AMUSE : un escape game pour la sécurité numérique

Florent Bruguier, Loïc Dalmasso, Pascal Benoit, Béatrice Pradarelli

AMUSE :
UN ESCAPE GAME POUR LA SÉCURITÉ NUMÉRIQUE

QUI ?

Programme IDEFI-FINMINA
Pôle CNFM de Montpellier - LIRMM
161 rue Ada - 34095 Montpellier Cedex 5

Porteurs :
Florent Bruguier, Loic Dalmasso, Pascal Benoit et Béatrice Pradarelli

QUOI ?

- ❑ Learning Lab / fab Lab
- ❑ Simulation
- ❑ Enseignement à distance
- ✔ Pédagogie innovante
- ❑ Orientation actives
- ❑ Evaluation interactives/ autoévaluation
- ✔ Serious Game
- ❑ Formation

POURQUOI ?

Un escape game de 7 à 99 ans pour découvrir les concepts de la cryptographie ! Vous êtes en quête de défi ? Arriverez-vous à ouvrir le coffre-fort en trouvant son code secret en moins de 5 minutes ? Vous n'aurez à votre disposition qu'une mallette renfermant des indices. En appliquant les concepts de la cryptographie, ces indices vous permettront de résoudre les énigmes qui vous conduiront au code secret. Concentration, mémorisation, logique et réactivité vous seront nécessaires pour défier le temps et battre le record.

L'objectif de ce jeu sérieux est d'introduire tous les concepts nécessaires à l'apprentissage de la sécurité numérique. Il permet à travers le jeu de sensibiliser les étudiants aux notions nécessaires à appréhender le monde numérique de demain et sa sécurité. Ce jeu est simple et facile d'accès et permet de renforcer l'intérêt des étudiants pour l'enseignement dispensé. Concentration, mémorisation, logique et réactivité vous seront nécessaires pour défier le temps et battre le record.

Ce « Serious Game » est au cœur d'un processus pédagogique qui comprend plusieurs étapes :

- Bilan des connaissances en cryptographie pour les stagiaires (collégiens, lycéens, étudiants, doctorant, personnel académique et privé) en début de séance
- Découverte en groupe des principaux concepts et méthodes de cryptage de l'information en lisant un poster et en répondant à un questionnaire
- Mise en pratique des acquis théoriques avec le « Serious Game »
- Bilan des compétences en cryptographie en fin de séance.

POUR QUI ?

Cet « Escape Game » s'adresse à tous les publics depuis la classe de 3ème au doctorat en passant par la formation continue. Au cours des deux dernières années, ce sont au total 974 personnes qui ont bénéficié de cette sensibilisation ou d'une formation à la Sécurité numérique.

COMMENT ?

L'objectif étant de proposer un jeu permettant d'appréhender des compétences nécessaires à la compréhension de la sécurité du monde numérique, il est d'abord nécessaire de les identifier :

1) Sensibiliser en premier lieu les étudiants à l'ingénierie sociale. Il s'agit de réaliser une manipulation psychologique afin de réaliser une escroquerie.
2) Ensuite, introduire le concept d'attaque par force brute. Une attaque par force brute consiste à tester la totalité des combinaisons d'un algorithme de chiffrement pour retrouver la clé secrète utilisée.
3) Présenter les techniques de base du chiffrement/déchiffrement. Le chiffrement par substitution est une technique de chiffrement. Il consiste à remplacer dans un message une lettre (ou un groupement de bits) par une autre définie à l'avance. Par exemple, dans le chiffre de César, un A sera remplacé par un D. Le chiffrement par transposition repose sur l'inversion de la position de lettres dans un message. Ces deux techniques sont associées dans la plupart des algorithmes de chiffrement modernes.
4) Une autre manière de mettre en œuvre la substitution est l'utilisation de boite de substitution. Celle-ci est également abordée. En fonction du niveau des étudiants, d'autres compétences/connaissances sont mises en jeu.
5) Les étudiants n'ayant que peu de connaissances du monde numérique et de l'électronique sont confrontés aux principes de fonctionnement d'un circuit électrique ainsi qu'au principe du codage binaire.
6) Les étudiants plus expérimentés ont l'occasion de goûter aux joies du pentesting ou « test de pénétration ». Le principe étant de venir mesurer des tensions directement sur un circuit numérique afin d'en extraire de l'information.

COMBIEN ?

Ce projet a un coût total de 20 206 € répartis en deux postes :

- Yannick Rolland, ingénieur plateforme SECNUM, a passé l'équivalent de 6 homme-mois à travailler sur ce projet pour un coût de 16 206 €
- La mise en place a nécessité un investissement dans divers objets et supports pour un coût d'environ 4 000 € (mallettes, cartes électroniques, lampes UV, coffre-fort…).

POUR ALLER PLUS LOIN

Les mallettes peuvent être utilisées sur plusieurs postes d'apprentissage en parallèle. Plus de 95% des formés ont acquis les notions enseignées en fin de formation. De plus, il est possible de former un nombre important de personnes et ce, sur plusieurs sites en France. Entre 2017 et 2019, ce sont plus de 970 personnes qui ont été formées. Le dispositif est en outre facilement transposable et l'investissement reste très raisonnable.

La cyber sécurité constitue un enjeu sociétal majeur. Ainsi, le 4 juin 2019, lors de la 5ème édition des Rencontres Cybersécurité en Occitanie, l'escape Game a gagné le prix « Coup de cœur » du jury.

Pour en savoir plus : Secnum@cnfm.fr