Travail de Bachelor 2025
Filière ISC
Orientation ISCS

Conception d’un nouveau serious game autour du « Ethical hacking »

Contexte et enjeux

Le jeu pédagogique **“Shana a disparu”**, développé par le pôle Y-Security de la HEIG-VD, a rencontré un grand succès auprès du public en proposant une initiation au ethical hacking grâce à une histoire immersive. Cependant, la majorité des participant·e·s ayant terminé ce scénario, il devient nécessaire de développer un nouveau jeu proposant des défis techniques plus avancés tout en maintenant l’accessibilité aux débutants. Ce projet vise à créer un nouveau scénario sur la plateforme *CyberGame*, **“Blackout dans le Centre Hospitalier Horizon Santé”**, qui plonge les joueur·euse·s dans une situation de crise réelle, tout en leur permettant d’acquérir des compétences pratiques en cybersécurité.

Le scénario “Blackout”

L’objectif principal du projet est de concevoir et de développer un scénario original combinant narration immersive et défis techniques progressifs. Le nouveau scénario plonge le joueur dans une situation de crise inspirée d’incidents réels. Le Centre Hospitalier Horizon Santé subit une attaque par ransomware qui paralyse ses systèmes informatiques et met en danger la vie de patients en salle d’opération. Dans la peau d’un membre de l’équipe de cybersécurité, le joueur doit résoudre sept challenges techniques progressifs pour infiltrer le système des attaquants, supprimer les données sensibles volées des patients et bloquer toute nouvelle tentative d’intrusion. Chaque étape aborde une thématique de la cybersécurité, comme l’OSINT, l’exploitation web, l’exploitation de failles de contrôle d’accès, la cryptographie, le reverse engineering, une attaque XSS ou encore la défense et l’analyse des logs. L’objectif est à la fois pédagogique et pratique : sensibiliser aux menaces numériques tout en transmettant des compétences concrètes.

Implémentation et résultats

L’implémentation s’appuie sur l’architecture existante de la plateforme CyberGame avec un frontend développé en HTML, CSS et JavaScript utilisant le framework Phaser, un backend Node.js avec Express, et des bases de données MongoDB et MySQL orchestrées par Docker. Plusieurs innovations techniques enrichissent l’expérience pédagogique, notamment un IDE Python embarqué fonctionnant avec Pyodide permettant d’exécuter du code directement dans le navigateur, des terminaux SSH interactifs pour accéder à des environnements isolés, et un système de bot Puppeteer automatisé simulant des interactions réalistes pour le challenge XSS. La validation des réponses repose sur un système sécurisé utilisant des hash SHA-3 256 stockés côté serveur. Des tests unitaires réalisés avec Jest ainsi que des tests utilisateurs aux profils variés ont permis d’identifier les points forts et les aspects à améliorer.

Impact et perspectives

Les tests utilisateurs révèlent des résultats positifs adaptés aux différents niveaux. Les profils avancés ont apprécié la diversité des challenges et la cohérence de l’histoire. Les débutants, bien que confrontés à des difficultés sur certains challenges techniques, ont maintenu leur motivation et exprimé une grande satisfaction lors de la résolution des défis. Ce projet démontre le potentiel des serious games comme outil de formation et de sensibilisation en cybersécurité. En proposant un scénario réaliste et engageant, il permet aux joueur·euse·s d’apprendre en expérimentant directement les mécanismes d’attaque et de défense. Le scénario développé constitue une base intéressante pour de futures évolutions et enrichit la plateforme du pôle Y-Security. Ainsi, ce travail pose les bases d’un dispositif durable, évolutif et adapté à un public varié.

Auteure: Camille Koestli
Prof. responsable: Sylvain Pasini
Sujet proposé par: Haute-Ecole d'Ingénerie et de Gestion Vaud