Des challenges de hacking pour développer la cybervigilance des étudiants en management des systèmes d'information

Philippe Lépinard, Yann Goetgheluck

29e Conférence de l'Association Information et Management

27-29 mai 2024 à Montpellier - La Grande-Motte

Des challenges de *hacking* pour développer la cybervigilance des étudiants en management des systèmes d'information

Philippe LÉPINARD, Univ Paris Est Créteil, IRG, F-94010 Créteil, France

Yann GOETGHELUCK, Univ Paris Est Créteil, IAE Paris-Est, F-94010 Créteil, France

Résumé

La sensibilisation et la formation à la cybersécurité des étudiants en Management des systèmes d'information (MSI) est actuellement laissée à la libre initiative des responsables de formation sans qu'aucune aide ciblée ne leur soit proposée. Pourtant, les compétences en cybersécurité, au sens large, sont dorénavant indispensables dans tout projet de systèmes d'information et deviennent parfois des conditions d'employabilité. Les objectifs de notre projet de recherche souhaitent donc combler cette absence d'accompagnement dans la montée en compétences cyber des étudiants inscrits dans les programmes de formation en MSI. À ce titre, nous envisageons la conception d'un référentiel de compétences commun autour de la cybervigilance intégrant nativement l'ensemble des ressources indispensables. Parmi ces dernières, nous étudions dans cet article les défis de type *Capture The Flag* (CTF) afin de proposer aux enseignants et étudiants une méthodologie ludique et adaptée pour l'apprentissage du *hacking* éthique.

Mots clés

Cybersécurité ; Capture de drapeaux ; *Hacking* éthique ; Management des systèmes d'information ; Gamification ; Cybervigilance

Hacking challenges to develop Information System Management students' cyber vigilance

Abstract

Cybersecurity awareness and training for Information Systems Management (ISM) students is currently left to the free initiative of training managers, without any targeted assistance being offered. However, cybersecurity skills, in the broadest sense of the term, are now essential to any information systems project, and are sometimes becoming a prerequisite for employability. The objectives of our research project are therefore to fill this gap in the cyber skills of students enrolled in ISM training programs. To this end, we plan to design a common skills framework for cyber vigilance, natively integrating all the essential resources. In this article, we look at capture-the-flag (CTF) challenges as a way of offering teachers and students a playful methodology for learning about ethical hacking.

Keywords

Cybersecurity ; Capture the flag ; Ethical hacking ; Information systems management ; Gamification ; Cyber vigilance

Des challenges de *hacking* pour développer la cybervigilance des étudiants en management des systèmes d'information

« The future of HFE [human factors and ergonomic, NDA] *in cyber defense is one of prime importance to life, as cyber threats target more aspects of our existence, and with increasing precision and impact »*
(Gutzwiller et al., 2015, p.325)

Introduction

Depuis quelques années, les challenges de *hacking* fleurissent de toute part. Proposées par des entreprises, des écoles, des associations ou même des organismes militaires[1], en ligne ou en présentiel, ces compétitions de type *Capture The Flag* (CTF) proposent à des équipes de se défier pour résoudre des énigmes de différentes natures généralement très techniques. À l'image de l'*esport*, les meilleures équipes deviennent alors les stars de leurs organisations respectives ; entraînant de fait une dimension fortement élitiste et renforçant l'aspect mystérieux de la cybersécurité pour la majorité de la population. Pourtant, ces défis ne sont pas inaccessibles et de nombreux dispositifs peuvent être mis en œuvre de manière simples et gratuits. Au-delà de l'aspect compétitif, les CTF sont avant tout destinés à développer les connaissances et compétences des participants en *hacking* éthique de manière gamifiée[2]. Le sujet de notre projet de recherche, mené dans le cadre du projet pédagogique et de recherche EdUTeam[3], est donc avant tout pédagogique. Si notre problématique générale s'intéresse aux compétences en cybersécurité que devraient posséder tout étudiant en management des systèmes d'information (MIS) pour réduire le *cybersecurity skills gap* (Cobb, 2016, p.1), le projet présenté dans cette communication est plus restreint puisque nous souhaitons nous questionner dans un premier temps sur l'intérêt des CTF dans le développement de la cybervigilance des étudiants en MSI. La première partie de notre article présente le concept de cybervigilance. La deuxième étape traite des différents modèles de CTF. Enfin, dans un dernier temps, nous présentons le projet de recherche sous-jacent à ces premiers travaux.

1. Cybervigilance

S'interroger sur le concept de cybervigilance revient à définir la notion de conscience de la situation cyber : « *The term cyber-cognitive situational awareness specifically refers to human operators' awareness of threats distributed across virtual landscapes* » (Guidetti, 2023, p.2).

[1] Par exemple, le CTF annuel « Passe ton hack d'abord » co-organisé par le Commandement de la cyberdéfense (COMCYBER) et la Direction générale de l'enseignement scolaire (DGESCO) : https://eduscol.education.fr/document/53682/download (consulté le 8 janvier 2024).
[2] « *Ethical hacking may be thought of as a methodology for assisting computer professionals and administrators in their efforts to secure networks. […] Finally, it may be defined as someone with the same skill sets as an attacker, but differs in the fact that permission has been granted from the owner to test the security system of the target* » (Hartley, 2015, p.96).
[3] Site du projet pédagogique et de recherche EdUTeam : https://eduteam.fr/.

Plus largement, et dans le champ des facteurs humains, d'autres auteurs se questionnent sur les liens entre la cybervigilance et la vigilance dans d'autres contextes (Sawyer *et al.*, 2014, p.1771) comme le contrôle du traffic aérien, la surveillance médicale, etc. En effet, si nous n'avons pas trouvé de définition stabilisée de la cybervigilance, il nous semble qu'elle peut s'appréhender par la capacité à maintenir une vigilance suffisante afin de ne pas tomber dans les pièges tendus par les cyberattaquants. L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) a mis en place le *hashtag* #CyberVigilant sur le réseau social X (ex-Twitter). Sa caractérisation semble adaptée à une approche simple de la cybervigilance : « *Avec #CyberVigilant, adoptez des réflexes simples, préconisés par l'ANSSI, pour vous prémunir efficacement des menaces sur Internet* »[4]. Il s'agit donc de fournir des éléments de base à l'ensemble des citoyens pour leur permettre de réagir efficacement à une attaque ou une tentative d'attaque. S'il n'est ici nullement question de *Cyber Threat Intelligence* (CTI) des experts en cybersécurité définit comme « *evidence-based knowledge representing threats that can inform decisions* » (2019, p.2), l'objectif est néanmoins de dépasser les dix règles de base de l'ANSSI[5] compte tenu de la population ciblée, les étudiants en MSI ; ces derniers devant à notre avis acquérir des connaissances et développer des compétences plus poussées du fait de leur implication dans les projets de SI et ce, afin d'améliorer également leur employabilité. La cybervigilance peut donc être appréhendée comme une compétence classique selon Tardif : « *savoir-agir complexe reposant sur la mobilisation et la combinaison efficaces d'une variété de ressources internes et externes à l'intérieur d'une famille de situations* » (2006, p.22).

2. Challenge *Capture The Flag* (CTF)

Initialement popularisé grâce à la conférence annuelle DEF CON[6] depuis 1996, un CTF est « *a challenge-based competition for gaining and training cyber security related skills by actively applying them. In a CTF, a team (or a single player) solves problems related to cyber security, and if their answer (also often referred to as flag or solution) to the problem is correct, they get rewarded with points. The aim is to score more points than other participants, which contributes to the competition. CTF platforms (also often referred to as CTF environments or CTF frameworks in literature) are typically used as game-like environments where participants may practice computer security abilities, skills and knowledge* » (Kucek & Leitner, 2020, p.1). Selon Cole (2022, p.470), les CTF peuvent prendre quatre formes principales :

- *Jeopardy* : il s'agit de défis de type questions – réponses et indépendants les uns des autres contre des machines,
- *Attack-defense* : deux équipes se font face (*red team* VS *blue team*[7]), une est en attaque et l'autre en défense (Ficco & Palmieri, 2019, p.109 ; Chindrus & Caruntu, 2023),
- *King of the hill* : plusieurs équipes sont en compétition pour le contrôle de ressources,

[4] Citation provenant de la page de l'ANSSI suivante : https://cyber.gouv.fr/actualites/sur-internet-soyez-toujours-cybervigilant (consulté le 8 janvier 2024).
[5] Les dix règles de base de l'ANSSI : https://www.ssi.gouv.fr/entreprise/precautions-elementaires/dix-regles-de-base/.
[6] Site de la conférence annuelle de la DEF CON : https://defcon.org/.
[7] Pour une présentation des blue, red et purple teams, nous vous conseillons la lecture du chapitre « *Establishing a Defense Program* » (Sehgal & Thymianis, 2023, p.3 à 14).

– *Hack quest* : défis liés entre eux dans le contexte d'une aventure narrative plus globale (Chothia *et al*., 2019) comme un « *challenge chains* » (Vykopal *et al*., 2019, p.2).

Les *flags* ou drapeaux sont des textes ou chaînes de caractères cachés à récupérer prouvant la réussite des différentes épreuves. Les CTF sont des dispositifs gamifiés par nature (Leune, 2017, Kim et *al.*, 2023) puisque, au-delà des compétitions, de nombreux mécanismes de gamification sont présents afin d'engager et de motiver les participants (Balon & Baggili, 2033, p.11763 ; Kartasasmita *et al.*, 2023, p.888) : points, passage de niveaux, quêtes, etc. D'ailleurs, si l'aspect compétitif peut rebuter, les plateformes de CTF en ligne peuvent parfaitement être utilisées de manière solitaire ou coopérative. À ce titre, nous pouvons aussi indiquer la présence de jeux vidéo de *hacking* comme *Hacknet* ou *Uplink*.

Dans l'enseignement supérieur, plusieurs usages de CTF ont été expérimentés lors de cours en cybersécurité, notamment dans le cadre de travaux pratiques (Gonzalez et *al.*, 2019 ; Vykopal, 2020 ; Karagiannis & Magkos, 2021 ; Ksiezopolski *et al.*, 2022), ou d'organisation de CTF par des étudiants comme Hack'lantique (Boudaud *et al*., 2023). Certains travaux déjà anciens valident l'intérêt des CTF dans la formation comme Cheung *et al.* (2011, p.530) : « *The students were able to improve their computer skills, security knowledge, ability to teach others and interest on the topic of cybersecurity* ». Les CTF sont également sources de nombreuses approches pédagogiques (hors enseignement supérieur) ou opérationnelles comme le recrutement (Sehgal & Thymianis, 2023, p.12), l'identification de nouvelles méthodes d'attaque (notamment via la *Cyber Kill Chain*®) et de défense (Strout, 2023, p.185), pour attirer des étudiants dans la cybersécurité (Alicia, 2017), la formation des professionnels de la cybersécurité déjà en poste (Wee *et al*., 2016) ou le développement des compétences de travail collaboratif (Chang *et al.*, 2022).

3. Projet de recherche

3.1 Première étape : expérimenter les CTF pédagogiques

Notre projet de recherche-action est destiné à répondre à la question suivante : quelles compétences en cybersécurité devraient posséder les étudiants en MSI ? Plus spécifiquement, et dans le cadre de cet article, nous souhaitons savoir dans un premier temps si les CTF peuvent permettre de développer la cybervigilance des étudiants en MSI. Dans ce contexte, et contrairement à la proposition d'un unique cours ludifié par Arduin & Costé (2022, p.7 et suivantes) nous avons décidé de créer une équipe CTF pédagogique au sein de l'IAE Paris-Est, l'école universitaire de management de l'Université Paris-Est Créteil (UPEC, Figure 1). Cette équipe, composée de dix étudiants volontaires de la Licence 1 au Master 2 en projet tutoré, a comme objectif l'organisation de CTF internes, obligatoires et régulièrement espacés durant l'année universitaire 2023-2024 pour l'ensemble du Parcours Informatique & Management, soit leurs 120 camarades[8] (Figure 2). Chaque CTF doit être accessible à tous les étudiants grâce à une progression adaptée. Plus largement, nous cherchons à réduire au maximum les limites des CTF identifiées par Szedlak & M'Manga (2020, p.3) et Vykopal *et al.* (2020, p.2) :

– la difficulté pour les débutants (et la frustration associée),

[8] À noter l'existence d'un autre projet tutoré associé concernant la gestion de crises cyber.

– l'ambiguïté (volontaire) de certains défis,
– l'absence de *feedback*.

Si les deux premières limites touchent aux épreuves et peuvent demander un travail conséquent de préparation, la 3e est nativement résolue dans nos travaux grâce à un compte rendu pédagogique apportant les connaissances nécessaires pour la réussite des défis. À noter que ce compte rendu est différent des *writeups* (ou *write-ups* selon les auteurs), document rédigé par les participants eux-mêmes pour expliquer leur démarche de résolution de problèmes durant les épreuves. Le dispositif dépasse donc la simple organisation de compétitions internes. Il intègre systématiquement une remédiation s'appuyant autant que possible sur de la documentation académique ou professionnelle reconnue afin que les étudiants développent des connaissances et compétences solides pour aller de plus en plus loin dans les CTF suivants. La littérature scientifique est également exploitée pour identifier des conseils ou pratiques pédagogiques garantissant (ou du moins facilitant) l'atteinte individuelle des objectifs d'apprentissage comme la gestion des indices (adaptatifs) et les techniques d'alerte de plagiats de Vykopal *et al.* (2020). Bien entendu, l'équipe est également invitée à participer à des CTF externes afin de s'imprégner de l'écosystème, de découvrir les sujets d'actualité et de rencontrer des experts du domaine. En octobre 2023, quatre membres ont concouru au *Purple Pill Challenge* où ils se sont classés 20e sur 30 équipes provenant de structures dédiées à la cybersécurité[9]. Au jour de l'écriture de cet article, l'équipe complète est engagée dans la compétition OSINT « Disparue(s) » organisée par le collectif Oscar Zulu[10], expérimente la toute nouvelle plateforme TOP portée par le Campus Cyber[11], tente de résoudre les épreuves quotidiennes du site d'archives des épreuves du *France Cybersecurity Challenge* (Hackropole[12]) proposé par l'ANSSI et à demander de participer au challenge « Passe ton hack d'abord » 2024 (hors compétition).

Figure 1. Logo de l'équipe CTF pédagogique de l'IAE Paris-Est (UPEC).

Les outils utilisés par l'équipe pour l'organisation de CTF sont gratuits. Il s'agit de la plateforme OZINT[13] (entraînement au renseignement d'origine sources ouvertes ou OSINT[14]) et des challenges des sites internet *OverTheWire*[15] et 247CTF[16]. Afin de s'auto-former, les membres de l'équipe ont chacun un abonnement annuel au *Battlehack* de la société Seela[17]

[9] Site du *Purple Pill Challenge* : https://www.purplepillchallenge.fr/.
[10] Site du challenge « Disparue(s) » : https://ctf.osintisnotacrime.com/ (consulté le 8 novembre 2023).
[11] Site de la plateforme TOP (The OSINT Project) : https://the-osint-project.fr/.
[12] Site d'archives d'épreuves Hackropole : https://hackropole.fr/fr/.
[13] Site de la plateforme OZINT : https://ozint.eu/.
[14] *« OSINT is about collecting information that has leaked or otherwise found its way onto the Internet or real world »* (Buchanan, 2014, p.98).
[15] Challenge Bandit du site *OverTheWire* : https://overthewire.org/wargames/bandit/.
[16] Plateforme 247CTF : https://247ctf.com/.
[17] Site du *Battlehack* : https://seela.io/battleh4ck/.

(pour environ 120 euros par étudiant). Par conséquent, les moyens à mettre en œuvre pour la réalisation de ce projet d'ordre pédagogique sont faibles et sa réplicabilité potentiellement élevée[18].

Figure 2. Un premier CTF a été organisé dès la semaine de pré-rentrée fin août pour les nouveaux bacheliers intégrant la Licence du Parcours Informatique & Management.

3.2 Seconde étape : concevoir un référentiel de compétences cyber avec les ressources associées

Pour autant, notre projet de recherche est plus ambitieux. Dans un second temps, nous souhaitons en effet travailler sur les compétences en cybersécurité des étudiants en MSI attendues par les employeurs afin de définir et diffuser un référentiel de compétences complet incluant l'étude initiale abordée dans ce texte (CTF pédagogiques) mais également des ressources gratuites et de qualité comme le MOOC SecNum*académie*[19] de l'ANSSI, le MOOC L'atelier RGPD[20] de la Commission nationale de l'informatique et des libertés (CNIL) et les différents MOOC proposés régulièrement sur la plateforme France Université Numérique (FUN MOOC)[21]. D'autres dispositifs pourront en parallèle être pris en compte comme le domaine « Protection et sécurité » de Pix[22] et la labellisation des formations de l'enseignement supérieur CyberEdu[23]. Enfin, il existe de nombreuses ressources qui pourront enrichir notre travail comme les ouvrages rédigés par des équipes CTF (Nu1L Team, 2022), les huit *Knowledge Areas (KAs)* du rapport *Cybersecurity Curricula 2017*[24] et la matrice MITRE ATT&CK qui « *enables an organization to search and navigate through the different types of cyberattack techniques, used to enhance, analyze, and test threat event identification and detection efforts* » (Möller, 2023, p.261). Nous souhaitons enfin disposer d'un guide pour mettre en œuvre une plateforme *open source* et libre adaptée aux besoins des étudiants en MSI

[18] *Udemy* propose une formation de découverte aux CTF : https://www.udemy.com/course/cyber-ctf-101/.
[19] MOOC SecNum*académie* de l'ANSSI : https://secnumacademie.gouv.fr/.
[20] MOOC L'atelier RGPD de la CNIL : https://atelier-rgpd.cnil.fr/login/index.php.
[21] Site de FUN MOOC : https://www.fun-mooc.fr/fr/.
[22] Pix est la version française du *DigComp Framework* européen. Les compétences du domaine *Safety* sont présentées sur cette page : https://joint-research-centre.ec.europa.eu/digcomp/digcomp-framework_en#ref-4-safety (Consulté le 8 janvier 2024).
[23] Site internet CyberEdu : https://www.cyberedu.fr/.
[24] Lien vers le texte : https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf (Consulté le 8 janvier 2024).

dans des parcours ayant une dimension technique importante mais également facilement déployable pour les enseignants. En effet, et comme le soulignent Trickel *et al.* (2017, p.1), les compétences et le temps nécessaires pour le déploiement d'un dispositif de CTF peut être substantiel. Pour ce faire, nous devrons mener un *benchmark* des outils existants comme PocketCTF (Karagiannis *et al.*, 2021) ou CyTrONE[25] en nous appuyant sur des grilles d'analyse ou guides de conception (Karagiannis *et al.*, 2021 ; Beuran et *al.*, 2023 ; Ortiz-Garces, 2023).

Toutefois, et comme le disent Švábenský *et al.* (2021), la cybervigilance doit intégrer des aspects managériaux et organisationnels: « *Although CTF challenges are excellent for practicing technical skills, they do not address topics such as phishing and general cybersecurity awareness. However, these topics are of utmost importance for mitigating the current advanced cyber threats* » (p.12). Les résultats de nos travaux devront donc définir un dispositif pédagogique de formation à la cybervigilance pour les étudiants des formations en MSI ; quels que soient leurs niveaux et leurs spécialisations.

Conclusion

Du fait de leur positionnement dans une zone grise entre les dimensions organisationnelle et technique de la cybersécurité, la sensibilisation et la formation des étudiants en MSI dans ce domaine particulièrement dynamique est actuellement laissée à la libre initiative des responsables de formation sans qu'aucune aide ciblée ne leur soit proposée. Pourtant, les compétences en cybersécurité, au sens large, sont dorénavant indispensables dans tout projet de systèmes d'information et deviennent parfois des conditions d'employabilité. Les objectifs de notre projet de recherche sont de combler cette absence d'accompagnement dans la montée en compétences cyber des étudiants inscrits dans les programmes de formation en MSI. À ce titre, nous envisageons la conception d'un référentiel de compétences commun autour de la cybervigilance intégrant nativement l'ensemble des ressources indispensables. Parmi ces dernières, nous avons étudié dans cet article les CTF et avons découvert que ces derniers sont d'une grande richesse, tant sur la forme que sur le fond. Toutefois, plusieurs auteurs mettent en avant des limites importantes, notamment leur accessibilité pour les débutants. Dans ce contexte, nous avons décidé de déployer une équipe d'étudiants en projet tutoré destinée à expérimenter des CTF pédagogiques et ainsi proposer aux enseignants et étudiants une méthodologie ludique et adaptée pour l'apprentissage du *hacking* éthique. Au-delà de la montée en compétences cyber des étudiants en MSI, ce projet pourrait être une sorte de préquel aux actions SETA (*Security Education, Training, and Awareness*) menées par les organisations destinées notamment à développer la vigilance cyber des employés (Hu *et al.*, 2022, p.752).

Références

Alicea, Y. (2017). Cybersecurity Competitions as Effective Cybersecurity Teaching Tools. *Annual Information Institute Conference*, Las Vegas, USA.

[25] Github de CyTrOne : https://github.com/crond-jaist/cytrone (Consulté le 8 janvier 2024).

Arduin, P.-E. (2022). Pirate ta fac ! Ludification de séances de cours sur la sécurité des systèmes d'information, *INFORSID 2022 - INFormatique des Organisations et Systèmes d'Information et de Décision*, Dijon, France.

Balon, T., Baggili, I. (2023). Cybercompetitions: A survey of competitions, tools, and systems to support cybersecurity education, *Educational and Information Technologies*, 28, 11759-11751.

Beuran, R., Vykopal, J., Belajová, D., Celeda, P., Tan, Y., Shinoda, Y. (2023). Capability Assessment Methodology and Comparative Analysis of Cybersecurity Training Platforms, *Computers & Security*, 128, 1-14.

Boudaud, J., Gilbert, C., Laurain, T., Métayer, C., Sarrazin, J., Autrel, F., Bouabdallah, A., Doyen, G., Efrain Navas, R. (2022). Hack'lantique : première expérience de CTF pédagogique, *Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information (RESSI)*, Chambon-sur-Lac, France.

Buchanan, C. (2014). *Kali Linux CTF Blueprints*, Packt Publishing.

Chang, S., Yoon, K., Wuthier, S., & Zhang, K. (2022). Capture the Flag for Team Construction in Cybersecurity. *ArXiv*, 1-7.

Cheung, R. S., Cohen, J. P., Lo, H. Z., Elia, F. (2011). Challenge based learning in cybersecurity education. *Proceedings of the International Conference on Security and Management (SAM'11)*, Las Vegas, USA, 524-529.

Chindrus, C., & Caruntu, C.-F. (2023). Securing the Network: A Red and Blue Cybersecurity Competition Case Study. *Information*, *14*(11), 1-24.

Chothia, T., Novakovic, C., Radu, A. I., Thomas, R. J. (2019). Choose Your Pwn Adventure: Adding Competition and Storytelling to an Introductory Cybersecurity Course. In *Lecture Notes in Computer Science* (pp. 141-172), Springer Verlag.

Cobb, S. (2016). Mind This Gap: Criminal Hacking and The Global Cybersecurity Skills Shortage, A Critical Analysis, *Virus Bulletin Conference*. Denver, USA.

Cole, S. (2022). Impact of Capture The Flag (CTF)-style vs. Traditional Exercises in an Introductory Computer Security Class, *27th ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE '22)*, New York, USA.

Ficco, M., Palmieri, F. (2019). Leaf: An open-source cybersecurity training platform for realistic edge-IoT scenarios, *Journal of Systems Architecture*, 97, 107-129.

Gonzalez, H., Llamas, R., Montaño, O. (2019), Using CTF Tournament for Reinforcing Learned Skills in Cybersecurity Course, *Research in Computing Science*, *148*(5), 133-141.

Guidetti, O.A., Speelman, C., Boulhas, P. (2023). A review of cyber vigilance tasks for network defense, *Frontiers in Neuroergonomics*, 4, 1-11.

Gutzwiller, R., Fugate, S., Sawyer, B., Hancock, P. A. (2015). The Human Factors of Cyber Network Defense, *Proceedings of the Human Factors and Ergonomics Society 59th Annual Meeting*, 322-327.

Hartley, R. (2015). Ethical Hacking Pedagogy: An Analysis and Overview of Teaching Students to Hack, *Journal of International Technology and Information Management*, *24*(4), 95-104.

Hu, S., Hsu, C., & Zhou, Z. (2022). Security Education, Training, and Awareness Programs: Literature Review. *Journal of Computer Information Systems*, *62*(4), 752–764.

Karagiannis, S., Magkos, E. (2021). Adapting CTF Challenges into Virtual Cybersecurity Learning Environments, *Information and computer security*, *29*(1), 105-132.

Karagiannis, S., Maragkos-Belmpas, E., Magkos, E. (2020). An Analysis and Evaluation of Open Source Capture the Flag Platforms as Cybersecurity e-Learning Tools, *13th IFIP World Conference on Information Security Education (WISE)*, Maribor, Slovénia.

Karagiannis, S., Ntantogian, C., Magkos, E., Ribeiro, L., Campos, L. (2021). PocketCTF: A Fully Featured Approach for Hosting Portable Attack and Defense Cybersecurity Exercises, *Information*, *12*(8), 1-13.

Kartasasmita, D. G., Timur C., Reksoprodjo, A. (2023). Enhancing Competency of Cybersecurity Through Implementation of the "CAPTURE THE FLAG" On College in Indonesia, *International Journal Of Humanities Education And Social Sciences*, *3*(2), 875-890.

Kim, J.B., Zhong, C. & Liu, H. (2023). Teaching Tip What You Need to Know about Gamification Process of Cybersecurity Hands-on Lab Exercises: Lessons and Challenges. *Journal of Information Systems Education*, *34*(4), 387-405

Kucek, S., Leitner, M. (2020). An Empirical Survey of Functions and Configurations of Open-Source Capture the Flag (CTF) Environments, *Journal of Network and Computer Applications*, 151, 1-19.

Ksiezopolski, B., Mazur, K., Miskiewicz, M., Rusinek, D. (2022). Teaching a Hands-On CTF-Based Web Application Security Course, *Electronics*, 11, 1-21.

Möller, D. (2023). *Guide to Cybersecurity in Digital Transformation - Trends, Methods, Technologies, Applications and Best Practices*, Springer.

Leune, K., Petrilli, S. (2017). Using Capture-the-Flag to Enhance the Effectiveness of Cybersecurity Education, *Proceedings of the 18th Annual Conference on Information Technology Education (SIGITE '17)*, New York, USA, 47-52.

Nu1L Team (2022), *Handbook for CTFers*, Springer.

Ortiz-Garces, I., Gutierrez, R., Guerra, D., Sanchez-Viteri, S., Villegas, W. (2023). Development of a Platform for Learning Cybersecurity Using Capturing the Flag Competitions, *Electronics*, 12, 1-15.

Sawyer, B., Finomore, V., Funke, G., Manusco, V., Funke, M., Mattews, G., Warm, J. (2014). Cyber Vigilance: Effects of Signal Probability and Event Rate, *Proceedings of the Human Factors and Ergonomics Society 58th Annual Meeting*, 1771-1775.

Sehgal, K., Thymianis, N. (2023). *Cybersecurity Blue Team Strategies. Uncover the secrets of blue teams to combat cyber threats in your organization*, Packt Publishing.

Strout, B. (2023). *The Vulnerability Researcher's Handbook - A comprehensive guide to discovering, reporting, and publishing security vulnerabilities*, Packt Publishing.

Švábenský, V., Celeda, P., Vykopal, J., Brišáková, S. (2021). Cybersecurity knowledge and skills taught in capture the flag challenges, *Computers & Security*, 102, 1-14.

Szedlak, D., M'manga, A. (2020). Eliciting Requirements for a Student-focussed Capture The Flag, *7th International Conference on Behavioural and Social Computing (BESC)*, Bournemouth, United Kingdom.

Tardif, J. (2006). *L'évaluation des compétences. Documenter le parcours de développement*, Chenelière Éducation.

Tounsin, W. (2019). What is Cyber Threat Intelligence and How is it Evolving?. In *Cyber-Vigilance and Digital Trust: Cyber Security in the Era of Cloud Computing and IoT* (pp. 1-49). Wiley.

Trickel, E., Disperati, F., Gustafson, E., Kalantari, F., Mabey, M., Tiwari, N., Safaei, Y., Doupé, A., Vigna, G. (2017). ShellWe Play A Game? CTF-as-a-service for Security Education, *USENIX Workshop on Advances in Security Education*, Vancouver, Canada.

Vykopal, J., Švábenský, V., Chang, E.-C. (2020). Benefits and Pitfalls of Using Capture the Flag Games in University Courses, *SIGCSE '20: Proceedings of the 51st ACM Technical Symposium on Computer Science Education*, Portland, USA.

Wee, C., Bashir, M.N., Memon, N.D. (2016). The Cybersecurity Competition Experience: Perceptions from Cybersecurity Workers, *Twelfth Symposium on Usable Privacy and Security*, Denver, USA.