Présentation de l'outil PingCastle, scénarios et actions de correction
autres outils avec Oradad, Forest Druid

Gaëtan CORLE, Michel GOILLANDEAU, Richard FERRERE

13 juin 2024

Présentation de l'outil PingCastle, scénarios et actions de correction
autres outils avec Oradad, Forest Druid

Gaëtan CORLE, Michel GOILLANDEAU, Richard FERRERE

13 juin 2024

Sommaire

Présentation de l'outil PingCastle

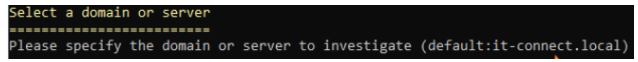
Outil d'audit et de diagnostic de sécurité pour l'AD

- Français et 2015, gratuit, facile à installer (Github) et à utiliser
- Identifier les vulnérabilités et failles (analyse complète)
- Proposer des mesures correctives
- Générer des rapports (risques potentiels)

Quels types d'actions correctives ?

- Comptes à risque (mot de passe n'expire jamais, comptes inactifs)
- Configuration de la sécurité (complexité des mots de passe, protocoles obsolètes)
- Permissions (comptes avec privilèges élevés, groupes avec accès étendus, droits Administrateurs non justifiés)
- Politique de sécurité et journaux (mot de passe, verrouillage des comptes, GPO, évènements suspects)

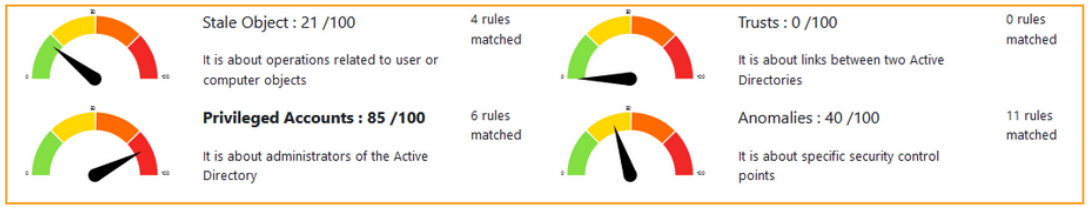
Réaliser l'audit de l'AD avec PingCastle



4 étapes très rapides !

1. Lancer **PingCastle.exe** qui ouvre un terminal
2. Appuyer sur **1-healthcheck-Score the risk of a domain**
3. Valider avec la touche **Entrée** (pour accepter le domaine découvert)
4. A la fin appuyer sur **les touches CTRL+C** et **non PAS sur Entrée** car sinon un traffic vers le serveur web (67.26.25.254) !
5. 2 rapports aux formats XML et **HTML à lire**

Cases orange et rouge = risques –> Corrections à apporter !



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

Protocole NTLM version 1 (15 points)

Stale Objects 1 : Interdire l'utilisation des protocoles NTLMv1 et LM non sécurisés

Ensure that the NTLMv1 and old LM protocols are banned

Rule ID:
S-OldNtlm

Description:
The purpose is to check if NTLMv1 or LM can be used by DC

Technical explanation:
NTLMv1 is an old protocol which is known to be vulnerable to cryptographic attacks.
It is typically used when a hacker sniffs the network and tries to retrieve NTLM hashes which can then be used to impersonate users.

This attack can be combined with coerced authentication attacks - a hacker forces the DC to connect to a controlled host.
In this case, NTLMv1 can be specified so the hacker can retrieve the NTLM hash of the DC, impersonates it and then take control of the domain.
This attack is still possible with NTLMv2 but this is more difficult.

Windows has default security settings regarding LM/NTLM. Windows XP: Send LM & NTLM responses; Windows Server 2003: Send NTLM response only; Vista/2008; Win7/2008 R2: Send NTLMv2 response only.

However Domain Controllers have relaxed default settings to accept the connection of older operating systems.
That means that by default, NTLMv1 is accepted on domain controllers.
If no GPO defines the LAN Manager Authentication Level, the DC fall back to the non secure default.

Advised solution:
After an audit of NTLMv1 usage (see the links below), you need to raise the LAN Manager Authentication Level to "Send NTLMv2 response only. Refuse LM & NTLM".
This can be done by editing the policy "Network security: LAN Manager authentication level" which can be accessed in Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options
The policy will be applied after a computer reboot.

Beware that you may break software which is not compatible with Ntlmv2 such as very old Linux stacks or very old Windows before Windows Vista.
But please note that Ntlmv2 can be activited on all Windows starting Windows 95 and other operating systems.

Points:
15 points if present

Documentation:
https://learn.microsoft.com/en-us/troubleshoot/windows-server/windows-security/audit-domain-controller-ntlmv1
https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-restrict-ntlm-ntlm-authentication-in-this-domain
https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-lan-manager-authentication-level
https://learn.microsoft.com/en-us/troubleshoot/windows-client/windows-security/enable-ntlm-2-authentication
[MITRE|T1557.001 Man-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay
[ERIANSSI - Recommandations de sécurité relatives à Active Directory - R37 [paragraph 3.6.2.1]

Details:
The detail can be found in Security settings

GPO	Value
Windows default without an active GPO	3

Stale Objects : 31 /100

It is about operations related to user or computer objects

Protocole NTLM, quésako ?

Stale Objects 1 : Interdire l'utilisation des protocoles NTLMv1 et LM non sécurisés

Qu'est ce que c'est ?

NTLMv1 et **LM** (**L**AN **M**anager) sont deux protocoles d'authentification utilisés par les systèmes Windows pour vérifier l'identité des utilisateurs et des ordinateurs sur un réseau.

Pourquoi NTLMv1 et LM sont dangereux ?

Possèdent des **failles de sécurité importantes** :

- **Attaques par relayage NTLM**

Un attaquant peut intercepter et modifier les communications d'authentification **NTLMv1** entre un utilisateur et un serveur, lui permettant de se connecter au serveur en se faisant passer pour l'utilisateur légitime.

- **Vol de hachage**

Les hachages des mots de passe stockés pour **NTLMv1** et **LM** peuvent être facilement volés et utilisés pour se connecter à des systèmes sans connaître le mot de passe réel.

Type de réponse par défaut

⇒ Windows XP: **LM & NTLM**

⇒ Windows Server 2003: **NTLM**

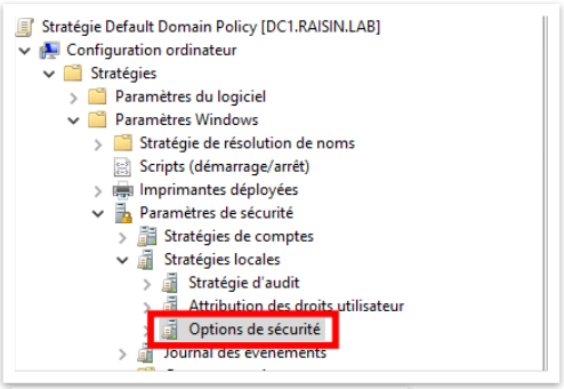
⇒ Vista/2008: Win7/2008 R2: **NTLMv2**

Cependant, les contrôleurs de domaine ont des **paramètres par défaut assouplis** pour accepter la connexion des anciens systèmes d'exploitation.

Cela signifie que **par défaut**, **NTLMv1 est accepté** sur les contrôleurs de domaine.

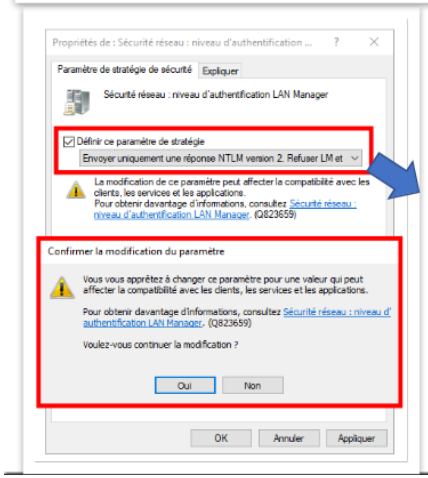
Comment désactiver NTLM ?

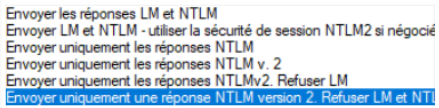
Stale Objects 1 : Interdire l'utilisation des protocoles NTLMv1 et LM non sécurisés

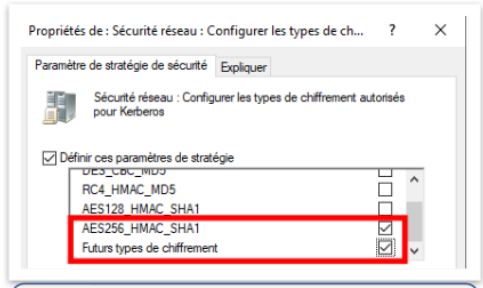


Autres GPOs disponibles

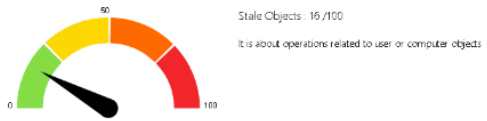
- ✅ Authentifications NTLM dans le domaine
- ❌ Comptes de domaine > NTLMv1 > serveurs de domaine [sauf exceptions]
- ❌ Comptes de domaine > NTLMv1 > contrôleurs de domaine [sauf exceptions]
- ❌ Serveurs de domaine > NTLMv1 > serveurs de domaine [sauf exceptions]
- ❌ Tout NTLM [sauf exceptions]
- ✅ Tout NTLM [sauf exceptions]







En bonus ... penser à désactiver les types de chiffrements obsolètes



Enregistrement et jonction à un domaine **(10 points)**

Stale Objects 2 : Vérifier le processus d'enregistrement des ordinateurs sur le domaine

Check the process of registration of computers to the domain

Rule ID:
S-ADRegistration

Description:
The purpose is to ensure that basic users cannot register extra computers in the domain

Technical explanation:
By default, a basic user can register up to 10 computers within the domain. This default configuration represents a security issue as basic users shouldn't be able to create such accounts and this task should be handled by administrators.

Note: this program checks also the GPO for SeMachineAccountPrivilege assignment. This assignment can be used to restrict the impact of the key ms-DS-MachineAccountQuota.

Advised solution:
To solve the issue, limit the number of extra computers that can be registered by a basic user. It can be reduced by modifying the value of *ms-DS-MachineAccountQuota* to zero (0). Another solution can be to remove the "Authenticated Users" group in the domain controllers policy altogether. Do note, that if you need to set delegation to an account, so it can add computers to the domain, it can be done through 2 methods: Delegation in the OU or by assigning the *SeMachineAccountPrivilege* to a special group

Points:
10 points if present

Documentation:
https://docs.microsoft.com/troubleshoot/windows-server/identity/default-workstation-numbers-join-domain
http://prajwaldesai.com/allow-domain-user-to-add-computer-to-domain/
http://blog.backslasher.net/preventing-users-from-adding-computers-to-a-domain.html
[MITRE]Mitre Att&ck - Mitigation - User Account Management

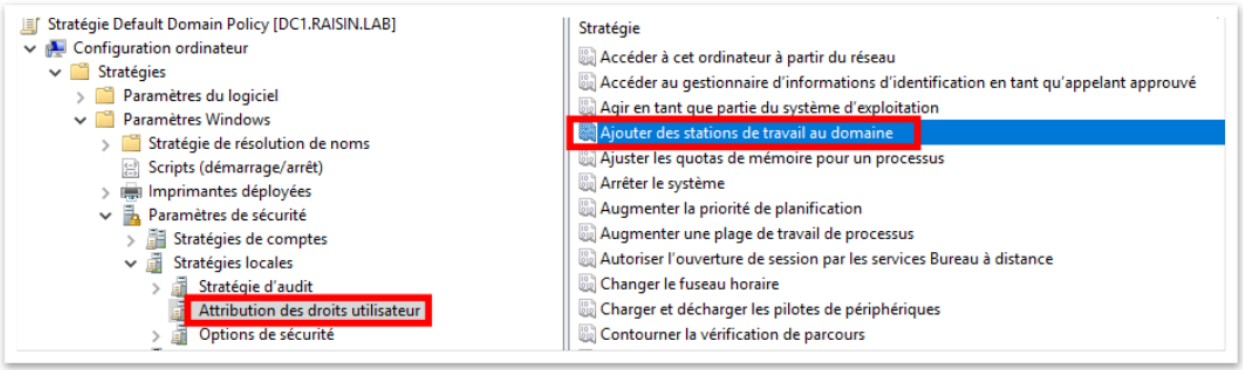
Vérification de la stratégie d'ajout

Stale Objects 2 : Vérifier le processus d'enregistrement des ordinateurs sur le domaine

Qu'est ce que c'est ?

Par défaut :

- tous les **utilisateurs authentifiés** peuvent ajouter jusqu'à **10 ordinateurs**.
- si **autorisations spéciales**, ils peuvent ajouter **plus d'ordinateurs** et devenir propriétaires des comptes d'ordinateurs.



Connaître la valeur de la variable ms-DS-MachineAccountQuota :

```
PS C:\Users\Administrateur> get-addomain | select -exp DistinguishedName | get-adobject -prop 'ms-DS-MachineAccountQuota' | select -exp ms-DS-MachineAccountQuota
10
```

Comment vérifier et désactiver ?

Stale Objects 2 : Vérifier le processus d'enregistrement des ordinateurs sur le domaine

Vérifier si un utilisateur a déjà joint une machine, et si oui, afficher laquelle :

```
PS C:\Windows\system32> get-adcomputer -fi {ms-DS-CreatorSID -like '*'} -prop ms-DS-CreatorSID | group ms-DS-CreatorSID | %{
    $ret = $_ | select Count,@{name='UserName';Expression={$_.Name}},@{name='ComputerNames';Expression={$_.Group | select -exp Name}}
    # Try to resolve the SID into an account
    try{
        $_.Name = $_.Name.Translate([System.Security.Principal.NTAccount])
    }catch{}
    $ret
}

Count UserName                                         ComputerNames
----- --------                                         -------------
    1 S-1-5-21-2831087528-748371308-1960284351-1105 WIN10-USER
```

```
PS C:\Windows\system32> wmic useraccount|findstr 1105
512         RAISIN\user-1                                      FALSE     RAISIN  Tommy Jones            FALSE       FALSE   user-1
    S-1-5-21-2831087528-748371308-1960284351-1105  1        OK
```

Mettre la variable à 0 et vérifier :

```
PS C:\Windows\system32> (Get-ADObject -Identity "DC=raisin,DC=lab" -Server "dc1" -Properties "ms-DS-MachineAccountQuota")."ms-DS-MachineAccountQuota"
10
PS C:\Windows\system32> Set-ADObject -Identity "DC=raisin,DC=lab" -Replace @{"ms-DS-MachineAccountQuota"=0} -Server "dc1"
PS C:\Windows\system32> (Get-ADObject -Identity "DC=raisin,DC=lab" -Server "dc1" -Properties "ms-DS-MachineAccountQuota")."ms-DS-MachineAccountQuota"
0
```

Stale Objects : 6 /100

It is about operations related to user or computer objects

Configuration réseau si multi sites **(5 points)**

Stale Objects 3 : Vérifier l'intégrité de la configuration réseau

Check for completeness of network declaration

Rule ID:
S-DC-SubnetMissing

Description:
The purpose is to ensure that the minimum set of subnet(s) has been configured in the domain

Technical explanation:
When multiple sites are created in a domain, networks should be declared in the domain in order to optimize processes such as DC attribution. In addition, PingCastle can collect the information to be able to build a network map. This rule has been triggered because at least one domain controller has an IP address which was not found in subnet declaration. These IP addresses have been collected by querying the DC FQDN IP address in both IPv6 and IPv4 format.

Advised solution:
Locate the IP address which was found as not being part of declared subnet, then add this subnet to the "Active Directory Sites" tool. If you have found IPv6 addresses and it was not expected, you should disable the IPv6 protocol on the network card.

Points:
5 points if present

Documentation:
[MITRE]Mitre Att&ck - Mitigation - Active Directory Configuration

Details:
The detail can be found in Domain controllers

Domain controller	ip
DC2	
DC1	

Stale Objects : 6 /100

It is about operations related to user or computer objects

En quoi cela consiste ?

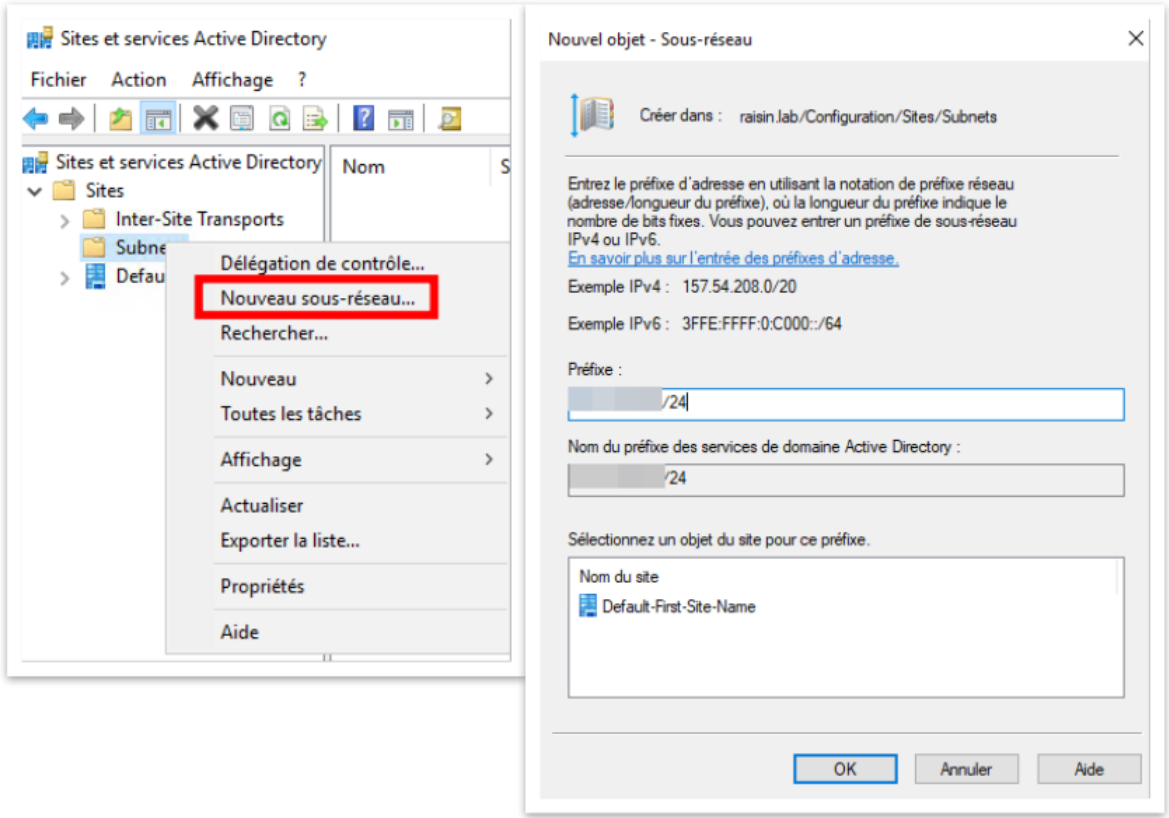
Stale Objects 3 : Vérifier l'intégrité de la configuration réseau

Qu'est ce que c'est ?

Lorsqu'il existe plusieurs sites dans un domaine, il est recommandé de déclarer les réseaux au sein du domaine afin d'optimiser des processus tels que l'attribution des contrôleurs de domaine (DC)

Comment le faire ?

Stale Objects 3 : Vérifier l'intégrité de la configuration réseau



Stale Objects : 1 /100

It is about operations related to user or computer objects

Délégation sur le compte Administrateur (20 points)

Privileged Account 1 : Vérifier si tous les comptes privilégiés font partie du groupe spécial Utilisateurs protégés

At least one administrator account can be delegated

Rule ID:
P-Delegated

Description:
The purpose is to ensure that all Administrator Accounts have the configuration flag "this account is sensitive and cannot be delegated" (or are members of the built-in group "Protected Users" when your domain functional level is at least Windows Server 2012 R2).

Technical explanation:
Without the flag "This account is sensitive and cannot be delegated" any account can be impersonated by some service account. It is a best practice to enforce this flag on administrators accounts.

Advised solution:
To correct the situation, you should make sure that all your Administrator Accounts have the check-box "This account is sensitive and cannot be delegated" active or add your Administrator Accounts to the built-in group "Protected Users" if your domain functional level is at least Windows Server 2012 R2 (some functionalities may not work properly afterwards, you should check the official documentation).
If you want to enable the check-box "This account is sensitive and cannot be delegated" but this is not possible because the box is not present (typically for GMSA accounts), you can add the flag manually by adding the number 1048576 to the attribute useraccountcontrol of the account.
Please note that there is a section below in this report named "Admin Groups" which gives more information.

Points:
20 points if present

Documentation:
[US]STIG V-36435 - Delegation of privileged accounts must be prohibited.
[MITRE]Mitre Att&ck - Mitigation - Active Directory Configuration

Details:
The detail can be found in Admin Groups

Privileged Accounts : 50 /100

It is about administrators of the Active Directory

En quoi cela consiste ?

Privileged Account 1 : Vérifier si tous les comptes privilégiés font partie du groupe spécial Utilisateurs protégés

Qu'est ce que c'est ?

Le groupe "Utilisateurs protégés" est un **groupe de sécurité global** Active Directory (AD) conçu pour se **défendre contre les vols de identifiants**. Ce groupe déclenche une protection non-configurable sur les appareils et les ordinateurs hôtes afin **d'empêcher la mise en cache des identifiants** lorsque les membres du groupe se connectent.

Protections offertes par les contrôleurs de domaine pour les utilisateurs protégés

Les comptes d'utilisateurs protégés qui s'authentifient sur un domaine exécutant Windows Server 2012 R2 ou une version ultérieure ne peuvent pas effectuer les actions suivantes :

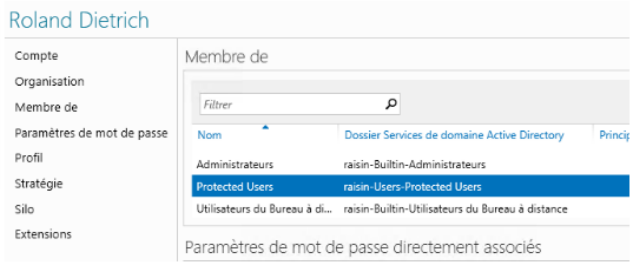
- S'authentifier avec l'authentification **NTLM.**
- Utiliser les types de chiffrement **DES** ou **RC4** dans la **pré-authentification Kerberos**.
- **Déléguer des droits** avec délégation contrainte ou non contrainte.
- **Renouveler** les tickets d'octroi de **ticket Kerberos** (TGT) au-delà de leur **durée de vie** initiale de **quatre heures**.

Administrateurs / Protected Users

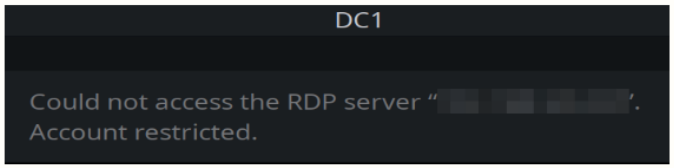
Privileged Account 1 : Vérifier si tous les comptes privilégiés font partie du groupe spécial Utilisateurs protégés

Group Name	Nb Admins
Account Operators	0
Administrators	2

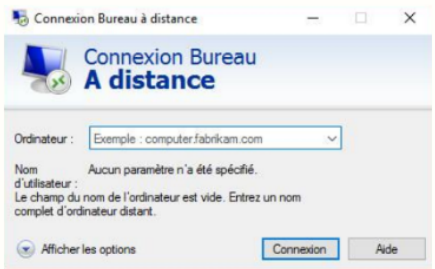
SamAccountName	Enabled	Active	Pwd never Expired
Administrateur	YES	YES	YES
rdp	YES	YES	NO



- Connexion via Remmina ❌ (NTLM)



- Connexion via Bureau à Distance ✅



Attention aux services distants, par exemple NAS joint à un domaine via un compte qui a utilisé l'authentification NTLM !

Privileged Accounts : 20 /100

It is about administrators of the Active Directory

Corbeille pour les objets de l'AD **(10 points)**

Privileged Account 2 : Activer la corbeille pour les objets ActiveDirectory

Ensure that the Recycle Bin feature is enabled

Rule ID:
P-RecycleBin

Description:
The purpose is to ensure that the Recycle Bin feature is enabled

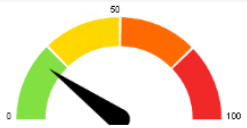
Technical explanation:
The Recycle Bin avoids immediate deletion of objects (which can still be partially recovered by its tombstone). This lowers the administration work needed to restore. It also extends the period where traces are available when an investigation is needed.

Advised solution:
First, be sure that the forest level is at least Windows Server 2008 R2.
You can check it with Get-ADForest or in the Domain Information section.
Then you can enable it using the PowerShell command:
Enable-ADOptionalFeature -Identity 'Recycle Bin Feature' -Scope ForestOrConfigurationSet -Target 'test.mysmartlogon.com'

Points:
10 points if present

Documentation:
https://enterinit.com/powershell-enable-active-directory-recycle-bin
[MITRE]Mitre Att&ck - Mitigation - Audit

Details:
The detail can be found in Domain Information



Privileged Accounts : 20 /100

It is about administrators of the Active Directory

Activation de la corbeille AD

Privileged Account 2 : Activer la corbeille pour les objets ActiveDirectory

Avantage de la corbeille Active Directory

Elle permet aux utilisateurs de **récupérer des objets Active Directory** sans avoir à effectuer une **restauration** à partir d'une sauvegarde et sans être obligés de **redémarrer les services** de domaine Active Directory ou les contrôleurs de domaine (DC).

Inconvénient de la corbeille Active Directory

- Modification du schéma **non réversible** sans une restauration complète de la forêt Active Directory.
- La **taille** de l'Active Directory augmente : **Deleted** + **Recycled**.
- Supprime définitivement tous les objets **Recycled**.

Fonctionnement

Quand activée, la suppression d'un objet conserve ses attributs un certain temps : **msDS-DeletedObjectLifetime** = **TombstoneLifetime**

Si : **msDS-DeletedObjectLifetime** = 0 ou rien
Alors : **msDS-DeletedObjectLifetime** = **TombstoneLifetime**

Si **TombstoneLifetime** = 0
Alors, par défaut, **TombstoneLifetime** = **60 jours**

Changement des attributs d'un objet Deleted

- Objet déplacé vers Objets Supprimés.
- Objet renommé : **Common-Name DEL:Object-Guid**
- Nouveaux attributs : **isDeleted / LastKnownParent** / ...

Exemple : compte utilisateur

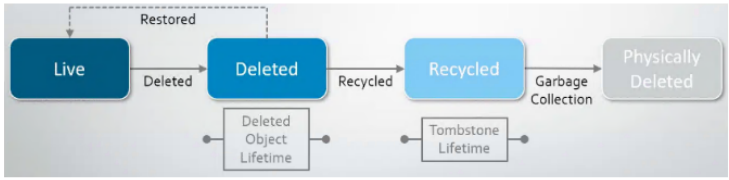
Lors de la suppression :

~~*objectCategory*~~ / ~~*sAMAccountType*~~

Lors de la restauration :

objectClass => objectCategory

userAccountControl => sAMAccountType



Comment activer et vérifier ?

Privileged Account 2 : Activer la corbeille pour les objets ActiveDirectory

```
PS C:\Users\Administrateur> Enable-ADOptionalFeature -Identity 'Recycle Bin Feature'
 -Scope ForestOrConfigurationSet -Target 'raisin.lab'
AVERTISSEMENT : L'activation de « Recycle Bin Feature » sur
« CN=Partitions,CN=Configuration,DC=raisin,DC=lab » est une action
irréversible ! Vous ne pourrez pas désactiver « Recycle Bin Feature » sur
« CN=Partitions,CN=Configuration,DC=raisin,DC=lab » si vous continuez.

Confirmer
Êtes-vous sûr de vouloir effectuer cette action ?
Opération « Enable » en cours sur la cible « Recycle Bin Feature ».
[O] Oui  [T] Oui pour tout  [N] Non  [U] Non pour tout  [S] Suspendre
[?] Aide(la valeur par défaut est « O ») : T
PS C:\Users\Administrateur>
```

```
PS C:\Users\Administrateur> Get-ADOptionalFeature -filter *


DistinguishedName  : CN=Recycle Bin Feature,CN=Optional Features,CN=Directory
                     Service,CN=Windows
                     NT,CN=Services,CN=Configuration,DC=raisin,DC=lab
EnabledScopes      : {CN=NTDS Settings,CN=DC2,CN=Servers,CN=Default-First-Site-Name
                     ,CN=Sites,CN=Configuration,DC=raisin,DC=lab,
                     CN=Partitions,CN=Configuration,DC=raisin,DC=lab, CN=NTDS Setti
                     ngs,CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=C
                     onfiguration,DC=raisin,DC=lab}
FeatureGUID        : 766ddcd8-acd0-445e-f3b9-a7f9b6744f2a
IsDisableable      : False
Name               : Recycle Bin Feature
ObjectClass        : msDS-OptionalFeature
ObjectGUID         : 01da4237-9f7d-45df-a61e-bb2f22e01d64
RequiredDomainMode :
RequiredForestMode : Windows2008R2Forest
```

Privileged Accounts : 10 /100

It is about administrators of the Active Directory

Administrateur du Schéma de l'AD

Privileged Account 3 : Le groupe Administrateurs du Schéma n'est pas vide

Avoid unexpected schema modifications which could result in domain rebuild

Rule ID:
P-SchemaAdmin

Description:
The purpose is to ensure that no account can make unexpected modifications to the schema

Technical explanation:
The group "Schema Admins" is used to give permissions to alter the schema. Once a modification is performed on the schema such as new objects, it cannot be undone. This can result in a rebuild of the domain. The best practice is to have this group empty and to add an administrator when a schema update is required, then remove this group membership.

Advised solution:
Remove the accounts or groups belonging to the "schema administrators" group.

Points:
10 points if present

Documentation:
[FR]ANSSI - Recommandations de sécurité relatives à Active Directory - R13 [subsection 3.2]
[US]STIG V-72835 - Membership to the Schema Admins group must be limited
[MITRE]Mitre Att&ck - Mitigation - Privileged Account Management

Details:
The detail can be found in Admin Groups

Privileged Accounts : 10 /100

It is about administrators of the Active Directory

Administrateur du Schéma de l'AD

Privileged Account 3 : Le groupe Administrateurs du Schéma n'est pas vide

Des modifications sont nécessaires lorsque les définitions préexistantes du schéma ne sont pas adaptées à certains besoins.

- Les modifications du schéma **sont globales** : elles impactent toute la forêt
- Les modifications du schéma **sont irréversibles** mais peuvent être désactivées.

⇒ Laisser le groupe **Administrateur du schéma vide**.

⇒ Ajouter le compte utilisateur faisant l'extension comme membre de ce groupe **le temps de l'opération uniquement**.

[**S**ecurity **T**echnical **I**mplementation **G**uides]

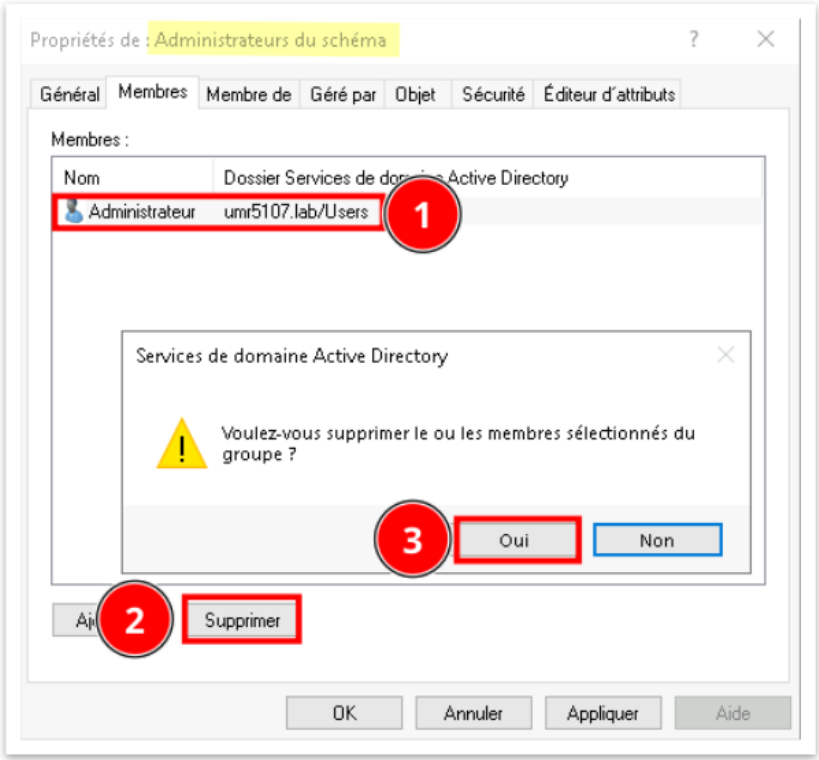
Contenu provenant de sources publiques et non classifiées : comme le **DOD**.

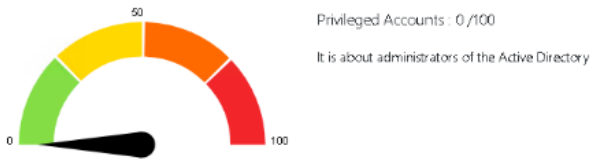
⇒ Laisser le groupe **Administrateur du schéma vide**.

⇒ Ajouter le compte utilisateur faisant l'extension comme membre de ce groupe **le temps de l'opération uniquement**.

Administrateur du Schéma de l'AD

Privileged Account 3 : Le groupe Administrateurs du Schéma n'est pas vide





Politique des mots de passe (10 points)

Anomalies 1 : Définir la longueur minimale des mots de passe

Check for short password length in password policy

Rule ID:
A-MinPwdLen

Description:
The purpose is to verify if the password policy of the domain enforces users to have at least 8 characters in their password

Technical explanation:
A check is performed to identify if the GPO regarding password policy allows less than 8 characters password. Short passwords represent a high risk because they can fairly easily be brute-forced or password sprayed. Most CERT and agencies advise for at least 8 characters (and often this number goes up to 12)

Advised solution:
To solve the issue, the best way is to either remove the GPO enabling short password, or to modify it in order to increase the password length to at least 8 characters

Points:
10 points if present

Documentation:
https://www.microsoft.com/en-us/research/publication/password-guidance/
[FR]ANSSI - Privileged group members with weak password policy (vuln2_privileged_members_password) 2
[MITRE]T1201 Password Policy Discovery

Details:
The detail can be found in Password policies

GPO
Default Domain Policy

Anomalies : 65 /100

It is about specific security control points

Quelle politique pour les mots de passe ? **12 caractères mini et complexité**
Quel niveau d'entropie (? bits)

Anomalies 1 : Définir la longueur minimale des mots de passe

RECOMMANDATIONS RELATIVES ÀL'AUTHENTIFICATION MULTIFACTEUR ETAUX MOTS DE PASSE [ANSSI]

Niveau de sensibilité	Longueur minimale en nombre de caractères	Taille de clé équivalente en bits [5]
Faible à moyen	Entre 9 et 11	≈ 65
Moyen à fort	Entre 12 et 14	≈ 85
Fort à très fort	Au moins 15	≥ 100

TABLE 3 – Recommandations concernant les longueurs minimales des mots de passe

CNIL : niveau minimal générique de **80 bits d'entropie** pour un mot de passe sans mesure complémentaire, et de laisser à chacun le loisir de définir sa politique de mot de passe :

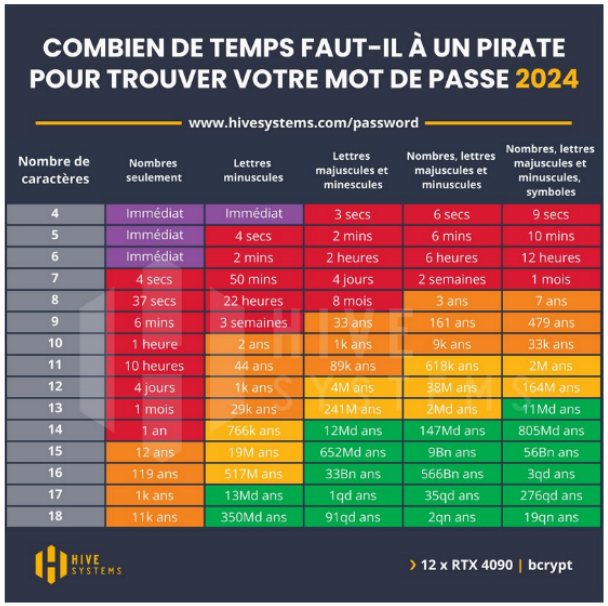
MDP **12 caractères** = A-Z + a-z + 1-9 + Spéciaux

Ou

MDP **14 caractères** = A-Z + a-z + 1-9

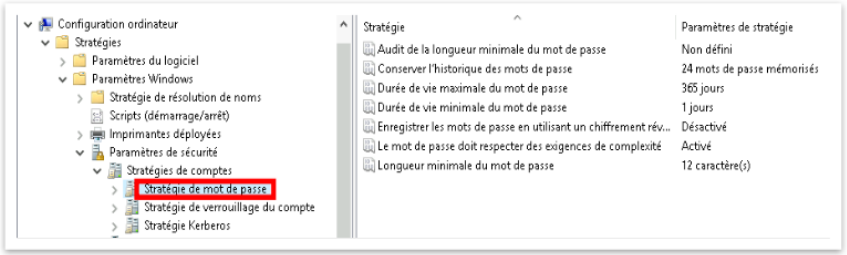
Ou

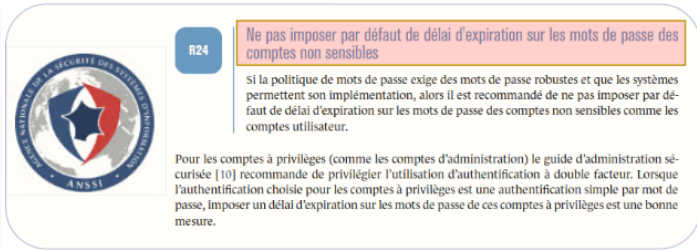
Passphrase de **7 mots** Minimum.

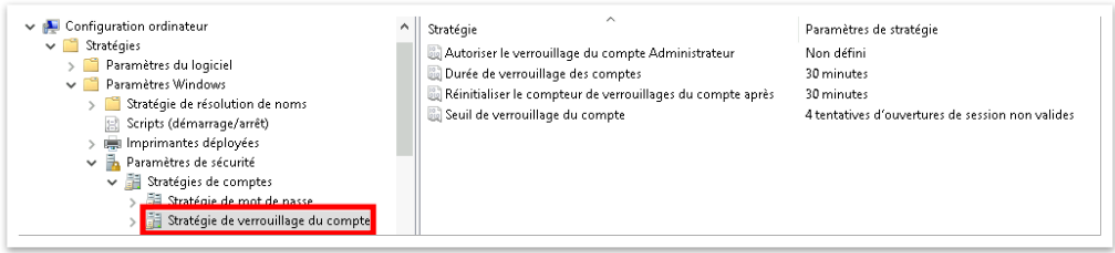


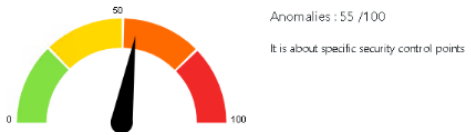
Comment définir cette politique ? Stratégie GPO

Anomalies 1 : Définir la longueur minimale des mots de passe









Service spouleur d'impression (10 points)

Anomalies 2 : Exploitation du service Spouleur pour récupérer les identifiants de L'AD

Ensure that the Print Spooler service cannot be abused to get the DC credentials

Rule ID:
A-DC-Spooler

Description:
The purpose is to ensure that credentials cannot be extracted from the DC via its Print Spooler service

Technical explanation:
When there's an account with unconstrained delegation configured (which is fairly common) and the Print Spooler service running on a computer, you can get that computers credentials sent to the system with unconstrained delegation as a user. With a domain controller, the TGT of the DC can be extracted allowing an attacker to reuse it with a DCSync attack and obtain all user hashes and impersonate them.

Advised solution:
The Print Spooler service should be deactivated on domain controllers. Please note as a consequence that the Printer Pruning functionality (rarely used) will be unavailable.

Points:
10 points if present

Documentation:
https://adsecurity.org/?p=4056
https://www.slideshare.net/harmj0y/derbycon-the-unintended-risks-of-trusting-active-directory
[MITRE]T1187 Forced Authentication

Details:
The detail can be found in Domain controllers

Domain controller
DC1
DC2

Anomalies : 55 /100

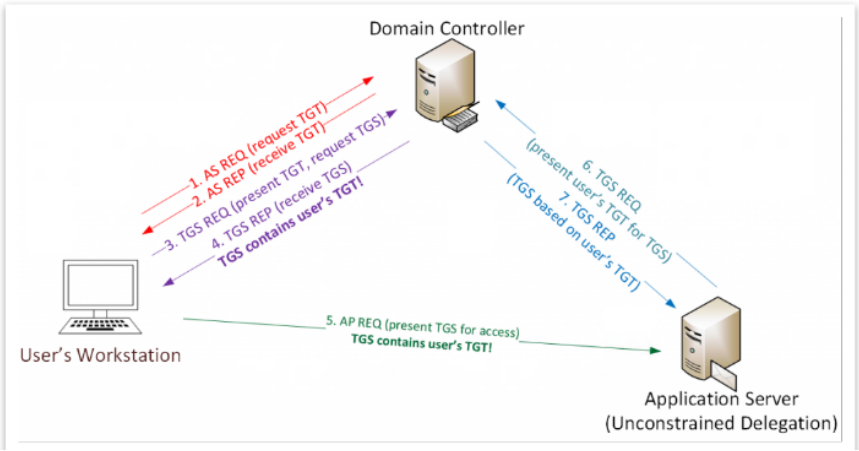
It is about specific security control points

Quel risque si activé ?

Anomalies 2 : Exploitation du service Spouleur pour récupérer les identifiants de L'AD

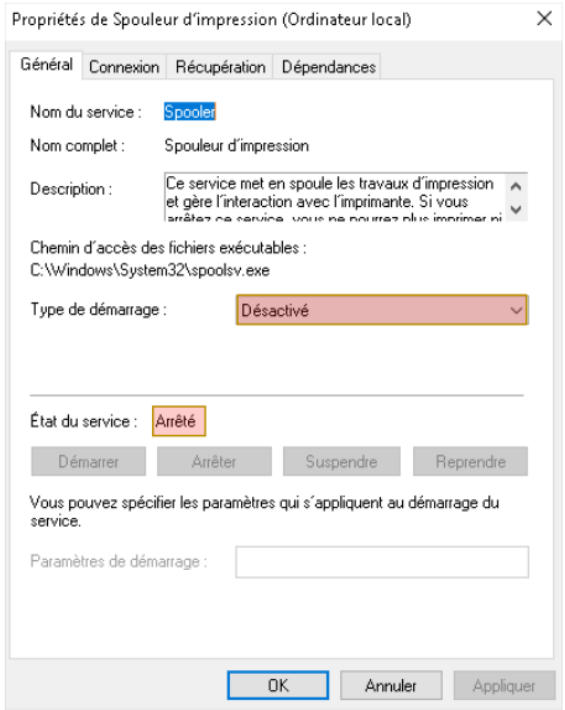
Déroulemnt de l'attaque :

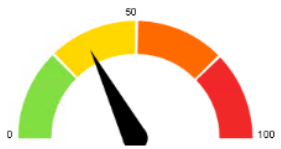
1. **Découverte** et **compromission** d'un système disposant de la délégation non contrainte Kerberos.
2. **Recherche** et **détection** d'un DC exécutant le service **Print Spooler**.
3. Envoie la requête **MS-RPRN RpcRemoteFindFirstPrinterChangeNotification** (authentification Kerberos) au serveur d'impression du DC.
4. DC répond en créant un ticket de service Kerberos (**TGS**) qui contient un ticket d'authentification Kerberos (**TGT**) du DC
5. L'attaquant dispose désormais du **TGT** Kerberos du DC et peut **usurper son identité**.
6. **DCSync** de toutes les informations d'identification de compte (ou autre attaque impliquant des informations d'identification de compte DA).



Comment le désactiver ?

Anomalies 2 : Exploitation du service Spouleur pour récupérer les identifiants de L'AD





Anomalies : 35 /100

It is about specific security control points

Stratégie d'audit sur l'AD **(10 points)**

Anomalies 3 : Vérifier si les contrôleurs de domaine disposent de la stratégie d'audit appropriée.

Check if there is the expected audit policy on domain controllers.

Rule ID:
A-AuditDC

Description:
The purpose is to ensure that the audit policy on domain controllers collects the right set of events.

Technical explanation:
To detect and mitigate an attack, the right set of events need to be collected.
The audit policy is a compromise between too much and too few events to collect.
To solve this problem, the suggested audit policy from adsecurity.org is checked against the audit policy in place.

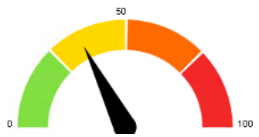
Advised solution:
Identify the Audit settings to apply and fix them.
Be aware that there are two places for audit settings.
For "Simple" audit configuration:
in Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Local Policies -> Audit Policies
For "Advanced" audit configuration:
in Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration
Also be sure that the audit GPO is applied to all domain controllers, as the underlying object may be in a OU where the GPO is not applied.

Points:
10 points if present

Documentation:
https://adsecurity.org/?p=3299
https://adsecurity.org/?p=3377
[MITRE]Mitre Att&ck - Mitigation - Audit

Details:
The detail can be found in Audit settings
The table below shows the settings that were not found as configured in a GPO for a given domain controller.

Type	Audit	Problem	Rationale	Domain controller
Advanced	Policy Change / Authentication Policy Change	No GPO check for audit success	Collect events 4713, 4716, 4739, 4867, to track trust modifications	DC1
Advanced	Account Management / Computer Account Management	No GPO check for audit success	Collect events 4741, 4742 to track computer changes	DC1
Advanced	Detailed Tracking / DPAPI Activity	No GPO check for audit	Collect event 4692 to track the export of DPAPI backup key	DC1



Anomalies : 35 /100

It is about specific security control points

Quel type de collecte pour l'audit ?

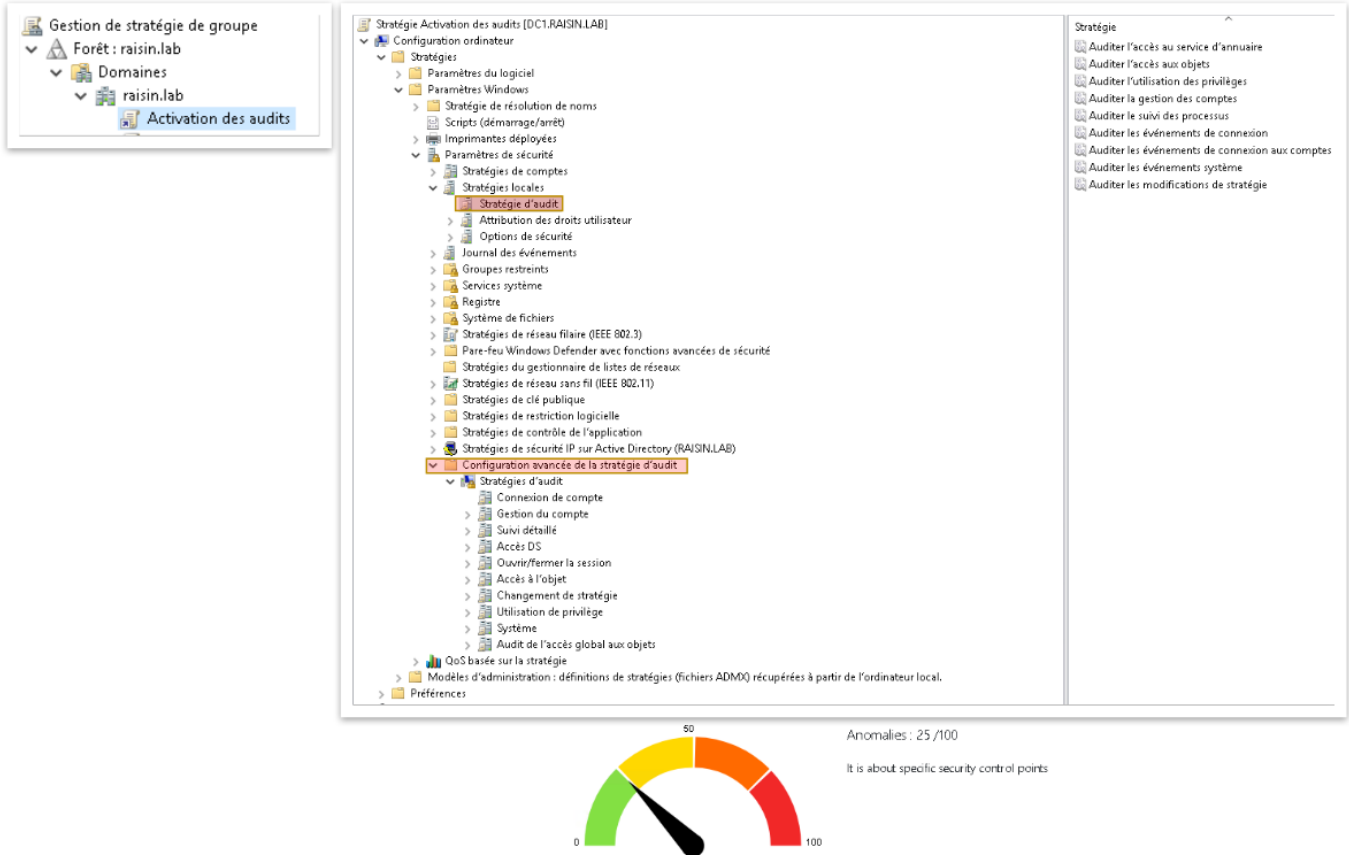
Anomalies 3 : Vérifier si les contrôleurs de domaine disposent de la stratégie d'audit appropriée.

Pour détecter et atténuer une attaque, il est essentiel de collecter le bon ensemble d'événements.
La stratégie d'audit représente un compromis entre collecter trop ou pas assez d'événements.
Afin de résoudre ce problème, la stratégie d'audit suggérée sur adsecurity.org est comparée à la stratégie d'audit en place.

Policy Change / Authentication Policy Change	Collect events 4713, 4716, 4739, 4867, to track trust modifications
Account Management / Computer Account Management	Collect events 4741, 4742 to track computer changes
Detailed Tracking / DPAPI Activity	Collect event 4692 to track the export of DPAPI backup key
Account Logon / Kerberos Authentication Service	Collect events 4768, 4771 for kerberos authentication
Account Logon / Kerberos Service Ticket Operations	Collect events 4769 for kerberos authentication
Logon/Logoff / Logoff	Collect events 4634 for account logoff
Logon/Logoff / Logon	Collect events 4624, 4625, 4648 for account logon
Detailed Tracking / Process Creation	Collect event 4688 to get the history of executed programs
Account Management / Security Group Management	Collect events 4728, 4732, 4756 for group membership change
System / Security System Extension	Collect events 4610, 4697 to track lsass security packages and services
Privilege Use / Sensitive Privilege Use	Collect events 4672, 4673, 4674 for privileges tracking such as the debug one
Logon/Logoff / Special Logon	Collect event 4964 for special group attributed at logon
Account Management / User Account Management	Collect events 4720,22,23,38,65,66,80,94 for user account mamangement

Comment activer l'audit sur l'AD ?
voir l'audit : dans **Observateur d'evenement** / **Journaux Windows** / **Sécurité** -> **onglet Details**

Anomalies 3 : Vérifier si les contrôleurs de domaine disposent de la stratégie d'audit appropriée.



Le Golden ticket !

Anomalies 4 : Atténuer l'attaque par Golden Ticket

Mitigate golden ticket attack via a regular change of the krbtgt password

Rule ID:
A-Krbtgt

Description:
The purpose is to alert when the password for the krbtgt account can be used to compromise the whole domain. This password can be used to sign every Kerberos ticket. Monitoring it closely often mitigates the risk of golden ticket attacks greatly.

Technical explanation:
Kerberos is an authentication protocol. It is using a secret, stored as the password of the krbtgt account, to sign its tickets. If the hash of the password of the krbtgt account is retrieved, it can be used to generate authentication tickets at will.
To mitigate this attack, it is recommended to change the krbtgt password between 40 days and 6 months. If this is not the case, every backup done until the last password change of the krbtgt account can be used to emit Golden tickets, compromising the entire domain.
Retrieval of this secret is one of the highest priority in an attack, as this password is rarely changed and offer a long term backdoor.
Also this attack can be performed using the former password of the krbtgt account. That's why the krbtgt password should be changed twice to invalidate its leak.

Advised solution:
The password of the krbtgt account should be changed twice to invalidate the golden ticket attack.
Beware: two changes of the krbtgt password not replicated to domain controllers can break these domain controllers You should wait at least 10 hours between each krbtgt password change (this is the duration of a ticket life).

There are several possibilities to change the krbtgt password.
First, a Microsoft script can be run in order to guarantee the correct replication of these secrets.
Second, a more manual way is to essentially reset the password manually once, then to wait 3 days (this is a replication safety delay), then to reset it again. This is the safest way as it ensures the password is no longer usable by the Golden ticket attack.

Points:
50 points if the occurence is greater than or equals than 1464
then 40 points if the occurence is greater than or equals than 1098
then 30 points if the occurence is greater than or equals than 732
then 20 points if the occurence is greater than or equals than 366

Documentation:
https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/faqs-from-the-field-on-krbtgt-reset/ba-p/2367838
https://github.com/microsoft/New-KrbtgtKeys.ps1
https://github.com/PSSecTools/Krbtgt
[FR]ANSSI CERTFR-2014-ACT-032
[FR]ANSSI - Krbtgt account password unchanged for more than a year (vuln2_krbtgt) 2
[MITRE]T1558.001 Steal or Forge Kerberos Tickets: Golden Ticket

Details:
The detail can be found in Krbtgt

20 à 50 points

Qu'est-ce que c'est ce jeton TGT ?

Anomalies 4 : Atténuer l'attaque par Golden Ticket

Qu'est-ce que l'attaque par Golden Ticket ?

L'attaque **Golden Ticket** est une technique d'élévation de privilèges dans les environnements Active Directory qui exploite le protocole d'authentification **Kerberos**.

⇒ Liée au compte spécial **KRBTGT**.

⇒ **Particulièrement dangereuse** car elle peut permettre à un attaquant de maintenir une **présence persistante** dans le réseau cible pendant une longue période.

Comment se déroule l'attaque ?

1. Obtenir le **hash** du mot de passe du compte Krbtgt (Kerberos Ticket Granting Ticket)
2. **HASH** => Faux ticket TGT du compte administrateur qu'il contrôle (**Golden Ticket**).
3. **Golden Ticket** => Tickets de service => Accède à des ressources spécifiques sur le réseau.
4. L'attaquant peut maintenant se faire passer pour un **utilisateur légitime** et accéder aux ressources cibles.

Comment l'attaquant peut-il obtenir le hash du mot de passe du compte KRBTGT ?

⇒ Un attaquant peut utiliser **Mimikatz** ou d'autres outils similaires pour **extraire le hash du mot** de passe **Krbtgt** de la **mémoire** du contrôleur de domaine.

⇒ Récupérer le **hash** à partir de **sauvegardes** qui contiennent des informations d'authentification.

20 à 50 points

Comment réduire la surface d'attaque ?

Anomalies 4 : Atténuer l'attaque par Golden Ticket

Pour commencer ...

La recommandation de l'ANSSI est de changer le mot de passe du compte KRBTGT tous les **40** jours.

J'aime les scripts !

https://github.com/zjorz/Public-AD-Scripts/blob/5666e5fcafd933c3288a47944cd6fb289dde54a1/Reset-KrbTgt-Password-For-RWDCs-And-RODCs.ps1

```
[2024-06-12 15:38:55] : Which mode of operation do you want to execute?
[2024-06-12 15:38:55] :
[2024-06-12 15:38:55] :  - 1 - Informational Mode (No Changes At All)
[2024-06-12 15:38:55] :
[2024-06-12 15:38:55] :  - 2 - Simulation Mode | Temporary Canary Object Created To Test Replication Convergence!
[2024-06-12 15:38:55] :
[2024-06-12 15:38:55] :  - 3 - Simulation Mode | Use KrbTgt TEST/BOGUS Accounts - No Password Reset/WhatIf Mode!
[2024-06-12 15:38:55] :
[2024-06-12 15:38:55] :  - 4 - Real Reset Mode | Use KrbTgt TEST/BOGUS Accounts - Password Will Be Reset Once!
[2024-06-12 15:38:55] :
[2024-06-12 15:38:55] :  - 5 - Simulation Mode | Use KrbTgt PROD/REAL Accounts - No Password Reset/WhatIf Mode!
[2024-06-12 15:38:55] :
[2024-06-12 15:38:55] :  - 6 - Real Reset Mode | Use KrbTgt PROD/REAL Accounts - Password Will Be Reset Once!
[2024-06-12 15:38:55] :
[2024-06-12 15:38:55] :
[2024-06-12 15:38:55] :  - 8 - Create TEST KrbTgt Accounts
[2024-06-12 15:38:55] :  - 9 - Cleanup TEST KrbTgt Accounts
[2024-06-12 15:38:55] :
[2024-06-12 15:38:55] :
[2024-06-12 15:38:55] :  - 0 - Exit Script
[2024-06-12 15:38:55] :
[2024-06-12 15:38:55] : Please specify the mode of operation:
```

En mode manuel :

⇒ Le mot de passe doit être changé **2 fois**.

⇒ On le change sur DC1.

⇒ On **attend 10hr** que la réplication soit effective

⇒ On **vérifie** que la réplication a bien eu lieu.

⇒ On attends **3 jours** de plus par sécurité.

⇒ On répète l'opération.

Nombre de jours depuis le dernier changement de mot de passe (KRBTGT)

```
PS C:\Users\Administrateur> (New-TimeSpan -Start (Get-ADUser krbtgt -Prop PasswordLastSet).PasswordLastSet ` -end (Get-Date)).Days
20
```

20 à 50 points

L'outil en immersion de l'ANSSI - Oradad

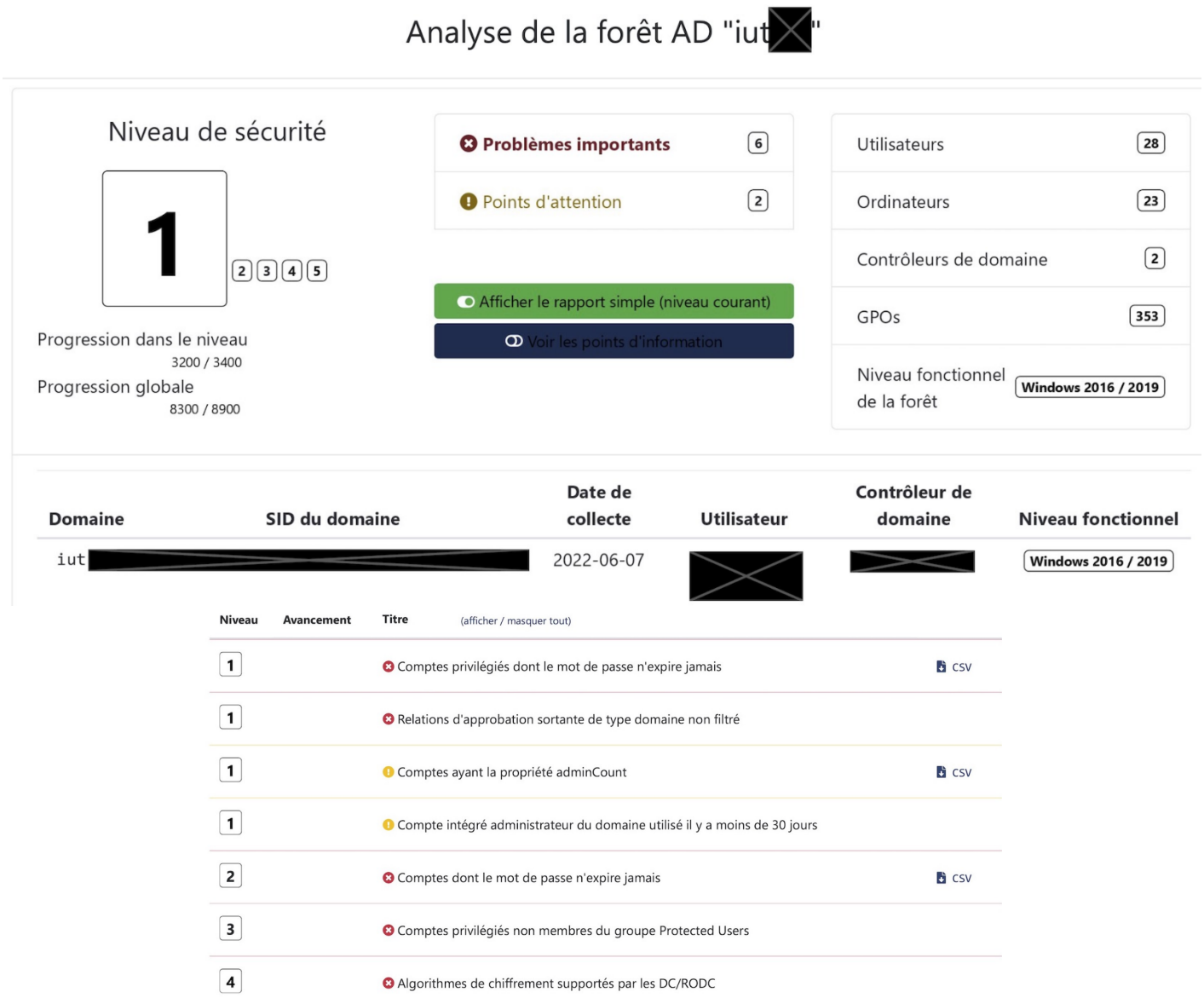
Principales fonctionnalités sur les données de l'AD

- Outil de diagnostic et de récupération automatique (Github)
- Identifier les vulnérabilités, faiblesse de la configuration et anomalies
- Offrir des rapports détaillés et personnalisables avec visualisation avancée
- Analyse en profondeur des politiques de sécurité, configurations

Sa mise en oeuvre ?

- Destiné aux experts en sécurité pour une analyse détaillée et approfondie (diagnostics précis)
- Recommandations personnalisables, conformité et alignement des pratiques
- Réservé OIV/OSE, démarche via la tutelle dont relève la sécurité (**pas de démarche individuelle !**)

Extraits d'un exemple d'analyse avec Oradad



Outil offensif et défensif pour l'AD : Forest Druid

Surveillance du Tier 0, analyse des chemins d'attaque, cartographie

- Outil open source écrit en Python, surveillance et audit
- Changements de configuration, des ACL, groupes dans l'AD
- Protection, gestion et à optimisation de l'Active Directory
- Réagir rapidement suite à un incident de sécurité, renforce la sécurité

Fin

PingCastle - véritable outil d'audit et de diagnostic pour la sécurité de l'AD

- Corrections apportées selon certains scénarios de risque
- Outil accessible, facile, la solution pour auditer l'AD
- Autres fonctionnalités (exports d'objets, scanner, schéma)
- Renforcer la sécurité de l'Active Directory de façon régulière
- Autres outils en complément de PingCastle : Forest Druid, Bloodhound

- Merci pour votre attention !

AVEZ-VOUS DES QUESTIONS ?