

DURCISSEMENT WINDOWS

- Comprendre les attaques de collections.
- Décortiquer et comprendre le fonctionnement de Bloodhound.
- Mettre en place une solution de détection des requêtes empoisonnées.
- Atténuer les attaques sur l'AD

DURCISSEMENT WINDOWS

- Définition du Hardening
- Présentation d'attaque interne (récolte d'informations)
- Décortiquer Bloodhound
- Prérequis
 - (Démonstration) attaque de collection (phase d'attaque)
 - Introduction AD et Ldap (phase d'audit)
 - (Démonstration) identifier et détecter l'attaque
 - Atténuer les attaques sur l'AD (bonne pratique)

DURCISSEMENT

- Le durcissement (hardening) consiste à réduire la surface d'attaque disponible pour l'attaque
- À mesure que les systèmes d'exploitation évoluent, le durcissement doit être ajusté pour suivre l'évolution de la technologie du système d'exploitation.
- Avant de penser à utiliser des outils/solutions, il faut déjà utiliser les fonctionnalités disponibles au niveau de l'OS
- Aucun registre de référence n' incite à utiliser des solutions spécifique (même coté AV)
 - CSI Benchmarks, Microsoft Security Baseline pour les DC, DoD STIG et même l'ANSSI.

DURCISSEMENT

R10 - Priorité 1

Il est important de noter qu'un antivirus est un applicatif. De ce fait, des failles logicielles pourraient être exploitées afin de compromettre la machine. L'installation d'un antivirus sur des serveurs critiques (comme les DC) augmente la surface d'attaque. Ainsi, il n'est pas recommandé d'installer de logiciels (que ce soit un antivirus, un agent de sauvegarde, d'inventaire, etc.) sur un contrôleur de domaine.

Il est envisageable d'utiliser une solution de surveillance pour les DC si elle répond aux critères suivants :

- mise en œuvre d'une infrastructure de surveillance dédiée aux DC ;
- utilisation de comptes de service dédiés à la solution ;
- aucun agent en écoute installé sur les DC ;
- outils utilisés développés par une source de confiance.

DURCISSEMENT - OBJECTIFS

- Prévention des scénarios d'attaque connus
- Réduction de la surface d'attaque
- Améliorer la protection des données
- Améliorer la protection des données
- Minimiser les décisions clés en matière de sécurité et de confidentialité ainsi que les choix de l'utilisateur
- Application de paramètres par défaut raisonnables pour empêcher les modifications par l'utilisateur.

DURCISSEMENT - OBJECTIFS

- Center for Internet Security (CIS) Benchmarks
- ANSSI (Guide de durcissement AD)
 - <https://www.cert.ssi.gouv.fr/uploads/guide-ad.html>
- Microsoft Security Baseline for Windows Servers (DC)
- DoD STIG Windows Server
 - Security Technical Implementation Guide (STIG)



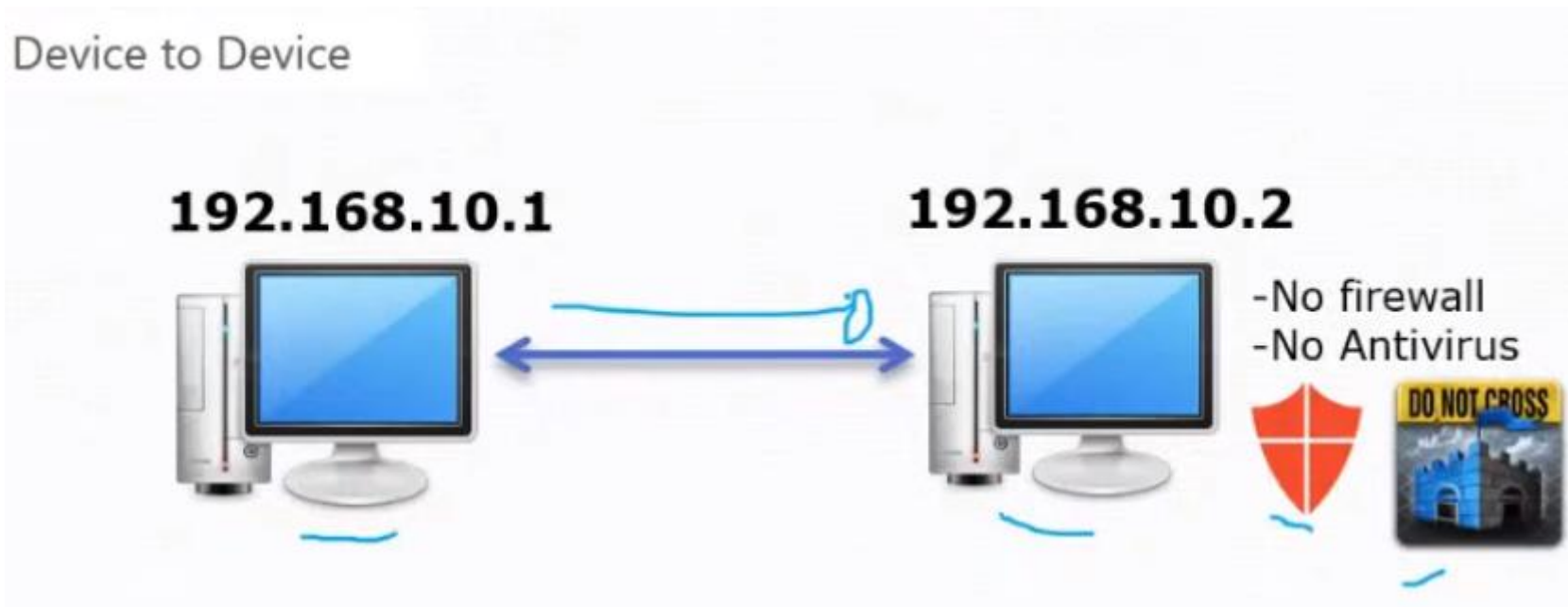
DURCISSEMENT WINDOWS

- Considéré comme la Cyber sécurité active, le Hardening (durcissement) est la partie la plus importante de la cybersécurité permettant de :
- sécuriser un système
- protéger les données sensibles
- réduire le risque en éliminant les droits non indispensables

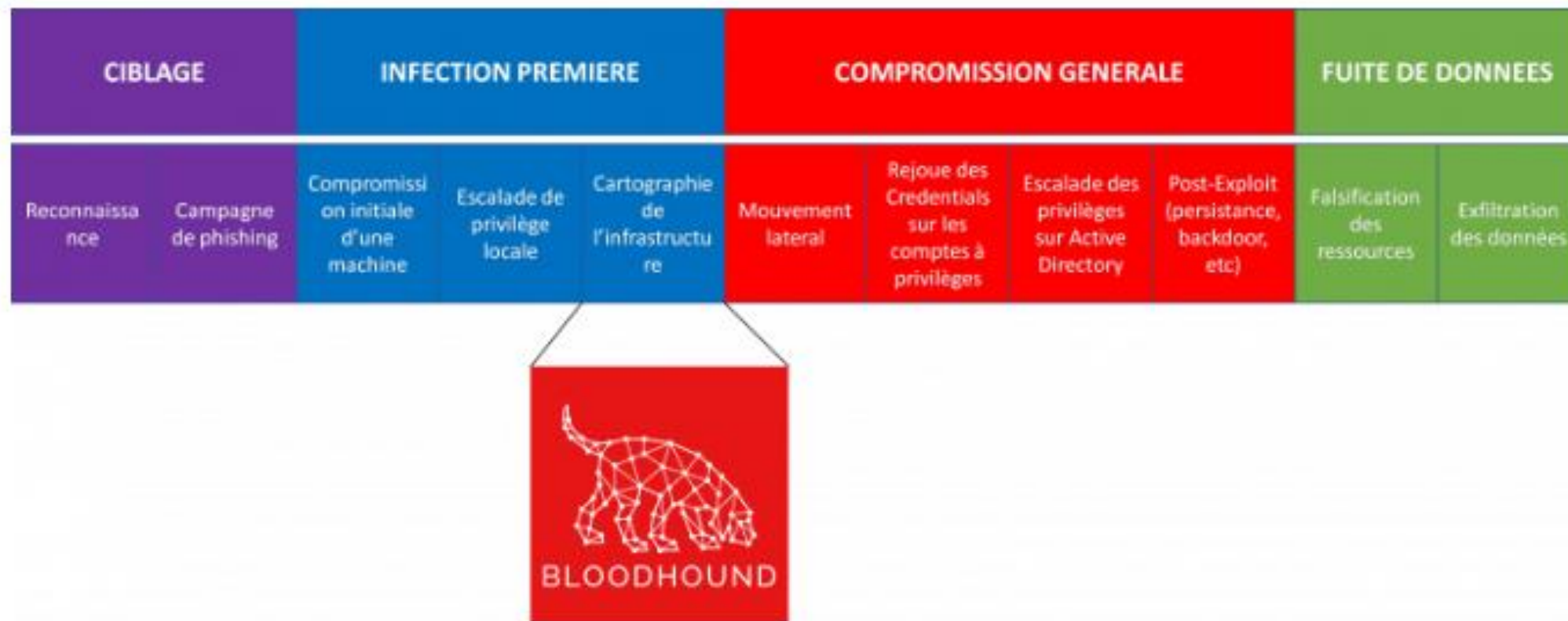
DURCISSEMENT WINDOWS

QUEL INTÉRÊT ?

- Contrairement à la cybersécurité passive (D to D), le but du hardening n'est pas d'impressionner, mais d'agir en proposant des solutions et des mesures de sécurité aux clients
 - Offrir les moyens et les solutions de défense



DURCISSEMENT WINDOWS RÉCOLTE D'INFORMATIONS - ÉTAPES D'ATTAQUES



Les étapes classiques d'une attaque visant Active Directory

PING CASTLE

- Détecte les principales erreurs de configurations ou bonnes pratiques non respectés au sein d'un AD.

- <https://www.pingcastle.com/>

```
C:\Users\Administrator\Downloads\PingCastle_2.10.1.1\PingCastle.exe
| @@@:
: .# Vincent LE TOUX (contact@pingcastle.com)
: .: twitter: @mysmartlogon https://www.pingcastle.com
Select a domain or server
=====
Please specify the domain or server to investigate (default:abalone.fr)

Free Edition of PingCastle 2.10.0 - Not for commercial use
Starting the task: Perform analysis for abalone.fr
[12:20:20] Getting domain information (abalone.fr)
[12:20:22] Gathering general data
[12:20:22] Gathering user data
[12:20:23] Gathering computer data
[12:20:23] Gathering trust data
[12:20:23] Gathering privileged group and permissions data
[12:20:23] - Initialize
[12:20:23] - Searching for critical and infrastructure objects
[12:20:23] - Collecting objects - Iteration 1
[12:20:23] - Collecting objects - Iteration 2
[12:20:23] - Collecting objects - Iteration 3
[12:20:23] - Collecting objects - Iteration 4
[12:20:23] - Collecting objects - Iteration 5
[12:20:23] - Completing object collection
[12:20:23] - Export completed
[12:20:24] Gathering delegation data
[12:20:24] Gathering gpo data
[12:20:25] Gathering pki data
[12:20:25] Gathering anomaly data
[12:20:25] Gathering dns data
[12:20:25] Gathering WSUS data
[12:20:25] Gathering MSOL data
[12:20:25] Gathering domain controller data (including null session)
[12:20:26] Gathering network data
[12:20:26] Computing risks
[12:20:26] Export completed
[12:20:26] Generating html report
[12:20:27] Generating xml file for consolidation report
[12:20:27] Export level is Normal
[12:20:27] Personal data will NOT be included in the .xml file (add --level Full to add it)
[12:20:27] Done
Task Perform analysis for abalone.fr completed
=====
Program launched in interactive mode - press any key to terminate the program
=====
```

PING CASTLE



abalone.fr

2022-03-15

About

abalone.fr - Healthcheck analysis

Date: 2022-03-15 - Engine version: 2.10.1.1

This report has been generated with the Basic Edition of PingCastle

Being part of a commercial package is forbidden (selling the information contained in the report).

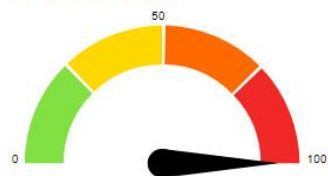
If you are an auditor, you MUST purchase an Auditor license to share the development effort.

Active Directory Indicators

This section focuses on the core security indicators.

Locate the sub-process determining the score and fix some rules in that area to get a score improvement.

Indicators



Domain Risk Level: 100 / 100

It is the maximum score of the 4 indicators and one score cannot be higher than 100. The lower the better

[Compare with statistics](#)

[Privacy notice](#)



Stale Object : 46 / 100

It is about operations related to user or computer objects

6 rules matched



Trusts : 0 / 100

It is about links between two Active Directories

0 rules matched



Privileged Accounts : 30 / 100

It is about administrators of the Active Directory

3 rules matched



Anomalies : 100 / 100

It is about specific security control points

14 rules matched

Risk model

Stale Objects

Inactive user or computer

Network topography

Object configuration

Obsolete OS

Old authentication protocols

Provisioning

Replication

Vulnerability management

Privileged accounts

Account take over

ACL Check

Admin control

Control paths

Delegation Check

Irreversible change

Privilege control

Read-Only Domain Controllers

Trusts

Old trust protocol

SID Filtering

SIDHistory

Trust impermeability

Trust inactive

Trust with Azure

Anomalies

Audit

Backup

Certificate take over

Golden ticket

Local group vulnerability

Network sniffing

Pass-the-credential

Password retrieval

Reconnaissance

Temporary admins

Weak password

Legend:

- score is 0 - no risk identified but some improvements detected
- score between 1 and 10 - a few actions have been identified
- score between 10 and 30 - rules should be looked with attention
- score higher than 30 - major risks identified

PING CASTLE

Maturity Level

This section represents the maturity score (inspired from [ANSSI](#)).

This feature is reserved for customers who have [purchased a license](#)

MITRE ATT&CK®

This section represents an evaluation of the techniques available in the [MITRE ATT&CK®](#)

This feature is reserved for customers who have [purchased a license](#)

Stale Objects



Stale Objects : 46 /100

It is about operations related to user or computer objects

Stale Objects rule details [6 rules matched on a total of 41]

Presence of Des Enabled account = 1

+ 15 Point(s)

Stale Objects rule details [6 rules matched on a total of 41]

Presence of Des Enabled account = 1

+ 15 Point(s)

Non-admin users can add up to 10 computer(s) to a domain

+ 10 Point(s)

SMB v1 activated on 1 DC

+ 10 Point(s)

The subnet declaration is incomplete [1 IP of DC not found in declared subnets]

+ 5 Point(s)

Presence of non-supported version of Windows 10 = 1

+ 5 Point(s)

Number of accounts which has never-expiring passwords: 126

+ 1 Point(s)

Privileged Accounts



Privileged Accounts : 30 /100

It is about administrators of the Active Directory

Privileged Accounts rule details [3 rules matched on a total of 42]

Anyone can interactively or remotely login to a DC

+ 15 Point(s)

PING CASTLE

Anomalies analysis



Anomalies : 100 /100

It is about specific security control points

Anomalies rule details [14 rules matched on a total of 62]

Last change of the Kerberos password: 738228 day(s) ago	+ 50 Point(s)
LAPS doesn't seem to be installed	+ 15 Point(s)
Last AD backup has been performed 12 day(s) ago	+ 15 Point(s)
Policy where the password length is less than 8 characters: 1	+ 10 Point(s)
The audit policy on domain controllers does not collect key events.	+ 10 Point(s)
The spooler service is remotely accessible from 1 DC	+ 10 Point(s)
The number of DCs is too small to provide redundancy: 1 DC	+ 5 Point(s)
No password policy for service account found (MinimumPasswordLength>=20)	Informative rule
The PowerShell audit configuration is not fully enabled.	Informative rule

The PowerShell audit configuration is not fully enabled.	Informative rule
DsHeuristics has not been set to enable the mitigation for CVE-2021-42291	Informative rule
No GPO has been found which implements NetCease	Informative rule
The PreWin2000 compatible group contains "authenticated users"	Informative rule
No GPO has been found which disables LLMNR or at least one GPO does enable it explicitly	Informative rule
Authenticated Users can create DNS records	Informative rule

Domain Information

This section shows the main technical characteristics of the domain.

Search:

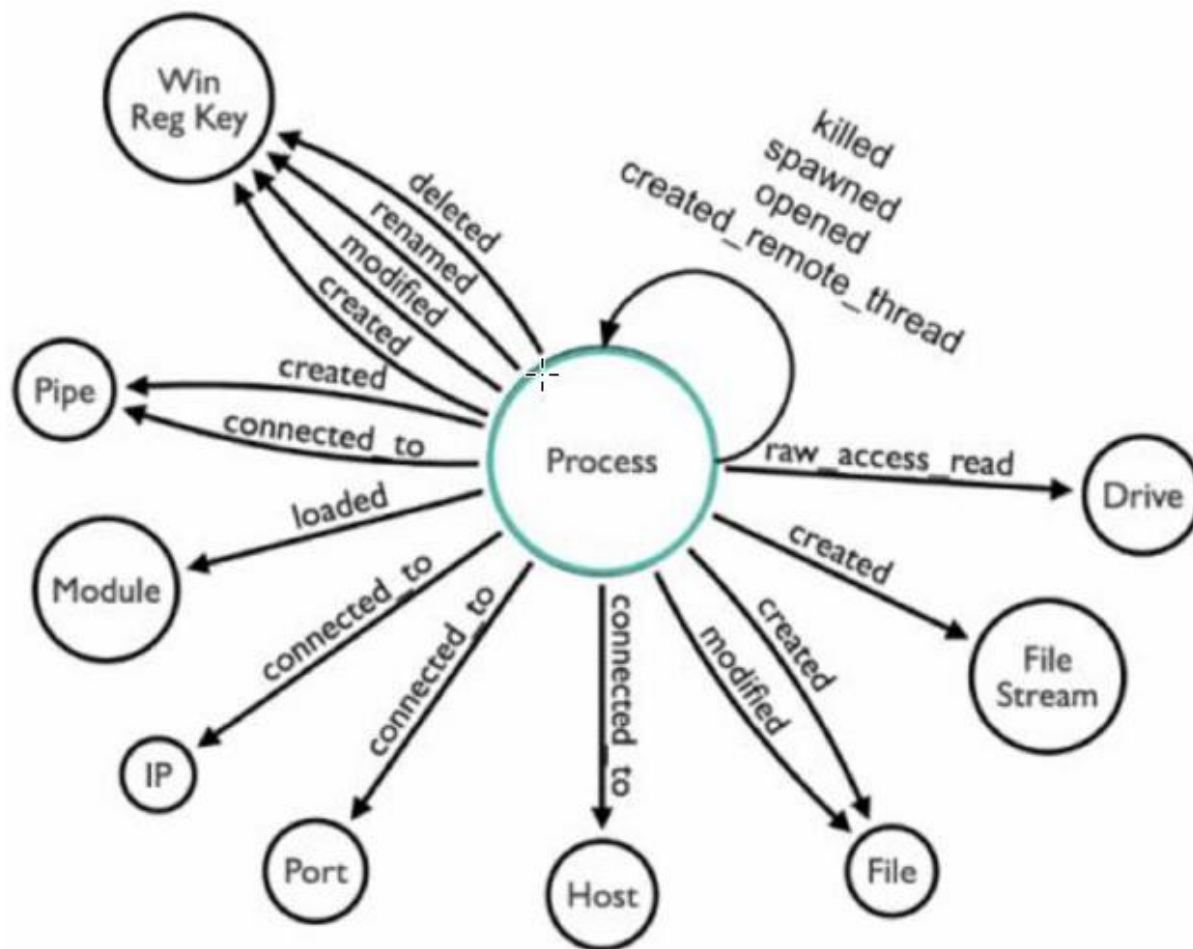
Domain ↑↓	Netbios Name ↑↓	Domain Functional Level ↑↓	Forest Functional Level ↑↓	Creation date ↑↓	DC count ↑↓	Schema version ↑↓	Recycle Bin enabled ↑↓
abalone.fr	ABALONE	Windows Server 2008 R2	Windows Server 2008 R2	2021-04-25 10:48:06Z	1	Windows Server 2016	FALSE

NOS JOURNAUX

- Objectif : Récupérer le plus de log possible - Récupérer les logs les plus intéressants !
- Ce n'est pas des logs par défaut qui récoltent ces informations !
- Nous allons donc ajouter un module complémentaire puis nous ferons remonter les logs dans un outil type Splunk :

■ SYSMON

- <https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon>
- <https://openclassrooms.com/fr/courses/1750566-optimisez-la-securite-informatique-grace-au-monitoring/7144938-collectez-des-logs-avec-sysmon-sous-windows>



NOS JOURNAUX

- **SYSMON**
- Il est vraiment utile, pour utiliser cet outil, d'utiliser derrière un corrélateur de Log afin de rendre **SYSMON** vraiment efficient.
- Par exemple pour le Threat Hunting.

LAPS

- L'un des problèmes les plus récurrents dans les SI : Password Reuse (réutilisation des mots de passes)
- Peut facilement être utilisé par des attaquants pour un mouvement latéral une fois que des informations d'identification valides sont collectées.
- Si vous pouvez gérer, auditer et sécuriser vos comptes administratifs dans toute votre entreprise, vous réduirez le risque considérablement
- Local Administrator Password Solution (LAPS) créée par Microsoft en mai 2015, s'agit d'un outil permettant de gérer en toute sécurité les mots de passe des comptes d'administrateur locaux (jointes au domaine)



LAPS

- Installation : <https://www.it-connect.fr/securite-proteger-les-comptes-administrateur-local-avec-laps/>



LOCAL SECURITY AUTHORITY SUBSYSTEM SERVICE

- Lsass.exe (Local Security Authority Subsystem) est un exécutable qui est nécessaire pour le bon fonctionnement de Windows.
- Il assure l'identification des utilisateurs (utilisateurs du domaine ou utilisateurs locaux).
- Les attaquants peuvent tenter d'accéder aux informations d'identification stockées dans la mémoire de processus du service de sous-système de l'autorité de sécurité locale (LSASS).
- Une fois qu'un utilisateur s'est connecté, le système génère et stocke une variété de documents d'identification dans la mémoire de processus LSASS.

LOCAL SECURITY AUTHORITY SUBSYSTEM SERVICE

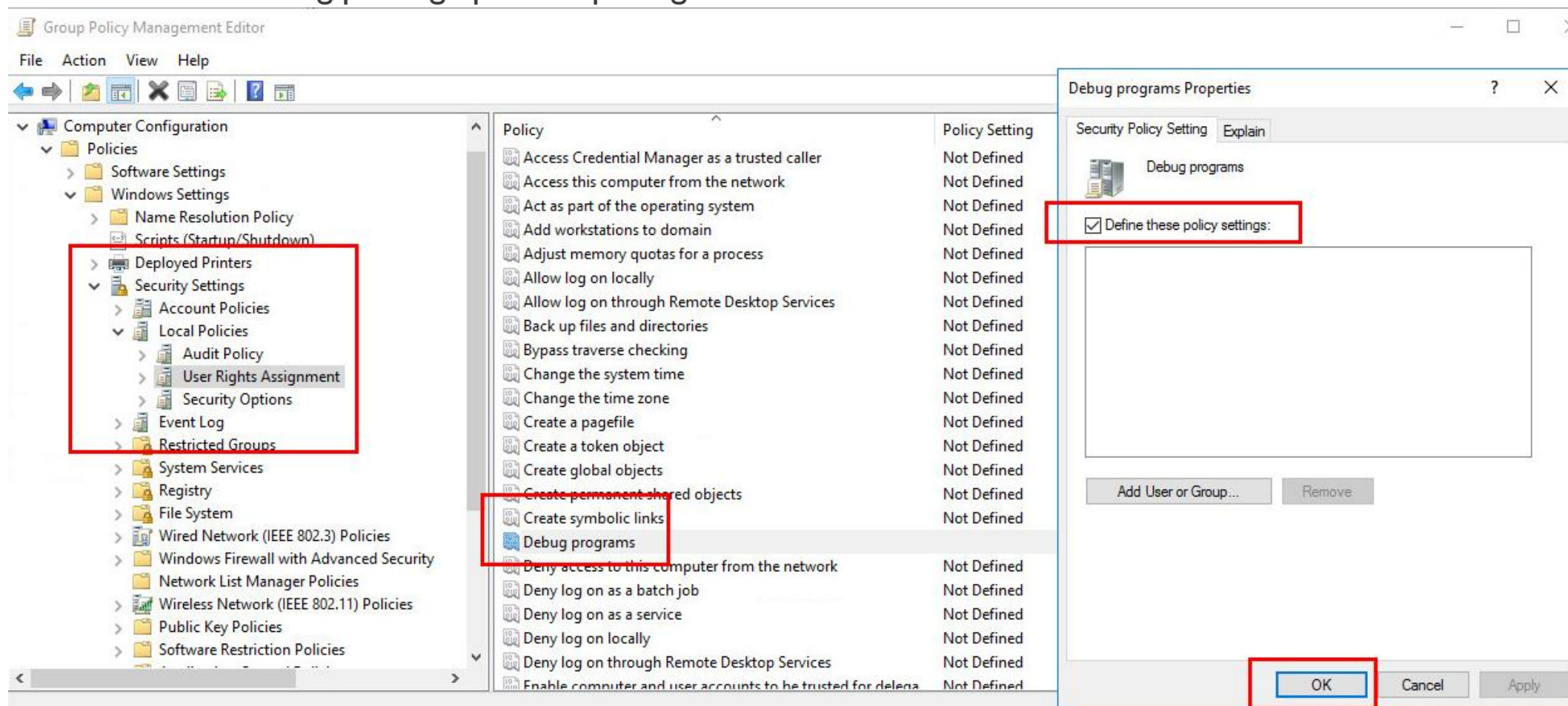
- mimikatz : Permet de récupérer différentes informations des comptes utilisateurs
 - On récupère les hash des mots de passe ou récupère des infos pour par exemple cracker des mots de passes
- process hacker : Petit soft qui gère les processus avec l'aide lsass.exe. (Permet par exemple de dump des process)

```
mimikatz 2.2.0 x64 (oe.eo)
#####> https://pingcastle.com / https://mysmartlogon.com ***/
mimikatz # privilege:debug
Privilege '20' OK
mimikatz # sekurlsa::logonPasswords
Authentication Id : 0 : 995 (00000000:000003e3)
Session : Service from 0
User Name : IUSR
Domain : NT AUTHORITY
Logon Server : (null)
Logon Time : 15/03/2022 11:57:58
SID : S-1-5-17
msv :
  tspkg :
  wdigest :
    * Username : (null)
    * Domain : (null)
    * Password : (null)
  kerberos :
  ssp :
  credman :
Authentication Id : 0 : 60502 (00000000:0000ec56)
Session : Interactive from 1
User Name : DWM-1
Domain : Window Manager
Logon Server : (null)
Logon Time : 15/03/2022 11:57:41
SID : S-1-5-90-0-1
msv :
  [00000003] Primary
    * Username : SRV-ADDC01$
    * Domain : ABALONE
    * Password : bcc426f921d5588c15969ed4927d5a46
    * SHA1 : FcFdb05803b200e85170fccb6112992af16bab8
  tspkg :
  wdigest :
    * Username : SRV-ADDC01$
    * Domain : ABALONE
    * Password : (null)
  kerberos :
    * Username : SRV-ADDC01$
    * Domain : abalone.fr
    * Password : 9b 8a 1c 32 79 7a 20 71 86 05 80 53 d1 b7 Fd 5c ef 43 2e 6f 83 c7 a9 40 24 37 63 6a 35 9f 37 36 1
b3 82 d9 a4 97 7a c4 35 a1 fc 73 85 e9 d0 e0 25 e1 45 31 2c c8 78 5e 93 81 ab 2c 28 a3 87 f0 c8 9e 46 59 50 7e dc 22 8
62 da 6b 5f 56 94 ac ad b0 c9 17 35 4b a4 9d cc 2f cf 22 59 a6 45 4f 82 6f 3c 0f 02 f9 71 32 5a c2 2f b5 22 5c 10 c6 d
04 b5 5f f8 47 07 30 1b 76 46 4e f4 1f c0 85 ad eb c7 7e 8e 1d 7c 7f b4 ab 54 81 ea 33 7e 48 f3 29 1c 77 81 db 4
19 00 ad 94 f1 b6 69 dd 63 6d bb 82 ae 82 6d ef 53 94 27 d1 b5 f9 65 bb ee d4 84 48 29 10 9b 7b d7 90 72 d8 f9 f5 6e 9
06 3e 21 ab 30 40 4e 57 12 3d fa 87 72 70 ad 3b 20 ed 03 1d 82 37 2c e4 7e 18 bf 9e b9 90 a6 86 31 9b f2 b8 97 5b 49 5
49 2e d1 4a ab 3d 2b
ssp :
  credman :
Authentication Id : 0 : 997 (00000000:000003e5)
Session : Service from 0
User Name : LOCAL SERVICE
Domain : NT AUTHORITY
Logon Server : (null)
Logon Time : 15/03/2022 11:57:42
SID : S-1-5-19
msv :
  tspkg :
  wdigest :
    * Username : (null)
    * Domain : (null)
    * Password : (null)
  kerberos :
    * Username : (null)
    * Domain : (null)
    * Password : (null)
  ssp :
  credman :
Authentication Id : 0 : 38243 (00000000:00009563)
Session : UndefinedLogonType From 0
User Name : (null)
Domain : (null)
Logon Server : (null)
Logon Time : 15/03/2022 11:57:32
SID :
msv :
  [00000003] Primary
```

Name	PID	CPU	I/O total ...	Private b...	User name	Description
System Idle Process	0	98,47			NT AUTHORITY\SYSTEM	
System	4	0,04		124 kB	NT AUTHORITY\SYSTEM	NT Kernel & System
smss.exe	412			396 kB	NT AUTHORITY\SYSTEM	Windows Session Manager
Interrupts		0,66		0		Interrupts and DPCs
csrss.exe	492			2,09 MB	NT AUTHORITY\SYSTEM	Client Server Runtime Process
csrss.exe	564			2,97 MB	NT AUTHORITY\SYSTEM	Client Server Runtime Process
wininit.exe	588			984 kB	NT AUTHORITY\SYSTEM	Windows Start-Up Application
services.exe	700			6,76 MB	NT AUTHORITY\SYSTEM	Services and Controller app
svchost.exe	908			6,4 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Ser...
WmiPrvSE.exe	4776			10,84 MB	N...\NETWORK SERVICE	WMI Provider Host
WmiPrvSE.exe	4772			12,41 MB	NT AUTHORITY\SYSTEM	WMI Provider Host
RuntimeBroker.exe	1624			11,25 MB	ABALONE\Administrato	Runtime Broker
ShellExperienceH...	3856			20,91 MB	ABALONE\Administrato	Windows Shell Experience Host
SearchUI.exe	4792			79,34 MB	ABALONE\Administrato	Search and Cortana application
ApplicationFrame...	6844			4,65 MB	ABALONE\Administrato	Application Frame Host
dllhost.exe	5528			51,04 MB	ABALONE\Administrato	COM Surrogate
dllhost.exe	8420			1,47 MB	ABALONE\Administrato	COM Surrogate
svchost.exe	964			6,98 MB	N...\NETWORK SERVICE	Host Process for Windows Ser...
svchost.exe	444			4,55 MB	N...\NETWORK SERVICE	Host Process for Windows Ser...
svchost.exe	1004			16,06 MB	NT A...\LOCAL SERVICE	Host Process for Windows Ser...
svchost.exe	120			10,61 MB	NT A...\LOCAL SERVICE	Host Process for Windows Ser...
svchost.exe	1076			15,34 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Ser...
WUDFHost.exe	1356			1,8 MB	NT A...\LOCAL SERVICE	Windows Driver Foundation - ...
svchost.exe	1128			10,01 MB	N...\NETWORK SERVICE	Host Process for Windows Ser...
vmacthlp.exe	1224			1,32 MB	NT AUTHORITY\SYSTEM	VMware Activation Helper
svchost.exe	1252			11,56 MB	NT A...\LOCAL SERVICE	Host Process for Windows Ser...
svchost.exe	1468			35,36 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Ser...
sihost.exe	448			4,06 MB	ABALONE\Administrato	Shell Infrastructure Host
taskhostw.exe	3672			5,2 MB	ABALONE\Administrato	Host Process for Windows Tas...
svchost.exe	1476			1,54 MB	N...\NETWORK SERVICE	Host Process for Windows Ser...
svchost.exe	1776			1,97 MB	NT A...\LOCAL SERVICE	Host Process for Windows Ser...
svchost.exe	2016			2,35 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Ser...
spoolsv.exe	2168			6,45 MB	NT AUTHORITY\SYSTEM	Spooler SubSystem App
Microsoft.ActiveDire...	2300			35,34 MB	NT AUTHORITY\SYSTEM	Microsoft.ActiveDirectory>We...
svchost.exe	2316			7,98 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Ser...
svchost.exe	2324			8,34 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Ser...
vmtoolsd.exe	2356	0,01		10,07 MB	NT AUTHORITY\SYSTEM	VMware Tools Core Service
ismsv.exe	2376			2 MB	NT AUTHORITY\SYSTEM	Windows NT Internets Messagi...
MsmPng.exe	2384			177,41 MB	NT AUTHORITY\SYSTEM	Antimalware Service Executable
svchost.exe	2436			4,76 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Ser...
svchost.exe	2448			3,77 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Ser...
VGAuthService.exe	2496			4,65 MB	NT AUTHORITY\SYSTEM	VMware Guest Authentication...
dfsr.exe	2504			16,41 MB	NT AUTHORITY\SYSTEM	Distributed File System Replic...
svchost.exe	2520			128,7 MB	N...\NETWORK SERVICE	Host Process for Windows Ser...
svchost.exe	2552			6,59 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Ser...
vm3dservice.exe	2560			1,44 MB	NT AUTHORITY\SYSTEM	VMware SVGA Helper Service
vm3dservice.exe	2820			1,52 MB	NT AUTHORITY\SYSTEM	VMware SVGA Helper Service

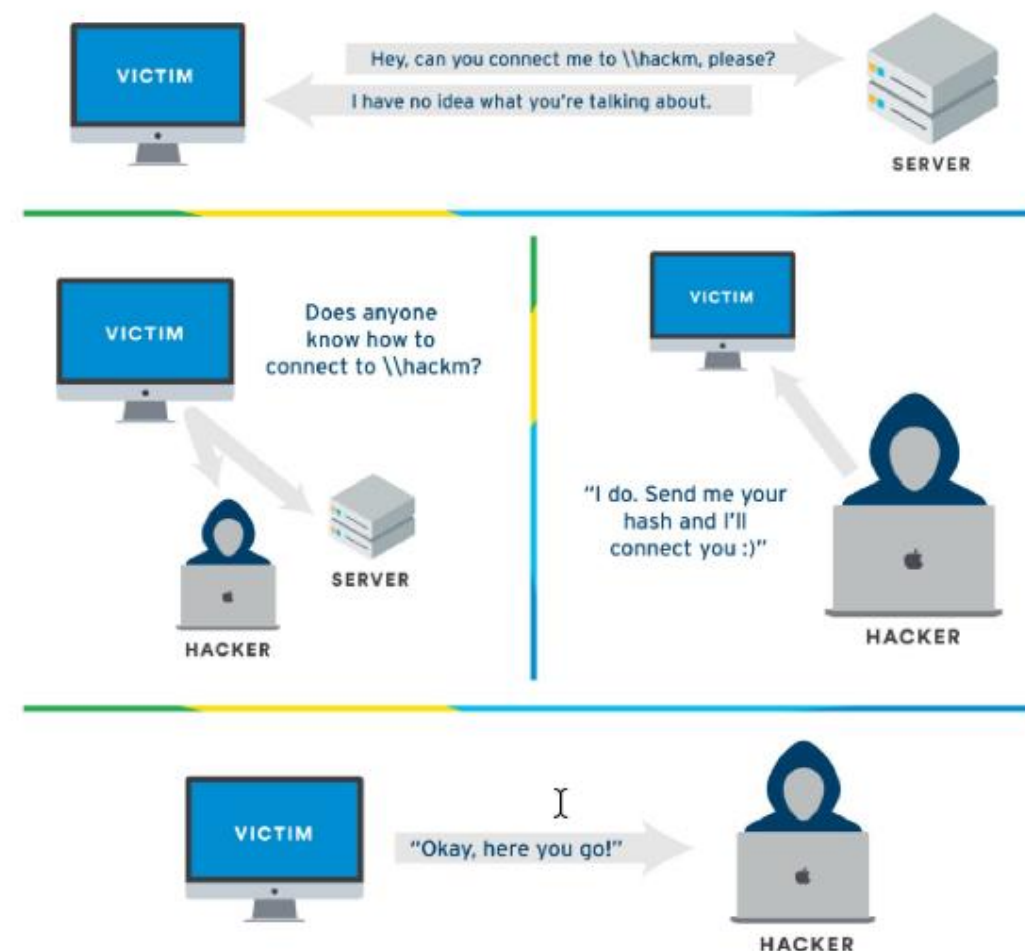
LOCAL SECURITY AUTHORITY SUBSYSTEM SERVICE

- Désactiver le set debug privilege pour se protéger de mimikatz.



LLMNR/NBT-NS POISONING

- Permet de récupérer des informations/hash ou prendre le contrôle de machines/utilisateurs qui sont accessibles sur le réseau en empoisonnant les requêtes netbios.
 - Il fait partie des protocoles les plus vulnérables.
 - Protocole qui fonctionne en broadcast
 - Va chercher des records appropriés pour récupérer des informations DNS qu'on va récupérer localement pour faire des requêtes sur tout le réseau. On peut aller jusqu'à récupérer un accès shell sur la machine.



LLMNR/NBT-NS POISONING

■ Désactiver le LLMNR

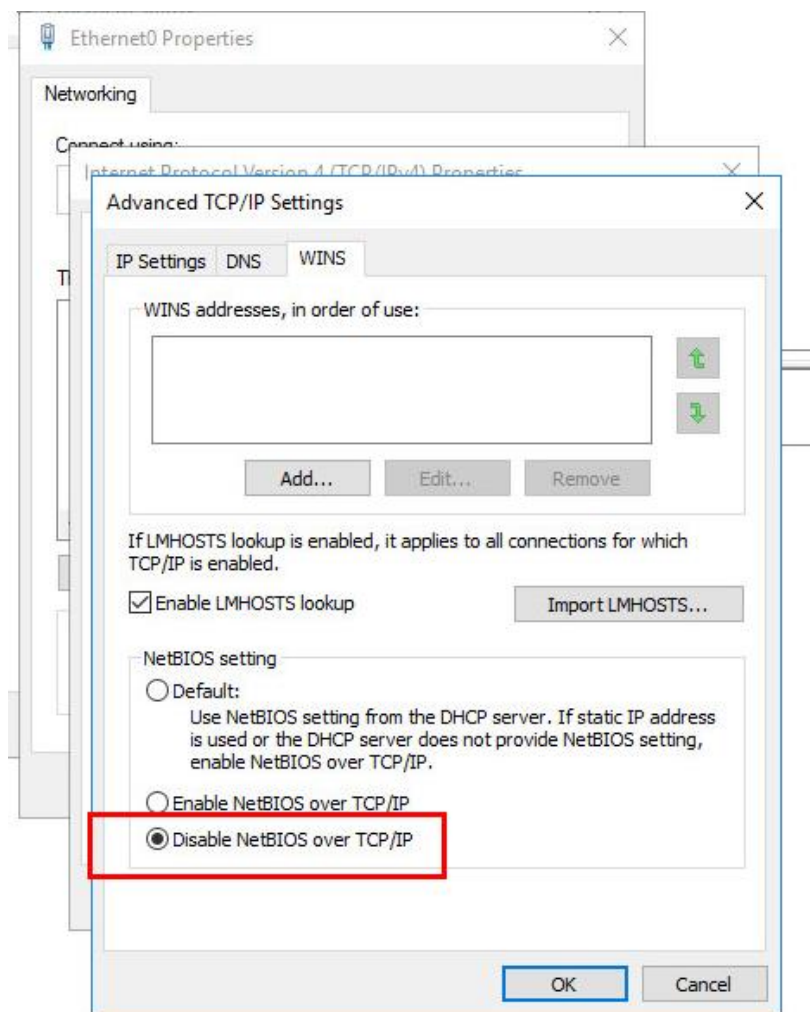
The screenshot displays the Group Policy Management Editor interface. On the left, the tree view shows the hierarchy: Computer Configuration > Administrative Templates > Network > DNS Client. The main pane shows the 'Turn off multicast name resolution' policy, which is currently set to 'Not configured'. The description states: 'Specifies that link local multicast name resolution (LLMNR) is disabled on client computers. LLMNR is a secondary name resolution protocol. With LLMNR, queries are sent using multicast over a local network link on a single subnet from a client computer to another client computer on the same subnet that also has LLMNR enabled. LLMNR does not require a DNS server or DNS client configuration, and provides name resolution in scenarios in which conventional DNS name resolution is not possible. If you enable this policy setting, LLMNR will be disabled on all available network adapters on the client computer. If you disable this policy setting, or you do not configure this policy setting, LLMNR will be enabled on all available network adapters.'

On the right, a dialog box titled 'Turn off multicast name resolution' is open. It shows the 'Turn off multicast name resolution' policy with the 'Enabled' radio button selected. The 'Supported on' field is set to 'At least Windows Vista'. The 'Help' text area contains the same description as the main pane. The 'Options' field is empty. The 'Previous Setting' and 'Next Setting' buttons are visible at the top of the dialog.

Setting	State	Comment
Allow NetBT queries for fully qualified domain names	Not configured	No
Allow DNS suffix appending to unqualified multi-label nam...	Not configured	No
Connection-specific DNS suffix	Not configured	No
Primary DNS suffix devolution level	Not configured	No
Turn off IDN encoding	Not configured	No
IDN mapping	Not configured	No
DNS servers	Not configured	No
Prefer link local responses over DNS when received over a n...	Not configured	No
Primary DNS suffix	Not configured	No
Register DNS records with connection-specific DNS suffix	Not configured	No
Register PTR records	Not configured	No
Dynamic update	Not configured	No
Replace addresses in conflicts	Not configured	No
Registration refresh interval	Not configured	No
TTL value for A and PTR records	Not configured	No
DNS suffix search list	Not configured	No
Turn off smart multi-homed name resolution	Not configured	No
Turn off smart protocol reordering	Not configured	No
Update security level	Not configured	No
Update top level domain zones	Not configured	No
Primary DNS suffix devolution	Not configured	No
Turn off multicast name resolution	Enabled	No

LLMNR/NBT-NS POISONING

- Désactiver le NETBIOS



LLMNR/NBT-NS POISONING

■ Désactiver le NTLM (login)

The screenshot shows the Windows Group Policy Editor window. The left pane displays the tree structure under 'Computer Configuration' > 'Policies' > 'Security Settings' > 'Local Policies' > 'Security Options'. The 'Security Options' folder is highlighted with a red rectangle. The right pane lists various policies. A red rectangle highlights the following policies:

Policy	Policy Setting
Network security: Restrict NTLM: Audit Incoming NTLM Traffic	Enable auditing for all accounts
Network security: Restrict NTLM: Audit NTLM authentication in this domain	Enable all
Network security: Restrict NTLM: Incoming NTLM traffic	Deny all accounts
Network security: Restrict NTLM: NTLM authentication in this domain	Deny all
Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers	Deny all

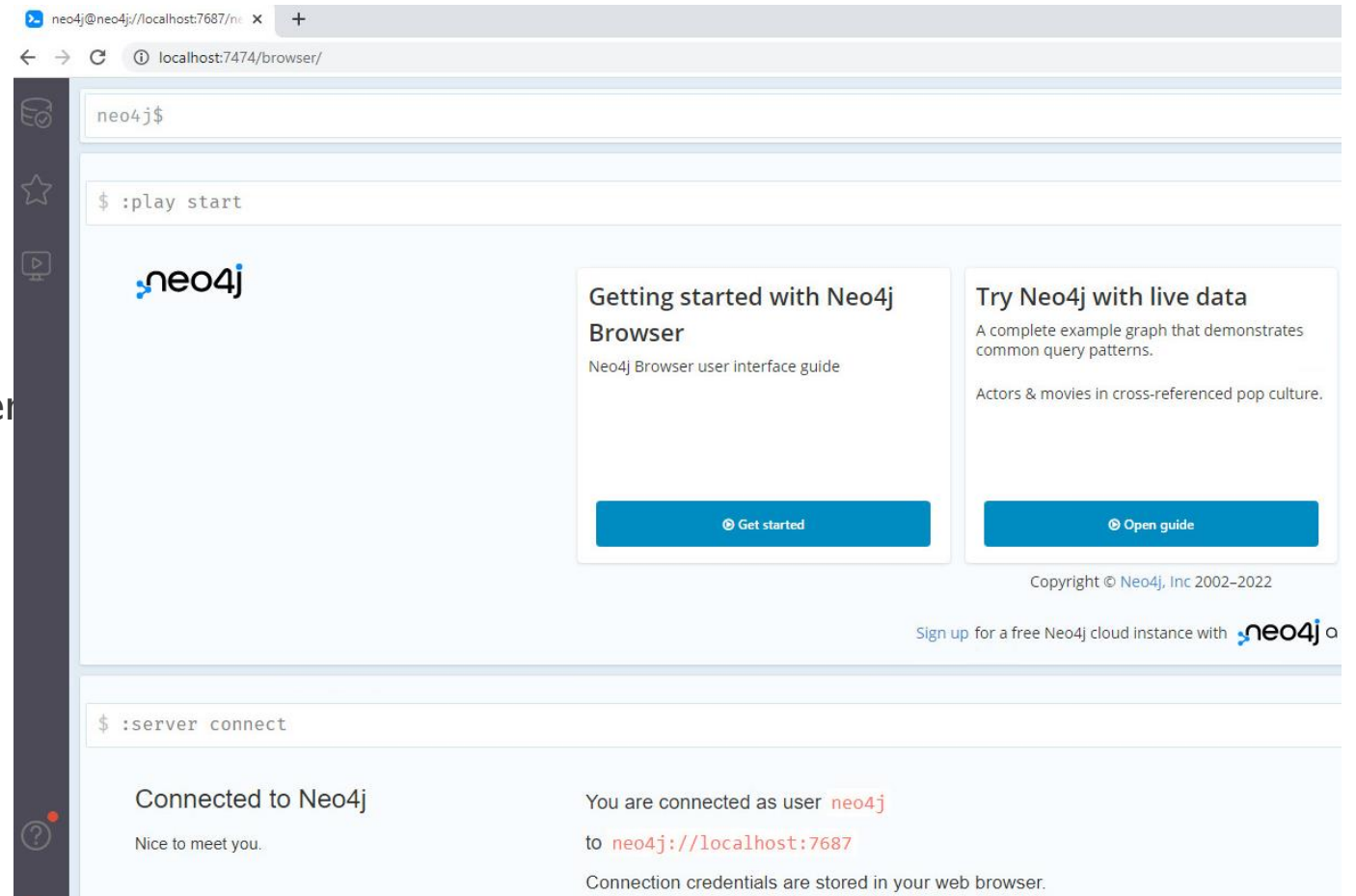
Below the highlighted policies, the policy 'Recovery console: Allow floppy copy and access to all drives and all folders' is highlighted in blue.

DURCISSEMENT WINDOWS BLOODHOUND

- Bloodhound est un outil d'analyse et de collecte de données.
- Il permet de trouver et d'identifier facilement des chemins d'attaque très complexes dans un environnement Active Directory qui seraient autrement impossibles à identifier rapidement.
- Il est en outre composé de trois éléments :
 - Neo4J (BDD)
 - l'applis Bloodhound
 - l'applis SharpHound ou scripts

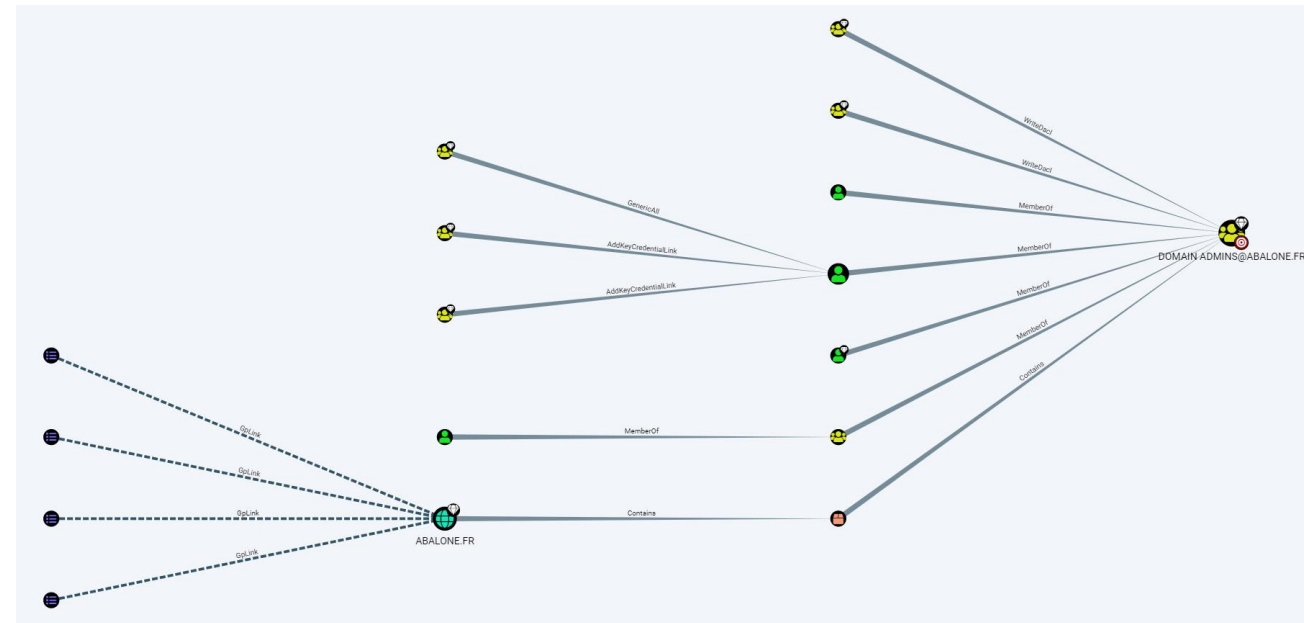
DURCISSEMENT WINDOWS NEO4J

- Une base de données de graphes
- Capable de découvrir des relations et calculer le chemin le plus court entre les objets en utilisant ses liens
- Ici seront les informations sensibles
- Login / MDP par défaut : neo4j/neo4j



DURCISSEMENT WINDOWS BLOODHOUND

- application Web compilé comme une application de bureau
- Permet de présenter sous forme de graphe les différentes relations des chemins découverts
- Ainsi qu'établir une cartographie du domaine AD
- Elle est disponible sous Windows et Linux
- Peut être utilisée à des fins d'attaques ou d'audit



DURCISSEMENT WINDOWS

SHARPHOUND

- SharpHound est le collecteur de données officiel de BloodHound
- collecter les données des contrôleurs de domaine et des systèmes Windows joints au domaine
- Existe sous forme d'un exe ou script PS1
- Un exemple de type d'information récoltées :
 - Appartenances aux groupes de sécurité
 - Approbations de domaine
 - Droits abusifs sur les objets Active Directory
 - Liens de stratégie de groupe
 - Structure arborescente de l'unité d'organisation
 - Plusieurs propriétés des objets ordinateur, groupe et utilisateur
 - Liens d'administration SQL

DURCISSEMENT WINDOWS

PRÉ-REQUIS

- Prérequis
- Avoir l'acquisition sur une machine appartenant au domaine
- Désactiver le pare feu
- Désactiver l'antivirus
- Avoir les droits admin local de la machine

DURCISSEMENT WINDOWS BLOODHOUND

- Démo :
- Utilisation de Bloodhound
 - deux comptes utilisateurs techI et userI du domaine, avec aucun privilège particulier

<https://www.itpro.fr/cybersecurite-techniques-de-cartographie-active-directory-avec-bloodhound/>

<https://bloodhound.readthedocs.io/en/latest/installation/windows.html>

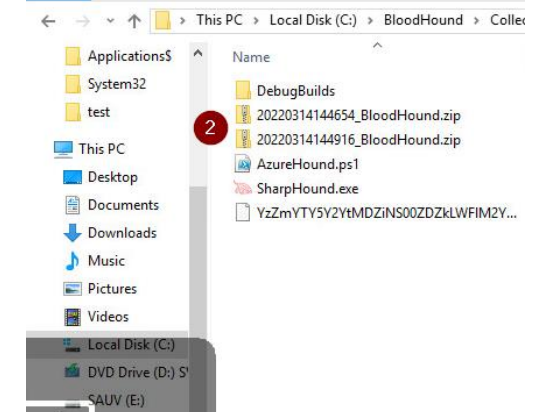
TP - Installer BloodHound

- Constituer la base Neo4j (changer le mot de passe etc...) puis lancer neo4j :
- C:\neo4j-community-4.4.4\bin>neo4j.bat console
- Récupérer les infos avec Sharp
- .\SharpHound.exe --CollectionMethods all
- Puis lancer Bloodhound

```
Administrator: cmd (running as abalone\toto99)
2022-03-14T15:19:10.7354114+01:00|INFORMATION|Status: 249 objects finished (+249 1.185714)/s -- Using 36 MB RAM
Closing writers
2022-03-14T15:19:18.0025897+01:00|INFORMATION|Output channel closed, waiting for output task to complete
2022-03-14T15:19:18.1900659+01:00|INFORMATION|Status: 261 objects finished (+12 1.197248)/s -- Using 37 MB RAM
2022-03-14T15:19:18.1900659+01:00|INFORMATION|Enumeration finished in 00:03:38.2388513
2022-03-14T15:19:18.3776238+01:00|INFORMATION|SharpHound Enumeration Completed at 15:19 on 14/03/2022! Happy Graphing!

c:\BloodHound\Collectors>SharpHound.exe -c all
2022-03-14T15:21:18.6929028+01:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, GPOLocalGroup, Session, LoggedOn, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2022-03-14T15:21:18.7085991+01:00|INFORMATION|Initializing SharpHound at 15:21 on 14/03/2022
2022-03-14T15:21:19.3024540+01:00|INFORMATION|Loaded cache with stats: 225 ID to type mappings.
237 name to SID mappings.
0 machine sid mappings.
2 sid to domain mappings.
0 global catalog mappings.
2022-03-14T15:21:19.3180799+01:00|INFORMATION|Flags: Group, LocalAdmin, GPOLocalGroup, Session, LoggedOn, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2022-03-14T15:21:19.5524953+01:00|INFORMATION|Beginning LDAP search for abalone.fr
2022-03-14T15:21:19.7087728+01:00|INFORMATION|Producer has finished, closing LDAP channel
2022-03-14T15:21:19.7087728+01:00|INFORMATION|LDAP channel closed, waiting for consumers
2022-03-14T15:21:49.8061958+01:00|INFORMATION|Status: 0 objects finished (+0 0)/s -- Using 34 MB RAM
2022-03-14T15:21:59.9942788+01:00|INFORMATION|Consumers finished, closing output channel
Closing writers
2022-03-14T15:22:00.0411755+01:00|INFORMATION|Output channel closed, waiting for output task to complete
2022-03-14T15:22:00.2755840+01:00|INFORMATION|Status: 261 objects finished (+261 6.525)/s -- Using 39 MB RAM
2022-03-14T15:22:00.2755840+01:00|INFORMATION|Enumeration finished in 00:00:40.7211457
2022-03-14T15:22:00.4631093+01:00|INFORMATION|SharpHound Enumeration Completed at 15:22 on 14/03/2022! Happy Graphing!

c:\BloodHound\Collectors>
```



TESTER DIRECTEMENT EN CMD

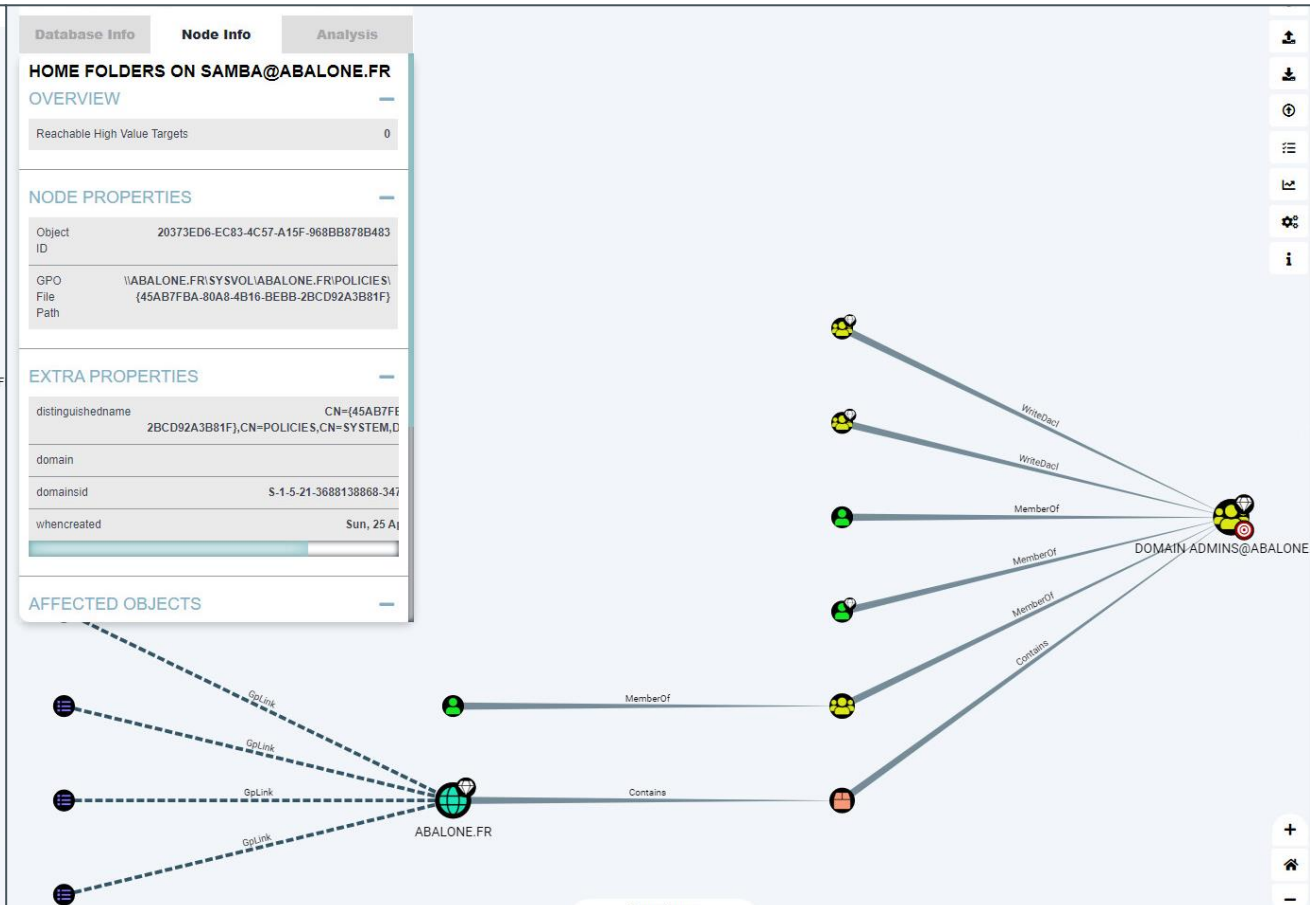
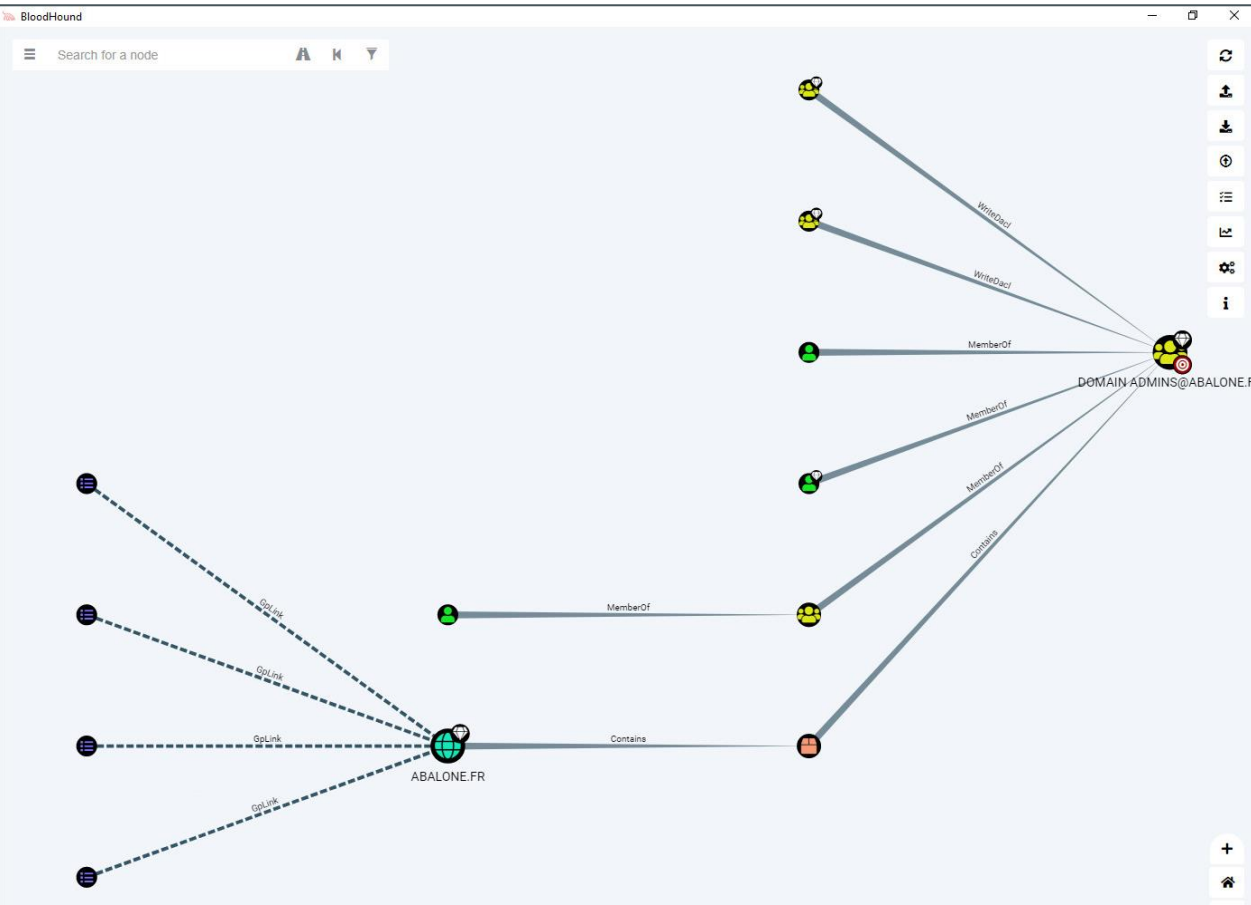
- `runas /user:info\userI cmd`
- `net group /domain`
 - Affiche les groupes du domaine (si ça s'affiche avec un user c'est pas normal)
- `net group ""Admins du Domaine"" /domain`
 - Affiche les users du groupe Domain Admin
- `net user vincent /domain`
 - Infos sur le user trouvé lors de la commande précédente
- Si on récupère des infos sur l'admin avec un user normal c'est pas bon.
- PS : `get-aduser vincent -Properties *`
- Si on récupère des informations, il faudra veiller à ce que ce ne soit plus le cas.
 - Fonctionnalités avancée → Cliquez droit sur Users → Enlever les droits de lectures sur les groupes voulus.

DURCISSEMENT WINDOWS BLOODHOUND - RÉSULTATS

Exécuté avec Administrator

==

Exécuté avec utilisateur du domaine



DURCISSEMENT WINDOWS BLOODHOUND - RÉSULTATS AVEC UN READ- DENY (USER)

- Résultats avec un Read - DENY (user) sur le dossier Users de l'AD

