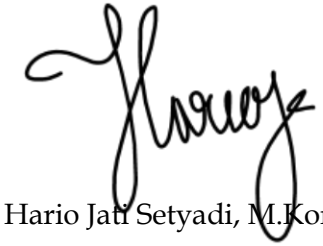
MATA KULIAH KEAMANAN INFORMASI

	KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET DAN TEKNOLOGI **UNIVERSITAS MULAWARMAN** **FAKULTAS TEKNIK** **SISTEM INFORMASI**	No. Dokumen	01/SI/RPS/07/2024
		Tanggal Terbit	12 Juli 2024
		Nomor Revisi	1

RENCANA PEMBELAJARAN SEMESTER

Mata Kuliah	Kode Mata Kuliah	Rumpun Mata Kuliah	Bobot (SKS)	Semester	Tgl. Penyusunan
Keamanan Informasi		Komputer	3	4	10 Juli 2024

	Koordinator Mata Kuliah	TIM Pengampu Mata Kuliah	Koordinator Program Studi
Otorisasi / Pengesahan	 Hario Jati Setyadi, M.Kom.		 Putut Pamilih Widagdo, M.Kom.

Capaian Pembelajaran (CP)	Capaian Pembelajaran Lulusan Program Studi (CPL-PRODI) yang Dibebankan Pada Mata Kuliah	
	CP1	Memahami Konsep Dasar dan Tren Terbaru Keamanan Informasi
	CP2	Menganalisis Kebutuhan dan Risiko Keamanan Informasi di Era Digital
	CP3	Merancang Sistem Keamanan Informasi yang Adaptif dan Proaktif
	CP4	Mengevaluasi dan Mengoptimalkan Sistem Keamanan Informasi dengan Teknik Modern

	CP5	Menerapkan Teknologi Keamanan Informasi Terkini dan Emerging Technologies
	CP6	Mematuhi Hukum, Peraturan, dan Etika dalam Keamanan Informasi Global
	CP7	Berkolaborasi dengan Tim
	Capaian Pembelajaran Mata Kuliah (CPMK)	
	Capaian Pembelajaran Mata Kuliah (CPMK) Keamanan Informasi mengharapkan mahasiswa mampu memahami konsep dasar keamanan informasi dan menganalisis kebutuhan serta risiko terkait teknologi terbaru. Mahasiswa juga harus dapat merancang, mengevaluasi, dan mengoptimalkan sistem keamanan, serta menerapkan teknologi keamanan terkini. Selain itu, mahasiswa diharapkan mampu berkomunikasi tentang isu-isu keamanan, bekerja dalam tim, mematuhi hukum dan etika global, dan mengikuti perkembangan terbaru dalam bidang keamanan informasi.	
PIP yang Diintegrasikan	a. Integritas: Mahasiswa didorong untuk berperilaku jujur, bertanggung jawab, dan memiliki etika profesional dalam setiap aspek pembelajaran dan penerapan keamanan informasi. b. Kerja sama: Mahasiswa belajar bekerja sama dalam tim, baik dalam diskusi kelas, proyek kelompok, maupun dalam simulasi kasus keamanan informasi. c. Kreativitas: Mahasiswa diharapkan mampu berpikir kreatif dalam merancang solusi keamanan informasi yang inovatif dan efektif. d. Tanggung jawab: Mahasiswa dilatih untuk bertanggung jawab terhadap tugas dan proyek yang diberikan, serta memahami pentingnya menjaga keamanan informasi di lingkungan profesional. e. Penguasaan Alat dan Teknologi Terkini: Mahasiswa dilatih menggunakan perangkat lunak dan alat keamanan informasi terkini seperti Wireshark, Metasploit, dan Nessus untuk mengatasi tantangan keamanan modern. f. Adaptasi Terhadap Teknologi Baru: Mahasiswa diajarkan untuk terus mengikuti dan mengadaptasi teknologi baru dalam keamanan informasi seperti AI-driven security dan blockchain. g. Kepatuhan Terhadap Hukum dan Etika: Mahasiswa memahami dan mematuhi hukum, peraturan, dan standar industri yang berlaku terkait keamanan informasi, serta mampu mengidentifikasi dan menangani isu-isu etika dalam praktik profesional. h. Keterampilan Komunikasi: Mahasiswa dilatih untuk berkomunikasi secara efektif mengenai isu-isu keamanan informasi kepada berbagai pemangku kepentingan, baik teknis maupun non-teknis. i. Pemahaman Konsep Dasar: Mahasiswa mendapatkan pemahaman yang mendalam tentang konsep dasar keamanan informasi, termasuk ancaman, kerentanan, dan risiko. j. Kemampuan Analisis dan Evaluasi: Mahasiswa mampu menganalisis kebutuhan dan risiko keamanan informasi serta mengevaluasi dan mengoptimalkan sistem keamanan informasi dengan teknik modern.	

Deskripsi Mata Kuliah	mata kuliah ini membahas prinsip-prinsip dan praktek keamanan sistem informasi yang ada yang dibahas secara mendalam dan komprehensif. Topik meliputi konsep dasar keamanan sistem informasi, teknik penyerangan umum, kebijakan keamanan bersama, kriptografi, otentikasi, kontrol akses, deteksi intrusi jaringan, keamanan jaringan, masalah hukum dan etika dalam keamanan sistem informasi.	
Referensi	1. Stallings, W., & Brown, L. (2019). Computer Security: Principles and Practice. Pearson. 2. Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems (3rd ed.). Wiley. 3. Harris, S. (2019). CISSP All-in-One Exam Guide, Eighth Edition. McGraw-Hill Education. 4. Ferguson, N., Schneier, B., & Kohno, T. (2021). Cryptography Engineering: Design Principles and Practical Applications. Wiley. 5. Bishop, M. (2021). Introduction to Computer Security. Addison-Wesley. 6. Offensive Security. (2021). *Kali Linux Revealed: Mastering the Penetration Testing Distribution*. Offensive Security. 7. Conti, M., Dragoni, N., & Gottardo, S. (2020). Blockchain Security and Privacy. Springer. 8. Weippl, E. (2022). Security in Computing and Information Technology. Springer. 9. Easttom, C. (2023). Network Defense and Countermeasures: Principles and Practices. Pearson. 10. Juels, A., & Garay, J. (2024). Cryptographic Systems for Secure Applications. Cambridge University Press. 11. Stallings, W. (2023). Network Security Essentials: Applications and Standards. Pearson.	
Media Pembelajaran	**Perangkat lunak :**	**Perangkat keras :**
	Figma	Laptop
Mata Kuliah Prayarat (Jika ada)	Manajenen jaringan Komputer , Sistem Operasi	

Perte-muan ke	Sub-CPMK	Indikator	Bahan Kajian	Strategi Pembelajaran (Model dan Metode)	Pengalaman Belajar Mahasiswa	Penilaian			Referensi
						Jenis	Kriteria	Bobot (%)	
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)
1	Mampu memahami target kemampuan mahasiswa yang ingin dicapai melalui mata kuliah ini.	a. Menjelaskan definisi, tugas, tujuan serta manfaat pengantar keamanan bagi sistem komputer. b. Menceritakan kembali sejarah perkembangan keamanan SI. c. Menjelaskan metode dalam keamanan SI .	Pendahuluan pengantar sistem operasi : a. Definisi Tujuan pengantar keamanan SI b. Fungsi dan sasaran pengantar sistem operasi c. Sejarah perkembangan keamanan SI d. Konsep keamanan SI	Ceramah dan Tanya Jawab		Tertulis, uraian subyektif	a. Mencatat semua informasi secara ringkas b. Kelengkapan Kebenaran penjelasan c. Kebenaran identifikasi		1,2,3
2.	memahami dengan baik tentang keamanan fisik dari jaringan komputer pada suatu sistem informasi	Menjelaskan keamanan pada lapisan OSI	Physical Layer Security	Ceramah dan Diskusi	Menjelaskan keamanan pada lapisan OSI Physical Layer Security	Tertulis, uraian subyektif	a. Tingkat komunikatif diskusi b. Ketepatan penjelasan c. Ketepatan identifikasi kasus		
3	memahami dengan baik tentang keamanan fisik dari jaringan komputer pada suatu sistem informasi	Mahasiswa mampu merancang sistem keamanan informasi yang efektif	Kontrol akses, enkripsi, otentikasi, kebijakan dan prosedur keamanan	Ceramah, Diskusi, Studi Kasus	Diskusi kasus, tugas merancang	Tertulis, uraian subyektif	a. Tingkat komunikatif diskusi b. Ketepatan penjelasan c. Ketepatan Analisis		

							kasus		
4	memahami pentingnya pengamanan aplikasi web	a. Menjelaskkan Manfaat keamanan web b. Menjelaskan kasus keamanan pada dunia nyata	Web Security, Web Firewall	Ceramah, Tanya Jawab	Tertulis, uraian subyektif		a. Tingkat komunikatif Diskusi. b. Ketepatan penjelasan Ketepatan Analisis kasus		
5	memahami pentingnya keamanan Web Server dengan melihat kasus nyata yang terjadi di dunia nyata	a. Menjelaskan definisi Access control b. Menjelaskan bagaimana proses control akses	Access Control	Ceramah, Tanya Jawab	Tertulis, uraian subyektif		a. Tingkat komunikatif Diskusi. b. Ketepatan penjelasan Ketepatan Analisis kasus		
6	Mematuhi hukum, peraturan, dan etika dalam keamanan informasi global	Mahasiswa memahami dan mematuhi hukum dan etika dalam keamanan informasi	Hukum, peraturan, standar industri, etika profesional global	Ceramah, Diskusi	Diskusi hukum dan etika, tugas analisis	Tugas	Kepatuhan hukum dan etika		
7	Mengikuti perkembangan tren dan isu keamanan informasi	Mahasiswa mampu mengikuti perkembangan tren dan isu keamanan informasi	Tren terbaru, isu keamanan, adopsi teknologi baru	Diskusi, Studi Kasus	Diskusi tren terbaru, studi kasus	Tugas dan Diskusi			
8									
9	Persiapan Lab Web Penetration dan OS yang akan di pakai	Mahasiswa mampu mempersiapkan lingkungan lab untuk pengujian penetrasi web dan sistem operasi yang diperlukan	Persiapan lingkungan lab, instalasi dan konfigurasi alat dan sistem operasi	Praktikum, Ceramah	Instalasi dan konfigurasi alat dan sistem operasi	Praktikum			

10	Jenis-jenis Keamanan Web Aplikasi dan Server	Mahasiswa mampu menjelaskan dan menerapkan berbagai teknik keamanan web aplikasi dan server	Jenis-jenis keamanan web aplikasi, teknik keamanan server, firewall, IDS/IPS	Ceramah, Praktikum	Diskusi teknik keamanan, praktikum implementasi keamanan	Tugas dan Praktikum			
11	Mahasiswa mampu melakukan reconnaissance dan OSINT untuk mencari informasi terkait suatu target.	1. Mahasiswa dapat menjelaskan konsep dan tujuan dari usability testing. 2. Mahasiswa mampu merancang dan melaksanakan usability testing. 3. Mahasiswa mampu mengumpulkan dan menganalisis data dari usability testing untuk memberikan rekomendasi perbaikan.	Usability testing: konsep, perencanaan, pelaksanaan, analisis	Ceramah, Praktikum	Praktikum merancang dan melaksanakan usability testing				
12	Mahasiswa mampu melakukan penetration testing dasar.	Mahasiswa mampu melakukan penetration testing dasar	Teknik penetration testing dasar, metodologi pengujian, alat dan teknik yang digunakan dalam penetration testing	Ceramah, Praktikum	Praktikum penetration testing	Tugas, Praktikum			
13	Mahasiswa mengenal berbagai kerentanan yang ada pada aplikasi web dan melakukan	Mahasiswa mampu mengidentifikasi kerentanan aplikasi web dan melakukan pengujian	Kerentanan aplikasi web, pengujian dasar, penggunaan Burp Suite	Ceramah, Praktikum	Praktikum pengujian aplikasi web menggunakan Burp Suit	Tugas dan Praktikum			

	pengujian dasar menggunakan tools Burp Suite.	dasar menggunakan Burp Suite							
14-15	Mahasiswa mampu melakukan pengujian lanjutan untuk kerentanan aplikasi web yang tidak dapat ditemukan oleh tools scanner.	Mahasiswa mampu mengidentifikasi dan mengeksploitasi kerentanan aplikasi web yang tidak terdeteksi oleh tools otomatis	Kerentanan aplikasi web lanjutan, teknik eksploitasi manual, bypass scanner tools	Ceramah, Praktikum	Praktikum pengujian manual aplikasi web	Tugas			
16	Presentasi Akhir Project / Quiz 2 / UAS								

Samarinda, 11 Juli 2024

Praktisi	Dosen Pengampu Mata Kuliah	Koordinator Program Studi
Syaiful Andy, ST., MT.	**Hario Jati Setyadi, S,Kom., M.Kom.**	**Putut Pamilih Widagdo, S.Kom.,M.Kom.**

Tabel Revisi RPS Mata Kuliah Keamanan Informasi

No.	Bagian yang Berubah	Sebelum Berubah	Setelah Berubah	Pertemuan	Halaman
1.	Capaian Pembelajaran Mata Kuliah				
	Memahami pentingnya pengamanan aplikasi web	Memahami pentingnya pengamanan aplikasi web	Jenis-jenis Keamanan Web Aplikasi dan Server	10	
	Memahamivpentingnya pengamanan aplikasi web	Memahami pentingnya pengamanan aplikasi web	Mahasiswa mampu melakukan reconnaissance dan OSINT untuk mencari informasi terkait suatu target.	11	
	Memahami pentingnya keamanan konten dengan melihat kasus nyata yang terjadi di dunia nyata	a. Menjelaskan konsep autentifikasi dan kelola akun b. MenjelaskanProses pengamanan konten dengan autentifikasi	Mahasiswa mampu melakukan penetration testing dasar.	12	
	Memahami pentingnya penggunaan metode kriptografi dalam SI	Memahami pentingnya penggunaan metode kriptografi dalam SI	Mahasiswa mengenal berbagai kerentanan yang ada pada aplikasi	13	

No.	Bagian yang Berubah	Sebelum Berubah	Setelah Berubah	Pertemuan	Halaman
			web dan melakukan pengujian dasar menggunakan tools Burp Suite.		
	Memahami pentingnya penggunaan metode kriptografi dalam SI	Memahami pentingnya penggunaan metode kriptografi dalam SI	Mahasiswa mampu melakukan pengujian lanjutan untuk kerentanan aplikasi web yang tidak dapat ditemukan oleh tools scanner.	14-15	

Samarinda, 11 Juli 2024

Praktisi	Dosen Pengampu Mata Kuliah	Koordinator Program Studi
Syaiful Andy, ST., MT.	**Hario Jati Setyadi, S,Kom., M.Kom.**	**Putut Pamilih Widagdo, S.Kom.,M.Kom.**