Implementation d'un test de pénétration sur Active Directory avec l'outil « Responder »

l'outil Responder est un utilitaire de pentest largement utilisé par les red teams et les pentesters pour intercepter des requêtes réseau telles que LLMNR, NBNS ou MDNS. En exploitant ces protocoles, l'attaquant peut capturer des identifiants Windows (souvent des hashs NTLMv1/v2), voire les relayer ou les casser pour obtenir un accès non autorisé à des ressources critiques. Le TP a donc un double objectif pédagogique : d'une part, démontrer de façon concrète comment une faille de configuration ou un manque de segmentation réseau peut compromettre l'ensemble du domaine Active Directory ; d'autre part, renforcer les bonnes pratiques de sécurisation (désactivation des protocoles vulnérables, surveillance réseau, filtrage ARP/LLMNR, etc.). Il s'agit d'une expérience pratique puissante pour comprendre les enjeux de sécurité liés à l'authentification Windows et à la communication entre machines dans un domaine, tout en expérimentant des techniques offensives dans un cadre encadré et contrôlé.

Prérequis et Initialisation du projet :

- **1 machine virtuelle Windows Server 2019**
- **1 machine Windows 10**
- **1 machine sous Kali Linux**
- **VMWare Workstation 17**

Prérequis du projet :

- **Configuration d'un domaine Active Directory (domaine utilisé dans notre TP : ais.lan)**
- **Création d'un utilisateur avec UPN (User Principal Name)**

Adressage réseau :

N°	Nom d'hôte	Rôle	Adresse IP	Environnement
1	DC1	Contrôleur de Domaine	192.168.1.182/24	Windows Server 2019
2	CLIENT-IMP	Machine Cliente	192.168.1.134/24	Windows 10
3	KALI	Machine Attaquante	192.168.1.156/24	Kali Linux dernière version

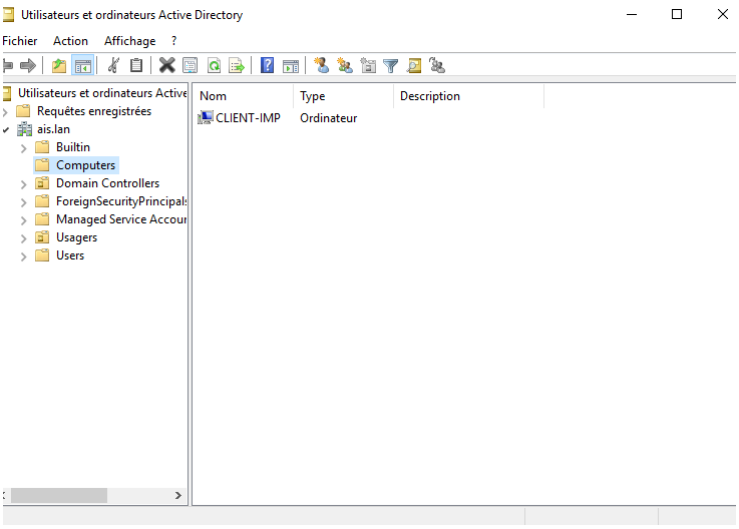
PRESENTATION DES CONFIGURATIONS DE BASE

Nous allons débuter par présenter les configurations de base qui ont été faites hormis la mise en

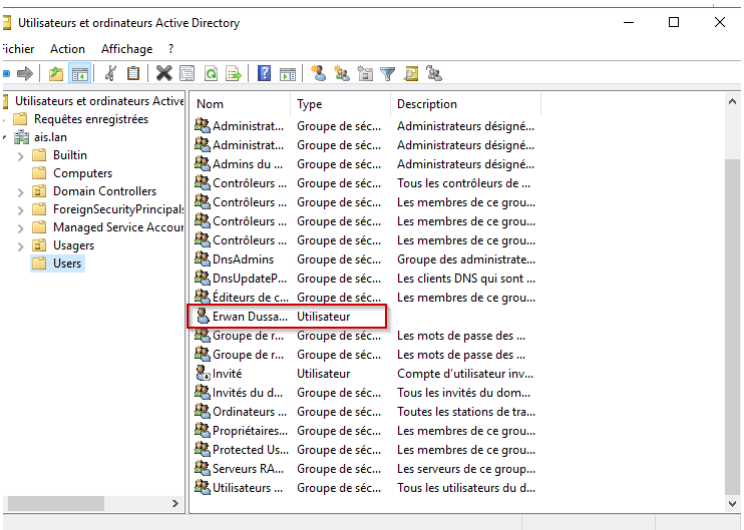
réseau.

L'hôte et l'Utilisateur :

Sur cette photo, nous voyons notre hôte "CLIENT-IMP" qui figure dans les ordinateurs du domaine ais.lan :



L'utilisateur avec l'UPN : Erwan.dussaux@ais.lan se trouve dans l'OU "Users" :



Exploitation des failles :

1. <u>Introduction au LLMNR</u>

LLMNR (Link-Local Multicast Name Resolution) est un protocole utilisé pour identifier les hôtes en cas d'échec du DNS. Il succède à NBT-NS (NetBIOS Name Service) et fonctionne via le port UDP 5355.

Lorsque un client recherche un nom sur le réseau, il suit plusieurs étapes :

- **Vérificartion du fichier hosts**
- **Consultation du cache DNS**
- **Recherche auprès des serveurs DNS configurés**
- **Utilisation de NBT-NS (broadcast) si échec**
- **Envoie une requête LLMNR (multicast) si nécessaire**
- **Si aucune réponse n'est reçue, alors la recherche échoue.**

A. Attaque par Poissoning

L'attaque par empoisonnement consiste à tromper un système en lui envoyant des réponses falsifiées à ses requêtes réseau. Dans le cas de LLMNR et NBT-NS, un attaquant se positionne sur le réseau et répond aux requêtes de résolution de noms avant le serveur légitime. Cela force la victime à se connecter à un faux serveur, où l'attaquant peut intercepter des identifiants sous forme de hash NTLMv1/v2.

B. Attaque avec Responder sous Kali Linux

L'outil Responder de Kali Linux permet d'exploiter cette faille en empoisonnant les requêtes LLMNR/NBT-NS et en capturant les identifiants des utilisateurs. L'attaque se déroulera comme suit :

<u>Capture des identifiants :</u>

- **- Lorsqu'une victime cherche un partage réseau inexistant, Responder envoie une fausse réponse.**
- **- La machine de la victime tente alors une connexion au serveur de l'attaquant, envoyant son hash NTLM.**

<u>Exploitation des hash capturés :</u>

- **- Les hash NTLM capturés sont stockés dans un fichier de logs et peuvent être déchiffrés avec des outils comme hashcat ou John the Ripper.**

2. <u>Mise en place de l'attaque :</u>

Vous pouvez installer l'outil Responder (Déjà préinstaller sur Kali)

```
┌──(kali㉿kali)-[~]
└─$ apt install responder
```

Nous lançons maintenant l'outil Responder

```
└─$ sudo responder -I eth0 -wd
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 3.1.5.0

  To support this project:
  Github → https://github.com/sponsors/lgandx
  Paypal  → https://paypal.me/PythonResponder

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CTRL-C


[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    MDNS                       [ON]
    DNS                        [ON]
    DHCP                       [ON]

[+] Servers:
    HTTP server                [ON]
    HTTPS server               [ON]
    WPAD proxy                 [ON]
```

Dans la syntaxe les options :

- **I: option pour interface**
- **w : permet d'exécuter un serveur WPAD. Le protocole WPAD (Web Proxy Auto-**

  Discovery Protocol) est une méthode utilisée par les navigateurs pour localiser l'URL d'un fichier de configuration. Une fois la détection et le téléchargement du fichier de configuration terminés, il peut être exécuté pour déterminer le proxy pour une URL spécifiée.

  d : cette option permet de répondre aux requêtes de suffixes de domaine.

Implementation d'un test de pénétration sur Active Directory avec l'outil « Responder »

l'outil Responder est un utilitaire de pentest largement utilisé par les red teams et les pentesters pour intercepter des requêtes réseau telles que LLMNR, NBNS ou MDNS. En exploitant ces protocoles, l'attaquant peut capturer des identifiants Windows (souvent des hashs NTLMv1/v2), voire les relayer ou les casser pour obtenir un accès non autorisé à des ressources critiques. Le TP a donc un double objectif pédagogique : d'une part, démontrer de façon concrète comment une faille de configuration ou un manque de segmentation réseau peut compromettre l'ensemble du domaine Active Directory ; d'autre part, renforcer les bonnes pratiques de sécurisation (désactivation des protocoles vulnérables, surveillance réseau, filtrage ARP/LLMNR, etc.). Il s'agit d'une expérience pratique puissante pour comprendre les enjeux de sécurité liés à l'authentification Windows et à la communication entre machines dans un domaine, tout en expérimentant des techniques offensives dans un cadre encadré et contrôlé.

Prérequis et Initialisation du projet :

- **1 machine virtuelle Windows Server 2019**
- **1 machine Windows 10**
- **1 machine sous Kali Linux**
- **VMWare Workstation 17**

Prérequis du projet :

- **Configuration d'un domaine Active Directory (domaine utilisé dans notre TP : ais.lan)**
- **Création d'un utilisateur avec UPN (User Principal Name)**

Adressage réseau :

N°	Nom d'hôte	Rôle	Adresse IP	Environnement
1	DC1	Contrôleur de Domaine	192.168.1.182/24	Windows Server 2019
2	CLIENT-IMP	Machine Cliente	192.168.1.134/24	Windows 10
3	KALI	Machine Attaquante	192.168.1.156/24	Kali Linux dernière version

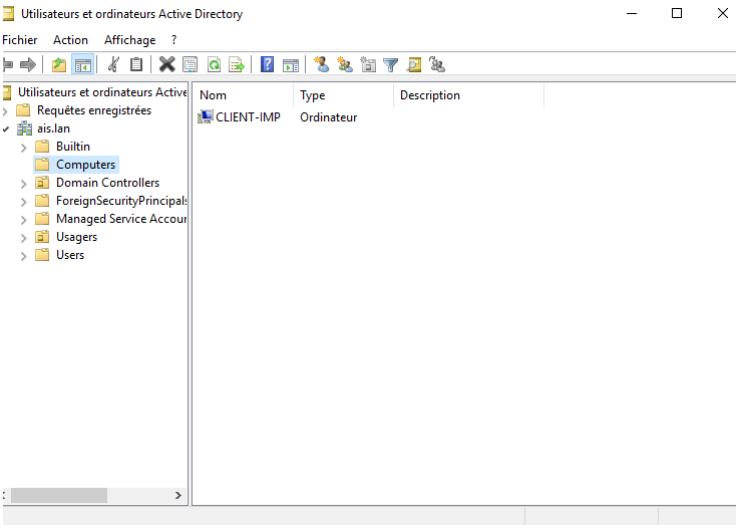
PRESENTATION DES CONFIGURATIONS DE BASE

Nous allons débuter par présenter les configurations de base qui ont été faites hormis la mise en

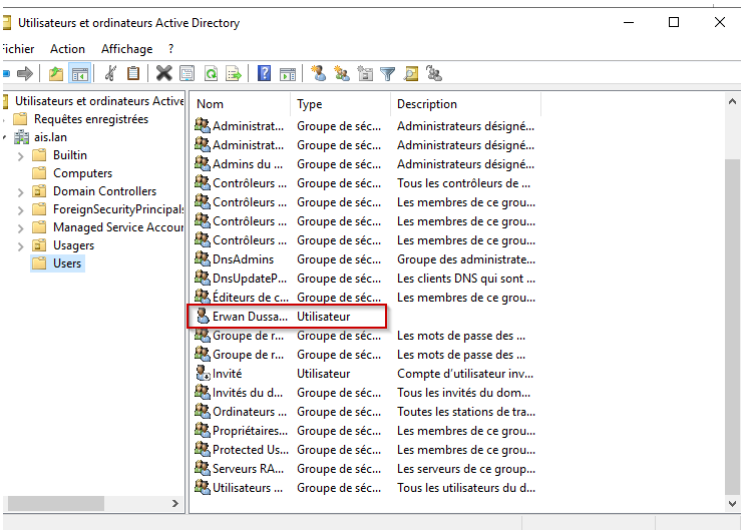
réseau.

<u>L'hôte et l'Utilisateur :</u>

Sur cette photo, nous voyons notre hôte "CLIENT-IMP" qui figure dans les ordinateurs du domaine ais.lan :



L'utilisateur avec l'UPN : Erwan.dussaux@ais.lan se trouve dans l'OU "Users" :



Exploitation des failles :

1. <u>Introduction au LLMNR</u>

LLMNR (Link-Local Multicast Name Resolution) est un protocole utilisé pour identifier les hôtes en cas d'échec du DNS. Il succède à NBT-NS (NetBIOS Name Service) et fonctionne via le port UDP 5355.

Lorsque un client recherche un nom sur le réseau, il suit plusieurs étapes :

- **Vérificartion du fichier hosts**
- **Consultation du cache DNS**
- **Recherche auprès des serveurs DNS configurés**
- **Utilisation de NBT-NS (broadcast) si échec**
- **Envoie une requête LLMNR (multicast) si nécessaire**
- **Si aucune réponse n'est reçue, alors la recherche échoue.**

C. Attaque par Poissoning

L'attaque par empoisonnement consiste à tromper un système en lui envoyant des réponses falsifiées à ses requêtes réseau. Dans le cas de LLMNR et NBT-NS, un attaquant se positionne sur le réseau et répond aux requêtes de résolution de noms avant le serveur légitime. Cela force la victime à se connecter à un faux serveur, où l'attaquant peut intercepter des identifiants sous forme de hash NTLMv1/v2.

D. Attaque avec Responder sous Kali Linux

L'outil Responder de Kali Linux permet d'exploiter cette faille en empoisonnant les requêtes LLMNR/NBT-NS et en capturant les identifiants des utilisateurs. L'attaque se déroulera comme suit :

<u>Capture des identifiants :</u>

- **- Lorsqu'une victime cherche un partage réseau inexistant, Responder envoie une fausse réponse.**
- **- La machine de la victime tente alors une connexion au serveur de l'attaquant, envoyant son hash NTLM.**

<u>Exploitation des hash capturés :</u>

- **- Les hash NTLM capturés sont stockés dans un fichier de logs et peuvent être déchiffrés avec des outils comme hashcat ou John the Ripper.**

2. <u>Mise en place de l'attaque :</u>

Vous pouvez installer l'outil Responder (Déjà préinstaller sur Kali)

```
┌──(kali㉿kali)-[~]
└─$ apt install responder
```

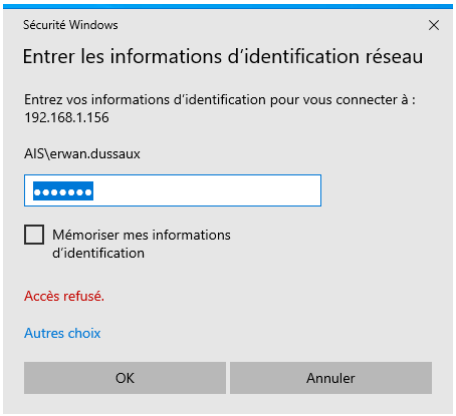
Nous lançons maintenant l'outil Responder

```
└─$ sudo responder -I eth0 -wd

           __
  .----.-----.-----.-----.-----.-----.--|  |.----.-----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 3.1.5.0

  To support this project:
  Github → https://github.com/sponsors/lgandx
  Paypal  → https://paypal.me/PythonResponder

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CTRL-C


[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    MDNS                       [ON]
    DNS                        [ON]
    DHCP                       [ON]

[+] Servers:
    HTTP server                [ON]
    HTTPS server               [ON]
    WPAD proxy                 [ON]
```

Dans la syntaxe les options :

- **I: option pour interface**
- **w : permet d'exécuter un serveur WPAD. Le protocole WPAD (Web Proxy Auto-Discovery Protocol) est une méthode utilisée par les navigateurs pour localiser l'URL d'un fichier de configuration. Une fois la détection et le téléchargement du fichier de configuration terminés, il peut être exécuté pour déterminer le proxy pour une URL spécifiée.**
- **d : cette option permet de répondre aux requêtes de suffixes de domaine.**

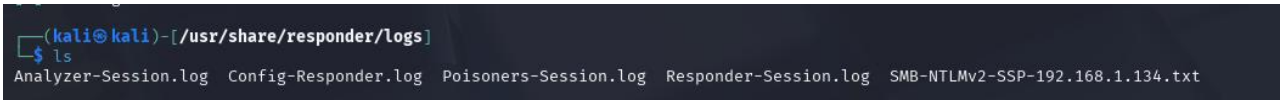
-
-
-
-
-
-
- **Sur notre machine Windows, nous allons ouvrir ‘’Exécuter’’ et tenter de nous connecter à notre machine linux avec l’adresse IP suivante « \\192.168.1.156».**
- **L’attaquant tentera de se connecter avec le compte de l’utilisateur « erwan dussaux » dont il ignore le mot de passe, juste dans le but de générer du trafic et par la suite essayer de retrouver le mot de passe à partir du trafic généré.**



On peut voir que notre outil Responder à bien récupérer le hash de la tentative de connexion comme o,n peut le voir ci-dessous :

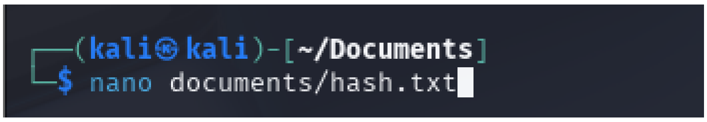
Nous allons donc récupérer le hash généré par l’outil en tapant la commande : cd /usr/share/responder/logs

Le fichier qui nous intéresse donc est « SMB-NTLMv2-SSP-192.168.1.134.txt »



On doit simplement lancer la commande « more [nom du fichier] pour voir les détails :

Je créer donc un fichier hash.txt pour contenir le hash généré



À ce niveau, nous allons passer au crack du mot de passe en utilisant « hashcat » pour essayer de retrouver le mot de passe de l'utilisateur « erwan dussaux » à partir du hash généré par « Responder ».

- Nous allons d'abord identifier le format du hash avec l'outil « hashid » préinstallé dans Kali.

- Pour notre attaque nous allons utiliser la wordlist « rockyou », par défaut fourni avec Kali.
- Nous procédons à présent à notre attaque

3. Contremesure de l'attaque

Les Contremesures pour lutter contre ces attaques :

- Désactiver LLMNR et NBT-NS ;
- Mots de passes utilisateurs forts (plus de 16 caractères) et complexes ;
- Changer régulièrement de mot de passe ;
- Filtrage de traffic;
- Signer le traffic SMB;
- Superviser le Traffic réseau afin de détecter les protocoles faibles.

<u>Se protéger complètement :</u>

Plusieurs solutions sont envisageables pour se protéger :

La 1ere, la plus radicale, mais la plus efficace est de désactiver ces protocoles sous Windows. Cela signifie que seul DNS sera utilisé pour la résolution.

Désactiver LLMNR :

- Ouvrez l'éditeur de stratégie de groupe locale : gpedit.msc
- Accédez à Stratégie de l'ordinateur local> Configuration ordinateur> Modèles d'administration> Réseau> Client DNS

- Sous Client DNS, positionnez l'option « Désactiver la résolution du nom de multidiffusion » sur Activé.

- Exécuter dans un cmd.exe ouvert en tant qu'administrateur la commande : gpupdate /force pour appliquer cette nouvelle stratégie.

Désactivation de NBT-NS :

- Ouvrez vos connexions réseau et affichez les propriétés de votre carte réseau.

-Sélectionnez Protocole Internet version 4 (TCP / IPv4) et cliquez sur Propriétés.

-Dans l'onglet Général, cliquez sur Avancé... et accédez à l'onglet WINS, puis sélectionnez « Désactiver NetBIOS sur TCP / IP ».

Attention, en ce qui concerne la désactivation de NBT-NS, la manipulation est à effectuer sur toutes les cartes connectées (Carte Wifi par exemple).

Il est aussi possible de désactiver de manière plus globale ce paramètre via DHCP en utilisant l'option « 001 Microsoft Disable NetBIOS Option » dans les Options du scope IP sous Avancé puis Microsoft Windows 2000 Options. Le paramètre à positionner est 0x2.

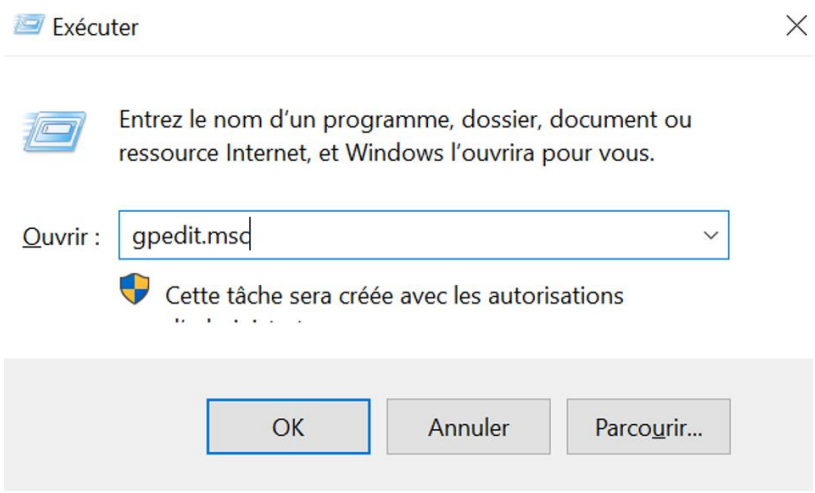
Enfin la commande PowerShell ci-dessous permet de désactiver plus facilement sur l'ensemble des interfaces :

Set-ItemProperty HKLM:\SYSTEM\CurrentControlSet\services\NetBT\Parameters\Interfaces\tcpip* -Name NetbiosOptions -Value 2

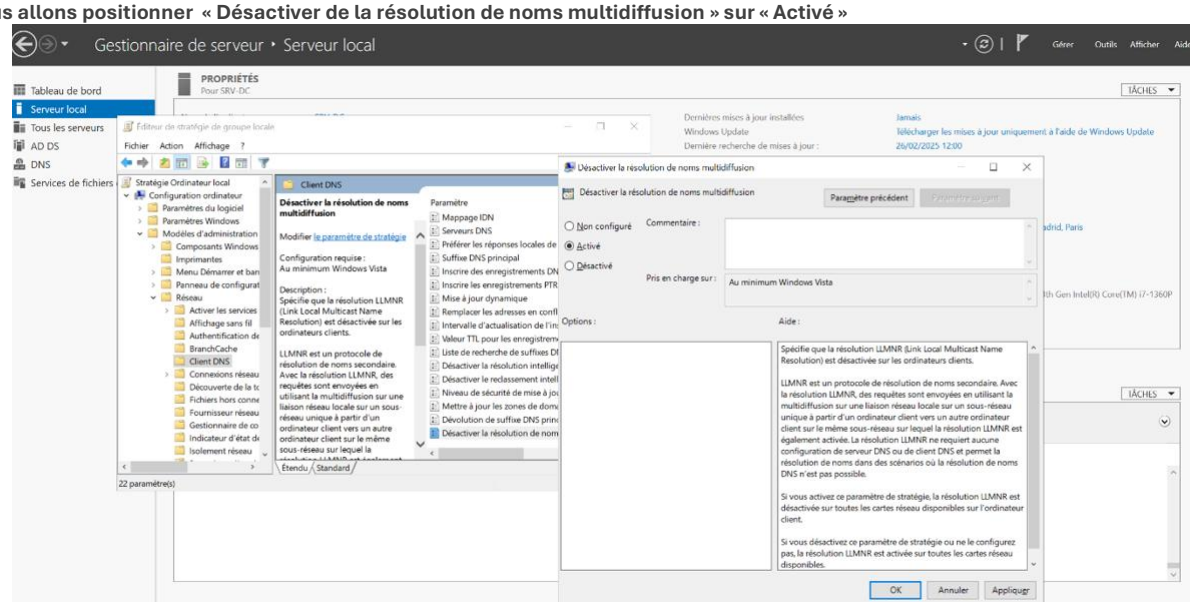
Implémentaion des contremesures :

Toutes les contremesures seront implémentées sur notre Contrôleur de Domaine.

1. **Désactivation de LLMNR**



Nous allons dans « Stratégie de l'ordinateur local > Configuration ordinateur > Modèles d'administration > Réseau > Client DNS » et nous allons positionner « Désactiver de la résolution de noms multidiffusion » sur « Activé »



Nous allons appliquer maintenant notre nouvelle stratégie

```
C:\Users\Administrateur>gpupdate /force
Mise à jour de la stratégie...

La mise à jour de la stratégie d'ordinateur s'est terminée sans erreur.
La mise à jour de la stratégie utilisateur s'est terminée sans erreur.
```

Désactivation de NBT-NS :

Nous allons utiliser une commande PowerShell pour désactiver le « NBT-NS » sur toutes les

Interfaces réseau :

```
PS C:\Users\Administrateur> Set-ItemProperty HKLM:\SYSTEM\CurrentControlSet\services\NetBT\Parameters\Interfaces\tcpip*
-Name NetbiosOptions -Value 2
PS C:\Users\Administrateur>
```

ET voilà maintenant Responder ne plus récupérer le hash lors de la connexion !