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

Extension du Jeu « Shana a disparu »

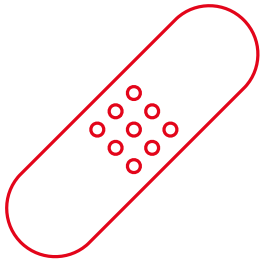
Camille Koestli

Sommaire

Présentation du projet

- Augmentation de l'intérêt sur la cybersécurité
- Potentiel des serious games pour rendre l'apprentissage ludique
- «Shana a disparu» a eu un grand succès mais trop de personnes l'ont complété et terminé
- Objectif : créer un nouveau serious game avec une approche narrative tout en proposant des challenges techniques

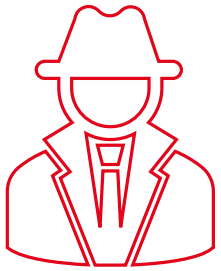
Choix du scénario



Scénario réaliste

Black out dans le Centre Hospitalier Horizon Santé

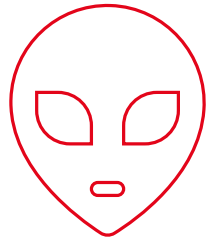
Randsomware dans un milieu hospitalier



Scénario aventure

Opération « CipherFox » Infiltration

Vol de données dans une entreprise



Scénario science-fiction

Fuite de l'Acheron

S'échapper d'un vaisseau spatial

Résumé du scénario

- L'hôpital subit une attaque par randsomware
- Black out des systèmes informatiques et des services critiques
- Vol des données sensibles concernant les patients
- Le joueur incarne un membre de l'équipe de sécurité
- Objectif : Résoudre les défis pour empêcher les attaquants de poursuivre leurs attaques

Challenge 1 : Mail Contagieux

- Le point d'entrer des attaquants est un email de phishing reçu
- Le joueur analyser l'email dans le but de retrouver le faux nom de domaine qu'ils ont utilisé
- Compétences travaillées : OSINT et forensic
- Ce challenge a pour objectif de sensibiliser aux signes d'un courriel d'hameçonnage

Challenge 2 : Portail VPN Fantôme

- Une fois le faux domaine identifié, le joueur découvre qu'il héberge un faux portail vpn pour exfiltrer les données
- Le joueur doit donc réussir à contourner le formulaire de connexion équipé d'un WAF
- Compétences travaillées : injection SQL
- Ce challenge a pour objectif de sensibiliser aux failles d'injection et montre qu'une protection insuffisante peut être contournée facilement

Challenge 3 : Archives compromises

- Dans le portail malveillant, le joueur voit une section «Document» avec un bouton pour télécharger le rapport du jour
- Les attaquants utilisent ce portail pour héberger les informations sensibles
- Le joueur donc faire une path traversal pour retrouver où sont stocker les dossiers concernant les patients
- Compétences travaillées : path traversal et analyse HTML
- Ce challenge sensibilise aux failles de type path traversal qui permet d'accéder à des fichiers sensibles

Challenge 4 : Clé cachée dans les commentaires

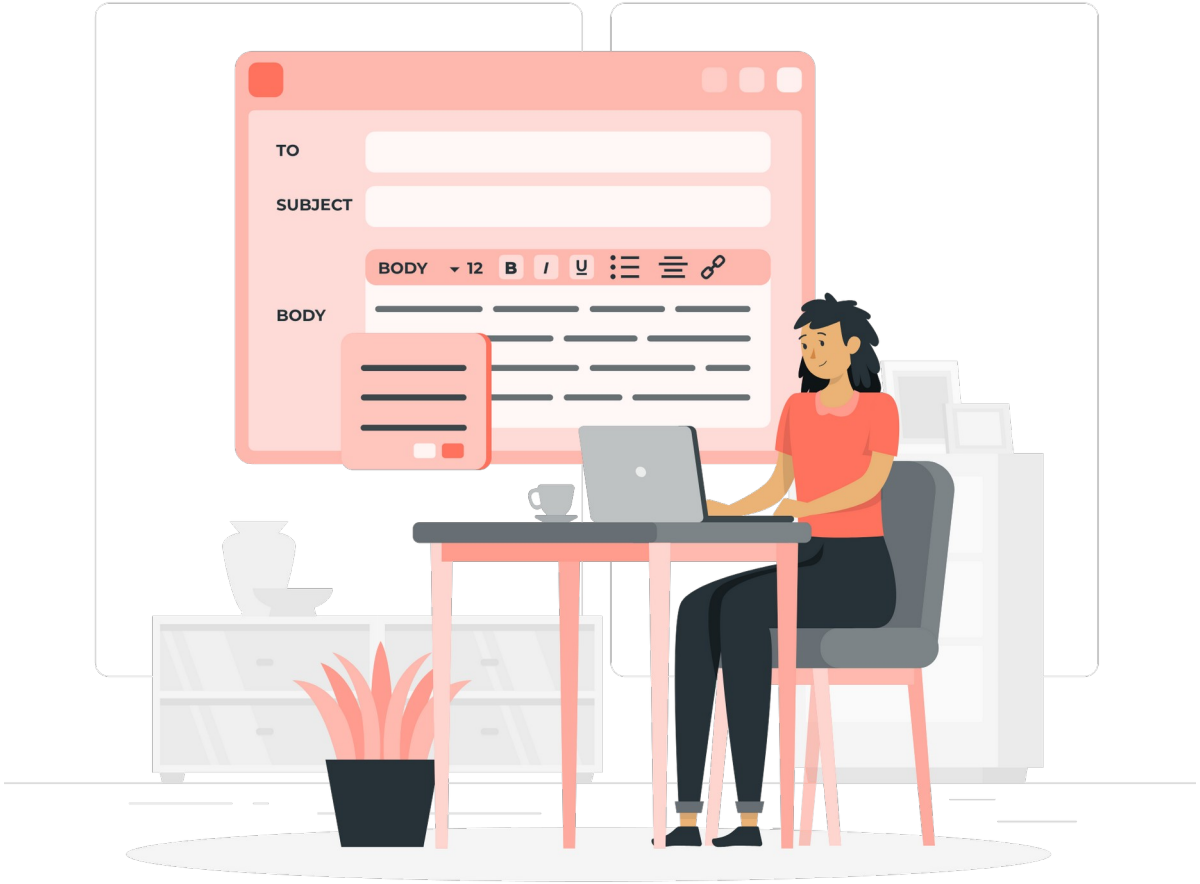
- Une fois les dossiers sensibles découverts, le joueur remarque qu'il y a un fichier zip mais il est chiffré
- Le joueur devra donc faire une investigation des métadonnées pour découvrir un commentaire contenant le SHA-1 qui chiffre le dossier
- Compétences travaillées : analyse des métadonnées et cryptographie
- Ce challenge montre l'importance de vérifier ces métadonnées mais aussi l'importance de la cryptographie

Challenge 5 : Script d'injection

- Une fois le zip décompressé, le joueur voit qu'il y a un script PowerShell mais il est brouillé qui sert à établir la connexion vers un serveur
- Il va décoder le fichier pour retrouver l'URL du serveur
- Compétences travaillées : dé-obfuscation
- Ce challenge montre comment les attaquants camouflent leurs logiciels et comment les analyser

Challenge 6 : Chat KO

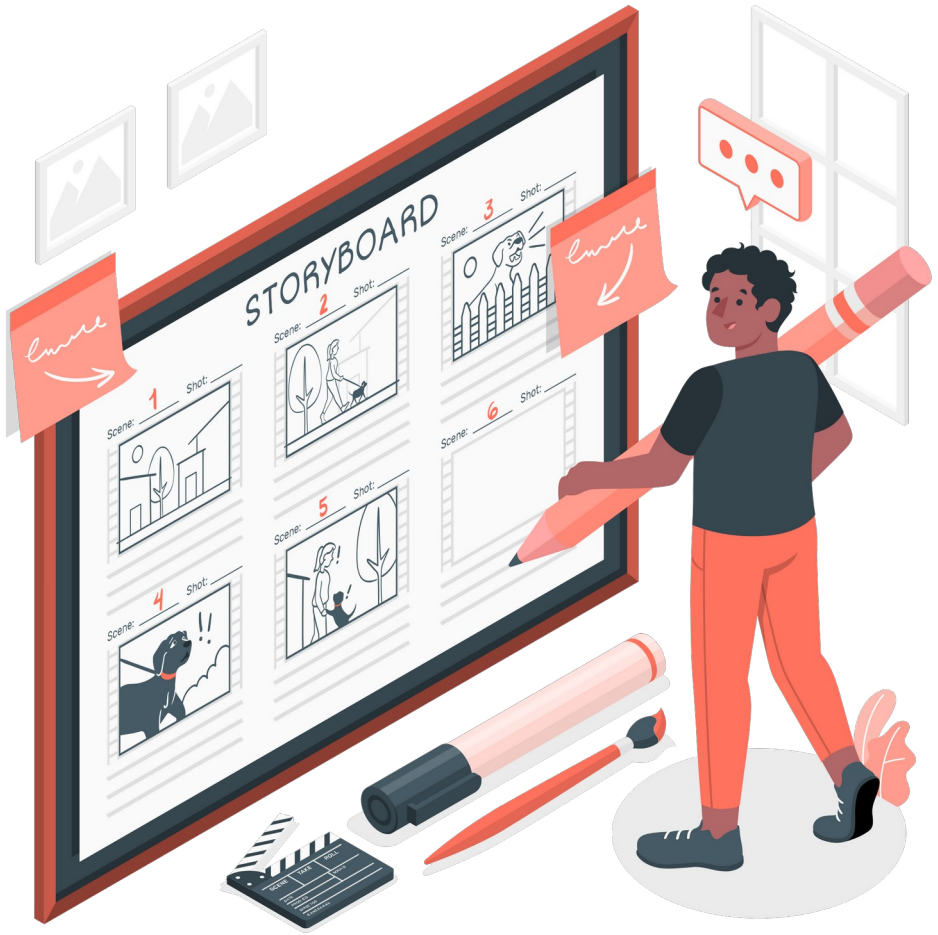
- Une fois dans le serveur, une page affiche un forum interne
- Le joueur réaliser une attaque XSS pour mettre le serveur hors service
- Compétences travaillées : Attaque XSS
- Ce challenge montre la gravité d'une entrée utilisateur non échappée



Challenge 7 : Blocage ciblé

- Une fois leur serveur HS, le joueur doit identifier l'adresse IP de l'attaquant pour la bloquer.
- Le joueur va se connecter sur le VPN de l'hôpital afin d'ajouter l'IP à la liste noire du pare-feu
- Compétences travaillées : défense et journalisation de log
- Ce challenge montre l'importance de surveiller les logs et de gérer les adresses IP suspects

Conclusion



- Ce scénario réaliste s'inspire de situation réaliste avec des attaques par randsomware
- Ce scénario mélange narration et apprentissage technique
- Approche progressive et immersive
- Permet d'aborder plusieurs aspects de la cybersécurité

HE IG VD

HAUTE ÉCOLE D'INGÉNIERIE ET DE GESTION DU CANTON DE VAUD