



Modèle RBAC - Toolbox

Automatisée de Pentest

Version: 1.0

Date: Janvier 2026

Auteur: Ingénieur Sécurité Opérationnelle

Client: Société de Cybersécurité Offensive

1. Architecture Système

Stack technique :

- Backend : FastAPI + Pydantic
 - Base de données : MariaDB
 - Cache : Redis + Celery
 - Déploiement : WSL2
 - Authentification : JWT (RS256)
-

2. Modèle RBAC - 3 Rôles



ADMIN (Administrateur)

Responsabilité : Gestion technique, maintenance, accès complet aux logs d'audit.

Permissions :

- ✓ Créer/supprimer des utilisateurs
- ✓ Changer les rôles des autres utilisateurs
- ✓ Lancer/arrêter les scans
- ✓ Configurer les paramètres des outils (Nmap, OpenVAS, SQLmap)
- ✓ Ajouter de nouvelles cibles (IP, URL, domaines)
- ✓ Voir les résultats bruts de scan
- ✓ Supprimer des résultats et historiques
- ✓ Générer et télécharger les rapports PDF
- ✓ Accès complet aux logs d'audit (immuables, non-répudiation)

- ✓ Voir la configuration du serveur
 - ✓ Gérer les alertes de sécurité
-

PENTESTER (Opérateur)

Responsabilité : Lancer les scans, analyser les résultats, rédiger les rapports clients.

Permissions :

- ✓ Lancer et arrêter les scans
- ✓ Configurer les paramètres de scan (Nmap, OpenVAS, SQLmap)
- ✓ Ajouter de nouvelles cibles (IP, URL, domaines)
- ✓ Voir les résultats bruts de scan
- ✓ Générer et télécharger les rapports PDF

Restrictions :

- × Créer/supprimer/modifier d'autres utilisateurs
 - × Changer les rôles d'autres utilisateurs
 - × Supprimer les historiques de scan (protection non-répudiation)
 - × Accéder aux logs d'audit complets
 - × Voir la configuration du serveur
-

ANALYST (Analyste / Lecteur)

Responsabilité : Consulter les tableaux de bord et télécharger les rapports finalisés.

Permissions :

- ✓ Voir les résultats de scan (lecture seule)
- ✓ Télécharger les rapports PDF finalisés
- ✓ Accéder au tableau de bord (dashboard)

Restrictions :

- × Lancer des scans
- × Modifier les paramètres
- × Générer de nouveaux rapports
- × Ajouter des cibles
- × Accéder aux logs d'audit

3. Matrice de Contrôle d'Accès

Action	ADMIN	PENTESTER	ANALYST
Gestion Utilisateurs			
Créer utilisateur	X		
Supprimer utilisateur	X		
Changer rôle	X		
Gestion Scans			
Lancer scan	X	X	
Arrêter scan	X	X	
Configurer paramètres	X	X	
Cibles et Résultats			
Ajouter cible	X	X	
Voir résultats	X	X	X
Supprimer résultats	X		
Rapports			
Générer rapport PDF	X	X	
Télécharger rapport	X	X	X
Audit et Logs			
Voir logs d'audit complets	X		
Voir configuration serveur	X		
Gérer alertes sécurité	X		

Table 1: Matrice de contrôle d'accès par rôle

4. Principes de Sécurité RBAC

1. Validation côté serveur obligatoire

- Le rôle est TOUJOURS vérifié en base de données MariaDB
- Jamais de confiance envers le contenu du JWT
- Chaque endpoint fastAPI vérifie les permissions avant exécution

2. Non-répudiation

- Chaque action est loggée (user_id, action, timestamp, ip_address)
- Les historiques de scan ne peuvent être supprimés que par l'ADMIN
- Les logs d'audit sont immuables (ajout uniquement, jamais de modification)

3. Moindre privilège

- ANALYST : lecture seule, aucune action d'écriture
- PENTESTER : peut créer/modifier, pas d'accès administrateur
- ADMIN : accès complet mais action auditée

4. Authentification

- JWT signé avec RS256 (clé privée protégée)
- Tokens HttpOnly cookies (pas localStorage)
- Expiration courte (15-30 minutes)
- Rotation des clés tous les 90 jours

8. Checklist Implémentation

Vérification	Status
JWT validé côté serveur (signature RS256)	☐
Rôles stockés en base de données	☐
HTTPS/TLS 1.3 obligatoire	☐
Validation des entrées avec Pydantic	☐
RBAC appliqué sur tous les endpoints	☐
Logs d'audit immuables (horodatage + signature)	☐
Secrets en variables d'environnement uniquement	☐
MariaDB avec authentification TLS	☐
Redis avec AUTH configuré	☐
Permissions fichiers restrictives (umask 0077)	☐