International Journal Of Humanities Education And Social Sciences ***(IJHESS)*** *E-ISSN:* **2808-1765**
Volume 3, Number 2, October 2023, *Page. 875 -890*
Email : editorijhess@gmail.com

Enhancing Competency of Cybersecurity Through Implementation of the "CAPTURE THE FLAG" On College in Indonesia

Dudi Gurnadi Kartasasmita[1)], **F.G Cempaka Timur** [2)], **Agus H.S Reksoprodjo**[3)]
[1,2,3)] Assymmetric Warfare, Indonesia Defense University, Indonesia

*Corresponding Author
Email: dudi@airputih.or.id

Abstract

Academic institutions encounter several challenges when it comes to determining the most effective pedagogical approaches for enhancing their students' proficiency in the domain of cybersecurity. Conversely, cybersecurity gamification, exemplified by Capture the Flag (CTF) events in the industry, is widely considered an appropriate avenue for fostering cybersecurity learning. This research endeavors to assess the effectiveness of employing gamification as an instructional tool to enhance cybersecurity competency within the college context. The study employs a quantitative research method, adopting an experimental approach with a pre-experimental design. The research findings reveal the following key points 1) the implementation of gamification resulted in a significant enhancement of students' competency in cryptography, web vulnerability, and overall cybersecurity, 2) the gamification experiment demonstrated a stronger influence on enhancing practical skills as opposed to theoretical knowledge, 3) the evaluation of gamification's effectiveness in augmenting cybersecurity competency yielded a medium level (medium-g) of efficacy, reaching 65.91%. Although the medium level of effectiveness was observed in the context of gamification, it should be acknowledged that gamification holds substantial potential for advancing cybersecurity competency. For the attainment of optimal improvement in cybersecurity skills, a consistent and regular integration of gamification is recommended, while concurrently addressing the three pillars of cybersecurity. Furthermore, the utilization of gamification also presents opportunities for cultivating cybersecurity incident handling capabilities and the simulation of cyberwarfare scenarios.

Keywords: Effectiveness, Competency, Gamification, Cybersecurity, College

INTRODUCTION

In the Indonesian Labor Law Number 13/2003 concerning employment, competence is defined as the work capability of everyone, encompassing aspects of knowledge, skills, and attitudes that align with established standards. This notion of competence resonates closely with McAshan's (1979) statement on the subject. According to him, competence denotes the knowledge, skills, and abilities that an individual acquires and internalizes, enabling them to manifest these attributes through cognitive, affective, and psychomotor behaviors.

The explanation provided regarding competence highlights that competent human resources are an absolute necessity and must be possessed by any institution, including those in the field of cybersecurity. In other words, human resources with cybersecurity competence play a crucial role in safeguarding infrastructure and information technology assets from various cyber threats and attacks (von Solms & van Niekerk, 2013). This proposition is rooted in the rationale that the increasing diversity of cyber threats and attacks necessitates the availability of personnel with the requisite competence, as they become the primary key to cybersecurity implementation (Gultom & Alrianto, 2016).

As conveyed by NICE, academic institutions are recognized as one of the most critical components in educating and preparing future cybersecurity experts. Naturally, these institutions face challenges in finding the most effective methods to enhance cybersecurity competence among their students. The goal of improving competence extends beyond the students' ability to

answer theoretical questions; it involves a deeper understanding of real-world cybersecurity occurrences in cyberspace.

Furthermore, during practical exercises and lab work, the tasks assigned to students should emulate real-life scenarios that commonly unfold in cyberspace. This necessitates the development of a suitable medium that can accurately represent the actual cybersecurity landscape present in the digital realm. W. Liu et al. (2019) also emphasized this point in their scholarly article, asserting that cybersecurity education cannot be solely based on theoretical explanations or conventional practical exercises.

In recent years, the cybersecurity industry has witnessed a surge in cybersecurity competitions commonly known as Capture the Flag (CTF). CTF is a cybersecurity game played by multiple teams, each consisting of several members, with the objective of honing their cybersecurity skills by solving various challenges presented on a designated platform (Costa et al., 2020).

Researchers have identified CTF as one of the gamification techniques applied in the field of cybersecurity (Li et al., 2016). Gamification can be defined as a strategy aimed at enhancing systems, services, management, and activities through experiences created in the form of games, with the goal of motivating users and improving their understanding and engagement (Hamari, 2019).

In recent years, there have been several research experiments on gamification in academic institutions. Two notable studies include Hugo Gonzalez et al. (2019) titled "Using a CTF Tournament for Reinforcing Learned Skills in Cybersecurity Course" and W Liu et al. (2019) titled "Virtual Laboratory: Facilitating Teaching and Learning in Cybersecurity for Students with Diverse Discipline." On the other hand, the experiment conducted by W Liu et al. (2019) concluded that gamification, when combined with gradual explanations, can enhance participants' understanding of cybersecurity.

Based on the explanations, the researchers contend that gamification could be a viable solution worth testing to ascertain whether there is an improvement in students' cybersecurity competence in academic institutions following the implementation of gamification. Based on the previously explained background, the research problem is proposed as follows:

a. What is the level of improvement in cryptography competence before and after the gamification experiment in college?
b. What is the level of improvement in web vulnerability competence before and after the gamification experiment in college?
c. What is the overall level of improvement in cybersecurity competence before and after the gamification experiment in college?
d. To what extent does the gamification experiment effectively enhance cybersecurity competence in college?

RESEARCH METHODS

This research employs a quantitative method with an experimental and pre-experimental design. According to Creswell (2013), quantitative research is commonly used to test theories and examine relationships between variables, where the variables are measured using research instruments. William Wiersma (2000) states that educational research labeled as "experimental" typically involves a condition where an independent variable is treated as an experimental variable. The experimental variable (gamification) is intentionally manipulated, modified, altered, or varied by the researcher with the aim of observing the response of the dependent

variable (competence). The researcher also conducted several tests to ensure that all stages of the experiment adhere to academic standards and using some of formulas such as Method of Successive Interval (MSI) (Suliyanto, 2017), Validity Test, Reliability Test (Sitinjak & Sugiarto, 2006), Normality Test (Shapiro-Wilk test) (Shapiro et al., 1968), Paired Sample T-Test (Widiyanto, 2013), Effectiveness Test (N-Gain) (Hake, 1998).
The sample for this study falls under purposive sampling, involving 40 respondents for the validity and reliability test, followed by 46 respondents during the actual experiment.

- **Cryptography Competence:**
  H_{oCR} :There is no significant improvement in cryptography competence before and after the gamification experiment ($Y_{2CR} = Y_{1CR}$).
  H_{1CR} :There is a significant improvement in cryptography competence before and after the gamification experiment ($Y_{2CR} > Y_{1CR}$).
- **Web Vulnerability Competence:**
  H_{oWV} : There is no significant improvement in web vulnerability competence before and after the gamification experiment ($Y_{2WV} = Y_{1WV}$).
  H_{1WV} :There is a significant improvement in web vulnerability competence before and after the gamification experiment ($Y_{2WV} > Y_{1WV}$).
- **Cybersecurity Competence:**
  H_o :There is no significant improvement in cybersecurity competence before and after the gamification experiment ($Y_2 = Y_1$).
  H_1 :There is a significant improvement in cybersecurity competence before and after the gamification experiment ($Y_2 > Y_1$).
- **Effectiveness of Gamification:**

If the hypothesis for cybersecurity competence yields a significance value less than 0.05 (2-tailed), then the effectiveness test can be conducted with the following categories low effectiveness ($G < 0.3$), moderate effectiveness ($0.7 > G \leq 0.3$) and high effectiveness ($G > 0.7$). The hypothesis is that gamification is highly effective in enhancing competence ($G > 0.7$).

RESULT AND DISCUSSION

Validity Test Results

The summary of the validity test calculations for the competence items can be found in Table 1. The validity test calculations were conducted using the JASP software.

Table 1. Summary of Validity Test on Competency Itemss in Questionnaire

Number	*Pearson's r*	*p-value*	Number	*Pearson's r*	*p-value*
1	0.480	0.002 **	21	0.469	0.002 **
2	0.611	< .001 ***	22	0.461	0.003 **
3	0.500	0.001 **	23	0.633	< .001 ***
4	0.659	< .001 ***	24	0.671	< .001 ***
5	0.683	< .001 ***	25	0.561	< .001 ***
6	0.522	< .001 ***	26	0.682	< .001 ***
7	0.642	< .001 ***	27	0.585	< .001 ***
8	0.652	< .001 ***	28	0.506	< .001 ***
9	0.585	< .001 ***	29	0.551	< .001 ***
10	0.576	< .001 ***	30	0.467	0.002 **
11	0.573	< .001 ***	31	0.684	< .001 ***
12	0.717	< .001 ***	32	0.715	< .001 ***

13	0.352	0.026 *	33	0.630	< .001 ***
14	0.689	< .001 ***	34	0.691	< .001 ***
15	0.568	< .001 ***	35	0.718	< .001 ***
16	0.611	< .001 ***	36	0.739	< .001 ***
17	0.629	< .001 ***	37	0.735	< .001 ***
18	0.617	< .001 ***	38	0.633	< .001 ***
19	0.696	< .001 ***	39	0.579	< .001 ***
20	0.656	< .001 ***	40	0.617	< .001 ***

* p < .05, ** p < .01, *** p < .001

The validity test results indicate that the obtained r_{count} values for all competence and gamification questionnaire items are greater than the critical value r_{table}, affirming the validity of each statement.

Table 2. Summary of Validity Test on Gamification Items in Questionnaire

Number	*Pearson's r*	*p-value*	Number	*Pearson's r*	*p-value*
41	0.677	< .001 ***	51	0.802	< .001 ***
42	0.829	< .001 ***	52	0.868	< .001 ***
43	0.766	< .001 ***	53	0.866	< .001 ***
44	0.742	< .001 ***	54	0.887	< .001 ***
45	0.84	< .001 ***	55	0.899	< .001 ***
46	0.833	< .001 ***	56	0.868	< .001 ***
47	0.851	< .001 ***	57	0.874	< .001 ***
48	0.847	< .001 ***	58	0.83	< .001 ***
49	0.808	< .001 ***	59	0.859	< .001 ***
50	0.883	< .001 ***	60	0.862	< .001 ***

* p < .05, ** p < .01, *** p < .001

Result of Reliability Test

The results of the reliability test for the competence questionnaire items and gamification questionnaire items are presented in Table 3. The reliability test for the competence questionnaire items and gamification questionnaire items was performed with the same sample size of 40 respondents and resulted in a Cronbach's alpha value of 0.957 and 0.977.

Table 3. Results of The Reliability Test for The Questionnaire Items

Estimate	Cronbach's α	
	Competence	Gamification
Point estimate	0.957	0.977
95% CI lower bound	0.932	0.964
95% CI upper bound	0.974	0.986

Result of Normality Test

Result of Normality Test for Cryptography Competence

The normality test was conducted for competence in cryptography scores using the JASP software. The results are presented as shown in Figure 1 and Table 4.

Figure 1. Histogram of Cryptography Competence

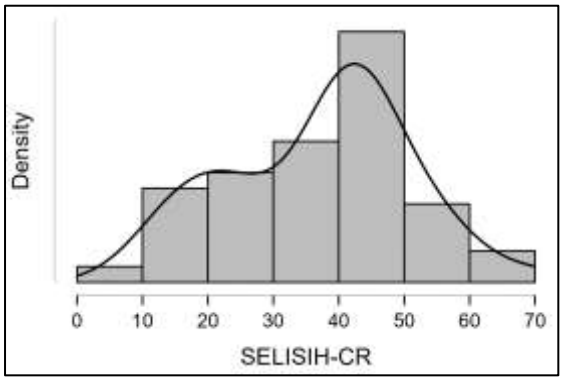

Table 4. Result of Shapiro-Wilk Cryptography

	DIFFERENCE-CR
Valid	46
Mean	36.998
Std. Deviation	14.056
Kurtosis	-0.445
Std. Error of Kurtosis	0.688
Shapiro-Wilk	0.968
P-value of Shapiro-Wilk	0.236

The Shapiro-Wilk normality test resulted in a p-value of 0.236 for the cryptography competence scores. Since the p-value is greater than the significance level (usually 0.05), the data can be considered normally distributed. This supports the assumption of normality for cryptography competence scores and justifies the use of parametric statistical tests in analyzing the data.

Result of Normality Test for Web Vulnerability Competence

Similarly, the normality test was conducted for the web vulnerability competence scores, and the results are shown in Figure 2.

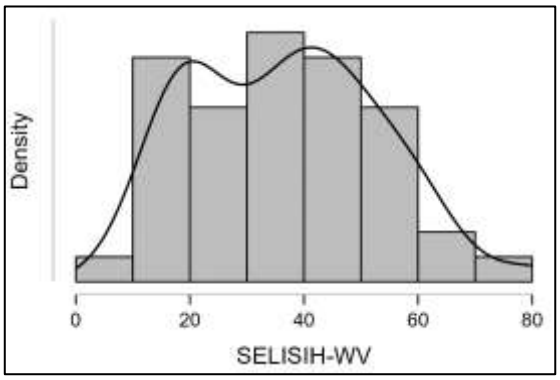

Figure 2. Histogram of Web Vulnerability Competence

Table 5. Result of Shapiro-Wilk Web Vulnerability

	DIFFERENCE-WV
Valid	46
Mean	36.628
Std. Deviation	16.362
Kurtosis	-0.474
Std. Error of Kurtosis	0.688
Shapiro-Wilk	0.963
P-value of Shapiro-Wilk	0.151

While the results of the Shapiro-Wilk test conducted using the JASP software yield a p-value of 0.151, as presented in Table 5, it can be inferred that the distribution of web vulnerability competence follows a normal distribution.

Result of Normality Test Cybersecurity Competence

The normality test of cybersecurity competence scores was conducted using the JASP software, and the results were visualized in the form of a histogram, as shown in Figure 3.

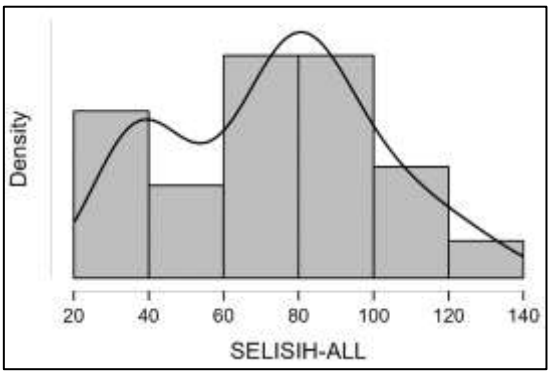

Figure 3. Histogram of Cybersecurity Competence

Table 6. Result of Shapiro-Wilk Cybersecurity

	DIFFERENCE-ALL
Valid	46
Mean	73.626
Std. Deviation	27.478
Kurtosis	-0.740
Std. Error of Kurtosis	0.688
Shapiro-Wilk	0.953
P-value of Shapiro-Wilk	0.063

The outcomes of the normality test conducted using the Shapiro-Wilk method in the JASP software are presented in Table 6. With a p-value of 0.063, it can be concluded that the difference in cybersecurity scores is normally distributed.

Paired Sample T-Test Result

The result of the paired sample t-test conducted using JASP software shows a p-value smaller than 0.001, as presented in table 7.

Table 7. Result of Paired T-Test Cryptography, Web Vulnerability and Cybersecurity

Measure 1		Measure 2	t	df	P
TOTAL-PRE-CR	-	TOTAL-POST-CR	-17.852	45	< .001
TOTAL-PRE-WV	-	TOTAL-POST-WV	-15.183	45	< .001
TOTAL-PRE	-	TOTAL-POST	-18.173	45	< .001

- Test for The Differences in Cryptography Competence
  The result of the test for the difference in cryptography competence, combining knowledge indicators and skill indicators, indicates that the significance value (p-value) is < 0.001.
- Test for The Difference in Web Vulnerability Competence
  The result of the test for the difference in web vulnerability competence, combining knowledge indicators and skill indicators, indicates that the significance value (p-value) is < 0.001.
- Test for The Difference in Cybersecurity Competence
  After conducting paired sample t-tests on cryptography and web vulnerability competencies, the next step is to perform a paired sample t-test on the cybersecurity competence, which is a combination of cryptography and web vulnerability competencies.

The result of the test for the difference in cybersecurity competence, combining cryptography and web vulnerability competencies, indicates that the significance value (p-value) is < 0.001, as seen in table 7. From Table 8, it is evident that the significance value obtained from the paired sample t-test calculation is also < 0.001, which means it is smaller than the predetermined significance level. Therefore, it can be stated that H_{oCR}, H_{oWV}, and H_o are rejected.

Table 8. Summary of Paired T-Test Result and Hypothesis

Num	Hypothesis Description	Hypothesis Test		Result
		H_o Requirements	Paired T-Test	
1	Cryptography Competence (H_{oCR})	$sig < 0.05$	$sig < 0.001$	Reject H_{oCR}
2	Web Vulnerability Competency (H_{oWV})	$sig < 0.05$	$sig < 0.001$	Reject H_{oWV}

3	Cybersecurity Competence ($H_{o)}$	$sig < 0.05$	$sig < 0.001$	Reject H_o

The Effectiveness Test Result

By using Hake's N-Gain formula, the calculation of the gamification effectiveness level is presented in Table 9.

Table 9. Result of Effectiveness Test

Respondent	Total *Pretest* Score	Respondent	Total *Pretest* Score	Respondent	Total *Posttest* Score	Respondent	Total *Posttest* Score
1	196	24	140	1	217	24	242
2	269	25	155	2	274	25	256
3	241	26	175	3	280	26	269
4	243	27	167	4	249	27	168
5	222	28	218	5	232	28	229
6	187	29	237	6	234	29	277
7	192	30	195	7	233	30	260
8	228	31	217	8	280	31	264
9	179	32	208	9	207	32	269
10	226	33	209	10	240	33	279
11	226	34	188	11	233	34	266
12	217	35	225	12	231	35	277
13	213	36	209	13	265	36	270
14	221	37	190	14	252	37	248
15	206	38	145	15	262	38	265
16	215	39	203	16	221	39	261
17	140	40	126	17	231	40	261
18	246	41	168	18	280	41	272
19	213	42	164	19	240	42	261
20	189	43	187	20	280	43	260
21	180	44	210	21	216	44	257
22	123	45	189	22	263	45	253
23	186	46	192	23	239	46	260
***Pretest Score Average* = 197.28**				***Posttest Score Average* = 251.80**			

$$N - Gain = \frac{251.80 - 197.28}{280 - 197.28} = \frac{54.52}{82.72}\ x\ 100\% = 65.91\%$$

The calculation result of N-Gain shows that the average N-Gain value is 65.91% (moderate effectiveness). However, the initial hypothesis that gamification has a high effectiveness in improving cybersecurity competence is not achieved.

Table 10. Average of Differences between Pretest Score and Posttest Score

Num	Description	Score Average		Average	Difference	Ranking
		Pretest	*Posttest*			
1	**Competency of Cryptography**	**102.13**	**126.09**	**114.11**	**23.96**	
	Knowledge Indicator	55.09	64.59	59.84	9.50	IV
	Skill Indicator	47.04	61.50	54.27	14.46	II
2	**Competency of Web Vulnerability**	**95.15**	**125.72**	**110.43**	**30.57**	
	Knowledge Indicator	51.04	64.13	57.59	13.09	III
	Skill Indicator	44.11	61.59	52.85	17.48	I
3	**Competency of Cybersecurity**	**197.28**	**251.80**	**224.54**	**54.52**	

Discussion on Cryptography Competence

From figure 4, it can be observed that the number of respondents who successfully surpassed the passing score is 15 (fifteen), while the other 31 (thirty-one) respondents, although showing an improvement in competence, still did not reach the average competence score required for the passing score.

Meanwhile, according to Table 11, it is evident that 2 (two) respondents agreed, and 29 (twenty-nine) respondents somewhat agreed that there was an improvement in cryptography competence after the implementation of gamification. It is noteworthy that 67.39% of the respondents provided a positive statement regarding the improvement in their cryptography competence.

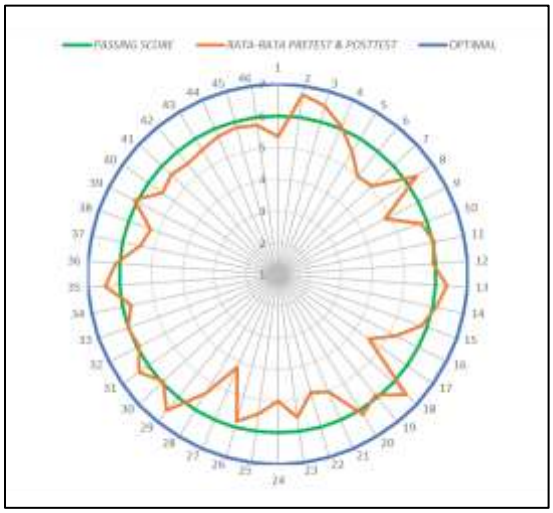

Figure 4. Cryptography Radar Chart

Table 11. Frequency Distribution Cryptography

Category	Interval	% Interval	Frequently	Percentage	Accumulative
Strongly Agree	85.71 s/d 120	≥ 85.71	0	0.00%	0.00%
Agree	51.43 s/d 85.71	71.43-85.71	2	4.35%	4.35%
Somewhat Agree	17.14 s/d 51.43	57.14-71.43	29	63.04%	67.39%
Neutral	-17.14 s/d 17.14	42.86-57.14	15	32.61%	100.00%
Somewhat Disagree	-51.43 s/d -17.14	28.57-42.86	0	0.00%	
Disagree	-85.71 s/d -51.43	14.29-28.57	0	0.00%	
Strongly Disagree	-120 s/d -85.71	≤ 14.29	0	0.00%	
TOTAL RESPONDENT			**46**	**100.00%**	

As shown in Figure 4 and Table 10, the average pretest score is 102.13, and the average posttest score is 126.09, while the overall average score for cryptography competence after gamification implementation is 114.11. Table 10 also indicates that there is an increase of 23.96 points in cryptography competence. This improvement is primarily driven by skill indicators, which increased by 14.46 points, and knowledge indicators, which increased by 9.50 points.

Discussion on Web Vulnerability Competence

The results of the web vulnerability competence calculation were processed and presented in the form of a frequency distribution as shown in Table 12 and a radar chart in Figure 5.

Table 12. Frequency Distribution Web Vulnerability

Category	Interval	% Interval	Frequently	Percentage	Accumulative
Strongly Agree	85.71 s/d 120	≥ 85.71	1	2.17%	2.17%
Agree	51.43 s/d 85.71	71.43-85.71	7	15.22%	17.39%
Somewhat Agree	17.14 s/d 51.43	57.14-71.43	23	50.00%	67.39%
Neutral	-17.14 s/d 17.14	42.86-57.14	15	32.61%	100.00%
Somewhat Disagree	-51.43 s/d -17.14	28.57-42.86	0	0.00%	
Disagree	-85.71 s/d -51.43	14.29-28.57	0	0.00%	
Strongly Disagree	-120 s/d -85.71	≤ 14.29	0	0.00%	
TOTAL RESPONDENT			**46**	**100.00%**	

From the frequency distribution, it is evident that 1 (one) respondent stated, "strongly agree," 7 (seven) respondents stated "agree," and 23 (twenty-three) respondents stated "somewhat agree" regarding the improvement in web vulnerability competence after the implementation of gamification.

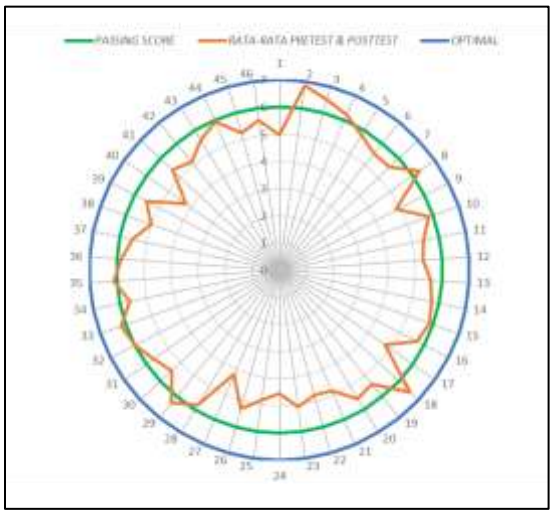

Figure 5. Web Vulnerability Radar Chart

From Figure 5, it is evident that there were 9 respondents who managed to exceed the passing score, while the remaining 37 respondents showed an improvement in their competency scores but still did not reach the passing score.
The results indicate that there was a significant increase in scores specifically related to the skill indicator in the field of web vulnerability compared to other indicators. This suggests that the implementation of gamification strategies has proven to be highly effective in enhancing web vulnerability skills. However, continuous improvement and ongoing training are still necessary to further enhance these skills.

Discussion on Cybersecurity Competence

In analyzing the improvement of cybersecurity competency, the researchers employed descriptive statistical calculations by constructing a frequency distribution of the overall posttest and pretest score differences, combining the competency scores in cryptography and web vulnerability. The results were presented in a radar chart, as depicted in Figure 6.
From Figure 6, it is evident that there were 9 respondents who managed to exceed the passing score, while the remaining 37 respondents showed an improvement in their competency scores but still did not reach the passing score.

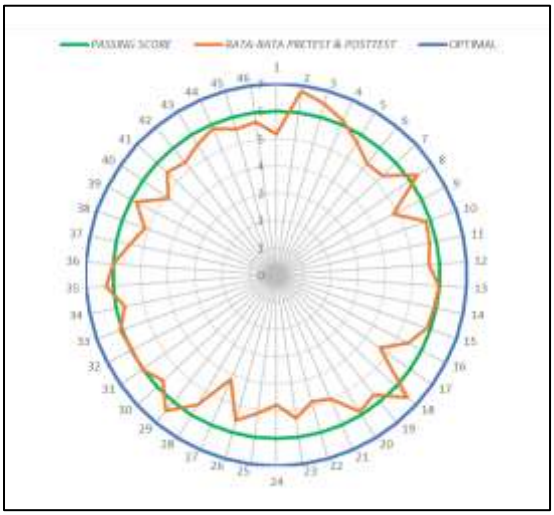

Figure 6. Cybersecurity Radar Chart

Table 13. Frequency Distribution Cybersecurity

Category	Interval	% Interval	Frequently	Percentage	Accumulative
Strongly Agree	171.42 s/d 240	≥ 85.71	0	0.00%	0.00%
Agree	102.85 s/d 171.42	71.43-85.71	4	8.70%	8.70%
Somewhat Agree	34.28 s/d 102.85	57.14-71.43	28	60.87%	69.57%
Neutral	-34.28 s/d 34.28	42.86-57.14	14	30.43%	100.00%
Somewhat Disagree	-102.85 s/d -34.28	28.57-42.86	0	0.00%	
Disagree	-171.42 s/d -102.85	14.29-28.57	0	0.00%	
Strongly Disagree	-240 s/d -171.42	≤ 14.29	0	0.00%	
TOTAL RESPONDENT			**46**	**100.00%**	

Table 13 illustrates that 4 (four) respondents expressed their agreement, and 28 (twenty-eight) respondents somewhat agreed that their cybersecurity competency improved after participating in gamification. It is evident that 69.57% of respondents provided positive statements regarding

the enhancement of their cybersecurity competency following the implementation of gamification.

From Table 10, it is also evident that the top-ranking increase in scores occurred in the skill indicator of web vulnerability competency, followed by the skill indicator of cryptography competency, then the knowledge indicator of web vulnerability competency, and finally the knowledge indicator of cryptography competency. The ranking shows that the two highest improvements were dominated by skill-based indicators, while the two lowest improvements were associated with knowledge-based indicators.

Combining the information from Table 10 and Figure 6, the pretest average score was found to be 197.28, and the posttest average score was 251.80. Thus, the overall average score for cybersecurity competency after implementing gamification was 224.54. The calculated increase in cybersecurity competency score after gamification implementation was 54.52 points. This increase was primarily driven by a 30.57-point improvement in web vulnerability competency and a 23.96-point improvement in cryptography competency. The analysis indicates that respondents' competencies improved significantly, particularly in the skill indicators, followed by the knowledge indicators.

Discussion of Gamification

The entire set of descriptive statistical calculations performed on cybersecurity competency can be compared with the game flags discovered by respondents during the gamification process. The results of the descriptive statistical calculations on the flags found by respondents are presented in Table 14.

Table 14. Descriptive Statistics of Flag Gamification Cybersecurity

Num	Competence	Level	Answer	Total	%	Total Respondent
1	*Cryptography*	*Easy*	Right	19	41.30%	46
			Wrong	27	58.70%	
		Medium	Right	17	36.96%	46
			Wrong	29	63.04%	
		High	Right	15	32.61%	46
			Wrong	31	67.39%	
2	*Web Vulnerability*	*Easy*	Right	30	65.22%	46
			Wrong	16	34.78%	
		Medium	Right	30	65.22%	46
			Wrong	16	34.78%	
		High	Right	28	60.87%	46
			Wrong	18	39.13%	

Out of a total of 46 respondents involved in the cryptography game, 19 respondents (41.30%) were able to find the flag or answer correctly at the easy level, while 17 respondents (36.96%) managed to find the flag at the medium level. At the high level, only 15 respondents (32.61%) were able to find the flag.

On the other hand, in the web vulnerability game, 30 respondents (65.22%) successfully found the flag at both the easy and medium levels, while 28 respondents (60.87%) were able to find the flag at the high level.

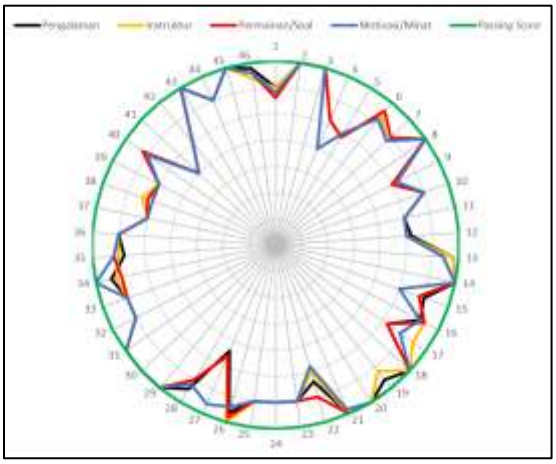

Figure 7. Gamification Radar Chart

Meanwhile, the descriptive statistical calculations on gamification were processed and presented as a frequency distribution, as shown in Table 15. The data were also visualized as a radar chart, as depicted in Figure 7.

Table 15. Frequency Distribution Gamification

Category	Interval	% Interval	Frequently	Percentage	Accumulative
Strongly Agree	124-140	≥ 88.00%	20	43.48%	43.48%
Agree	107-123	76.00-87.99%	15	32.61%	76.09%
Somewhat Agree	90-106	64.00-75.99%	10	21.74%	97.83%
Neutral	72-89	51.00-63.99%	1	2.17%	100.00%
Somewhat Disagree	55-71	39.00-50.99%	0	0.00%	
Disagree	38-54	27-38.99%	0	0.00%	
Strongly Disagree	20-37	≤ 26.99	0	0.00%	
TOTAL RESPONDENT			**46**	**100%**	

On average, Table 15 shows that 20 respondents (43.48%) expressed strong agreement, 15 respondents (32.61%) agreed, and 10 respondents (21.74%) somewhat agreed that the implemented gamification improved their cybersecurity competency. Overall, 97.83% of the respondents provided positive statements indicating that gamification facilitated the learning and practical application of cybersecurity through real-world-oriented approaches. Additionally, 97.83% of respondents expressed a positive opinion regarding the positive impact of gamification on enhancing their cybersecurity competency.

These responses align with the findings of Gonzalez et al. (2019), who emphasized that cybersecurity experiences could be fostered through Capture the Flag (CTF) tournaments, aimed at enhancing respondents' knowledge and skills.

Experience Indicator:

Most respondents responded positively towards the implemented gamification. The positive feedback on the experience indicator is consistent with Hamari's (2019) notion that gamification aims to create experiences that closely resemble real-world situations, thus providing respondents with practical experiences like those encountered in the cybersecurity industry.

The positive sentiments expressed by respondents included the alignment between teaching materials and gamification implementation. Approximately 95.65% of respondents acknowledged the appropriateness of the instructional materials and gamification conducted by the researchers. This instructional material arrangement and tutorials were modified based on the

research of W. Liu et al. (2019), stating that a detailed and meticulous gamification approach aids respondents in enhancing their understanding of cybersecurity.
Moreover, 95.65% of respondents expressed that learning cybersecurity through gamification was more enjoyable than studying theoretical concepts in a classroom. This aligns with the concepts presented by Yurcik & Doss (2001), who criticized traditional lecture approaches for limiting students' opportunities to delve deeper into exploring their knowledge and skills.
Wibowo (2013) emphasized that a person's competence is greatly influenced by their knowledge and skills over time. As a game, gamification aims to create a new experience for respondents, ultimately leading to an enhancement of their competencies (Gonzalez et al., 2019). This notion is reinforced by respondents' statements, indicating that gamification successfully improved their skills, particularly in skill-based indicators, followed by knowledge-based indicators.

Instructor Indicator:

During the gamification experiment, the researchers incorporated instructors as a crucial indicator to enhance respondents' cybersecurity competencies. This decision was informed by the research of Costa et al. (2020), which noted that cybersecurity gamification is often associated with experts in the field, while the cybersecurity industry also requires beginners or newcomers, making gamification an essential bridge to enhance beginners' competencies.

This aligns with the response of 97.83% of the respondents, who stated that instructors in gamification should possess actual cybersecurity experience in the real world. This supports Gasiba et al.'s (2020) findings that gamification cannot be simply introduced to beginners without tailored content suitable for the target audience, requiring personnel capable of creating such content. This is further corroborated by Yurcik & Doss (2001), who mentioned that involving experts is one of the best techniques for cybersecurity learning. Gultom & Alrianto (2016) also emphasized the importance of human resources in cybersecurity implementation.
One key responsibility of instructors during gamification is to integrate media and teaching methods into the gamification process. Approximately 97.83% of respondents positively evaluated the combination of media and teaching methods employed in this study, as the researchers modified the gamification by combining gaming formats with teaching techniques (Yurcik & Doss, 2001).

Moreover, respondents acknowledged other essential instructor attributes, including delivery techniques, the ability to explain the relevance between cybersecurity theory and real-world incidents, technical skills in using software, and real-world cybersecurity experience.

Game/Question Indicator:

As known, cybersecurity encompasses various subfields beyond cryptography and web vulnerability (Spafford, 1998), such as personal data protection, open-source intelligence, and many others. Since this study limited itself to cryptography and web vulnerability, the researchers sought respondents' opinions on the games designed by the researchers. More than 90% of respondents expressed the need for diverse games in both cryptography and web vulnerability. This is reasonable since a variety of games would increase respondents' knowledge, skills, and experiences, leading to an improvement in their competencies.
One approach to achieving diverse cybersecurity games is to employ an integrated gaming platform (Karagiannis et al., 2020). The availability of cybersecurity gaming platforms is intended to facilitate respondents' access to instructional materials, tutorials, and target machines used in the learning process (Karagiannis et al., 2020). 97.82% of respondents also positively regarded the utilization of virtlab as a cybersecurity gaming platform in this study, finding it highly beneficial for their cybersecurity learning.

Motivation/Interest Indicator:

Cumulatively, 95.65% of respondents stated they remained interested in furthering their knowledge of cybersecurity. Additionally, 93.48% of respondents acknowledged that the cybersecurity games in this experiment were challenging and not easily mastered, as evidenced by the flags, where not all respondents could answer them correctly. In cryptography, less than 50% of respondents could find the flag, while in web vulnerability, the maximum percentage of respondents able to find the flag was 65.22%, and only for the easy and medium levels. Furthermore, the number of respondents who found the flag in cryptography correlated with low total cryptography competency scores, indicating consistency between the lack of improvement in cryptography knowledge and skills and respondents' ability to find cryptography game flags.

However, despite not all respondents finding the flags in the games, 93.48% of respondents stated that the challenges in the games were surmountable through consistent and continuous gamification. Most respondents believed that, although cybersecurity might be difficult to learn, continuous gamification would aid in enhancing their competencies.

CONCLUSION

As outlined in the research problem and objectives, this study addressed four research questions concerning cryptography competency, web vulnerability competency, cybersecurity competency, and the effectiveness of competency enhancement after the implementation of gamification.

a. Since the beginning of the research, the researcher set a criterion for hypothesis fulfillment, indicating that the hypothesis could be met if the normality test yielded a significance value greater than 0.05, and the paired-sample T-test resulted in a significance value less than 0.05 (2-tailed). Based on these criteria, the following conclusions can be drawn:
b. The paired-sample T-test for cryptography competency yielded a significant value less than 0.001, indicating $Y_{2CR} > Y_{1CR}$. This result leads to the rejection of the H_{oCR} hypothesis, suggesting a significant increase in cryptography competency pre- and post-gamification.
c. The paired-sample T-test for cybersecurity competency resulted in a significant value less than 0.001, indicating $Y_2 > Y_1$. Consequently, the H_o hypothesis is rejected, signifying a significant improvement in cybersecurity competency pre- and post-gamification.
d. The results indicate that gamification primarily contributes to enhancing competencies in skill-based indicators rather than knowledge-based indicators, in both cryptography and web vulnerability fields.

The effectiveness test shows that the competency improvement after gamification amounts to 65.91%. According to Hake's effectiveness categories, this falls within the moderate effectiveness category, contrary to the initial hypothesis, which stated that gamification would be highly effective.

REFERENCES

Costa, G., Lualdi, M., Ribaudo, M., & Valenza, A. (2020). A NERD DOGMA: Introducing CTF to Non-expert Audience. *SIGITE 2020 - Proceedings of the 21st Annual Conference on Information Technology Education*, 413–418. https://doi.org/10.1145/3368308.3415405

Creswell, John. W. (2013). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. In *Research design Qualitative quantitative and mixed methods approaches*.

Gasiba, T., Lechner, U., Pinto-Albuquerque, M., & Zouitni, A. (2020). Design of secure coding challenges for cybersecurity education in the industry. *Communications in Computer and Information Science*, *1266 CCIS*. https://doi.org/10.1007/978-3-030-58793-2_18

Ghozali, I. (2018). Aplikasi Analisis Multivariate dengan Program IBM SPSS. Yogyakarta: Universitas Diponegoro. *(Edisi 9). Semarang: Badan Penerbit Universitas Diponegoro*.

Gonzalez, H., Llamas, R., & Montaño, O. (2019). Using a CTF Tournament for Reinforcing Learned Skills in Cybersecurity Course. *Research in Computing Science*, *148*(5). https://doi.org/10.13053/rcs-148-5-15

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*.

Guntara, Y. (2021). *Normalized Gain: Ukuran Keefektifan Treatment*. https://www.researchgate.net/profile/Yudi-Guntara/publication/340232572_Normalized_gain_ukuran_keefektifan_treatment/links/5e7df34092851caef4a24f24/Normalized-gain-ukuran-keefektifan-treatment.pdf

Hake, R. R. (1998). Interactive-engagement versus traditional methods: A six-thousand-student survey of mechanics test data for introductory physics courses. *American Journal of Physics*, *66*(1). https://doi.org/10.1119/1.18809

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

Karagiannis, S., Maragkos-Belmpas, E., & Magkos, E. (2020). An Analysis and Evaluation of Open Source Capture the Flag Platforms as Cybersecurity e-Learning Tools. *IFIP Advances in Information and Communication Technology*, *579 IFIP*. https://doi.org/10.1007/978-3-030-59291-2_5

Li, C., Kulkarni, M. R., & Kulkarni, R. (2016). *Survey of Cybersecurity Education through Gamification Cybersecurity Education through Gamification-the CTF Approach*.

Love, J., Selker, R., Marsman, M., Jamil, T., Dropmann, D., Verhagen, J., Ly, A., Gronau, Q. F., Šmíra, M., Epskamp, S., Matzke, D., Wild, A., Knight, P., Rouder, J. N., Morey, R. D., & Wagenmakers, E. J. (2019). JASP: Graphical statistical software for common statistical designs. *Journal of Statistical Software*, *88*(1). https://doi.org/10.18637/jss.v088.i02

McAshan, H. H. (1979). *Competency-based education and behavioral objectives*. Englewood Cliffs, N.J. : Educational Technology Publications. https://archive.org/details/competencybasede0000mcas/page/n7/mode/2up

Shapiro, S. S., Wilk, M. B., & Chen, H. J. (1968). A Comparative Study of Various Tests for Normality. *Journal of the American Statistical Association*, *63*(324). https://doi.org/10.1080/01621459.1968.10480932

Sitinjak, T. J., & Sugiarto. (2006). *Lisrel*. Penerbit Graha Ilmu.

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

Suliyanto. (2017). PERBEDAAN PANDANGAN SKALA LIKERT SEBAGAI SKALA ORDINAL ATAU SKALA INTERVAL. *Sewindu Statistika*.

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

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

Wibowo. (2013). Manajemen Kinerja edisi ketiga. In *Manajemen Kinerja edisi ketiga*.

Widiyanto, M. A. (2013). *Statistika Terapan*. Elex Media Komputindo.

Wiersma, W. (2000). *Research Methods in Education an Introduction*. Allyn and Bacon.

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