Cahier des charges

Projet FIC24H

Version du document : version 1.2

Auteur : Jennifer,Adrien,Sharon,Clément

Date : 11/10/2018

Historique des modifications

Date	Version	Description	Auteur
07/10/2018	1.0	Besoins initiaux et retour réunion	Groupe entier
11/10/2018	1.2	Mise en forme / Ajout des parties réalisées	Adrien Lasalle

SOMMAIRE

1 - Introduction

Le but de ce document est de recueillir, d'analyser et de définir les besoins et les caractéristiques des épreuves Forensics pour le Forum International de Cybersécurité et les 24h des IUT. Il met l'accent sur les capacités requises par les intervenants et les utilisateurs cibles, et les raisons qui conduisent à ces besoins.

Dans ce cahier des charges, vous trouverez toutes les informations nécessaires à la compréhension du projet. Ce document permet à l'équipe de rendre compte du projet au tuteur et à travailler de manière logique afin que le projet soit en concordance avec les exigences que cela entraîne tel que les restrictions juridiques, le public visé...

On retrouvera dans ce document toutes les parties présentes dans ce sommaire tel que les parties prenantes, les utilisateurs, les différents besoins...

2 - Description du problème

La première partie du projet qui nous a été demandé consiste à créer des épreuves ciblées Forensics dans le cadre du Forum International de Cybersécurité de divers niveaux visant des professionnels pendant une durée de 4 heures.

Contexte: En 2007, la région la Gendarmerie s'allie à la région Haut de france, dans un but financier, afin de créer le Forum International de Cybersécurité (FIC). Nous voilà maintenant en 2018 et la Licence CDAISI (Cyber Défense, Anti-Intrusion des Systèmes d'Informations) participe depuis quelques années à la création des épreuves de Forensics du selon. 15 épreuves nous sont alors demandés pour l'édition 2019 qui se déroulera en le 23 Janvier 2019.

Après avoir réalisé l'ampleur du projet, nous avons dû mettre en place une stratégie visant à répondre aux objectifs des besoins du projet. La deadline étant plus courte que pour les autres projets et n'ayant pas commencé les cours de Forensic, nous avons opté par commencé à s'autoformer sur le sujet.

Dans un premier temps, nous allons nous documenter sur le Forensics. En effet, n'ayant aucune connaissance en la matière, nous ne savons pas en quoi cela consiste et il nous faut donc une première base.

Puis, des épreuves existent sur les sites comme Root Me ou encore Hack This, ce qui nous permettra de résoudre des épreuves et en comprendre le fonctionnement.

Ensuite, Nous nous baserons sur les épreuves des années précédentes et sur les connaissances de nos tuteurs afin de nous aiguiller sur la marche à suivre grâce notamment à la méthode AGILE et les réunions qui seront mit en place pour le projet.

Enfin, nous compléterons les épreuves grâce au cours que nous effectuerons au sein de notre formation et qui vont arriver prochainement.

La cybersécurité est devenu un enjeu important dans notre monde actuel. Elle vise à faire face aux cyber attaques dont nous faisons face. Le FIC a vu le jour avec de débattre des enjeux stratégiques en matière de Cybersécurité et de Cyber Défense.

Les étudiants CDAISI sont l'avenir du métier "Ethical Hacking" et donc ils sont amenés à lutter contre des Cyber Attaques, c'est pourquoi ils doivent s'intégrer au monde professionnel qui sera le leur et commencer à prendre connaissance des enjeux.

Dans la seconde partie du projet, on devra créer des épreuves de sécurité diverses pour des étudiants ayant des notions de sécurité. Les épreuves dureront 8h en ce qui concerne la sécurité. Les épreuves seront au nombre de 20.

Contexte: Les 24h IUT est composé de 3 épreuves informatiques d'une durée de 8h chacune. Elle se décompose en: Développement, Sécurité et robotique. Elle vise à mettre en relation des étudiants du domaine de l'informatique de plusieurs IUT. Ce challenge était organisé par au sein de IUT de maubeuge mais, désormais, le challenge bouge chaque année dans toute la France.

Ces épreuves seront des épreuves de niveaux plus faciles que les précédentes car elle ne visent pas un public déjà expérimenté. Pour cela, nous allons décomposer les épreuves en divers sujet de cybersécurité: Forensics, Faille web, Basic+, SQLi,...

Nous débutons et donc nous allons nous inspirer des épreuves déjà présentent afin d'en créer de nouvelle. Par ailleurs, nous pouvons reprendre les épreuves faciles du Forensics et/ou les adapter.

Ces épreuves se passeront après le FIC et donc une fois ces dernières terminées, on devra enchaîner sur ces épreuves afin d'être dans les temps pour le challenge.

Ces épreuves seront aussi managées via la méthode AGILE afin de respecter au mieux les besoins de notre tuteur.

Le challenge vise, via un challenge, à regrouper des étudiants avec la même passion pour l'informatique dans une entente conviviale et avec des épreuves qui leur correspondent.

3 - Parties Prenantes

Maître d'ouvrage

Responsable de la définition des objectifs du projet et de la décision d'investir dans le projet -> Tuteur (M.Hennecart)

Maître d'oeuvre

Chargée par le maître d'œuvre de la réalisation du projet ->Chef de projet (Jennifer Bonillo)

Equipe projet

L'équipe est composées de 4 personnes

- 1 RSSI - Delvalle Clement
- 1 Expert Technique - Panthier Sharon-Joyce
- 1 Chef de projet - Bonillo Jennifer
- 1 RAQ (Responsable assurance qualité) - Lasalle Adrien

Comité de pilotage

Tuteur (M.Hennecart)

Client

Forum International de Cyber sécurité

Fournisseurs

Faculté de Maubeuge

3.1 - Utilisateurs

Les utilisateurs du projets concerne tous les participants inscrit au Forum International de la Cybersécurité

- Utilisateurs finaux du système
- Validation de flag pour passer à l'étape suivante

4 - Besoins des utilisateurs principaux et des parties prenantes

Depuis plusieurs années, les challenges forensics commencent à prendre de l'ampleur et ceux grâce à plusieurs raisons.

Premièrement, la sécurité informatique prend une place importante dans nos sociétés. En effet, de plus en plus de fonctionnalités et d'outils sortent informatiquement et chaque type de donnée, que ce soit des données personnelles ou encore des codes d'application, se doivent d'être sécurisé pour faire face à une éventuelle attaque informatique.

Les challenges Forensics permettent à des passionnés, que ce soient des professionnels ou des particuliers de n'importe quels niveaux, de tester leurs compétences sous forme de concours en équipes.

Les équipes devront s'affronter pour récupérer des drapeaux cachés sous forme de mot de passe, dans des dossiers, fichiers, etc. Chaque mot de passe permet d'accéder au challenge suivant en le saisissant sur une plateforme en ligne. Cette plateforme permet aux équipes d'accéder aux challenges et d'avoir un petit aperçu de leur classement.

A la fin du challenge, l'équipe qui aura le plus de points, c'est à dire, trouvés le plus de drapeaux, remporte le challenge.

Les recommandations suivantes sont valables pour les challenges FIC et 24H IUT.

5 - Besoin fonctionnels

Notre objectif est de réaliser 15 épreuves forensics pour les participants du challenge FIC de l'année 2019 ainsi que pour le challenge 24H UIT. Pour bien prendre en comptes les fonctions que nous devons réaliser dans ce projet, une étude des besoins fonctionnels a été réalisée.

Auto-formation forensic:

- **Object:** former les membres du projet aux méthodes forensics
- **Description:** L'équipe projet doit s'auto-former sur les méthodes forensics par le biais de sites de challenges ou de documentation technique.
- **Niveau de priorité:** Haute

Créer des challenges forensic:

- **Objectif:** Mettre en pratique nos connaissance en forensic pour réaliser des challenges de tous les niveaux. Facile, moyen et difficile.
- **Description:** Le chef de projet va attribuer des challenges à réaliser aux membres du projet (seuls ou à plusieurs).
- **Niveau de priorité:** Haute

Effectuer Des tests sur les challenges réalisés:

- **Objectif:** Mettre en pratique nos connaissances et tester les challenges
- **Description:**L'équipe projet devra tester chaque challenges afin de trouver des failles ou améliorations pour les challenges
- **Niveau de priorité:** Haute

6 - Restrictions

Restriction juridique:

- Tous les droits sont la propriété de l'Université de Valenciennes

Restrictions temporelles:

- Les challenges pour le Forum International CyberSécurité doivent être livrés au client avant le début du challenge FIC. Pareil pour les challenges du 24H IUT.
- Chaque réunions avec le client fera l'objet d'un compte rendu pour garder une trace du projet afin de comparer le prévu au réalisé et aider à la communication de l'avancée du projet.

Restriction de conceptions:

- Le projet sera mis en place suivant les méthodes de conceptions agiles
- Chaque challenges réalisé par les membres de l'équipe devra être mis en pratique et testé.

Restrictions matérielles

- Le matériel disponible pour la réalisation du projet sera le matérial des membres de l'équipe projet ainsi que le matériels mis à la disposition des étudiants par l'université.

Restrictions budgétaires:

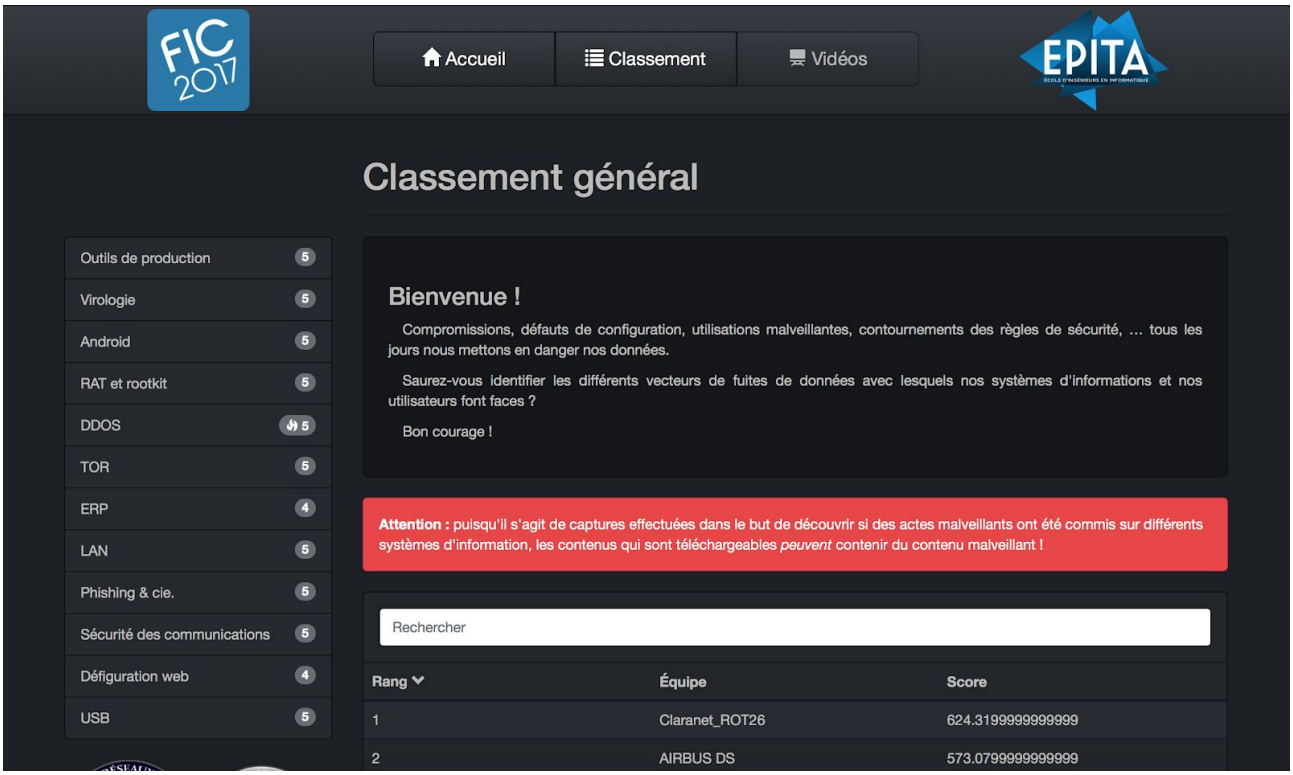
- Le projet doit respecter le budget mis en place pour la réalisation de celui-ci

7 - Benchmarking

Challenge du FIC EPITA :

Points forts :

- plusieurs types de challenge
- plateforme du réseau qui gère l'avancée des équipes
- bonne convivialité durant le challenge



Points faible :

- 4h d'épreuves (on aimerait plus)

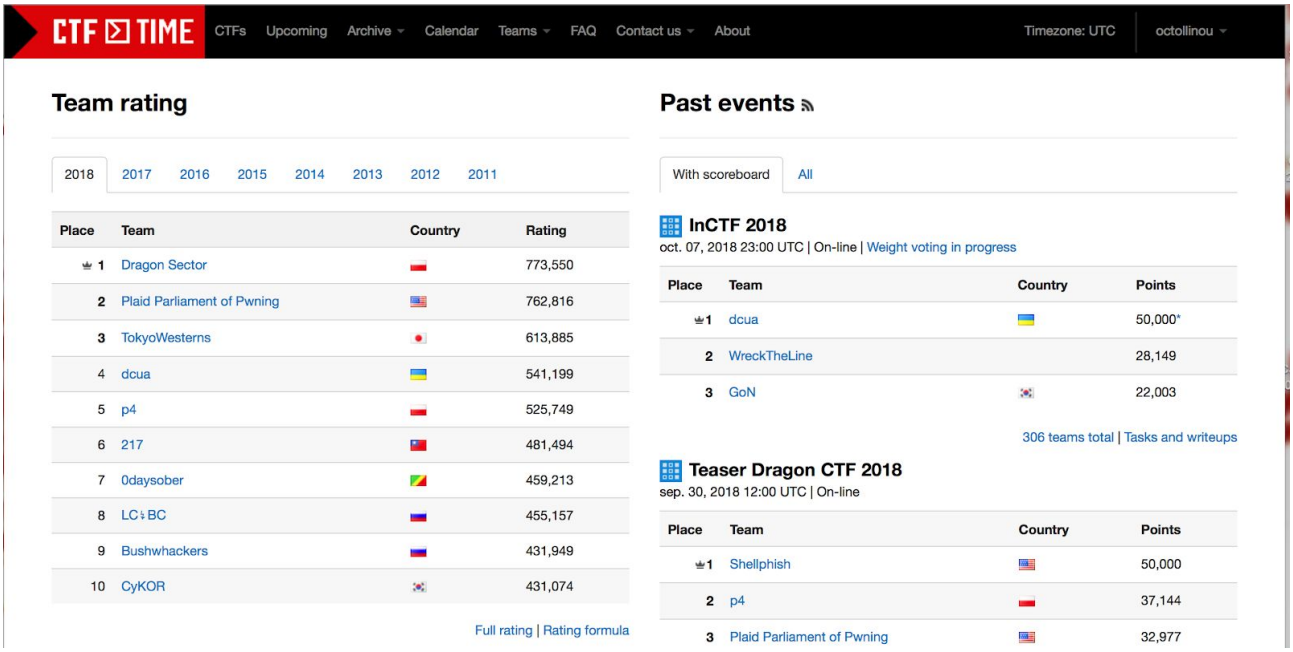
L'école EPITA mettra en place des challenges durant le challenge du FIC

CTFtime, capture de drapeaux :

Sur ctftime.org :

Points fort :

- accessible depuis chez soi
- plusieurs épreuves chaque week-end organisé par des équipes ou des boîtes informatiques
- plusieurs niveaux d'épreuves
- pas seulement du forensic
- aide à comprendre et apprendre



Points faible :

- les ctf ne sont pas toujours pour les débutants qui voudraient commencer.
- comme les captures sont internationales les horaires ne sont pas toujours les meilleurs

8 - Glossaire

- **CTF:** Capture The Flag (capture de drapeaux)
- **IUT:** Institut Universitaire de Technologies
- **FIC :** Forum International CyberSécurité

9 - Annexes

Compte rendu réunion 1

Compte rendu de réunion

Projet : Challenge FIC

Date de la rencontre : 25 Septembre 2018

Personnes présentes :

Hennecar Jérome - Tuteur projet

Crocfer Robert - Intervenant sur le projet

Jennifer Bonillo - Chef de projet - Technicien

Lasalle Adrien – Responsable assurance qualité - Technicien

Sharon-Joyce Panthier – Expert technique – Technicien

Clément Delvallée – Responsable sécurité des système d'information - Technicien

1 Objectifs de la réunion

Prise de contacte avec le tuteur pour parler du projet, des épreuves et du futur cahier des charges.

3 pôles importants pour ce projet

- 15 épreuves pour le FIC (épreuves de Forensic) le plus important)
- Plateforme avec validation en temps et affichage en temps réel de l'avancée de chaque équipe
- 20 épreuves pour les 24H des IUT

2 Sujets abordés

2.1 Sujet 1 : Challenge FIC

Forensic : recherche des traces de preuves sans modification de données.

Possibilité de mettre à jour la plateforme existante

CTF système de validation et EBP est un registre (faire des recherches dessus)

Si besoin d'aide :
- Robert Crocfer : faille physique + prise d'empreinte
- Franck Ebel : buffer-overflow, crack me (ce n'est pas du forensic), python, faille application.

Faire un retour des avis des challengers pour le FIC.

Idée :
- Tenir un faux Facebook pour faire une recherche d'information à partir de ce profil.
- Métadonnées d'une photo + Base de données
- Cacher des éléments de pistes dans une photo, un fichier audio ou autres.

2.2 Sujet 2 : 24h IUT

8h d'épreuves de sécurité

Faire une vingtaine d'épreuves

Faire des épreuves faciles et les rendre de plus en plus compliquées

Plateforme à gérer.

Les épreuves ne sont pas que du Forensic.

3 Prochaine réunion

Présentation du cahier des charges

4 Commentaires et appréciations générales

Se renseigner sur le forensic et élaborer des épreuves.