

Pengembangan Sistem Capture the Flag dan Attack-Defense untuk Persiapan Kompetisi Gemastik

Hafizh Fathurrosy¹, Bana Handaga²

¹ Universitas Muhammadiyah Surakarta, Jl. A. Yani, Mendungan, Pabelan, Kec.
Kartasura, Kabupaten Sukoharjo, Jawa Tengah, Indonesia

² Universitas Muhammadiyah Surakarta, Jl. A. Yani, Mendungan, Pabelan, Kec.
Kartasura, Kabupaten Sukoharjo, Jawa Tengah, Indonesia

 Email korespondensi: l200210005@student.ums.ac.id

Abstrak. Pentingnya keamanan siber di era digital mendorong kebutuhan akan tenaga ahli di berbagai sektor. Kompetisi seperti GEMASTIK menguji kemampuan mahasiswa dalam keamanan siber melalui tantangan *Capture The Flag* (CTF) dan simulasi Attack-Defense. Namun, kurangnya platform pelatihan yang memadai menjadi kendala bagi mahasiswa yang ingin mempersiapkan diri. Penelitian ini bertujuan untuk mengembangkan sistem latihan CTF dan Attack-Defense untuk persiapan kompetisi GEMASTIK. Sistem ini memanfaatkan platform CTFd untuk soal CTF dan membangun lingkungan virtual untuk simulasi Attack-Defense. Metode yang digunakan adalah Research and Development (R&D) dengan model waterfall, meliputi analisis kebutuhan, perancangan sistem, implementasi, pengujian, dan evaluasi. Hasil pengujian *black-box testing* menunjukkan semua fungsionalitas sistem berjalan dengan baik (100% berhasil). Evaluasi menggunakan System Usability Scale (SUS) menghasilkan skor rata-rata 82.6, mengindikasikan bahwa sistem ini memiliki kegunaan yang baik menurut pengguna dan layak digunakan sebagai platform latihan. Meskipun demikian, terdapat keterbatasan pada simulasi Attack-Defense karena berjalan di jaringan lokal, sehingga disarankan untuk pengembangan lebih lanjut agar lebih menyerupai kompetisi aslinya.

Kata kunci: keamanan siber; kompetisi; GEMASTIK; CT

PENDAHULUAN

Pengetahuan tentang keamanan siber sangatlah penting untuk kita miliki walau hanya sebatas dasarnya saja, dikarenakan perkembangan zaman dan teknologi informasi yang sangat cepat sehingga meningkatnya jumlah serangan siber seperti phishing, malware, dan eksploitasi sistem telah mendorong pentingnya kesadaran dan kesiapan



dalam menghadapi ancaman tersebut [1]. Maka dari itu kebutuhan akan tenaga ahli dalam keamanan siber sangatlah krusial di berbagai sektor seperti pemerintah, industri, dan pendidikan.

Dari bidang-bidang tersebut yang paling dekat dengan kita untuk sekarang adalah bidang pendidikan, dan seperti yang kita tahu bahwa ilmu tanpa kompetisi tidak akan ada nilainya, maka dari itu Puspresnas Kemendikbudristek mengadakan sebuah kompetisi yang bernama GEMASTIK (Pagelaran Mahasiswa Nasional Bidang Teknologi Informasi dan Komunikasi) untuk menguji kompetensi mahasiswa di bidang teknologi dan komunikasi. Kompetisi ini terdapat beberapa kategori dan salah satunya adalah Cyber Security. Dalam kategori ini, mahasiswa diuji untuk pengetahuan tentang keamanan siber dengan memberikan tantangan dalam bentuk Capture The Flag (CTF) dan simulasi Attack-Defense secara langsung [2].

Capture The Flag (CTF) merupakan sebuah bentuk kompetisi pada bidang keamanan siber yang dirancang untuk melatuh dan mengukur kemampuan peserta dalam mendeteksi, menganalisis, dan mengeksploitasi sebuah sistem. Dalam kompetisi ini peserta ditugaskan untuk mencari sebuah "flag" dalam bentuk string teks tertentu yang disembunyikan dan bisa dicari dengan metode-metode seperti kriptografi, analisis forensik digital, reverse engineering, keamanan aplikasi web, dan eksploitasi sistem [3]

Untuk soal-soal yang digunakan pada CTF ditekankan pada kemampuan teknis seperti eksploitasi kerentanan, reverse engineering, kriptografi, dan analisis forensik digital [4]. Dan untuk simulasi Attack-Defense berfokus pada kerjasama tim dalam menjaga dan menyerang sebuah server yang disediakan dan diadakan secara langsung, pada simulasi ini para mahasiswa selain di uji pada kemampuan teknis nya, mereka juga di uji pada kemampuan koordinasi tim mereka.

Namun dengan kondisi yang sekarang persiapan untuk mengikuti kompetisi GEMASTIK sangat kurang, dan mahasiswa hanya bermodalkan kemampuan mandiri dengan belajar secara daring bahkan tanpa platform yang memadai. Maka dari itu dibutuhkan sebuah sistem agar para mahasiswa yang ingin mengikuti kompetisi GEMASTIK mendapatkan alur pelatihan yang baik.

Untuk menjawab kebutuhan tersebutlah penelitian ini dibuat dan bertujuan untuk mengembangkan sebuah sistem yang bisa memberikan para mahasiswa sebuah gambaran bagaimana mengerjakan soal CTF tantangan nantinya. Sistem yang dibuat setidaknya akan memberikan gambaran bagaimana kegiatan CTF dilaksanakan dengan bantuan platform **CTFd** (Capture The Flag Framework), yang telah digunakan secara luas dalam penyelenggaraan kompetisi CTF di tingkat nasional maupun internasional (CTFd, n.d.). Dan juga dengan membangun lingkungan virtual untuk simulasi Attack-Defense, untuk meningkatkan kesiapan mahasiswa.

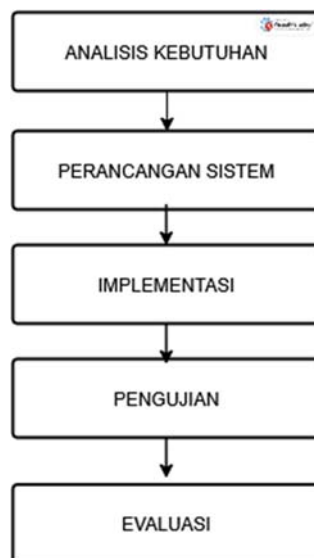


METODE

Bagian metode menjelaskan secara rinci tentang cara penelitian dilakukan, mencakup pendekatan penelitian, desain eksperimen atau observasi, tempat dan waktu penelitian, populasi atau sampel penelitian, teknik pengumpulan data, serta alat dan bahan yang digunakan. Penulis wajib menuliskan metode analisis data yang digunakan secara jelas, baik secara statistik maupun secara deskriptif. Detail metode harus cukup informatif sehingga pembaca dapat menilai validitas serta reliabilitas hasil penelitian, dan memungkinkan penelitian ini untuk direplikasi oleh peneliti lain di kemudian hari. Jelaskan pula alasan pemilihan metode tersebut untuk mencapai tujuan penelitian secara efektif.

Penelitian ini bersifat kualitatif deskriptif dengan pendekatan Research and Development (R&D). Metode R&D dipilih karena memungkinkan peneliti untuk tidak hanya menghasilkan produk (sistem latihan), tetapi juga menguji efektivitasnya dalam konteks penggunaan nyata (Sugiyono, 2017).

Model pengembangan sistem yang digunakan adalah waterfall. Model ini dipilih karena pengembangan yang dilakukan bersifat terstruktur. Waterfall sesuai digunakan dalam pengembangan sistem yang kebutuhan utamanya telah didefinisikan secara jelas di awal (Pressman & Maxim, 2020). Untuk alur pengembangannya bisa kita lihat pada gambar 1 dibawah ini.



Gambar 1. Diagram Alir Pengembangan

Analisis kebutuhan dilakukan untuk mengetahui hal-hal yang perlu disiapkan dalam membangun sistem pelatihan sesuai dengan kebutuhan kompetisi GEMASTIK, termasuk pembagian sesi menjadi babak penyisihan dan final, serta pembentukan tim



peserta. Setelah itu, dilakukan perancangan sistem sebagai blueprint alur kerja, diikuti implementasi berupa deployment platform CTFd untuk sesi penyisihan dan skenario Attack-Defense untuk sesi final, dengan menyesuaikan keterbatasan alat yang tersedia. Sistem yang dibangun kemudian diuji menggunakan metode black-box testing untuk memastikan fungsionalitas sesuai harapan. Terakhir, evaluasi dilakukan melalui observasi dan kuesioner pengguna guna mengukur efektivitas sistem, yang hasilnya dijadikan dasar perbaikan ke depan [8].

Analisis Kebutuhan

Pertama kita akan melakukan analisis kebutuhan, tujuannya adalah untuk mengetahui apa saja yang perlu disiapkan untuk membuat sistemnya. Disini beberapa hal yang perlu kita perhatikan dalam membuat sistem ini adalah kita perlu tahu kebutuhan seperti apa yang diperlukan di kompetisi GEMASTIK dan bisa kita jadikan referensi. Contohnya adalah untuk aturan sistem latihan ini.

a. Fungsional.

Secara fungsionalitas, analisis kebutuhan ini terbagi menjadi dua yaitu kebutuhan admin dan user. Dari segi admin, sistem harus mampu melakukan pengunggahan soal CTF yang nantinya dapat dilihat di sisi user. Sistem juga harus bisa melakukan penghitungan skor secara otomatis dan peringkat dari peserta otomatis dapat tertampil. Lalu kemudian untuk segi user, sistem harus dapat menampilkan soal CTF yang sudah diunggah oleh admin, dan juga pada saat melakukan simulasi attack-defense sistem dapat menghubungkan semua peserta kedalam satu jaringan.

b. Non-Fungsional.

Untuk analisis kebutuhan nonfungsional mencakup perangkat apa saja yang diperlukan untuk membangun sistem kita kali ini. Untuk perangkat keras yang digunakan yaitu terbagi menjadi dua salah satunya untuk server dan yang lain untuk client. Untuk server kita menggunakan PC yang memiliki spesifikasi 12 core CPU, 32GB RAM, 2.5TB Storage. dan untuk user kita menggunakan spesifikasi 12 core CPU, 8GB RAM, 500GB Storage . dibutuhkan juga switch 24-port sebagai terminal penghubung antara server dan client nya dan tentu saja kabel UTP sebagai media kabelnya. kemudian Docker yang digunakan sebagai deploy web karena kita menggunakan jaringan lokal, lalu VMWare Workstation sebagai media untuk menjalankan Virtual Machine (VM), dan yang terakhir adalah VM yang digunakan untuk Attack-Defense yang memiliki spesifikasi OS Linux Ubuntu 24.04.



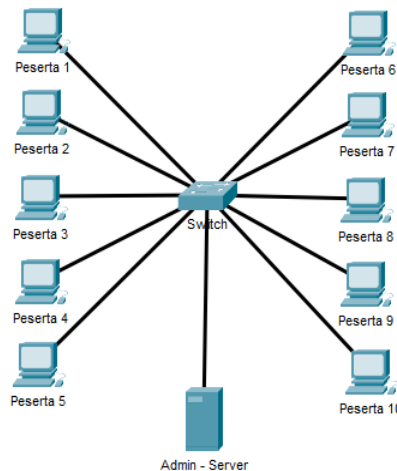
Lalu untuk alat yang kita butuhkan diantaranya yaitu framework CTFd. Framework CTFd itu sendiri adalah sebuah framework Capture The Flag (CTF) open-source yang dirancang untuk menyelenggarakan dan mengelola kompetisi keamanan siber CTF. Secara sederhana, CTFd menyediakan platform lengkap bagi penyelenggara untuk membuat, menyajikan, dan menilai tantangan CTF, serta bagi peserta untuk mengerjakan tantangan tersebut dan mendapatkan poin. Alasan mengapa saya memilih CTFd sebagai platform submit soal CTF dibandingkan dengan platform lain adalah karena platform CTFd ini sudah mencakup fitur-fitur yang dibutuhkan untuk mendukung sistem latihan yang saya buat, Fitur utamanya mencakup manajemen tantangan yang fleksibel untuk berbagai jenis soal, sistem poin otomatis yang bisa statis atau dinamis, dan papan peringkat real-time untuk memicu semangat kompetisi. CTFd juga menyediakan manajemen tim dan pengguna yang efisien, dukungan plugin untuk kustomisasi dan ekstensi fungsionalitas, serta kemampuan untuk menyelenggarakan berbagai mode CTF seperti Jeopardy-style dan Attack-Defense. Dengan antarmuka pengguna yang intuitif untuk admin dan peserta, serta sifatnya yang open-source, CTFd menjadi pilihan populer untuk menciptakan pengalaman CTF yang interaktif dan transparan. Namun salah satu keterbatasan framework ini adalah masih menggunakan bahasa inggris.

Perancangan Sistem

a. Perancangan Lingkungan

Pada proses ini kita akan membuat rancangan pada sistem yang akan digunakan. Pertama, dari perangkat tadi kita bikin sebuah lab sederhana dimana semua PC saling terhubung satu sama lain dan disini kita hanya menghubungkannya dengan kabel dan switch. Dan dikarenakan kita hanya menggunakan jaringan lokal yang menggunakan switch maka untuk peserta hanya kita batasi sebanyak 10 orang. Untuk lebih memperjelas gambarannya, bisa dilihat desain pemetaan pada gambar dibawah.





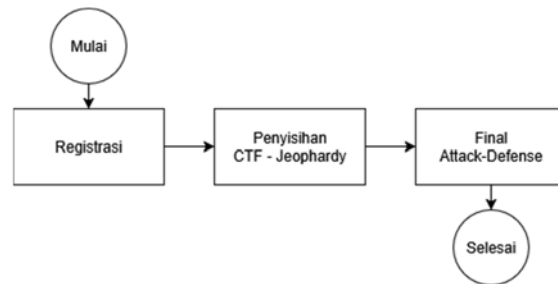
Gambar 2. Pemetaan Rancangan Sistem

Bisa kita lihat bahwa setiap PC dan Server saling terhubung melalui satu switch, dan semua sudah terkonfigurasi alamat IP dengan network yang sama. Dengan begini semua PC bisa saling terhubung. Selanjutnya kita akan melakukan konfigurasi alamat IP pada masing-masing PC, disini saya menggunakan network 192.168.1.0/24, misal PC peserta 1 menggunakan IP 192.168.1.1/24, lalu peserta 2 menggunakan IP 192.168.1.2/24, dan seterusnya, untuk server kita menggunakan IP 192.168.1.99. setiap PC akan di install VM yang nantinya digunakan untuk simulasi Attack-Defense. Dan setelah kita sudah merancang lingkungan sistemnya selanjutnya kita akan merancang alur sistem dan membuat rule atau aturan agar sistem dapat berjalan dengan lancar.

b. Perancangan Alur dan Aturan

Untuk alur sistem dimulai dengan pendaftaran tim. Kemudian akan dilanjutkan di babak penyisihan. Pada babak penyisihan ini akan diadakan kompetisi CTF dengan format jeopardy, jadi nanti akan ada beberapa soal CTF dengan berbagai kategori dan poin skor yang berbeda dan peserta bebas mau mengerjakan soal CTF manapun dengan batas waktu yang sudah ditentukan, tim yang paling banyak mengumpulkan skor akan lanjut ke sesi selanjutnya. Lalu untuk sesi kedua yaitu kompetisi final kita akan buat simulasi Attack-Defense dimana peserta dalam bentuk tim akan diberikan server untuk mereka jaga dan mereka diharuskan untuk menyerang tim lawan. Masing-masing tim akan diberikan "flag" yang nantinya akan mereka jaga, poin didapat dengan mencari "flag" lawan dan melakukan submit di platform CTFd.





Gambar 3. Diagram Alur Sistem

Kemudian untuk aturan dalam sistem ini dibuat dengan beberapa pertimbangan dari infrastruktur yang ada maka dapat dibentuk aturan seperti dibawah ini

Bagian 1: Aturan Umum

- Pendaftaran Tim:
 - Setiap tim harus terdiri dari minimal 1 dan maksimal 2 peserta.
 - Setiap anggota tim harus mendaftar secara individu dan kemudian mendaftarkan tim mereka dengan nama tim yang unik.
- Etika dan Sportivitas:
 - Peserta diharapkan menjunjung tinggi sportivitas dan etika selama kompetisi.
 - Tindakan curang, seperti kolusi antar tim, berbagi jawaban, atau serangan terhadap infrastruktur kompetisi (selain target yang ditentukan), akan mengakibatkan diskualifikasi.
 - Penggunaan alat atau teknik yang tidak etis atau ilegal dilarang keras.
- Lingkungan Kompetisi:
 - Seluruh aktivitas kompetisi akan berlangsung di dalam jaringan lokal yang disediakan.

Bagian 2: Aturan Sesi Penyisihan (CTF)

- Format Soal CTF:
 - Soal CTF akan beragam, meliputi kategori seperti reverse engineering, forensics, web exploitation, cryptography, pwn, dll.
 - Setiap soal CTF memiliki poin yang berbeda, sesuai tingkat kesulitannya dan apabila soal sudah dijawab oleh peserta lain maka skor dari soal akan turun
- Pengunggahan Jawaban:
 - Jawaban (flag) harus diunggah melalui platform CTFd.



- Flag harus dalam format yang benar sesuai petunjuk soal. Contoh :
FKI{contoh_flag}
- Peringkat:
 - Peringkat tim akan ditentukan berdasarkan total poin yang dikumpulkan.
 - Jika ada poin yang sama, tim yang mencapai poin tersebut lebih cepat akan menempati peringkat yang lebih tinggi.
- Dukungan:
 - Panitia akan menyediakan hint atau klarifikasi soal CTF jika diperlukan, namun hanya pada waktu yang ditentukan atau jika ada kesalahan dalam soal CTF.

Bagian 3: Aturan Sesi Final (Attack-Defense)

- Skenario Attack-Defense:
 - Setiap tim akan diberikan server yang sama dengan flag di dalamnya.
 - Tujuan tim adalah mengamankan server mereka sendiri (Defense) dan menyerang server tim lawan untuk mendapatkan flag (Attack).
 - Tim akan diberi waktu selama 2 jam untuk melakukan sesi defense pada server masing-masing, lalu jeda istirahat 1 jam kemudian dilanjutkan sesi attack selama 2 jam
 - Poin diperoleh dari submit flag lawan
- Larangan:
 - Dilarang melakukan serangan Denial of Service (DoS) yang bertujuan melumpuhkan server lawan secara permanen. Fokus serangan adalah mendapatkan flag.
 - Dilarang mengubah direktori dari flag yang sudah dipasang
- Pengawasan:
 - Panitia akan memantau aktivitas jaringan dan server untuk memastikan keadilan dan kepatuhan terhadap aturan.

Implementasi

Untuk platform CTF kita akan menggunakan CTFd yang merupakan framework web CTF yang nantinya dapat kita gunakan sebagai pengunggahan soal-soal CTF. Setelah itu kita tinggal lakukan deploy web CTFd di Docker. Melalui web ini admin akan mengunggah soal dan di web ini juga para peserta melakukan pengerjaan soal.

Konfigurasi awal server CTFd yaitu saya menggunakan sebuah PC server sebagai tempat melakukan deploy web CTFd. Setelah berhasil, maka kita sudah bisa mengakses web nya di jaringan lokal, buka browser dan masukan alamat IP server dengan port 8000. Kemudian kita membuat akun terlebih dahulu, akun ini akan berperan sebagai admin.



Setelah masuk menggunakan akun admin tersebut kita akan dipandu untuk mengkonfigurasi awal web CTFd nya seperti mengisi nama event, dan tampilan dari webnya secara singkat. Setelah melakukan konfigurasinya kita akan langsung masuk ke halaman admin, disini kita akan melihat dashboard dari sistem ini. Lalu sebagai admin, kita bisa langsung melakukan upload soal CTF.

Untuk implementasi Attack-Defense kita akan menggunakan Virtual Machine (VM) yang nantinya akan terinstall linux yang digunakan sebagai server yang nantinya akan digunakan untuk menyerang dan yang akan dipertahankan oleh para peserta. Untuk melakukan submit "flag" lawan, disini kita menggunakan CTFd juga sebagai platformnya. Jadi sebagai admin kita tinggal mengatur soal di CTFd menjadi "flag" dari masing-masing VM.

Pengujian

Disini dilakukan uji fungsionalitas pada sistem yang sudah dibuat dengan metode pengujian blackbox-testing dan kuisisioner untuk penilaian saya menggunakan System Usability Scale (SUS) [9].

Black-box testing adalah metode pengujian perangkat lunak yang mengevaluasi fungsionalitas sistem dari luar, tanpa pengetahuan tentang struktur internal atau kode, memperlakukan perangkat lunak sebagai "kotak hitam" [10]. Penguji berinteraksi hanya dengan input dan output untuk memverifikasi kesesuaian dengan spesifikasi. Teknik umum yang digunakan meliputi Equivalence Partitioning, Boundary Value Analysis, Decision Table Testing, State Transition Testing, Use Case Testing, dan Error Guessing. Dengan metode tersebut kita bisa fokus pada input dan output dari sistem dan apakah fungsionalitas sistemnya sudah seperti apa yang kita harapkan [11].

Sementara itu System Usability Scale (SUS) merupakan metode kuisisioner yang digunakan untuk mengukur skala penggunaan berdasarkan persepsi user. SUS terdapat 10 pertanyaan dengan masing-masing memiliki 5 skala yaitu mulai dari "Sangat Tidak Setuju" sampai "Sangat Setuju" [12].

Evaluasi

Proses ini merupakan proses terakhir pada penelitian kali ini, evaluasi sangatlah penting sebagai proses tinjauan dari produk [13]. Dan untuk sistem ini cukup bisa berjalan dengan baik walaupun dengan keterbatasan infrastruktur yang ada. Tentu saja sistem ini masih dapat dikembangkan lebih jauh lagi sehingga lebih menyerupai kompetisi GEMASTIK yang asli.



HASIL

Hasil dari penelitian diatas menunjukkan bahwa sistem latihan GEMASTIK ini dapat digunakan sebagai platform latihan untuk mempersiapkan diri menghadapi kompetisi aslinya. Walaupun belum terlalu mirip dengan aslinya karena beberapa keterbatasan namun dengan sistem ini setidaknya orang awam bisa menggambarkan bagaimana alur dan kondisi kompetisi GEMASTIK yang asli. Selain itu, penggunaan sistem ini bisa mengikuti perkembangan soal CTF karena kita sebagai admin dapat mengubah, dan menambahkan soal CTF yang terbaru kedalam sistem ini. Yang jadi kekurangan di sistem ini mungkin terletak pada bagian Attack-Defense nya karena memang dengan server yang bersifat lokal jadi kita harus memikirkan alternatif agar simulasi Attack-Defense bisa menyerupai kompetisi aslinya.

Tampilan Sistem

Ketika sistem diakses maka akan diarahkan ke landing page, disini kita diharuskan untuk login terlebih dahulu, untuk tampilannya bisa dilihat di gambar ini.



Gambar 4. Landing Page

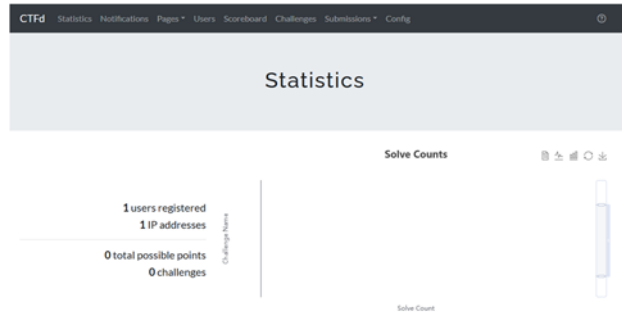
Selanjutnya adalah tampilan halaman login, disini kita disuruh untuk mengisi username dan password untuk masuk ke dalam sistem ini dan menggunakan fiturnya. Kalau belum punya akun untuk masuk kita diharuskan untuk mendaftarkan dulu di menu "Register". Untuk tampilan registrasi dan login bisa dilihat dibawah ini.



Gambar 5. Halaman Registrasi

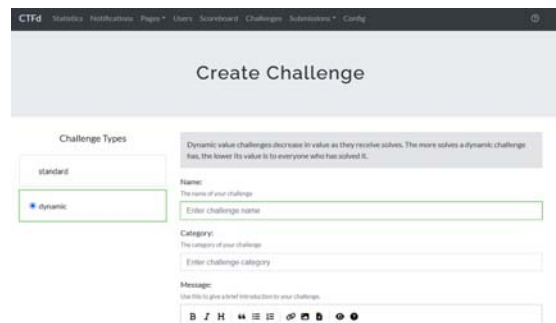
Gambar 6. Halaman Login

Setelah melakukan login dan kita menggunakan akun admin, kita akan melihat halaman dashboard dari admin yang memperlihatkan statistik sistem secara ringkas, bisa kita lihat di gambar berikut ini



Gambar 7. Dashboard (Admin)

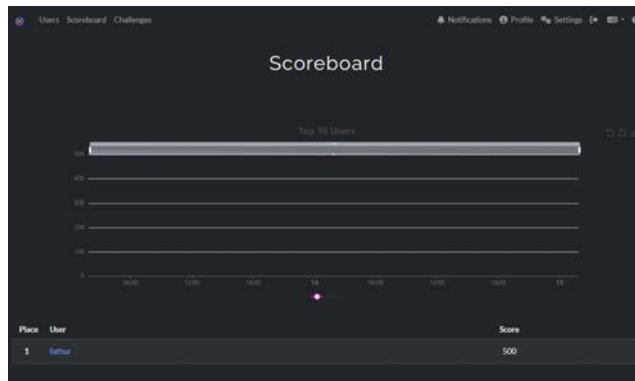
Untuk melakukan upload soal bisa dilakukan pada menu navigasi pada bagian “Challenges” yang nantinya ada tombol create challenges. Disana kita bisa melakukan upload soal CTF yang nantinya akan ditampilkan di peserta (user). Untuk tampilannya seperti di Gambar 8.



Gambar 8. Upload Soal CTF (admin)

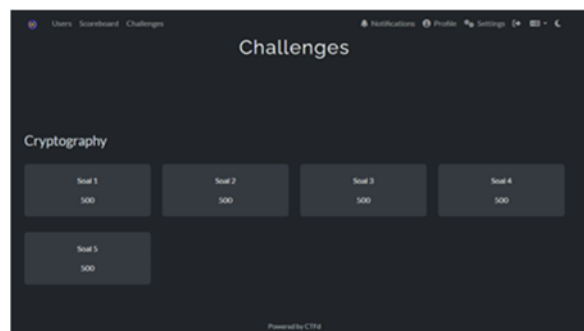
Setelah kita unggah beberapa soal CTF, kita akan coba cek menggunakan akun peserta dan seharusnya soal CTF yang kita buat tadi sudah bisa tertampil seperti gambar dibawah ini.





Gambar 9. Soal CTF dari Admin (User)

Dan terakhir, ketika kita berhasil menjawab soal CTF, maka sistem akan otomatis menghitung skor yang didapatkan dan akan ditampilkan kedalam “Scoreboard”. Menu ini dapat diakses oleh admin maupun peserta (user) dan tampilannya seperti yang terlihat di Gambar 10.



Gambar 10. Scoreboard (admin & user)

Hasil Pengujian Sistem

a. Hasil Pengujian Blackbox

Setelah dilakukan pengujian secara fungsionalitas dengan menggunakan metode blackbox, kita mendapatkan hasil seperti dibawah ini. Fitur yang diuji sudah cukup untuk mencakup kegunaan sistem untuk media latihan GEMASTIK [14].

Tabel 1. *Black-Box* Testing Sistem

No	Skenario	Test Case	Hasil Yang Diharapkan	Hasil Uji	Ket
1	Pendaftaran peserta	Peserta melakukan	Akun peserta sudah terbuat dan bisa melakukan login	Berhasil	100%



		pendaftaran di CTFd			
2	Pengunggahan soal CTF oleh admin	Panitia mengunggah soal CTF di platform CTFd	Soal dapat dilihat oleh para peserta	Berhasil	100%
3	Pengerjaan soal CTF dan pengiriman "flag" oleh peserta	Peserta mengakses soal CTF dan mengirim flag	Sistem menerima flag dan memberikan skor jika benar	Berhasil	100%
4	Sistem penilaian otomatis	Sistem memberikan skor otomatis saat flag benar	Skor tercatat di scoreboard peserta	Berhasil	100%
5	Tampilan scoreboard	Peserta melihat perolehan skor masing-masing	Skor tampil real-time di halaman scoreboard	Berhasil	100%
6	Notifikasi admin	Admin mengirimkan notifikasi (clue atau pengumuman waktu)	Peserta menerima pesan notifikasi	Berhasil	100%
7	Penilaian hasil babak penyisihan	Sistem menampilkan tim dengan skor tertinggi	Tim dengan skor tertinggi lanjut ke babak final	Berhasil	100%
8	Penilaian pengambilan flag di final	Tim berhasil mengambil flag	Skor tambahan diberikan jika flag ditemukan	Berhasil	100%



lawan dalam
waktu serangan

b. Hasil Pengujian System Usability Scale

System Usability Scale (SUS) terbagi menjadi 10 pertanyaan: “Sangat Tidak Setuju” (STS) dengan skor 1 sampai “Sangat Setuju” (SS) dengan skor 5. Untuk perhitungannya, pada pertanyaan dengan nomor ganjil, skor yang diserahkan oleh narasumber dikurangi 1. Sedangkan pada pertanyaan dengan nomor genap, skor akhir dihitung dengan mengurangkan nilai 5 dari skor yang diserahkan oleh narasumber. Total nilai SUS kemudian dihitung melalui penjumlahan skor dari masing-masing pertanyaan, lalu hasilnya dikalikan 2,5 [15] . Untuk rumus matematikanya seperti dibawah ini

Misalkan P_i adalah skor yang diberikan pengguna untuk pertanyaan ke- i :

$$SUS_{score} = \left(\sum_{i \in \{1,3,5,7,9\}} (P_i - 1) + \sum_{i \in \{2,4,6,8,10\}} (5 - P_i) \right) \times 2.5$$

Tabel 2. Tabel SUS

No.	Skor Hasil Hitung										Jumlah	Nilai (Jumlah x 2,5)
	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10		
1.	3	3	3	3	2	3	3	3	3	2	28	70
2.	2	4	4	4	4	3	3	3	4	3	34	85
3.	2	3	3	3	3	3	3	3	3	3	29	73
4.	4	2	3	4	4	2	4	3	2	3	31	78
5.	4	4	4	2	4	2	4	3	4	4	35	88
6.	2	4	4	4	4	4	4	4	3	4	37	93
7.	4	4	4	4	3	3	3	4	3	3	35	88
8.	4	1	4	2	4	4	4	4	4	4	35	88



9.	3	3	3	2	3	3	3	3	2	2	27	68
10.	2	4	4	4	4	4	4	4	4	4	38	95
TOTAL RATA-RATA											82.6	

Setelah mengetahui skor akhir dari SUS kita bisa simpulkan bahwa sistem ini berkategori baik menurut pengguna dengan skor 82.6 dan pengujian SUS memiliki tiga kategori penilaian, yaitu Not Acceptable, Marginal, dan Acceptable (Brooke, 2013).

PEMBAHASAN

Sistem pelatihan untuk persiapan kompetisi GEMASTIK yang dikembangkan dalam penelitian ini menunjukkan hasil yang menjanjikan, meskipun terdapat beberapa keterbatasan. Hasil pengujian fungsionalitas menggunakan metode black-box testing menunjukkan bahwa semua fungsionalitas sistem berjalan dengan baik, mencapai 100% keberhasilan. Ini mencakup pendaftaran peserta, pengunggahan soal CTF oleh admin, pengerjaan soal CTF oleh peserta, sistem penilaian otomatis, tampilan scoreboard, notifikasi admin, penilaian hasil babak penyisihan, dan penilaian pengambilan flag di final2.

Evaluasi menggunakan System Usability Scale (SUS) menghasilkan skor rata-rata 82.6, yang menunjukkan bahwa sistem ini memiliki kegunaan yang baik menurut pengguna dan layak digunakan sebagai platform latihan. Skor ini menempatkan sistem dalam kategori "Acceptable" berdasarkan penilaian SUS4.

Sistem ini berhasil menyediakan platform untuk latihan CTF dengan memanfaatkan CTFd, yang memungkinkan admin untuk mengunggah soal dan peserta untuk mengerjakan tantangan. Keunggulan CTFd meliputi manajemen tantangan yang fleksibel, sistem poin otomatis, papan peringkat

real-time, manajemen tim dan pengguna, dukungan plugin, dan antarmuka pengguna yang intuitif6. Untuk simulasi Attack-Defense, lingkungan virtual dibangun menggunakan Virtual Machine (VM) berbasis Linux Ubuntu 24.04 yang terhubung dalam jaringan lokal, dengan CTFd juga digunakan untuk pengiriman flag.

Meskipun sistem ini dapat digunakan sebagai platform latihan dan memberikan gambaran tentang alur dan kondisi kompetisi GEMASTIK yang asli, terdapat keterbatasan pada simulasi Attack-Defense karena berjalan di jaringan lokal. Keterbatasan ini menyarankan perlunya pengembangan lebih lanjut agar simulasi lebih menyerupai kompetisi aslinya. Namun, kemampuan admin untuk terus memperbaiki



dan menambahkan soal CTF terbaru menjadikan sistem ini relevan dengan perkembangan soal CTF.

KESIMPULAN

Kesimpulan penelitian kali ini adalah dengan dibuatnya sistem latihan GEMASTIK ini dapat memudahkan para mahasiswa untuk mencari platform belajar dan sistem ini dapat bekerja dengan cukup baik walaupun hanya berjalan di jaringan lokal. Dengan pengujian fungsionalitas yang memiliki hasil yang baik dan juga pengujian menggunakan SUS yang menghasilkan skor yang cukup baik pula menjadikan sistem ini bisa dikatakan layak untuk digunakan.

UCAPAN TERIMA KASIH

Ucapan terima kasih kami sampaikan kepada pihak laboratorium komputer UMS atas dukungan teknis dan fasilitas yang telah diberikan selama penelitian ini berlangsung. Kami juga mengucapkan terima kasih kepada dosen pembimbing atas bantuan dan masukan yang berharga dalam penyusunan artikel ini.

DAFTAR PUSTAKA

- [1] M. Conti, A. Dehghantanha, and T. Dargahi, "Cyberthreat Intelligence: Challenges and Opportunities".
- [2] Puspresnas *et al.*, "PEDOMAN PAGELARAN MAHASISWA NASIONAL BIDANG TIK TAHUN 2023 Tema TIK untuk Pembangunan Indonesia Maju dan Berkelanjutan".
- [3] V. Švábenský, P. Čeleda, J. Vykopal, and S. Brišáková, "Cybersecurity Knowledge and Skills Taught in Capture the Flag Challenges", doi: 10.1016/j.cose.2020.102154.
- [4] C. Sauerwein, A. Yasin, and C. Huth, "Capture the Flag as a Learning Method for Cybersecurity: Analysis and Research Directions. In 2017 International Conference on Interactive Collaborative Learning (ICL). , " 2017.
- [5] "CTFd : The Easiest Capture The Flag Platform." Accessed: Jul. 25, 2025. [Online]. Available: <https://ctfd.io/>
- [6] Sugiyono, "Metode Penelitian Dan Pengembangan Untuk Bidang Pendidikan, Manajemen, Sosial, Teknik : Research And Development/ R&D , " 2017.
- [7] R. S. Pressman and B. R. Maxim, "Software Engineering: A Practitioner's Approach (9th ed.). McGraw-Hill Education., " 2020.
- [8] S. W. Ambler, "Agile Modeling: Effective Practices for eXtreme Programming and the Unified Process. John Wiley & Sons. , " 2002.
- [9] B. Beizer, "Software Testing Techniques (2nd ed.). Van Nostrand Reinhold. , " 1990.



- [10] B. Beizer, "Black-box testing: techniques for functional testing of software and systems," *John Wiley & Sons*, 1995.
- [11] D. J. Mosley and B. Posey, "Just Enough Software Test Automation," *Prentice Hall*, 2002.
- [12] P. Vlachogianni and N. Tselios, "Perceived usability evaluation of educational technology using the System Usability Scale (SUS): A systematic review. *Journal of Research on Technology in Education*," 2021.
- [13] L. Judijanto, "Metodologi research and development: Teori dan penerapan metodologi RnD."
- [14] G. J. Myers, T. Badgett, and T. M. Sandler, "The Art of Software Testing (3rd ed.)," *John Wiley & Sons*, 2012.
- [15] C. Kaner, J. Bach, and R. Pettichord, "Lessons Learned in Software Testing: A Context-Driven Approach.," *John Wiley & Sons*, 2002.

