ÉCHANTILLON · DONNÉES ANONYMISÉES

GYK

● RAPPORT DE TEST D'INTRUSION

Audit de Sécurité Offensive Active Directory & Application Web

Test d'intrusion interne — approche boîte grise
Méthodologie PTES / OWASP

Client : CONFIDENTIEL (anonymisé) | **Périmètre :** AD interne + application métier
Consultant : Guyani Youmbi Kameni — Pentester Offensif | **Version :** 1.0
Classification : Confidentiel | **Portfolio :** portfolio-gur.netlify.app

Note. Ceci est un rapport d'exemple destiné à mon portfolio. Toutes les données client, adresses IP, noms de domaine et preuves sont fictifs ou masqués. Il illustre ma structure de livrable, ma notation CVSS et mes recommandations — pas un engagement réel.

1. Synthèse exécutive

L'audit visait à évaluer la résistance du système d'information interne face à un attaquant disposant d'un accès utilisateur standard. En partant d'un simple compte de domaine, il a été possible d'obtenir le contrôle complet du domaine Active Directory (`Domain Admin`) ainsi qu'un accès non autorisé aux données d'autres utilisateurs via l'application métier.

Le chemin d'attaque principal n'a nécessité aucune vulnérabilité « zero-day » : il repose sur des défauts de configuration et de gestion des comptes de service, classiques mais à fort impact. La remédiation est réaliste à court terme.

Indicateur	Résultat
Objectif de mission	Compromission du domaine atteinte (Domain Admin)
Vulnérabilités identifiées	1 Critique · 2 Élevées · 1 Moyenne
Vecteur initial	Compte utilisateur standard (boîte grise)
Temps jusqu'au Domain Admin	< 1 journée

Vue d'ensemble des risques

ID	Vulnérabilité	Sévérité	CVSS
F-01	Kerberoasting — compte de service à mot de passe faible	ÉLEVÉE	8.1
F-02	DCSync via délégation d'ACL excessive	CRITIQUE	9.1
F-03	IDOR — accès aux ressources d'autres utilisateurs (API)	ÉLEVÉE	7.5
F-04	Absence de verrouillage de compte (bruteforce possible)	MOYENNE	5.3

2. Périmètre & méthodologie

PÉRIMÈTRE TESTÉ

- Domaine Active Directory interne : [redacted] (anonymisé)
- Application métier web exposée en interne : [redacted]
- Plage réseau interne : [redacted]

APPROCHE Boîte grise — un compte utilisateur standard fourni au départ, simulant un employé malveillant ou un poste compromis par phishing.

MÉTHODOLOGIE PTES (reconnaissance → énumération → exploitation → post-exploitation → reporting) et OWASP Testing Guide pour le volet applicatif. Notation des risques selon CVSS v3.1.

3. Chemin d'attaque (résumé)

```
[1] Énumération AD authentifiée (BloodHound) → identification de comptes kerberoastables
[2] Kerberoasting du compte de service → hash TGS extrait → mot de passe cassé hors-ligne
[3] Le compte de service dispose d'ACL excessives sur le domaine
[4] Abus de ces droits → DCSync → extraction du hash du compte Administrateur
[5] Pass-the-Hash → accès Domain Admin obtenu
```

4. Vulnérabilités détaillées

F-02 · DCSync via délégation d'ACL excessive

CRITIQUE

CVSS v3.1 : 9.1 · CWE-269 (Improper Privilege Management) · MITRE ATT&CK T1003.006

Description. Un compte de service compromis (voir F-01) disposait du droit étendu `DS-Replication-Get-Changes-All` sur l'objet domaine. Ce droit permet de simuler un contrôleur de domaine et de répliquer les secrets de tous les comptes (attaque DCSync).

Impact. Extraction du hash NTLM de n'importe quel compte, y compris `Administrateur`. Compromission totale et persistante du domaine.

Preuve (masquée).

```
secretsdump.py -just-dc-user Administrator [redacted]@[redacted]
[*] Dumping Domain Credentials
Administrator:500:[redacted]:[redacted]:::
```

Recommandations.

- Auditer les ACL du domaine (`BloodHound`, `Get-DomainObjectAcl`) et retirer les droits de réplication non nécessaires.
- Appliquer le principe du moindre privilège aux comptes de service.
- Surveiller les requêtes de réplication anormales (event ID 4662) côté SIEM.

F-01 · Kerberoasting — mot de passe de service faible

ÉLEVÉE

CVSS v3.1 : 8.1 · CWE-262 (Weak Password) · MITRE ATT&CK T1558.003

Description. Un compte de service avec un SPN enregistré utilisait un mot de passe faible. Tout utilisateur authentifié peut demander un ticket de service (TGS) et tenter de casser le mot de passe hors-ligne, sans interaction avec le compte cible.

Impact. Récupération des identifiants du compte de service, point de départ de l'escalade vers Domain Admin (voir F-02).

Preuve (masquée).

```
Rubeus.exe kerberoast /nowrap
[+] SPN : MSSQLSvc/[redacted]:1433
$krb5tgs$23$*svc_xxxx$CORP.LOCAL$[redacted]
[+] hashcat -m 13100 → mot de passe cassé : [redacted]
```

Recommandations.

- Utiliser des comptes de service gérés (gMSA) avec rotation automatique du mot de passe.
- Imposer des mots de passe de service ≥ 25 caractères aléatoires.
- Réduire le nombre de SPN exposés aux comptes strictement nécessaires.

F-03 · IDOR — accès non autorisé aux ressources (API)

ÉLEVÉE

CVSS v3.1 : 7.5 · CWE-639 (Authorization Bypass) · OWASP A01:2021

Description. L'API de l'application métier exposait des objets via un identifiant séquentiel (`/api/v1/invoices/{id}`) sans vérifier que la ressource appartenait à l'utilisateur connecté. En modifiant l'identifiant, il était possible de consulter les données d'autres clients.

Impact. Fuite de données confidentielles entre utilisateurs (factures, informations personnelles). Risque de conformité RGPD.

Preuve (masquée).

```
GET /api/v1/invoices/[redacted]   → 200 OK  (ressource de l'utilisateur courant)
GET /api/v1/invoices/[redacted]   → 200 OK  (ressource d'un AUTRE utilisateur — fuite)
```

Recommandations.

- Vérifier l'autorisation côté serveur sur chaque accès objet (contrôle propriétaire/rôle).
- Remplacer les identifiants séquentiels par des identifiants non devinables (UUID).
- Ajouter des tests d'autorisation automatisés dans la CI.

F-04 · Absence de verrouillage de compte

MOYENNE

CVSS v3.1 : 5.3 · CWE-307 (Improper Restriction of Authentication Attempts)

Description. Le portail d'authentification n'appliquait pas de limitation du nombre de tentatives, autorisant des attaques par dictionnaire / password spraying.

Impact. Compromission de comptes à mots de passe faibles, facilitant l'accès initial.

Recommandations.

- Mettre en place un verrouillage progressif et une temporisation après échecs répétés.
- Déployer le MFA sur les accès sensibles.
- Surveiller les pics d'échecs d'authentification (password spraying).

5. Conclusion

La compromission du domaine a été obtenue via un enchaînement réaliste reposant sur des défauts de configuration courants plutôt que sur des vulnérabilités exotiques. Les correctifs prioritaires (durcissement des comptes de service, revue des ACL, contrôle d'autorisation applicatif) sont réalisables rapidement et réduisent fortement la surface d'attaque.

Prochaines étapes recommandées : revue des ACL AD sous 30 jours, migration vers gMSA, correction de l'IDOR avant mise en production, et test de re-validation après remédiation.

Rapport d'exemple — Guyani Youmbi Kameni · Pentester Offensif (Red Team & Active Directory) · portfolio-gur.netlify.app · Structure et niveau de détail représentatifs de mes livrables réels (FR/EN).