Journal of Applied Informatics and Computing (JAIC)
Vol.x, No.x, Juli 201x, pp. xx~xx
e-ISSN: 2548-6861

Respon Mahasiswa Pada Pemahaman *Penetration Testing* Melalui Gamifikasi *Capture The Flag* (Studi Kasus Program Studi Rekayasa Keamanan Siber Politeknik Negeri Batam)

Yunita Tri Indriani [1]*, Dodi Prima Resda [2]*, Antoni Haikal [3]*
* Rekayasa Keamanan Siber, Politeknik Negeri Batam
yunitatind@gmail.com [1], dodi.prima@polibatam.ac.id [2], antoni@polibatam.ac.id [3]

Article Info

Article history:

Received …
Revised …
Accepted …

Keyword:

Capture the Flag, Penetration Testing, Cybersecurity.

ABSTRACT

The increase in cybercrime is one of the triggers for knowledge about cybersecurity. The ever-evolving cyber knowledge is the task of teachers in finding solutions on how to keep up with the knowledge that continues to evolve every time. Cybersecurity knowledge has been applied in various ways, one of which is in the form of gamification capture the flag. Gamification of capture the flag has become the choice of many students to learn the understanding of penetration testing. This solution requires the support of student responses in its implementation in the Batam State Polytechnic Cybersecurity Engineering Study Program. This study program has supported learning with capture the flag gamification and collaborated with project-based learning penetration testing so that the respondents taken meet the requirements in this study. This research aims to help teachers determine the right learning techniques and get responses related to the implementation of gamification capture the flag with an understanding of penetration testing. In this study, the method used is a quantitative method with descriptive statistical analysis with three factors analyzed, namely theoretical understanding, practical understanding, and awareness of the importance of penetration testing. The results of this study resulted in a good response from students regarding the understanding of penetration testing through gamification capture the flag, both in theoretical understanding, practical understanding, and awareness of the importance of penetration testing.

I. PENDAHULUAN

Kejahatan siber terus berkembang mengikuti improvisasi teknologi di bidang keamanan informasi. Kejahatan siber yang begitu marak dapat membahayakan sistem yang telah dibangun oleh suatu organisasi atau instansi. Pengetahuan dalam keamanan siber sangat penting untuk menghindari ancaman dari kejahatan siber [1], [2]. Praktik *penetration testing* merupakan salah satu pengetahuan dalam keamanan siber. *Penetration testing* yang disingkat dengan pentesting merupakan proses simulasi serangan siber yang dilakukan untuk mengidentifikasi kerentanan dan eksploitasi dalam sistem keamanan informasi [3]. Evolusi praktik pentest memerlukan pendekatan pembelajaran yang fleksibel dan berkelanjutan. Berbagai pendekatan diteliti demi mendapatkan teknik pembelajaran yang baik untuk meningkatkan pengetahuan pentest.

Bentuk pendekatan dalam pembelajaran pentest bermacam-macam, yaitu pembelajaran dengan melakukan latihan traditional di kelas ditemani oleh instruktur, belajar secara mandiri melalui simulasi lab *hacking* [4], implementasi dalam bentuk *project based-learning*, sampai implementasi dengan bentuk gamifikasi [5]. *Project based-learning* disingkat PBL adalah pendekatan dalam implementasi pembelajaran yang di desain dengan pembelajaran aktif [6], yaitu dengan langsung terjun di suatu proyek. Gamifikasi merupakan pendekatan yang memanfaatkan elemen-elemen permainan untuk mengatasi masalah di luar konteks permainan [7]. Gamifikasi ini telah menjadi tren dalam dunia pembelajaran untuk menambah motivasi pelajar dalam proses belajar [8]. Dalam mengikuti perkembangan ilmu keamanan

e-ISSN: 2548-6861

siber terlebihnya dalam praktik pentest, gamifikasi *capture the flag* sedang menjadi tren untuk mempelajari pentest. Pengajar dapat menggunakan bentuk gamifikasi yang bernama *capture the flag* [9]. *Capture the flag* disingkat CTF merupakan sebuah kompetisi berbasis tantangan, yang memiliki tujuan untuk mengasah dan mendapatkan keterampilan dalam keamanan siber dengan cara penerapan secara praktis [10]. CTF memiliki berbagai bentuk implementasi, yang sering diimplementasikan adalah *jeopardy-style* dan *attack-defense*. *Jeopardy-style* merupakan bentuk tantangan statis atau menjawab pertanyaan dalam kategori yang telah ditentukan dengan mengumpulkan bendera atau yang dikenal dengan *flag* [5]. *Attack-defense* yaitu bentuk simulasi mempertahankan mesin virtual milik pribadi dan menyerang mesin virtual milik lawan.

Angkatan pertama program studi Rekayasa Keamanan Siber (RKS) dimulai pada tahun 2020. Program studi ini telah menerapkan dukungan terhadap gamifikasi CTF dalam kompetisi dan pembelajaran pentest bagi mahasiswanya. Beberapa platform CTF yang digunakan oleh mahasiswa RKS adalah Pico CTF, Haris CTF, Hack The Box, dan Try Hack Me. Mahasiswa program studi RKS juga telah mengikuti *project based-learning* (PBL) *penetration testing* yang disediakan oleh Politeknik Negeri Batam. PBL ini menerapkan praktik pentest dengan menggunakan metodologi tertentu dalam prosesnya dan memiliki keluaran berupa hasil laporan dari pengerjaan pentest. Tetapi belum terdapat informasi terhadap respon mahasiswa program studi RKS mengenai pemahaman pentest melalui gamifikasi CTF. Penelitian ini diharapkan dapat memberikan gambaran kepada pengajar sebagai pertimbangan dalam pengimplementasian CTF untuk pemahaman pentest. Berbagai kategori bidang pembelajaran yang disediakan CTF diantaranya adalah eksploitasi web, kriptografi, *reverse engineering*, *osint*, dan forensik siber [11].

CTF dibuktikan dapat meningkatkan motivasi pelajar dalam menambah pengetahuan dalam memecahkan tantangan [12]. CTF juga bisa menjadi solusi agar pembelajaran tidak terasa membosankan, hal ini dibuktikan dari grafik survey skala likert yang merupakan hasil respon pelajar pada perbandingan pembelajaran secara tradisional dengan menerapkan gamifikasi CTF [5]. CTF dapat menguntungkan bagi instruktur dan pelajar karena instruktur dapat menghemat waktu dalam penilaian sedangkan pelajar dapat berlatih secara praktik sambil menikmati prosesnya [9]. Hasil survey di *Polytechnic University of San Luis Potosi* membuktikan bahwa CTF dapat menambah kepercayaan diri pelajar untuk mengeksekusi eksploitasi ketika melakukan praktik pentest [12]. Dalam beberapa penelitian, CTF dapat memberikan pengaruh baik terhadap pembelajaran keamanan siber [5], [12], [13]. Tetapi untuk lebih spesifiknya penelitian ini akan menganalisis hasil respon mahasiswa RKS untuk memberikan data terkait pemahaman pentest melalui gamifikasi CTF.

Untuk mendapatkan data tanggapan mahasiswa RKS terkait pemahaman pengetahuan pentest melalui gamifikasi CTF, dilakukannya kuesioner dengan metode skala likert dengan responden yang pernah bermain CTF dan berpengalaman dalam PBL pentest. Penelitian bertujuan untuk memberikan gambaran hasil respon mahasiswa RKS terkait pemahaman pentest melalui gamifikasi CTF yang disajikan dalam bentuk analisis statistik deskriptif. Dari pengetahuan yang dapat diambil dalam pengetahuan pentest, yang menjadi faktor dalam pemahaman pentest melalui gamifikasi CTF adalah pemahaman teori, pemahaman praktik, dan kesadaraan akan pentingnya pentest.

II. METODE

Capture the flag telah menjadi salah satu gamifikasi yang mendukung pembelajaran keamanan siber terutama pentest [14]. Penelitian ini bertujuan memberikan hasil respon mahasiswa RKS pada pemahaman pentest melalui gamifikasi CTF.

A. Teknik Sampling dan Pengumpulan Sampel

Dalam penelitian ini penentuan sampel menggunakan Teknik *purposive sampling*, yaitu dengan mengambil sampel berdasarkan kriteria tertentu. Kriteria yang dibutuhkan untuk menjadi responden dalam penelitian ini yaitu mahasiswa yang pernah bermain CTF dan melakukan PBL pentest. Roscoe berpendapat bahwa ukuran sampel berkisar antara 30 hingga 500 dianggap sesuai untuk penelitian [15]. Populasi yang diambil adalah mahasiswa RKS dan sampel yang memenuhi ketentuan untuk menjadi responden adalah 40 sampel.

B. Instrumen Penelitian

Kuesioner dibuat dengan memfokuskan pada pengambilan pendapat pada 3 faktor yaitu pemahaman teori, pemahaman praktik, dan kesadaran akan pentingnya pentest. Kuesioner yang diberikan kepada mahasiswa adalah kuesioner tertutup yang memiliki 25 pernyataan terkait pemahaman dan kesadaran mahasiswa terhadap pentest. Kuesioner ini terdiri dari 12 pernyataan untuk mengetahui tanggapan tentang pemahaman teori pentest, 8 pernyataan tentang pemahaman praktik pentest, dan 5 pernyataan tentang kesadaran pentingnya pentest. Kuesioner tertutup dapat memudahkan peneliti untuk mempercepat pengolahan data dan membantu menetapkan nilai yang telah diberi batas [15]. Penelitian ini menggunakan skala likert dengan skala Sangat Setuju (SS), Setuju (S), Ragu-Ragu (RR), Tidak Setuju (TS), dan Sangat Tidak Setuju (STS). Teknik ini telah digunakan oleh banyak penelitian survey [16], [17].

C. Prosedur Pengambilan Data

Pengambilan data dilakukan melalui kuesioner menggunakan google forms dan responden yang telah terdaftar dengan email. Kuesioner ini disebarkan melalui platform sosial media grup RKS. Penggunaan kuesioner secara online digunakan untuk kemudahan dalam

pengambilan data. Peneliti menggunakan teknik *purposive sampling* untuk menentukan siapa yang dapat mengisi kuesioner. Pengambilan data ini memungkinkan untuk pengambilan responden yang memenuhi ketentuan [15].

D. Teknik Analisis

Uji reliabilitas yang dilakukan dengan data penelitian ini adalah dengan uji Cronbach Alpha. Cronbach Alpha adalah salah satu pengujian alat ukur yang sering digunakan. Pengujian dilakukan dengan bantuan alat SPSS untuk menentukan nilai Cronbach Alpha. Dalam uji reliabilitas penelitian ini, bertujuan untuk mengetahui seberapa jauh instrumen pengukuran bekerja dengan baik [18]. Jika hasil dari uji ini adalah > 0,6 maka instrumen penelitian tersebut reliabel, sebab jika hasil semakin dekat dengan 1 maka instrumen pengukuran yang digunakan semakin reliabel [18].

Klasifikasi tanggapan penelitian diperlukan untuk mengukur tanggapan mahasiswa terhadap pemahaman pentest melalui gamifikasi CTF. Persentase skor aktual dapat menjadi solusi dalam memberikan kriteria hasil kuesioner yang telah diolah [17].

Tabel di bawah menyediakan interval skor tanggapan responden terhadap skor ideal dengan rentang 5.

TABEL I
INTERVAL SKOR PEMAHAMAN MAHASISWA.

Interval 100%	Skor
84% - 100%	Sangat Baik (SB)
68% - 84%	Baik (B)
52% - 68%	Cukup Baik (CB)
36% - 52%	Tida Baik (TB)
20% - 36%	Sangat Tidak Baik (STB)

Analisis data dapat dilakukan dengan berbagai cara, salah satunya adalah dengan statistik deskriptif. Statistik deskriptif mendukung pengolahan data kuantitatif dengan memberikan gambaran yang jelas terkait karakteristik data [15]. Analisis statistik deskriptif dalam penelitian ini digunakan untuk memudahkan pengolahan data secara ringkas dan menampilkan data yang mudah dipahami pada pembaca.

Analisis data yang dilakukan adalah dengan menyajikan data mean atau rata-rata dari setiap faktor yang datanya telah diolah. Selanjutnya dilakukan analisis frekuensi dari masing-masing faktor. Analisis pada frekuensi dilakukan untuk mengetahui jumlah pilihan terbanyak dari masing-masing indikator. Analisis ini dapat mendukung untuk menentukan indikator mana yang memiliki hasil setuju dan tidak setuju dari tanggapan mahasiswa yang menjadi sampel [19].

III. HASIL DAN PEMBAHASAN

Dari mahasiswa RKS yang memenuhi untuk menjadi sampel adalah 40 mahasiswa. Terdapat tiga faktor yang difokuskan untuk menggambarkan hasil respon mahasiswa terkait implementasi gamifikasi CTF terhadap pemahaman pentest dalam penelitian ini, yaitu pemahaman teori, pemahaman praktik, dan kesadaran pentingnya pentest.

TABEL II
HASIL UJI STATISTIK RELIABILITAS MENGGUNAKAN SPSS.

Cronbach's Alpha	N of items
0.961	25

Tabel II menampilkan hasil dari uji reliabilitas menggunakan bantuan aplikasi SPSS. Uji ini dilakukan pada 25 indikator pengukuran berupa pernyataan dan memiliki hasil 0.961, yang berarti indikator di dalam kuesioner tersebut reliabel karena nilai Cronbach Alpha yang dihasilkan > 0,6 dan mendekati 1 [18].

TABEL III
HASIL PENGUKURAN PERSENTASE SKOR AKTUAL RESPON MAHASISWA TERHADAP PEMAHAMAN PENTEST MELALUI GAMIFIKASI CTF.

Faktor	Skor Aktual	Skor Ideal	Presentase (%) Skor Aktual	Keterangan
Pemahaman teori	49	60	81,67	Baik
Pemahaman praktik	32	40	80,0	Baik
Kesadaran pentingnya *penetration testing*	20	25	80,0	Baik
Rata-Rata	**33,67**	**41,67**	**80,55**	**Baik**

Berdasarkan Tabel III pemahaman teori pentest melalui gamifikasi CTF disajikan dalam persentase skor aktual untuk mengetahui respon dari skor pemahaman teori mahasiswa. Skor aktual dalam pemahaman teori adalah 49 dan skor idealnya adalah 60, sehingga persentase skor aktual yang didapat adalah 81,67% yang memiliki kriteria Baik (B). Pemahaman praktik memiliki skor aktual dengan nilai 32 dan skor ideal 40, sehingga menghasilkan persentase skor aktual 80% yang memiliki kriteria Baik (B). Kesadaran akan pentingnya pentest juga turut dihitung untuk skor persentase aktualnya. Skor aktual yang dimiliki yaitu 20 dan skor idealnya adalah 25. Persentase skor aktual yang didapat dari formulasi tersebut adalah 80% yang masuk dalam kriteria Baik (B).

Dari keseluruhan hasil Tabel III didapat rata-rata dari persentase skor aktual keseluruhan indikator yaitu 80,55% yang termasuk kriteria Baik (B). Hal ini menjelaskan bahwa mahasiswa setuju bahwa CTF dapat mendukung pemahaman teori pentest [5], [12], [13].

TABEL IV
MEAN HASIL TANGGAPAN RESPONDEN TENTANG PEMAHAMAN PETEST MELALUI GAMIFIKASI CTF.

Faktor	Mean
Pemahaman teori	4,08
Pemahaman praktik	4,05
Kesadaran pentingnya pentest	4,09

e-ISSN: 2548-6861

Tabel IV menyajikan mean atau rata-rata dari tiga faktor yang diukur. Dilakukan formulasi dari masing-masing rata-rata faktor untuk mengukur pemahaman dan kesadaran. Pemahaman teori memiliki rata-rata 4,08 dari skala 5, pemahaman praktikal memiliki rata-rata 4,05 dari skala 5, dan kesadaran pentingnya pentest memiliki rata-rata 4,09 dari skala 5. Dari nilai rata-rata di atas, kesadaran akan pentingnya dilakukan pentest memiliki nilai tertinggi rata-rata.

Tabel V menyediakan data frekuensi dan persentase frekuensi dari masing-masing indikator terhadap pemahaman teori pentest melalui gamifikasi CTF.

TABEL V
FREKUENSI DAN BENTUK PERSENTASE FREKUENSI TANGGAPAN PEAMAHAN TEORI MAHASISWA RKS.

Pernyataan	SS F%	S F%	RR F%	TS F%	STS F%
Saya merasa CTF berpengaruh dalam pemahaman *penetration testing*.	20 50,0	17 42,5	2 5,0	1 2,5	0 0
Saya merasa CTF bermanfaat untuk memahami *penetration testing*.	21 52,5	17 42,5	2 5,0	0 0	0 0
Capture the flag membantu saya memperkuat pemahaman tentang *penetration testing*.	19 47,5	16 40,0	4 10,0	1 2,5	0 0
Saya memahami konsep dasar pengujian *penetration testing* setelah mengikuti permainan CTF.	13 32,5	12 30,0	10 25,0	4 10,0	1 2,5
Saya memahami metodologi *penetration testing* setelah memainkan *capture the Flag*.	10 25,0	12 30,0	11 27,5	6 15,0	1 2,5
CTF memberikan saya pengetahuan tentang *tools*/alat-alat yang digunakan untuk melakukan *penetration testing*.	19 47,5	16 40,0	5 12,5	0 0	0 0
Capture the flag memberikan gambaran yang jelas kepada saya tentang risiko keamanan yang mungkin dihadapi dalam sistem.	14 35,0	19 47,5	6 15,0	1 2,5	0 0
Capture the flag memberikan kemampuan kepada saya untuk mengembangkan strategi mitigasi risiko.	11 27,5	15 37,5	12 30,0	1 2,5	1 2,5
Saya dapat memahami *Proof of Concept* (PoC) *penetration testing* melalui pembuatan *write-up* CTF.	13 32,5	17 42,5	7 17,5	3 7,5	0 0
Capture the flag membantu saya memahami perbedaan antara serangan aktif dan pasif dalam *penetration testing*.	13 32,5	15 37,5	10 25,5	2 5,0	0 0
Capture the flag membantu saya memahami pentingnya melakukan *penetration testing* secara terstruktur.	15 37,5	18 45,0	4 10,0	1 2,5	2 5,0
Dengan mengikuti *capture the flag* saya mendapatkan wawasan dalam menentukan risiko yang terjadi terhadap celah keamanan yang ditemukan.	15 37,5	16 40,0	6 15,0	3 7,5	0 0

Pada tabel V diketahui bahwa 20 (50%) responden sangat setuju dan 17 (42,5%) responden setuju bahwa CTF mempegaruhi pemahaman pentest, sebaliknya sedikit responden yang tidak setuju yaitu 1 (2,5%) responden. 21 (52,5%) responden merasa sangat setuju bahwa CTF bermanfaat untuk pemahaman pentest, serta 17 (42,5%) mahasiswa menaruh jawaban setuju. Untuk lebih jelasnya terdapat data yaitu sebanyak 19 (47,5%) sangat setuju bahwa memainkan CTF dapat memperkuat pemahaman pentest, 16 (40%) mahasiswa RKS setuju dan terdapat 1 (2,5%) responden tidak setuju dengan pernyataan tersebut. Terdapat 13 (32,5%) sangat setuju bahwa CTF juga dapat mampu memberikan konsep dasar pentest, 12 (30%) setuju, serta 4 (10%) tidak setuju dan 1 (2,5%) responden yang sangat tidak setuju akan pernyataan ini. Untuk memahami metodologi pentest, 10 (25%) responden sangat setuju bahwa CTF dapat menambah pemahaman tersebut, 12 (30%) setuju, tetapi 6 (15%) responden tidak setuju dan 1 (2,5%) responden sangat

tidak setuju karena tidak merasa bahwa CTF dapat mendukung pemahaman metodologi pentest. Tidak hanya itu, CTF membantu 19 (47,5%) responden yang sangat setuju dan 16 (40%) setuju untuk memberikan pengetahuan terkait *tools* atau alat-alat yang digunakan dalam pentest. Gambaran jelas tentang risiko keamanan yang mungkin terdapat dalam sistem dapat disampaikan melalui permainan CTF, hal ini didukung oleh 14 (35%) responden sangat setuju dan 19 (47,5%) setuju, dengan 1 (2,5%) tidak setuju terkait hal itu. Kemampuan mengembangkan strategi mitigasi risiko yang didapat dari gamifikasi CTF didukung oleh responden sebanyak 11 (27,5%) sangat setuju dan 15 (37,5%) mahasiswa setuju, tersisa 1 (2,5%) mahasiswa tidak setuju dan 1(2,5%) mahasiswa sangat tidak setuju. PoC menjadi salah satu indikator pemahaman yang disetujui yaitu terdapat 13 (32,5%) tanggapan sangat setuju, 17 (42,5%) responden tanggapan setuju, dan 3 (7,5%) tanggapan tidak setuju. Dilanjutkan dengan pemahaman perbedaan pada serangan aktif dan serangan pasif yang terjadi ketika pentest, 13 (32,5%) responden sangat setuju, 15 (37,5%) setuju dan 2 (5%) responden tidak setuju. Pemahaman implementasi pentest secara terstruktur didukung oleh 15 (37,5%) responden sangat setuju, 18 (45%) setuju, dan 1 (2,5%) tidak setuju, dan 2 (5%) sangat tidak setuju. 15 (37,5%) sangat setuju dan 16 (40%) responden setuju bahwa CTF menambahan wawasan dalam menentukan risiko dari celah yang ditemukan, terdapat 3 (7,5%) responden yang tidak setuju dengan pernyataan ini.

TABEL VI
FREKUENSI DAN BENTUK PERSENTASE FREKUENSI TANGGAPAN PEMAHAMAN PRAKTIK MAHASISWA RKS.

Pernyataan	SS F%	S F%	RR F%	TS F%	STS F%
Saya lebih percaya diri dalam mengaplikasikan konsep-konsep *penetration testing* setelah mengikuti c*apture the flag*.	10 25,0	17 42,5	8 20,0	5 12,5	0 0
Permainan CTF membantu saya mempraktikan langkah-langkah *penetration testing* secara terstruktur.	13 32,5	13 32,5	11 27,5	3 7,5	0 0
Permainan CTF membantu saya mengidentifikasi kerentanan sistem secara praktik.	18 45,0	17 42,5	4 10,0	1 2,5	0 0
Permainan CTF membantu saya untuk memberikan pengalaman dalam mengeksploitasi kerentanan sistem.	19 47,5	16 40,0	4 10,0	1 2,5	0 0
Saya dapat mengaplikasikan teknik-teknik *penetration testing* yang dipelajari dalam pelajaran CTF ke *dalam Project Based-Learning* (PBL) *penetration testing.*	13 32,5	22 55,0	3 7,5	2 5,0	0 0
Capture the flag membantu saya meningkatkan kemampuan saya dalam menganalisis hasil *penetration testing.*	15 37,5	16 40,0	7 17,5	2 5,0	0 0
Dengan memainkan *capture the flag* saya dapat mengetahui cara *patching* kerentanan yang ditemukan.	12 30,0	14 35,0	10 25,0	3 7,5	1 2,5
Pembuatan *write-up Capture the Flag* membantu saya memahami dalam pembuatan laporan *penetration testing.*	14 35,0	19 47,5	3 7,5	4 10,0	0 0

Tabel VI menyajikan data frekuensi dalam pengaruh pemahaman praktik pentest setelah memaikan permainan CTF. 10 (25%) responden merasa bahwa CTF membantu memahami pengaplikasian konsep-konsep pentest dengan menanggapi pernyataa sangat setuju, 17 (42,5%) setuju, dan 5 (12,5%) tidak setuju. Dalam mempraktikan langkah-langkah pentest CTF dapat membantu pengaplikasian tersebut secara terstruktur dengan hasil sangat setuju oleh 13 (32,5%) responden, 13 (32,5%) memberikan tanggapan setuju dan 3 (7,5%) tidak setuju terkait hal itu. CTF melatih pengidentifikasian kerentanan sistem secara praktik sangat disetujui oleh 18 (45%), diberikan tanggapan setuju oleh 17 (42,5%) responden dan terdapat 1 (2,5%) responden yang tidak setuju. Didapatkan hasil 19 (47,5%) responden sangat setuju dengan pernyataan CTF memberikan pengalaman dalam mengeksploitasi kerentanan sistem, 16 (40%) responden memberikan jawaban setuju dan 1 (2,5%) responden tidak setuju terhadap hal tersebut. Pemahaman dalam pengaplikasian teknik-teknik pentest ke dalam PBL pentest sangat disetujui oleh 13 (32,5%) responden, disetujui oleh 22 (55%) responden, dan terdapat 2 (5%) responden tidak setuju. Pemahaman dalam analisis hasil dari pentest didukung oleh 15 (37,5%) dengan jawaban sangat setuju dan

e-ISSN: 2548-6861

16 (40%) memberikan jawaban setuju, sedangkan 2 (5%) reponden memilih untuk tidak setuju dengan penrnyataan tersebut. Mengetahui cara *patching* kerentanan memungkinkan untuk dipelajari dari permainan CTF dengan 12 (30%) responden sangat setuju, 16 (40%) responden setuju, sedangkan 3 (7,5%) responden tidak setuju dan 1 (2,5%) responden sangat tidak setuju. Pembuatan *write-up* dari gamifikasi CTF membantu mahasiswa RKS untuk membuat laporan pentest, hal ini didukung oleh tanggapan mahasiswa yaitu 14 (35%) mahasiswa RKS sangat setuju dan 19 (47,5%) setuju, sedangkan yang memilih untuk tidak setuju terdapat 4 (10%) mahasiswa RKS.

TABELVII
FREKUENSI DAN BENTUK PERSENTASE FREKUENSI TANGGAPAN KESADARAN PENTINGNYA PENTEST.

Pernyataan	**SS F%**	**S F%**	**RR F%**	**TS F%**	**STS F%**
Capture the flag membantu saya meningkatkan kesadaran pentingnya implementasi *penetration testing* terhadap suatu sistem.	17 42,5	16 40,0	6 15,0	1 2,5	0 0
CTF memberikan saya pemahaman yang lebih baik tentang etika dan tanggung jawab dalam melakukan *penetration testing*.	14 35,0	14 35,0	7 17,5	2 5,0	3 7,5
Dengan memainkan *capture the flag* terlebih dahulu membuat saya siap melakukan *penetration testing*.	12 30,0	15 37,5	8 20,0	5 12,5	0 0
Capture the flag memberikan gambaran yang jelas kepada saya tentang pentingnya pengujian keamanan secara menyeluruh.	19 47,5	14 35,0	5 12,5	2 5,0	0 0
Capture the flag memberikan perspektif yang lebih luas tentang pentingnya mengikuti tren atau perkembangan terbaru dalam keamanan siber.	18 45,0	17 42,5	4 10,0	1 2,5	0 0

Hasil tanggapan mahasiswa RKS terkait dengan kesadaran akan pentingnya pentest melalui gamifikasi CTF disajikan di table VII. Ditampilkan pada tabel di atas terdapat 17 (42,5%) mahasiswa sangat setuju dan 16 (40%) mahasiswa setuju terkait dengan pernyataan CTF dapat membantu meningkatkan kesadaran pentingnya mengimplementasikan pentest ke suatu sistem dan 1 (2,5%) mahasiswa memilih tidak setuju. Etika dan tanggung jawab dalam pentest dapat disadarkan melalui permainan CTF disetujui oleh 14 (35%) dengan memberikan jawaban sangat setuju dan 14 (35%) mahasiswa memberikan jawaban setuju, sedangkan 2 (5%) mahasiswa memilih tidak setuju dan 3 (7,5%) mahasiswa sangat tidak setuju akan hal ini. Pernyataan CTF membantu responden merasa siap dalam melakukan pentest dirasakan oleh 12 (30%) responden dengan memberikan tanggapan sangat setuju dan 15 (37,5%) memberikan tanggapan setuju, serta 5 (12,5%) responden memilih untuk tidak setuju dengan pernyataan tersebut. 19 (47,5%) responden sangat setuju dan 14 (35%) responden setuju bahwa CTF memberikan gambaran pentingnya untuk pengujian keamanan secara menyeluruh, sedangkan 2 (5%) responden tidak setuju dengan pernyataan ini. Pernyataan CTF dapat memberikan perspektif yang lebih luas terhadap pentingnya mengikuti tren atau perkembangan terbaru dalam keamanan siber dipilih sangat setuju oleh 18 (45%) responden dan dipilih setuju oleh 17 (42,5%) responden, sedangkan terdapat 1 (2,5%) responden yang memilih tidak setuju.

IV. KESIMPULAN

Gamifikasi CTF dapat menjadi salah satu pilihan dalam menambah pemahaman pentest. Hal ini telah dibuktikan dari hasil respon mahasiswa RKS terhadap pemahaman pentest melalui gamifikasi CTF yang telah di analisis. Pemahaman yang didapat dari hasil bermain CTF membantu pengerjaan pentest dari segi pemahaman teori, pemahaman praktik, dan kesadaran pentingnya melakukan pentest.

Hasil respon yang dihasilkan dari mahasiswa RKS mendapatkan kriteria baik dari skala interval persentase skor aktual yang memiliki nilai sebesar 80,55%, yang artinya CTF

merupakan salah satu sarana yang yang disetujui oleh mahasiswa RKS untuk pemahaman pentest. Pernyataan untuk pemahaman teori pentest melalui gamifikas CTF banyak disetujui oleh responden, terbukti dari hasil rata-rata dan frekuensi tanggapan yang ditunjukkan condong ke arah ST dan S. CTF merupakan sarana yang bermanfaat bagi mahasiswa RKS terbukti dari tingginya tingkat persentase frekuensi, yaitu terdapat 52,5% sampel yang memilih ST dengan pernyataan ini. Mahasiswa RKS juga menyetujui bahwa CTF membantu pemahaman praktik pentest, hal ini didukung nilai rata-rata pemahaman praktik pentest dan persentase frekuensi lebih besar condong ke arah tanggapan ST dan S. Menambah pengalaman eksploitasi kerentanan dan pengalaman ini dapat membantu pengerjaan PBL pentest karena terdapat 47,5% sampel yang sangat setuju dengan pernyataan ini. CTF juga berperan untuk menyadarkan para mahasiswa RKS betapa pentingnya pengujian keamanan suatu sistem secara menyeluruh, pernyataan ini diberikan tanggapan ST dengan persentase frekuensi 47,5% dari jumlah sampel.

DAFTAR PUSTAKA

[1] E. Budi, D. Wira, and A. Infantono, "Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0," *Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia (SENASTINDO)*, vol. 3, pp. 223–234, Dec. 2021, doi: 10.54706/senastindo.v3.2021.141.

[2] F. Cremer *et al*., "Cyber risk and cybersecurity: a systematic review of data availability," *Geneva Papers on Risk and Insurance: Issues and Practice*, vol. 47, no. 3, pp. 698–736, Jul. 2022, doi: 10.1057/s41288-022-00266-6.

[3] M. C. Ghanem and T. M. Chen, "Reinforcement learning for efficient network penetration testing," *Information (Switzerland)*, vol. 11, no. 1, Jan. 2020, doi: 10.3390/info11010006.

[4] T. Wilhelm, *Professional Penetration Testing: Creating and Learning in a Hacking Lab*, 2nd ed. Newnes, 2013.

[5] S. V. Cole, "Impact of Capture The Flag (CTF)-style vs. Traditional Exercises in an Introductory Computer Security Class," in *Annual Conference on Innovation and Technology in Computer Science Education, ITiCSE*, Association for Computing Machinery, Jul. 2022, pp. 470–476. doi: 10.1145/3502718.3524806.

[6] Y. Dilekli, "Project-Based Learning," pp. 53–68, 2020, doi: 10.4018/978-1-7998-3146-4.CH004.

[7] F. Marisa, T. M. Akhriza, A. L. Maukar, A. R. Wardhani, S. W. Irianandа, and M. Andarwati, "Gamifikasi (Gamification) Konsep dan Penerapan," *JOINTECS (Journal of Information Technology and Computer Science)*, vol. 5, no. 3, p. 219, Sep. 2020, doi: 10.31328/JOINTECS.V5I3.1490.

[8] A. Pfeiffer, S. Bezzina, N. König, and S. Kriglstein, "Beyond Classical Gamification: In- and Around-Game Gamification for Education," 2020. Accessed: May 28, 2024. [Online]. Available: https://www.um.edu.mt/library/oar/bitstream/123456789/88207/1/Beyond%20classical%20gamification.pdf

[9] J. Vykopal, V. Svabensky, and E. C. Chang, "Benefits and Pitfalls of Using Capture The Flag Games in University Courses," *SIGCSE 2020 - Proceedings of the 51st ACM Technical Symposium on Computer Science Education*, pp. 752–758, Feb. 2020, doi: 10.1145/3328778.3366893.

[10] S. Kucek and M. Leitner, "An Empirical Survey of Functions and Configurations of Open-Source Capture the Flag (CTF) Environments," *Journal of Network and Computer Applications*, vol. 151, p. 102470, Feb. 2020, doi: 10.1016/J.JNCA.2019.102470.

[11] "CTFtime.org / What is Capture The Flag?" Accessed: May 14, 2024. [Online]. Available: https://ctftime.org/ctf-wtf/

[12] H. Gonzalez, R. Llamas, and O. Montaño, "Using a CTF Tournament for Reinforcing Learned Skills in Cybersecurity Course," *Research in Computing Science*, vol. 148, no. 5, pp. 133–141, Dec. 2019, doi: 10.13053/rcs-148-5-15.

[13] K. Leune and S. J. Petrilli, "Using capture-the-flag to enhance the effectiveness of cybersecurity education," in *SIGITE 2017 - Proceedings of the 18th Annual Conference on Information Technology Education*, Association for Computing Machinery, Inc, Sep. 2017, pp. 47–52. doi: 10.1145/3125659.3125686.

[14] A. Aibekova and V. Selvarajah, "Offensive Security: Study on Penetration Testing Attacks, Methods, and their Types," *IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics, ICDCECE 2022*, 2022, doi: 10.1109/ICDCECE53908.2022.9792772.

[15] Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif, dan R&D*. Bandung: PT. Alfabet, 2017.

[16] Owusu-Fordjour, C. 1i, C. K. Koomson, and D. Hanson, "European Journal of Education Studies THE IMPACT OF COVID-19 ON LEARNING-THE PERSPECTIVE OF THE GHANAIAN STUDENT", doi: 10.5281/zenodo.3753586.

[17] "View of EFEKTIVITAS PEMANFAATAN CANVA SEBAGAI MEDIA PEMBELAJARAN DARING." Accessed: May 14, 2024. [Online]. Available: https://prosiding.rcipublisher.org/index.php/prosiding/article/view/132/23

[18] H. Supardi, *Metode Penelitian Pendidikan*. PT Refika Aditama, 2017.

[19] M. A. Almulla, "The Effectiveness of the Project-Based Learning (PBL) Approach as a Way to Engage Students in Learning," *Sage Open*, vol. 10, no. 3, Jul. 2020, doi: 10.1177/2158244020938702/FORMAT/EPUB.