



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: , Dst: Broadcast (ff:ff:ff:ff:ff:ff)

▶ Internet Protocol Version 4, Src: 192.168.42.102, Dst: 192.168.42.255

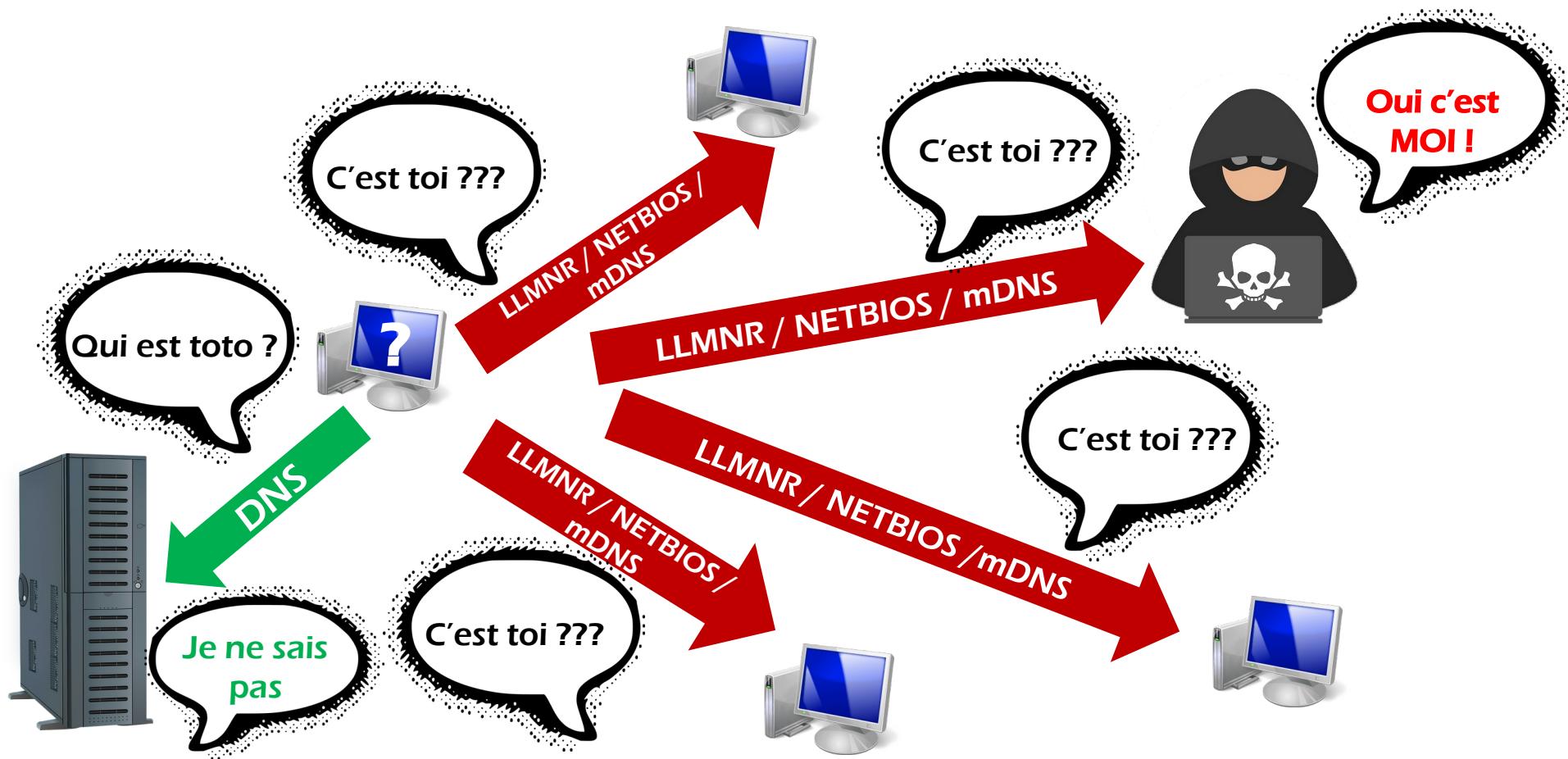
▶ User Datagram Protocol, Src Port: 137, Dst Port: 137

▶ 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





```

[+] NBT-NS, LLMNR & MDNS Responder 3.1.3.0
To support this project:
Patreon -> https://www.patreon.com/PythonResponder
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]

```



Exemple d'exploitation avec Responder

Je cherche le
serveur SMB
toto



C'est toi ???

LLMNR / NetBIOS / mDNS

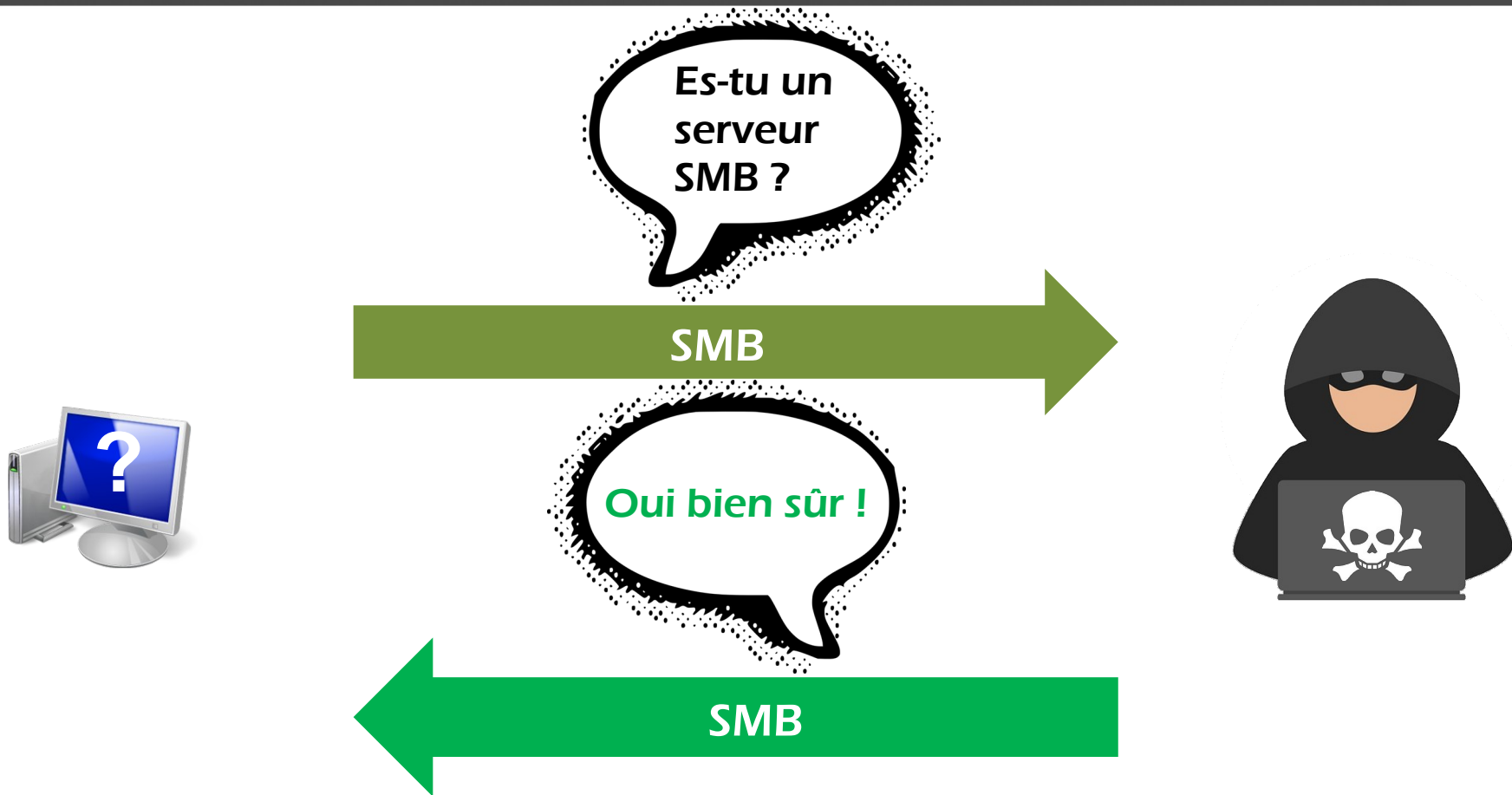
Oui c'est MOI !

LLMNR / NetBIOS / mDNS



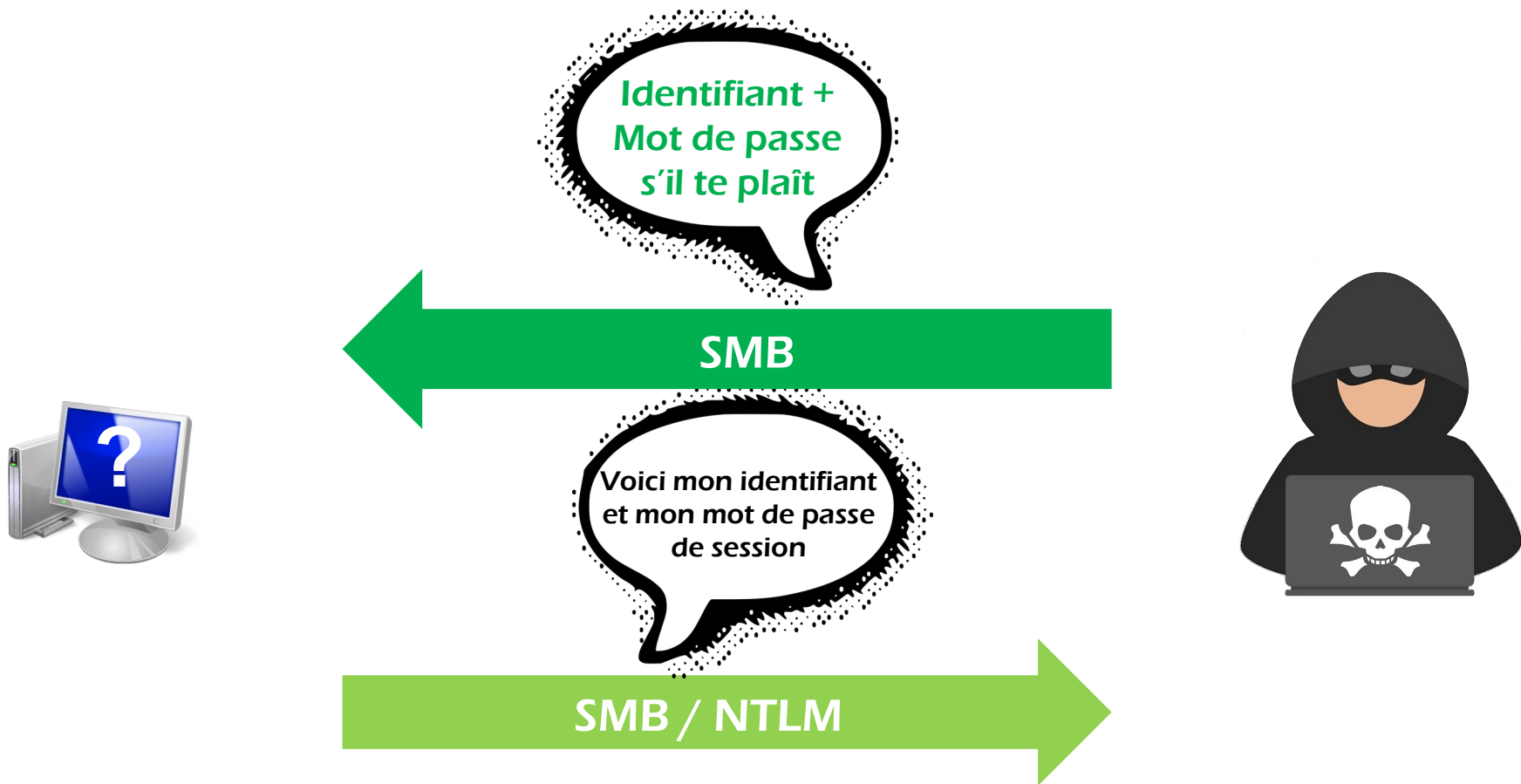


Exemple d'exploitation avec Responder



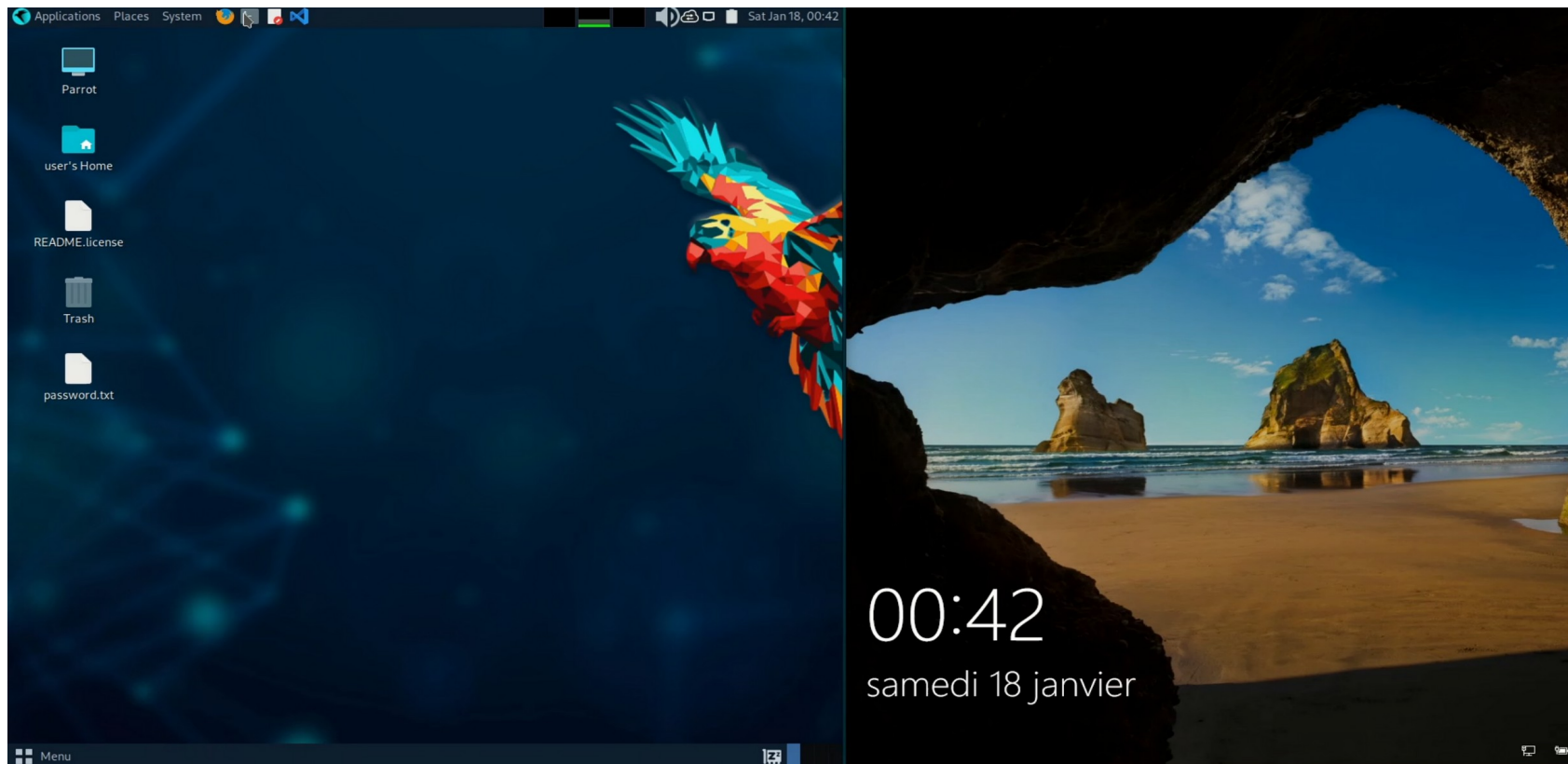


Exemple d'exploitation avec Responder





Exemple d'exploitation avec Responder





Détecter l'utilisation de ces protocoles sur le réseau



Stamus - Dashboards x EveBox x CyberChef x +

← → ↺ https://selks.pawpatrules.fr/evebox/#/inbox

EveBox Inbox Escalated Alerts Stats Events Reports ▾

Last 1 Hour ▾ Help ⚙ 0

Refresh Select All Search... Apply Clear

Alerts 1-3 of 3

Newest Newer Older Oldest

<input type="checkbox"/>	#	Timestamp ▾	Src / Dst	Signature	
<input checked="" type="checkbox"/>	1	2025-01-17 23:10:55 22 minutes ago	S: 192.168.42.104 D: 224.0.0.252	LLMNR protocol 🚩 in use - Multicast query from Windows 🚩 observed	Archive 🗄 ▾
<input type="checkbox"/>	1	2025-01-17 23:10:55 22 minutes ago	S: 192.168.42.104 D: 224.0.0.251	MDNS protocol 🚩 in use - Multicast query observed	Archive 🗄 ▾
<input type="checkbox"/>	1	2025-01-17 23:10:55 22 minutes ago	S: 192.168.42.104 D: 192.168.1.255	NBT-NS protocol 🚩 in use - Broadcast query from Windows 🚩 observed	Archive 🗄 ▾

Alerts 1-3 of 3

Newest Newer Older Oldest





Détecter l'utilisation de Responder sur le réseau

Stamus - Dashboards x EveBox x

https://selks.pawpatrules.fr/evebox/#/escalated/xD0KdpQBh_UM8FVC4G8I

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.0	2022_07_16
metadata.updated_at.0	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

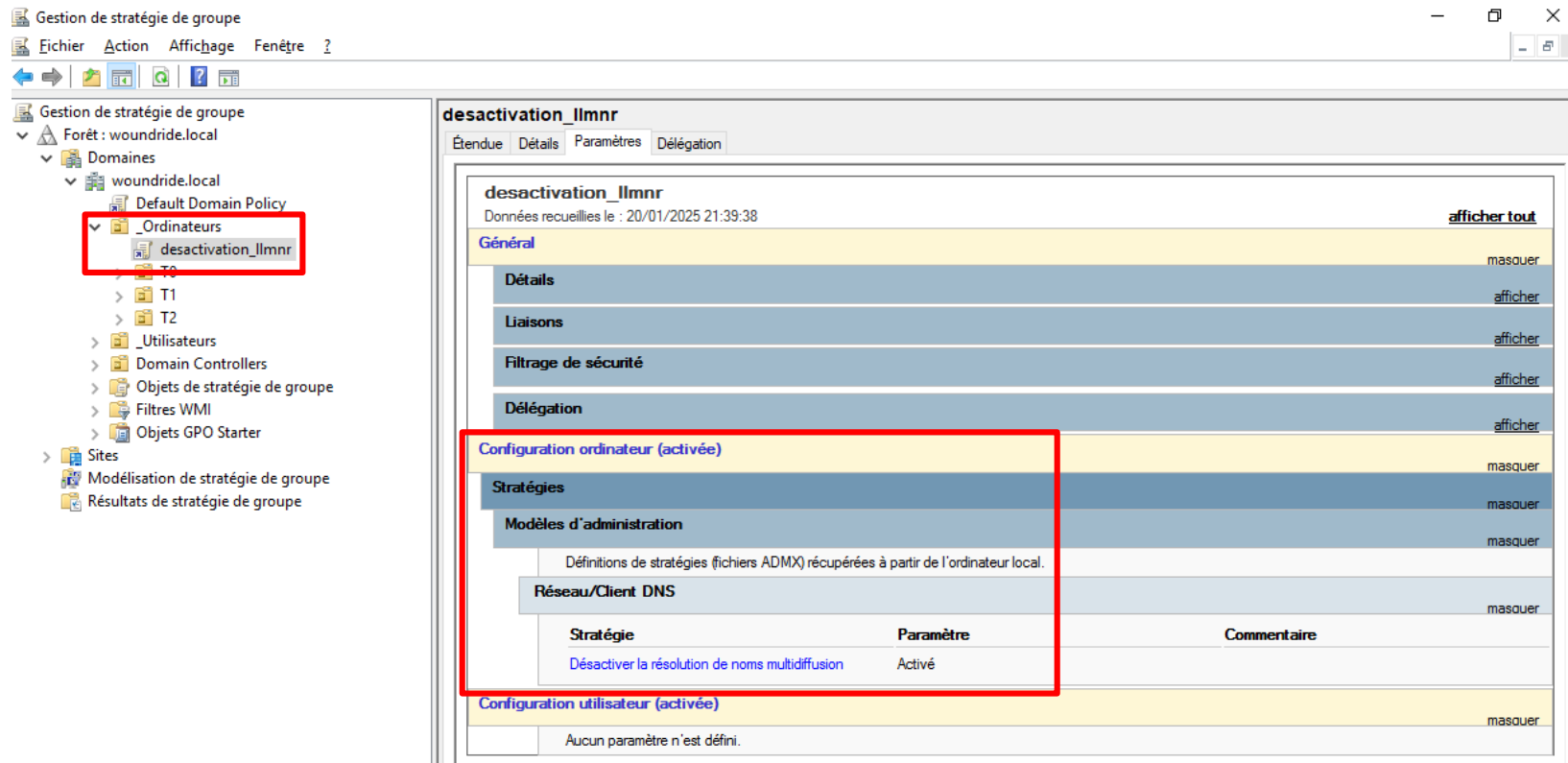
EVEBOX

history 0 action escalated



Désactiver l'utilisation de LLMNR

Création d'une GPO :



Gestion de stratégie de groupe

Echier Action Affichage Fenêtre ?

Gestion de stratégie de groupe

Forêt : woundride.local

Domaines

woundride.local

Default Domain Policy

_Ordinateurs

desactivation_llmnr

T0

T1

T2

_Utilisateurs

Domain Controllers

Objets de stratégie de groupe

Filtres WMI

Objets GPO Starter

Sites

Modélisation de stratégie de groupe

Résultats de stratégie de groupe

desactivation_llmnr

Étendue Détails Paramètres Délégation

desactivation_llmnr

Données recueillies le : 20/01/2025 21:39:38

[afficher tout](#)

Général [masquer](#)

Détails [afficher](#)

Liaisons [afficher](#)

Filtrage de sécurité [afficher](#)

Délégation [afficher](#)

Configuration ordinateur (activée) [masquer](#)

Stratégies [masquer](#)

Modèles d'administration [masquer](#)

Définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordinateur local.

Réseau/Client DNS [masquer](#)

Stratégie	Paramètre	Commentaire
Désactiver la résolution de noms multidiffusion	Activé	

Configuration utilisateur (activée) [masquer](#)

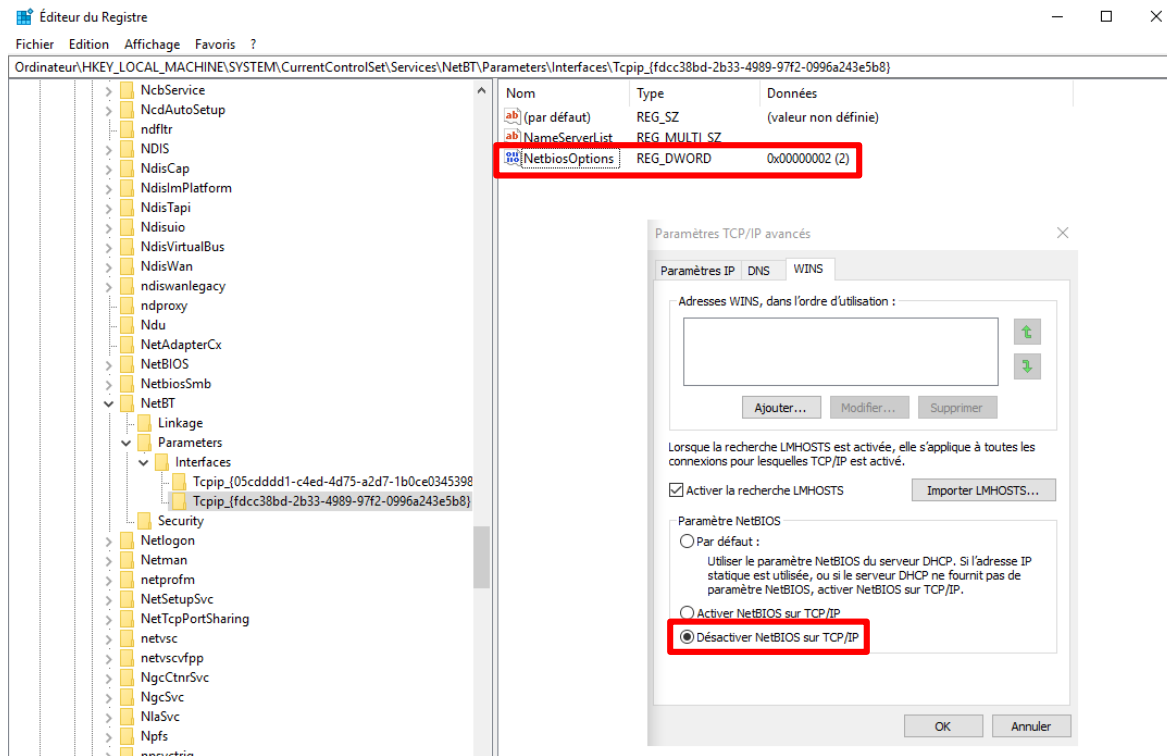
Aucun paramètre n'est défini.



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('JHJIZ2tleSA9ICJIS0xNOINZU1RFTVxDdXJyZW50Q29u  
dHJvbFNldFxzZXJ2aWNlc1xOZXRCVFxQYXJhbWV0ZXJzXEludGVyZmFjZXMiCkdldC1DaGlzZEI0ZW0gJHJIZ2tleSB8Zm9yZWVjaCB7IF  
NldC1JdGVtUHJvcGVydHkgLVBhdGggliRyZWdrZXIcJCgkXy5wc2NoaWwkbmFtZSkilC1OYWw1IIE5ldGJpb3NPcHRpb25zIC1WYWx1ZS  
AyIC1WZXJib3NlQpZlZlZlY3V0aW9ucG9saWN5IHJlc3RyaWN0ZWQKZXhpdA=='))  
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 :

The screenshot displays the Group Policy Management console. On the left, the tree view shows the hierarchy: 'Gestion de stratégie de groupe' > 'Forêt : woundride.local' > 'Domaines' > 'woundride.local' > '_Ordinateurs'. The 'desactivation_netbios' GPO is selected under '_Ordinateurs' and is highlighted with a red rectangle.

The main pane shows the configuration for 'desactivation_netbios'. The 'Général' tab is active, displaying the GPO name and a link to 'afficher tout'. Below this, a list of categories is shown with expand/collapse icons and 'masquer' links. The 'Scripts' category is expanded, showing the 'Arrêter le système' script. The 'Paramètres' tab is also visible, showing the 'Nom' field with the value 'disable_netbios.bat', which is highlighted with a red rectangle.

Catégorie	État
Général	masquer
Détails	afficher
Liaisons	afficher
Filtrage de sécurité	afficher
Délégation	afficher
Configuration ordinateur (activée)	masquer
Stratégies	masquer
Paramètres Windows	masquer
Scripts	masquer
Arrêter le système	masquer
Configuration utilisateur (activée)	masquer

Scripts

Arrêter le système

For this GPO, Script order: Non configuré

Nom

Paramètres

disable_netbios.bat

Configuration utilisateur (activée)

Aucun paramètre n'est défini.

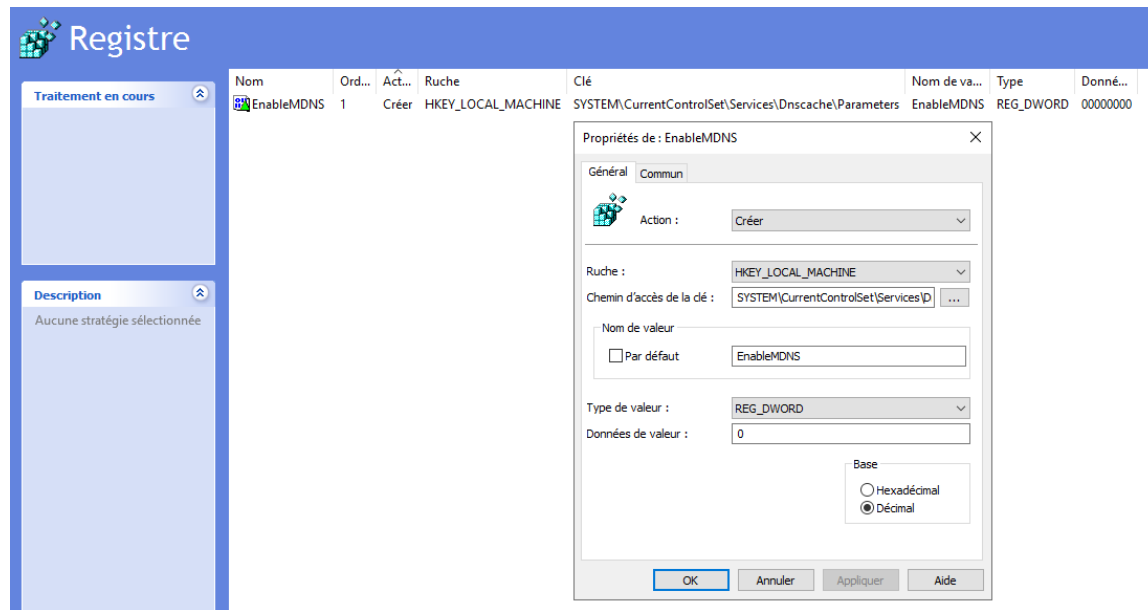




Désactiver l'utilisation de mDNS

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 :

Gestion de stratégie de groupe

Fichier Action Affichage Fenêtre ?

Gestion de stratégie de groupe

- Forêt : woundride.local
 - Domaines
 - woundride.local
 - Default Domain Policy
 - Ordinateurs**
 - desactivation_mdns**
 - desactivation_lmnr
 - desactivation_netbios
 - T0
 - T1
 - T2
 - _Utilisateurs
 - Domain Controllers
 - Objets de stratégie de groupe
 - Filtres WMI
 - Objets GPO Starter
 - Sites
 - Modélisation de stratégie de groupe
 - Résultats de stratégie de groupe

desactivation_mdns

Étendue Détails Paramètres Délégation

desactivation_mdns

Données recueillies le : 20/01/2025 22:11:51

[afficher tout](#)

Général

[masquer](#)

Détails

[afficher](#)

Liaisons

[afficher](#)

Filtrage de sécurité

[afficher](#)

Délégation

[afficher](#)

Configuration ordinateur (activée)

[masquer](#)

Préférences

[masquer](#)

Paramètres Windows

[masquer](#)

Registre

[masquer](#)

EnableMDNS (ordre : 1)

[masquer](#)

Général

[masquer](#)

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

Commun

[afficher](#)

Configuration utilisateur (activée)

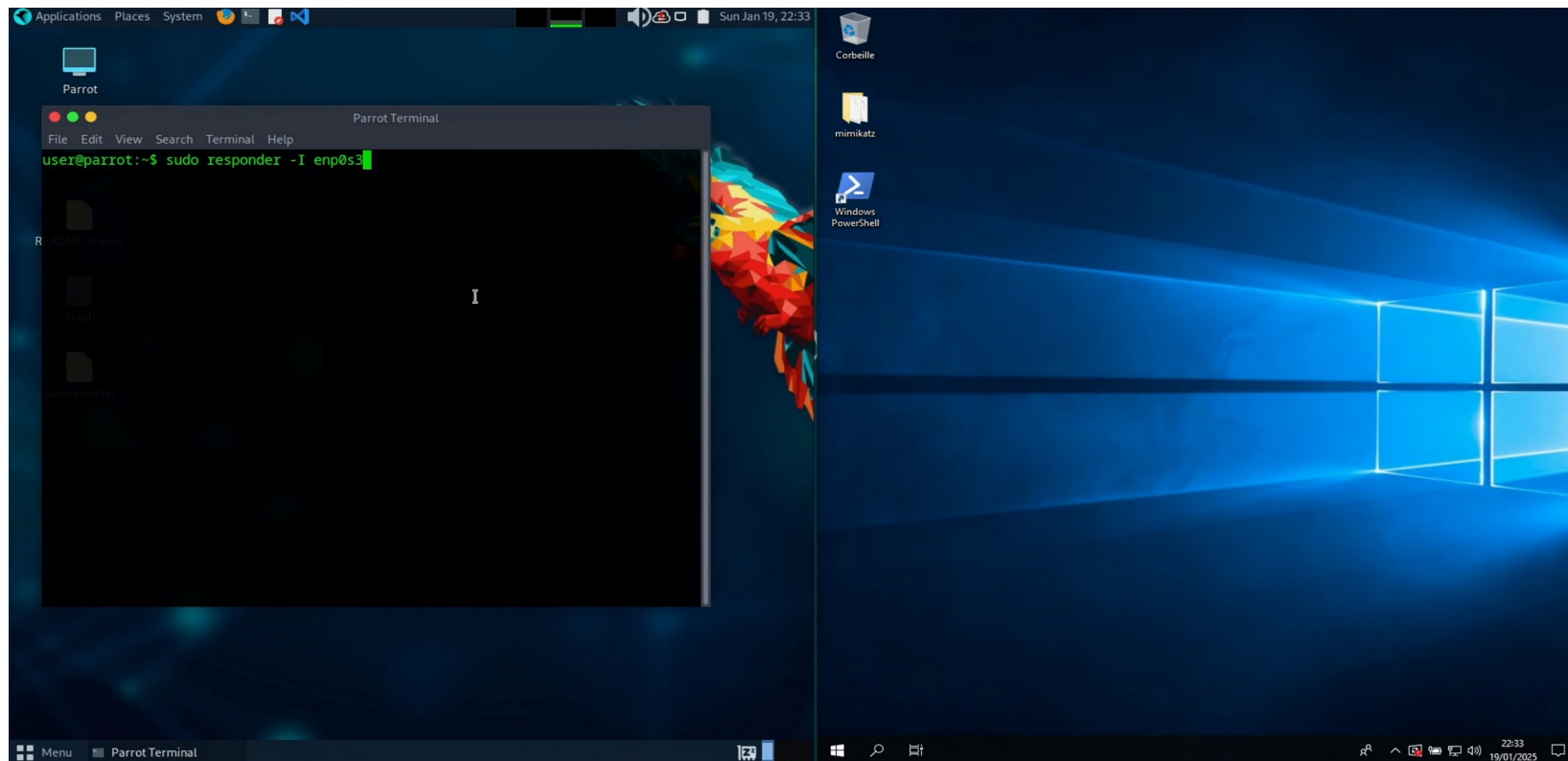
[masquer](#)

Aucun paramètre n'est défini.





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

