1 Présentation générale du TP

Ce travail pratique a pour objectif de vous initier à la méthode *Scrum* à travers l'utilisation de l'outil *JIRA*, dans un contexte réaliste de **sécurité informatique et réseau**. Vous serez amené à gérer un projet complet, depuis l'analyse des besoins jusqu'au suivi de l'avancement, en appliquant les principes fondamentaux de Scrum. Le TP est réalisé sous forme de *travail individuel*. Chaque étudiant doit créer son propre compte JIRA (version gratuite) et mettre en place un projet Scrum personnel. Même si vous travaillez seul, vous devrez jouer successivement les rôles de Product Owner, Scrum Master et Développeur, afin de comprendre la logique et les responsabilités associées à chacun de ces rôles. Le contexte du projet est celui d'une PME souhaitant renforcer la sécurité de son système informatique et de son réseau interne. Votre mission consiste à concevoir, organiser et documenter une solution de sécurité couvrant la sécurisation du réseau, la gestion des accès, la surveillance des activités suspectes et la gestion des incidents de sécurité.

— Acceder au https ://www.atlassian.com/software/jira et creer votre compte.

2 Votre rôle dans le projet Scrum

Dans ce TP, vous jouez l'ensemble des rôles Scrum, mais à des moments différents du projet.

2.1 Vous agissez comme Product Owner

— Identifier les besoins en sécurité

— Créer les Epics

— Rédiger les User Stories sous la forme *« En tant que ... je veux ... afin de ... »*

— Organiser le Product Backlog de manière cohérente

2.2 Vous agissez comme Scrum Master

— Créer le projet Scrum sur JIRA

— Planifier les sprints

— Utiliser le Scrum Board

— Suivre régulièrement l'avancement des tâches

2.3 Vous agissez comme Développeur

— Découper les User Stories en tâches

— Analyser les solutions de sécurité proposées

— Mettre à jour l'état des tickets

— Documenter votre travail

3 Product Backlog : User Stories et tâches

Dans cette partie, vous allez créer les extbfUser Stories puis les extbftâches associées directement dans JIRA. Les Epics ne sont pas utilisés dans ce TP afin de simplifier la prise en main de l'outil.

EPIC 1 : Sécurisation du réseau

US1 : En tant qu'administrateur réseau, je veux segmenter le réseau en VLAN afin de réduire la surface d'attaque et de limiter la propagation des menaces internes.

— Analyser l'architecture réseau existante

— Identifier les types d'utilisateurs

— Définir les VLAN nécessaires

— Proposer un schéma de segmentation

— Décrire les règles de communication entre VLAN

US2 : En tant qu'administrateur réseau, je veux configurer un pare-feu afin de contrôler le trafic entrant et sortant et de bloquer les communications non autorisées.

— Identifier les flux autorisés et interdits

— Définir des règles de filtrage

— Tester les règles avec différents scénarios

— Analyser les résultats obtenus

— Documenter la configuration

EPIC 2 : Gestion des accès

US3 : En tant qu'administrateur sécurité, je veux mettre en place une authentification forte afin de renforcer la protection des comptes utilisateurs contre les accès non autorisés.

— Étudier les méthodes d'authentification existantes

— Proposer une solution d'authentification forte

— Décrire le processus d'authentification

— Identifier les risques liés à une authentification simple

— Rédiger une synthèse explicative

US4 : En tant qu'administrateur système, je veux définir des rôles et des permissions afin de garantir que chaque utilisateur n'accède qu'aux ressources strictement nécessaires.

— Identifier les rôles utilisateurs

— Définir les permissions associées

— Construire une matrice rôles/permissions

— Vérifier le respect du principe du moindre privilège

— Documenter la gestion des accès

EPIC 3 : Surveillance et détection

US5 : En tant qu'analyste sécurité, je veux déployer un système de détection d'intrusion afin d'identifier rapidement les comportements suspects sur le réseau.

— Expliquer le fonctionnement d'un IDS

— Choisir un type d'IDS

— Identifier les attaques détectables

— Définir des règles de détection

— Décrire les alertes générées

US6 : En tant qu'analyste sécurité, je veux centraliser les journaux de sécurité afin de faciliter la détection, l'analyse et l'investigation des incidents.

— Identifier les sources de logs

— Proposer une architecture de centralisation

— Définir les informations importantes à surveiller

— Expliquer comment analyser les logs

— Documenter le processus

EPIC 4 : Gestion des incidents

US7 : Définir un plan de réponse aux incidents

— Identifier les types d'incidents possibles

— Définir les étapes de réponse

— Identifier les responsabilités

— Décrire les actions après incident

— Rédiger le plan de réponse

4 Organisation des sprints

— Sprint 1 : Sécurisation du réseau

— Sprint 2 : Gestion des accès

— Sprint 3 : Surveillance et gestion des incidents

5 Utilisation du Scrum Board

— Vous devez utiliser le Scrum Board de JIRA tout au long du projet afin de suivre l'avancement réel de votre travail et d'avoir une vision claire de l'état des User Stories et des tâches.

— Les tâches doivent être déplacées manuellement entre les colonnes *A FAIRE*, *EN COURS* et *TERMINE* en fonction de leur état d'avancement.

— Une User Story est considérée comme terminée uniquement lorsque toutes les tâches qui lui sont associées sont terminées et placées dans la colonne *TERMINE*.

— Le Scrum Board doit refléter une progression logique et continue du travail, et non un déplacement massif des tâches en fin de TP.

6 Travail obligatoire sur JIRA

— Le projet JIRA doit contenir l'ensemble des éléments Scrum, notamment les Epics, les User Stories et les tâches associées, correctement organisées.

— Les sprints doivent être clairement définis et planifiés dans JIRA, avec une répartition cohérente des User Stories selon les objectifs de chaque sprint.

— Le Scrum Board doit être utilisé régulièrement et montrer l'évolution naturelle des tâches au cours du temps.

— Chaque ticket doit contenir des commentaires ou des descriptions permettant de comprendre le travail réalisé et les décisions prises.

— L'historique du projet JIRA doit montrer une progression réaliste et cohérente du projet, reflétant votre implication tout au long du TP.