BAB I
PENDAHULUAN

1.1 Latar Belakang

Keamanan informasi adalah sebuah disiplin ilmu yang melibatkan sebuah rangkaian proses dan praktik yang digunakan untuk melindungi data, sistem, dan jaringan dari ancaman atau akses yang tidak sah. Disiplin ini meliputi pengidentifikasian, pengevaluasian, dan pengelolaan risiko terkait dengan keamanan informasi serta penerapan teknologi, prosedur, dan praktik yang tepat untuk melindungi informasi dari kerusakan, kehilangan, atau pengungkapan yang tidak sah [1].

Keamanan informasi memiliki aspek utama yang juga menjadi pokok bahasan, batasan, dan standarisasi yang meliputi:

- Kerahasiaan: Aspek yang berkaitan dengan perlindungan terhadap informasi agar tidak dapat diakses oleh pihak yang tidak berhak. Hal ini menguatkan standarisasi organisasi dan pengguna melalui kebijakan keamanan sistem informasi [2].
- Integritas: Aspek yang berkaitan dengan keotentikan dan keutuhan data yang menunjukkan bahwa data tersebut benar benar asli dari sumber yang berwenang serta tidak mengalami perubahan atau manipulasi yang tidak sah [2].
- Ketersediaan: Aspek yang berkaitan dengan ketersediaan akses terhadap informasi yang diperlukan dimana dapat memastikan bahwa informasi dapat diakses oleh pihak yang berhak kapanpun tanpa ada gangguan atau kegagalan sistem [2].
- Keaslian: Aspek yang Berkaitan dengan keabsahan suatu entitas atau pengguna dalam melakukan transaksi atau akses terhadap sistem sebagai bentuk identifikasi pengguna [2].
- Keandalan: Aspek yang berkaitan dengan konsistensi dan keandalan sistem keamanan informasi yang dapat konsisten melindungi informasi dari ancaman dan serangan [2].

Dalam era digital yang semakin maju saat ini, keamanan informasi menjadi sangat krusial karena semakin banyak informasi yang disimpan dan dibagikan melalui jaringan internet. Risiko keamanan informasi meliputi serangan peretasan, pencurian identitas, serta pengungkapan data sensitif. Oleh karena itu, organisasi harus memberikan prioritas utama pada keamanan informasi dan terus-menerus mengevaluasi serta meningkatkan praktik keamanan mereka agar dapat melindungi data dan sistem mereka dari kemungkinan ancaman [3].

Dari permasalahan diatas, tim AMIKOM DEEPWEB fokus untuk mengadakan sharing session mengenai keamanan di bidang keamanan informasi dan mengikuti kompetisi dibidang keamanan informasi seperti GEMASTIK XIV – Cyber Security pada tahun 2021 dalam rangka meningkatkan wawasan dalam bidang keamanan computer dan informasi.

1.2 Uraian Lomba

GEMASTIK atau Pagelaran Mahasiswa Nasional Bidang Teknologi Informasi dan Komunikasi, merupakan program Pusat Prestasi Nasional, Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi. Program ini ditujukan untuk meningkatkan kompetensi mahasiswa Indonesia, sehingga mampu mengambil peran sebagai agen perubahan dalam memajukan TIK dan pemanfaatannya, baik ketika masih dalam masa studi maupun kelak sesudah lulus studi. Pagelaran ini diselenggarakan bersama salah satu perguruan tinggi yang ditunjuk oleh Pusat Prestasi Nasional, Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi sebagai penyelenggara.

Pada aktivitas tersebut, keamanan siber menjadi topik utama sebagai hal yang melatarbelakangi kondisi masyarakat sekarang ini. Melalui jalur kegiatan kompetisi keamanan siber tingkat nasional, kami mencoba untuk meningkatkan potensi skill yang dimiliki di ranah keamanan sistem. Hal ini menjadi ketertarikan yang unik karena melihat keadaan Indonesia menjadi negara dengan peringkat ke-6 negara di seluruh dunia perihal keamanan siber, hal tersebut menjadi motivasi untuk peningkatan sistem karena dapat dikatakan Indonesia masih tergolong rentan

terhadap kesadaran keamanan siber dan keamanan informasinya baik secara teknis maupun sosial.

Dalam kegiatan kompetisi GEMASTIK XIV tahun 2021 cabang Keamanan Siber ini memiliki dukungan kompetensi penggalian seni keamanan siber adalah dari kemampuan sistem administrator dimana menjadi hal mendasar di dalam fundamental konsep jaringan dan cara kerja sistem operasi. Kemudian, ilmu forensik dan web security menjadi hal lanjutan karena dalam kompetisi ini serta di lingkungan nyata, hal tersebut digunakan untuk analisis kerentanan pada suatu sistem seperti malware, kriptografi, reverse engineering, dan ilmu infrastruktur jaringan.

Secara umum, divisi keamanan siber GEMASTIK merupakan kompetisi yang baik untuk meningkatkan kompetensi dan pengetahuan siswa dalam bidang keamanan siber, serta untuk meningkatkan kesadaran akan masalah keamanan di dunia teknologi [4].

1.3 Keunikan Event

GEMASTIK (Gemar Menyelami Ilmu Teknik dan Informatika) adalah kegiatan tahunan yang diselenggarakan oleh Kementerian Pendidikan dan Kebudayaan (Kemendikbud) untuk meningkatkan kompetensi dan minat siswa dalam bidang teknologi informasi dan komunikasi (TIK). Salah satu divisi dari GEMASTIK adalah divisi keamanan siber [4].

Divisi keamanan siber GEMASTIK memiliki beberapa keunikan dibandingkan dengan kompetisi keamanan siber lainnya, diantaranya:

1. Ditujukan untuk Mahasiwa perguruan tinggi: Divisi keamanan siber GEMASTIK ditujukan untuk mahasiswa perguruan tinggi, sehingga dapat memperkenalkan bidang keamanan siber pada generasi muda sejak dini.
2. Kompetisi online: Divisi keamanan siber GEMASTIK diadakan secara online, sehingga memungkinkan peserta dari seluruh Indonesia untuk ikut serta dalam kompetisi.

3. Fokus pada aspek teknis: Divisi keamanan siber GEMASTIK fokus pada aspek teknis dalam keamanan siber, seperti cracking password, encryption, dan lain-lain, sehingga dapat meningkatkan kompetensi siswa dalam aspek tersebut.
4. Ditinjau oleh pakar: Divisi keamanan siber GEMASTIK ditinjau oleh pakar dalam bidang keamanan siber, sehingga dapat memberikan feedback yang berkualitas bagi peserta.
5. Menumbuhkan semangat kompetitif: Divisi keamanan siber GEMASTIK menumbuhkan semangat kompetitif dan kerja sama antar peserta untuk menyelesaikan tantangan yang diberikan.
6. Menambah wawasan dan kesadaran: Divisi keamanan siber GEMASTIK dapat memberikan wawasan dan kesadaran akan masalah keamanan siber yang mungkin terjadi dalam dunia teknologi dan memberikan solusi untuk mengatasinya.

1.4 Manfaat dan Tujuan Event

Capture the Flag (CTF) adalah kompetisi yang menantang para peserta untuk menemukan dan menyelesaikan tantangan keamanan komputer dalam waktu yang ditentukan. CTF dapat memberikan beberapa manfaat bagi para peserta [5]. Diantaranya :

1. Peningkatan kompetensi dan pengetahuan: CTF menantang peserta untuk mengaplikasikan pengetahuan teknis mereka dalam menyelesaikan tantangan yang diberikan, sehingga dapat meningkatkan kompetensi dan pengetahuan mereka dalam bidang keamanan komputer.
2. Mengenal potensi diri: CTF memberikan kesempatan bagi peserta untuk mengevaluasi dan mengenal potensi diri mereka dalam bidang keamanan computer.
3. Menumbuhkan semangat kompetitif: CTF meningkatkan semangat kompetitif dan kerja sama antar peserta untuk menyelesaikan tantangan yang diberikan.
4. Memperkuat kesadaran akan masalah keamanan: CTF meningkatkan kesadaran akan masalah keamanan yang mungkin terjadi dalam dunia teknologi dan memberikan solusi untuk mengatasinya.
5. Memperluas jaringan: CTF memberikan kesempatan bagi peserta untuk berkomunikasi dan berinteraksi dengan peserta lainnya, sehingga dapat memperluas jaringan mereka dalam bidang keamanan komputer.
6. Memperoleh pengalaman praktis: CTF memberikan kesempatan bagi peserta untuk mendapatkan pengalaman praktis dalam menyelesaikan tantangan yang diberikan dan mendapatkan feedback dari para pakar yang mengevaluasi hasil kerja peserta.