**Réf : …../………… AU : 2024 - 2025**

**Université de Sousse**

**Ecole Nationale d’Ingénieurs de Sousse**



**Conception et mise en œuvre d'une plateforme automatisée de scan et tests de sécurité basée sur des outils open source**

**Réalisé par :**

**RAOUF BRAHEM, NAJD ELADEL & HOUSSEM EDDIN CHAOUACH**

**Encadré par :**

**Mme OLFA DALLEL**

**Département :**

**Informatique Industrielle**

**Groupe :**

**IA2.2**

# Cahier des charges

## Présentation générale du projet

Ce projet vise à concevoir une plateforme automatisée de scan et de tests de sécurité utilisant des outils open source pour **détecter efficacement les vulnérabilités**. Il répond au besoin croissant d'accessibilité et d'efficacité dans la cybersécurité, notamment pour les PME. En centralisant et standardisant les processus, il réduit les coûts, améliore la rapidité d'analyse et renforce la sécurité des systèmes.

## Problématique

Dans un contexte où les attaques informatiques deviennent de plus en plus sophistiquées et fréquentes, les entreprises ont besoin de solutions rapides, précises et adaptées pour protéger leurs systèmes. Les solutions de sécurité commerciales, bien que puissantes, sont souvent coûteuses et limitées en personnalisation. De plus, les tests manuels demandent une expertise avancée et sont difficilement reproductibles à grande échelle.

## Solution

Ce projet a pour objectif de concevoir et de déployer une plateforme intégrée pour automatiser les processus de reconnaissance, de scan de vulnérabilités et de tests de sécurité. En tant qu'élèves ingénieurs, nous explorerons des outils open source et documenterons les workflows pour en assurer le maintien. Ce projet répond à ces défis en proposant une plateforme automatisée basée sur des outils open source, combinant des technologies modernes pour :

* **Automatiser la détection des vulnérabilités** grâce à des scans réguliers et ciblés, réduisant le temps d’analyse par rapport aux méthodes traditionnelles ;
* **Intégrer des outils éprouvés et modulables** pour un coût réduit, tout en permettant une adaptation rapide aux besoins spécifiques ;
* **Standardiser et centraliser les processus de test**, garantissant une méthodologie reproductible et une couverture exhaustive des menaces potentielles.

## Analyse de l’existant

### Solutions existantes

#### Pentest-tools.com

A screenshot of a computer

Description automatically generatedObtenez la perspective d'un hacker sur vos applications web, votre réseau et votre cloud. Pentest-Tools.com aide les équipes de sécurité à réaliser les étapes clés d'un test de pénétration, facilement et sans compétences spécialisées en hacking. Basé en Europe (à Bucarest, Roumanie), ***Pentest-Tools.com*** propose des outils de cybersécurité offensifs et des logiciels de scanner de vulnérabilités propriétaires pour les testeurs de pénétration et autres professionnels de la sécurité informatique. Les équipes de sécurité utilisent notre boîte à outils pour identifier les chemins que les attaquants peuvent emprunter pour compromettre votre organisation, afin que vous puissiez réduire efficacement votre exposition aux cyberattaques.

**Figure 1 : Pesntest-tools.com platform**

#### Intruder

***Intruder*** est une plateforme de gestion des vulnérabilités qui offre une vue en temps réel des surfaces d'attaque grâce à une surveillance continue du réseau, un scan automatisé des vulnérabilités et une réponse proactive aux menaces. Avec des rapports prêts pour les audits et des résultats exploitables priorisés par contexte, ***Intruder*** aide plus de 2 500 clients à travers le monde à se concentrer sur la correction des problèmes essentiels, rendant la gestion des vulnérabilités facile et efficace. ***Intruder*** s'intègre à AWS, Azure, Google Cloud, Slack, Jira, et bien plus encore.

A screenshot of a computer

Description automatically generated

**Figure 2 : Imtruder platform**

### Tableau comparatif

Ce tableau compare les deux plateformes, **Intruder** et **Pentest-Tools.com**, en termes de fonctionnalités, avantages et désavantages. Il met en évidence leurs principales différences, telles que la gestion continue des vulnérabilités et la flexibilité des tests de pénétration. Ce comparatif permet de mieux comprendre quel outil convient selon les besoins spécifiques en cybersécurité.

|  |  |  |
| --- | --- | --- |
| **Critère** | **Intruder** | **Pentest-tools** |
| **Type de Plateforme** | Gestion des vulnérabilités avec tests automatisés | Tests de pénétration automatisés |
| **Fonctionnalités** | Surveillance continue du réseau, scan de vulnérabilités automatisé, réponse proactive aux menaces | Outils pour la reconnaissance, scan de vulnérabilités, tests de pénétration |
| **Cible** | Entreprises cherchant une gestion continue des vulnérabilités | Utilisateurs cherchant à effectuer des tests de pénétration ponctuels |
| **Rapports** | Rapports prêts pour les audits, résultats exploitables priorisés par contexte | Rapports détaillés avec des suggestions de correction |
| **Intégrations** | AWS, Azure, Google Cloud, Slack, Jira, etc. | Intégrations limitées, mais outils compatibles avec diverses plateformes |
| **Facilité d'utilisation** | Interface intuitive, principalement automatisée | Interface plus technique, adaptée aux utilisateurs expérimentés |
| **Public Cible** | PME et grandes entreprises cherchant une gestion proactive de la sécurité | Pentesters et professionnels de la cybersécurité |
| **Méthodologie de Test** | Scans réguliers et tests automatisés | Tests ponctuels via divers outils d'attaque |
| **Accès aux Outils** | Accès complet via abonnement, plan basé sur les besoins | Abonnement basé sur l'accès aux outils spécifiques |
| **Rapidité d'Analyse** | Temps d'analyse en temps réel, continuellement mis à jour | Temps d'analyse plus long, dépend des tests manuels |
| **Tarification** | Abonnement mensuel basé sur les services choisis | Abonnement à la carte en fonction des outils utilisés |
| **Avantages** | |  | | --- | |  |  |  | | --- | | - Surveillance continue et proactive des vulnérabilités - Rapports prêts pour les audits - Intégration avec des outils populaires (AWS, Azure, Slack, Jira) | | - Outils spécifiques pour divers tests de pénétration - Grande flexibilité dans le choix des outils - Convient aux pentesters expérimentés |
| **Désavantage** | - Moins adapté pour les tests ponctuels - Moins de contrôle sur les tests manuels - Coût récurrent basé sur l'abonnement mensuel | - Moins de gestion continue des vulnérabilités - Interface plus complexe et moins automatisée - Nécessite une expertise technique plus élevée |

**Table 1 : Comparaison entre Intruder et Pentest-Tools.com**

## Besoins et technologies

### Besoins fonctionnels

* **Scan de vulnérabilités automatisé** : La plateforme doit être capable d'effectuer des scans de vulnérabilités sur les applications web, les réseaux, et les infrastructures cloud de manière automatisée.
* **Identification des vulnérabilités** : La plateforme doit pouvoir identifier une large gamme de vulnérabilités, telles que les injections SQL, les failles XSS, les erreurs de configuration, etc.
* **Rapports détaillés** : Fournir des rapports clairs et détaillés sur les vulnérabilités identifiées, y compris des recommandations de correction.
* **Surveillance continue** : La plateforme doit offrir une fonction de surveillance continue des systèmes pour détecter rapidement de nouvelles vulnérabilités.
* **Gestion des utilisateurs** : Permettre à plusieurs utilisateurs avec différents niveaux d'accès d'interagir avec la plateforme (administrateurs, analystes, etc.).
* **Intégrations externes** : Supporter des intégrations avec des outils tiers populaires comme AWS, Azure, Google Cloud, Slack, et Jira pour faciliter le flux de travail.
* **Alertes et notifications** : Offrir des alertes en temps réel concernant de nouvelles vulnérabilités ou des menaces potentielles.

### Besoins non fonctionnels

* **Scalabilité :** La plateforme doit être capable de gérer un grand nombre de requêtes et d'utilisateurs simultanés sans compromettre les performances.
* **Sécurité :** Assurer que les données sensibles, comme les résultats des scans et les informations des utilisateurs, sont stockées et transmises de manière sécurisée.
* **Disponibilité :** La plateforme doit être disponible 24/7 avec un temps de disponibilité élevé, garantissant un service fiable.
* **Performance :** Les scans et les analyses doivent être réalisés dans des délais raisonnables, avec un faible temps de réponse.

### Technologies utilisées

PYTHON, BASH, SUBFINDER, NMAP, OWASP, ZAP, GOPHISH.

**Contrainte :** Kali Linux VM.