

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, beaucoup de personnes l'ont déjà terminé, il devient nécessaire de développer un nouveau jeu proposant des défis techniques plus avancés tout en maintenant l'accessibilité aux débutants mais aussi aux joueur·euse·s plus expérimenté·e·s.

Le scénario “Intrusion”

L'objectif principal du projet est de concevoir et de développer un scénario original combinant narration immersive et défis techniques progressifs. L'histoire de passe dans le Centre Hospitalier Horizon Santé qui subit une attaque par ransomware. Les attaquants menacent de publier les données sensibles des patients. 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 volées des patients et bloquer les futures tentatives. 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, orchestrée avec Docker Compose. Les services incluent un frontend développé en HTML, CSS et JavaScript, un backend Node.js avec Express, et des bases de données MongoDB et MySQL. Pour enrichir

l'expérience pédagogique, des terminaux SSH interactifs pour accéder à des environnements isolés, un IDE Python embarqué y est intégré permettant d'exécuter du code directement dans le navigateur. Un système de bot Puppeteer automatisé faillible aux attaques XSS.

Impact et perspectives

Les tests utilisateurs aux profils variés ont permis d'identifier les points forts et les aspects à améliorer. Ils 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 enrichit la plateforme du pôle Y-Security.

