**CAHIER DES CHARGES - CYBERNADE**

**Application Desktop Multi-Tool Cybersécurité**

**1. CONTEXTE ET OBJECTIFS**

**1.1 Contexte du Projet**

Le projet CYBERNADE vise à développer une application desktop complète dédiée à la cybersécurité, regroupant l'ensemble des outils nécessaires aux professionnels de la sécurité informatique. Cette solution se positionne comme une alternative open-source aux outils commerciaux existants.

**1.2 Objectifs Principaux**

* **Centralisation** : Regrouper tous les outils de cybersécurité en une seule interface
* **Accessibilité** : Rendre les outils complexes accessibles via une interface intuitive
* **Modularité** : Architecture modulaire permettant l'ajout de nouvelles fonctionnalités
* **Performance** : Optimisation pour une utilisation professionnelle intensive
* **Sécurité** : Respect des standards de sécurité et bonnes pratiques éthiques

**1.3 Public Cible**

* Pentesters et consultants en sécurité
* Analystes SOC (Security Operations Center)
* Étudiants et chercheurs en cybersécurité
* Administrateurs systèmes et réseaux
* Bug bounty hunters

**2. SPÉCIFICATIONS FONCTIONNELLES**

**2.1 Module OSINT & Reconnaissance**

**2.1.1 Recherche d'Informations**

**Fonctionnalités obligatoires :**

* Recherche par IP, domaine, email, username
* Intégration APIs : Shodan, Censys, Hunter.io, HaveIBeenPwned
* Extraction métadonnées (PDF, images, documents Office)
* Géolocalisation IP avec cartes interactives
* Historique des recherches avec système de tags

**Fonctionnalités optionnelles :**

* Integration VirusTotal pour analyse de domaines
* Recherche dans les bases de données de leaks
* Export des résultats en JSON/CSV/PDF

**2.1.2 Analyse Réseaux Sociaux**

**Fonctionnalités obligatoires :**

* Recherche multi-plateformes (Twitter, LinkedIn, Instagram)
* Collecte d'informations publiques
* Génération de graphiques de relations

**Contraintes :**

* Respect des APIs officielles uniquement
* Conformité RGPD et politiques de confidentialité
* Limitation du taux de requêtes

**2.2 Module Analyse de Vulnérabilités**

**2.2.1 Scan de Ports et Services**

**Fonctionnalités obligatoires :**

* Interface graphique pour Nmap
* Détection de services et versions
* Visualisation des résultats sous forme de graphiques
* Sauvegarde des scans avec horodatage

**2.2.2 Détection de Vulnérabilités**

**Fonctionnalités obligatoires :**

* Lookup CVE via NVD API
* Base de données locale de vulnérabilités
* Score CVSS et criticité
* Recommandations de correction

**2.3 Module Outils Réseau**

**2.3.1 Analyse de Trafic**

**Fonctionnalités obligatoires :**

* Capture de paquets avec Scapy
* Filtrage et analyse en temps réel
* Détection de protocoles suspects
* Export PCAP

**2.3.2 Audit Wi-Fi**

**Fonctionnalités obligatoires :**

* Scan des réseaux Wi-Fi disponibles
* Analyse des protocoles de sécurité
* Détection WPS activé
* Cartographie des points d'accès

**2.4 Module Cryptographie**

**2.4.1 Chiffrement/Déchiffrement**

**Fonctionnalités obligatoires :**

* Support AES, RSA, DES, 3DES
* Interface simple pour chiffrement de fichiers/texte
* Génération de clés sécurisées
* Vérification d'intégrité (hash)

**2.4.2 Analyse Cryptographique**

**Fonctionnalités obligatoires :**

* Analyse de force des mots de passe
* Détection de chiffrements faibles
* Support des hash MD5, SHA1, SHA256, SHA512

**2.5 Module Stéganographie**

**Fonctionnalités obligatoires :**

* Dissimulation LSB dans les images
* Extraction de données cachées
* Support formats : PNG, JPEG, BMP
* Analyse d'entropy pour détection

**2.6 Module Forensic**

**2.6.1 Analyse de Fichiers**

**Fonctionnalités obligatoires :**

* Extraction de strings
* Calcul d'entropy
* Détection de format réel (magic bytes)
* Recherche de signatures malware

**2.6.2 Analyse Système**

**Fonctionnalités obligatoires :**

* Surveillance processus en temps réel
* Analyse de logs système
* Détection de modifications de fichiers
* Timeline d'activités

**2.7 Module Pentesting**

**2.7.1 Brute Force**

**Fonctionnalités obligatoires :**

* Support SSH, FTP, HTTP, SMB
* Gestion de wordlists personnalisées
* Système de proxies et rotation IP
* Limitation de taux configurable

**2.7.2 Exploitation**

**Fonctionnalités obligatoires :**

* Interface pour exploits manuels
* Génération de payloads personnalisés
* Gestion de reverse shells
* Logs détaillés des actions

**3. SPÉCIFICATIONS TECHNIQUES**

**3.1 Architecture Technique**

**3.1.1 Technologies**

* **Langage** : Python 3.10+
* **Interface** : PyQt5 (interface moderne) ou Tkinter (légère)
* **Base de données** : SQLite (local) + Redis (cache optionnel)
* **APIs** : Requests, aiohttp pour requêtes asynchrones
* **Réseau** : Scapy, python-nmap, netaddr
* **Cryptographie** : PyCryptodome, cryptography

**3.1.2 Architecture Modulaire**

CYBERNADE/

├── core/ # Noyau de l'application

│ ├── \_\_init\_\_.py

│ ├── app.py # Application principale

│ ├── config.py # Configuration globale

│ ├── database.py # Gestionnaire BDD

│ └── plugin\_manager.py # Gestionnaire de plugins

├── modules/ # Modules fonctionnels

│ ├── osint/

│ ├── vuln\_scanner/

│ ├── network\_tools/

│ ├── crypto/

│ ├── forensic/

│ └── pentest/

├── gui/ # Interface graphique

│ ├── main\_window.py

│ ├── components/

│ └── themes/

├── utils/ # Utilitaires

├── config/ # Fichiers de configuration

├── data/ # Données statiques

└── plugins/ # Plugins externes

**3.2 Interfaces et Ergonomie**

**3.2.1 Interface Principale**

* **Design** : Interface sombre (Dark Theme) par défaut
* **Navigation** : Menu latéral avec icônes pour chaque module
* **Dashboard** : Page d'accueil avec statistiques et raccourcis
* **Notifications** : Système d'alertes non-intrusives

**3.2.2 Expérience Utilisateur**

* **Temps de réponse** : < 2 secondes pour les actions standards
* **Accessibilité** : Support des raccourcis clavier
* **Personnalisation** : Thèmes, disposition des panneaux
* **Aide contextuelle** : Tooltips et documentation intégrée

**3.3 Gestion des Données**

**3.3.1 Stockage Local**

* **Configuration** : Fichiers JSON/YAML
* **Logs** : SQLite avec rotation automatique
* **Cache** : Système de mise en cache des requêtes API
* **Exports** : Support PDF, CSV, JSON, XML

**3.3.2 Sécurité des Données**

* **Chiffrement** : Données sensibles chiffrées localement
* **Authentification** : Mode professionnel avec authentification
* **Audit** : Logs complets des actions utilisateur

**4. CONTRAINTES ET EXIGENCES**

**4.1 Contraintes Techniques**

**4.1.1 Performance**

* **RAM** : Utilisation < 500 MB en fonctionnement normal
* **CPU** : Optimisation des algorithmes intensifs
* **Stockage** : Application < 100 MB, données < 1 GB
* **Réseau** : Gestion des timeouts et reconnexions

**4.1.2 Compatibilité**

* **OS** : Windows 10+, Linux (Ubuntu 20.04+), macOS 10.15+
* **Python** : Version 3.10 minimum
* **Dépendances** : Gestion via requirements.txt et pip

**4.2 Contraintes Légales et Éthiques**

**4.2.1 Aspects Légaux**

* **Disclaimer** : Avertissement d'usage responsable obligatoire
* **Logs** : Traçabilité des actions pour audit
* **Conformité** : Respect des lois locales sur la cybersécurité

**4.2.2 Éthique**

* **Pas de backdoor** : Code source transparent
* **Pas de collecte** : Aucune donnée envoyée vers des serveurs tiers
* **Mode éducatif** : Documentation des risques et bonnes pratiques

**4.3 Sécurité de l'Application**

**4.3.1 Sécurité du Code**

* **Code review** : Validation par pairs obligatoire
* **Tests de sécurité** : Audit de sécurité régulier
* **Mise à jour** : Système de mise à jour sécurisé

**4.3.2 Protection des Données**

* **Chiffrement** : AES-256 pour les données sensibles
* **Authentification** : Hachage sécurisé des mots de passe
* **Isolation** : Sandboxing des modules critiques

**5. PLANNING ET LIVRABLES**

**5.1 Phases de Développement**

**Phase 1 - MVP (8 semaines)**

* Interface graphique de base
* Module OSINT simplifié
* Module scan réseau basique
* Configuration et base de données

**Phase 2 - Core Features (6 semaines)**

* Modules cryptographie et stéganographie
* Module forensic de base
* Système de plugins
* Tests et debugging

**Phase 3 - Advanced Features (8 semaines)**

* Module pentesting complet
* Outils réseau avancés
* Dashboard et reporting
* Documentation utilisateur

**Phase 4 - Polish & Release (4 semaines)**

* Tests de sécurité complets
* Optimisation des performances
* Packaging et distribution
* Formation et support

**5.2 Livrables**

**Livrables Techniques**

* Code source commenté et documenté
* Tests unitaires et d'intégration
* Documentation technique complète
* Scripts de déploiement

**Livrables Utilisateur**

* Application packagée (exécutable)
* Manuel utilisateur
* Tutoriels vidéo
* FAQ et troubleshooting

**6. CRITÈRES D'ACCEPTATION**

**6.1 Critères Fonctionnels**

* ✅ Tous les modules définis sont implémentés et fonctionnels
* ✅ Interface utilisateur intuitive et responsive
* ✅ Gestion des erreurs et exceptions robuste
* ✅ Système de logs et audit opérationnel

**6.2 Critères de Performance**

* ✅ Temps de démarrage < 5 secondes
* ✅ Utilisation mémoire conforme aux spécifications
* ✅ Pas de fuite mémoire après utilisation intensive
* ✅ Interface réactive même sous charge

**6.3 Critères de Sécurité**

* ✅ Audit de sécurité réalisé sans faille critique
* ✅ Données sensibles correctement chiffrées
* ✅ Pas de vulnérabilité dans les dépendances
* ✅ Code source exempt de backdoors

**6.4 Critères de Qualité**

* ✅ Code coverage des tests > 80%
* ✅ Documentation complète et à jour
* ✅ Installation simplifiée sur tous les OS cibles
* ✅ Support utilisateur réactif

**7. RISQUES ET MITIGATION**

**7.1 Risques Techniques**

| **Risque** | **Probabilité** | **Impact** | **Mitigation** |
| --- | --- | --- | --- |
| Problèmes de compatibilité OS | Moyen | Élevé | Tests sur VMs, CI/CD |
| Performance insuffisante | Faible | Moyen | Profiling régulier, optimisation |
| Dépendances obsolètes | Élevé | Moyen | Monitoring automatisé |

**7.2 Risques Légaux**

| **Risque** | **Probabilité** | **Impact** | **Mitigation** |
| --- | --- | --- | --- |
| Usage malveillant | Élevé | Élevé | Disclaimers, logs, éducation |
| Violation APIs tierces | Moyen | Moyen | Respect ToS, rate limiting |
| Réglementation locale | Faible | Élevé | Consultation juridique |

**8. BUDGET ET RESSOURCES**

**8.1 Ressources Humaines**

* **Lead Developer** : 1 développeur Python senior (6 mois)
* **Security Expert** : 1 expert cybersécurité (2 mois)
* **UX/UI Designer** : 1 designer (1 mois)
* **QA Tester** : 1 testeur (2 mois)

**8.2 Infrastructure**

* **Développement** : Serveurs de test et intégration continue
* **APIs** : Coûts d'accès aux APIs tierces (Shodan, etc.)
* **Distribution** : Hébergement et CDN pour les releases

**8.3 Budget Estimé**

* **Développement** : 40 000€ - 60 000€
* **Infrastructure** : 2 000€ - 5 000€
* **APIs et licences** : 1 000€ - 3 000€
* **Marketing et communication** : 2 000€ - 5 000€

**Total estimé : 45 000€ - 73 000€**

*Ce cahier des charges est un document évolutif qui sera mis à jour selon les besoins du projet et les retours des parties prenantes.*