SYNACKTIV

OUned

L'exploitation des Unités Organisationnelles en environnement Active Directory

BARBHACK 2024

31/08/2024

Whoami

SYNACKTIV

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

Quentin Roland

Pentester

Introduction

Introduction

SYNACKTIV

- 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

Agenda

SYNACKTIV

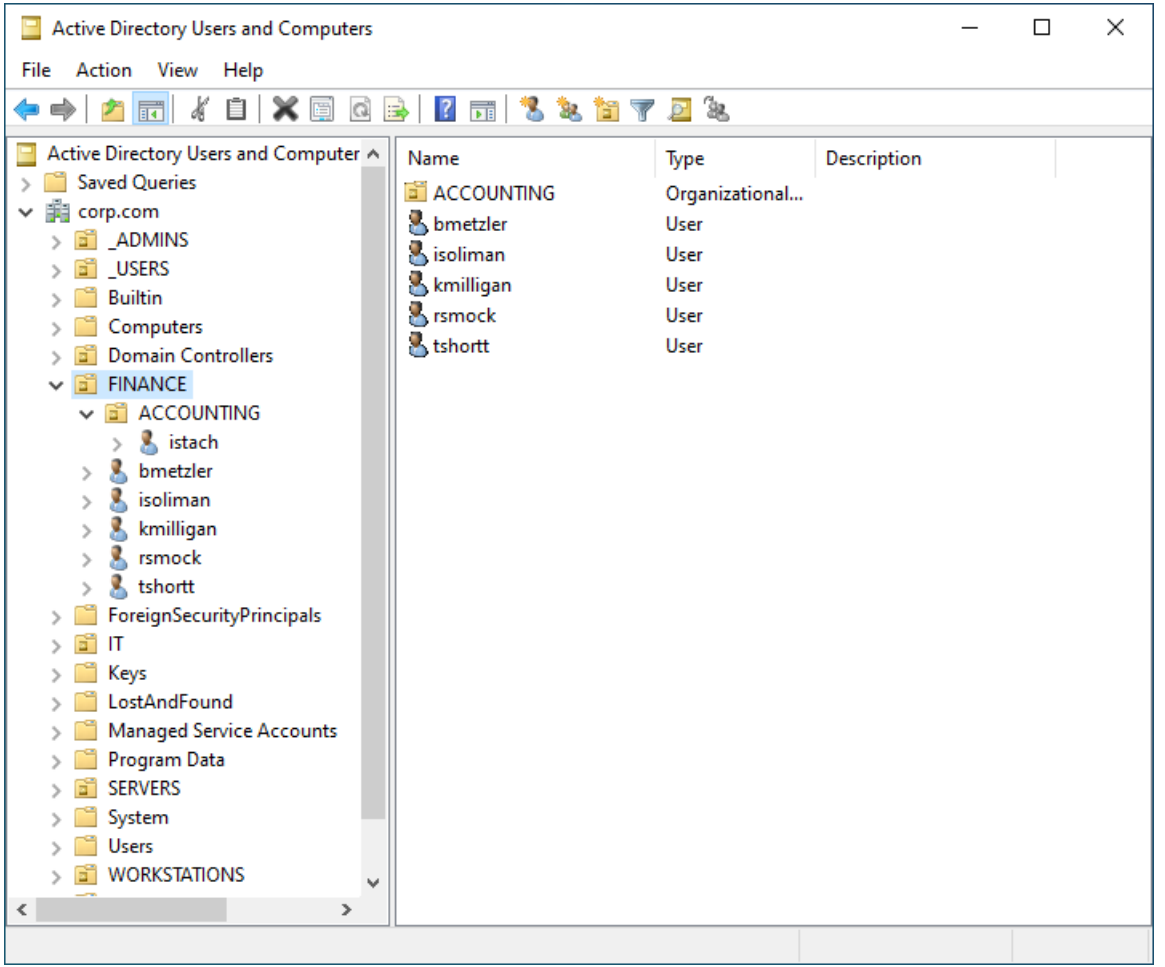
- Unités Organisationnelles : définitions et ACLs
- Compromission d'OUs via héritage d'ACL : exploitation et limites
- Un vecteur d'attaque alternatif : empoisonnement de l'attribut gPLink
- Démonstration d'exploitation par OUned.py & vidéo

Unités Organisationnelles : définitions et ACLs

Unités Organisationnelles : définitions et ACLs

SYNACKTIV

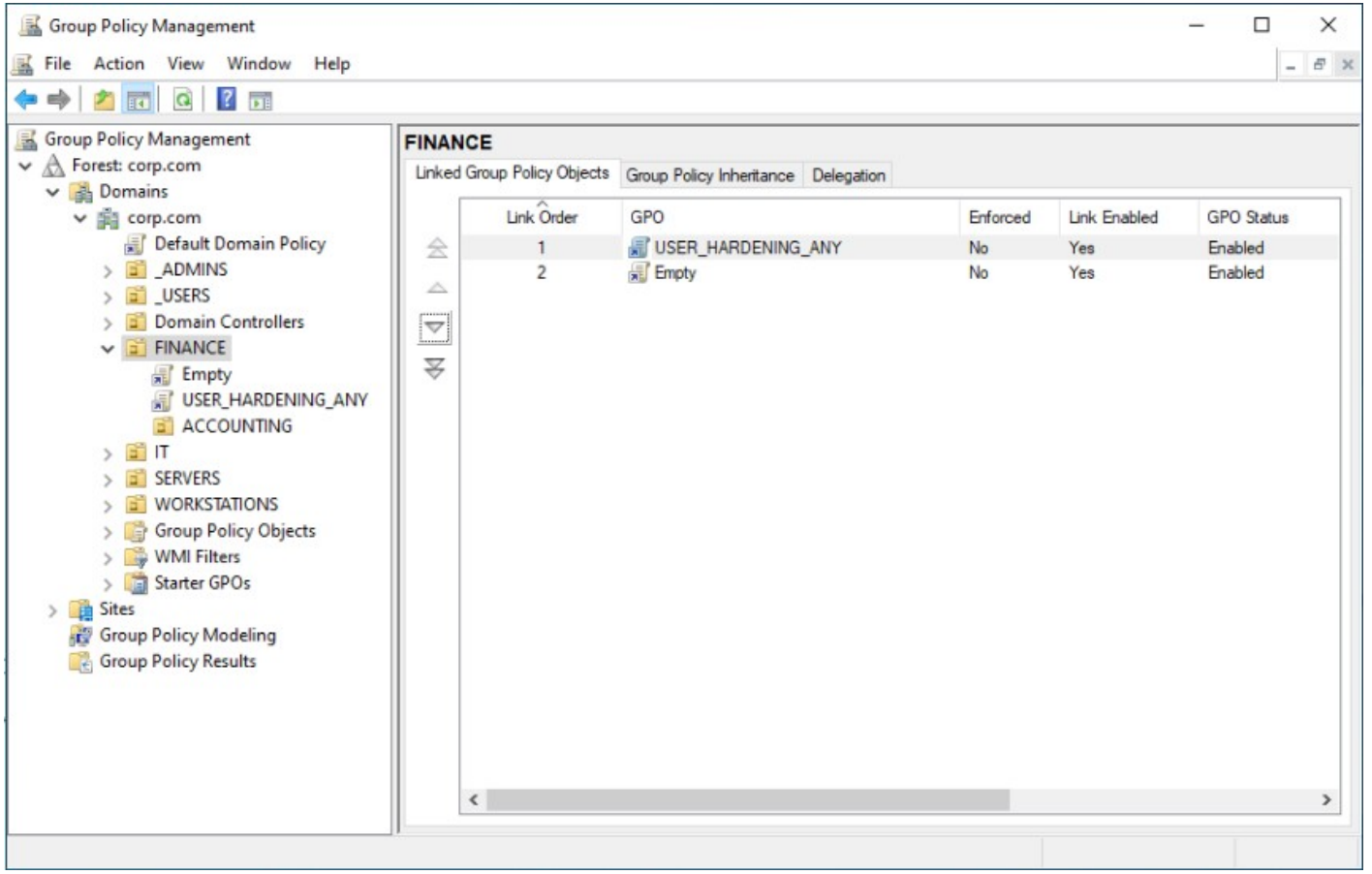
OUs : conteneurs logiques organisant les objets Active Directory en sous-ensembles



Unités Organisationnelles : définitions et ACLs

SYNACKTIV

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



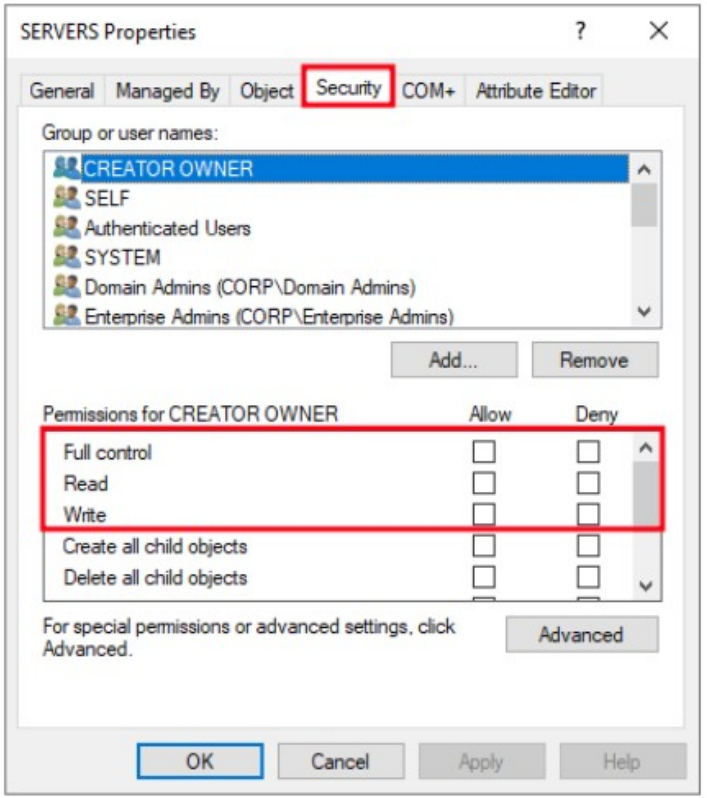
Unités Organisationnelles : définitions et ACLs

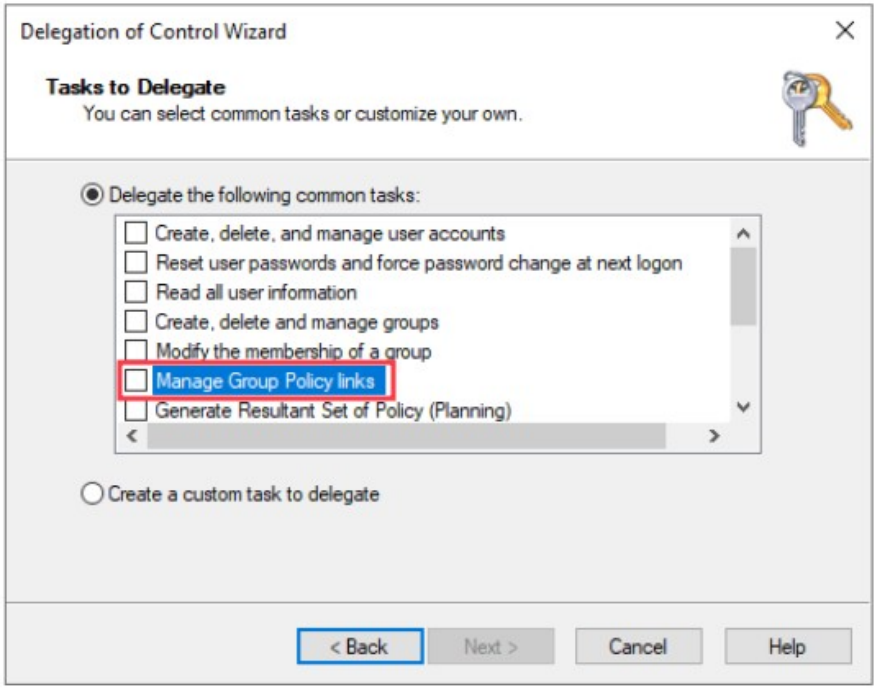
SYNACKTIV

- **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

SYNACKTIV





Unités Organisationnelles : définitions et ACLs

SYNACKTIV

- 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

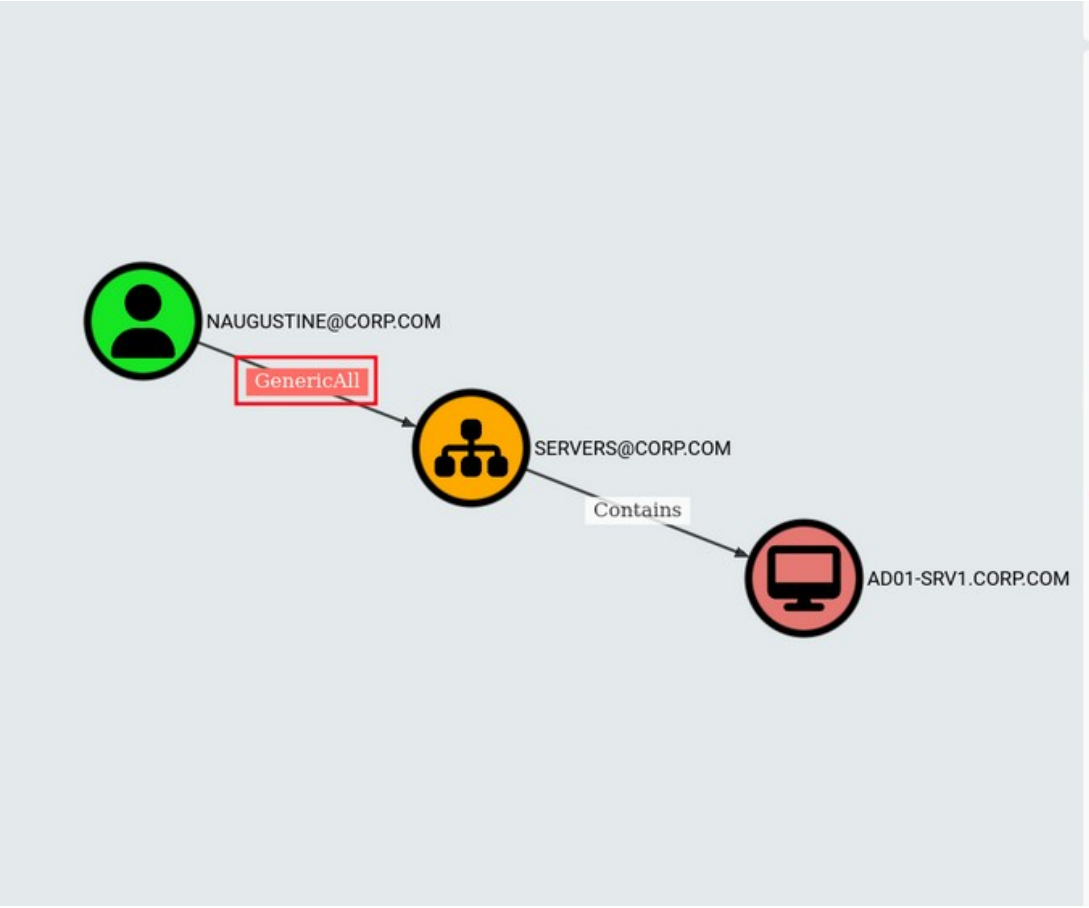
Compromission d'OUs via héritage d'ACL : exploitation et limites

SYNACKTIV

- **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

SYNACKTIV



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 'OUDistinguishedName' 'domain'/'user':'password'
```

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

Targeted Descendent Object Takeoever

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

SYNACKTIV

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

[...]

[*] DACL modified successfully!


$ dacledit.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)
```

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

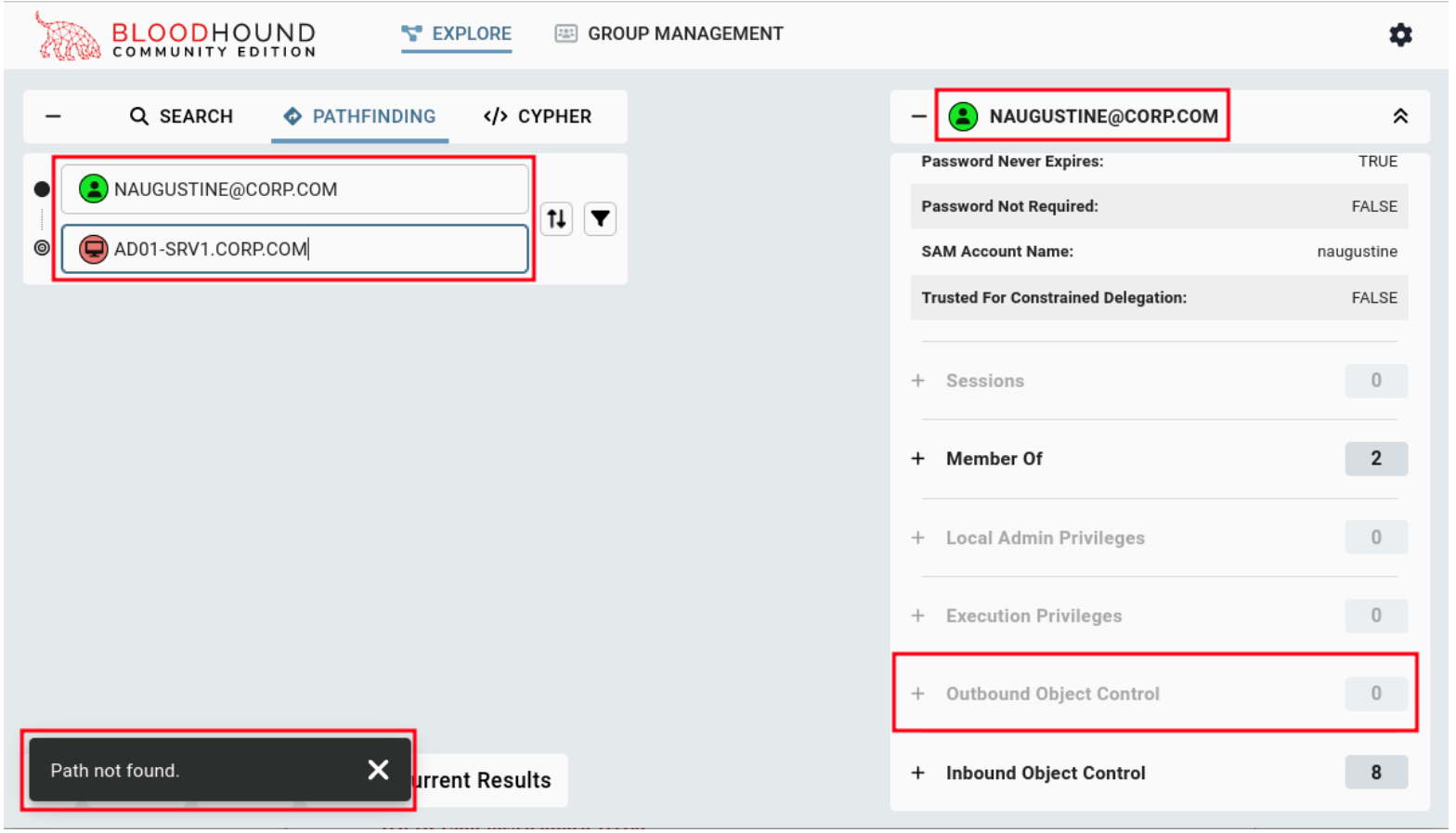
SYNACKTIV

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

SYNACKTIV



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

SYNACKTIV

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

SYNACKTIV

- **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}
```

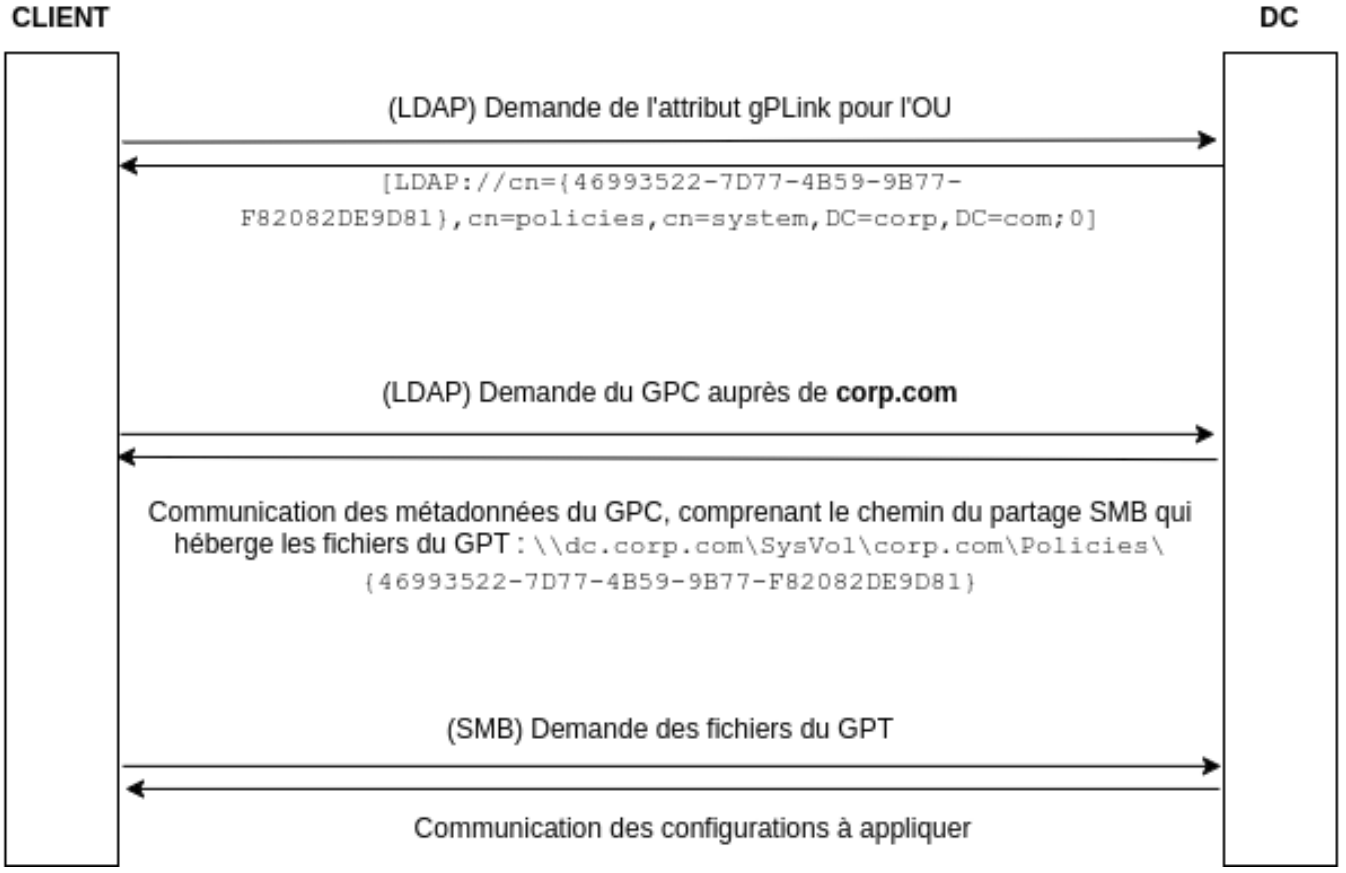
SYNACKTIV

- **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

SYNACKTIV

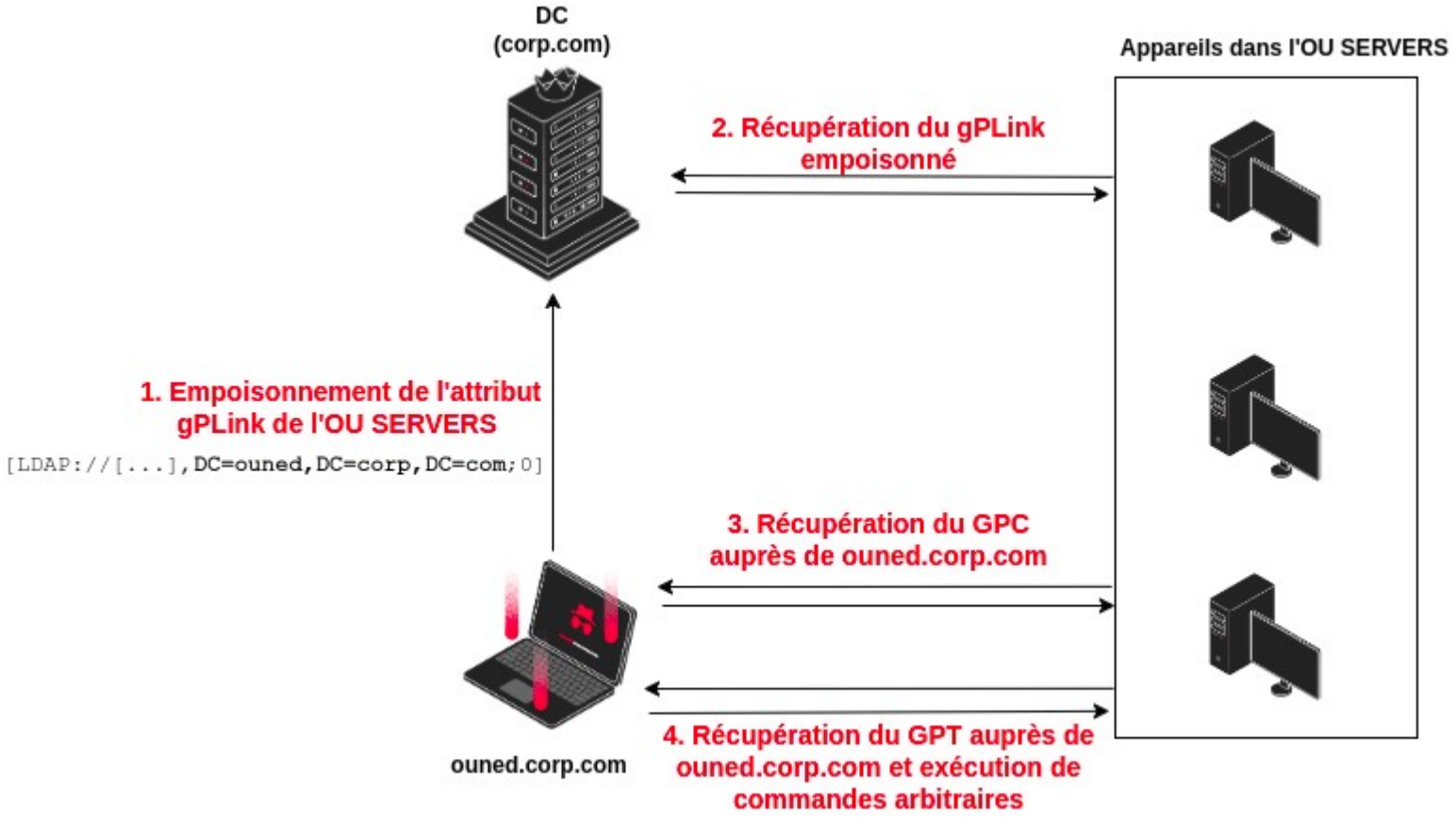


- **Attaque par empoisonnement de l'attribut gPLink**

  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

SYNACKTIV



Démonstration d'exploitation par OUned.py

Démonstration d'exploitation par OUned.py

SYNACKTIV

- **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**

Démonstration d'exploitation par OUned.py

SYNACKTIV

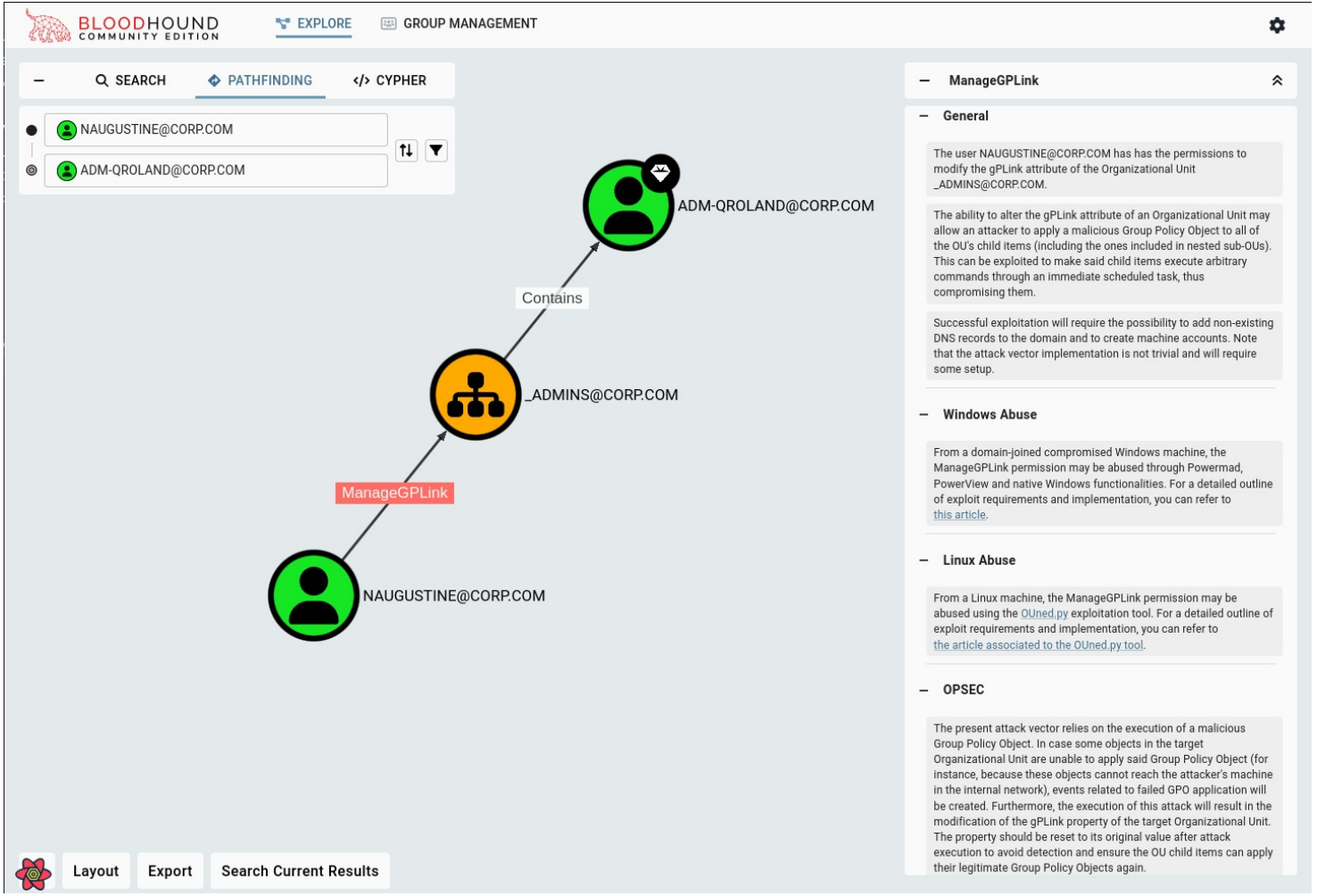
- **Détails d'implémentation pratique**
  - Utilisation d'un contrôleur de domaine factice pour simuler le serveur LDAP. Forward de l'ensemble du traffic LDAP.
  - Ticket de service LDAP des clients : **LDAP@ouned.corp.com**. Pour que le DC puisse les déchiffrer :
    - Le nom de domaine du DC factice 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

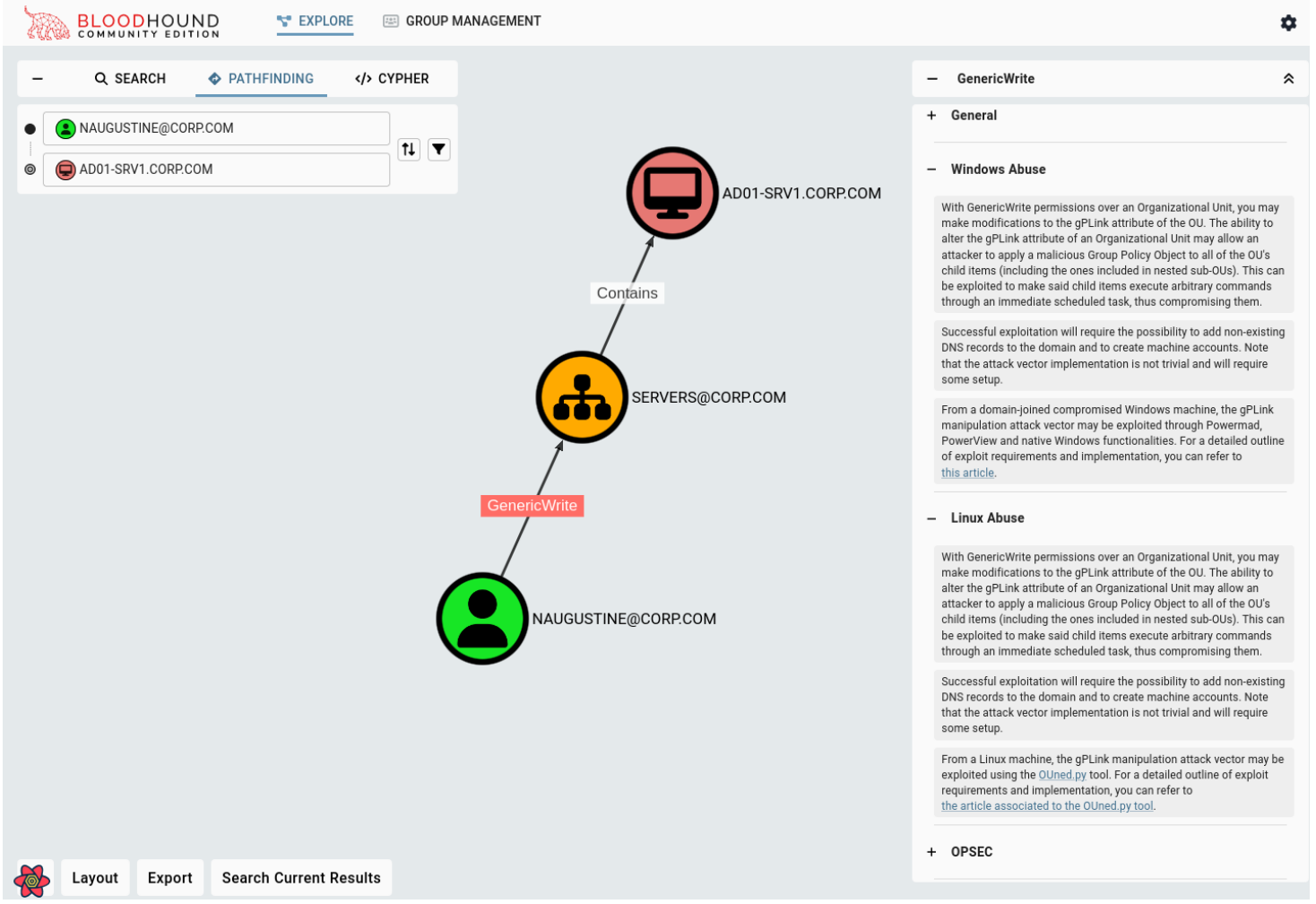
Conclusion

SYNACKTIV



Conclusion

SYNACKTIV



SYNACKTIV

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

https://twitter.com/synacktiv

https://synacktiv.com