RENCANA PEMBELAJARAN SEMESTER (RPS)

(KEAMANAN SISTEM KOMPUTER)

(Fardian, S.T., M.Sc)

PROGRAM STUDI TEKNIK ELEKTRO
FAKULTAS TEKNIK
UNIVERSITAS SYIAH KUALA
(2018)

RENCANA PEMBELAJARAN SEMESTER (RPS)

Mata Kuliah	: Keamanan Sistem Komputer	Semester : 7	Kode : TEL557	SKS : 3(2-1)
Program Studi	: Teknik Elektro	Dosen :	1) Fardian, S.T., M.Sc	

Capaian Pembelajaran Program Studi (CP-PRODI) :

D. Memiliki pengetahuan teoritis yang luas untuk mengidentifikasi, merumuskan, menganalisa dan menyelesaikan masalah atau memberikan solusi alternatif dalam bidang teknik elektro dan pengetahuan khusus yang mendalam pada bidang keahliannya.

Capaian Pembelajaran Mata Kuliah (CP-MK) :

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 sistem pendeteksi intrusi

10 Mampu memahami protokol dan standar pada keamanan jaringan dan merancang suatu sistem keamanan jaringan sederhana yang mengacu pada protokol dan standar yang ada.

Kriteria Penilaian:

Nomor	Nilai Angka	Nilai Huruf
1	≥87	A
2	78 - <87	AB
3	69 - <78	B
4	60 - <69	BC
5	51 - <60	C
6	41 - <51	D
7	<41	E

Item Penilaian :

Item	%
Kuis	30%
Tugas	20%
Tes Kelas	5%
Ujian Tengah Semester	20%
Ujian Akhir Semester	25%
Total	**100%**

JADWAL, URAIAN MATERI DAN KEGIATAN PERKULIAHAN

Minggu Ke-	Kemampuan Akhir Yang Diharapkan	Bahan Kajian (Materi Pelajaran)	Strategi Pembelajaran/Metode Pembelajaran	Waktu Belajar (menit)	Pengalaman Belajar Mahasiswa	Kriteria Penilaian (Indikator)	Bobot Nilai (%)
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
1	✓ Memahami kontrak kuliah; ✓ Mengetahui definisi keamanan komputer dan mampu menjelaskan komponen-komponen utama pada sistem keamanan komputer ✓ Mampu menjelaskan jenis-jenis ancaman, serangan, dan aset ✓ Mengetahui prinsip dasar suatu perancangan sistem 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	Ceramah, tanya-jawab,	510		a. Presentasi Kelas b. Tugas	Kuis (0 %) Tugas (10 %) Prak (0 %)

Minggu Ke-	Kemampuan Akhir Yang Diharapkan	Bahan Kajian (Materi Pelajaran)	Strategi Pembelajaran/Metode Pembelajaran	Waktu Belajar (menit)	Pengalaman Belajar Mahasiswa	Kriteria Penilaian (Indikator)	Bobot Nilai (%)
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
2	✓ Mengetahui konsep Social Engineering ✓ Mampu membedakan tipe social engineering ✓ Mengetahui sejarah dan evolusi Social Engineering ✓ Ancaman Social Engineering	➢ 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 terorganisir, Penyerang internal	Ceramah, tanya-jawab, tugas bacaan.	510		Berhasil mempresentasikan pemahaman di hadapan kelas	Kuis (0 %) Tugas (0 %) Prak (0 %)
3	✓ Mengetahui dua cabang utama Kriptologi dan definisinya ✓ Memahami konsep dasar Kriptografi dan ✓ Memahami Mode Chiper ✓ Memahami Symmetric Encryption ✓ Memahami Authentication	➢ 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	Ceramah, tanya-jawab, tugas bacaan.	510		a. Presentasi Kelas b. Tugas	Kuis (0%) Tugas (10%) Prak (0%)

Minggu Ke-	Kemampuan Akhir Yang Diharapkan	Bahan Kajian (Materi Pelajaran)	Strategi Pembelajaran/Metode Pembelajaran	Waktu Belajar (menit)	Pengalaman Belajar Mahasiswa	Kriteria Penilaian (Indikator)	Bobot Nilai (%)
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	dan Hash Function ✓ Mampu menjelaskan Digital Signatures dan Key Management						
4	✓ Mampu menjawab pertanyaan QUIZ 1	➢ QUIZ	Ujian Tulis.	510		a. Menjawab soal	Kuis (15%) Tugas (0%) Prak (0%)
5	✓ Memahami sejarah penyembunyian pesan dengan Steganography ✓ Memahami konsep dan prinsip Steganography dan Steganalysis ✓ Mampu memahami beberapa teknik Steganography	➢ 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	Ceramah, tanya-jawab, tugas bacaan.	510		a. Presentasi Kelas	Kuis (0%) Tugas (0%) Prak (0%)

Minggu Ke-	Kemampuan Akhir Yang Diharapkan	Bahan Kajian (Materi Pelajaran)	Strategi Pembelajaran/Metode Pembelajaran	Waktu Belajar (menit)	Pengalaman Belajar Mahasiswa	Kriteria Penilaian (Indikator)	Bobot Nilai (%)
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	✓ Mampu memahami Watermarking dan Proteksi Hak Cipta						
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	Ceramah, tanya-jawab, tugas program, tugas bacaan.	510		a. Presentasi Kelas b. Tes Kelas	Kuis (0%) Tugas (0%) Tes (5 %)

Minggu Ke-	Kemampuan Akhir Yang Diharapkan	Bahan Kajian (Materi Pelajaran)	Strategi Pembelajaran/Metode Pembelajaran	Waktu Belajar (menit)	Pengalaman Belajar Mahasiswa	Kriteria Penilaian (Indikator)	Bobot Nilai (%)
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
7	✓ Memahami prinsip Access Control ✓ Memahami hak Subjek, Object, dan Assets ✓ Memahami Role-based Access Control ✓ Memahami Attribute-based Access Control ✓ Memahami Identitas, Credential, dan Manajemen Akses	➢ Access Control Principles ➢ Subject, Object, and Assest Rights ➢ Role-based Access Control ➢ Attribute-based Access Control ➢ Identity, Credentil, and Access Management	Ceramah, tanya-jawab	510		a. Presentasi Kelas	Kuis (0%) Tugas (0%) Prak (0%)
8	Mampu menjawab pertanyaan UTS.	Semua materi yang telah dipelajari sebelumnya	Ujian Tertulis	100		Menjawab semua pertanyaan	UTS (20 %)
9	✓ Memahami kebutuhan keamanan pada sistem Basis Data ✓ Mengerti Sistem	➢ Database Security ➢ Database Management System ➢ Relational Database ➢ SQL Injection Attacks ➢ Database Access Control ➢ Cloud Computing	Ceramah, tanya-jawab, tugas bacaan.	510		a. Mengerjakan Tugas	Tugas (10%)

Minggu Ke-	Kemampuan Akhir Yang Diharapkan	Bahan Kajian (Materi Pelajaran)	Strategi Pembelajaran/Metode Pembelajaran	Waktu Belajar (menit)	Pengalaman Belajar Mahasiswa	Kriteria Penilaian (Indikator)	Bobot Nilai (%)
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	Manajemen Basis Data ✓ Memahami Relational Databases ✓ Memahami serangan secara injeksi SQL ✓ Memahami akses kontrol pada Basis Data ✓ Memahami konsep Cloud Computing ✓ Memahami resiko pada Cloud Computing ✓ Memahami konsep proteksi data pada Cloud	➢ Cloud Security Risks and Countermeasures ➢ Data Protection in the Cloud ➢ Cloud Security as a Service					
10	✓ Memahami tipe Malware ✓ Memahami teknik serangan dengan metode propagasi	➢ Tipe serangan Malware ➢ Teknik serangan Propagasi ➢ Teknik serangan Payload	Ceramah, tanya-jawab	510		b. Presentasi Kelas	Kuis (0%) Tugas (0%) Prak (0%)

Minggu Ke-	Kemampuan Akhir Yang Diharapkan	Bahan Kajian (Materi Pelajaran)	Strategi Pembelajaran/Metode Pembelajaran	Waktu Belajar (menit)	Pengalaman Belajar Mahasiswa	Kriteria Penilaian (Indikator)	Bobot Nilai (%)
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	✓ Memahami teknik serangan dengan metode Payload ✓ Memahami teknik penangangan serangan ✓	➢ Teknik Penanganan Serangan					
11	✓ Memahami teknik serangan Denial of Service ✓ Memahami teknik serangan Flooding	➢ Denial-of-Service Attacks ➢ Flooding Attacks ➢ Distributed-Denial-of-Service				c.	
12	✓ Mampu menjawab pertanyaan QUIZ 2	➢ QUIZ 2	Ujian Tulis.	510		b. Menjawab soal	Kuis (15%) Tugas (0%) Prak (0%)
13	✓ Memahami pentingnya penggunaan Firewall ✓ Memahami karakteristik Firewall dan	➢ Firewall, definisi dan penggunaan ➢ Karakteristik Firewall dan Access Policy ➢ Tipe Firewall ➢ Intrusion Prevention System	Ceramah, tanya-jawab	510		d. Presentasi Kelas	Kuis (0%) Tugas (0%) Prak (0%)

Minggu Ke-	Kemampuan Akhir Yang Diharapkan	Bahan Kajian (Materi Pelajaran)	Strategi Pembelajaran/Metode Pembelajaran	Waktu Belajar (menit)	Pengalaman Belajar Mahasiswa	Kriteria Penilaian (Indikator)	Bobot Nilai (%)
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	Kebijakan Akses ✓ Mengetahui tipe Firewall ✓ Mengetahui sistem pencegahan instrusi						
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	Ceramah, tanya-jawab, praktikum, tugas program, tugas bacaan.	510		a. Membuat dan menjalankan aplikasi b. Mengerjakan Kuis c. Mengerjakan Tugas d. Mengikuti Praktikum	Kuis (2%) Tugas (2%) Prak (2%)
15	✓ Memahami dan mampu menjelaskan tentang konsep Wireless Network Security	➢ Wireless Security ➢ Mobile Device Security ➢ Wireless LAN Security	Ceramah, tanya-jawab, praktikum, tugas program, tugas bacaan.	510		a. Membuat dan menjalankan aplikasi b. Mengerjakan Kuis c. Mengerjakan Tugas d. Mengikuti Praktikum	Kuis (1%) Tugas (0%) Prak (0%)
16	Mampu menjawab pertanyaan UAS.	UAS	Ujian.	100		Menjawab semua pertanyaan pada UAS	UAS (30 %)
TOTAL							**100**

Sumber Belajar/ Referensi

[1]. Computer Security Principles and Practice, 3rd edition, Williams Stallings, Pearson, 2015
[2]. Social Engineering in IT Security: Tools, Tactics, and Techniques Social Engineering in IT Security: Tools, Tactics, and Techniques, Sharon Conheady, McGraw-Hill Osborne Media, 2014
[3]. An Introduction to Cryptography, M. Barakat, Lecture Notes University of Kaiserslautern, 2018
[4]. Information Hiding techniques for Steganography and Digital Watermarking, Stefan Katzenbeisser, Artech House, 2000

Mengetahui,	Banda Aceh, 03 September 2018
Ketua Program Studi,	Koordinator/ Penanggungjawab,
(Zulhelmi, S.T., M.Sc)	(Fardian, S.T., M.Sc.)
NIP. 197907022003121001	NIP. 197901022003121004