

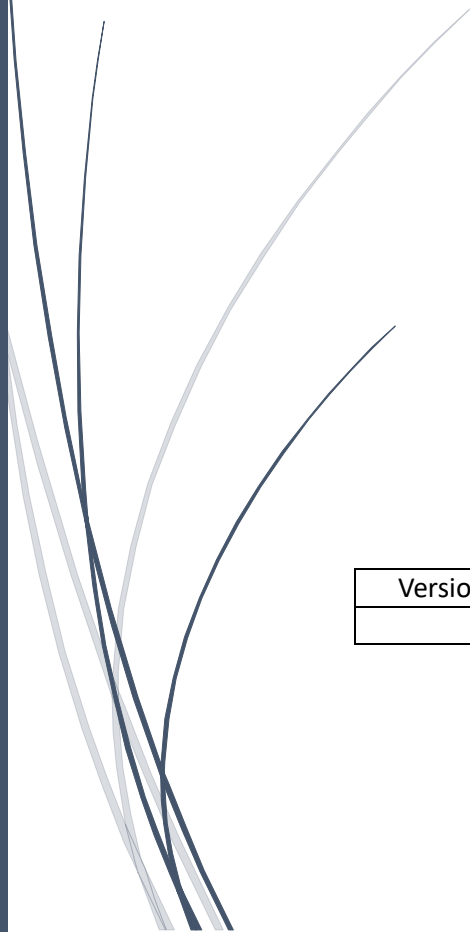
A dark blue vertical bar runs along the left edge of the page. A blue arrow points to the right, overlapping the vertical bar and the title.

Rapport d'Audit de la Sécurité du Système d'Information

De « Logie Ciel »

Auditeur chargé de la mission : Benjamin, Tony

Signature :

A stylized, handwritten signature in dark blue ink, consisting of several sweeping, overlapping loops, is positioned below the 'Signature :' label.

Version du document	Date	Diffusion
1.0	05/12/2023	Document Confidentiel

Table des matières

1. Cadre de la mission.....	2
2.Synthèse Managériale	2
3.Références	4
4.Champ d’audit	4
4.1. Liste des Structures à Auditer.....	4
4.2. Description des Systèmes d'Information	4
5.Méthodologie	5
6.Présentation des Vulnérabilité	6
7.Annexe.....	8

1. Cadre de la mission

Dans le cadre de la loi n°5 de 2004 et du décret 2004-1250 régissant les normes de sécurité informatique, la présente mission d'audit a été initiée pour évaluer la sécurité de l'infrastructure informatique de **Logie Ciel**. Cette mission d'audit s'inscrit dans le cadre d'un examen exhaustif visant à évaluer la conformité du serveur Windows 2022 ADDS, du serveurs Linux et de l'API REST par rapport aux standards de sécurité établis.

L'objectif principal de cette mission est de dresser un état de conformité par rapport aux normes établies, d'identifier les vulnérabilités potentielles et les risques de sécurité encourus par l'entreprise. Nous visons également à formuler des recommandations spécifiques et un plan d'action pour renforcer la sécurité de l'infrastructure et des applications concernées.

Notre mission d'audit se concentrera spécifiquement sur l'analyse approfondie du serveur Windows 2022 ADDS, du serveurs Linux et de l'API REST, en recherchant activement les failles potentielles, les lacunes de sécurité et les risques identifiés. Cette évaluation sera réalisée par rapport aux standards métier de référence afin de garantir la robustesse et la fiabilité de l'environnement informatique de **Logie Ciel**.

2.Synthèse Managériale

Synthèse Managériale

L'audit de sécurité entrepris au sein de l'entreprise de développement de logiciels a été mené avec rigueur et professionnalisme, visant à évaluer la robustesse de l'infrastructure informatique et à identifier les risques potentiels en matière de sécurité.

Objectifs de l'Audit

L'objectif principal était d'évaluer la sécurité de l'infrastructure Windows Active Directory (AD). L'audit visait à identifier les vulnérabilités, à évaluer la conformité aux normes de sécurité, et à fournir des recommandations pour renforcer la posture globale de sécurité.

Vulnérabilités Identifiées

Au cours de l'audit, diverses vulnérabilités ont été identifiées, notamment des problèmes liés à la gestion des droits d'accès, la gestion des groupes et leurs utilisateurs, des configurations non conformes de mot de passe, et des vulnérabilités spécifiques aux protocoles de sécurité utilisés.

Recommandations

Des recommandations spécifiques ont été formulées pour remédier aux vulnérabilités identifiées. Celles-ci incluent des ajustements de configurations dans les GPOs, groupes et les droits d'accès aux utilisateurs, la mise en œuvre de correctifs de sécurité concernant l'utilisation de certains protocoles, des pratiques recommandées pour renforcer la sécurité de l'AD et la sensibilisation aux utilisateurs sur les différentes règles à respecter.

Considérations Éthiques et Légales

Toutes les activités d'audit ont été menées conformément aux lois et règlements applicables, en respectant la confidentialité des données sensibles. Les autorisations nécessaires ont été obtenues, et des mesures ont été prises pour garantir l'éthique tout au long du processus.

Conclusion

En conclusion, l'audit de sécurité a fourni une vision approfondie de la posture actuelle de sécurité. Les recommandations formulées visent à renforcer la résilience de l'infrastructure face aux menaces actuelles et émergentes. L'engagement envers la sécurité continue et la mise en œuvre diligente des recommandations contribueront à maintenir un environnement informatique robuste et sécurisé au sein de l'entreprise.

3. Références

Les documents et référentiels suivants ont été utilisés comme base pour la réalisation de l'audit :

Guide ANSSI Active Directory (AD)

Benchmarks CIS pour Windows Server 2022

Référentiel PASSI pour l'Audit de Sécurité

Normes et Guides de l'ANSI pour l'Audit de la Sécurité des Systèmes d'Informations

Rapports de Configuration et Bonnes Pratiques du Fabricant (Microsoft, Linux)

4. Champ d'audit

4.1. Liste des Structures à Auditer

Structure
Serveur Windows 2022 ADDS

Le périmètre géographique de cette mission d'audit concerne les différentes composantes de l'infrastructure informatique centrale de **Logie Ciel**, à savoir le serveur Windows 2022 et de son infrastructure active directory, du serveurs Linux et de l'API REST.

Les critères d'échantillonnage ont été définis en prenant en considération l'importance stratégique de chaque composant pour l'activité opérationnelle de l'entreprise, leur interdépendance et leur impact sur la sécurité globale du système d'information.

4.2. Description des Systèmes d'Informations

Serveur Windows 2022

Système d'exploitation Windows Server 2022 avec ses services et rôles spécifiques.

Services AD DS pour la gestion des identités et des accès, comprenant le DNS du domaine AD.

Service SSH et WinRM

Partage SMB : un partage "Read only" accessible à tous en lecture et un partage "Read Write" accessible à tous en lecture et écriture.

Service Web disponible sur la boucle locale

5.Méthodologie

L'audit sera réalisé en conformité avec le référentiel PASSI (Prestations d'Audit de la Sécurité des Systèmes d'Information) et en se basant sur les guides de sécurité de l'ANSSI (Agence nationale de la sécurité des systèmes d'information) ainsi que les standards CIS (Center for Internet Security).

Les outils sélectionnés pour l'audit incluront BloodHound, Sharphound, PingCastle, et des scripts personnalisés pour évaluer la sécurité de l'infrastructure AD

L'analyse sera réalisée en utilisant des méthodes manuelles et automatisées. Cela comprendra l'examen des configurations, l'analyse des journaux, et l'utilisation d'outils d'évaluation automatisés.

Phase 1 : Collectes d'Informations

Objectifs de la phase : Collecter des informations sur l'infrastructure, y compris la topologie réseau, les services exposés, les configurations DNS, etc.

Méthodes de collecte d'informations : Scans réseau, analyse des configurations.

Outils utilisés : PingCastle, Bloodhound, scripts personnalisés.

Livrables attendus : Rapport de collecte d'informations.

Phase 2 : Analyses des Vulnérabilités

Objectifs de la phase : Identifier les vulnérabilités potentielles dans l'infrastructure Active directory

Méthodes d'analyse des vulnérabilités : Scans de vulnérabilités, évaluation des configurations.

Outils utilisés : PingCastle, Bloodhound, scripts personnalisés, ANSSI, PASSI.

Livrables attendus : Rapport d'analyse des vulnérabilités.

Phase 3 : Évaluations des Configurations

Objectifs de la phase : Évaluer les configurations de l'Active Directory par rapport aux bonnes pratiques de sécurité.

Méthodes d'évaluation des configurations : Examen manuel des paramètres de sécurité, utilisation de guides de référence.

Outils utilisés : PingCastle, Bloodhound, scripts personnalisés, ANSSI, PASSI.

Livrables attendus : Rapport d'évaluation des configurations.

6.Présentation des Vulnérabilités

Facilité d'exploitation / Impact	Difficile	Elevée	Modérée	Facile
Mineur	Mineur	Mineur	Important	Majeur
Important	Mineur/Important	Important	Important	Majeur
Majeur	Important	Majeur	Majeur	Critique
Critique	Important	Majeur	Critique	Critique

Serveur Windows 2022

Titre	Description	Preuve	Recommandation
NTLMv1 et LM	Ce sont des anciens protocoles d'authentification, lorsqu'ils sont utilisés, ces protocoles peuvent être exploités par des attaquants pour intercepter des hachages NTLM, ouvrant ainsi la porte à une usurpation d'identité et à des attaques potentielles contre le contrôleur de domaine.	ANNEXE 1	Restreindre l'utilisation de NTLMv1 en configurant les paramètres d'authentification pour n'autoriser que les réponses NTLMv2, refusant ainsi l'utilisation des protocoles LM et NTLM.
Politique de mot de passe	La longueur minimale des mots de passe définie dans la politique de mot de passe de votre domaine est inférieure à 8.	ANNEXE 2	La solution recommandée pour remédier à cette vulnérabilité consiste à modifier la politique de mot de passe en supprimant la GPO autorisant les mots de passe court.
Compte sans preauth kerberos	Des comptes n'imposent pas la pré authentification Kerberos. Sans pré authentification il est possible d'obtenir un ticket chiffré avec un des secrets associés au compte correspondant. Il est ensuite possible de lancer une attaque afin de retrouver le mot de passe de l'utilisateur, ce qui peut être facilité s'il n'est pas assez robuste.	ANNEXE 3	La propriété DONT_REQUIRE_PREAUTH doit être supprimée pour ces comptes et le mot de passe doit être changé.
Admin sans preauth kerberos	Des comptes privilégiés n'imposent pas la pré authentification Kerberos. Sans pré authentification il est possible d'obtenir un ticket chiffré avec un des secrets associés au compte correspondant. Il est ensuite possible de lancer une attaque afin de retrouver le mot de passe de l'utilisateur, ce qui peut être facilité s'il n'est pas assez robuste.	ANNEXE 4	La propriété DONT_REQUIRE_PREAUTH doit être supprimée pour ces comptes et le mot de passe doit être changé.

Utilisateurs avec des droits administrateur indirects	Des comptes ont des droits administrateurs avec lesquels ils peuvent se mettre admin du domaine.	ANNEXE 5	Enlever les droits administrateurs si l'utilisateur ne fait pas parti de la DRI et essayé de réduire le nombre d'objets ayant un accès indirect.
Utilisateurs qui peuvent ajouter un pc au domaine	Certains utilisateurs peuvent ajouter jusqu'à 10 ordinateurs dans le domaine.	ANNEXE 6	N'autoriser que les administrateurs du domaine à ajouter un ordinateur dans le domaine.
Control Path	Un grand nombre d'utilisateurs ou d'ordinateurs peuvent prendre le contrôle d'un objet clé du domaine en abusant des autorisations ciblées	ANNEXE 7	Limiter les autorisations données aux utilisateurs.
Le service spooler est accessible à distance depuis 1 DC	Lorsqu'un compte avec délégation sans contrainte est configuré et que le service Print Spooler fonctionne sur un ordinateur, il est possible d'obtenir les informations d'identification de cet ordinateur envoyées au système avec délégation sans contrainte en tant qu'utilisateur. Avec un contrôleur de domaine, le TGT du DC peut être extrait, ce qui permet à un attaquant de le réutiliser avec une attaque DCSync et d'obtenir tous les hashes des utilisateurs et d'usurper leur identité.	ANNEXE 8	Le service Print Spooler doit être désactivé sur les contrôleurs de domaine. A noter que la fonctionnalité d'élagage des imprimantes ne sera pas disponible.
Comptes invité trouvé	Le compte Invité permet aux utilisateurs réseau non authentifiés de se connecter en tant qu'Invité sans mot de passe. Ces utilisateurs non autorisés peuvent accéder à toutes les ressources accessibles au compte Invité sur le réseau. Cette fonctionnalité signifie que tous les objets ou dossiers partagés avec des autorisations qui autorisent l'accès au compte Invité, au groupe Invités du domaine, au groupe Invités, ou au groupe Tout le monde sont accessibles sur le réseau, ce qui peut entraîner l'exposition ou l'altération des données.	ANNEXE 9	Désactiver le compte Invité.

7. Annexe

Annexe 1 :

Stale Objects rule details [8 rules matched on a total of 50]

The LAN Manager Authentication Level allows the use of NTLMv1 or LM.

+ 15 Point(s)

Annexe 2 :

Password policies

Note: PSO (Password Settings Objects) will be visible only if the user, which collected the information, has the permission to view it. PSO shown in the report will be prefixed by "PSO:"

Policy Name	Complexity	Max Password Age	Min Password Age	Min Password Length	Pass
Default Domain Policy	True	42 day(s)	1 day(s)	7	

Annexe 3 :

```
PS C:\Users\Administrateur> Get-ADObject -LDAPFilter "(userAccountControl:1.2.840.113556.1.4.803:=4194304)"

DistinguishedName      Name      ObjectClass ObjectGUID
-----
CN=Administrateur,CN=Users,DC=AIS,DC=FR      Administrateur      user      a8dfe481-1c35-4...
CN=ERMA_PRICE,OU=Test,OU=SEC,OU=Tier 2,DC=AIS,DC=FR      ERMA_PRICE      user      2689cca6-cc4e-4...
CN=DUDLEY_BOLTON,OU=ESM,OU=Stage,DC=AIS,DC=FR      DUDLEY_BOLTON      user      0e9260c9-5721-4...
CN=STACEY_TILLMAN,OU=Test,OU=TST,OU=Stage,DC=AIS,DC=FR      STACEY_TILLMAN      user      17536805-d874-4...
CN=FRANCIS_MACIAS,OU=Groups,OU=AZR,OU=Stage,DC=AIS,DC=FR      FRANCIS_MACIAS      user      94db00c9-c960-4...
CN=GINGER_COTTON,OU=Test,OU=ITS,OU=Stage,DC=AIS,DC=FR      GINGER_COTTON      user      d5096c38-75ce-4...
CN=PATRICIA_GOMEZ,OU=Groups,OU=ITS,OU=Stage,DC=AIS,DC=FR      PATRICIA_GOMEZ      user      309e0024-c9e8-4...
CN=CHELSEA_REID,OU=Groups,OU=FSR,OU=Tier 1,DC=AIS,DC=FR      CHELSEA_REID      user      a522561f-0aee-4...
CN=GEORGINA_LLOYD,OU=Devices,OU=FIN,OU=Tier 1,DC=AIS,DC=FR      GEORGINA_LLOYD      user      b2be38f0-7e6b-4...
CN=ALBERT_HATFIELD,OU=Devices,OU=FIN,OU=Tier 2,DC=AIS,DC=FR      ALBERT_HATFIELD      user      e23fdd26-30dc-4...
```

Annexe 4 :

```
PS C:\Users\Administrateur> Get-ADObject -LDAPFilter "(userAccountControl:1.2.840.113556.1.4.803:=4194304)"

DistinguishedName      Name      ObjectClass ObjectGUID
-----
CN=Administrateur,CN=Users,DC=AIS,DC=FR      Administrateur      user      a8dfe481-1c35-4a8f-aa7c-6317d0...
```

Annexe 5 :

Group or user account ?	Priority ?	Users member ?	Computer member of the group ?	Indirect control ?	Unresolved members ?
Domain Controllers	Critical	5 (Details)	1 (Details)	630 including EVERYONE (Details)	

Annexe 6 :

Rules: 1 Score: 10

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




Annexe 7 :

Priority to remediate ?	Critical Object Found ?	Number of objects with Indirect ?	Max number of indirect numbers ?	Max ratio ?
Critical	YES	3	631	15775
High	YES	3	632	31600
Medium	YES	7	632	63200
Other	YES	1	631	63100

Annexe 8 :

```
PS C:\Users\Administrateur> netstat -ano | findstr ":135"
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 928
TCP [::]:135 [::]:0 LISTENING 928
TCP [fe80::8c15:84d7:7a87:3b99%11]:61213 [fe80::8c15:84d7:7a87:3b99%11]:135 TIME_WAIT 0
```

Annexe 9 :

Nom	Type	Description
 Invités du domaine	Groupe	Tous les invités du c
 Invités	Groupe	Les membres du gr
 Invité	Utilisateur	Compte d'utilisateu