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

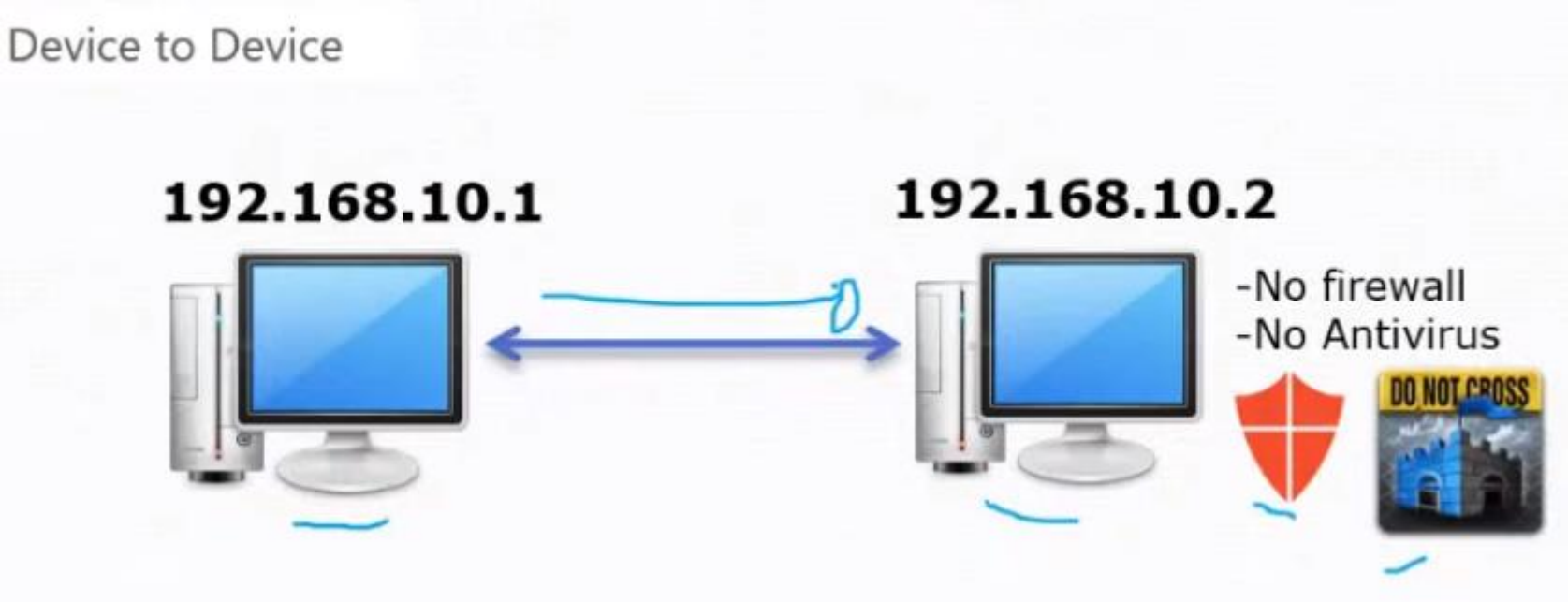
- Center for Internet Security (CIS) Benchmarks
- ANSSI (Guide de durcissement AD)
  - https://www.cert.ssi.gouv.fr/uploads/guide-ad.html
- Microsoft Security Baseline for Windows Servers (DC)
- DoD STIG Windows Server
  - Security Technical Implementation Guide (STIG)

DURCISSEMENT WINDOWS

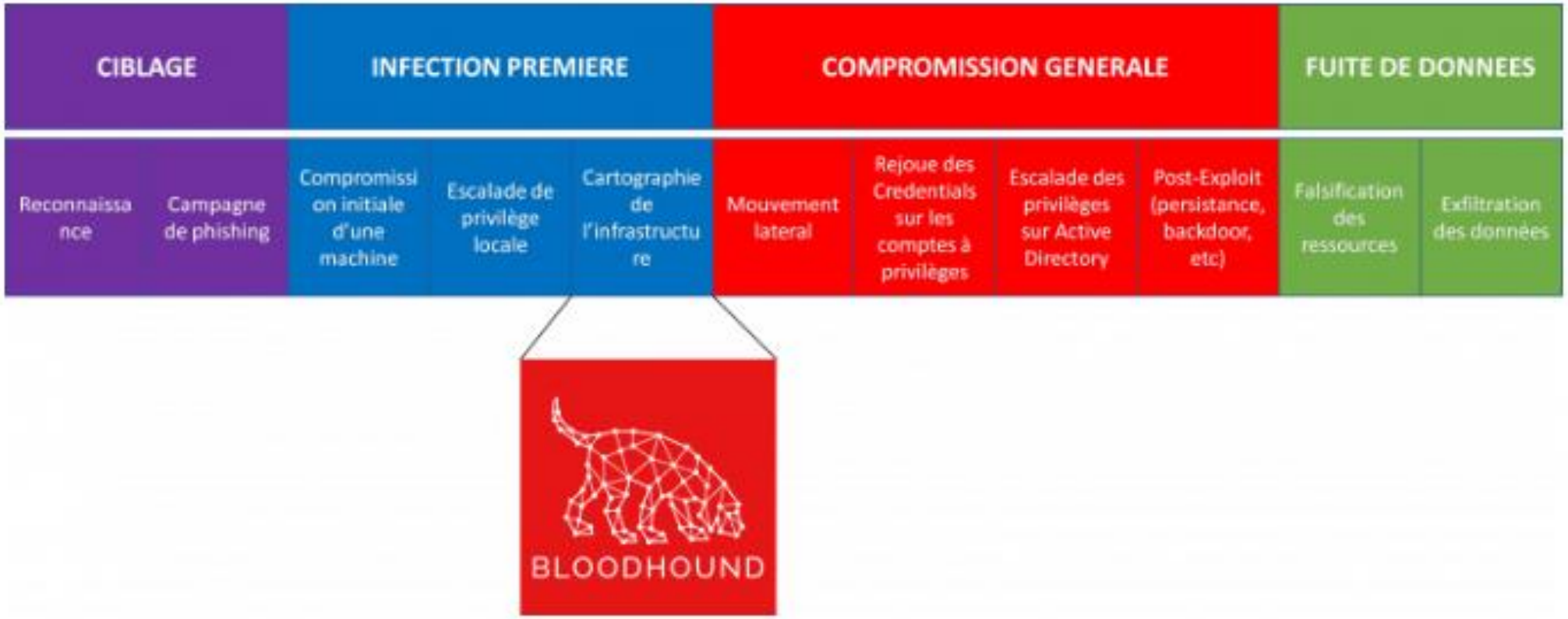
- Considéré comme la Cyber sécurité active, le Hardening (durcissement) et la partie la plus importante de la cybersécurité permettant de :
- sécuriser un système
- protéger les données sensibles
- réduire le risque en éliminant les droits non indispensables

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



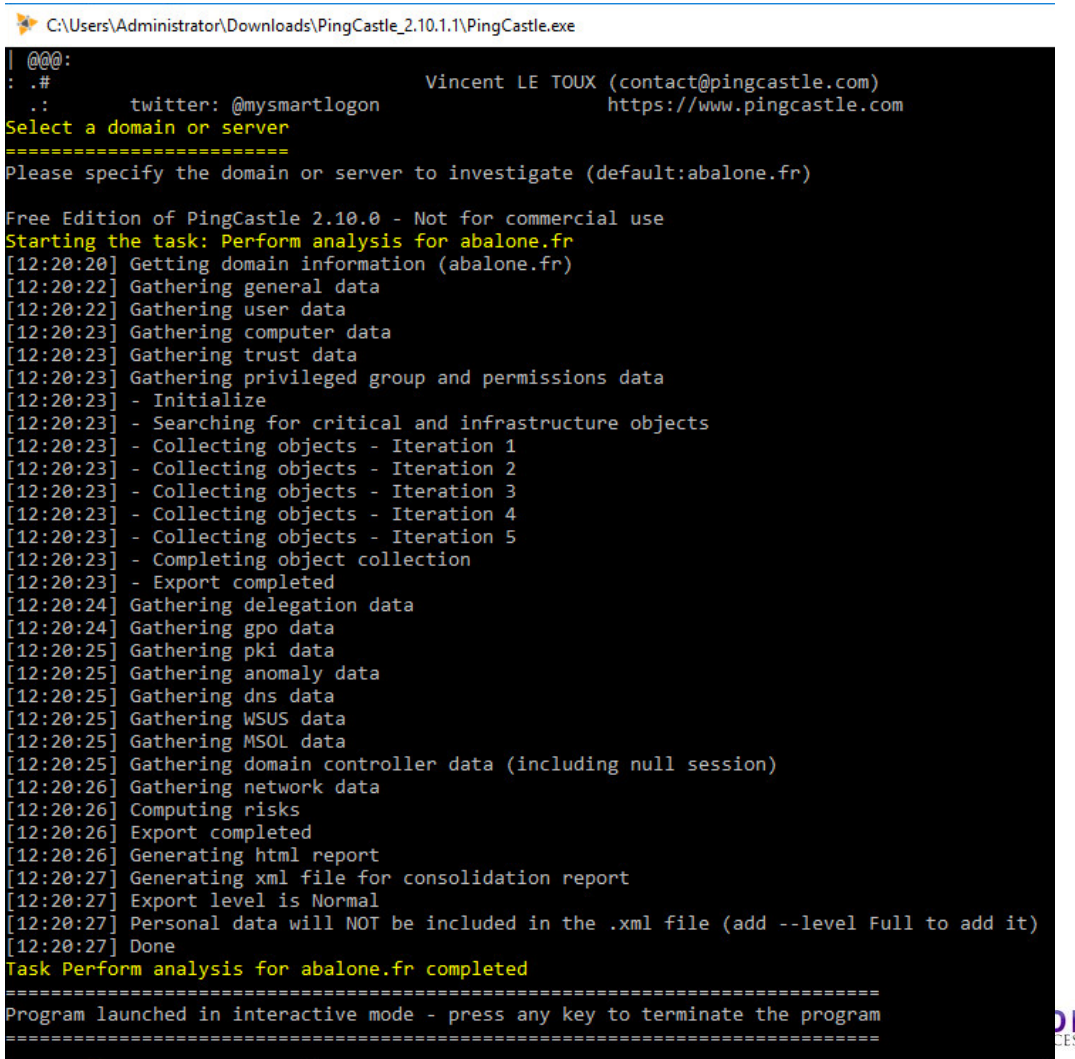
DURCISSEMENT WINDOWS
RÉCOLTE D'INFORMATIONS - ÉTAPES D'ATTAQUES



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/



PING CASTLE

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 — 6 rules matched

It is about operations related to user or computer objects

Trusts : 0 /100 — 0 rules matched

It is about links between two Active Directories

Privileged Accounts : 30 /100 — 3 rules matched

It is about administrators of the Active Directory

Anomalies : 100 /100 — 14 rules matched

It is about specific security control points

Risk model

Stale Objects	Privileged accounts	Trusts	Anomalies
Inactive user or computer	Account take over	Old trust protocol	Audit
Network topography	ACL Check	SID Filtering	Backup
Object configuration	Admin control	SIDHistory	Certificate take over
Obsolete OS	Control paths	Trust impermeability	Golden ticket
Old authentication protocols	Delegation Check	Trust inactive	Local group vulnerability
Provisioning	Irreversible change	Trust with Azure	Network sniffing
Replication	Privilege control		Pass-the-credential
Vulnerability management	Read-Only Domain Controllers		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

ANDN SERVICES

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*
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

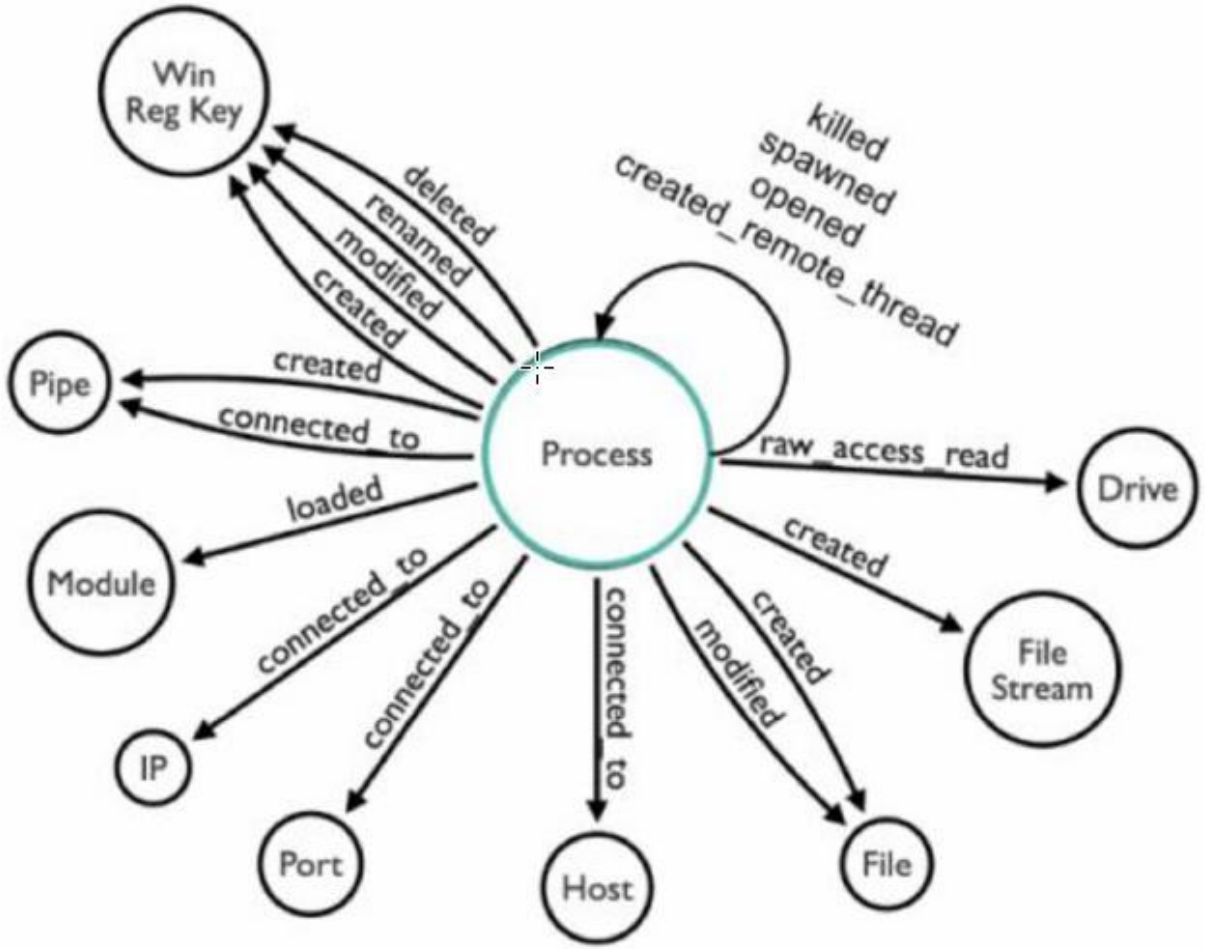
This section shows the main technical characteristics of the domain.

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

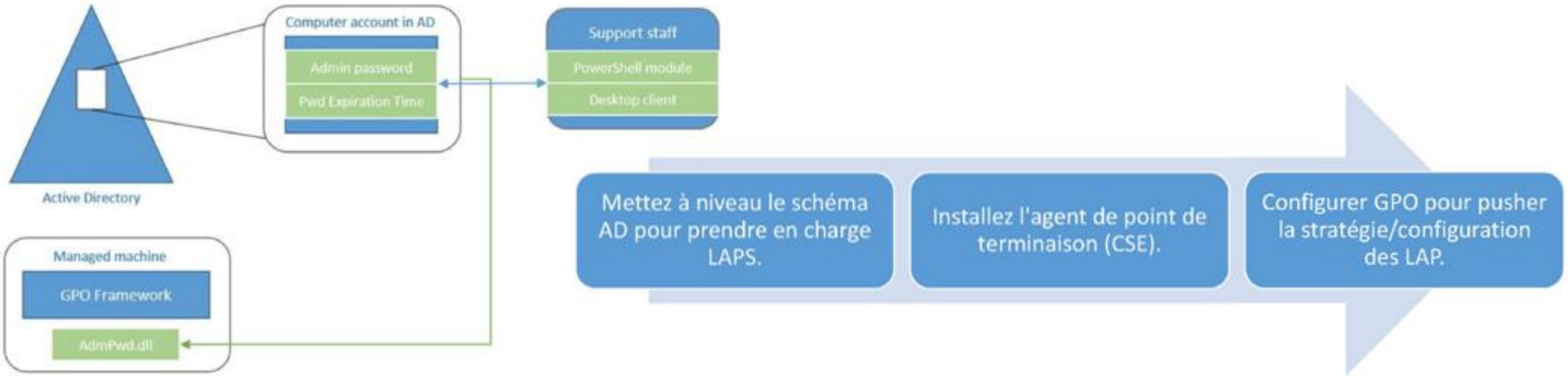


NOS JOURNAUX

- **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 récurant dans les SI : Pasword Reuse (réutilisation des mots de passes)
- Peut facilement être utilisé par des attaquant 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 (joints au domaine)



LAPS

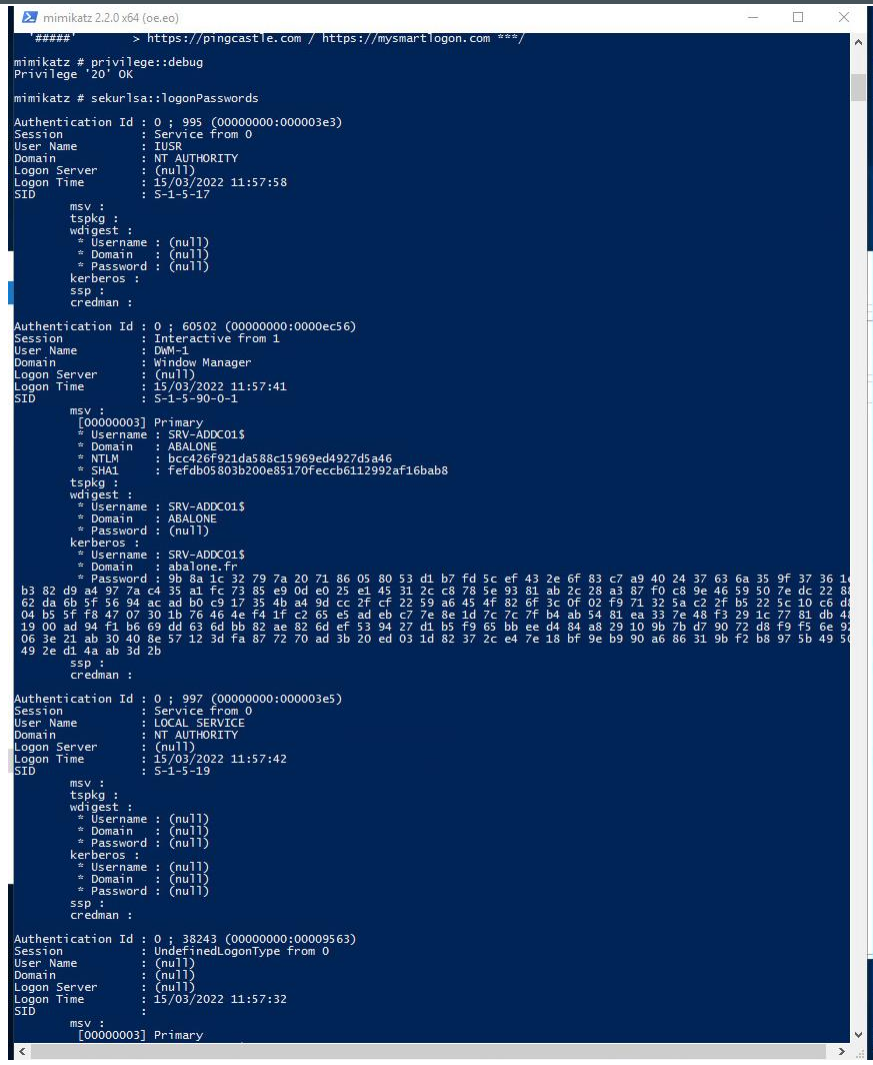
- Installation : https://www.it-connect.fr/securite-proteger-les-comptes-administrateur-local-avec-laps/

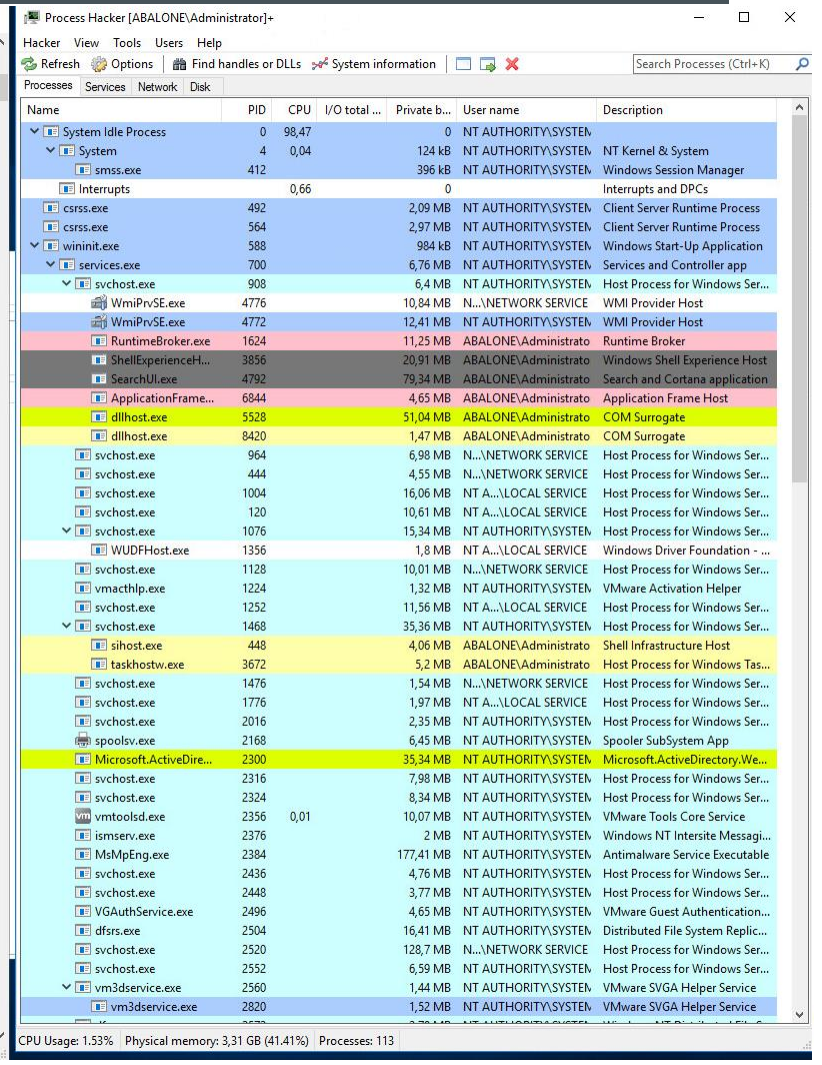
LOCAL SECURITY AUTHORITY SUBSYSTEM SERVICE

- 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

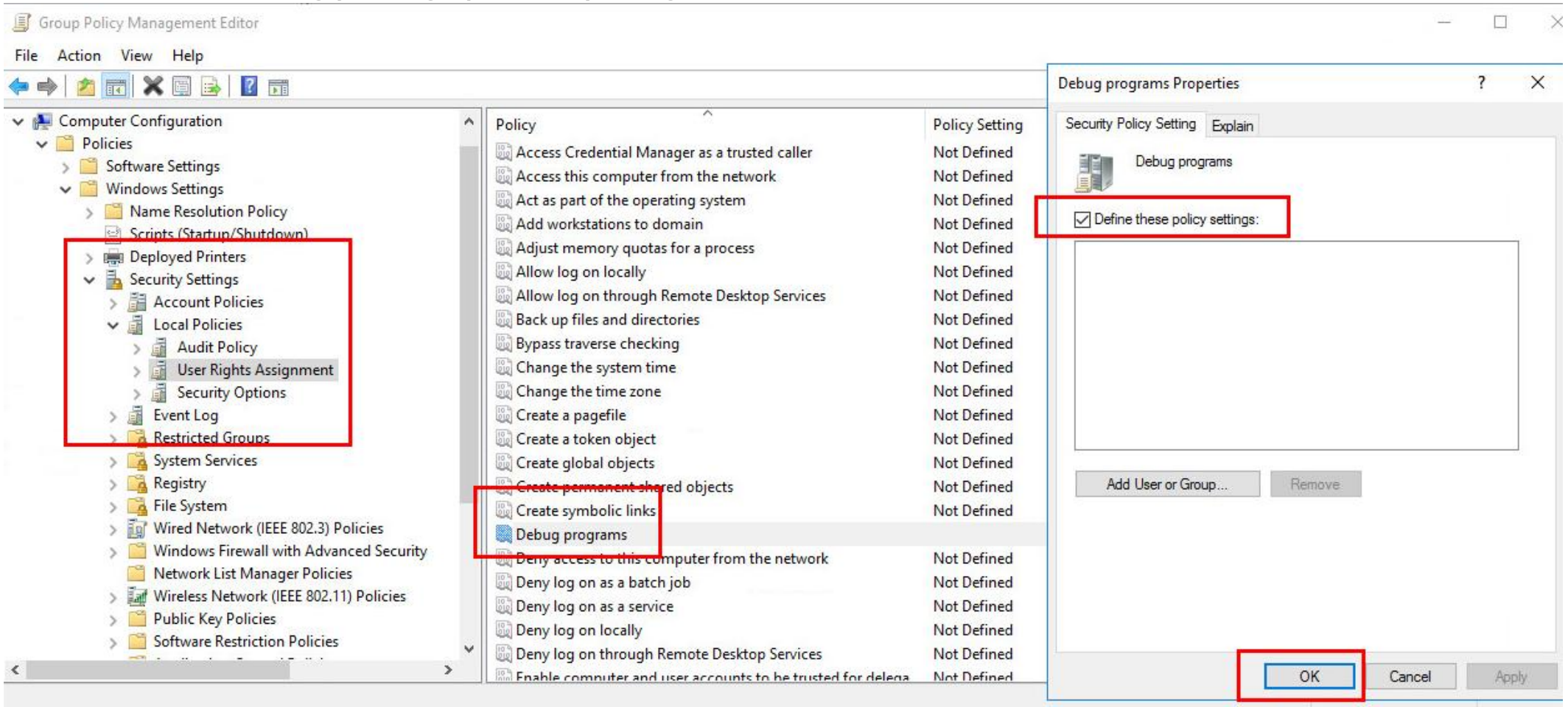
- mimikatz : Permet de récupérer différentes informations des comptes utilisateurs
  - On récupère les hash des mots de passe ou récupère des infos pour par exemple cracker des mots de passes
- process hacker : Petit soft qui gère les processus avec l'aide lsass.exe. (Permet par exemple de dump des process)





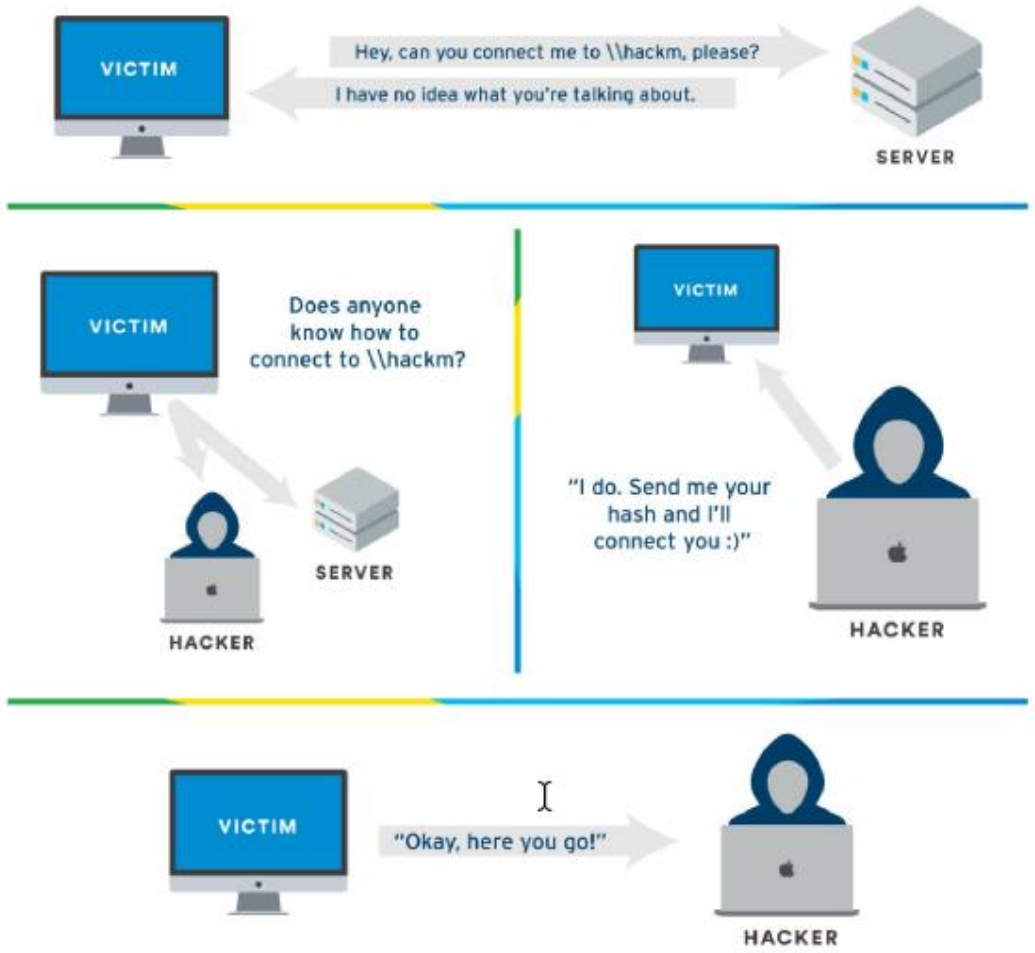
LOCAL SECURITY AUTHORITY SUBSYSTEM SERVICE

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



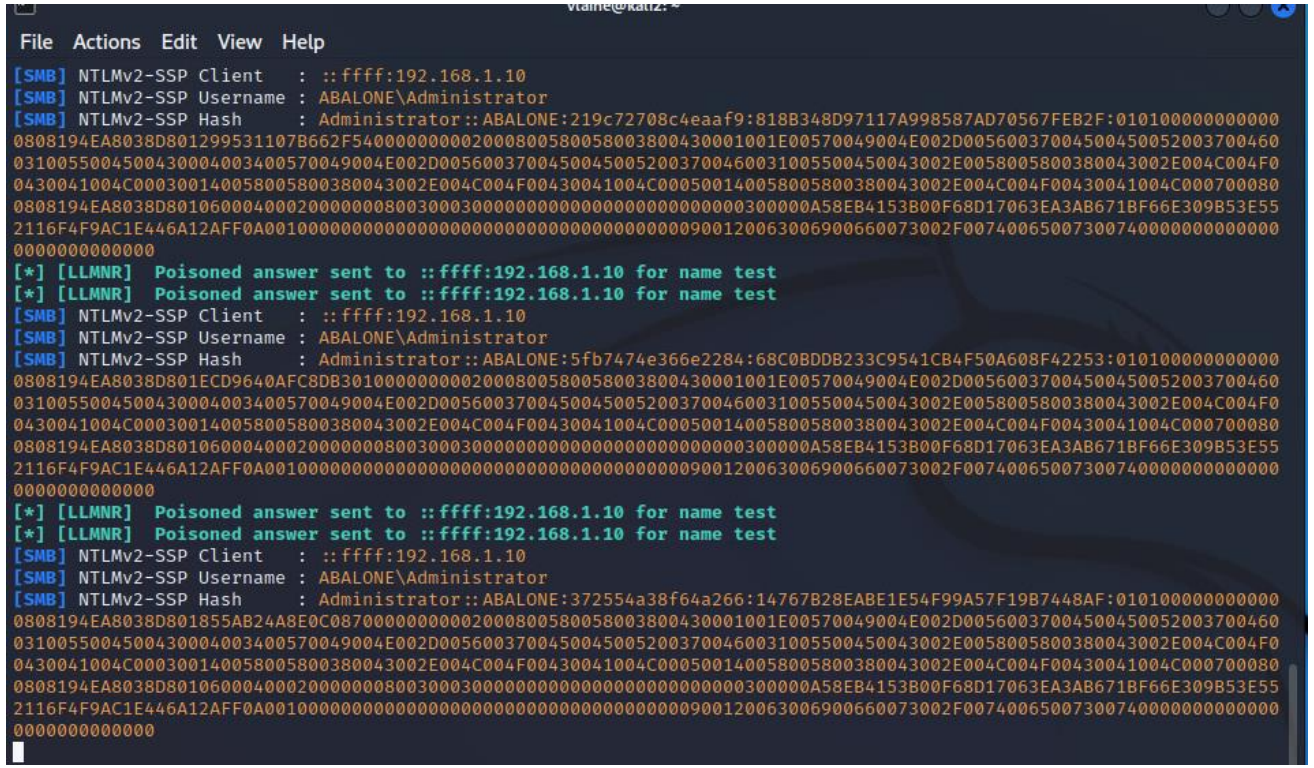
LLMNR/NBT-NS POISONING

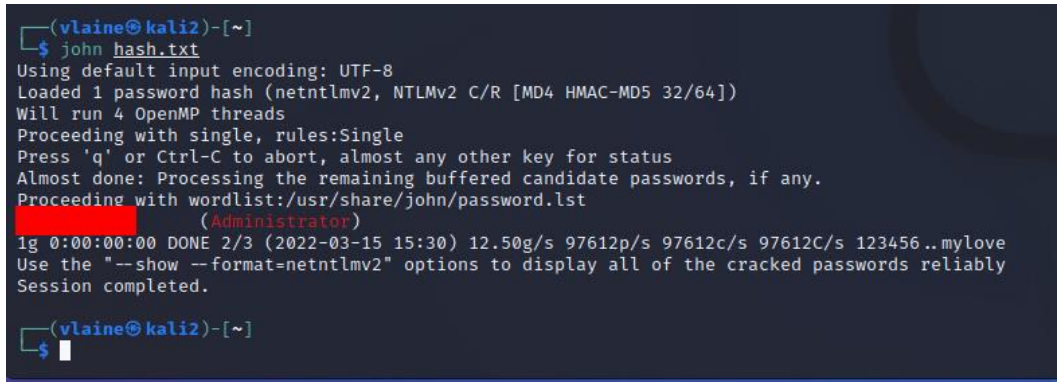
- Permet de récupérer des informations/hash ou prendre le contrôle de machines/utilisateurs qui sont accessible sur le réseau en empoisonnant les requêtes netbios.
  - Il fait partie des protocoles les plus vulnérables.
  - Protocole qui fonctionne en broadcast
  - Va chercher des records appropriés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



LLMNR/NBT-NS POISONING

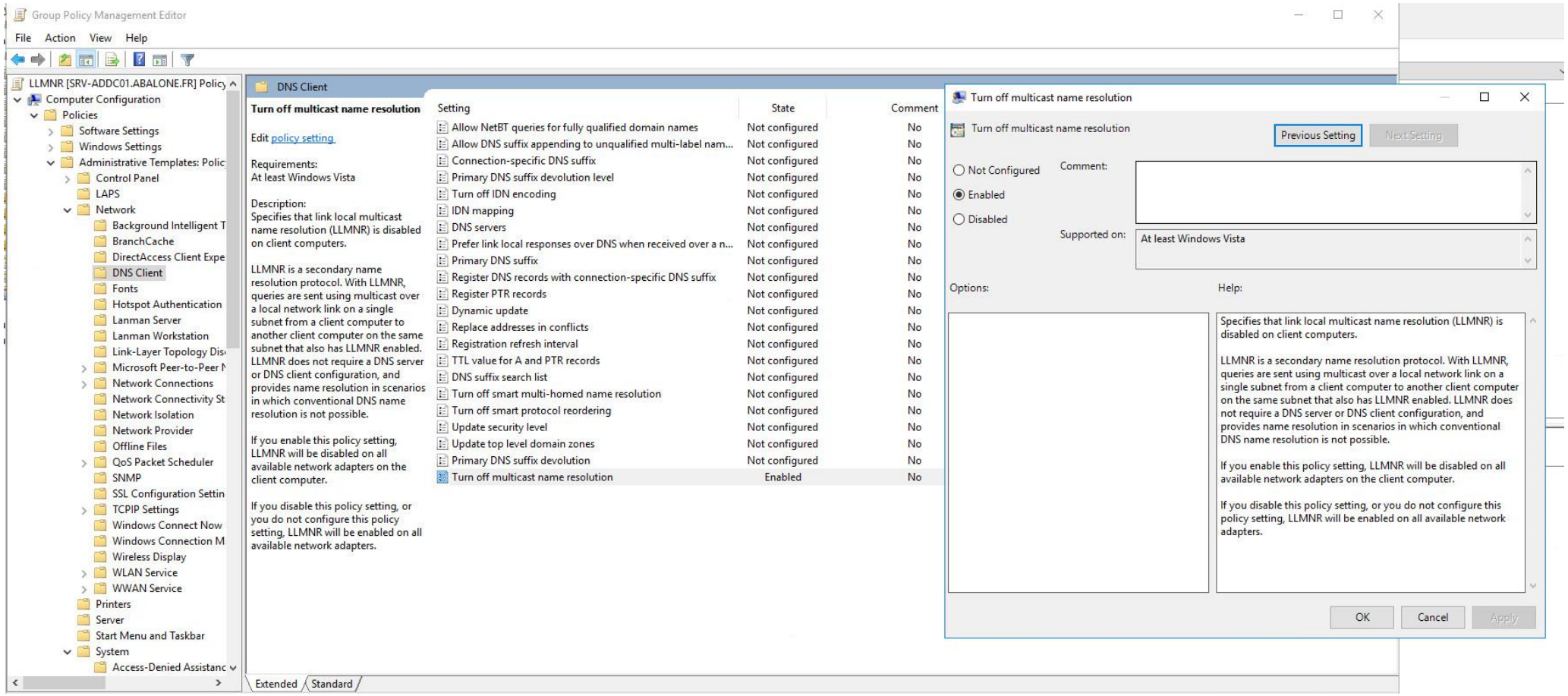
- Test d'attaques :
- Ouvrez votre Kali
- sudo responder -I eth0 -wv
- Lancer un faux partage sur votre AD
  - \\partegaerronée





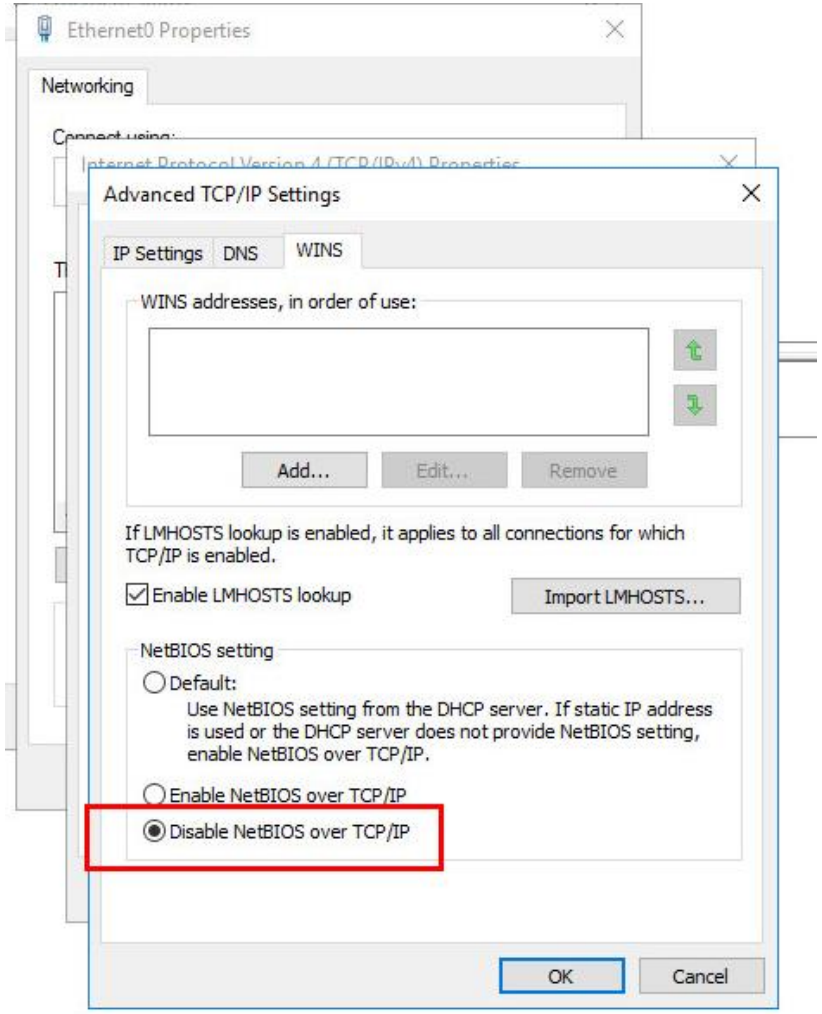
LLMNR/NBT-NS POISONING

- Désactiver le LLMNR



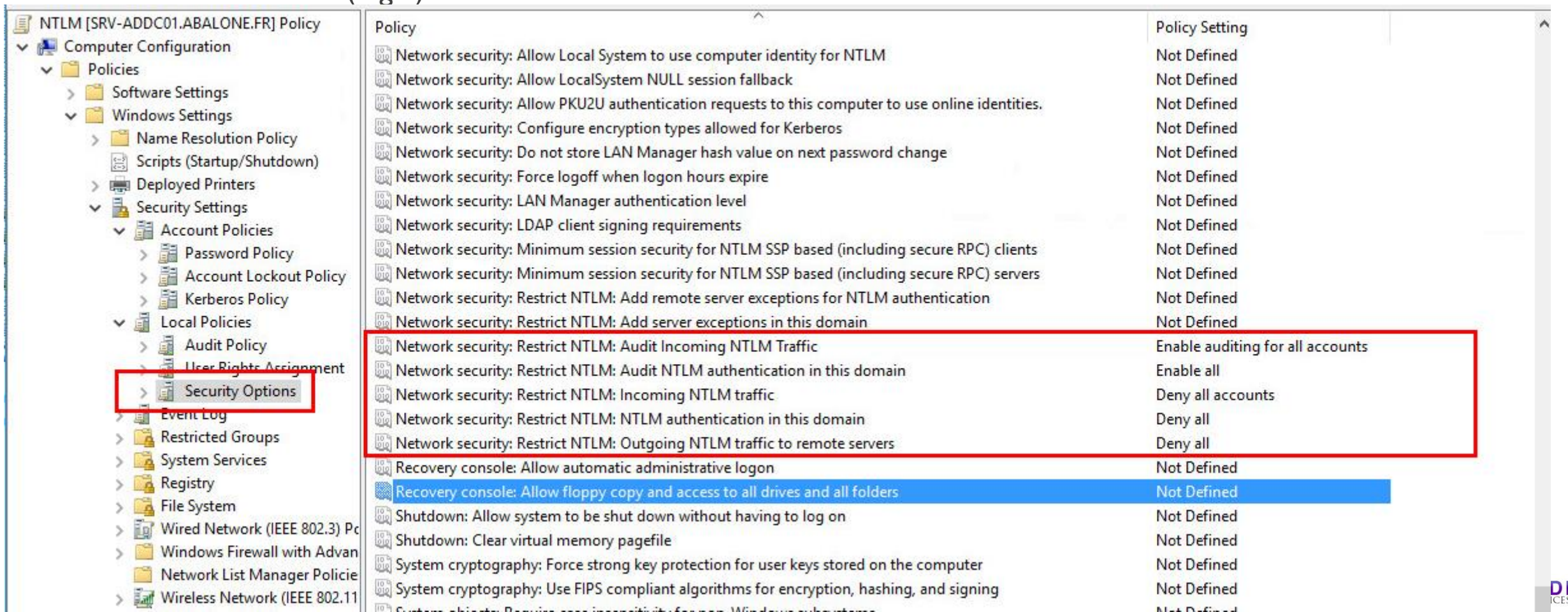
LLMNR/NBT-NS POISONING

- Désactiver le NETBIOS



LLMNR/NBT-NS POISONING

- Désactiver le NTLM (login)

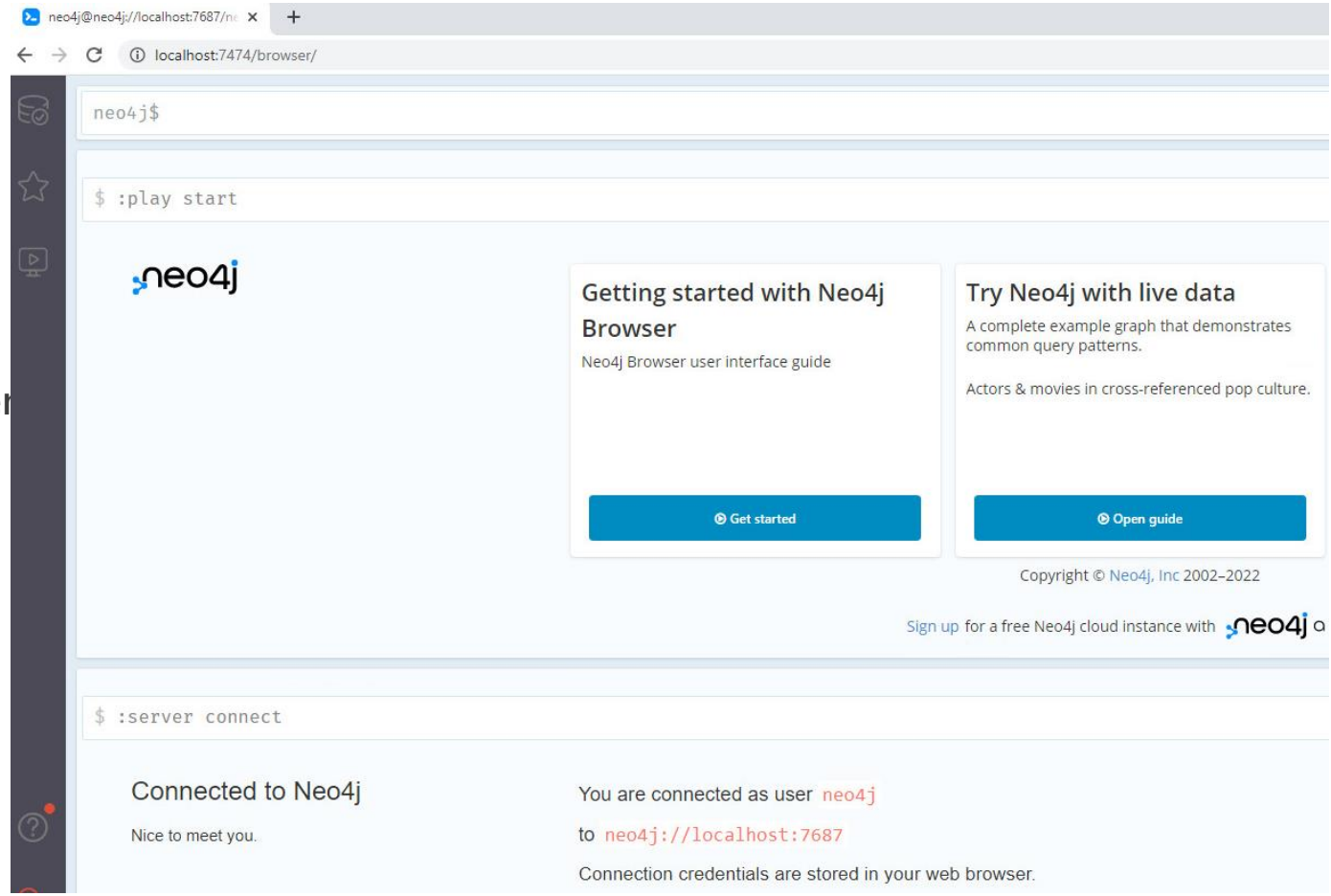


DURCISSEMENT WINDOWS BLOODHOUND

- 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 autre composé de trois éléments :
  - Neo4J (BDD)
  - l'applis Bloodhound
  - l'applis SharpHound ou scripts

DURCISSEMENT WINDOWS NEO4J

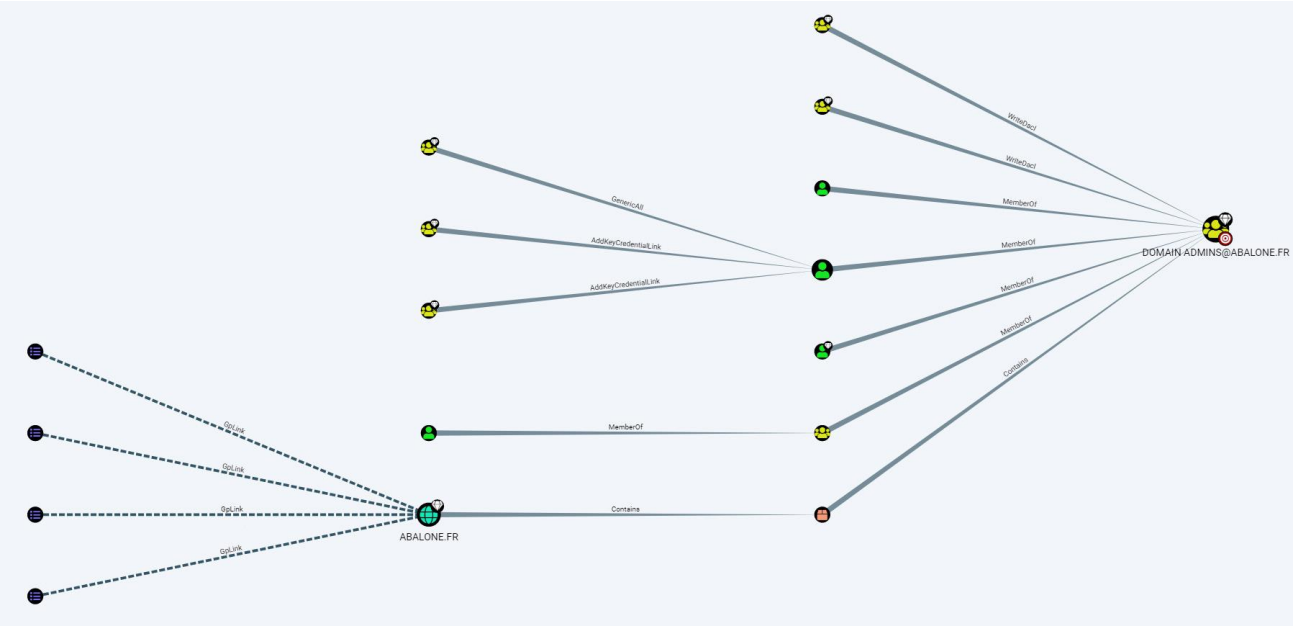
- Une base de données de graphes
- Capable de découvrir des relations et calculer le chemin le plus court entre les objets en utilisant ses liens
- Ici seront les informations sensibles
- Login / MDP par défaut : neo4j/neo4j



ANDN SERVICES

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

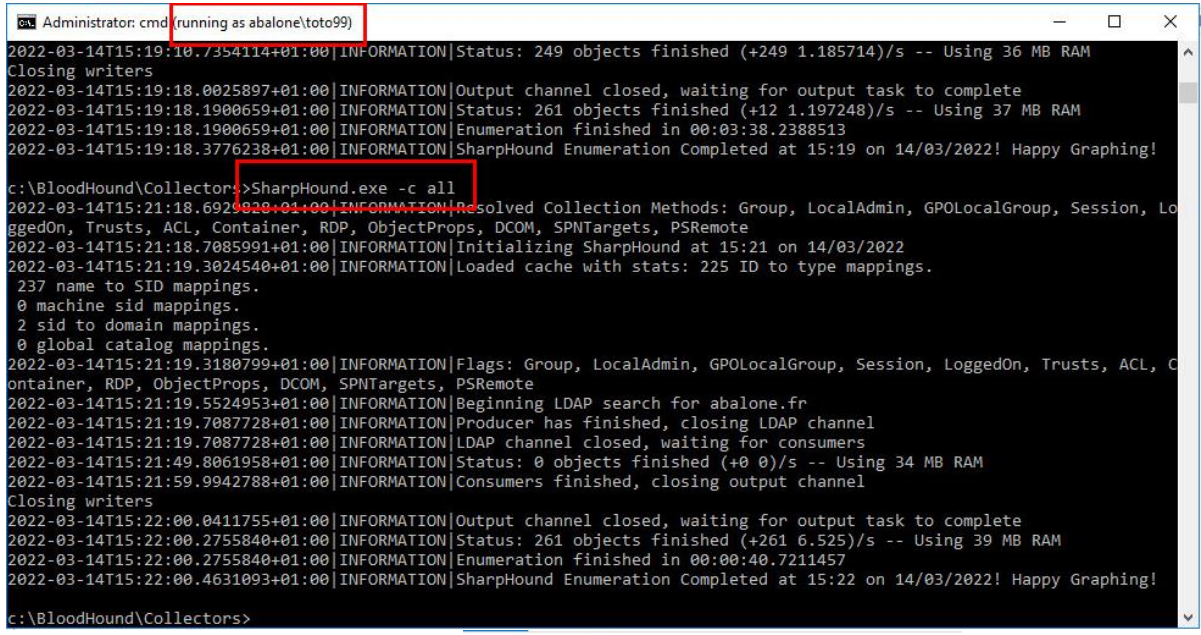
- Démo :
- Utilisation de Bloodhound
  - deux comptes utilisateurs tech1 et user1 du domaine, avec aucun privilège particulier

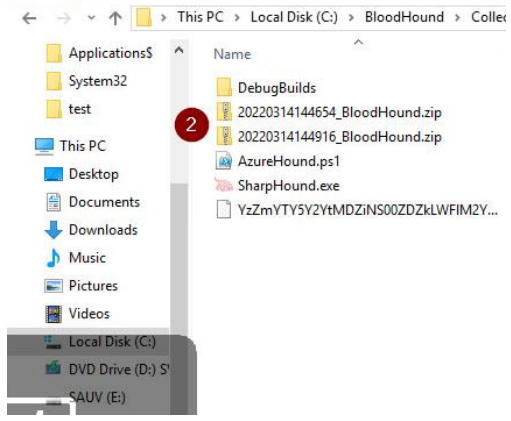
https://www.itpro.fr/cybersecurite-techniques-de-cartographie-active-directory-avec-bloodhound/

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

TP - Installer BloudHound

- 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





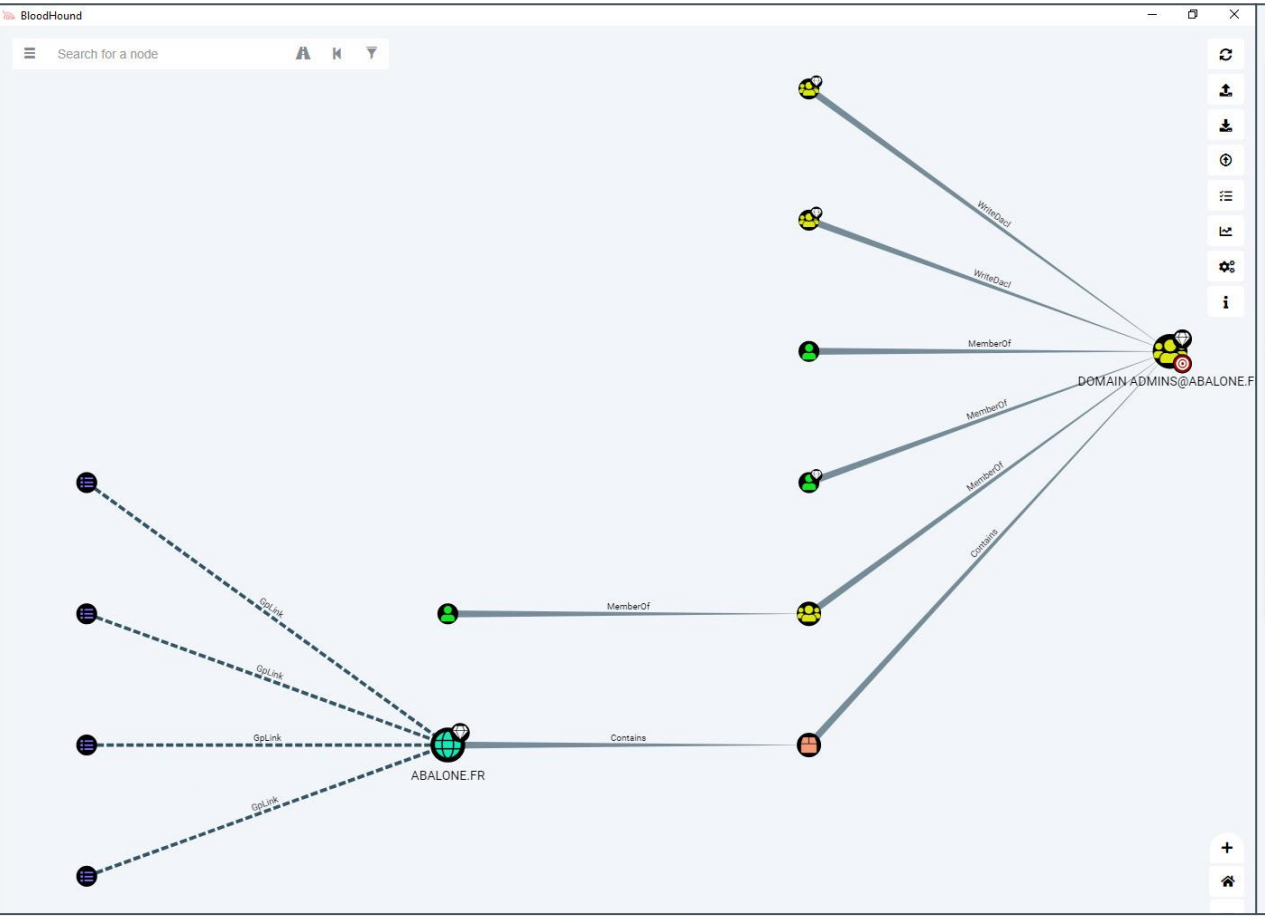
ANDN SERVICES

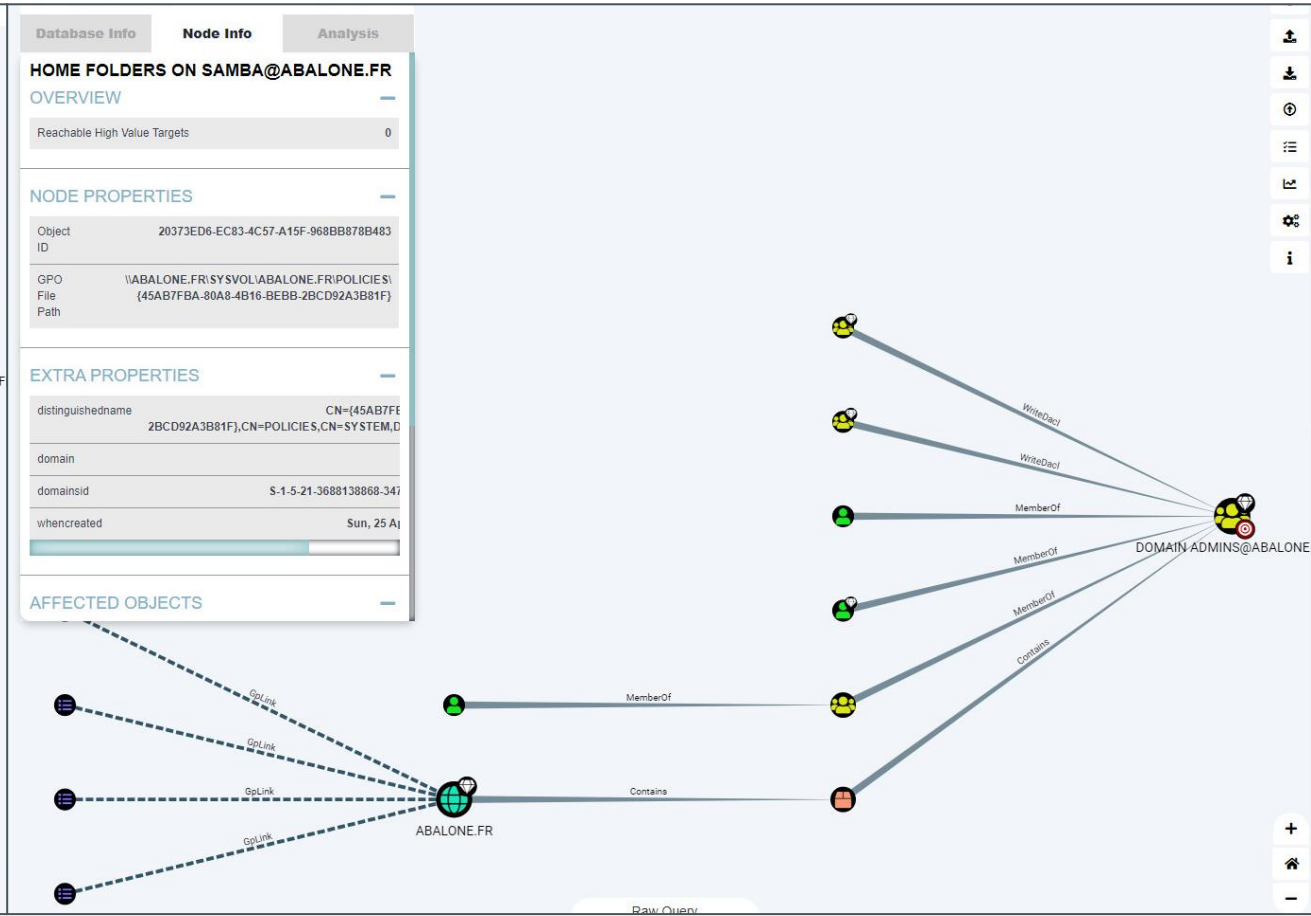
TESTER DIRECTEMENT EN CMD

- runas /user:info\user1 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 → Clique 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