Hack'lantique : première expérience de CTF pédagogique

Jules Boudaud, Camille Gilbert, Titouan Laurain, Coralie Métayer, Jonathan Sarrazin, Fabien Autrel, Ahmed Bouabdallah, Guillaume Doyen, Renzo Efrain Navas

Hack'lantique : première expérience de CTF pédagogique

Jules Boudaud, Camille Gilbert, Titouan Laurain, Coralie Métayer, Jonathan Sarrazin
3ème année d'ingéniorat - TAF Cyber - IMT Atlantique - Campus de Rennes - France
equipe-ctf@imt-atlantique.fr

Fabien Autrel, Ahmed Bouabdallah, Guillaume Doyen, Renzo Navas
Département SRCD - IMT Atlantique - Campus de Rennes - France
responsables-taf-cyber@imt-atlantique.fr

***Résumé*—Ce document présente un partage d'expérience concernant la création ex-nihilo d'un événement de type *Capture The Flag* (CTF) par un groupe de cinq étudiantes et étudiants en dernière année de formation d'ingénieur à IMT Atlantique au sein de la spécialité sécurité. Ce projet contribue à l'évaluation formative des étudiants impliqués dans le projet. L'évènement associé qui en est à sa première édition, s'est limité aux étudiants d'IMT Atlantique, mais a cependant suscité un intérêt notable auprès des étudiants n'ayant aucun acquis en sécurité. Il offre par la même occasion aux enseignants impliqués dans l'encadrement du projet, l'opportunité d'amorcer une réflexion concernant le potentiel pédagogique de ce type d'évènement dans le cadre des cursus en sécurité délivrés dans l'enseignement supérieur.**

***Index Terms*—CTF, sécurité, pédagogie alternative**

I. Introduction

La sécurité informatique, du fait de sa transversalité structurelle, est un domaine vaste qu'il est difficile de couvrir de manière exhaustive. La problématique est d'intérêt autant pour l'expert et le chercheur que pour l'impétrant, pour l'enseignant et le formateur que pour l'étudiant. La tentation d'en acquérir des savoirs effectifs en butinant de façon ludique et au gré de ses caprices, s'impose naturellement comme une démarche alternative intéressante et gratifiante. En échappant à la pression psychologique des études universitaires traditionnelles qui peuvent être perçues sous un angle fastidieux et contraignant, les compétitions du type *Capture The Flag* (CTF) sont des moments privilégiés durant lesquels il est possible de découvrir et expérimenter de nouvelles techniques issues du hacking dans une ambiance joyeuse, studieuse et désintéressée. Le CTF Hack'lantique, créé par un groupe d'étudiantes et d'étudiants passionnés, dynamiques et entreprenants, est l'opportunité de se doter à demeure d'un tel évènement. En plus de constituer à l'échelle d'IMT Atlantique, un moment conjuguant des qualités souvent considérées comme antinomiques telles que "festif" et "studieux", il permet de se doter d'un objet d'étude original susceptible d'offrir un nouveau champ d'expérimentations pédagogiques.

Si la diffusion massive des CTFs accompagnée de leur démocratisation, remonte au début de la décennie précédente [1], ils ont véritablement reçu leurs lettres de noblesse à DEFCON [2], [3] évènement majeur qui a très tôt et de façon régulière, accompagné les grandes conférences académiques sur la sécurité informatique durant les années 90. Avec le recul [4], on distingue principalement trois types de CTFs. En *mode compétition*, le CTF est centré sur le score atteint et le temps nécessaire à la résolution de challenges techniques couvrant les domaines habituels de la sécurité (réseau, cryptographie, web, rétro-ingénierie, ...). Le *mode attaque et défense* consiste dans un contexte scénaristique imaginaire mais souvent ancré dans l'actualité courante, à attaquer les services de ses rivaux pour marquer des points tout en se défendant et en réparant ses propres vulnérabilités pour éviter d'en perdre. Finalement certains CTFs dits en *mode hybride* combinent les deux modes précédents.

La multiplicté des CTFs a acquis une telle ampleur que plusieurs sites ciblent leur recensement selon des spécialisations variées [5]–[10]. Initialement réservé à des experts chevronnés, les CTFs sont progressivement apparus comme des outils remarquablement souples, versatiles et parfaitement adaptés à l'exploration des arcanes de la sécurité numérique sous les angles complémentaires de l'attaque et de la défense. En étudiant par exemple le comportement des pratiquants, certaines recherches s'efforcent de sonder en creux le spectre des comportements possibles des attaquants pour mieux les anticiper et s'en prémunir [11], [12]. La potentiel pédagogique des CTFs s'est aussi rapidement révélé notamment dans l'acquisition rapide d'expertises sophistiquées [13]–[15], la remotivation de l'apprentissage de la sécurité dans un contexte de perte de niveau [16] ou la définition de modalités d'évaluation fine et au chausse-pied pour des MOOCs en sécurité [4]. La valeur formative des CTFs pourrait aussi se lire de façon empirique au travers des CVs des personnes à la recherche d'un emploi dans le secteur de la sécurité informatique. Il y est en effet, de plus en plus souvent mentionné la participation à des CTFs disposant d'une bonne notoriété.

Au niveau national, l'ANSSI a rapidement pris sa part en offrant une approche méthodologique solide [17]. Il existe aussi nombre de CTFs organisés par des établissements d'enseignement supérieur, dont certains ont acquis une renommée notable (ENSIBS, ESNA, Telecom Nancy, ...). Hors de ce cadre nous pouvons également citer le Breizh'CTF à l'initiative de Bretagne Développement Innovation et la team Hexpresso. Certaines entreprises ont également leurs propres challenges,

comme Sopra Steria, Wavestone ou Orange. Parfois, ces CTFs prennent la forme d'événements internes. Enfin le site ROOT ME [18] est souvent considéré comme la référence dans le milieu étudiant.

Ce document comporte les parties suivantes. La section II présente les principes fondateurs du CTF Hack'lantique. La section III rend compte et partage l'expérience acquise par cette première édition. La section IV passe en revue les éléments techniques de mise en oeuvre. Pour terminer, la section V fournit quelques éléments de reflexion prospectifs sur ce projet, au stade où il en est actuellement.

II. Le CTF Hack'lantique

Le cahier des charges du CTF Hack'lantique, tel qu'il émerge a posteriori, accorde une priorité importante à l'initiation ludique à la sécurité informatique [19]. Il n'exige du futur participant aucun pré-requis conceptuel ni pratique, tout en supposant cependant comme disposition initiale, une solide dose d'intérêt, de curiosité, d'ouverture et d'imagination [20]. L'enjeu étant de permettre au participant dans une *posture intégralement active*, d'acquérir grâce à l'expérimentation induite par la réflexion et la résolution des différents challenges, une vision concrète et étendue de la sécurité numérique susceptible d'éveiller son intérêt intellectuel et son appétence pour des approfondissements plus classiques. L'articulation avec les enseignements spécialisés de sécurité délivrés à IMT Atlantique apparaît en filigrane des différents challenges et en constituent implicitement le premier horizon.

Le CTF Hack'lantique dont cette année sera la première édition se conforme au schéma habituel de ce type d'évènement : compétition en équipes, classement et récompenses, organisation et gestion du déroulé efficace et détendu. Une fois un challenge réalisé, c'est-à-dire que le drapeau (preuve de résolution prenant la forme d'une chaîne de caractères) est trouvé, le participant rentre celle-ci dans un espace dédié, ce qui lui permet de gagner des points. L'équipe ayant accumulé le plus de points à la fin du temps imparti remporte le CTF.

Une attention particulière a été accordée par l'équipe organisatrice de ce CTF, à la nécessité de faciliter la reprise et la poursuite l'année suivante par un autre groupe d'étudiants. Cette qualité de reproductibilité du CTF s'est déclinée sous un angle organisationnel et sous un angle technique. Il s'agit dans les deux cas de préserver l'expérience acquise durant la préparation de cette première édition et la transmettre aux générations suivantes, pour garantir aux futures occurrences de l'événement une qualité au moins identique à la première édition. Cela permettra aussi d'ouvrir plus simplement la voie aux innovations que pourraient apporter les futures équipes.

À l'issue de cette première édition de Hack'lantique, une réflexion sera initiée pour identifier et analyser les différentes dimensions pédagogiques des CTFs, leurs possibilités et leurs limites ainsi que leur valorisation potentielle dans les cursus notamment en les utilisant comme modalité alternative d'évaluation. Le premier risque clairement identifié concerne l'étiolement ou la perte de la dimension ludique sur laquelle il conviendra de rester mobilisé et attentif pour garantir sa préservation.

III. Organisation du projet

La méthodologie Agile Kanban a été suivie comme méthode de getion de projet. Le projet dans son ensemble est divisé en Epics, c'est-à-dire des tâches majeures qui sont subdivisées en sous-tâches. Cinq Epics ont été identifiés : Infrastructure, Challenges, Communication, Logistique, Gestion de projet.

L'équipe organisatrice étant composée de cinq étudiantes et étudiants, chacun s'est vu attribuer une Epic principale dans laquelle il est référent et décisionnaire et une Epic secondaire, pour maximiser le temps de travail. Cela permet à chaque acteur de superviser un sujet majeur, mais également d'avoir à la fois une vision globale du projet, et par ailleurs, de monter en compétence sur tous les aspects du projet.

Une première étude préliminaire a permis de déterminer le cadre du projet : définition du besoin et formalisation des premières tâches pour commencer leur planification. Un premier planning prévisionnel a ainsi été mis en place dans lequel les jalons essentiels du projet ont été positionnés permettant d'avoir quelques dates butoirs pour les tâches majeures et ainsi de respecter les grandes étapes du planning imposé.

A. Rétro-planning

Pour construire le projet autour des jalons, il a été nécessaire de définir au plus tôt la date et le lieu de l'événement. Le CTF Hack'lantique se tiendra le 3 mars 2022 de 14h à 20h dans les locaux Rennais d'IMT Atlantique. Cette première édition de Hack'lantique est organisée en présentiel sur le campus de Rennes pour deux raisons : faciliter la gestion de l'événement en étant sur place (accompagnement des participants, remédiation en cas de dysfonctionnement de la plateforme ou des challenges) et promouvoir un esprit de collectif entre les différents campus [1] en réunissant les participants physiquement. Il a par ailleurs été décidé que le CTF soit restreint, pour sa première édition, à 40 participants, nécessairement étudiants d'IMT Atlantique. Étant donné le déroulement exclusivement en présentiel de l'événement, les responsables du campus ont dû procéder sur la base du dossier sous-jacent, à la validation des aspects techniques et de la sécurité, notamment en ce qui concerne les restrictions liées à la pandémie.

Le rétro-planning du projet est détaillé dans le tableau I. On voit que la période d'organisation est d'une durée de 6 mois, compatible avec le déroulé d'un projet étudiant sur un semestre, facilitant son rejeu et sa valorisation dans le cadre d'une unité d'enseignement. Il apparaît aussi que cette organisation, bien que largment centrée sur un travail technique avec la mise en production d'une infrastructure de test opérationnelle et fiable, ainsi que la conception et le recettage de plus de 35 challenges, s'accompagne aussi d'une part conséquente de tâches annexes (communication, définition du règlement, lots pour les gagnants, etc.). L'ensemble de ces

1. IMT Atlantique dispose de 3 campus localisés à Brest, Nantes et Rennes

Début	Durée	Tâche
D - 27 sem.	4 sem.	Définition et validation du projet
D - 25 sem.	4 sem.	Etude du lieu et date, validation par l'école
D - 23 sem.	4 sem.	Etude de la solution technique (CyberRange)
D - 22 sem.	20 sem.	Conception des 35 challenges
D - 20 sem.	6 sem.	Mise en oeuvre de la solution technique
D - 16 sem.	1 sem.	Sondage d'intérêt auprès des étudiants de l'école
D - 8 sem.	8 sem.	Communication sur l'événement
D - 6 sem.	2 sem.	Période d'inscription
D - 4 sem.	1 jour	Annonce des équipes définitives
D - 2 sem.	1 jour	Beta-test des challenges par les enseignants
D - 2 jours	2 jours	Mise en place de la salle (réseau et logistique)
D	1 jour	Déroulé du CTF
D + 2 sem.	2 sem.	Retour d'expérience

TABLE I
RETRO-PLANNING DE L'ORGANISATION DU CTF

tâches constituant une charge de travail conséquente, le volume de travail individuel à accorder, permettant de garantir la bonne réalisation du projet a été validée dès le début entre l'équipe organisatrice et les enseignants-chercheurs en charge du suivi du projet, avec au total, un temps de travail global estimé à 660h, soit 8h par semaine pour chaque membre de l'équipe.

B. Estimation du public concerné et choix d'infrastructure

Afin d'estimer le public qui pourrait être accueilli lors du CTF et par voie de conséquences dimensionner l'ensemble de la logistique et l'infrastructure technique associées, un sondage à destination de l'ensemble des élèves de l'école, tous niveaux, cursus et campus confondus, a été mis en place dès le début du travail d'organisation. Ce sondage a par ailleurs permis de collecter des informations importantes concernant la nature du public attendu et là aussi, guider les choix de conception des challenges. 94 réponses ont été collectées, montrant l'intéret général des éléves pour ce type d'évènement. Au delà, il est apparu qu'une grande majorité d'étudiants non initiés aux CTFs souhaitent y participer. En effet, seuls 20% des sondés ont déjà participé à un ou plusieurs évènements du genre, et 60% ne connaissent pas le terme. De plus, l'intérêt pour le challenge s'est révélé auprès d'un public plutôt hétérogène dans les différentes filières : de la première à la troisième année et parmi toutes les spécialités. On note toutefois que ce sont les premières années et les étudiants de la spécialité cybersécurité qui ont particulièrement exprimé un intérêt montrant une volonté d'acquérir de nouvelles compétences et une expertise nouvelle pour les étudiants de la spécialité et une volonté de découvrir le domaine et s'initier pour ceux de première année. C'est pourquoi il a été décidé de concentrer l'événement sur un format à but pédagogique, avec des challenges accessibles à tous types de niveaux. Enfin, le sondage a permis d'identifier un dimensionnement raisonnable de participants, soit 40 personnes, et ainsi faire le choix de l'infrastructure technique nécessaire pour abriter l'événement ainsi que sur le lieu où celui-ci se déroulera. Le choix de la plateforme hébergeant le CTF s'est ainsi porté sur la CyberRange d'Airbus [2].

2. https://airbus-cyber-security.com/products-and-services/prevent/cyberrange/

C. Adossement à la formation

Afin de s'assurer du caractère pédagogique de l'événement et matérialiser le lien entre les challenges conçus et les apprentissages dispensés dans les différentes unités d'enseignement des spécialités de l'école (réduites au campus Rennais, étant donné leur lien étroit avec les attendus d'un CTF), une matrice qui croise les thématiques des UEs et les thèmes des challanges a été établie. Embryonnaire pour cette première édition, elle montre toutefois la volonté de proposer des challenges en lien avec l'ensemble des cours sans nécessairement mobiliser des compétences exclusivement dispensés dans la spécialité Cybersécurité de l'école, permettant ainsi à des équipes constituées d'éléves de différentes spécialités de nourrir les avancées de l'équipe par les compétences qu'ils mobilisent.

Catégories / Modules	App-Script	Cryptanalyse	Forensic	Programmation	Réseau	Steganographie	Web-client	Web-serveur	OSINT	Physique
Réseaux sans fils pour les objets					X					X
DevOps				X				X		
Sécurité des applications Web							X	X		
Réseaux mobiles 4G/5G					X					
Bases des réseaux					X					
Introduction à la cryptologie Cryptologie avancée		X				X				
Virtualisation des réseaux					X					
Protection des données									X	
Sécurité de l'IoT et des systèmes embarqués					X					X
Sécurité des réseaux	X				X					
Sécurité des OS	X									
Systèmes d'exploitation	X									
Blockchain et consensus				X						
Plateformes pour le Cloud					X			X		

FIGURE 1. Challenges proposés

D. Budget de l'événement

Les projets effectués par les étudiants de l'école n'ont pas pour vocation de se voir être dotés d'un budget dédié. Dans le cas du CTF Hack'lantique, la valorisation des équipes finalistes par diverses récompenses et la nécessité de travailler autour de la communication et d'un rayonnement "école" a nécessité la mise en place d'un budget octroyé par le département. Pour cette première édition, ce budget s'élève à quelques milliers d'euros. Dans les grandes masses, on note qu'un tiers de ce budget concerne les récompenses des équipes, avec une volonté de valoriser les 3 premières équipes gagnantes sur les 8 participantes par des lots à caractère ludique et pédagogique comme par exemple un Starter pack Raspberry Pi4 (4GB) pour chaque membre de l'équipe classée première. La communication persistante qui permet de valoriser l'événement en amont et aval, et par ce biais faciliter sa pérénnisation, a aussi été considérée comme stratégique et à ce titre 20% du budget ont été octroyés pour différents goodies et supports de communication. Ensuite, les challenges proposés

pouvant revêtir un caractère physique, des équipements dédiés, comme par exemple des cadenas de lockpicking, ont été intégrés à hauteur de 15% du budget. Enfin, de par la nature festive de l'événement, qui est un élément essentiel à sa reussite, environ 15% du budget ont été dédiés à des frais de restauration et décoration de type son et lumière. Au delà, le reste a été consacré aux petites dépenses diverses et aux imprévus.

E. Règlement du CTF

Afin que l'événement se déroule dans les meilleures conditions possibles, il a été rédigé un règlement du CTF à destination des participants. Un certain nombre de règles ont été mises en place, notamment en termes de charte de bonne conduite et de règles du jeu, et il est demandé à chacun d'y adhérer en signant un formulaire donnant droit à participatioin. Celui-ci comprend notamment les conditions de participation à l'événement, les détails de participation (heure d'arrivée, de fin, prérequis et accès), mais il mentionne également l'interdiction pour les participants d'attaquer la plate-forme, de partager les solutions, d'utiliser des outils de bruteforce sur les réponses et appelle au respect des autres participants et des organisateurs.

IV. Mise en oeuvre technique

Pour des raisons de dimensionnement de l'événement mais aussi de facilité d'utilisation de par le partenariat actif entre IMT Atlantique et Airbus, la CyberRange [3] a été sélectionnée comme infrastructure support à l'ensemble du CTF. La CyberRange permet de concevoir des réseaux virtualisés ou hybrides efficacement et rapidement grâce à l'interface web LADE et tolère le déploiement et le remplacement à la volée de machines virtuelles et conteneurs. Elle apporte une facilité de configuration et de déploiement des challenges et en fait donc une plateforme idéale pour héberger ce type d'événement.

A. Besoins identifiés

Concernant l'aspect technique, la première étape était de réfléchir à l'architecture réseau permettant à chaque équipe d'accéder aux challenges indépendamment les unes des autres. Il est nécessaire de veiller à ce que les différentes équipes disposent d'un espace de travail étanche, ne puissent communiquer entre elles et à ce que les participants puissent se connecter de façon simple. Par ailleurs, l'authentification doit aussi être assurée afin de n'accepter que les personnes autorisées. Enfin, il est vital d'assurer que la plateforme puisse supporter la charge durant toute l'événement, quelle que soit la nature des activités autorisées effectuées par les participants.

B. Solution mise en oeuvre

1) Accès réseau: Afin de répondre à ces différentes problématiques, le choix s'est porté sur une segmentation multiple du réseau. L'accès à la plateforme se fait via le réseau Wifi de l'école, Eduroam. Afin de garantir un accès optimal et fiable en toutes circonstances, il est nécessaire d'assurer un débit suffisant et éviter tout goulot d'étranglement. Ainsi des points d'accès supplémentaires seront mis en oeuvre par les services techniques de l'école pour l'occasion.

Pour accéder aux challenges, un fichier de configuration OpenVPN est mis à disposition de chaque équipe pour se connecter à son sous-réseau privé dédié, au début de l'événement. Chaque sous-réseau est connecté à un pare-feu donnant accès à la plateforme web du CTF et permet de filtrer en détail les flux entrants et sortants à destination du sous-réseau des challenges.

2) Hébergement et configuration des challenges: Les challenges sont pour la très grande majorité virtualisés. Certains challenges nécessitent des droits d'écriture sur les machines, donc doivent être hébergés sur une machine dédiée par équipe. D'autres ne nécessitant que des droits de lecture, peuvent être mutualisés entre les différentes équipes. La plupart sont hébergés sur des conteneurs docker afin de minimiser les ressources nécessaires à leur fonctionnement. Certains challenges sont également hébergés sur du matériel dédié comme des RaspberryPi, par exemple, et sont interconnectés sur le réseau de la CyberRange.

V. Bilan et conclusion

Le CTF Hack'lantique est la première édition d'un événement qui a pour vocation à devenir pérenne. Au moment de soumettre ce document, il reste encore un mois avant la date de l'événement qui s'apparente donc toujours à un projet mais qui permet de partager certains objectifs et choix qui ont été faits dans sa conception et sa mise en oeuvre. Au delà, un retour d'expérience sera conduit, à la fois de la part des participants, mais aussi de l'équipe d'organisation et de l'équipe d'encadrement du projet, afin de pouvoir planifier au mieux les éditions suivantes du CTF d'IMT Atlantique. On relève à ce stade une volonté d'associer le CTF à une modalité d'apprentissage complémentaire des différents cours, travaux pratiques et projets traditionnellement dispensés dans une formation d'enseignement supérieur. La conception des challenges, articulée autour d'une matrice d'unités d'enseignement, a permis d'identifier un premier guide pour l'acquisition de compétences en lien avec les apprentissages de l'école. Pour les années futures, il est prévu de développer plus avant cet aspect en associant les responsables des unités d'enseignement aux acquis d'apprentissage qu'ils souhaitent voir être dispensés voire validés par ce biais, tout en gardant à l'esprit que le CTF n'a pas pour vocation à devenir une modalité d'évaluation supplémentaire pour conserver son caractère ludique. Au delà, la question de la co-organisation ou mutualisation de ce type d'événement au niveau national avec d'autres formations de l'enseignement supérieur est un point sur lequel l'équipe enseignante d'encadrement souhaite aussi mener une reflexion pour les années futures.

Remerciements

Les auteurs remercient Yann Busnel responsable du département SRCD d'IMT Atlantique ainsi que Vincent Guillo

3. https://airbus-cyber-security.com/fr/produits-services/prevenir/cyberrange/

et Franck Benard en charge du support logistique et technique du campus de Rennes, pour leur aide et leur soutien.

RÉFÉRENCES

[1] R. Raman, S. Sunny, V. Pavithran, and K. Achuthan, "Framework for evaluating Capture the Flag (CTF) security competitions," in Int. Conf. for Convergence for Technology, 2014, Pune, India, DOI : 10.1109/I2CT.2014.7092098

[2] https ://defcon.org/

[3] https ://en.wikipedia.org/wiki/DEF_CON

[4] Q. Yan, W. Lai, and Z. Wang, "Online Experiments Based on the CTF Model for Information Security MOOC Courses," in 16th Int. Conf. on Computer Science & Education (ICCSE), 2021, Lancaster, UK, DOI : 10.1109/ICCSE51940.2021.9569691

[5] https ://ctftime.org/

[6] https ://github.com/ctfs

[7] https ://github.com/CTFd/CTFd

[8] https ://github.com/facebookarchive/fbctf

[9] https ://github.com/easyctf/librectf

[10] https ://github.com/picoCTF

[11] K. Ferguson-Walter, M. Major, D. Van Bruggen, S. Fugate, and R. Gutzwiller, "The World (of CTF) is Not Enough Data : Lessons Learned from a Cyber Deception Experiment," in 5th Int. Conf. on Collaboration and Internet Computing, 2019, Los Angeles, USA, DOI : 10.1109/CIC48465.2019.00048

[12] Z. Liu, H. Qiu, J. Zhu, and Z. Zeng "AAG : A Model for Attack Behavior Judgment in CTF-style Cyber Security Training," in 10th Int. Conf. on Software Engineering and Service Science, 2019, Beijing, China, DOI : 10.1109/ICSESS47205.2019.9040727

[13] S. Roschke, C. Willems, and C. Meinel, "A security laboratory for CTF scenarios and teaching IDS," 2nd Int. Conf. on Education Technology and Computer, 2010, Shanghai, China. DOI : 10.1109/ICETC.2010.5529213

[14] W. Wu and W-C. Feng, "Game to Dethrone : A Least Privilege CTF," in 6th Int. Conf. on Smart Cloud, 2021, Newark, USA. DOI : 10.1109/SmartCloud52277.2021.00030

[15] Z. Romano, J. Windsor, M. VanDerPol, and J. Coffman, "Election Security in the Cloud : A CTF Activity to Teach Cloud and Web Security", Frontiers in Education Conference, 2021, Lincoln, USA, DOI : 10.1109/FIE49875.2021.9637368

[16] A.D.B. Ibrahim, A.H.A. Hanafi, H. Rokman, M.N.A. Zawawi, Z-A. Ibrahim, and F.A. Rahim, "Comparative Analysis on Student's Interest in Cyber Security among Secondary School Students using CTF Platform", Int. Conf. on Information Technology and Multimedia, 2020, Selangor, Malaysia, DOI : 10.1109/ICIMU49871.2020.9243561

[17] https ://www.ssi.gouv.fr/actualite/france-cybersecurity-challenge-un-defi-qui-rassemble-tous-les-talents/

[18] https ://www.root-me.org/

[19] G. Costa, M. Lualdi, M. Ribaudo, and A. Valenza, "A NERD DOGMA : Introducing CTF to Non-Expert Audience," in Proc. 21st Annual Conference on Information Technology Education, ser. SIGITE '20. New York, NY, USA, ACM, 2020, p. 413–418. [Online].Available : https ://doi.org/10.1145/3368308.3415405

[20] M. Malone, Y. Wang, K. James, M. Anderegg, J. Werner, and F. Monrose, "To Gamify or Not ? On Leaderboard Effects, Student Engagement and Learning Outcomes in a Cybersecurity Intervention," in Proc. 52nd ACM Technical Symposium on Computer Science Education, ser. SIGCSE '21. New York, NY, USA : ACM, 2021, p. 1135–1141. [Online]. Available : https ://doi.org/10.1145/3408877.3432544