reNgine-ng 🥷

Suite de reconnaissance nouvelle génération

reNgine-ng 🥷

Suite de reconnaissance nouvelle génération

Version 2.3.0 - Pour pentesters et bug bounty hunters

Qu'est-ce que reNgine-ng ? 🎯

Suite de reconnaissance complète

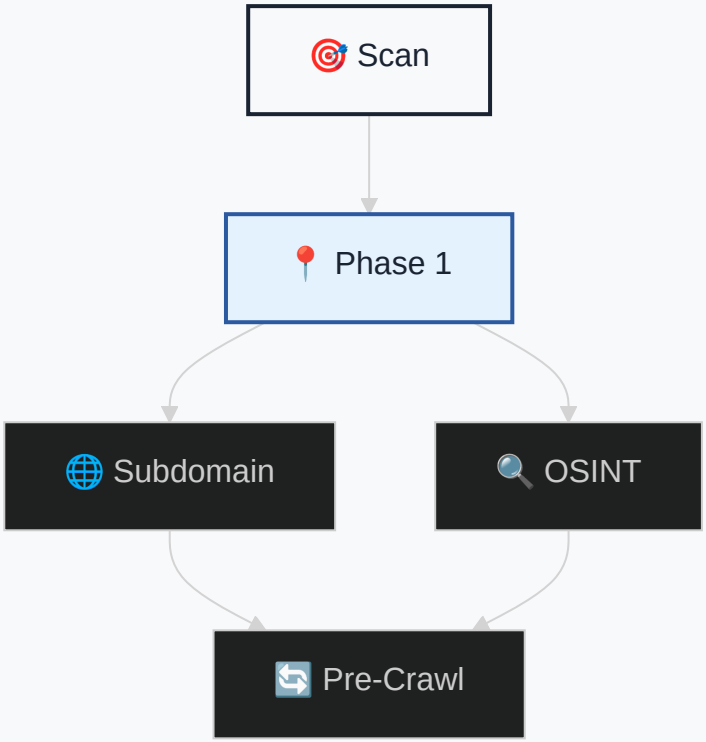
- **Reconnaissance web** : Découverte de sous-domaines, endpoints, ports
- **Scan de vulnérabilités** : Nuclei, Dalfox, CRLFuzzer, S3
- **OSINT** : Meta info, employees, emails, Google Dorking
- **Base de données** : Corrélation et organisation des données

Fonctionnalités avancées

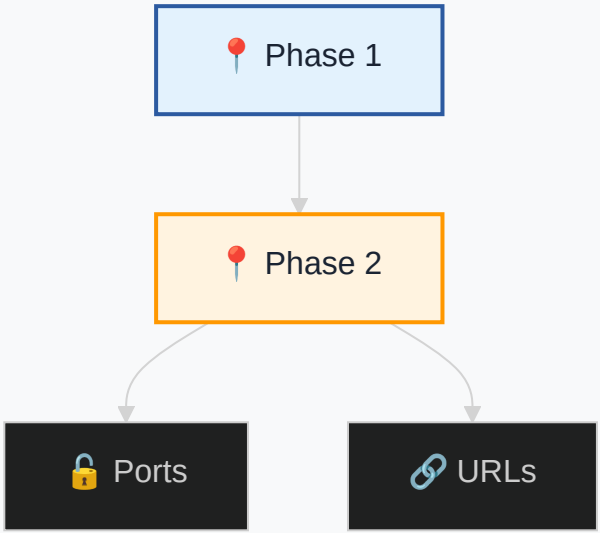
- **LLM-powered Analysis** : Analyse IA (Ollama/OpenAI)
- **Support GPU** : Accélération GPU pour LLM (NVIDIA/AMD)
- **Subscans** : Scans ciblés sur sous-domaines
- **Monitoring continu** : Scans programmés avec notifications

Architecture reNgine-ng 🏗️

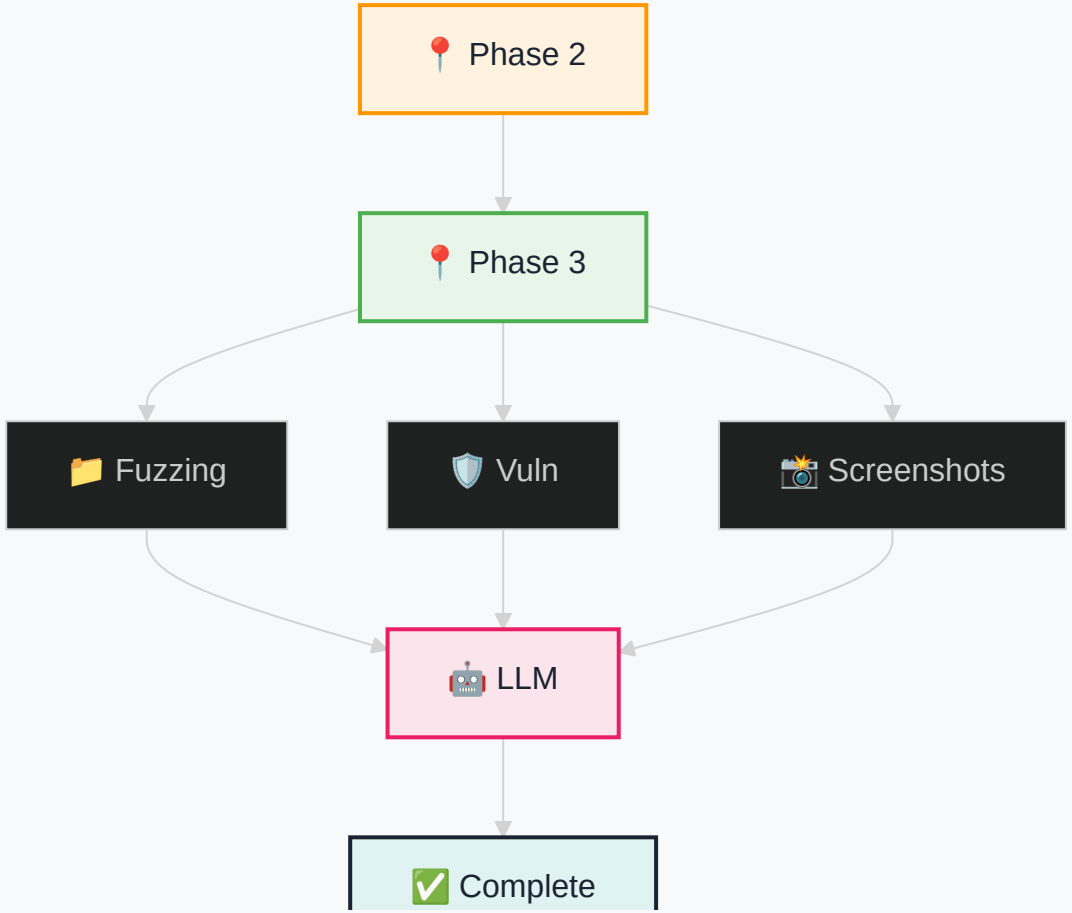
Workflow multi-phase



Workflow multi-phase



Workflow multi-phase



Fonctionnalités principales ⭐

Outils de reconnaissance intégrés

- **Subfinder, Amass, Findomain** : Découverte multi-source de sous-domaines
- **Naabu, Nmap** : Scan de ports et identification de services
- **HTTPx, Katana** : Découverte et crawl d'endpoints
- **FFuF, GoBuster** : Fuzzing de répertoires et fichiers
- **Aquatone, Eyewitness** : Capture automatique de screenshots

Scanners de vulnérabilités

- **Nuclei** : Scan de vulnérabilités avec templates personnalisables
- **Dalfox** : Scanner XSS spécialisé
- **CRLFuzzer** : Détection d'injections CRLF
- **S3Scanner** : Détection de buckets S3 mal configurés
- **WAFW00F** : Identification de WAF

Outils OSINT

- **TheHarvester** : Collecte d'emails et d'informations
- **Metagoofil** : Extraction de métadonnées
- **Google Dorking** : Recherche d'informations sensibles
- **WHOIS** : Enrichissement des données de domaine

Gestion avancée des données

- **Query Language** : Filtrage avec opérateurs (`http_status>0&name=admin`)
- **Corrélation automatique** : Liens entre subdomains, IPs, ports, endpoints
- **Détection de changements** : Nouveaux/retirés subdomains et endpoints
- **Déduplication intelligente** : Basée sur titre et longueur de contenu

Organisation et collaboration

- **Gestion de projets** : Espaces séparés par mission/client
- **Rôles et permissions** : Sys Admin, Pentester, Auditor
- **Notifications** : Discord, Slack, Telegram pour alertes
- **Export/Import** : Compatibilité avec autres outils

Avantages pour la sécurité 

Pour tous les professionnels

- **Pentesters** : Reconnaissance automatisée, corrélation, rapports
- **Bug Bounty Hunters** : Découverte rapide, scans, monitoring
- **Équipes sécurité** : Gestion projets, rôles, LLM

Installation et utilisation 🛠️

Installation rapide

- **Prérequis** : Docker, Docker Compose, Make

```
git clone https://github.com/Security-Tools-Alliance/rengine-ng.git
cd rengine-ng
sudo ./install.sh
```

Utilisation basique

1. **Créer un scan** : Via l'interface web
2. **Configurer** : Choisir les outils et paramètres
3. **Lancer** : Exécution automatique
4. **Consulter** : Interface web avec visualisation

Rapports et interface 

Formats de rapports

- **PDF** : Rapports professionnels personnalisables (texte d'intro, couleurs, en-têtes/pieds de page)
- **HTML** : Visualisation interactive via l'interface web
- **LLM Integration** : Descriptions, impacts et remédiations générées automatiquement
- **Dashboard** : Interface intuitive avec visualisation des données

Ressources 📚

Documentation et communauté

- **GitHub** : https://github.com/Security-Tools-Alliance/rengine-ng
- **Wiki** : https://github.com/Security-Tools-Alliance/rengine-ng/wiki
- **Discord** : https://discord.gg/KE5QGTqJpS

Roadmap : Release v3.0.0 - Février 2026 🚀

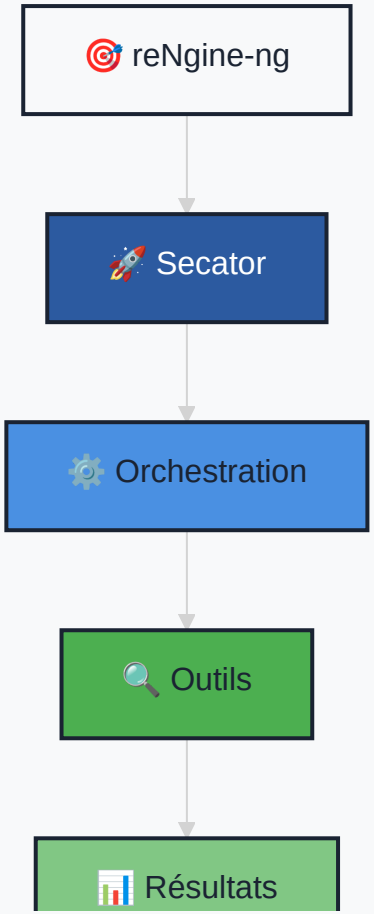
Intégration de Secator en tant qu'Engine

- **Bibliothèque Python** : Orchestration d'outils de reconnaissance
- **Distribution** : Via Celery pour exécution distribuée
- **Gestion dépendances** : Ordre d'exécution automatique
- **API Hooks** : Remontée automatique des résultats

Caractéristiques principales

- **Orchestration** : Exécution séquentielle ou parallèle
- **Profils** : Vitesse et furtivité configurables
- **Workflows** : Workflows prédéfinis ou personnalisés
- **Distribution** : Workers distants via Redis

Flux de travail Secator



Workers Secator distants

- **Workers distants** : VPS ou réseaux internes
- **Redis** : File de tâches Celery
- **API** : Remontée automatique des résultats
- **Cas d'usage** : Multi-location, réseaux internes, scalabilité

Intégration BurpNgine

- **Plugin Burp Suite** : Couplage avec Burp Suite Professional/Community
- **Synchronisation bidirectionnelle** : Envoi de cibles depuis reNgine-ng vers Burp
- **Import de résultats** : Récupération des résultats Burp dans reNgine-ng
- **Workflow intégré** : Reconnaissance reNgine-ng → Tests Burp → Corrélation

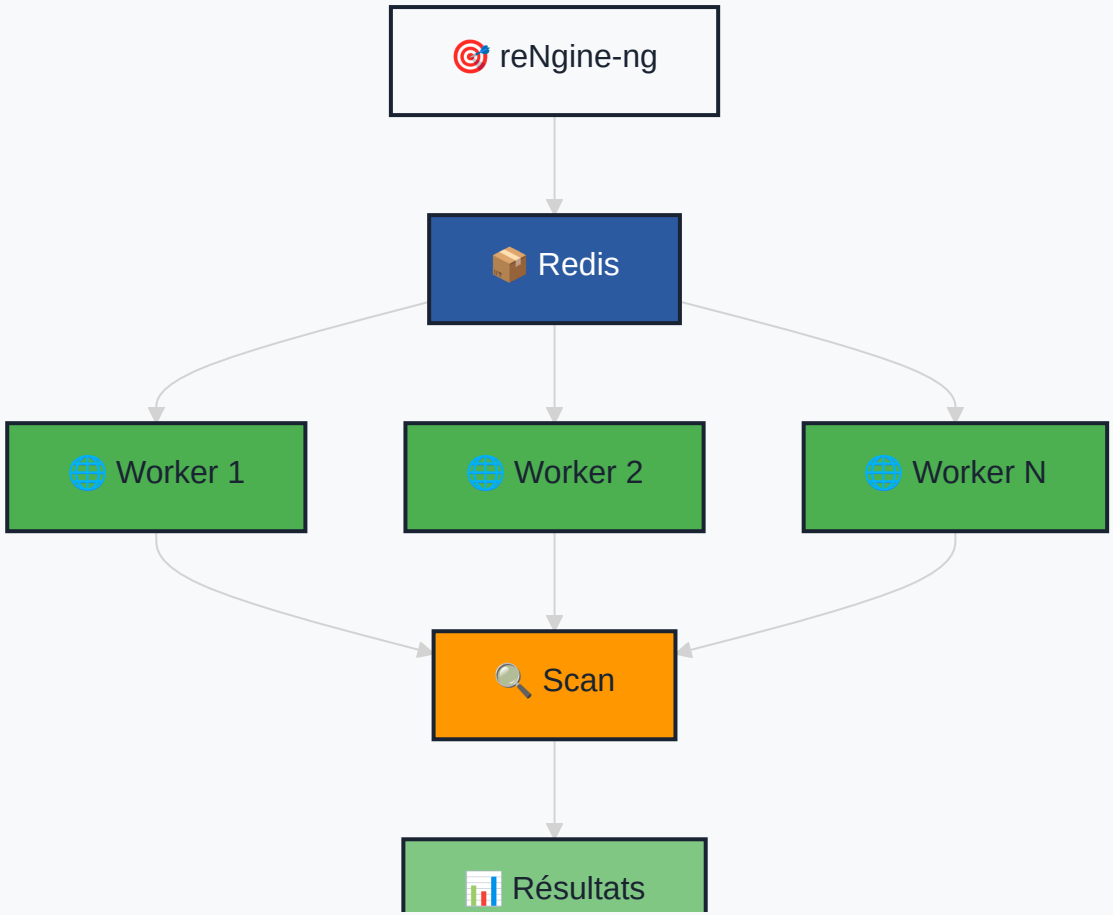
Amélioration de l'API

- **API REST complète** : Accès à toutes les fonctionnalités via API
- **Documentation Swagger** : Documentation interactive de l'API
- **Authentification renforcée** : API keys et tokens sécurisés
- **Webhooks** : Notifications en temps réel via webhooks

Interface CLI

- **CLI officiel** : Pilotage de reNgine-ng depuis le terminal
- **Gestion complète** : Création de scans, consultation de résultats
- **Export de données** : Export de subdomains, endpoints, vulnérabilités
- **Intégration scripts** : Automatisation via scripts shell/Python

Workflow workers distants



Merci ! 🙏

Vous pouvez venir à ma rencontre pour une démo plus en profondeur de l'outil

Questions ?