<table>
<tr><td rowspan="3"></td><td colspan="2">KEMENTERIAN RISET, TEKNOLOGI DAN PENDIDIKAN TINGGI
INSTITUT INFORMATIKA DAN BISNIS DARMAJAYA
Jl. Zainal Abidin Pagar Alam No.93 Labuhan Ratu – Bandar Lampung, 35142
FORMULIR
RENCANA PEMBELAJARAN SEMESTER (RPS)</td><td>No. Dokumen
4FM-DP40103</td></tr>
<tr><td>No. Revisi
00</td><td>Hal
1 dari …</td><td>Tanggal Terbit
03 November 2021</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td>Mata Kuliah : Keamanan Komputer dan Jaringan</td><td>Semester: 8 (Delapan)</td><td>SKS: 2/2</td><td>Kode MK: SKO19426</td></tr>
<tr><td>Program Studi : Sistem Komputer</td><td colspan="3">Dosen Pengampu/Penanggung jawab : Ari Widiantoko, S.Kom.,M.Tech</td></tr>
<tr><td>Capaian Pembelajaran Lulusan (CPL)</td><td colspan="3"><u>Sikap</u>
1. Dapat bekerja sama dan memiliki kepekaan sosial serta kepedulian terhadap masyarakat dan lingkungan;
2. Menunjukkan sikap bertanggungjawab atas pekerjaan di bidang keahliannya secara mandiri;
<u>Pengetahuan</u>
1. Menguasai konsep teoritis bidang pengetahuan Sistem Komputer secara umum dan konsep teoritis bagian khusus dalam bidang pengetahuan tersebut secara mendalam, serta Mampu memformulasikan penyelesaian masalah prosedural;
2. Memiliki pengetahuan yang memadai terkait dengan cara kerja system komputer dan Mampu merancang dan mengembangkan berbagai produk piranti berbasis digital;
3. Mempunyai pengetahuan dasar matematika dan statistika;
<u>Keterampilan Umum</u>
1. Mampu menunjukkan kinerja mandiri, bermutu, dan terukur;
2. Mampu bertanggungjawab atas pencapaian hasil kerja kelompok dan melakukan supervisi dan evaluasi terhadap penyelesaian pekerjaan yang ditugaskan kepada pekerja yang berada di bawah tanggungjawabnya;
3. Mampu melakukan proses evaluasi diri terhadap kelompok kerja yang berada dibawah tanggung jawabnya, dan Mampu mengelola pembelajaran secara mandiri;
4. Memiliki keMampuan untuk mengembangkan perancangan jaringan dan perangkat keras (hardware) dalam organisasi.</td></tr>
</table>

	Keterampilan Khusus 1. Menguasai konsep keamanan sistem jaringan komputer dan membangun keamanan jaringan; 2. Mampu merancang dan mengaplikasikan jaringan nirkabel *(wireless networking);* 3. Mampu melaksanakan tugas sebagai administrator jaringan komputer dan sistem operasi dan membangun sistem dengan manajemen yang baik; dan 4. Mampu membangun dan memanajemen sistem terdistribusi dan jaringan komputer dengan manajemen yang baik dan aman.
Capaian Pembelajaran Mata Kuliah (CPMK)	1. Memahami pengetahuan tentang konsep keamanan sistem komputer berikut berbagai tipe ancaman, serangan, dan memahami pentingnya prinsip dasar pada suatu perancangan sistem keamanan sistem. 2. Memahami konsep Social Engineering pada sistem keamanan komputer. 3. Memahami konsep kriptografi, penerapan sejumlah teknik kriptografi, otentikasi dan fungsi hash, serta pemanfaat digital signatures dan manajemen key. 4. Memahai konsep steganografi dan penerapannya untuk penyembunyian pesan serta mampu membuat aplikasi sederhana yang menerapkan konsep steganografi. 5. Mengetahui prinsip otentikasi pengguna sistem elektronik, dan penerapan sejumlah sistem otentikasi seperti password-based, token- based, biometric, dan remote user authentication 6. Mampu memahami prinsip kontrol akses, hak subjek, objek dan akses, dan identitas, credential, dan manajemen aset. 7. Mampu memahami dan menjelaskan pentingnya aspek keamanan pada basis data dan sistem cloud termasuk sistem manajemen dan akses kontrol pada basis data serta proteksi data pada sistem cloud. 8. Mampu memahami dan menjelaskan tentang ancaman-ancaman dan serangan pada sistem komputer. 9. Mampu memahami dan menjelaskan tentang pentingnya mekanisme pengamanan sistem seperti penerapan Firewall dan sistempendeteksi intrusi 10. Mampu memahami protokol dan standar pada keamanan jaringan dan merancang suatu sistem keamanan jaringan sederhana yangmengacu pada protokol dan standar yang ada.
Deskripsi Mata Kuliah :	Matakuliah ini mempelajari teknik keamanan sistem komputer dan jaringannya dengan tujuan untuk menjaga kinerja dan proses komputer agar tetap optimal dan untuk mencegah serta mendeteksi adanya usaha modifikasi, interupsi, dan gangguan dalam sistem oleh orang yang tidak berwenang.

Minggu Ke	Kemampuan yang diharapkan (Sub-CPMK)	Bahan Kajian/Materi Pembelajaran	Bentuk, Metode Pembelajaran dan Pengalaman Belajar	Waktu (Menit)	Penilaian		
					Teknik	Indikator	Bobot (%)
1	➢ Memahami kontrak kuliah; ➢ Mengetahui definisi keamanan komputer dan mampu menjelaskan komponen-komponen utama pada sistem keamanan komputer ➢ Mampu menjelaskan jenis-jenis ancaman, serangan, danaset ➢ Mengetahui prinsip dasarsuatu perancangansistem keamanan komputer	➢ Kontrak Kuliah ➢ Definisi Keamanan Sistem Komputer ➢ Confidentiality, Integrity, Availibility, Authenticaty ➢ Security Levels: Low, Moderate, High Computer Security Terminology ➢ Threats: Unauthorized Disclosure, Deception, Disruption, Usurpation ➢ Fundamental Design: Economy of Mechanism, Fail-safe default, Complete mediation, Open design ➢ Attack Surfack & Attack Tree Computer Security strategy	➢ Pemaparan materi ➢ Mendengarkan penjelasan dosen tentang CP Mata kuliah ➢ Mendengarkan penjelasan dosen	4x50 Menit 4x60 Menit 4x60 Menit		a. Kelengkapan dan penguasaan materi b. Partisipasi	Etika (1 %) Tugas (0 %) Presensi (0,625%)
2	➢ Mengetahui konsep Social Engineering ➢ Mampu membedakan tipe social engineering ➢ Mengetahui sejarah dan evolusi Social	➢ Tipe Social Engineering: ➢ Physical, Remote, dan Combination Attacks ➢ Social Engineering pada tahun 1920an, 1940an, 1950an, 1970-1990s, dan sejak 2000 ➢ Sumber ancaman:	➢ Mendengarkan penjelasan dosen ➢ Mempelajari sumber – sumber pembelajaran ➢ Menyelesaikan Kasus Soal	4x50 Menit 4x60 Menit 4x60		a. Ketepatan menjawab b. Kelengkapan dan penguasaan penjelasan. c. Analisis d. Partisipasi	Etika (1 %) Tugas (5 %) Presensi (0,625%)

	Engineering ➢ Ancaman Social Engineering	Oportunis, Penyerang yang terorganisir, Penyerang internal		Menit			
3	➢ Mengetahui dua cabang utama Kriptologi dan definisinya ➢ Memahami konsep dasar Kriptografi dan Memahami Mode Chiper ➢ Memahami Symmetric Encryption ➢ Memahami Authentication dan Hash Function ➢ Mampu menjelaskan Digital Signatures dan Key Management	➢ Cryptology : Cryptography dan Cryptanalysis ➢ Cryptography: Basic Concepts ➢ Chiper Modes: Block Chipers dan Stream Chipers ➢ Symetric Chipers ➢ Authentication dan Hash Function ➢ Digital Signatures dan Key Management	➢ Mendengarkan penjelasan dosen ➢ Mempelajari sumber – sumber pembelajaran ➢ Membuat tugas latihan	4x50 Menit 4x60 Menit 4x60 Menit		a. Kelengkapan dan penguasaan materi b. Partisipasi	Etika (1 %) Tugas (0 %) Presensi (0,625%)
4	➢ Mampu menjawab pertanyaan QUIZ 1	➢ QUIZ 1	➢ Ujian.	4x50 Menit 4x60 Menit 4x60 Menit		a. Menjawab soal b. Partisipasi	Etika (1 %) Tugas (5 %) Presensi (0,625%)
5	➢ Memahami sejarah penyembunyian pesan dengan	➢ Terminologi sistem ➢ Sejarah penyembunyian pesan	➢ Mendengarkan penjelasan dosen ➢ Mempelajari	4x50 Menit		a. Kelengkapan dan penguasaan materi	Etika (1 %) Tugas (0 %)

	Steganography ➢ Memahami konsep dan prinsip Steganography dan Steganalysis ➢ Mampu memahami beberapa teknik Steganography ➢ Mampu memahami Watermarking dan Proteksi ➢ Hak Cipta	➢ Framework pada komunikasi rahasia ➢ Keamanan pada sistem Steganography ➢ Pengantar Sistem Substitusi dan Transform Domain Technique ➢ Teknik Watermarking, sejarah dan prinsip dasar	sumber – sumber pembelajaran ➢ Membuat tugas latihan	4x60 Menit 4x60 Menit		b. Partisipasi	Presensi (0,625%)
6	➢ Memahami prinsip otentikasi pengguna elektronik ➢ Memahami prinsip otentikasi berbasis Password ➢ Memahami prinsip otentikasi berbasis Token ➢ Memahami prinsip otentikasi Biometric ➢ Memahami otentikasi berbasis Remote User Authentication	➢ Electronic User Authentication Principles ➢ Password-based Authentication ➢ Token-based Authentication ➢ Biometric Authentication ➢ Remote User Authentication	➢ Mendengarkan penjelasan dosen ➢ Mempelajari sumber – sumber pembelajaran ➢ Menyelesaikan Kasus Soal	4x50 Menit 4x60 Menit 4x60 Menit		a. Berhasil mempresentasikan pemahaman di hadapan kelas b. Partisipasi	Etika (1 %) Tugas (5 %) Presensi (0,625%)
7	➢ Memahami prinsip Access Control ➢ Memahami hak Subjek, Object, dan Assets	➢ Access Control Principles ➢ Subject, Object, and Assest Rights ➢ Role-based Access Control ➢ Attribute-based Access	➢ Mendengarkan penjelasan dosen ➢ Mempelajari sumber – sumber pembelajaran	4x50 Menit 4x60		a. Kelengkapan dan penguasaan materi b. Partisipasi	Etika (1 %) Tugas (0 %) Presensi

	➢ Memahami Role-based Access Control ➢ Memahami Attribute- based Access ➢ Control ➢ Memahami Identitas, Credential, dan Manajemen Akses	Control ➢ Identity, Credentil, and Access Management	➢ Membuat tugas latihan	Menit 4x60 Menit			(0,625%)
8	➢ Mampu menjawab pertanyaan UTS.	➢ Semua materi yang telah dipelajari sebelumnya	➢ Ujian Tertulis	90		a. Menjawab semua pertanyaan b. Partisipasi	Etika (1 %) UTS (25%) Presensi (0,625%)
9	➢ Memahami kebutuhan keamanan pada sistem Basis Data ➢ Mengerti Sistem Manajemen Basis Data ➢ Memahami Relational Databases ➢ Memahami serangan secara injeksi SQL ➢ Memahami akses kontrol pada Basis Data ➢ Memahami konsep Cloud Computing	➢ Cloud Security Risks and Countermeasures ➢ Data Protection in the Cloud ➢ Cloud Security as a Service	➢ Mendengarkan penjelasan dosen ➢ Mempelajari sumber – sumber pembelajaran ➢ Menyelesaikan Kasus Soal	4x50 Menit 4x60 Menit 4x60 Menit		a. Berhasil mempresentasikan pemahaman di hadapan kelas b. Partisipasi	Etika (1 %) Tugas (5 %) Presensi (0,625%)

	➢ Memahami resiko pada Cloud Computing ➢ Memahami konsep proteksi data pada Cloud						
10	➢ Memahami tipe Malware ➢ Memahami teknik serangan dengan metode propagasi ➢ Memahami teknik serangan dengan metode Payload ➢ Memahami teknik penangangan serangan	➢ Teknik Penanganan Serangan	➢ Mendengarkan penjelasan dosen ➢ Mempelajari sumber – sumber pembelajaran ➢ Membuat tugas latihan	4x50 Menit 4x60 Menit 4x60 Menit		a. Kelengkapan dan penguasaan materi b. Partisipasi	Etika (1 %) Tugas (0 %) Presensi (0,625%)
11	➢ Memahami teknik serangan Denial of Service ➢ Memahami teknik serangan Flooding	➢ Denial-of-Service Attacks ➢ Flooding Attacks ➢ Distributed-Denial-of-Service	➢ Mendengarkan penjelasan dosen ➢ Mempelajari sumber – sumber pembelajaran ➢ Membuat tugas latihan	4x50 Menit 4x60 Menit 4x60 Menit		a. Kelengkapan dan penguasaan materi b. Partisipasi	Etika (1 %) Tugas (0 %) Presensi (0,625%)
12	➢ Mampu menjawab pertanyaan QUIZ 2	➢ QUIZ 2	➢ Ujian.	4x50 Menit 4x60 Menit 4x60		a. Menjawab soal	Etika (1 %) Tugas (5 %) Presensi (0,625%)

				Menit			
13	➢ Memahami pentingnya penggunaan Firewall ➢ Memahami karakteristik Firewall dan Kebijakan Akses ➢ Mengetahui tipe Firewall ➢ Mengetahui sistem pencegahan instrusi	➢ Firewall, definisi dan Penggunaan Karakteristik Firewall dan Access Policy ➢ Tipe Firewall ➢ Intrusion Prevention System	➢ Mendengarkan penjelasan dosen ➢ Mempelajari sumber – sumber pembelajaran ➢ Membuat tugas latihan	4x50 Menit 4x60 Menit 4x60 Menit		a. Kelengkapan dan penguasaan materi b. Partisipasi	Etika (1 %) Tugas (0 %) Presensi (0,625%)
14	➢ Mampu memahami dan menjelaskan Internet Security Protocol dan Standard	➢ Secure E-Mail dan S/MIME ➢ SSL (Secure Socket Layer) dan TSL (Transport Layer Security) ➢ HTTPS IPv4 vs IPv6 Security	➢ Mendengarkan penjelasan dosen ➢ Mempelajari sumber – sumber pembelajaran ➢ Membuat tugas latihan	4x50 Menit 4x60 Menit 4x60 Menit		a. Membuat dan menjalankan aplikasi b. Mengerjakan Kuis c. Mengerjakan Tugas d. Mengikuti Praktikum	Etika (1 %) Tugas (0 %) Presensi (0,625%)
15	➢ Memahami dan mampu menjelaskan tentang konsep Wireless Network Security	➢ Wireless Security ➢ Mobile Device Security ➢ Wireless LAN Security	➢ Mendengarkan penjelasan dosen ➢ Mempelajari sumber – sumber pembelajaran ➢ Membuat tugas latihan	4x50 Menit 4x60 Menit 4x60 Menit		a. Membuat dan menjalankan aplikasi b. Mengerjakan Kuis c. Mengerjakan Tugas d. Mengikuti Praktikum	Etika (1 %) Tugas (0 %) Presensi (0,625%)
16	➢ Mampu menjawab pertanyaan UAS.	➢ UAS	➢ Ujian.	90		a. Menjawab semua pertanyaan pada UAS	UAS (25%) Presensi

						b. Partisipasi	(0,625%)

Daftar Referensi :

1. “The Underground Guide to Computer Security“, Alexander, M., Addison-Wesley Publishing, 1994
2. “Computer Under Attack : Intruders, Worms, and Viruses“, Denning, Peter J., AddisonWesley Publishing, 1991
3. “Computer Communications Security“, Ford, Warwick, Prentice-Hall, 1994
4. “Security in computing“, Pfleeger, C.P. Prentice-Hall, 1997
5. “Cryptography and Secure Communications“, Rhee, Man Young, McGraw Hill, 1994
6. “Building A Secure Computer System“, Morrie Grasser, Edisi 4, Nelson Canada, 1988
7. “COMPUTER NETWORKING A Top-Down Approach”, Authors: James F. Kurose University of Massachusetts, Amherst Keith W. Ross Polytechnic Institute of NYU, Publisher: Pearson, ISBN-13: 978-0-13-285620-1
8. “Information Technology Security Handbook”, Authors: George Sadowsky, James X. Dempsey, Alan Greenberg, Barbara J. Mack, Alan Schwartz, Publisher: Global Informationand Communication Technologies Department the World BANK, ISBN: 0-9747888-0-5

Rencana Tugas dan Penilaian

1. **Tugas**

Minggu Ke	Bahan Kajian/Materi Pembelajaran	Tugas		Waktu (Menit)	Penilaian	Indikator	Bobot (%)
2	➢ Kontrak Kuliah ➢ Definisi Keamanan Sistem Komputer ➢ Confidentiality, Integrity, Availibility, Authenticaty ➢ Security Levels: Low, Moderate, High ➢ Computer Security Terminology ➢ Threats: Unauthorized Disclosure, Deception, Disruption, Usurpation ➢ Fundamental Design: Economy of Mechanism, Fail-safe default, Complete mediation, Open design. ➢ Attack Surfack & Attack Tree Computer Security strategy ➢ Tipe Social Engineering: ➢ Physical, Remote, dan Combination Attacks ➢ Social Engineering pada tahun 1920an, 1940an, 1950an, 1970-1990s, dan sejak 2000 ➢ Sumber ancaman: Oportunis, Penyerang yang	Mandiri					
		Terstruktur	Presentasi Kelas	4x60		Mampu mempresentasikan pemahaman di hadapan kelas	5

	terorganisir, Penyerang internal						
4	➢ Cryptology : Cryptography dan Cryptanalysis ➢ Cryptography: Basic Concepts ➢ Chiper Modes: Block Chipers dan Stream Chipers ➢ Symetric Chipers ➢ Authentication dan Hash Function ➢ Digital Signatures dan Key Management	Mandiri	Membuat dan menjalankan aplikasi	4x60		Mampu Membuat dan menjalankan aplikasi	5
		Terstruktur					
6	➢ Terminologi sistem ➢ Sejarah penyembunyian pesan ➢ Framework pada komunikasi rahasia ➢ Keamanan pada sistem Steganography ➢ Pengantar Sistem Substitusi dan Transform Domain Technique ➢ Teknik Watermarking, sejarah dan prinsip dasar ➢ Electronic User Authentication Principles ➢ Password-based Authentication ➢ Token-based Authentication ➢ Biometric Authentication ➢ Remote User	Mandiri					
		Terstruktur	Presentasi Kelas	4x60		Mampu mempresentasikan pemahaman di hadapan kelas	5

	Authentication						
9	➢ Access Control Principles ➢ Subject, Object, and Assest Rights ➢ Role-based Access Control ➢ Attribute-based Access Control Identity, Credentil, and Access Management ➢ Cloud Security Risks and Countermeasures ➢ Data Protection in the Cloud Cloud Security as a Service	Mandiri					
		Terstruktur	Presentasi Kelas	4x60		Mampu mempresentasikan pemahaman di hadapan kelas	5
12	➢ Teknik Penanganan Serangan Denial-of-Service Attacks ➢ Flooding Attacks Distributed-Denial-of-Service ➢ Firewall, definisi dan penggunaan ➢ Karakteristik Firewall dan Access Policy ➢ Tipe Firewall Intrusion Prevention System ➢ Secure E-Mail dan S/MIME ➢ SSL (Secure Socket Layer) dan TSL (Transport Layer Security) ➢ HTTPS IPv4 vs IPv6	Mandiri	Membuat dan menjalankan aplikasi	4x60		Mampu Membuat dan menjalankan aplikasi	5
		Terstruktur					

2. Penilaian

Aspek Penilaian

1) **Sikap** **:** cara menyampaikan pendapat dalam diskusi, tanggungjawab dalam menyelesaikan tugas
2) **Pengetahuan** : penguasaan materi yang ditunjukkan dalam diskusi, presentasi, ujian tengah semester dan ujian akhir semester
3) **Keterampilan** **:** kreatifitas membuat ppt, menggunakan program kimia komputasi, membuat diagram prosedur proses kimia

Bobot Penilaian

Bobot Nilai Tugas (NT)	= 25%
Bobot Nilai Ujian Tengah Semester (UTS)	= 25%
Bobot Nilai Ujian Akhir Semester (UAS)	= 25%
Bobot Etika (E)	= 15%
Presensi (P)	= 10%

Nilai Akhir

Nilai Akhir = 25% NT + 25% UTS + 25% UAS + 15% E + 10% P

Bandar Lampung, 03 November 2021

Disusun oleh	Diperiksa oleh	Diperiksa oleh	Disahkan oleh
(Ari Widiantoko, S.Kom.,M.Tech) **Dosen Penanggungjawab**	**Penanggungjawab** **Kelompok Bidang Keilmuan (KBK)**	**Ketua Program Studi** **Sistem Komputer**	**Dekan** **Fakultas Ilmu Komputer**