Journal of Engineering Education Transformations ,
Volume 38, No. 4 , April 2025 , ISSN 2349-2473, eISSN 2394-1707

10.16920/jeet/2024/v38i4/25094

Capture the Flag (CTF) Implementation in The Informatics Engineering Study Program Indonesia Defense University

Dudi Gurnadi Kartasasmita [1], Fauzia Gustarina Cempaka Timur [2]

[1, 2] Asymmetric Warfare Program Study, Indonesia Defence University
[1] dudi@airputih.or.id
[2] fg.cempaka@idu.ac.id

Abstract—The evolution of the internet of things and big data has increased cyber threats, making cybersecurity a critical issue. Simultaneously, cybersecurity personnel competencies are required to protect digital assets from cyber threats. Obtaining personnel competency in cybersecurity is possible through the university, particularly through the Informatics Engineering Study Program. Nowadays, there is a cybersecurity competition called Capture the Flag that takes place on the internet (CTF). One of the CTF's goals is to improve personnel cybersecurity competency. The study employs a qualitative descriptive approach to provide an overview of CTF implementation as a strategy in the Informatics Engineering study program at the Indonesia Defense University (IDU). To present a comprehensive illustration of Capture the Flag (CTF), the IDU Informatics Engineering requires a dedicated server for virtualization and scoreboard. This study also entails software like Proxmox VE, VirtualBox, and Kali Linux. Alongside hardware and software requirements, an isolated network is essential to prevent disruptions to the existing computer network due to CTF implementation. In addition, skillful instructors well-versed in cybersecurity skills are crucial, playing a significant role in preparing relevant teaching materials. Furthermore, because cybersecurity is a broad scientific domain, variations of CTF scenarios are required to follow the trend of vulnerabilities. Thus, students will be motivated to study various vulnerabilities in cybersecurity.

Keywords— capture the flag; cybersecurity; informatics engineering study program; indonesia defense university.

1. Introduction

The development of the Internet of Things and big data is currently growing rapidly. This is marked by the increasing number of various digital devices used in various aspects of life, and almost all these digital devices are connected to the internet (Puslitbang Kominfo, 2020). Of course, when all these small devices are connected to the internet, it is certain that various types of data will flow from one device to another. At that time, it is certain that the protection of personal data will become an important issue (Puslitbang Kominfo, 2019). Ultimately, this will lead to increasing cyber threats, making cybersecurity a very important issue.

In Indonesia itself, news has often spread about the leakage of personal data or even the destruction of

Dudi Gurnadi Kartasasmita
Asymmetric Warfare Program Study,
Indonesia Defence University
fg.cempaka@idu.ac.id

public services by irresponsible people. The State Cyber and Password Agency (BSSN) monitors Indonesian internet traffic 24/7 (twenty-four hours a day, seven days a week). According to monitoring data, there were 976,429,996 (nine hundred seventy-six million four hundred twenty-nine thousand nine hundred ninety-six) cyber-attacks directed at Indonesia in 2022with the highest Indonesian internet connection traffic was achieved in January 2022 with a total number of attacks reaching 272,962,734 (two hundred seventy-two million nine hundred sixty-two thousand seven hundred thirty-four) (BSSN, 2023). Not all these attacks became incidents, but nonetheless, they endangered Indonesia (Rizki & Cempaka Timur, 2021).

Meanwhile, Nippon Telegraph and Telephone Corporate (NTT) published the 2021 Global Threat Intelligence Report. NTT (NTT, 2021) stated that the financial industry was attacked the most by 23% during 2020. The biggest attack was 42%, and it was dominated by the "application specific attack" category, while the "web application attack" category accounted for 31% of all attacks on the financial sector. More details can be seen in Table 1.

Referring to Table 1 above, AS is an Application-Specific, WA is a Web-Application, RC is a Reconnaissance, KBS is a Known Bad Source, BF is a Brute Foce. Web-application attacks and application-specific attacks are the most frequent attacks in various industrial sectors. Based on this, vulnerabilities often occur in the applications or websites that are used. On that ground, it can be concluded that one of the most important factors in the development of technology or information systems is the cybersecurity factor (Ericka & Prakasa, 2020).

Table 1 :
Percentage of Attacks And Types of Attacks on Industrial Sectors Globally (ntt, 2021)

Industry and percent of global attacks	Industrial Attack Types Percentage
Finance (23%)	AS (42%) WA (31%) RC (12%)
Manufacture Industry (22%)	AS (49%) RC (24%) WA (20%)
Health Industry (17%)	WA (59%) AS (38%) KBS (20%)
Professional Industry (10%)	RC (53%) AS (13%) BF (12%)
Education (6%)	WA (24%) AS (22%) RC (21%)

Cybersecurity can be defined as all activities, processes, and technologies used to perform security and protection covering 3 factors, namely: confidentiality, integrity, and availability (Dhillon & Backhouse, 2001). This definition proves that information is an asset for an organization, and therefore it must be protected from all threats, both internally and externally. To ensure that all information technology infrastructure and assets are always protected, personnel who have competence in cybersecurity are required (Gultom & Alrianto, 2016).

Cybersecurity basically relies heavily on three components, namely technology, processes, and personnel (Schneier, 1999). Schneier explained that the three components are interrelated and inseparable. In other words, no matter how good the technology and management processes are, if they are handled by personnel who do not have competence in cybersecurity, the protection of digital assets will be in vain (Kartasasmita et al., 2023). It can be concluded that the availability of personnel plays the most important role in cybersecurity (von Solms & van Niekerk, 2013).

A. Gamification & Capture the Flag

Cybersecurity is a very broad domain of knowledge with many branches of science (Spafford, 1998), but it is usually associated with the ability to attack and defend in cyberspace. Having the ability to attack and defend in cyberspace is not adequate if done only through a theoretical explanation. It also requires an appropriate practice medium to describe the actual conditions (W Liu et al., 2019). For this reason, the method that is often used in studying cybersecurity is gamification (Boopathi et al., 2015). Gamification is a strategy that aims to improve systems, services, management, and activities through experiences created in the form of games, with the goal of motivating and involving users (Hamari, 2019). One form of gamification in cybersecurity is Capture the Flag or referred to as CTF.

A CTF is a game played by several teams where each team consists of several personnel with the aim of training the capabilities of personnel in cybersecurity by solving various problems on a platform. (Švábenský et al., 2021). In the world of cybersecurity, there is an adage that "the best defense is a good offense" (W. W. Abbot & Founders Online, 199 C.E.). This adage can be interpreted if the best step in defense is to carry out a well-planned attack. CTF provides an opportunity for all participants to legally carry out attacks on a service that was designed from the start to have security holes. From the attack process carried out, participants will be able to understand the concept of a good cyber defense in real conditions (Mansurov, 2016).

To get an application or service that can be attacked, the application or service will be built using the concept of "vulnerable by design". Vulnerable by design is a concept used to provide applications or services that were originally designed to have vulnerabilities so that they can be exploited (Román Muñoz et al., 2018). This concept allows participants to learn the process of attack, defense, and analysis in cybersecurity according to the conditions that have been set and desired from the start.

B. CTF Development

In 1993, DEF CON (the world's largest hacker conference) held its first conference (DEFCON, 2021b). At this conference, DEF CON introduced cybersecurity training in CTF format. At the 4th conference in 1996, DEF CON started the competition for cybersecurity using the CTF format. At that time, the CTF format as a game in cybersecurity was not widely known on the internet. CTF was only contested at the DEF CON conference using an offline format (DEFCON, 2021a).

CTF started appearing on the internet in 2003 when the website hackthissite.org introduced a 15-level web security game, and eventually, many internet users played all the web security games on the website (HackThisSite, 2021). This step by hackthissite.org has finally begun to be followed by various cybersecurity communities and organizations to date. With the increasing number of CTF competitions being held around the world, this has led some people to create a website called ctftime.org in 2011. Ctftime.org has become the main website that distributes information about various CTF competitions around the world until now (CTFTIME, 2021a). Many cybersecurity practitioners, including hacker groups, are involved and take part in the CTF competition posted on the site. In recent years, the CTF has attracted much interest from the cybersecurity community (Chothia & Novakovic, 2015) and is often used as an annual competition event at various cybersecurity conferences taking place around the world.

Cybersecurity has been active in Indonesia since 2007, precisely on May 4, 2007, when the Ministry of Communication and Information of the Republic of Indonesia through Ministerial Regulation Number 26/PER/M.KOMINFO/5/2007 formed the Indonesia Security Incident Response Team on Internet and Infrastructure/Coordination Center (ID-SIRTII/CC) with the aim of supervising the security of telecommunication networks based on internet protocols (Kemenkominfo, 2007). One of the work programs of ID-SIRTII/CC is to conduct security awareness training for the public, including groups of practitioners and observers of cybersecurity in Indonesia (ID-SIRTII, 2021). This work program was translated by ID-SIRTII/CC, one of which was by holding a CTF competition called Cyber Jawara (cyberjawara.id, 2021).

The Cyber Jawara CTF competition was first held by ID-SIRTII/CC in 2012, and since then, the CTF competition has started to bloom and develop in Indonesia. This can be seen by the increasing participation of the community, private sector, military, and education starting to participate in holding CTF competitions for the public. It was recorded that there were several CTF competitions on a national scale, such as the Cyber Defense Competition (CDC) organized by the Ministry of Defense Data and Information Center (Kemhan, 2016), and the National Student Show in Information and Communication Technology (Gemastik) organized by the Ministry of Education, Culture, Research, and Technology (Gemastik, 2021). The Army Cyber Community Competition (KKS TNI-AD) is organized by the Indonesian Army Cyber and Crypto Center (Pussansiad) (KKS TNI-AD, 2021) and various other CTF competitions.

Basically, the CTF competition aims to raise awareness of educational and ethical enhancement in information security through a series of cyber competitions covering forensics, ethical hacking, and defense. In other words, since ID-SIRTII was formed and the CTF competition began to be held for the

public, the issue of cybersecurity has begun to receive wider attention and recognition in Indonesia.

Although cybersecurity CTF competitions have often been held in Indonesia, there are not many, or even no studies, that examine the potential use of CTF in academia. This study will discuss the potential application of CTF in the education curriculum in the Informatics Engineering study program in Indonesia in general and at the Indonesia Defense University (IDU) in particular.

Therefore, the formulation of the problem to be answered in this study is:

1) Has the IDU Informatics Engineering study program implemented CTF in learning cybersecurity courses?

2) What is the right strategy to implement CTF as part of cybersecurity learning in the Informatics Engineering study program at IDU?

2. Research Methods

This study was conducted using a descriptive approach with the aim of providing an overview of the application of CTF in the Informatics Engineering study program at Indonesia Defense University as a strategy for studying cybersecurity. The data was collected using a literature study and then examined objectively, as it is in accordance with the observations associated with the literature study. Research data is obtained from primary or secondary sources.

Primary data was obtained directly by the researcher using interview and observation techniques, while secondary data was obtained from various articles, books, and other relevant references related to the object of research being studied. All the data from this research is presented in the form of diagrams and tables adapted to the object of research.

3. Results And Discussion

Referring to the universal concept of Indonesia's national defense, the availability of competent personnel in cybersecurity is basically a form of implementing defense in cyberspace, and this is the responsibility of all parties, including the government, military, education, and industrial sectors (Aptika, 2016).

In terms of education, the fulfillment of personnel needs in cybersecurity can be met at the university level, for example, through the Informatics Engineering Study Program. For example, one of the competencies that students in the Informatics Engineering study program must possess is the ability to have knowledge, expertise, and abilities in cybersecurity, cyber warfare, network centric warfare, C4ISR, cloud computing, and the Internet of Things (UNHAN, 2020).

This study focuses on implementing CTF in the Informatics Engineering study program of IDU, considering that IDU has just opened this major in 2020 and the purpose of its establishment is to provide human resources that are ready to use and have competence in cyber defense. However, the results of this study can also be applied to other fields of Informatics Engineering. Obviously, some modifications are required to be able to implement the findings of this study, particularly in the teaching materials and curriculum in the major in question.

According to Yurcik and Doss (2001), there are several approaches that can be taken in the cybersecurity teaching and learning process, such as the traditional lecture approach, the writer's scribe approach, the expert/mentor approach, the tutorial approach, the project approach, the research/teaching synergy approach, and the laboratory attack/defense isolated approach. Currently, IDU's Informatics Engineering study program is still using the traditional lecture approach mechanism. The traditional lecture approach is the most frequently used teaching and learning method in cybersecurity.

Students will obtain cybersecurity materials through the instructor's explanation and continue with assignments like middle semester examination and final sSemester examination, which must be done by the students based on the material that has been taught. Even if there is practice, it is usually still theoretical and it is not close to the actual conditions experienced by the industry. This method is often criticized on the grounds that it teaches students to be passive and inactive in understanding the real problem of cybersecurity in cyberspace (Yurcik & Doss, 2001).

The Informatics Engineering Study Program of IDU already uses e-learning as a learning medium and has a cyber laboratory for practice but has not yet implemented CTF as a cybersecurity teaching and learning process. Students and lecturers in the

Informatics Engineering study program at IDU already know and understand the concept of CTF but have not implemented it and have never participated in CTF competitions, which are often held at the national or international level. The instructor has also never made teaching materials using the concept of vulnerable by design. However, currently there is a plan from the IDU Informatics Engineering study program to include students in CTF competitions at the national or international level.

For this reason, the strategy that must be prepared by the Informatics Engineering study program at IDU to apply the CTF concept in cybersecurity learning must pay attention to several factors, such as:

A. Hardware

The application of the CTF concept requires hardware that acts as a server as well as a client. From the results of the field study, it is known that the computer specifications in the cyber laboratory are more than sufficient to be used as a cybersecurity learning tool for students. However, the availability of the server that will be used as an attack target is not yet available. This server will need to be configured using virtualization techniques such as KVM and dockerized (Perrone & Romano, 2017) so that each student can get a virtual computer that they can learn from.

A minimum of two hardware devices are required to act as servers. The first server functions as a scoreboard to which the CTFd application will be installed. The second server will function as a server that runs virtual machines which will later become teaching materials and will run on top of virtualization. This second server will have the Proxmox Virtual Environment (PVE) software installed.

B. Software

In addition to the hardware, the implementation of CTF also requires the availability of software on the server and client sides. The software that will be installed on student computers is the Kali Linux software.

Kali Linux is an operating system based on Debian Linux which was developed by Offensive Security and has more than 300 software with functions that are usually used in computer network penetration (Kali.org, 2021). Kali Linux will be activated on the computer in the cyber lab. Students will use virtualization techniques in running Kali Linux and the virtualization software that will be used in this study is VirtualBox.

VirtualBox is a virtualization software that can create virtual environments for Operating Systems. In simple terms, VirtualBox is tasked with separating and creating a new space for the operating system to be installed on top of Virtualbox (VirtualBox.org, 2021). By using VirtualBox, the cyber laboratory can still be used to practice other courses.

Apart from Kali Linux and VirtualBox, a scoreboard application such as CTFd is also needed. CTFd is a software that focuses on ease of use for CTF competitions. CTFd is a web application which is responsible for providing an interface for participants, which gives access to their respective assignments via a web browser. The CTFd framework is a framework that is usually used to carry out CTF competitions with the Jeopardy format (Amrie et al., 2021)

This application is used to record the teams that will be involved in the CTF as well as function as a place to send answers or read the narration of the questions given. Some of these scoreboard applications are paid and some are open. However, there is also a scoreboard application whose format is like that of e-learning applications in general.

For each team to have a virtual machine that can be studied or attacked, a software called Proxmox Virtual Environment (PVE) is needed. PVE is a Debian-based Operating System that functions as a virtualization management platform with a web interface for virtual equipment operations and management (Proxmox.com, 2021). PVE will serve to prepare virtual machines for each team which will later be used as teaching materials.

C. CTF Deployment Architecture

Considering that this CTF will be applied to cyber laboratories that already exist at the Indonesia Defense University, it is necessary to develop a network that applies to CTF services. This needs to be done, considering that this network will later be used by students in simulating attacks and has destructive power so that it has the potential to disrupt the network. To minimize errors in carrying out attacks, this network needs to be separated from the existing

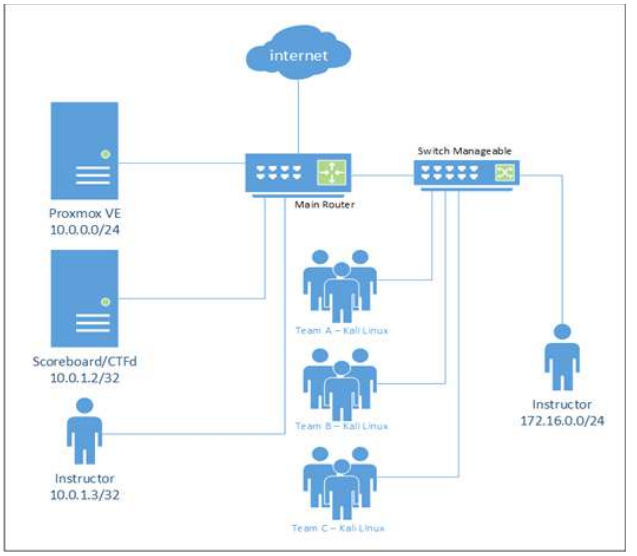

Fig 1: CTF Deployment Architecture

network.

Hardware, software, and network configuration in implementing CTF in the Informatics Engineering study program of IDU can be seen in Figure 1.

D. Instructors

When CTF is implemented, instructors are not only required to master cybersecurity theory but also have cybersecurity competence, especially in making CTF teaching materials. Instructors must be able to give examples of how the exploitation process can occur and explain how the attack process occurs at each stage. For this reason, instructors are strongly advised to have a Certified Ethical Hacker – CEH (EC-Council, 2021) or Offensive Security Certified Professional – OSCP (Offensive-security, 2021) certification.

As stated by Gultom and Alrianto (2016) that personnel are the main element in cybersecurity hence when CTF is implemented, the instructors must have sufficient competence in cybersecurity, so that the learning materials made by instructors will always evolve and to be kept updated.

E. Teaching Materials and Curriculum

Teaching Materials and CTF Curriculum consists of three types of scenarios including Attack-Defense, Jeopardy, and Mixed (Vigna, 2003). In the Jeopardy scenario, participants will be given several questions and asked to answer. For each question that is successfully answered, the participant will get a certain value and the participant who gets the highest score is the winner. The Attack-Defense scenario is implemented by dividing the participants into several teams. Each team plays a role to carry out attacks on other participants' systems and at the same time they also defend their own systems from being attacked by other teams. Each team that successfully carries out an attack is required to get a flag (confidential information). The Mixed scenario is a combination of the two (CTFTIME, 2021b).

Teaching materials can be developed through a variety of ready-to-use materials such as those provided by vulnhub.com (Vulnhub, 2021) or you can build your own referring to the vulnerable by design concept (Román Muñoz et al., 2018) using Common Vulnerabilities and Exposures (CVE) which is routinely released by MITRE (CVE, 2021). Espinha Gasiba et al (2019) stated that the topics most frequently addressed in CTF invariably encompass steganography, cryptography, web application security, mobile security, reverse engineering, forensics, and others. However, this study will solely focus on utilizing instructional materials related to cryptography and web vulnerabilities, covering authentication and software vulnerability. These three teaching materials can be implemented and adapted to cybersecurity courses at the IDU Informatics Engineering using the Jeopardy and Attack-Defence methods as shown in Table 2.

Table 2 :
Class Schedule of Cybersecurity Introduction at Informatics Engineering Study Program

Week	Type	Materials
1	Class	Introduction computer security & computer crime
2	Class	Basic principle in cybersecurity & cyber crime
3	Class	Cryptosystem & Cryptography
4	Class	Cryptography Technique
5	CTF	Cryptography (jeopardy)
6	Class	Malfunction Software
7	Class	Network Security
8	Class	Middle Semester Examination
9	Class	Security on Operating System Level
10	Class	Security on Information system
11	Class	Database Security & Recovery
12	CTF	Authentication (jeopardy)
13	CTF	Web Security (attack -defence)
14	Class	Ethical Hacking
15	Class	Cyber Law & UU ITE
16	Class	Final Semester Examination

F. Often Faced Obstacles

As explained in table 2, the application of CTF in educational institutions as part of a cybersecurity curriculum is certainly not an easy task considering it requires the availability of hardware, software and instructors must also have sufficient technical knowledge and expertise. In addition, periodic maintenance is also required to ensure that all CTF services are in prime condition and ready to be used at any time. Not to mention, the rapid development of security vulnerabilities requires the alertness of instructors to always adjust teaching materials so that they are always evolving and not outdated.

The explanation above is one of the things that makes various CTF services appear in the world as part of cybersecurity learning in educational institutions. It is recorded that there are several services such as hackthebox.eu, immersivelabs.com, offensive-security.com and many others. In Indonesia, there are currently virtlab.id and sekolahhacker.com that provide similar services.

The positive side of using services like this is that the educational institutions do not need to provide hardware, software, or create new teaching materials as usually they have been prepared by the service provider. New teaching materials will usually be provided by the service providers because usually, they will always follow the security development trends. The negative side is that the educational institutions must provide an annual budget on a regular basis to use this service every year; this will, of course, need to be considered, because if it stops midway, it will be detrimental for students who are already using this service to study.

Conclusion

Studying cybersecurity is not an easy thing because in addition to requiring theoretical knowledge about cybersecurity, it also requires technical expertise for the instructor when compiling teaching materials.

However, if this can be done, then CTF can be a means for Informatics Engineering students to study cybersecurity. Of course, to achieve this, curriculum adjustments are needed, including what courses can be combined with the CTF concept.

This study also serves as an opportunity for researchers and lecturers of cybersecurity courses to provide CTF teaching materials for students, in a hope that student competencies can increase and be ready to compete in the cybersecurity industry in Indonesia.

In addition, cybersecurity is a science in which there are many branches. The CTF teaching materials provided by the instructors must be more varied and follow the development of cybersecurity at the world level so that students are also more motivated to learn about various potential security holes in cybersecurity.

Finally, it is necessary to go into more details to ensure whether the application of CTF or the implementation of gamification in cybersecurity courses can improve the understanding of students of the Informatics Engineering study program at IDU.

REFERENCES

Amrie, B. U., Tungadi, E., & Syamsuddin, I. (2021). Teknologi Open Source Untuk Lomba Keamanan Jaringan Berbasis CTF.

Aptika. (2016, March 10). Kebijakan Keamanan dan Pertahanan Siber. Kementerian Komunikasi Dan Informatika RI. https://aptika.kominfo.go.id/2016/03/kebijakan-keamanan-dan-pertahanan-siber/

Boopathi, K., Sreejith, S., & Bithin, A. (2015). Learning cyber security through gamification. Indian Journal of Science and Technology, 8(7), 642–649. https://doi.org/10.17485/ijst/2015/v8i7/67760

BSSN. (2023). LANSKAP KEAMANAN SIBER INDONESIA 2022. https://cloud.bssn.go.id/s/3S5B2ToddAFsiXs

Chothia, T., & Novakovic, C. (2015). An Offline Capture The Flag-Style Virtual Machine and an Assessment of its Value for Cybersecurity Education. http://ictf.cs.ucsb.edu

CTFTIME. (2021a). About CTF Time. CTFTIME.ORG. https://ctftime.org/about/

CTFTIME. (2021b). What is Capture The Flag? CTFTIME.ORG. https://ctftime.org/ctf-wtf/

CVE. (2021). About the CVE Program. CVE.ORG.

https://www.cve.org/About/Overview

cyberjawara.id. (2021). CYBER JAWARA | National Hacking Competition and Seminar. Cyberjawara. https://www.cyberjawara.id/

DEFCON. (2021a). A History of Capture the Flag at DEF CON. DEF CON Hacking Conference. https://defcon.org/html/links/dc-ctf-history.html

DEFCON. (2021b). Frequently asked questions about DEF CON. DEF CON Hacking Conference. https://defcon.org/html/links/dc-faq/dc-faq.html

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. Information Systems Journal, 11(2), 127–153.

EC-Council. (2021). About the Certified Ethical Hacker (Practical). EC-Council Certification. https://cert.eccouncil.org/certified-ethical-hacker-practical.html

Ericka, J., & Prakasa, W. (2020). Peningkatan Keamanan Sistem Informasi Melalui Klasifikasi Serangan Terhadap Sistem Informasi. Jurnal Ilmiah Teknologi Informasi Asia, 14(2).

Espinha Gasiba, T., Beckers, K., Suppan, S., & Rezabek, F. (2019). On the requirements for serious games geared towards software developers in the industry. Proceedings of the IEEE International Conference on Requirements Engineering, 2019-September. https://doi.org/10.1109/RE.2019.00038

Gemastik. (2021). Gemastik. Kementerian Pendidikan, Kebudayaan, Riset, Dan Teknologi. https://gemastik.kemdikbud.go.id/

Gultom, R. A. G., & Alrianto, B. (2016). Enhancing Network Security Environment by Empowering Modeling and Simulation Strategy. Eleventh International Conference on Internet Monitoring and Protection.

HackThisSite. (2021). About The Project. HackThisSite. https://www.hackthissite.org/info/about

Hamari, J. (2019). Gamification. In The Blackwell Encyclopedia of Sociology (pp. 1–3). John Wiley & Sons, Ltd. https://doi.org/10.1002/9781405165518.wbeos1321

ID-SIRTII. (2021). Ruang Lingkup ID-SIRTII/CC. ID-SIRTII. https://idsirtii.or.id/halaman/tentang/ruang-lingkup.html

Kali.org. (2021). Kali Linux. Kali Linux. https://www.kali.org/

Kartasasmita, D. G., Cempaka Timur, F. G., & Reksoprodjo, A. H. S. (2023). Enhancing Competency of Cybersecurity Through Implementation of the "CAPTURE THE FLAG" On College in Indonesia. International Journal Of Humanities Education and Social Sciences (IJHESS), 3(2). https://doi.org/10.55227/ijhess.v3i2.710

Kemenkominfo. (2007). Peraturan Menteri Kominfo Nomor 26 Tahun 2007 Tentang ID-SIRTII.

Kemhan. (2016). Kemhan Adakan Pekan Bela Negara Pertahanan Siber Nusantara. Kementerian Pertahanan. https://www.kemhan.go.id/2016/11/30/kemhan-adakan-pekan-bela-negara-pertahanan-siber-nusantara.html

KKS TNI-AD. (2021). KKS TNI-AD. KKS TNI-AD. https://kks-tniad.id/

Mansurov, A. (2016). A CTF-Based Approach in Information Security Education: An Extracurricular Activity in Teaching Students at Altai State University, Russia. Modern Applied Science, 10(11), 159. https://doi.org/10.5539/mas.v10n11p159

NTT. (2021). 2021 Global Threat Intelligence Report - Technical Report. https://hello.global.ntt/en-us/insights/-/media/87B5306BCCA74075A22C3BAF5B27F828.ashx

Offensive-security. (2021). The official OSCP certification course - now enjoy more flexibility and go at your own pace with a Learn subscription. OFFENSIVE-SECURITY.COM.

https://www.offensive-security.com/pwk-oscp/

Perrone, G., & Romano, S. P. (2017). The docker security playground: A hands-on approach to the study of network security. 2017 Principles, Systems and Applications of IP Telecommunications, IPTComm 2017, 2017-September, 1–8. https://doi.org/10.1109/IPTCOMM.2017.8169747

Proxmox.com. (2021). Proxmox.com. Proxmox. https://www.proxmox.com/en/proxmox-ve

Puslitbang Kominfo. (2019). Strategi Implementasi Regulasi Perlindungan Data Pribadi di Indonesia.

Puslitbang Kominfo. (2020). Studi Kebijakan Penomoran Internet of Things (IoT)/Machine To Machine Communication Pada Jaringan Seluler. Puslitbang Sumber Daya, Perangkat, Dan Penyelenggaraan Pos Dan Informatika Badan Penelitian Dan Pengembangan Sumber Daya Manusia Kementerian Komunikasi Dan Informatika, 3.

Rizki, A., & Cempaka Timur, F. G. (2021). SYNERGY OF MULTI-STAKEHOLDERS IN DEFENDING INDONESIA FROM CYBER THREATS. Journal of Social Political Sciences, 2(4). https://doi.org/10.52166/jsps.v2i4.80

Román Muñoz, F., Sabido Cortes, I. I., & García Villalba, L. J. (2018). Enlargement of vulnerable web applications for testing. Journal of Supercomputing, 74(12), 6598–6617. https://doi.org/10.1007/s11227-017-1981-2

Schneier, B. (1999). Schneier on Security. Schneier on Security. https://www.schneier.com/blog/archives/2013/01/people_process.html

Spafford, E. F. (1998). Teaching the Big Picture of InfoSec. 2nd National Colloquium for Information System Security Education. James Madison University.

Švábenský, V., Čeleda, P., Vykopal, J., & Brišáková, S. (2021). Cybersecurity knowledge and skills taught in capture the flag challenges. Computers and Security, 102. https://doi.org/10.1016/j.cose.2020.102154

UNHAN. (2020, August 17). Prodi Teknik Informatika. Universitas Pertahanan. https://www.idu.ac.id/teknik-informartika/kompetensi-prodi-sarjana-teknik-informatika

Vigna, G. (2003). Teaching Network Security Through Security Live Exercises (Red Team / Blue Team, Capture the Flag, and Treasure Hunt). Third Annual World Conference on Information Security Education (WISE3).

VirtualBox.org. (2021). VirtualBox. VirtualBox. https://www.virtualbox.org/

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. Computers and Security, 38, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Vulnhub. (2021). About Vulnhub. VULNHUB.COM. https://www.vulnhub.com/about/

W Liu, D. Y., Luo, X., Y Leung, A. C., Ho Patrio Chiu, P., Ho Au, M., Kong SAR, H., Wo Tarloff Im, S., M Lam, W. W., & Hong Kong SAR, K. (2019). Virtual Laboratory: Facilitating Teaching and Learning in Cybersecurity for Students with Diverse Disciplines. https://doi.org/10.1109/tale48000.2019.9225863

W. W. Abbot, & Founders Online, N. A. (199 C.E.). From George Washington to John Trumbull, 25 June 1799. The Papers of George Washington, Retirement Series. https://founders.archives.gov/documents/Washington/06-04-02-0120

Yurcik, W., & Doss, D. (2001). Different Approaches in the Teaching of Information Systems Security. The Proceedings of the Information Systems Education Conference (ISECON). http://avirubin.com/courses.html