



Les protocoles réseau à risque actifs par défaut

(environnement Windows)





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

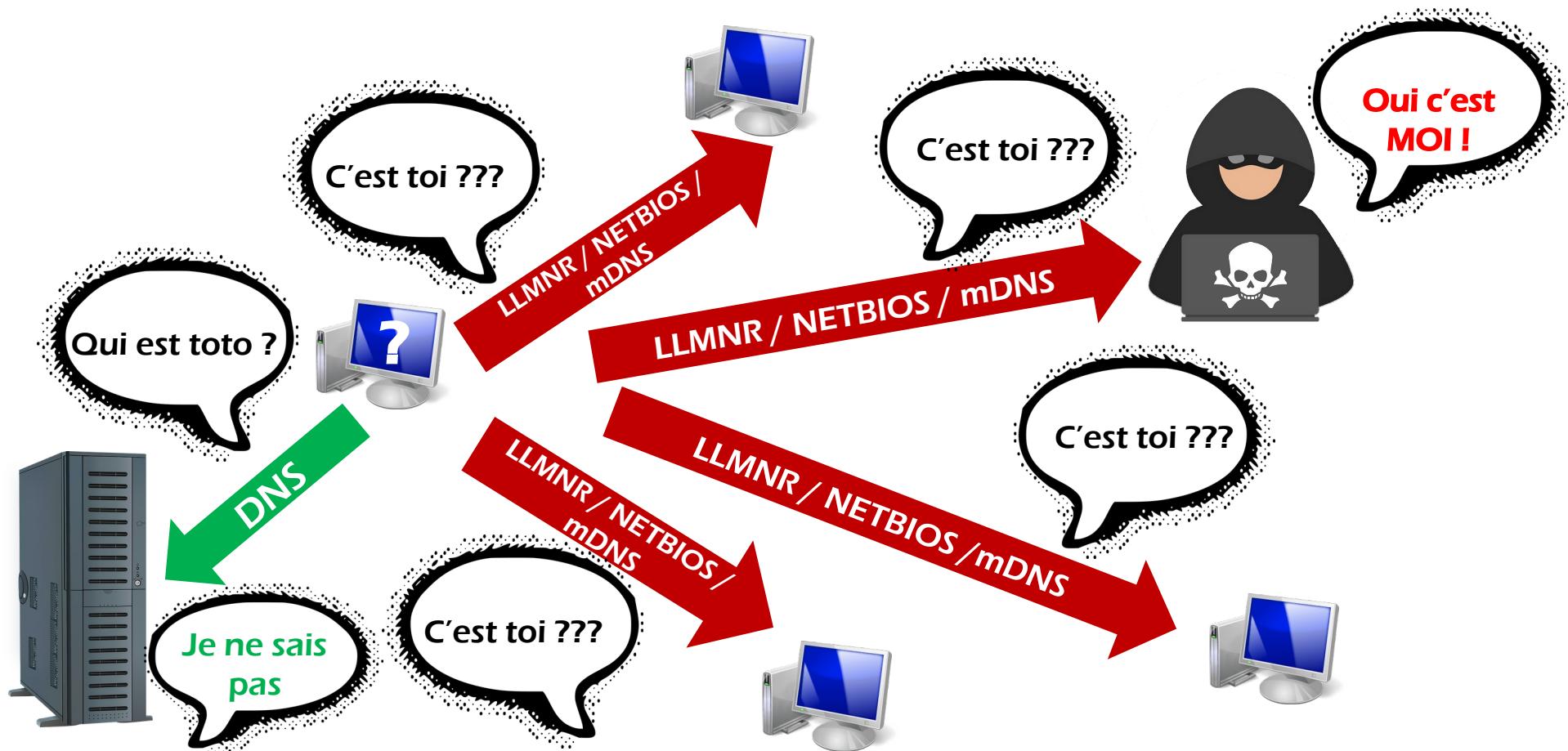
Les paquets reçus par toutes les machines voisines :

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] ([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 20	46 45 45 50 46 45 45 50 43	-----F	EEPFEPC
0040	41 43 41 43 41 43	41 43 41 43 41 43 41 43	ACACACAC	ACACACAC
0050	41 43 41 43 41 43	00 00 20 00 01	ACACACA· · · · ·	

Fonctionnement des protocoles LLMNR, NetBIOS et mDNS

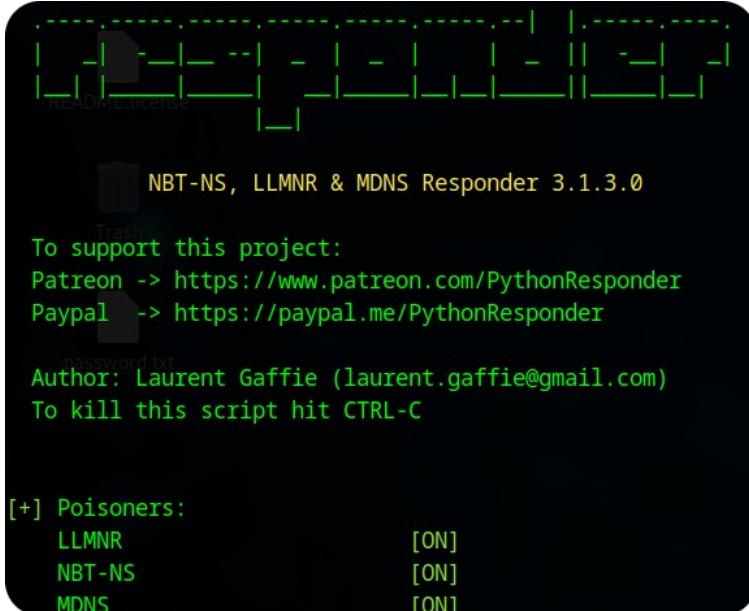




Exemple d'exploitation avec Responder

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)



NBT-NS, LLMNR & MDNS Responder 3.1.3.0

Trach

To support this project:
Patreon -> <https://www.patreon.com/PythonResponder>
Paypal -> <https://paypal.me/PythonResponder>

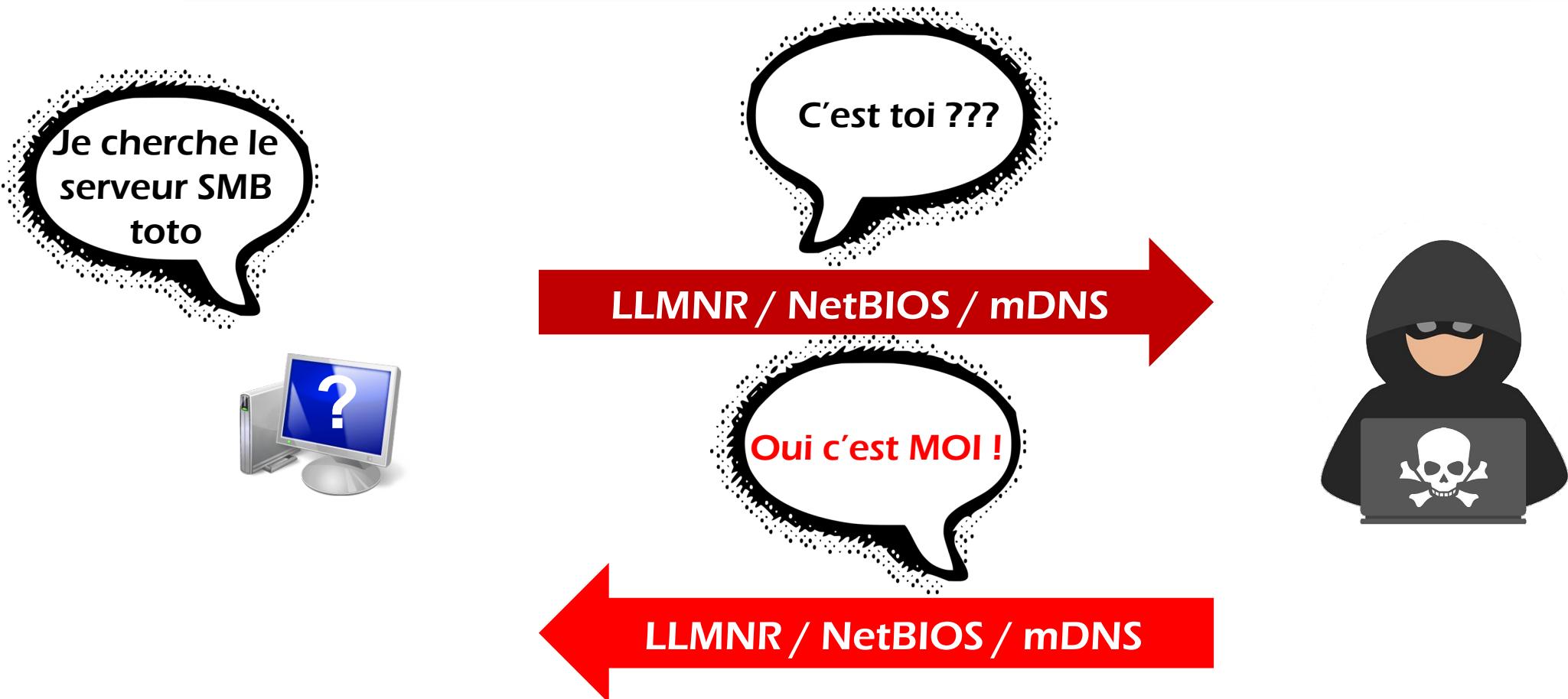
password.txt

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

[+] Poisoners:

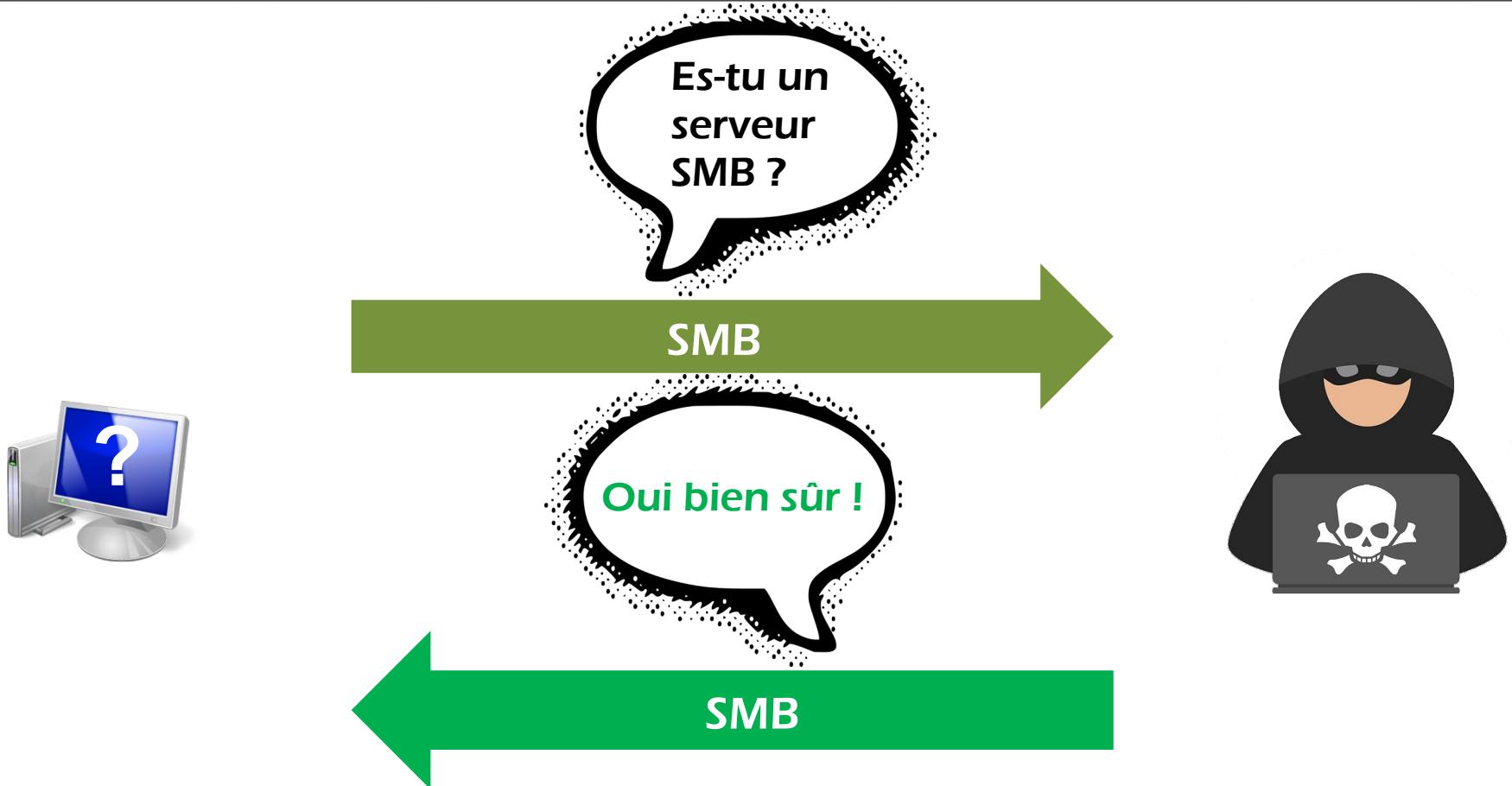
LLMNR	[ON]
NBT-NS	[ON]
MDNS	[ON]

Exemple d'exploitation avec Responder



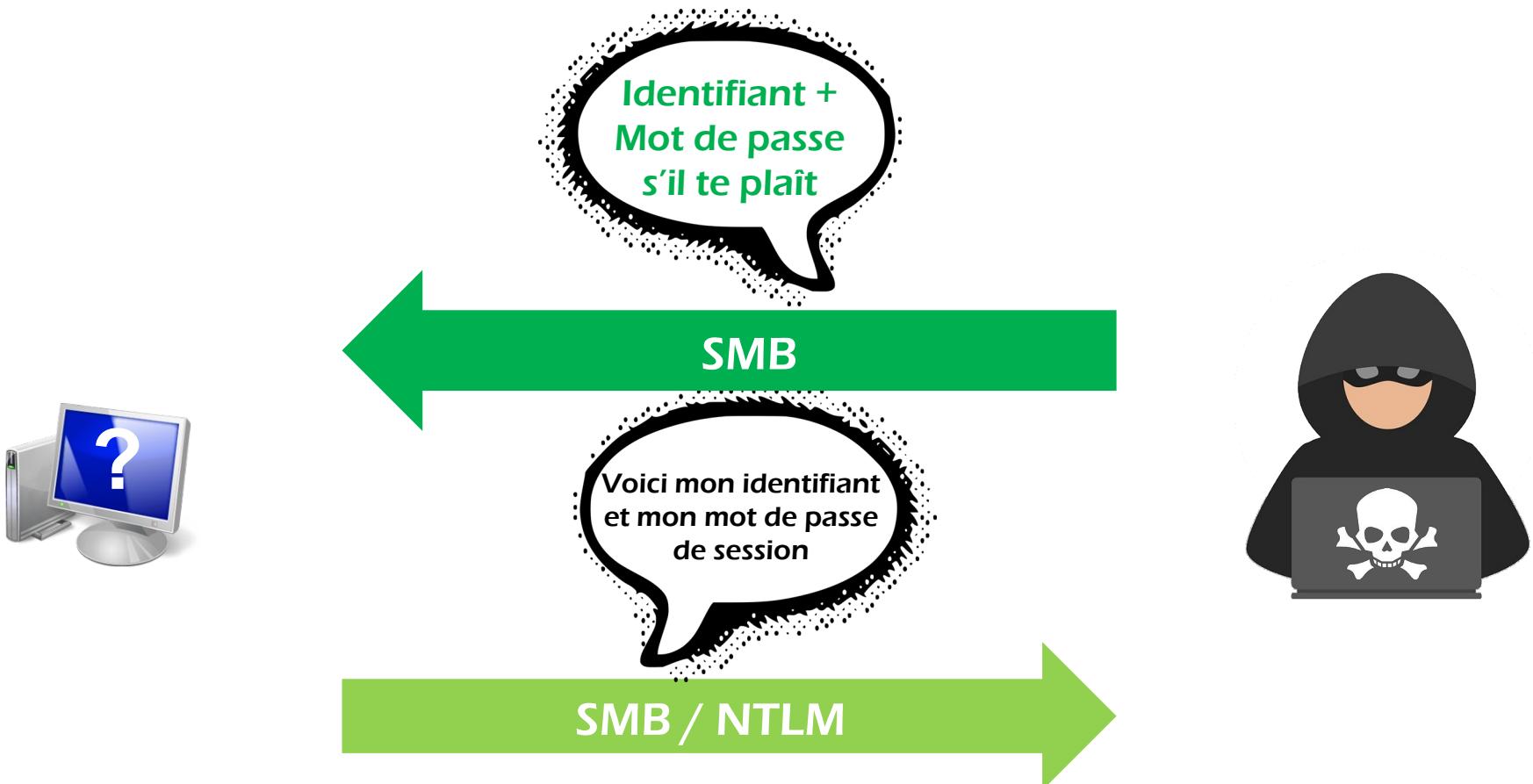


Exemple d'exploitation avec Responder

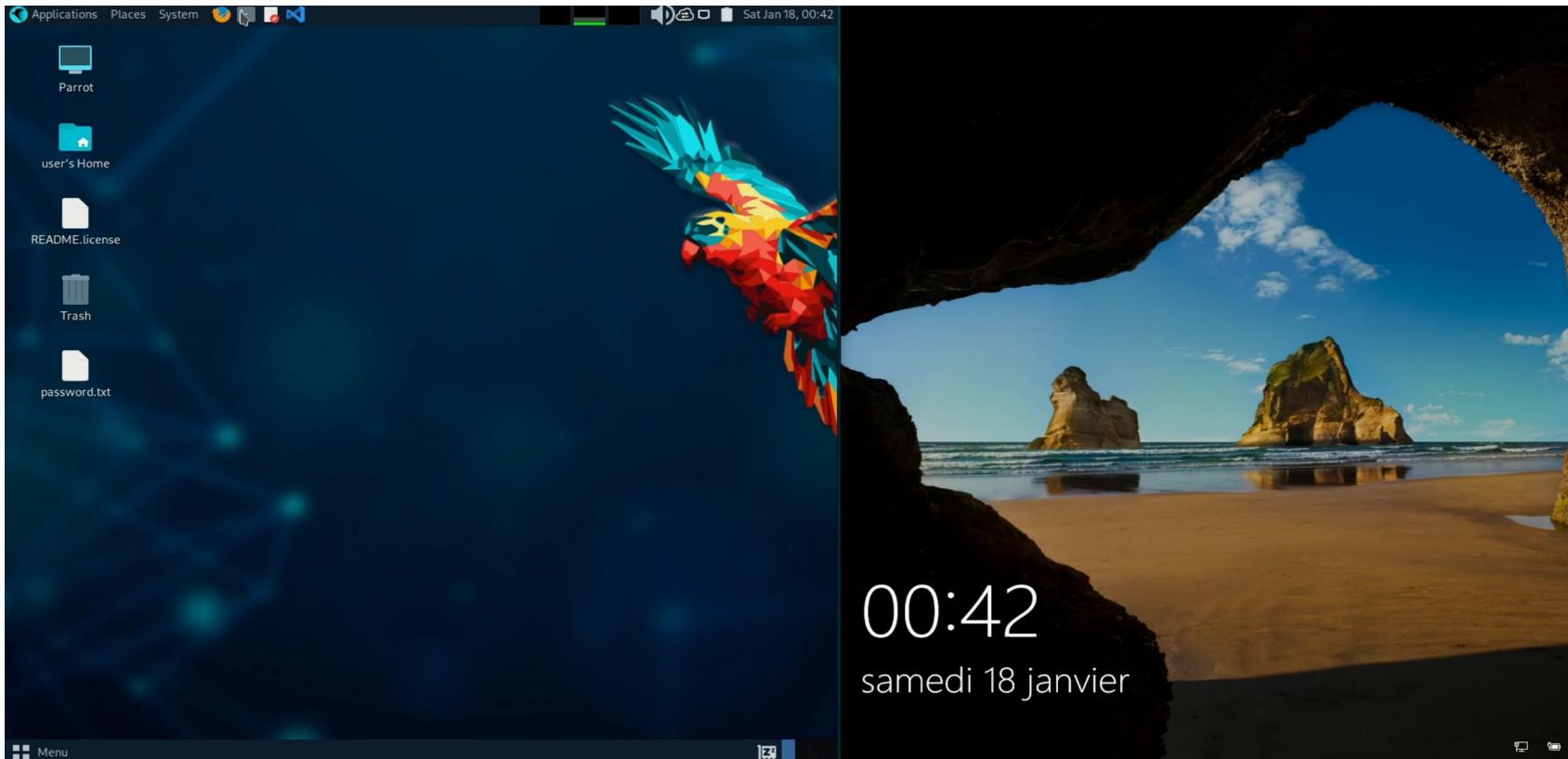




Exemple d'exploitation avec Responder



Exemple d'exploitation avec Responder





Déetecter l'utilisation de ces protocoles sur le réseau



#	Timestamp	Src / Dst	Signature
1	2025-01-17 23:10:55	S: 192.168.42.104 22 minutes ago	D: 224.0.0.252 LLMNR protocol in use - Multicast query from Windows observed
1	2025-01-17 23:10:55	S: 192.168.42.104 22 minutes ago	D: 224.0.0.251 MDNS protocol in use - Multicast query observed
1	2025-01-17 23:10:55	S: 192.168.42.104 22 minutes ago	D: 192.168.42.255 NBT-NS protocol in use - Broadcast query from Windows observed





Déetecter l'utilisation de Responder sur le réseau



S Stamus - Dashboards x EveBox + https://selks.pawpatrulles.fr/evebox/#/escalated/xD0KdpQBh_UM8fVC4G8l

EveBox Inbox Escalated Alerts Stats Events Reports Last 3 Days Help 0

Back Archive (40) De-escalate

ALERT: - LLMNR query response observed - Possible Poisoning Attack to Windows - T1557.001 [40 Occurrences]

Timestamp	2025-01-17 21:53:31.316
Sensor	suricata
Protocol	UDP
Source	192.168.42.101:[5355] ⓘ
Destination	192.168.42.102:[62916] ⓘ
In Interface	eno1
Flow ID	1077437227871013
Community ID	1:pYh0N-lwqo9PGiCzvpHAWnteVpl=

Signature	- LLMNR query response observed - Possible Poisoning Attack to Windows - T1557.001
Category	Potential Corporate Privacy Violation
Severity	1
Signature ID	3300144
Generator ID	1
Revision	9

All Alert Flow EVEBOX TAGS PACKET_INFO

Alert	
action	allowed
category	Potential Corporate Privacy Violation
gid	1
metadata.created_at	2022_07_16
metadata.updated_at	2022_12_21
rev	9
severity	1
signature	- LLMNR query response observed - Possible Poisoning Attack to Windows - T1557.001
signature_id	3300144

Flow	
bytes_toclient	0
bytes_toserver	96
dest_ip	192.168.42.102
dest_port	62916
pkts_toclient	0
pkts_toserver	1
src_ip	192.168.42.101
src_port	5355
start	2025-01-17T20:53:31.316396+0000

EVEBOX
history: 0 action
escalated



Désactiver l'utilisation de LLMNR

Création d'une GPO :

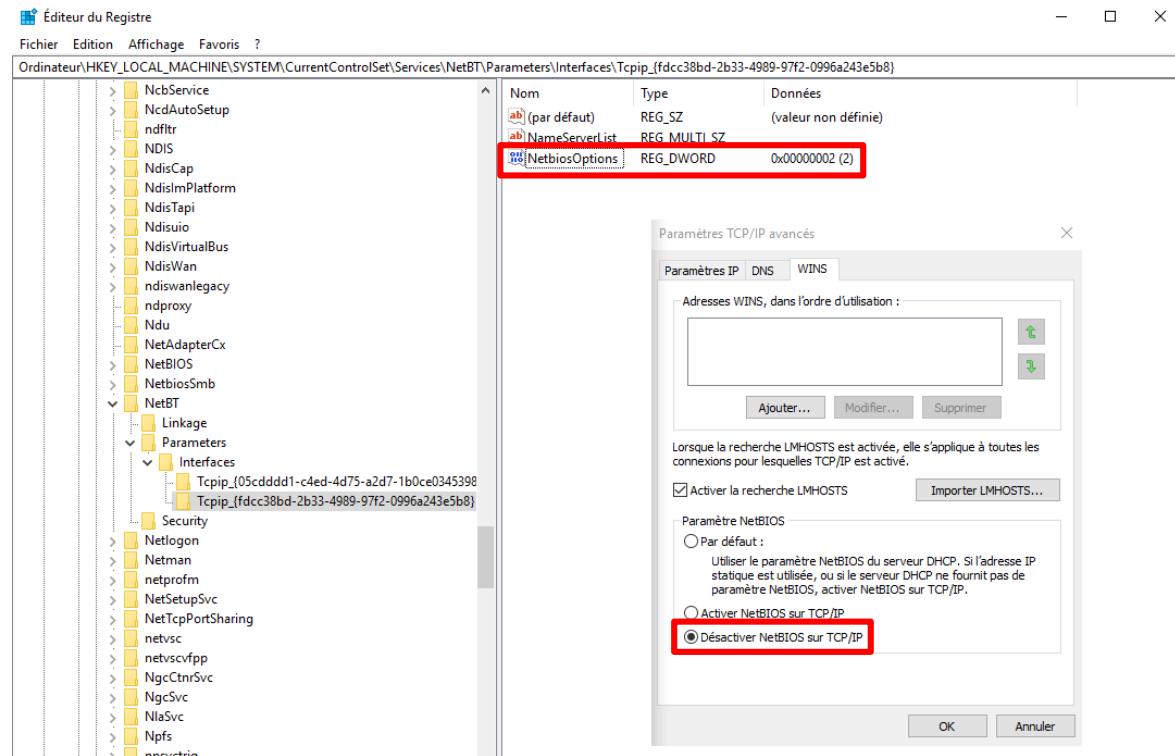
The screenshot shows the 'Gestion de stratégie de groupe' (Group Policy Management) console. On the left, the navigation pane shows the 'Forêt : woundride.local' and 'Domaines' section, with 'woundride.local' expanded. Inside 'woundride.local', a new GPO named 'desactivation_llmnr' is selected and highlighted with a red box. The main pane displays the properties of this GPO. The 'Général' tab is selected, showing the GPO name and last collection time (20/01/2025 21:39:38). The 'Configuration ordinateur (activée)' section is expanded and highlighted with a red box, showing the 'Stratégies' and 'Modèles d'administration' sections. The 'Modèles d'administration' section contains a note: 'Définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordinateur local.' The 'Réseau/Client DNS' section shows a single policy: 'Désactiver la résolution de noms multidiffusion' with the value 'Activé'. The 'Configuration utilisateur (activée)' section is empty.

Stratégie	Paramètre	Commentaire
Désactiver la résolution de noms multidiffusion	Activé	

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) :

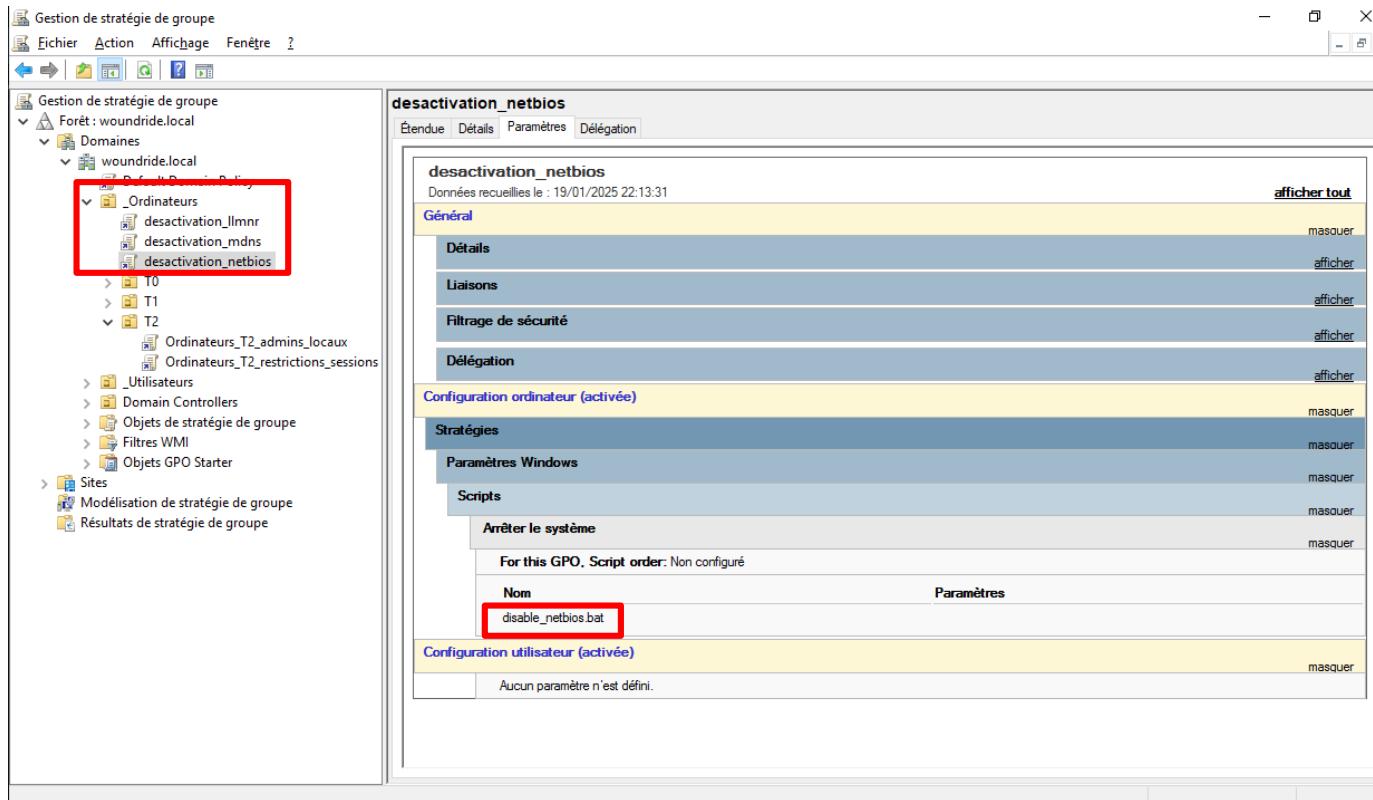
powershell.exe

```
[System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('JHJIZ2tIeSA9ICJIS0xNOINZU1RFTVxDdXJyZW50Q29u
dHJvbFNIdFxzZXJ2aWNlc1xOZXRCVFxQYXJhbWV0ZXJzXEIudGVyZmFjZXMiCkdIdC1DaGIsZEI0ZW0gJHJIZ2tIeSB8Zm9yZWFrjaCB7IF
NIdC1JdGVtUHJvcGVydHkgLBhdGggliRyZWdrZXlcJCgkXy5wc2NoaWxkbmFtZSkilC1OYW1IIE5IdGJpb3NPcHRpb25zIC1WYWx1ZS
AylC1WZXJib3NlfcOpzZXQtZXhIY3V0aW9ucG9saWN5IHJlc3RyaWN0ZWQKZXhpda==')) > C:\ProgramData\disable_netbios.ps1
&& powershell.exe -executionpolicy unrestricted -command C:\ProgramData\disable_netbios.ps1
```



Désactiver l'utilisation de NetBIOS

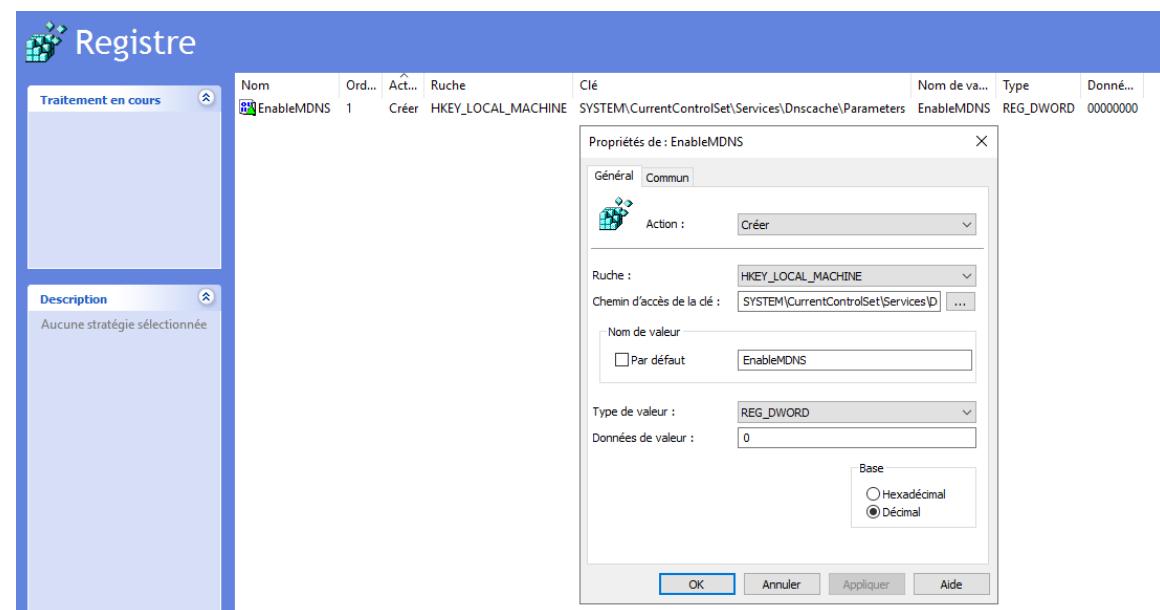
Création d'une GPO permettant de lancer le script :



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 »



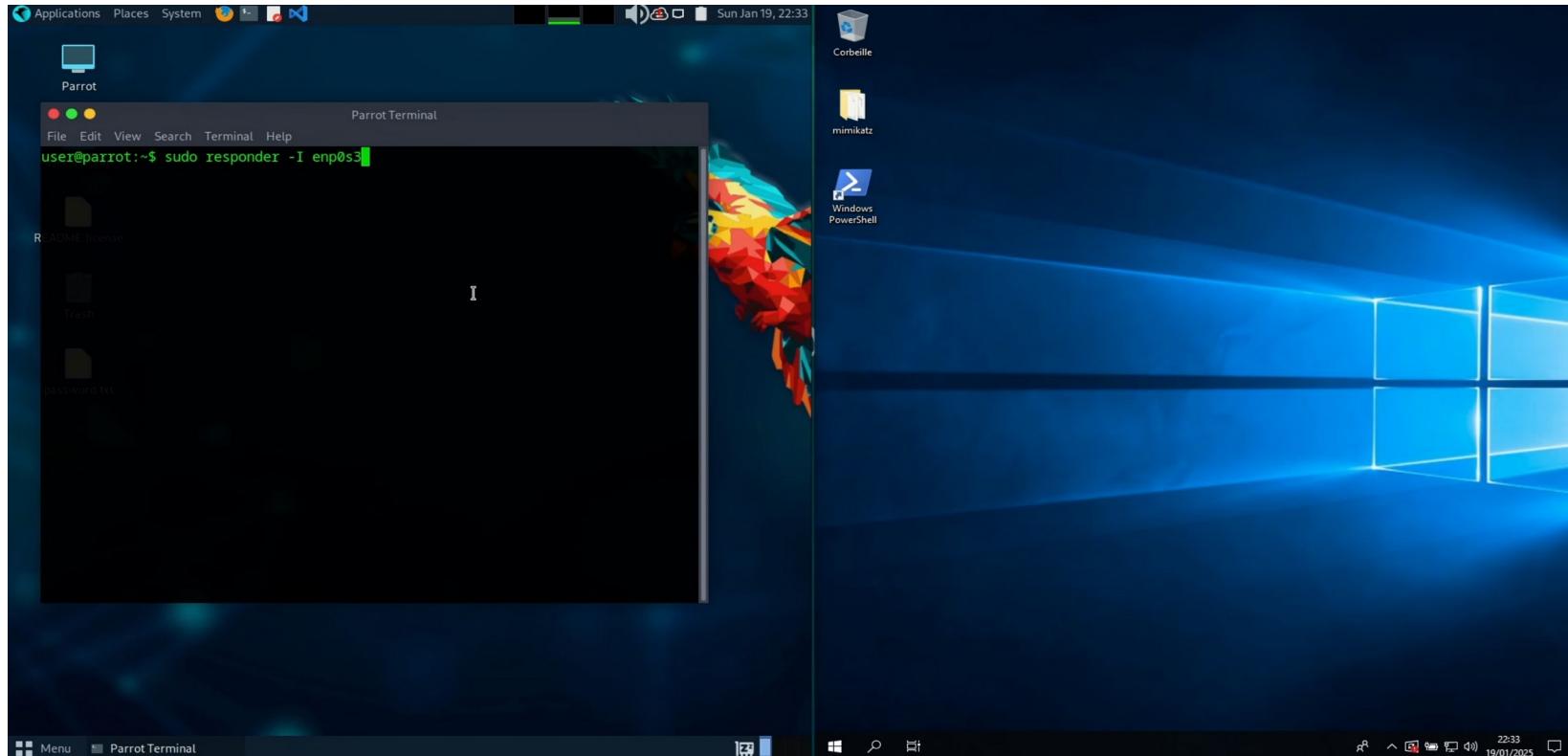
Désactiver l'utilisation de mDNS

Création d'une GPO :

The screenshot shows the 'Gestion de stratégie de groupe' (Group Policy Management) console. On the left, the navigation pane shows the forest 'woundride.local' and its domains, with 'woundride.local' expanded. Under 'woundride.local', a new GPO named 'desactivation_mdns' is selected. This GPO is highlighted with a red box. The main pane displays the properties of this GPO, with the 'Paramètres' (Parameters) tab selected. The 'Paramètres Windows' (Windows Parameters) section is expanded, showing a policy named 'EnableMDNS (ordre : 1)'. This policy is also highlighted with a red box. The 'Action' column for this policy shows the following details:

Action	Créer
Ruche	HKEY_LOCAL_MACHINE
Chemin d'accès à la clé	SYSTEM\CurrentControlSet\Services\Onscache\Parameters
Nom de la valeur	EnableMDNS
Type de la valeur	REG_DWORD
Données de la valeur	0x0 (0)

Tentative d'exploitation avec Responder contrée





Ressources et outils utilisés

- **Responder (Laurent GAFFIÉ) :**
<https://github.com/Igandx/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

