ability to alter the gPLink attribute of an Organizational Unit may allow an attacker to apply a malicious Group Policy Object to all of the OU's child items (including the ones included in nested sub-OUs). This can be exploited to make said child items execute arbitrary commands through an immediate scheduled task, thus compromising them.

Successful exploitation will require the possibility to add non-existing DNS records to the domain and to create machine accounts. Note that the attack vector implementation is not trivial and will require some setup.

From a domain-joined compromised Windows machine, the gPLink manipulation attack vector may be exploited through Powermad, PowerView and native Windows functionalities. For a detailed outline of exploit requirements and implementation, you can refer to [this article](#).

**Linux Abuse**

With GenericWrite permissions over an Organizational Unit, you may make modifications to the gPLink attribute of the OU. The ability to alter the gPLink attribute of an Organizational Unit may allow an attacker to apply a malicious Group Policy Object to all of the OU's child items (including the ones included in nested sub-OUs). This can be exploited to make said child items execute arbitrary commands through an immediate scheduled task, thus compromising them.

Successful exploitation will require the possibility to add non-existing DNS records to the domain and to create machine accounts. Note that the attack vector implementation is not trivial and will require some setup.

From a Linux machine, the gPLink manipulation attack vector may be exploited using the `OUned.py` tool. For a detailed outline of exploit requirements and implementation, you can refer to [the article associated to the OUned.py tool](#).

**OPSEC**



The logo for SYNACKTIV features a stylized icon on the left consisting of a 3x3 grid of squares, with the top-right square containing a red dot. To the right of this icon, the word "SYNACKTIV" is written in a bold, sans-serif font. "SYN" is in white, and "ACKTIV" is in red. Below the text is a horizontal line composed of six red rectangular segments.

# SYNACKTIV



<https://www.linkedin.com/company/synacktiv>



<https://twitter.com/synacktiv>



<https://synacktiv.com>