# Les protocoles réseau à risque actifs par défaut

## (environnement Windows)



Version 1.0 - 2025

# LLMNR, NetBIOS et mDNS

## Points communs à ces trois protocoles de résolution de noms :

- Interrogent les machines voisines d'un réseau local en l'absence de résolution DNS
- Actifs par défaut sur les systèmes Windows
  - Depuis Windows 2000 pour NetBIOS (2000)
  - Depuis Windows XP pour LLMNR (2001)
  - Depuis Windows 10 1703 (2017)
- Génèrent beaucoup de « bruit » sur le réseau
- Plus ou peu utiles sur un SI professionnel de nos jours
- Largement exploités par les attaquants et pentesters

# LLMNR, NetBIOS et mDNS

## Les différences :

| Protocole | Destination | Port | Encodage du nom | Création |
|---|---|---|---|---|
| NetBIOS | Broadcast | 137/UDP | OUI | Sytek, Inc. 1983 |
| mDNS | Multicast 224.0.0.251 | 5353/UDP | NON | Bill Woodcock Bill Manning 2000 |
| LLMNR | Multicast 224.0.0.252 | 5355/UDP | NON | Windows 2000 |

LLMNR = Link-local Multicast Name Resolution

MDNS = Multicast DNS

# LLMNR, NetBIOS et mDNS

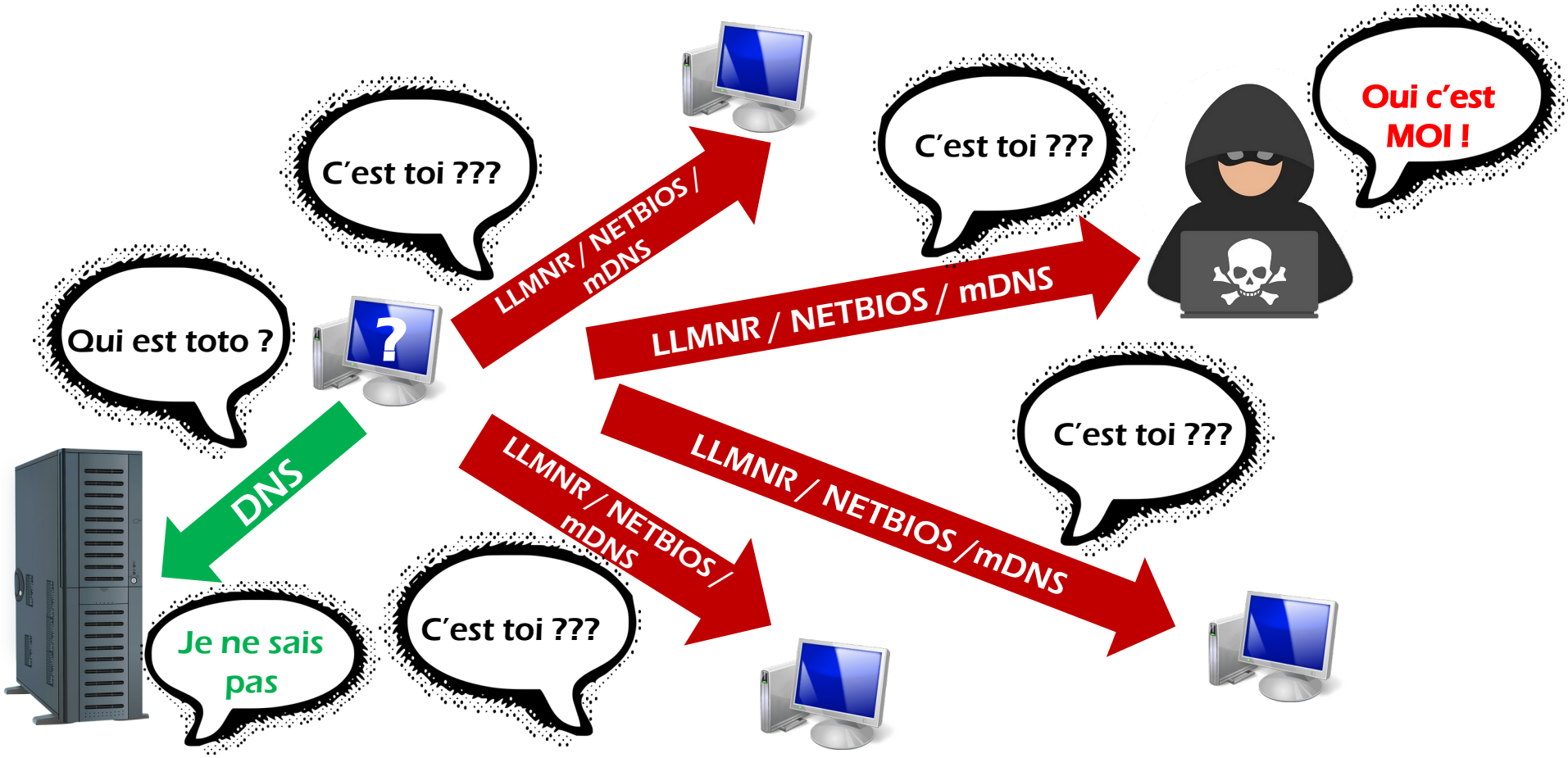
## Les paquets reçus par toutes les machines voisines :

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000 | 192.168.42.102 | 192.168.42.255 | NBNS | 92 | Name query NB TOTO<20> |
| 2 | 0.000667 | 192.168.42.102 | 224.0.0.251 | MDNS | 70 | Standard query 0x0000 AAAA toto.local, "QM" question |
| 3 | 0.001792 | 192.168.42.102 | 224.0.0.252 | LLMNR | 64 | Standard query 0xe469 A toto |
| 4 | 0.002379 | 192.168.42.102 | 224.0.0.252 | LLMNR | 64 | Standard query 0x5cfa AAAA toto |
| 5 | 0.370116 | 192.168.42.102 | 224.0.0.252 | LLMNR | 64 | Standard query 0x5cfa AAAA toto |
| 6 | 0.370129 | 192.168.42.102 | 224.0.0.252 | LLMNR | 64 | Standard query 0xe469 A toto |
| 7 | 0.660772 | 192.168.42.102 | 192.168.42.255 | NBNS | 92 | Name query NB TOTO<20> |
| 8 | 1.338044 | 192.168.42.102 | 192.168.42.255 | NBNS | 92 | Name query NB TOTO<20> |

```
▸ Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
▸ Ethernet II, Src: [redacted], Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▸ Internet Protocol Version 4, Src: 192.168.42.102, Dst: 192.168.42.255
▸ User Datagram Protocol, Src Port: 137, Dst Port: 137
▸ NetBIOS Name Service
```

```
0000  ff ff ff ff ff ff 08 00  27 4d 1e 76 08 00 45 00   ······ ·· 'M·v··E·
0010  00 4e 2d b2 00 00 80 11  36 37 c0 a8 2a 66 c0 a8   ·N-····· 67··*f··
0020  2a ff 00 89 00 89 00 3a  30 a5 9b 9c 01 10 00 01   *·····: 0·······
0030  00 00 00 00 00 00 20 46  45 45 50 46 45 45 50 43   ····· F EEPFEEPC
0040  41 43 41 43 41 43 41 43  41 43 41 43 41 43 41 43   ACACACAC ACACACAC
0050  41 43 41 43 41 43 41 00  00 20 00 01              ACACACA· · ··
```

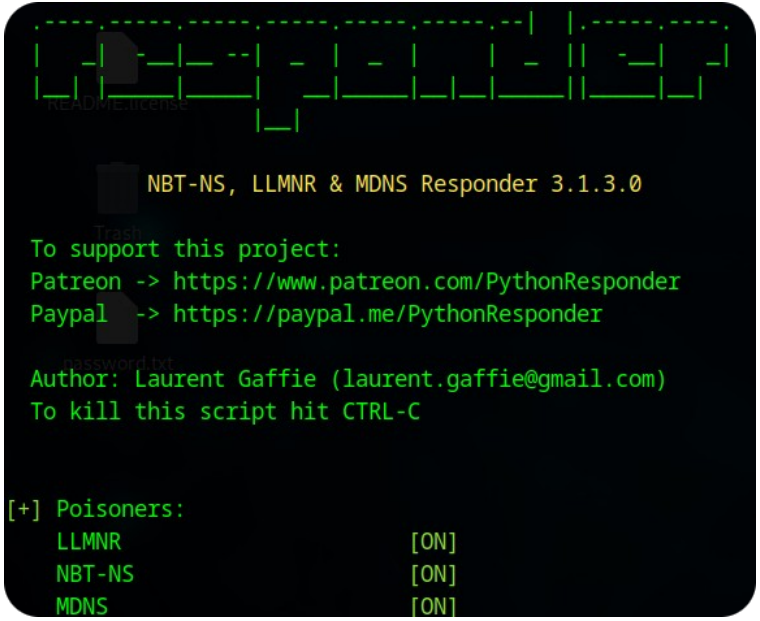
# Fonctionnement des protocoles LLMNR, NetBIOS et mDNS



# Exemple d'exploitation avec Responder

## Fonctionnement de Responder :

- Répond à toutes les requêtes LLMNR, NetBIOS et mDNS en fournissant l'adresse IP de la carte configurée en écoute sur la machine attaquante
- Présente des services connus tels que SMB, HTTP, HTTPS, FTP, RDP, LDAP...
- Enregistre toutes les tentatives d'authentification reçues, notamment les condensats NetNTLM de l'utilisateur victime envoyés automatiquement par Windows lors d'une tentative d'accès à un service (script, application qui tente de se connecter à un service qui n'est plus disponible)



# Exemple d'exploitation avec Responder

Je cherche le serveur SMB toto

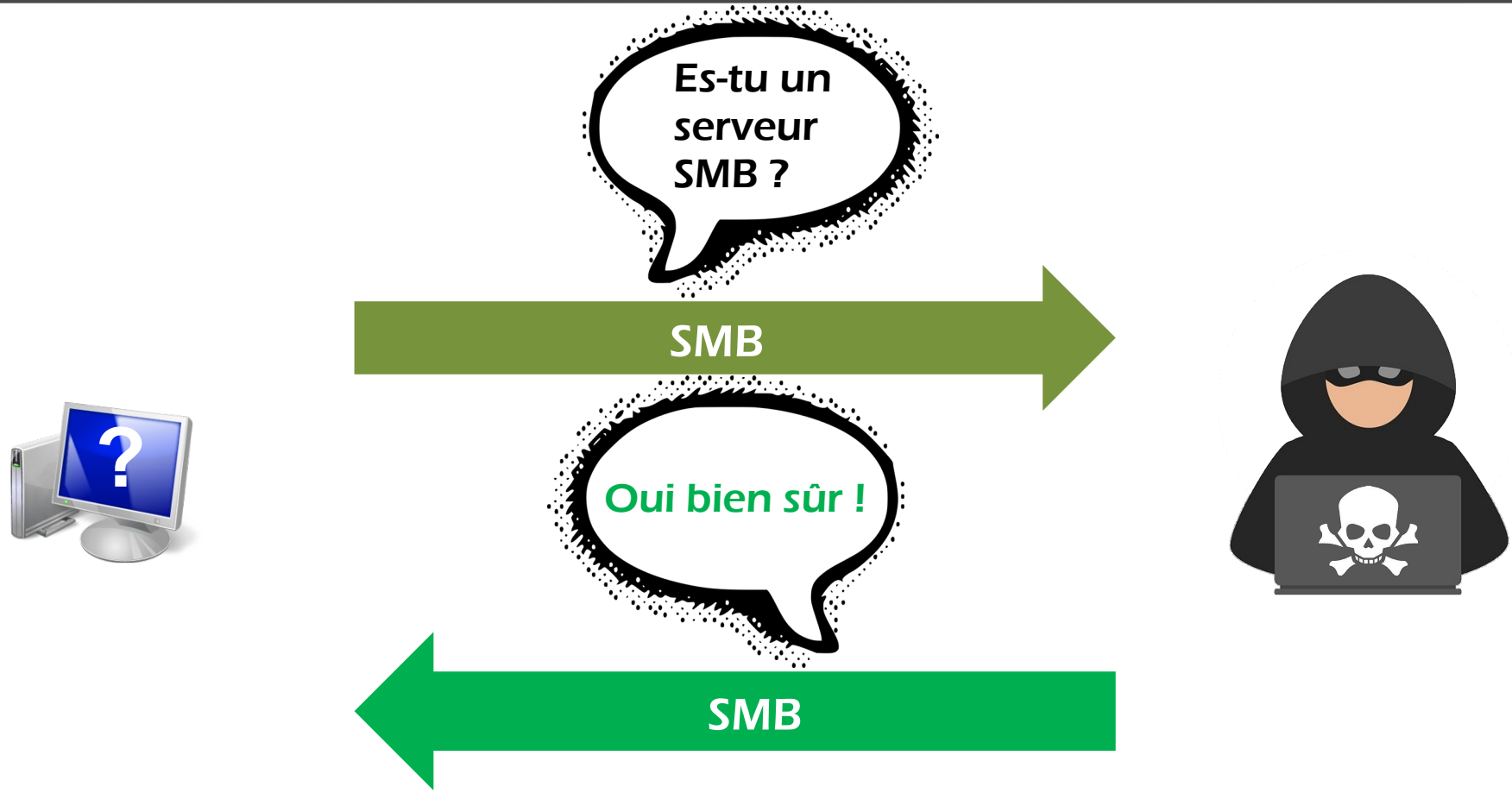
C'est toi ???

LLMNR / NetBIOS / mDNS

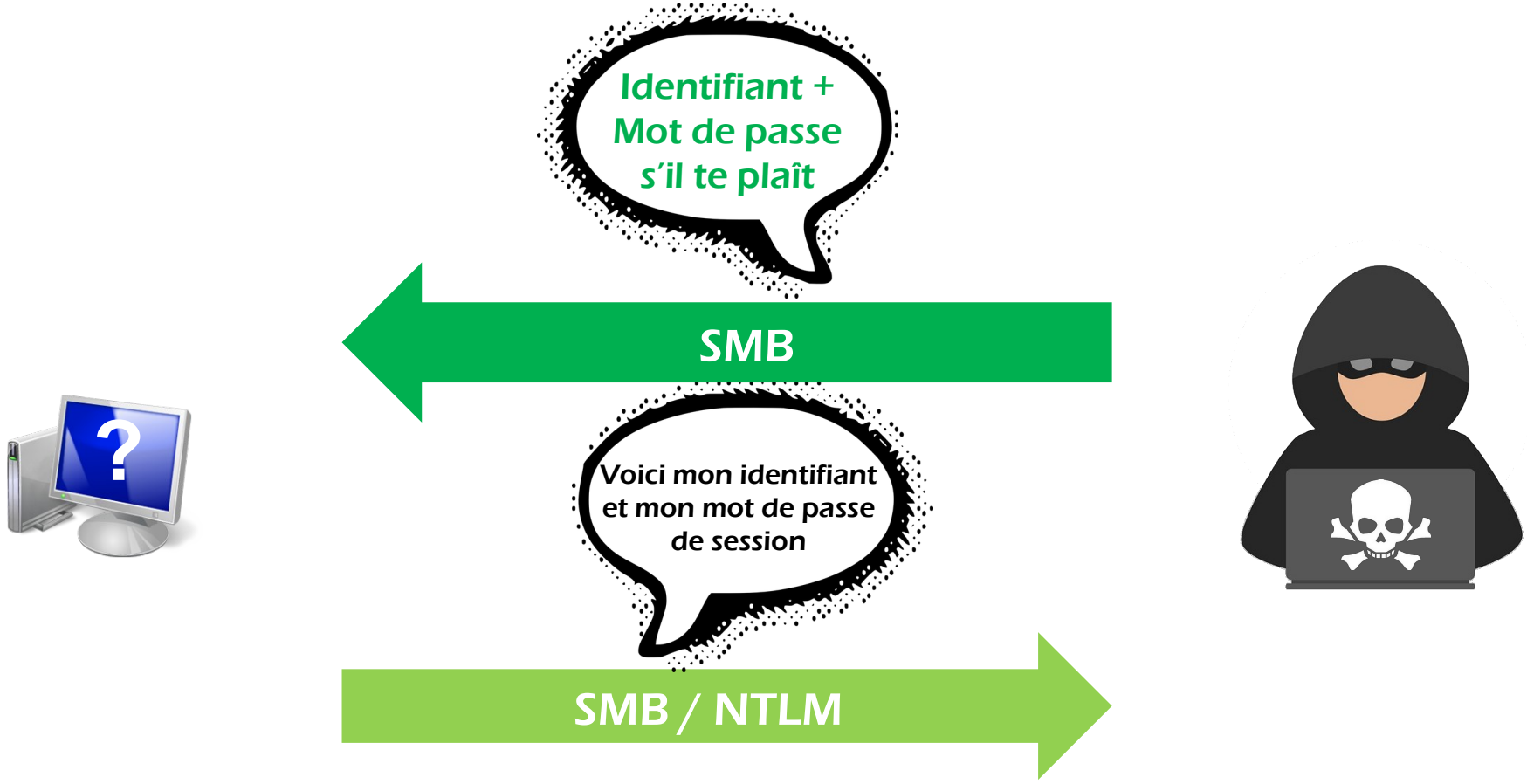
Oui c'est MOI !

LLMNR / NetBIOS / mDNS

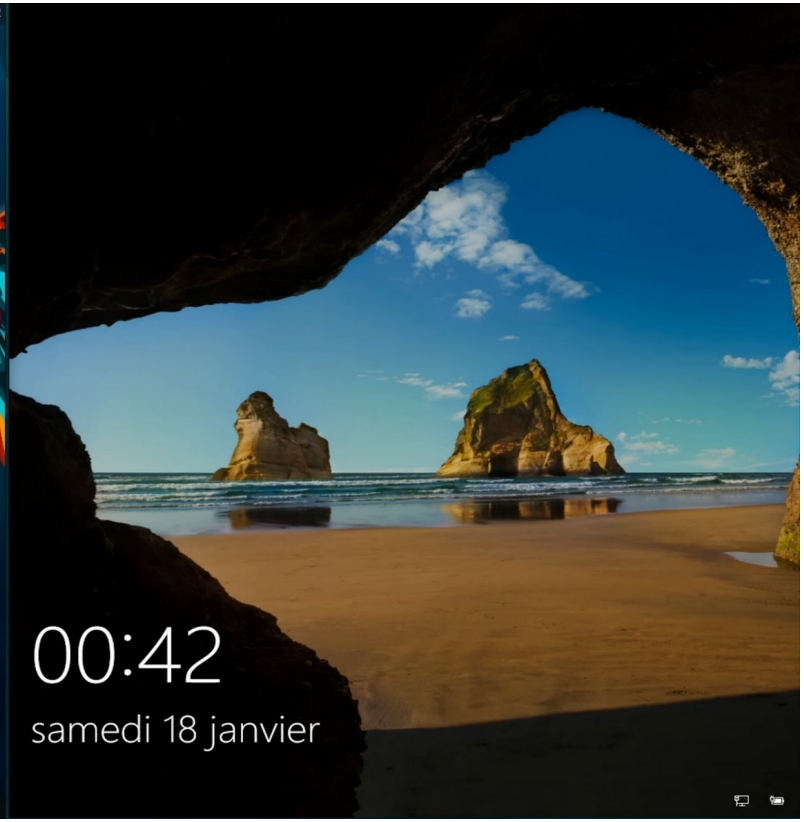
# Exemple d'exploitation avec Responder



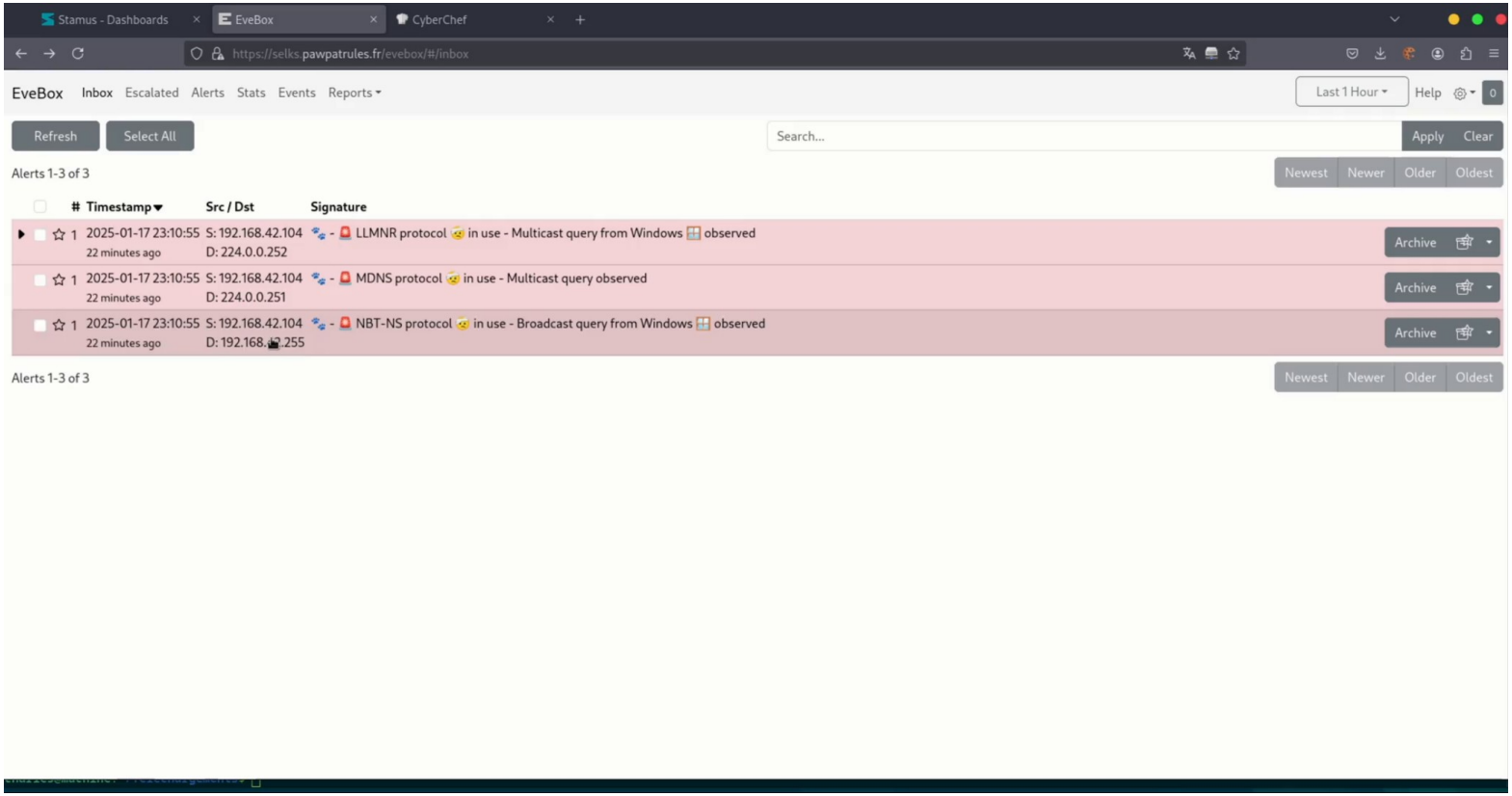
# Exemple d'exploitation avec Responder



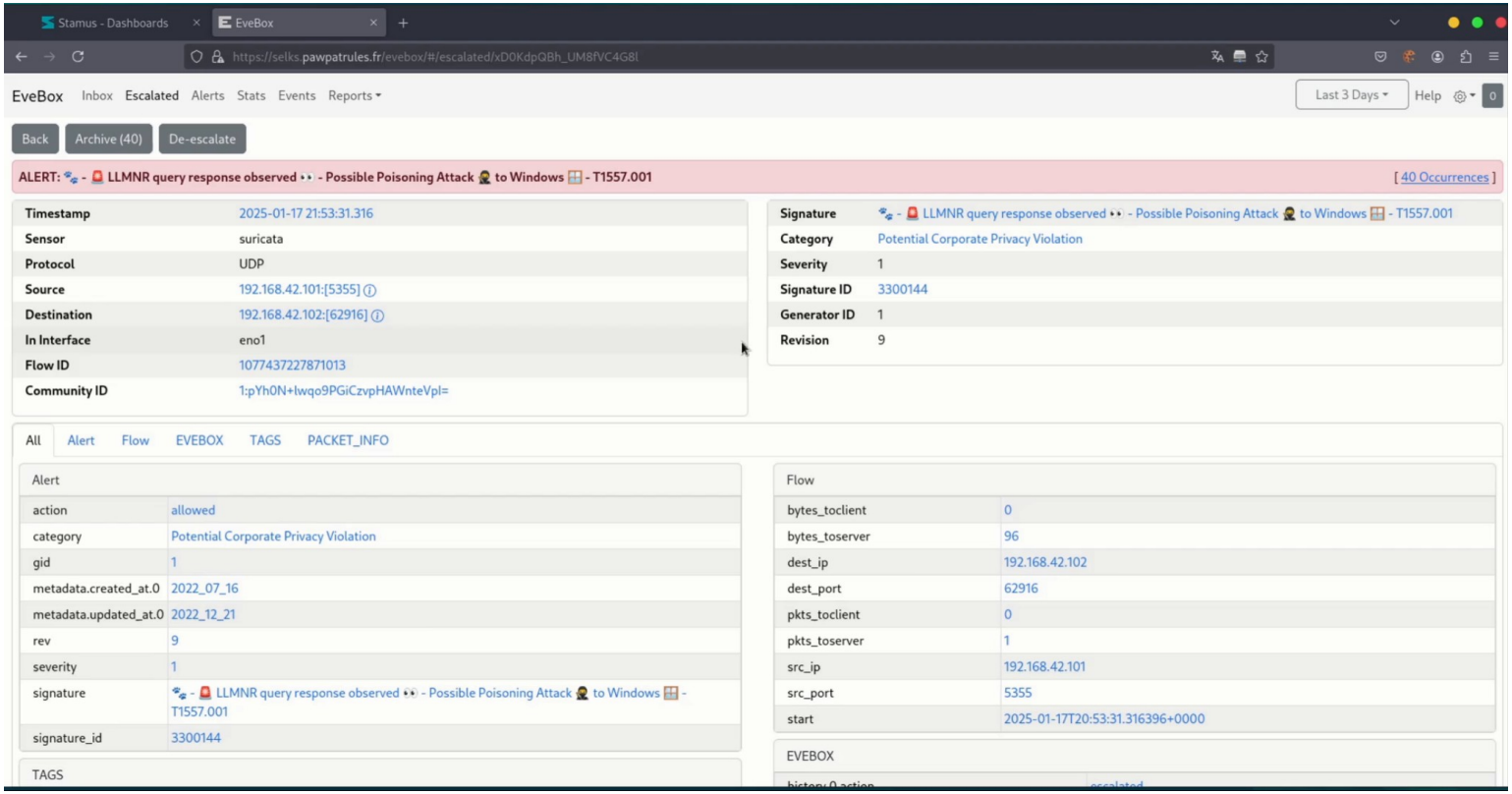
# Exemple d'exploitation avec Responder

# Détecter l'utilisation de ces protocoles sur le réseau

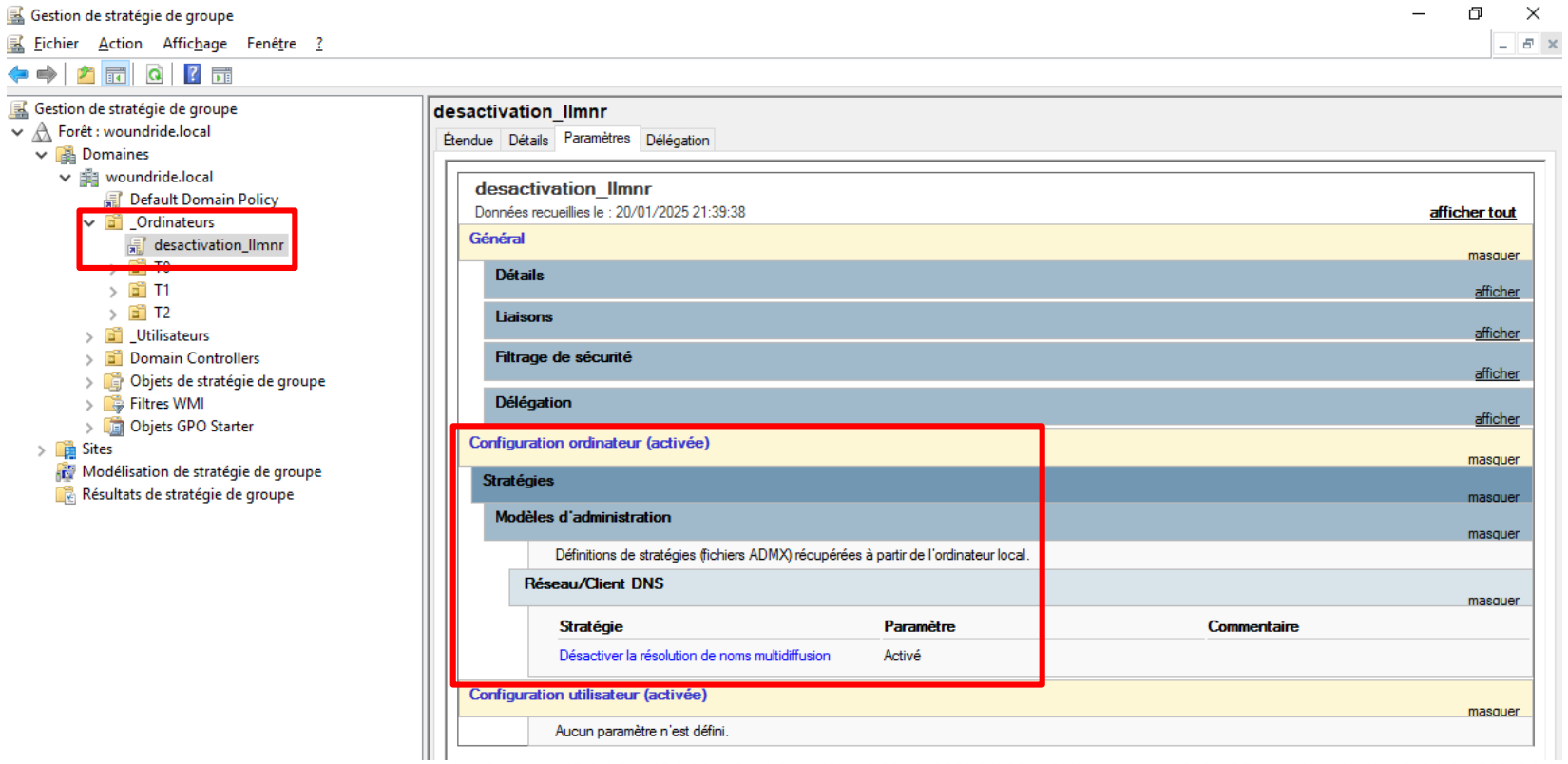


# Détecter l'utilisation de Responder sur le réseau



# Désactiver l'utilisation de LLMNR

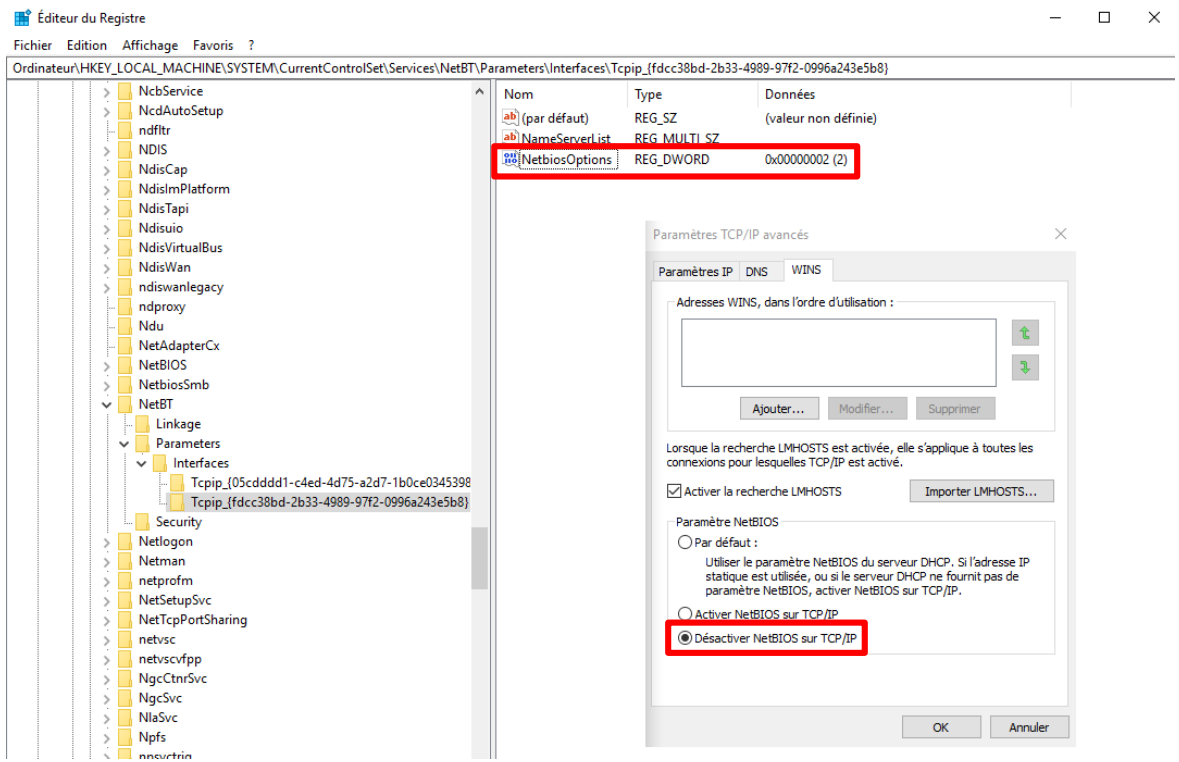
## Création d'une GPO :



# Désactiver l'utilisation de NetBIOS

## En pratique :

- Pas paramétrable dans les modèles ADMX
- La définition d'une clé de registre n'est pas possible car chaque carte réseau dispose d'un **identifiant (SID) différent et aléatoire**
- Contournement : lancement d'un script à l'arrêt du système. Au redémarrage suivant de la machine, le protocole est désactivé



# Désactiver l'utilisation de NetBIOS

## Script de désactivation de NetBIOS :

- Le script Powershell permettant de créer la clé de registre sur chaque carte réseau :

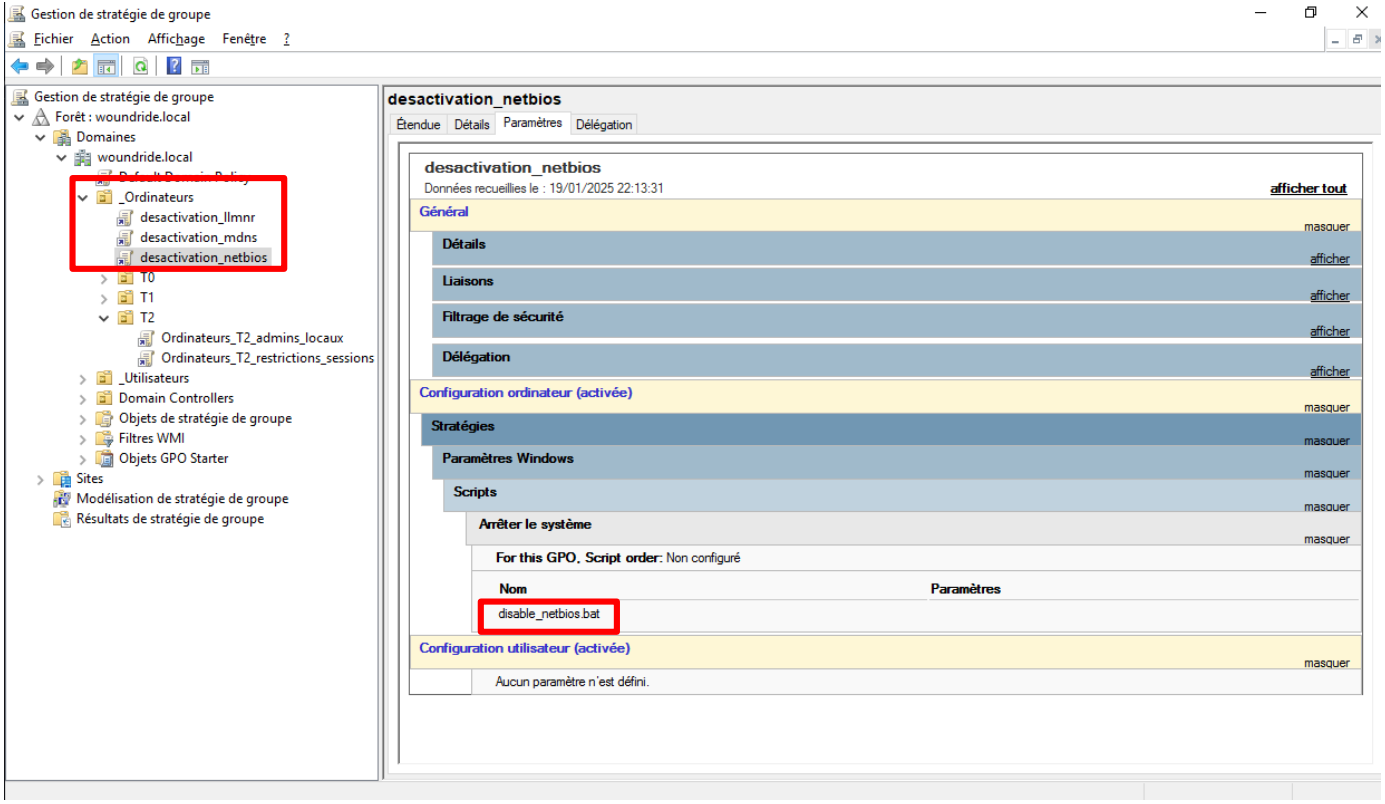
```
$regkey = "HKLM:SYSTEM\CurrentControlSet\services\NetBT\Parameters\Interfaces"
Get-ChildItem $regkey |foreach { Set-ItemProperty -Path "$regkey\$($_.pschildname)" -Name NetbiosOptions -Value 2 -Verbose}
set-executionpolicy restricted
exit
```

- Le script batch lancé sur la machine pour créer et exécuter le script Powershell ci-dessus (contenu du script encodé en base 64) :

```
powershell.exe
[System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('JHJlZ2tleSA9ICJlS0xNOlNZU1RFTVxDdXJyZW50Q29u
dHJvbFNldFxzZXJ2aWNlc1xOZXRCVFxQYXJhbWV0ZXJzXEludGVyZmFjZXMiCkdldC1DaGlsZEl0ZW0gJHJlZ2tleSB8Zm9yZWFjaCB7IF
NldC1JdGVtUHJvcGVydHkgLVBhdGggIiRyZWdrZXlcJCgkXy5wc2NoaWxkbmFtZSkiIC1OYW1lIE5IdGJpb3NPcHRpb25zIC1WYWx1ZS
AyIC1WZXJib3NlfQpzZXQtZXhlY3V0aW9ucG9saWN5IHJlc3RyaWN0ZWQKZXhpdA==')|| > C:\ProgramData\
disable_netbios.ps1&&powershell.exe -executionpolicy unrestricted -command C:\ProgramData\disable_netbios.ps1
```

# Désactiver l'utilisation de NetBIOS

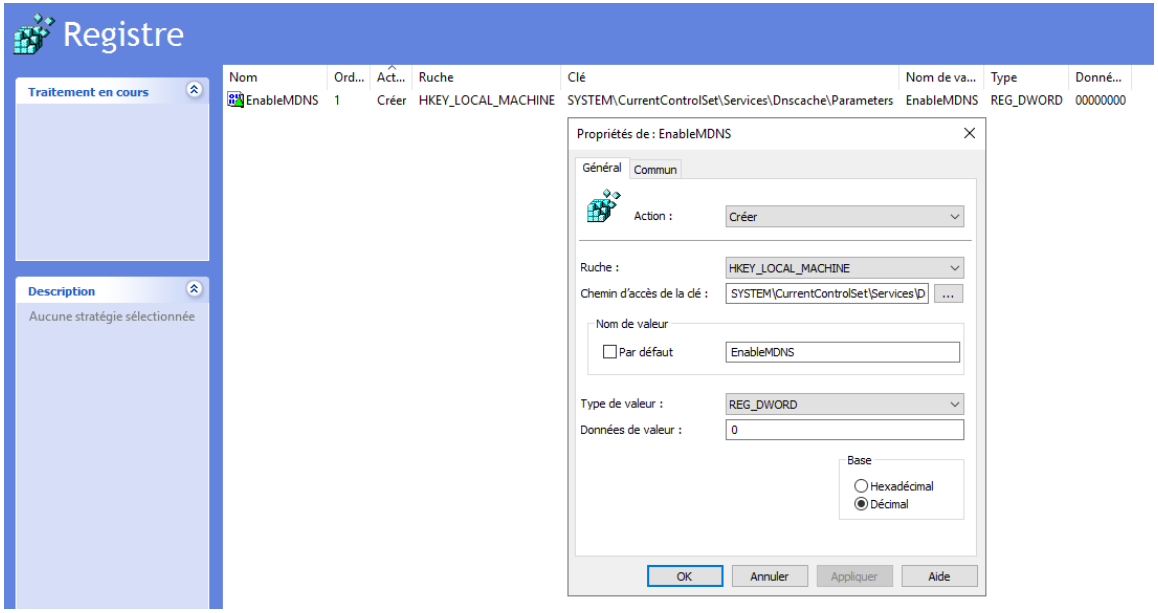
## Création d'une GPO permettant de lancer le script :



# Désactiver l'utilisation de mDNS

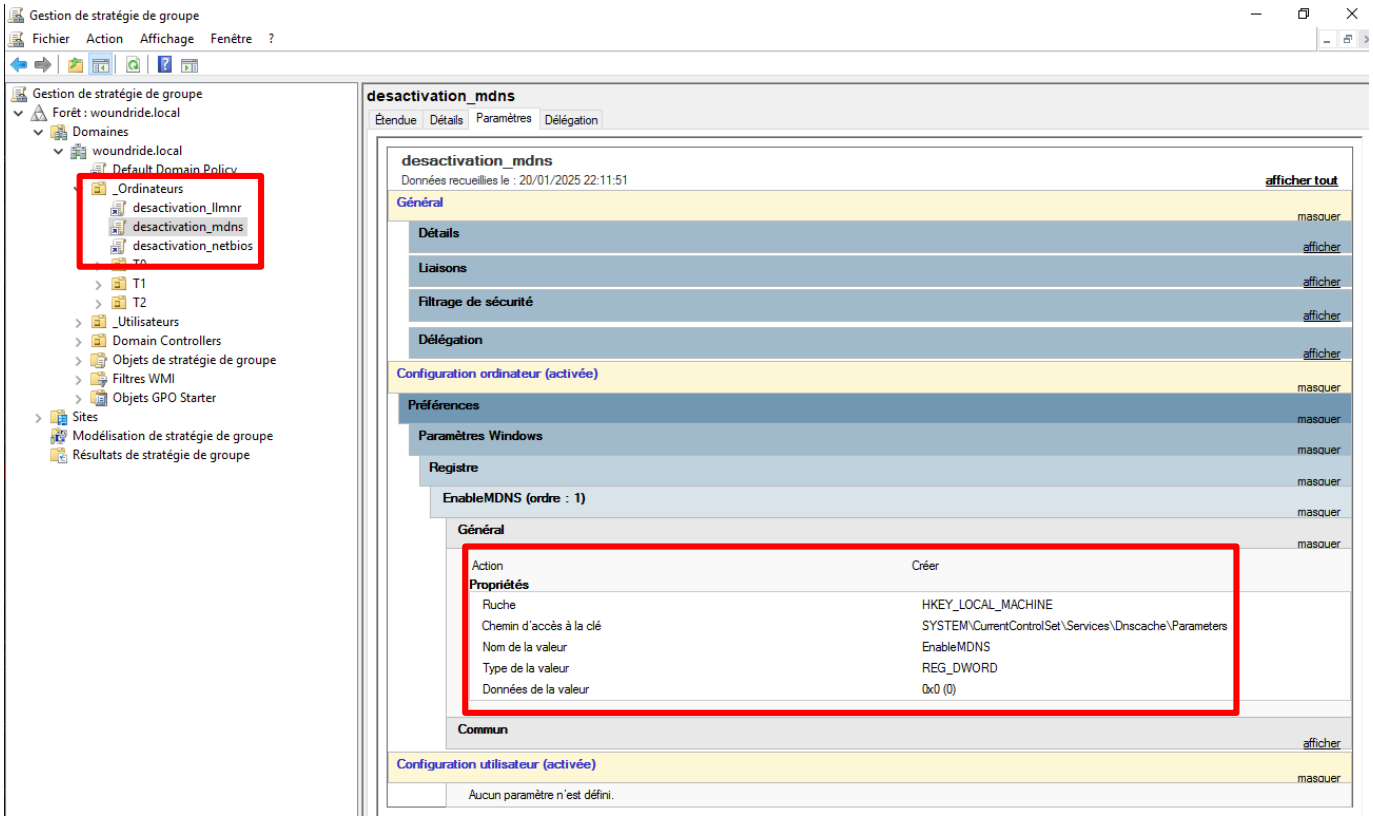
## En pratique :

- Pas paramétrable dans les modèles ADMX
- La définition d'une clé de registre est possible ici
- Création d'une GPO permettant de créer la clé de registre définissant le paramètre d'activation de mDNS à « désactivé »

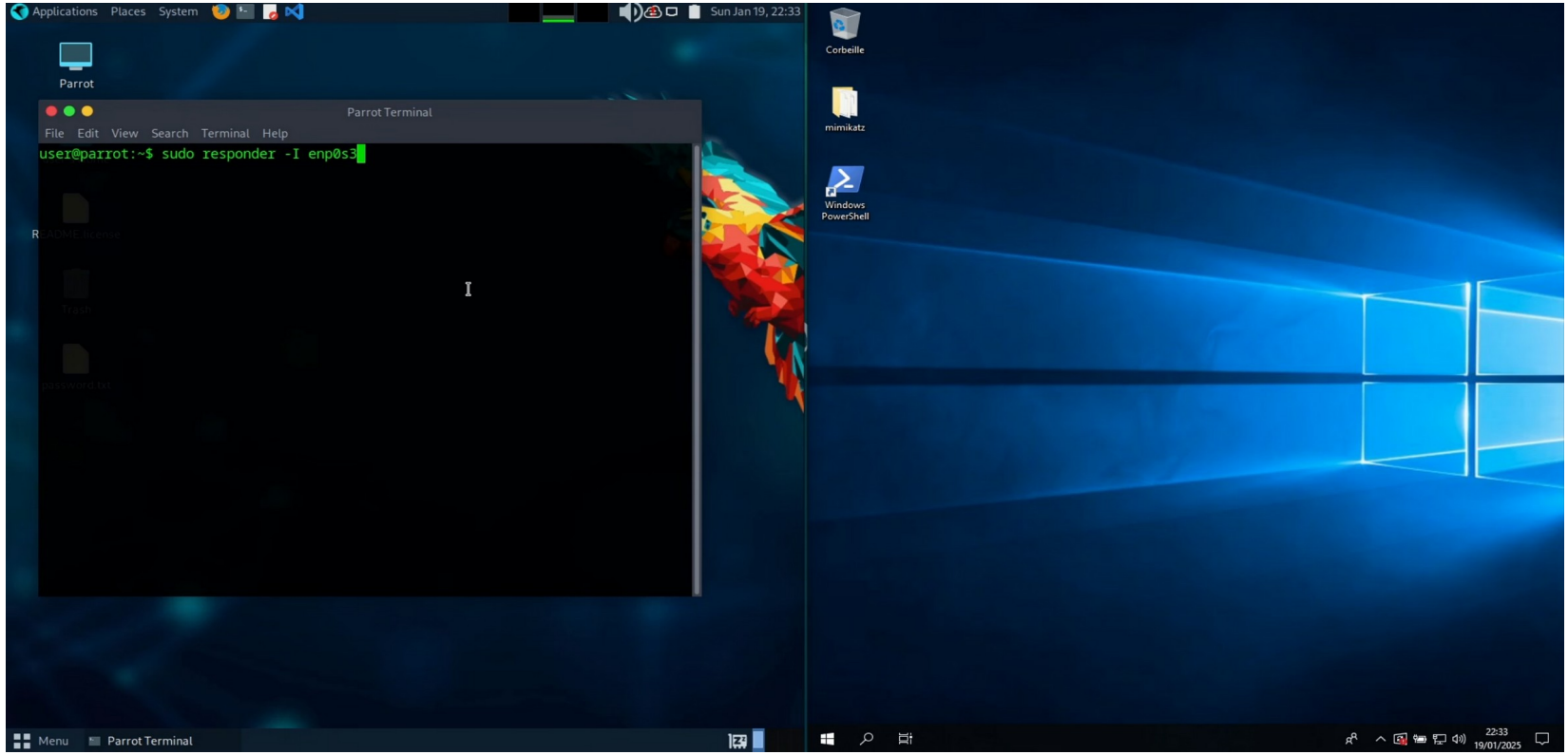


# Désactiver l'utilisation de mDNS

## Création d'une GPO :



# Tentative d'exploitation avec Responder contrée



# Ressources et outils utilisés

- Responder (Laurent GAFFIÉ) :
  https://github.com/lgandx/Responder
- Hashcat :
  https://hashcat.net/
- Suricata (OISF) :
  https://suricata.io/
- Clear NDR Community [anciennement SELKS] (Stamus Networks) :
  https://www.stamus-networks.com/clear-ndr-community
- EveBox (Jason Ish) :
  https://evebox.org/
- PawPatrules (Charles BLANC-ROLIN) :
  https://pawpatrules.fr/
- Script de désactivation de NetBIOS (Charles BLANC-ROLIN) :
  https://github.com/woundride/scripts_for_active_directory/blob/main/disable_netbios.bat