

JOSY Sécurisation AD - 26 & 27 juin 2024

Auditer son AD

PurpleKnight / PingCastle / ORADAD

Anne-Sophie LEDOUX | UMR 1283/8199 EGENODIA EGID PRECIDIAB

Patrice LANGLOIS | UAR 5261 BIOLuM

EGENODIA UMR:



- ▶ Domaine de recherche : Génomique sur le diabète de type 2 et les maladies associées
- ▶ Institut européen sur le diabète et l'obésité : **EGID**
 - ▶ 5 UMR
 - ▶ 6 plateformes
- ▶ Centre national de médecine de précision du diabète : **PreciDIAB**
- ▶ IT infrastructure & data security : 2 personnes
- ▶ Taille du SI :
 - ▶ 500 utilisateurs
 - ▶ Un domaine Active Directory
 - ▶ 3 Po de données
 - ▶ Une 100aine de serveurs



EGID INNOVATION

IMPACT PM

BIOLuM UAR:

Cemipai

- ▶ Domaine de recherche: Biologie
- ▶ Service Système d'Information: 4 personnes
- ▶ Taille du SI:
 - ▶ 3 UMR CRBM, IGMM, IRIM, 1 UAR CEMIPAI
 - ▶ 500 utilisateurs
 - ▶ Un domaine Active Directory
 - ▶ Plus de 1Po de données
 - ▶ Une 100aine de serveurs

CRBM  Centre de Recherche
en Biologie cellulaire
de Montpellier

igmm
INSTITUT DE GÉNÉTIQUE
MOLÉCULAIRE DE MONTPELLIER

IRI m  Institut de Recherche
en Infectiologie
de Montpellier

Pourquoi auditer son AD ?

- ▶ Risque d'attaque élevé : Permet de détecter et de répondre aux menaces internes, aux abus de privilèges et à d'autres indices de compromission
- ▶ Conséquences désastreuses
- ▶ Permet d'appuyer les décisions qu'on prend vis-à-vis des directions
- ▶ Excellent moyen de formation
- ▶ Pourquoi multiplier les outils d'audit ?

- ▶ Démystifier l'audit (Tout ASR peut auditer son AD)

Les outils

- ▶ PurpleKnight - Gratuit
 - ▶ Aide à quantifier notre posture de sécurité et à obtenir des informations approfondies sur la sécurité sur la base des IOE et des IOC
 - ▶ Simple utilisateur
- ▶ PingCastle - Gratuit avec une version payante
 - ▶ Fournit des informations contextuelles sur la sécurité
 - ▶ Simple utilisateur
- ▶ ORADAD - Gratuit, fourni par l'ANSSI
 - ▶ Rapport différé
 - ▶ Simple utilisateur

Qu'est ce que purpleknight ?

Intègre les bonnes pratiques de l'ANSSI

- ▶ Outil pour auditer les annuaires Active Directory, édité par la société Semperis, totalement gratuit
- ▶ Objectif : **Améliorer la sécurité de son AD**
- ▶ Génère un **rapport complet** et indique un **score** qui reflète le niveau de sécurité de son AD
- ▶ Prend aussi en charge l'**analyse d'Azure AD** : pour ceux qui travaillent sur un environnement cloud, et en mode hybride avec les solutions Microsoft
- ▶ Vérifie **100 points** au niveau de l'AD local : gestion des comptes, la délégation, les relations d'approbation, la stratégie de groupe, la partie Kerberos
- ▶ Outil **complémentaire à Ping Castle** (gratuit) : points communs entre les 2 mais présenté différemment
- ▶ Prérequis pour le télécharger : **renseigner une adresse mail**

Télécharger et installer purpleknight ?



- ▶ <https://www.purple-knight.com/request-form/>
- ▶ Compléter un formulaire sur le site officiel afin de recevoir un e-mail avec un lien de téléchargement
- ▶ Pas demandé avec PingCastle
- ▶ Archive ZIP de 100 Mo environ à extraire
- ▶ 2 fichiers PDF : documentation d'utilisation
- ▶ répertoire "Scripts" contient un ensemble de scripts PowerShell signés que l'outil va exécuter pour réaliser son audit

Lancer un audit avec purple knight ?

- ▶ Exécuter le fichier « PurpleKnight.exe » en tant qu'utilisateur sur un pc relié au domaine à auditer
- ▶ Un assistant s'ouvre ...

Etape 1

- ▶ Accepter les conditions d'utilisation :

The screenshot shows the 'PURPLE KNIGHT (Community edition)' application window. At the top, there is a progress bar with five steps: Agreement (1), Environment (2), Indicators (3), Progress (4), and Summary (5). Step 1 is highlighted with a purple circle. Below the progress bar, the text reads 'Confirm the following agreement:'. A white box contains the 'PURPLE KNIGHT LICENSE AGREEMENT' text. At the bottom of the white box, there is a checkbox labeled 'I accept the terms in the license agreement' which is checked. A 'NEXT' button is located at the bottom right of the application window.

PURPLE KNIGHT (Community edition)

Agreement Environment Indicators Progress Summary

1 2 3 4 5

Confirm the following agreement:

PURPLE KNIGHT LICENSE AGREEMENT

THIS LICENSE AGREEMENT (THE "AGREEMENT") GOVERNS THE USE OF THE SEMPERIS "PURPLE KNIGHT" TOOL AND THE DOCUMENTATION BUNDLED THEREWITH (COLLECTIVELY, THE "SOFTWARE"). PLEASE CAREFULLY READ THE TERMS AND CONDITIONS OF THIS AGREEMENT BEFORE PROCEEDING WITH DOWNLOADING THE SOFTWARE.

THIS AGREEMENT CONSTITUTES A BINDING CONTRACT BETWEEN AND AMONG SEMPERIS ("SEMPERIS"), YOU, ANY OTHER PERSON, COMPANY, ORGANIZATION OR OTHER ENTITY (INDIVIDUALLY AND COLLECTIVELY REFERRED TO AS "YOU" OR "YOUR") DOWNLOADING, USING OR BENEFITTING FROM THE USE OF THE SOFTWARE. IF YOU ARE ACTING ON BEHALF, OR FOR THE BENEFIT, OF ANY OTHER PERSON, A COMPANY, AN ORGANIZATION OR OTHER ENTITY, THEN YOU REPRESENT AND WARRANT THAT YOU ARE DULY AUTHORIZED TO ENTER INTO THIS AGREEMENT ON ITS BEHALF AND HAVE THE PROPER AUTHORITY TO LEGALLY BIND ALL PARTIES TO THIS AGREEMENT.

THIS AGREEMENT BECOMES EFFECTIVE UPON: (A) CLICKING THE "I AGREE" BUTTON; (B) DOWNLOADING OR INSTALLING THE SOFTWARE; (C) USING THE SOFTWARE IN ANY WAY; OR (D) OTHERWISE ASSENTING TO THIS AGREEMENT. BY PERFORMING ANY OF THE FOREGOING, YOU ARE EXECUTING THIS AGREEMENT AND AGREEING TO BE BOUND BY ITS TERMS IN THE SAME WAY THAT A PAPER CONTRACT BINDS YOU. THIS AGREEMENT LIMITS YOUR RIGHTS AND LIMITS SEMPERIS' LIABILITY AND OBLIGATIONS AS SET FORTH HEREIN. IF THE TERMS AND CONDITIONS OF THIS AGREEMENT ARE NOT ACCEPTABLE IN THEIR ENTIRETY, THEN THE SOFTWARE MAY NOT BE DOWNLOADED OR USED IN ANY WAY.

1. Definitions.

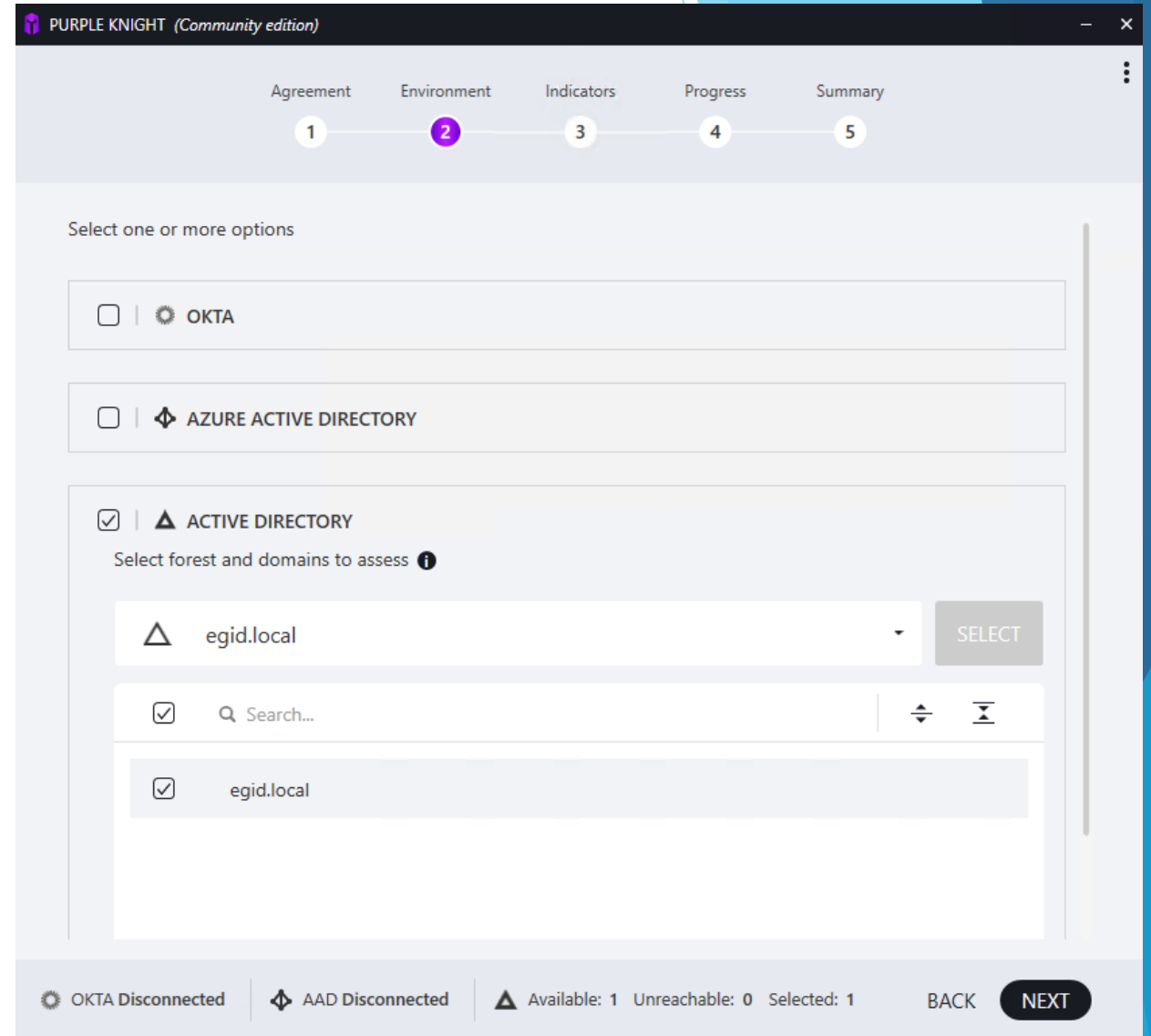
1.1. "Active Directory Environment" means the environment in which you execute or apply the Software.

I accept the terms in the license agreement

NEXT

Etape 2

- ▶ Sélectionner l'environnement cible :



Etape 3

- ▶ Sélectionner les éléments à analyser :

The screenshot shows the Purple Knight (Community edition) interface. At the top, there is a progress bar with five steps: Agreement (1), Environment (2), Indicators (3), Progress (4), and Summary (5). Step 3, 'Indicators', is currently selected and highlighted in purple.

Below the progress bar, the text reads: "The assessment will include the following tests:". A yellow banner below this text states: "BEST PRACTICE For an accurate assessment, the tool should run all security indicators on the selected forest".

The main area displays a list of security indicators with checkboxes and counts:

- AD Delegation (18)
- Account Security (30)
- AD Infrastructure Security (31)
- Group Policy Security (8)
- Kerberos Security (18)
- Hybrid (2)

On the right side, the details for the selected "AD Infrastructure Security" indicator are shown:

- AD Infrastructure Security**
- Description**
AD Infrastructure Security indicators pertain to the security configuration of core parts of AD's own infrastructure configuration.
- Weight**
7

At the bottom of the interface, it shows "Available: 107 Selected: 107". There are "BACK" and "RUN TESTS" buttons.

in progress ...

- ▶ Audit rapide
- ▶ ne nécessite que 1 ou 2 min pour vérifier environ 100 points différents.

PURPLE KNIGHT (Community edition)

Agreement Environment Indicators Progress Summary

1 2 3 4 5

Status: Running Elapsed Time: 00:00:07 Done: 30 of 107 (28%) STOP

Search... All

Category	Progress	Count
AD Delegation	<div style="width: 22.2%;"></div>	4/18
Account Security	<div style="width: 16.7%;"></div>	5/30
AD Infrastructure Security	<div style="width: 45%;"></div>	14/31
Group Policy Security	<div style="width: 12.5%;"></div>	1/8
Kerberos Security	<div style="width: 50%;"></div>	4/18
Hybrid	<div style="width: 100%;"></div>	2/2

NEXT

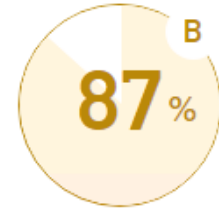
Résultats

- ▶ Cliquer sur "View report" pour afficher le rapport HTML dans un navigateur.
- ▶ Export possible au format PDF ou au format CSV avec le bouton "Save as"

The screenshot displays the Purple Knight (Community edition) interface. At the top, a navigation bar includes the title 'PURPLE KNIGHT (Community edition)' and a progress indicator with five steps: Agreement (1), Environment (2), Indicators (3), Progress (4), and Summary (5). The main content area shows the results for an 'Active Directory' scan. The 'Forest' is identified as 'egid.local', 'IOEs found' are 30, and the scan was 'Run by' 'EGID\Administrateur'. A large circular gauge on the right indicates a score of 87% with a grade 'B'. The bottom navigation bar contains buttons for 'NEW SCAN', 'SAVE AS ...', and 'VIEW REPORT'. The date '26/06/2024' and the number '13' are also visible at the bottom.

Interpréter le rapport d'audit - IOE

- ▶ L'AD de mon labo a obtenu la lettre B et le score de 87%
- ▶ Plus le score est élevé, mieux c'est !
- ▶ "IOEs found" : 30
- ▶ IOE signifie Indicators of Exposure (Indicateurs d'exposition) : correspond au nombre de règles pour lesquelles l'AD n'est pas conforme aux recommandations.



▲ ACTIVE DIRECTORY

▲ Forest	egid.local
🗄️ No. of Domains	1
🕒 Duration	00:00:47
👤 Run by	EGID\Administra...

Indicators

Evaluated	104
🚫 Not selected	0
🚨 IOEs found	30
✅ Passed	74
❌ Failed to run	0
ℹ️ Not Relevant	3
⏸️ Canceled	0

Critical IOE

- ▶ Traiter les IOE critiques en priorité
- ▶ Cliquer sur le lien "Read More« : renvoi direct à la section du rapport qui donne des détails techniques sur la règle, mais aussi les éléments de l'AD concernés.

CRITICAL IOEs FOUND

Certificate templates that allow requesters to spe...

This indicator checks if certificate templates are enabling requesters to specify a subjectAltName in the CSR.

[Read More](#)

Print spooler service is enabled on a DC

This indicator scans Domain Controllers for a running print spooler service....

[Read More](#)

Privileged Users with Weak Password Policy

This indicator looks for privileged users in each domain that don't have a strong password policy enforced, according to ...

[Read More](#)

Score par catégorie

- ▶ Semperis précise sur son site "Le score global moyen de Purple Knight est de 61 %, la sécurité de Kerberos étant en moyenne de 43 % et celle de Group Policy de 58 %."
- ▶ Cliquer sur "Read More" ou menu de gauche pour parcourir chaque section et voir l'ensemble des points vérifiés avec le résultat associé.

ACTIVE DIRECTORY RESULTS

Categories



AD DELEGATION

AD delegation is a critical part of security and compliance. By delegating control over Active Directory, you can grant users or

[Read More](#)



ACCOUNT SECURITY

Account Security indicators pertain to security weaknesses on individual accounts - built-in or otherwise, within Active

[Read More](#)



AD INFRASTRUCTURE SECURITY

AD Infrastructure Security indicators pertain to the security configuration of core parts of AD's own infrastructure configuration.

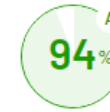
[Read More](#)



GROUP POLICY SECURITY

Group Policy Security indicators pertain to the security configuration of GPOs and their deployment within AD.

[Read More](#)



KERBEROS SECURITY

Kerberos Security indicators pertain to the configuration of Kerberos capabilities on computer and user accounts within AD.

[Read More](#)



HYBRID

Hybrid indicators help you understand and mitigate the risks associated with a hybrid identity environment. Active Directory is a

[Read More](#)

Remédiation - objectif 90 - 100 %

- ▶ Analyser chaque point afin de mettre un plan d'action pour y remédier - objectif 90-100%
- ▶ Niveau de sévérité, description, probabilité de compromission en exploitant cette faiblesse, des détails sur les éléments de l'AD concernés par la règle
- ▶ Etapes à réaliser pour résoudre ce défaut de sécurité
- ▶ Rapports d'audit placés dans le répertoire "Output" de Purple Knight

Remédiation - exemple



SECURITY INDICATOR
Users with old passwords

IOE Found



SEVERITY

Informational

WEIGHT

2

Security Frameworks

MITRE ATT&CK

- Credential Access
- Persistence

MITRE D3FEND

- Harden - Strong Password Policy

Description

This indicator looks for user accounts whose password has not changed in over 180 days. This could make these account ripe for password guessing attacks.

Likelihood of Compromise

Stale passwords that aren't changed over a long period of time and are not supported by multi-factor authentication are ripe targets for attackers. These present opportunities for attackers to move laterally through the environment or elevate privileges.

Result

The following 77 users were returned. Note the following: users with DaysSinceLastSet and ReplicationMetadata higher than 180 days have not changed passwords in over 180 days. Users with PwdLastSet over 180 days and ReplicationMetadata is N/A - permission was denied to read these users' metadata. These users may be using smartcard for interactive logon instead of passwords - in which case it is ok that their passwords have not changed.

DistinguishedName	SamAccountName	PasswordLastSet	DaysSinceLastSet	Ignored
CN=[REDACTED],OU=NGS,OU=UMR8199,OU=Utilisateurs,DC=egid,DC=local	[REDACTED]		2644	False

Appendix - ANSSI

APPENDIX 3 - ANSSI SCORECARD

The following section displays the breakdown of indicators within the framework of the French National Agency for the Security of Information Systems (ANSSI).
For more information visit: https://www.cert.ssi.gouv.fr/uploads/ad_checklist.html

ANSSI LEVEL

1

Critical weaknesses and misconfigurations pose an immediate threat to all hosted resources. Corrective actions should be taken as soon as possible.

EVALUATED
39/39

INDICATORS FOUND
10

PASSED
29

FAILED TO RUN
0

CANCELED
0

NOT SELECTED
0

ANSSI ID	INDICATOR NAME	ACTION
! vuln1_password_change_priv	Built-in domain Administrator account with old password (180 days)	Full Results
! vuln1_user_accounts_dormant	Enabled admin accounts that are inactive	Full Results

- ▶ Guide "Point de contrôle de l'Active Directory" de l'ANSSI :
https://www.cert.ssi.gouv.fr/uploads/ad_checklist.html

Qu'est ce que pingcastle ?














- ▶ Outil d'audit d'AD
- ▶ Société française
- ▶ Gratuit si utilisé dans un cadre non commerciale
- ▶ <https://www.pingcastle.com/>

PingCastle



- ▶ Facilité d'exécution
- ▶ Permet:
 - ▶ D'évaluer son degré de sécurité
 - ▶ De Supprimer les risques critiques
 - ▶ Priorisé son plan d'action
 - ▶ D'avoir un support documentaire

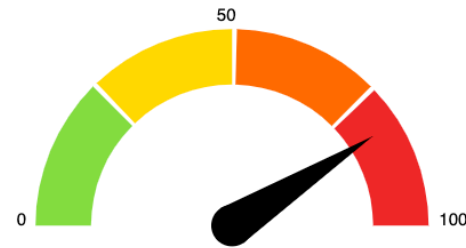
> Ce PC > Téléchargements > PingCastle_3.2.0.1

Nom	Modifié le	Type	Taille
 Active Directory Security Self Assessment...	18/06/2024 16:03	Adobe Acrobat D...	386 Ko
 changelog	18/06/2024 16:03	Document texte	35 Ko
 license	18/06/2024 16:03	Format RTF	13 Ko
 Newtonsoft.Json.dll	18/06/2024 16:03	Extension de l'app...	686 Ko
 PingCastle v3.0.0	18/06/2024 16:03	Adobe Acrobat D...	1 657 Ko
 PingCastle	18/06/2024 16:03	Application	2 370 Ko
 PingCastle.exe.config	18/06/2024 16:03	Fichier CONFIG	6 Ko
 PingCastle.pdb	18/06/2024 16:03	Fichier PDB	2 362 Ko
 PingCastleAutoUpdater	18/06/2024 16:03	Application	47 Ko
 PingCastleAutoUpdater.exe.config	18/06/2024 16:03	Fichier CONFIG	1 Ko
 PingCastleAutoUpdater.pdb	18/06/2024 16:03	Fichier PDB	24 Ko

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

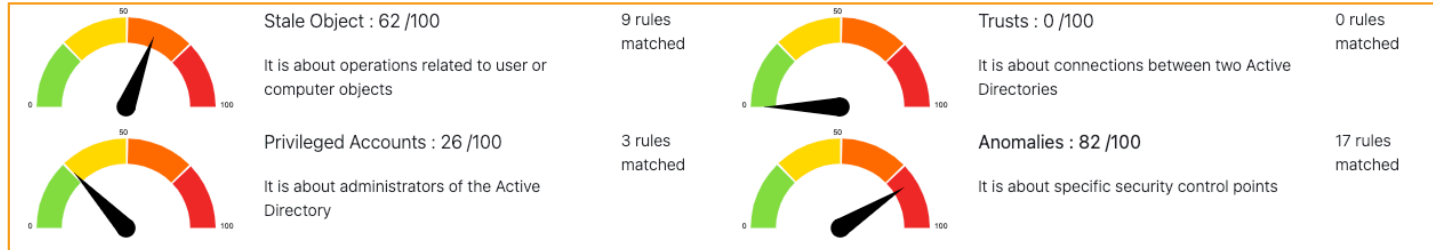


Domain Risk Level: 82 / 100

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](#)



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

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 occurrence is greater than or equals than 1464
then 40 points if the occurrence is greater than or equals than 1098
then 30 points if the occurrence is greater than or equals than 732
then 20 points if the occurrence 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

Last change of the Kerberos password: 598 day(s) ago	+ 20 Point(s)
[REDACTED]	+ 15 Point(s)
[REDACTED]	+ 15 Point(s)
[REDACTED]	+ 10 Point(s)
[REDACTED]	+ 10 Point(s)
WSUS is configured with unencrypted HTTP instead of HTTPS	+ 5 Point(s)
[REDACTED]	+ 5 Point(s)
[REDACTED]	+ 5 Point(s)
[REDACTED]	+ 1 Point(s)
[REDACTED]	+ 1 Point(s)

ORADAD

- ▶ Développé par l'ANSSI
- ▶ Fichier ORADAD.exe
- ▶ Génération d'un fichier *.mla
- ▶ Envoie à l'ANSSI via le RSSI CNRS
- ▶ Rapport en html



Analyse de la forêt AD [redacted]

Niveau de sécurité



Progression dans le niveau

3300 / 3500

Progression globale

7900 / 8900

Problèmes importants 2

Points d'attention 2

Afficher le rapport complet (tous niveaux)

Voir les points d'information

Télécharger les données au format JSON

Domaine	[redacted]
Utilisateurs	[redacted]
Ordinateurs	[redacted]
Contrôleurs de domaine	[redacted]
GPOs	[redacted]
Niveau fonctionnel de la forêt	[redacted]

Domaine	<u>Filtre</u>	SID du domaine	<u>Contrôleur de domaine</u>	<u>Utilisateur</u>	<u>Niveau fonctionnel</u>
[redacted]	<input type="checkbox"/>	[redacted]	[redacted]	[redacted]	[redacted]

Entrez une partie de nom distingué (DN) pour filtrer le contenu du rapport

La fonctionnalité de filtrage vous permet d'afficher et d'extraire une sous-partie de ce rapport au format JSON (via le bouton de téléchargement plus haut, ou point par point ci-dessous). Ce fichier JSON peut alors être relu par [la visionneuse en ligne disponible sur le site du CERT-FR](#).
Les dates du rapport sont calculées à partir de la date de collecte

Niveau	Progression	Titre	ID	CSV
1	[redacted]	Comptes privilégiés dont le mot de passe n'expire jamais	vuln1_dont_expire_priv	[data]

Description de la vulnérabilité

Certains comptes privilégiés possèdent des mots de passe n'expirant pas.

Si aucun mécanisme de sécurité ne force le changement de ces mots de passe, la récupération d'un compte privilégié permet à un individu malveillant de conserver ces droits d'accès au domaine sur le long terme.

Conclusion

- ▶ 3 Outils:
 - ▶ 3 analyses différentes mais complémentaires
 - ▶ Le meilleur ?
- ▶ PurpleKnight
- ▶ Pingcastle
- ▶ ORADAD

Conclusion

- ▶ Outils de progression pour son SI
- ▶ Outils pour développer ses compétences
- ▶ Simple - Gratuit et ça peut rapporter gros
- ▶ Ne pas hésiter à en abuser

Sources

- ▶ Site web Semperis : <https://www.semperis.com/>
- ▶ Site web Purple Knight : <https://www.purple-knight.com/>
- ▶ Site web PingCastle : <https://www.pingcastle.com/>
- ▶ Site web ORADAD : <https://github.com/ANSSI-FR/ORADAD>
- ▶ ANSSI : <https://www.ssi.gouv.fr/>
- ▶ CERT : <https://www.cert.ssi.gouv.fr/>

MERCI !
QUESTIONS ?