Direction générale

Service Cybersécurité

Automatisation d’un test d’intrusion

CAHIER DES CLAUSES TECHNIQUES PARTICULIÈRES

Table des matières

1 RESUME DU PROJET

L’objet du projet sera de développer une toolbox automatique qui sera conçue pour simplifier le processus de réalisation de tests d'intrusion en automatisant de nombreuses tâches. Elle permettra également d'améliorer l'efficacité des tests en utilisant des techniques avancées d'analyse de vulnérabilités.

2 OBJET DU DOCUMENT

L'objectif de ce projet professionnel en cybersécurité est de concevoir et développer une toolbox automatisée pour la réalisation de tests d'intrusion, permettant ainsi d'identifier les vulnérabilités et de renforcer la sécurité des systèmes informatiques et des réseaux.

3 NORMES ET RÈGLEMENTS APPLICABLES

L'ensemble des ouvrages demandés devra répondre aux prescriptions des normes et règlements selon les bonnes pratiques cohérentes avec l’état de l’art.

Bien noter qu'en cas de divergence entre spécifications, la plus contraignante sera toujours retenue.

3.1 LOIS, DÉCRETS ET REGLEMENT

Les propositions de la MOE devront être conformes aux clauses de l'ensemble des lois, décrets, arrêtés, règlements, circulaires, normes et tous les textes nationaux ou locaux applicables aux ouvrages de la présente opération.

Les documents, ci-après, sont applicables dans leur dernière édition. Cette liste n'est pas limitative.

- Loi no 78-17 du 6 janvier 1978
- Règlement européen 2016/679 dit RGPD
- Directive 2016/1148 dite NIS

3.2 DOCUMENT TECHNIQUES ET NORMES

De même, tous les travaux devront répondre aux prescriptions techniques et fonctionnelles définies par les textes normatifs ou documents techniques auxquels ils se réfèrent et notamment :

• Famille de Normes ISO27000 et son approche EBIOS-RM

• Famille de normes ISO31000

La sécurité applicative ainsi que la souveraineté des données seront des objets d'attention permanente. La pertinence des préconisations de l'ANSSI seront évaluées au vu des solutions techniques retenues par la MOE.

3.4 AUTRES DOCUMENTS

Toutes modifications nécessaires au respect de ces documents font partie intégrante du périmètre de responsabilité de la MOE et ne donneront pas lieu à révision des conditions de l'intervention.

Le fait de ne pas énumérer tous ces documents nommément, ne pourra être pris pour argument d'ignorance par l'Entreprise, celle-ci étant réputée les connaître, du seul fait de soumissionner.

4 DESCRIPTION DU PROJET

4.1 GÉNÉRALITTÉS

L'entreprise X est une société de cybersécurité spécialisée dans les tests d'intrusion pour les entreprises et les organisations gouvernementales. Elle est reconnue pour sa capacité à réaliser des tests d'intrusion complets et précis pour aider ses clients à renforcer la sécurité de leurs systèmes informatiques et de leurs réseaux.

Cependant, l'entreprise X est confrontée à des défis tels que des délais serrés et une charge de travail importante pour répondre aux demandes croissantes de ses clients. Pour résoudre ces problèmes, l'entreprise souhaite développer une toolbox automatisée pour la réalisation de tests d'intrusion, qui permettra de simplifier et d'accélérer le processus de réalisation des tests, tout en améliorant la qualité des résultats.

Le projet consistera donc à concevoir et développer cette toolbox automatisée en utilisant des technologies modernes telles que Python et des bibliothèques spécialisées dans la cybersécurité. La toolbox sera également intégrée à des outils de visualisation des résultats pour faciliter l'interprétation des résultats.

L'objectif final du projet est de fournir à l'entreprise X une solution efficace et automatisée pour réaliser des tests d'intrusion de haute qualité dans des délais plus courts, ce qui améliorera la satisfaction des clients et la réputation de l'entreprise dans le domaine de la cybersécurité.

4.2 FONCTIONNEMENT GÉNÉRAL

Le présent projet consiste en la conception et le développement d'une toolbox automatisée pour la réalisation de tests d'intrusion. Cette toolbox permettra à l'entreprise X de simplifier et d'accélérer le processus de réalisation des tests, tout en améliorant la qualité des résultats.

La toolbox sera conçue pour fonctionner de manière autonome et automatisée, en utilisant des technologies modernes telles que Python et des bibliothèques spécialisées dans la cybersécurité. Les utilisateurs de la toolbox n'auront pas besoin d'avoir une connaissance approfondie des tests d'intrusion ou des outils de cybersécurité pour l'utiliser efficacement.

La toolbox sera dotée de fonctionnalités telles que la découverte de ports et de services, la détection de vulnérabilités, l'analyse de la sécurité des mots de passe et la réalisation de tests d'authentification. La toolbox sera également capable de fournir des résultats clairs et détaillés, présentés sous forme de rapports et de visualisations graphiques, pour aider les utilisateurs à comprendre les vulnérabilités identifiées et à prendre des mesures pour les corriger.

Le fonctionnement général de la toolbox comprendra les étapes suivantes :

1. Configuration : L'utilisateur configurera la toolbox pour répondre aux besoins spécifiques du test d'intrusion.
2. Exploration : La toolbox explorera le système cible pour identifier les ports, les services et les vulnérabilités.
3. Exploitation : La toolbox exploitera les vulnérabilités identifiées pour obtenir un accès non autorisé au système cible.
4. Post-exploitation : La toolbox effectuera une analyse approfondie du système cible pour identifier les données sensibles et les mesures de sécurité en place.
5. Reporting : La toolbox produira des rapports détaillés sur les résultats des tests d'intrusion et les vulnérabilités identifiées, ainsi que des visualisations graphiques pour aider les utilisateurs à comprendre les résultats.

Le fonctionnement général de la toolbox sera conçu pour être simple, efficace et automatisé, permettant ainsi à l'entreprise X de réaliser des tests d'intrusion de haute qualité dans des délais plus courts, améliorant ainsi la satisfaction des clients et la réputation de l'entreprise dans le domaine de la cybersécurité.

4.3 FONCTIONS PRINCIPALES

La toolbox automatisée pour les tests d'intrusion développée dans ce projet offrira plusieurs fonctions principales pour permettre une réalisation complète et efficace des tests d'intrusion.

1. Découverte de ports et de services : La toolbox explorera le système cible pour identifier les ports et les services en cours d'exécution. Cela permettra à l'utilisateur de connaître l'architecture du système cible et les services disponibles.
2. Détection de vulnérabilités : La toolbox recherchera les vulnérabilités connues dans les ports et les services identifiés précédemment. Elle pourra également identifier les vulnérabilités qui n'ont pas été corrigées par les mises à jour de sécurité.
3. Analyse de la sécurité des mots de passe : La toolbox sera capable d'analyser la sécurité des mots de passe utilisés pour accéder aux services du système cible. Elle pourra identifier les mots de passe faibles, réutilisés et potentiellement compromis.
4. Tests d'authentification : La toolbox pourra réaliser des tests d'authentification pour vérifier si les identifiants et mots de passe fournis sont valides.
5. Exploitation de vulnérabilités : La toolbox sera capable d'exploiter les vulnérabilités identifiées pour obtenir un accès non autorisé au système cible. Cette fonction sera utilisée pour vérifier l'efficacité des mesures de sécurité en place et pour identifier les vulnérabilités qui peuvent être exploitées pour un accès non autorisé.
6. Post-exploitation : La toolbox pourra effectuer une analyse approfondie du système cible pour identifier les données sensibles et les mesures de sécurité en place.
7. Reporting : La toolbox produira des rapports détaillés sur les résultats des tests d'intrusion et les vulnérabilités identifiées, ainsi que des visualisations graphiques pour aider les utilisateurs à comprendre les résultats.

Ces fonctions principales seront développées en utilisant des bibliothèques spécialisées dans la cybersécurité et en suivant les meilleures pratiques de développement pour garantir la sécurité, la qualité et la fiabilité de la toolbox. Ces fonctions seront conçues pour être simples, automatisées et efficaces, permettant ainsi à l'entreprise X de réaliser des tests d'intrusion de haute qualité dans des délais plus courts.

4.4 LES APPLICATIONS FONCTIONNELLES

Une description résumée des fonctionnalités des solutions proposées sera fournie par la MOE pour chacune des demandes ci-après.

4.5 LES OUTILS

Dans le cadre du projet de développement d'une toolbox automatisée pour les tests d'intrusion, il est important de noter que de nombreux outils et bibliothèques open-source sont disponibles gratuitement sur des plateformes telles que GitHub. Ces outils peuvent être utilisés et intégrés dans la toolbox à condition qu'ils soient compatibles avec les fonctions principales du projet. En effet, l'utilisation d'outils open-source permet de gagner du temps et de l'argent en évitant de recréer des fonctionnalités qui existent déjà.

Cependant, il est important de vérifier que les outils et bibliothèques sont autorisés à être utilisés pour un usage commercial et qu'ils sont sous une licence open-source. Dans le cas où l'outil ou la bibliothèque est soumis à une licence propriétaire, une autorisation écrite du propriétaire doit être obtenue avant de l'utiliser.

5 LES PREREQUIS TECHNIQUE

Avant de commencer le développement de la toolbox automatisée pour les tests d'intrusion, il est important de s'assurer que les prérequis techniques nécessaires sont en place. Les prérequis techniques pour le projet comprennent :

- Un environnement de développement intégré (IDE) tel que Visual Studio Code ou PyCharm pour faciliter la programmation et la gestion du code source.
- Un système d'exploitation compatible avec les outils et bibliothèques utilisés dans le projet, tels que Kali Linux, Debian ou Ubuntu.
- Des connaissances de base en langage de programmation Python et en développement de scripts pour la cybersécurité.
- Des connaissances en tests d'intrusion et en analyse de vulnérabilité.
- Un accès à Internet pour installer et mettre à jour les outils et bibliothèques nécessaires pour le projet.
- Un environnement de test pour tester la toolbox avant sa mise en production.

Il est important de noter que les prérequis techniques peuvent varier en fonction des exigences spécifiques du projet et des technologies utilisées. Par conséquent, il est important de vérifier les prérequis techniques spécifiques avant de commencer le développement de la toolbox automatisée pour les tests d'intrusion.

6 DESCRIPTION DES PRESTATIONS

6.1 LIVRABLES

La MOE doit, au titre du projet, la remise des composants suivant sous formats numérique géré en configuration :

- Le schéma d'architecture et la justification des composants ainsi que des choix
- Solution de simulation des différentes unités (sources, exe, installateur)
- Solution de contrôle des données et de persistance (sources, exe, installateur)
- Solution d'affichage et d'exploitation des données et des alertes (sources, exe, installateur)
- Les outils de génération des jeux de test
- Les outils d'orchestration éventuels (configuration)

La documentation constituant le plan projet incluant :

- La méthode de réalisation permettant d'obtenir les résultats escomptés
- Le planning prévisionnel de la prestation avec les livrables intermédiaires
- La liste des dépendances
- La liste des contraintes et risques éventuels et leurs impacts
- La liste et les versions des composants entrant dans la réalisation du système
- La liste des licences utilisées et la preuve des droits acquis éventuels au titre du projet
- Et le mode d'emploi opérationnel (configuration, usage) des différents composants

Les prestations devront être réalisées selon l'état de l'art tant sur la qualité, que le sur le choix des outils ou des méthodes d'obtention.

6.2 MISE EN OEUVRE

La MOE devra les prestations suivantes :

- L'intégration de tous les composants constituant la solution dans un ensemble exécutable conforme, cohérent, représentatif et opérationnel.
- La mise en œuvre de la solution de simulation permettant d'alimenter le système et de contrôler ses fonctionnalités.

6.3 LA RECETTE

La procédure de recette, réalisée par la MOE, doit apporter la preuve :

- Que les systèmes mis en place sont parfaitement opérationnels ;
- Que l'ergonomie générale du système est conforme aux besoins décrits ;
- Que les performances annoncées sont conformes ;
- Que la sécurité générale des systèmes vis-à-vis des exigences est respectée.
- Que les différents cas d'erreurs sont traités
- Que la liste des restrictions et limitation résiduelles éventuelles est clairement identifiée et qu'un plan d'action réaliste pour les lever est proposé.

Pour résumer, l'ensemble des livrables décris ci-dessus peuvent être déposé au sein d'un GitHub partagé sur l'adresse électronique suivante :

formateur_nathan.bramli@supdevinci-edu.fr