Identifying Large Young Hacker Concentration in Indonesia

Onno W. Purbo^{1*}, Prasetyo Purnomo², Dimaz Arno Prasetio³, Agung Budi Prasetio⁴ and Dr. Tubagus Asep Nurdin⁵

^{1*}Faculty Computer Science, Institute of Technology Tangerang Selatan, Indonesia. onno@itts.ac.id, onno@indo.net.id, https://orcid.org/0000-0002-7602-9817

²Faculty Computer Science, Institute of Technology Tangerang Selatan, Indonesia. prasetyo@itts.ac.id, https://orcid.org/0009-0000-6574-8480

³Faculty Computer Science, Institute of Technology Tangerang Selatan, Indonesia. dimaz@itts.ac.id, https://orcid.org/0000-0002-6036-5613

⁴Faculty Computer Science, Institute of Technology Tangerang Selatan, Indonesia. agung@itts.ac.id, https://orcid.org/0000-0001-5872-5272

⁵IT Division, Tangerang Selatan City Government, Indonesia. tubagusasep79@gmail.com, https://orcid.org/0009-0005-4513-5333

Received: October 05, 2023; Accepted: December 12, 2023; Published: February 29, 2024

Abstract

An Indonesian 2023 Capture the Flag competition for 18-year-olds is looked at for the first time. It engaged a diverse participant profile, encompassing high school students and the general public from various regions. Java Island saw the most participation, especially in East Java, with little interest from Jakarta's youth, possibly due to the abundance of distractions. Despite varied educational backgrounds, vocational institutes, notably in East Java, featured prominently. Gender diversity was limited, with no female participants progressing to the final stage. Analysis of problem categories indicated diverse performance, highlighting challenges in digital signature, online hacking, network analysis, and database assault. Normalization emphasized problems within high school students' capabilities, suggesting the integration of cybersecurity education into curricula. Finalists predominantly hail from Central and East Java, indicating a regional concentration. Younger, non-Javanese participants underscored passion's role in success. Successful profiles revealed independent skill acquisition through online platforms, especially John Hammond's YouTube channel, emphasizing the need for accessible cybersecurity education resources. The study advocates prioritizing ICT education, particularly in networking, online hacking, OSINT, and cryptography, to enhance high school CTF participation and performance. The findings showcase the significance of passion-driven, self-directed learning in fostering ethical hacking skills among Indonesian youth.

Keywords: Cyber Security, CTF, Capture the Flag, High School, Hacking.

1 Introduction

In the early months of 2023, a significant security breach occurred, resulting in the unauthorized acquisition of 34 million Indonesian passports by hackers (Huang & Leu 2011). The release of personal

Journal of Internet Services and Information Security (JISIS), volume: 14, number: 1 (February), pp. 52-63. DOI: 10.58346/JISIS.2024.11.004

^{*}Corresponding author: Faculty Computer Science, Institute of Technology Tangerang Selatan, Indonesia.

information, including names, passport numbers, expiration dates, birth dates, and genders, occurred in the year 2023 (KUK, 2023). In 2022, BSI, the largest Islamic bank in Indonesia, discovered that the credentials of its 15 million clients were exposed online (Sulaiman, 2023). In the year 2021, the data of two million users of BRI Life was sold through an online auction for a sum of \$7,000. Photographs serve as the medium via which health records, birth certificates, and electronic ID cards are submitted. In May 2021, a significant online breach occurred, resulting in the compromising of around 2.3 million data records belonging to the Indonesian General Elections Commission. In 2020, Raidforums facilitated the sale of around 2.9 million personal members' data. Subsequently, the occurrence of a data breach affecting two prominent Indonesian e-commerce websites was brought to light once more. In May 2020, a significant number of personal details were illicitly acquired from Indonesian e-commerce platforms (Nugraha, 2021). Indonesia is facing a pressing demand for an increased number of specialists specializing in cyber security and hacking in the aftermath of significant data breaches affecting both financial institutions and governmental entities.

The Capture the Flag (CTF) competition is an alternative way to find these cyber security specialists. CTF was inspired by the largest open computer security hacking competition, Defcon's CTF. (Cowan, 2003). Capture the Flag (CTF) is a game that combines network security and information concerns. Competitors in a CTF must use specially vulnerable websites or applications to capture flags from other players or the game's creators. (Chapman *et.al.*, 2014; Taylor *et.al.*, 2017; Chicone *et.al.*, 2020; Kaplan *et.al.*, 2022; Chase *et.al.*, 2022; Cole, 2022; Legg *et.al.*, 2023). CTF competitions offer numerous benefits. CTF competitions help teams cultivate critical thinking skills and educate them on how security vulnerabilities occur. Instruction will be provided on incident response, employee participation, and creative thinking. CTFs evaluate the preparedness and response capabilities of an organization, construct a capable response team, and identify security vulnerabilities. (Legg *et.al.*, 2023). In CTF competitions, security expertise is assessed. (Cole, 2022).

Competition versus practice? CTF activities teach teams about security breaches and foster critical thinking. Students and experts can accomplish the assignment online. Technical topics can be challenging for instructors to convey to non-technical students. Gamification uses gaming techniques to motivate students. Capture the Flag (CTF) competitions can introduce students to numerous technical concepts within the computer science curriculum (McDaniel *et.al.*, 2016). Capture the Flag activities, in which students engage in game-like exercises, are a prevalent component of cybersecurity education. Websites, credentials, and unsecured networks are targets. It is unclear how these assignments teach cybersecurity skills, however. Future Capture the Flag competitions should include non-technical elements to combat advanced cyber threats and increase cybersecurity participation (Švábenský *et.al.*, 2021).

CTF is used to teach cyber security to high school students (Legg *et.al.*, 2023). Certain college CTF training courses provide students with cybersecurity experience and knowledge (OConnor *et.al.*, 2022). PicoCTF and TryHackMe are apparently the most popular training platforms (Vykopal *et.al.*, 2020; Abd Rahman *et.al.*, 2022). PicoCTF is an offensive web-based game with 2,000 teams competing for 12 hours. Numerous secondary institutions now teach PicoCTF (Chapman *et.al.*, 2014). GenCyber programs instruct students on technological topics via capture-the-flag competitions (McDaniel *et.al.*, 2016). The primary objective is to introduce high school students with no prior knowledge to computer security and digital forensics. It introduces children to these topics and encourages continued study after camp (Abd Rahman *et.al.*, 2022).

There are few vocational and high school CTF competitions in Indonesia. CTFs such as BINUS and LKS-SMK are examples (PUSPRENAS, 2021). The DIKNAS CTF Student Skills Contest employed

Jeopardy-style questions, an attacker competition, and a defense competition (Junior *et.al.*, 2022). The ultimate grade was determined by a 70% web-based assessment and a 30% jury decision. In contrast to other CTFs, the 2023 CTF Hacking Olympiad, organized by the Institute of Technology Tangerang Selatan (ITTS), implemented the Jeopardy paradigm (searching for concealed flags) and vulnerability detection in three phases. The Lawrence Livermore National Laboratory Cyber Defenders group has hosted an intern CTF competition for the past eight years. For improved results, they suggested CTF Catalyst Security Challenge Framework architectures (Taylor *et.al.*, 2017).

2 Method

In contrast to many high school CTF competitions, participants in the Indonesian 2023 CTF Hacking Olympiad organized by the Institute of Technology Tangerang Selatan (ITTS), receive four (4) months of training via webinars. Webinars are predominantly demonstrations of attack techniques and practical knowledge, including ethics, with topics such as phishing and social engineering. The webinar titles are,

- CTF for novices
- How to become a bug hunter
- Hacking techniques
- CTF (Capture the Flag) in the Context of Cybersecurity
- The Effectiveness of Open Source Intelligence (OSINT)
- The Top Ten OWASP Applications for Phishing
- Artificial Intelligence Attacks

The workshops have been recorded as unlisted YouTube videos and are available for public viewing, extending beyond the participants of the CTF. The online hacking workshops have garnered significant participation from a large number of individuals, reaching tens of thousands of participants. The workshop participants are geographically dispersed around the nation of Indonesia. It is noteworthy that the individuals who expressed interest in engaging with the tutorial we offered were primarily individuals residing outside of Jakarta. The level of interest among young individuals residing in Jakarta towards the field of hacking appears to be comparatively lower than that observed in regions outside Jakarta. Jakarta, the capital city of Indonesia, exhibits a plethora of amenities and diversions that tend to captivate the attention of young individuals. Conversely, regions situated outside Jakarta are characterized by a dearth of facilities and a strong inclination towards knowledge pursuits, such as hacking and cyber security.

In Capture the Flag (CTF) competitions, various categories of obstacles are present. Jeopardy CTFs, which concentrate on a series of challenges provided by competition administrators, are the most prevalent variety. Another variation is attack-defense, in which teams are tasked with defending vulnerable systems while concurrently assaulting those of opposing teams (Chicone *et.al.*, 2020). The third type incorporates attack, defense, and risk. CTF contestants compete for the highest score by capturing flags during security-themed challenges. These flags are embedded in purposely vulnerable programs or websites, and when a participant successfully completes a challenge, they are awarded a flag, which they then submit to the CTF server (Raman *et.al.*, 2014).

The Indonesian 2023 CTF Hacking Olympiad took place in April over the duration of three sessions of four days each, with two sessions of CTF Jeopardy in the preliminary rounds, and one final session of CTF Write Up (narration and video presentation on YouTube) in late April 2023, followed by an interview. Fifty percent of competitors dropped out because they were unable to or did not do the work during the first and second competition sessions, indicating that the competition process is quite difficult. Forty (40) of the top competitors competed in session three (3), which required them to compose CTF

essays and YouTube presentations in response to extremely challenging questions. Twenty of the top competitors successfully completed this stage. Interviews were used to determine the top 10 competition champions.

Due to the process orientation of the learning domain, it is difficult to improve the practical cybersecurity training's quality. Process mining has a great deal of potential for transforming events into behavioral graphs, which may offer superior cognitive properties than raw data for understanding user behavior. The entire workflow for the post-training analysis of Capture the Flag games (Hubert *et.al.*, 2022), including data preparation, data mapping, and the application of process models, can be quite instructive.

The server-side CTFd applications are utilized in the CTF hacking competition alongside fairly standard auxiliary tools (OConnor *et.al.*, 2022). The CTFd instance is hosted on a server with an AMD EPYC 7302P 16-Core Processor, 16 GB of total memory, and a peak bandwidth usage of 40 Mbps. The South Tangerang City Government ICT provides a Nutanix server with a total of four core processors and sixteen gigabytes of random access memory. At the grand final session, CTFd is used to manage the attack by the forty finalists.

3 Result and Discussion



Figure 1: Distribution map of 2023 CTF participants

The primary objective of Capture the Flag (CTF) events is to cultivate individual player engagement, in contrast to participation that is centered around teams. The event consisted of a cohort of 206 high school students and 43 individuals from the general public, mainly 18-year-olds, originating from various locations around Indonesia. The graphical representation of the distribution of involvement is illustrated in Figure 1. It is noteworthy that a significant proportion of young individuals involved in hacking operations in Indonesia are mostly focused on Java Island, with a modest presence found on Sumatra Island, specifically in West Sumatra and the Bangka Belitung Islands. Each province exhibits a substantial number of individuals who have registered within their primary target areas. In regions characterized by low population densities, it is conceivable for a province to have either a solitary participant or no participant at all. The registration rate among individuals hailing from the eastern region of Indonesia exhibited a significant decline.

The profiles of the participants demonstrate a diverse range of distinct characteristics. Approximately 20% of the participants are now enrolled in secondary schools; however, the vast majority of individuals

are actively pursuing their education in vocational institutes. It is noteworthy to mention that a substantial percentage of participants in CTF events originate from the East Java region. The majority of participants originating from East Java were discovered to be enrolled in three vocational schools located in Malang City, namely SMK Telkom Malang, SMKN 6 Malang, and SMKN 8 Malang. The majority of participants in the Central Java region were students from SMKN 7 Semarang and SMKN 2 Surakarta. The educational institutions SMKN 1 Cibinong and SMK Wikrama Bogor have exhibited a significant presence throughout the West Java Province. Despite having undergone a workshop procedure that was free of charge, Over a period of four (4) months, there was a lack of substantial participant presence in Jakarta. Jakarta, being the capital city of Indonesia, provides numerous amenities that engender diversions for the youth residing in the area. The aforementioned factor may contribute to the limited participation of young individuals in Jakarta in the CTF hacking competition.

SMKN 4 Payakumbuh, an educational institution situated in West Sumatra, demonstrates a significant level of influence beyond the confines of Java, particularly within the Sumatra region. SMKN 2 Pangkalpinang and SMKN 1 Batang Angkola hold the positions of second and third place in the rankings, respectively. Therefore, it is apparent that a significant number of young Indonesian hackers primarily inhabit Java Island, demonstrating noteworthy clustering in East Java Province and certain areas of Sumatra Province. A group consisting of at least six female participants and two individuals falling within the age range of junior high school were identified. Regrettably, none of the female participants were able to progress to the final stage.

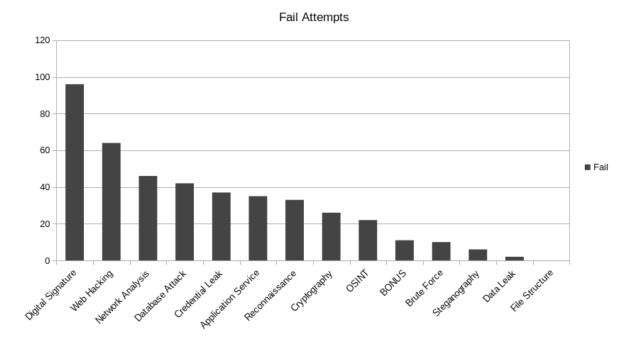


Figure 2: Fail attempts level of various problem category in 2023 CTF

Application Service (Razzaq *et.al.*, 2014; Babiker *et.al.*, 2018; Duo *et.al.*, 2022), Brute Force (Najafabadi *et.al.*, 2014; Hofstede *et. al.*, 2017; Shah *et. al.*, 2023) Credential Leak (Ning *et. al.*, 2016; Pal *et.al.*, 2019), Cryptography (Katz *et.al.*, 2020; Menezes *et.al.*, 2018), Data Leak (Shu *et.al.*, 2015; Papadimitriou *et.al.*, 2010), Database Attack (Hylkema, 2017; Al-Khurafi *et.al.*, 2015), Digital Signature, File Structure, Network Analysis (Hoque *et.al.*, 2014; Hansman *et.al.*, 2005), OSINT (Pastor-Galindo *et.al.*, 2020; Glassman *et.al.*, 2012; Suryotrisongko *et.al.*, 2022; Williams *et.al.*, 2018),

Reconnaissance, Steganography (Kaur *et.al.*, 2022; Mandal *et.al.*, 2022), Web Hacking (Yadav *et.al.*, 2022; Saraswathi *et.al.*, 2022), and bonus questions were developed for this CTF competition. There are a lot of bonus questions, especially in the first elimination round. The bonus questions are questions that are simple to answer and are designed to motivate participants to continue working on the next round of CTF.

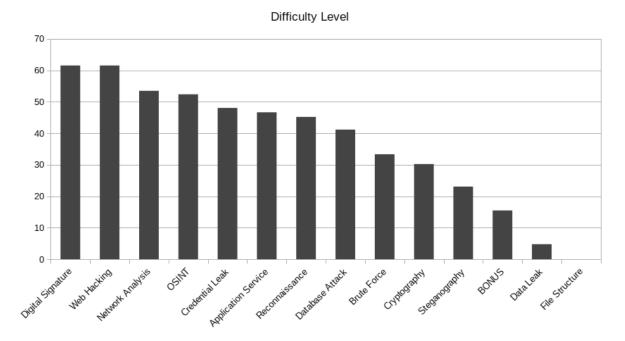


Figure 3: Difficulty level of problem category in 2023 CTF

Based on the analysis of the participants' submissions and the statistical data acquired, it was found that a total of 2455 (40.24%) of the problems were successfully answered. The rate of failed submissions appears to be elevated, with 3646 tries accounting for 59.75% of the total. This observation indicates that the inquiries posed by the jury panel are really within the capabilities of high school students to resolve. Figure 2 illustrates the failure rates associated with the different categories. The data indicates that the prevailing instances of failure are mostly associated with digital signature, online hacking, network analysis, database assault, and credential leak. The file structure, data leak, steganography, and brute force are among the concerns that are quite straightforward to resolve.

In order to enhance the ease of visualization, it is necessary to normalize the failure value in relation to the total number of questions that need to be answered. The approach employed in this study involves the normalization of the level of complexity associated with each category. This normalization process was implemented with the intention of facilitating the evaluation of participants' replies. The formula is expressed by the subsequent equation:

Difficulty Level = Failed Attempts * 100% / (Failed Attempts + Solved Attempts) (1)

Figure 3 shows the relative difficulty level for each type of question category using the simple equation outlined above. During the first preliminary session, bonus problems—which are made up of a few easy tasks—were used to motivate participants to work on CTF. The majority of participants had insignificant difficulties solving operating system, file system, and data leakage problems. This may mean that knowledge of the file system and operating system has already been effectively addressed. It was discovered that network analysis, OSINT, digital signatures, and web hacking were more

challenging to solve. The quality of the students appears to be increased by including materials or modules on cyber security in classes on enhanced networking, online hacking, open source intelligence (OSINT), and cryptography.



Figure 4: Distribution map of 2023 CTF finalists

Figure 4 illustrates the dispersion of participants who successfully advanced to the final round of the Capture the Flag (CTF) game. There are slight variations between the finished map and the collective maps of all participants. One notable observation regarding the CTF 2023 is the absence of finalists hailing from eastern Indonesia or Sumatra. The majority of the applicants originate from the regions of Central and East Java, situated at distances ranging from 200 to 850 kilometers away from Jakarta. It appears that students in Jakarta, the Indonesian capital city, exhibit a lack of interest in acquiring proficiency in CTF (Capture the Flag) and hacking abilities, while possessing enhanced accessibility to resources, information, and educational facilities. Livio Hardi, known by the codename LeonTech, is a tenth-grade student hailing from Berau, Kalimantan Island. Livio has been acquiring knowledge and skills in the field of hacking for a duration of five years, commencing from his enrollment in the sixth grade. Livio is among the initial participants to register for the CTF 2023 competition. Two individuals who have emerged as victors are currently enrolled in the 10th grade. The individuals in question originate from the regions of Kalimantan and the island of Lombok, located in the province of West Nusa Tenggara. Due to their status as the youngest recipients and their non-Javanese background, they exhibit a notable distinction. Hence, it may be inferred that passion plays a significant role in determining individuals' success.

It is evident that these youthful victors have adept hacking skills and comprehended intricate concepts that are not commonly included in collegiate curricula. The majority of winners primarily acquire knowledge independently, with minimal assistance from their educational institution. Many individuals acquire knowledge via online platforms such as YouTube, with a particular emphasis on John Hammond's channel. This channel serves as a valuable resource for learning various Capture the Flag (CTF) techniques. The significance of utilizing CTF practice platforms like PicoCTF (https://PicoCTF.org/) and TryHackMe (https://tryhackme.com/) is emphasized in all of the aforementioned discussions. In addition, several individuals utilize the virtual machine (VM) available

on the website https://www.vulnhub.com/ as an educational resource. It was discovered that a majority of the victors had acquired hacking skills within a timeframe ranging from six months to one year. Individuals with proficiency in coding often exhibit a greater aptitude for acquiring hacking skills. The individual who emerged victorious in the CTF 2023 challenge acquired the skill of hacking within a span of about four (4) months. Prior to this, he had previously acquired proficiency in Python programming and utilized data analysis techniques for machine learning and deep learning throughout his high school tenure.

4 Conclusion

In conclusion, the Capture the Flag (CTF) event conducted in Indonesia showcased a diverse participation profile, involving both high school students and individuals from the general public, predominantly aged 18, from various regions. The distribution of participants revealed a concentration of young hackers on Java Island, particularly in East Java, while areas with low population densities exhibited fewer or no participants. The educational backgrounds of participants varied, with a significant presence from vocational institutes, notably in East Java. Notably, despite Jakarta's status as the capital city, its youth exhibited limited interest in the CTF competition, possibly due to the abundance of distractions and amenities. The gender diversity in the competition was limited, with no female participants progressing to the final stage.

The analysis of problem categories and difficulty levels in the CTF competition indicated a varied performance among participants. While some categories, such as file structure and data leak, were relatively easy for participants to resolve, others like digital signature, online hacking, network analysis, and database assault posed greater challenges. The normalization process revealed that the majority of problems were within the capabilities of high school students, emphasizing the potential for incorporating cybersecurity education into school curricula. The distribution map of finalists highlighted a lack of representation from eastern Indonesia and Sumatra, with most successful participants hailing from Central and East Java. The achievements of younger participants, particularly from non-Javanese backgrounds, underscored the role of passion in determining success in hacking.

The profiles of successful participants revealed that many acquired hacking skills independently, utilizing online platforms and resources such as YouTube channels, CTF practice platforms, and virtual machines. Proficiency in coding, especially in languages like Python, correlated with a higher aptitude for hacking skills. The findings suggest the importance of promoting cybersecurity education and providing accessible resources to nurture the talents and passion of young individuals interested in ethical hacking.

5 Acknowledgements

The author extends appreciation to multiple organizations and entities, such as the National Cyber and Crypto Agency (BSSN), the ICT Division of the South Tangerang City Government, PT. Astra International Tbk., PANDI, Linksys, SalmaNet Internet Service Provider, APTIKOM, ITTS, ICTWATCH, RudexTech, Ethic Ninja, Ganesha Systems PT Ganesha Tradika Pancadaya, Time Excellindo ICT Service Provider, Bintang Raya Computer Shop, and Onno Center International Foundation. This endeavor is anticipated to aid the improvement of Indonesia's human capital in the field of cyber security.

References

- [1] Abd Rahman, N.A., Jojo, H., Hussain, I.A., Khan, Y., & Ismail, N. (2022). Millennial Psychology Towards Hacking Activities. *Journal of Applied Technology and Innovation*, 6(2), 22-28.
- [2] Al-Khurafi, O.B., & Al-Ahmad, M.A. (2015). Survey of web application vulnerability attacks. *In 4th International Conference on Advanced Computer Science Applications and Technologies* (ACSAT), 154-158.
- [3] Babiker, M., Karaarslan, E., & Hoscan, Y. (2018). Web application attack detection and forensics: A survey. *In 6th international symposium on digital forensic and security (ISDFS)*, 1-6.
- [4] Chapman, P., Burket, J., & Brumley, D. (2014). {PicoCTF}: A {Game-Based} computer security competition for high school students. *In USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*, 1-10.
- [5] Chase, J.D., & Uppuluri, P. (2022). High School Cybersecurity? Challenge Accepted–Radford University's RUSecure CTF Contest for High School Students. *In Journal of The Colloquium for Information Systems Security Education*, *9*(1), 1-6.
- [6] Chicone, R.G., & Ferebee, S. (2020). A comparison study of two cybersecurity learning systems: facebook's open-source capture the flag and CTFd. *Issues in Information Systems*, 21(1), 202-212.
- [7] Cole, S.V. (2022). Impact of Capture the Flag (CTF)-style vs. Traditional Exercises in an Introductory Computer Security Class. In Proceedings of the 27th ACM Conference on Innovation and Technology in Computer Science Education, 1, 470-476.
- [8] Cowan, C., Arnold, S., Beattie, S., Wright, C., & Viega, J. (2003). Defcon capture the flag: Defending vulnerable code from intense attack. *In Proceedings DARPA information survivability conference and exposition*, *1*, 120-129.
- [9] Duo, W., Zhou, M., & Abusorrah, A. (2022). A survey of cyber attacks on cyber physical systems: Recent advances and challenges. *IEEE/CAA Journal of Automatica Sinica*, 9(5), 784-800.
- [10] Glassman, M., & Kang, M.J. (2012). Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT). *Computers in Human Behavior*, 28(2), 673-682.
- [11] Hansman, S., & Hunt, R. (2005). A taxonomy of network and computer attacks. *Computers & Security*, 24(1), 31-43.
- [12] Hofstede, R., Jonker, M., Sperotto, A., & Pras, A. (2017). Flow-based web application brute-force attack and compromise detection. *Journal of network and systems management*, 25, 735-758.
- [13] Hoque, N., Bhuyan, M.H., Baishya, R.C., Bhattacharyya, D.K., & Kalita, J.K. (2014). Network attacks: Taxonomy, tools and systems. *Journal of Network and Computer Applications*, 40, 307-324.
- [14] Huang, Y.L., & Leu, F.Y. (2011). Constructing a Secure Point-to-Point Wireless Environment by Integrating Diffie-Hellman PKDS RSA and Stream Ciphering for Users Known to Each Other. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 2*(3), 96-107.
- [15] Hubert, R., Bánáti, A., Erdődi, L., & Fleiner, R. (2022). Strengthening Database Security with Capture the Flag Exercises. In IEEE 26th International Conference on Intelligent Engineering Systems (INES), 000137-000142.
- [16] Hylkema, M. (2009). A survey of database inference attack prevention methods. *Educational Technology Research*.

- [17] Junior, A.O., Funchal, G., Queiroz, J., Loureiro, J., Pedrosa, T., Parra, J., & Leitao, P. (2022). Learning Cybersecurity in IoT-based Applications through a Capture the Flag Competition. *In IEEE 20th International Conference on Industrial Informatics (INDIN)*, 560-565.
- [18] Kaplan, Z., Zhang, N., & Cole, S.V. (2022). A Capture the Flag (CTF) Platform and Exercises or an Intro to Computer Security Class. In Proceedings of the 27th ACM Conference on Innovation and Technology in Computer Science Education, 597-598.
- [19] Katz, J., & Lindell, Y. (2020). *Introduction to Modern Cryptography: 3rd ed.* Chapman and hall/CRC.
- [20] Kaur, S., Singh, S., Kaur, M., & Lee, H.N. (2022). A systematic review of computational image steganography approaches. Archives of Computational Methods in Engineering, 29(7), 4775-4797.
- [21] KUK (2023) Hacker breaches data of 34 million Indonesian passports, Asia News Network. https://asianews.network/hacker-breaches-data-of-34-million-indonesian-passports/
- [22] Legg, P., Mills, A., & Johnson, I. (2023). Teaching Offensive and Defensive Cyber Security in Schools using a Raspberry Pi Cyber Range. In Journal of the Colloquium for Information Systems Security Education, 10(1), 1-9.
- [23] Mandal, P.C., Mukherjee, I., Paul, G., & Chatterji, B.N. (2022). Digital image steganography: A literature survey. *Information sciences*, *609*, 1451-1488.
- [24] McDaniel, L., Talvi, E., & Hay, B. (2016). Capture the flag as cyber security introduction. *In* 49th Hawaii international conference on system sciences (HICSS), 5479-5486.
- [25] Menezes, A.J., Van Oorschot, P.C., & Vanstone, S.A. (2018). *Handbook of applied cryptography*. CRC press.
- [26] Najafabadi, M.M., Khoshgoftaar, T.M., Kemp, C., Seliya, N., & Zuech, R. (2014). Machine learning for detecting brute force attacks at the network level. *In IEEE International Conference* on Bioinformatics and Bioengineering, 379-385.
- [27] Ning, J., Cao, Z., Dong, X., & Wei, L. (2016). White-box traceable CP-ABE for cloud storage service: How to catch people leaking their access credentials effectively. *IEEE Transactions on Dependable and Secure Computing*, 15(5), 883-897.
- [28] Nugraha, R.M. (2021). 6 major data breach cases in Indonesia in the past 1.5 years, Tempo.
- [29] OConnor, T.J., Mann, C., Petersen, T., Thomas, I., & Stricklan, C. (2022). Toward an automatic exploit generation competition for an undergraduate binary reverse engineering course. In Proceedings of the 27th ACM Conference on Innovation and Technology in Computer Science Education, 442-448.
- [30] Pal, B., Daniel, T., Chatterjee, R., & Ristenpart, T. (2019). Beyond credential stuffing: Password similarity models using neural networks. *In IEEE Symposium on Security and Privacy (SP)*, 417-434.
- [31] Papadimitriou, P., & Garcia-Molina, H. (2010). Data leakage detection. *IEEE Transactions on knowledge and data engineering*, 23(1), 51-63.
- [32] Pastor-Galindo, J., Nespoli, P., Mármol, F.G., & Pérez, G.M. (2020). The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. *IEEE Access*, *8*, 10282-10304.
- [33] PUSPRENAS (2021) Technical Description: XXIX National Level Student Competition (LKS) 2021, National Achievement Center.
- [34] Raman, R., Sunny, S., Pavithran, V., & Achuthan, K. (2014, April). Framework for evaluating Capture The Flag (CTF) security competitions. *In International Conference for Convergence* for Technology-2014, 1-5.
- [35] Razzaq, A., Latif, K., Ahmad, H.F., Hur, A., Anwar, Z., & Bloodsworth, P.C. (2014). Semantic security against web application attacks. *Information Sciences*, 254, 19-38.
- [36] Saraswathi, V.R., Ahmed, I.S., Reddy, S.M., Akshay, S., Reddy, V.M., & Reddy, S.M. (2022). Automation of recon process for ethical hackers. *In International Conference for Advancement in Technology (ICONAT)*, 1-6.

- [37] Shah, P.G., & Ayoade, J. (2023). An Empirical Study of Brute Force Attack on Wordpress Website. *In 5th International Conference on Smart Systems and Inventive Technology (ICSSIT)*, 659-662.
- [38] Shu, X., Zhang, J., Yao, D.D., & Feng, W.C. (2015). Fast detection of transformed data leaks. *IEEE Transactions on Information Forensics and Security*, *11*(3), 528-542.
- [39] Sulaiman, S. (2023) Indonesia's biggest Islamic Bank says customer data safe amid reports of Breach, Reuters. https://www.reuters.com/business/finance/indonesias-biggest-islamic-banksays-customer-data-safe-amid-reports-breach-2023-05-16/
- [40] Suryotrisongko, H., Musashi, Y., Tsuneda, A., & Sugitani, K. (2022). Robust botnet DGA detection: Blending XAI and OSINT for cyber threat intelligence sharing. *IEEE Access*, 10, 34613-34624.
- [41] Švábenský, V., Čeleda, P., Vykopal, J., & Brišáková, S. (2021). Cybersecurity knowledge and skills taught in capture the flag challenges. *Computers & Security*, 102, 102154.
- [42] Taylor, C., Arias, P., Klopchic, J., Matarazzo, C., & Dube, E. (2017). {CTF} : {State-of-the-Art} and Building the Next Generation. *In USENIX Workshop on Advances in Security Education (ASE 17)*, 1-11.
- [43] Vykopal, J., Švábenský, V., & Chang, E.C. (2020). Benefits and pitfalls of using capture the flag games in university courses. *In Proceedings of the 51st ACM Technical Symposium on Computer Science Education*, 752-758.
- [44] Williams, H.J., & Blum, I. (2018). Defining second generation open source intelligence (OSINT) for the defense enterprise. Santa Monica: Rand Corporation.
- [45] Yadav, K., & Agrawal, R. (2022). Ethical Hacking and Web Security: Approach Interpretation. In Second International Conference on Artificial Intelligence and Smart Energy (ICAIS), 1382-1384.

Authors Profile



Onno W. Purbo, Ph.D. holds a Ph.D. in Electrical Engineering from the University of Waterloo, Canada, and is a copy leftist, educator, and ICT evangelist. He has published more than 50 books. He led the first Internet connection at the Institute of Technology in Bandung (ITB) in 1993–2000 and built the first Indonesian education network. Since 2021, he has been active as a senior lecturer and vice rector at the Institute of Technology Tangerang Selatan (ITTS). Faculty Computer Science, Institute of Technology Tangerang Selatan, Indonesia.



Prasetyo Purnomo, M.Kom is an academician and specialist in cyber security. After earning his master's degree in information technology from AMIKOM University in 2017, he began working as a network engineer for the company. His thesis on the "Password Cracking Method" led him to participate in various cyber security competitions and made him an expert in the field. His duties vary from teaching students to training professionals, building network infrastructures, and maintaining system security. Faculty Computer Science, Institute of Technology Tangerang Selatan, Indonesia.



Dimaz Arno Prasetio, M.Kom. balances his role as CEO at Ethic Ninja with academic duties as a lecturer. His work involves practical applications of cybersecurity in the industry and guiding students in understanding the complexities of Infosec at Institut Teknologi Tangerang Selatan. Faculty Computer Science, Institute of Technology Tangerang Selatan, Indonesia.



Agung Budi Prasetio, Ph.D. Completed Education Ph.D in 2023. His interest is research on Cybersecurity, Data Science, Social Science and Good Governance. And now my jobs are Lecture, Software Entrepreneur, and Expertise Government. Faculty Computer Science, Institute of Technology Tangerang Selatan, Indonesia.



Dr. Tubagus Asep Nurdin received his Doctoral degree in 2023. He currently serves as the Head of the Department of Communication and Informatics in South Tangerang City. His expertise is in the fields of Information Technology (IT) and education and one of the founders of the South Tangerang Institute of Technology.