

**RENCANA PEMBELAJARAN SEMESTER (RPS)
(T.A. GANJIL 2021/2022)**

**TSI-5363
PENGUJIAN PENETRASI SISTEM INFORMASI**



**universitas
MALIKUSSALEH**

Tim Penyusun:

**Teuku Afriliansyah, S. Kom., M. Kom
Rahma Fitria, B.Tech(Hons), M.Sc**

**PROGRAM STUDI SISTEM INFORMASI
JURUSAN TEKNIK ELEKTRO
FAKULTAS TEKNIK
UNIVERSITAS MALIKUSSALEH
2022**

PROFIL MATA KULIAH

Mata Kuliah	:	Pengujian Penetrasi Sistem Informasi	
Kode Mata Kuliah	:	TSI-5363	
SKS	:	3 SKS	
Semester	:	III	
Bentuk Perkuliahan	:	Kuliah Luring	
Alokasi Waktu	:	16 x 150 Menit	
Pelaksanaan Pembelajaran	:	Tatap Muka	2 jam 30 menit per minggu
		Praktikum	jam per minggu
Mata Kuliah Prasyarat	:	Kode Mata Kuliah:	Nama Mata Kuliah:
Rumpun Mata Kuliah	:	Infrastruktur Teknologi Informasi	
Capaian Pembelajaran Lulusan Program Studi	CP-S2	Menjunjung tinggi nilai kemanusiaan dalam menjalankan tugas berdasarkan agama, moral, dan etika.	
	CP-S8	Menginternalisasi nilai, norma, dan etika akademik.	
	CP-S9	Menunjukkan sikap bertanggung jawab atas pekerjaan di bidang keahliannya secara mandiri	
	CP-S13	Memiliki kepribadian dan interaksi sosial yang berempati dan humanis	
	CP-PA2	Menguasai konsep-konsep bahasa pemrograman, serta mampu membandingkan berbagai solusi serta berbagai model bahasa pemrograman.	
	CP-PA4	Menguasai konsep basis data, metode analisis, perancangan, pembangunan, manajemen dan administrasi basis data	

	CP-PA8	Memahami konsep dan metode evaluasi, manajemen, dan tata kelola SI/TI.
	CP-KU1	Mampu menerapkan pemikiran logis, kritis, sistematis, dan inovatif dalam konteks pengembangan atau implementasi ilmu pengetahuan dan teknologi yang memperhatikan dan menerapkan nilai humaniora yang sesuai dengan bidang keahliannya
	CP-KU2	Mampu menunjukkan kinerja mandiri, bermutu, dan terukur
	CP-KU5	Mampu mengambil keputusan secara tepat dalam konteks penyelesaian masalah di bidang keahliannya, berdasarkan hasil analisis informasi dan data
	CP-KU8	Mampu melakukan proses evaluasi diri terhadap kelompok kerja yang berada dibawah tanggung jawabnya, dan mampu mengelola pembelajaran secara mandiri
	CP-KU9	Mampu mendokumentasikan, menyimpan, mengamankan, dan menemukan kembali data untuk menjamin kesahihan dan mencegah plagiasi
	CP-KKA5	Mampu mengimplementasikan aspek Keamanan Informasi sebagai bagian terintegrasi pada kompetensi embedded system perancangan bangun alat.
	CP-KKB1	Mahasiswa mampu memahami konsep dasar digital signature
	CP-KKB2	Mampu mengelola risiko keamanan dan integritas data dan infrastruktur SI/TI.
Capaian Pembelajaran Mata Kuliah	1. Mahasiswa mampu menjelaskan sejarah dan konsep dasar perekayasaan Keamanan Informasi 2. Mahasiswa mampu merumuskan masalah dan mencari solusi terkait keamanan jaringan 3. Mahasiswa mampu menjelaskan berbagai metode umum pokok bahasan Keamanan Informasi 4. Mahasiswa mampu mensimulasikan keterampilan terkait Keamanan Informasi dan mengkorelasikannya dengan aspek budaya dan kearifan lokal	
Capaian SN-Dikti/KKNI		
Sikap		Pengetahuan
CP-S2, CP-S8, CP-KU9, CP-S13		CP-PA2, CP-PA4. CP-PA8

Keterampilan Umum	Keterampilan Khusus
CP-KU1, CP-KU2, CP-KU5, CP-KU8, CP-KU9	CP-KKA5, CP-KKB1, CP-KKB2
Deskripsi Mata Kuliah	
ada mata kuliah ini mahasiswa difasilitasi tentang konsep dan penerapan Keamanan Informasi di mulai dari sejarah pengaplikasian penyandian keamanan, sampai kepada pengayaan yang relevan pada penerapan aspek Keamanan Informasi seperti wireless security, internet protocol security, intrusion detection system, ad hoc networking .	
Daftar Pustaka	
1. Cryptography and Network Security – William Stallings 2. A Guide to Computer Network Security – Joseph Migga Kizza 3. Introduction to Cryptography – Nigel Smart	

RENCANA PEMBELAJARAN SEMESTER (RPS)

Minggu ke-	Kemampuan Akhir yang Diharapkan	Pokok Bahasan dan Sub Pokok Bahasan	Strategi/Metode Pembelajaran	Waktu Belajar	Pengalaman Belajar Mahasiswa	Penilaian	
						Kriteria Penilaian (Indikator)	Bobot Nilai (%)
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
1	1. Mahasiswa mampu mengenali Konsep alir komunikasi pada infrastruktur jaringan dan protokol komunikasi 2. Mahasiswa mampu menganalisis kelemahan yang dapat terjadi pada jaringan komputer	Sejarah Keamanan Informasi, dimulai dengan ditemukannya turing machine, enigma machine	Ceramah, diskusi tanya jawab Tugas 1; Mencari bahan referensi tentang sejarah Keamanan Informasi	150 menit	Setelah mempelajari pokok bahasan ini mahasiswa mampu mengenali Konsep alir komunikasi dan menganalisis kelemahan yang dapat terjadi pada jaringan komputer	Indikator • Perluasan wawasan sejarah Keamanan Informasi Bentuk non-tes; • Tulisan bertemplate IEEE	
2	1. Mahasiswa mampu memahami konsep tujuan kunci keamanan informasi 2. Mahasiswa mampu membedakan jenis serangan aktif dan pasif pada jaringan internet.	Konsep yang melatarbelakangi serangan pasif dan aktif pada sebuah jaringan internet	Ceramah,Diskusi tanya jawab	150 menit	Setelah mempelajari pokok bahasan ini mahasiswa mampu memahami konsep tujuan kunci keamanan informasi dan membedakan jenis serangan	Indikator • Perluasan wawasan tentang metode yang umum dipakai hacker Bentuk non-tes; Presentasi Tugas	

Minggu ke-	Kemampuan Akhir yang Diharapkan	Pokok Bahasan dan Sub Pokok Bahasan	Strategi/Metode Pembelajaran	Waktu Belajar	Pengalaman Belajar Mahasiswa	Penilaian	
						Kriteria Penilaian (Indikator)	Bobot Nilai (%)
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
					aktif dan pasif pada jaringan internet.		
3	1. Mahasiswa mampu memahami fungsi dari kriptografi, kriptanalisis dan Kriptologi 2. Mahasiswa mampu mengklasifikasikan teknik penyandian substitusi, transposisi dan gabungan 3. Mahasiswa mampu mengkonstruksi teknik penyandian sederhana	Konsep dan implementasi dasar dari teknik yang terdapat pada kriptografi seperti perpaduan teknik substitusi, transposisi dan gabungan	- Ceramah, Diskusi tanya jawab - Tugas 2; Mengkreasikan teknik penyandian self customized	150 menit	Setelah mempelajari pokok bahasan ini mahasiswa mampu memahami fungsi dari kriptografi, kriptanalisis dan Kriptologi dan juga teknik penyandian substitusi, transposisi dan gabungan serta mengkonstruksi teknik penyandian sederhana	Perluasan wawasan tentang konsep kriptografi	
4	1. Mahasiswa mampu memahami konsep private key pada teknik penyandian	Mempelajari tentang konsep dasar private key management pada penyandian dari client	- Ceramah, diskusi tanya jawab - Tugas Kelompok 1 :	150 menit	Setelah mempelajari pokok bahasan ini mahasiswa	Indikator • Perluasan wawasan tentang konsep	

Minggu ke-	Kemampuan Akhir yang Diharapkan	Pokok Bahasan dan Sub Pokok Bahasan	Strategi/Metode Pembelajaran	Waktu Belajar	Pengalaman Belajar Mahasiswa	Penilaian	
						Kriteria Penilaian (Indikator)	Bobot Nilai (%)
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	kriptografi 2. Mahasiswa mampu membangun aplikasi private key berdasarkan teknik kriptografi	– host atau sebaliknya	Mensimulasikan bentuk serangan dan penyandian pada Keamanan Informasi		mampu memahami konsep private key pada teknik penyandian kriptografi	private key encryption	
5	1. Mahasiswa mampu memahami konsep private key pada teknik penyandian kriptografi 2. Mahasiswa mampu membangun aplikasi private key berdasarkan teknik kriptografi	Mempelajari tentang konsep dasar private key management pada penyandian dari client – host atau sebaliknya	- Ceramah, diskusi tanya jawab - Tugas Kelompok 1 : Mensimulasikan bentuk serangan dan penyandian pada Keamanan Informasi	150 menit	Setelah mempelajari pokok bahasan ini mahasiswa mampu membangun aplikasi private key berdasarkan teknik kriptografi	tugas, praktik	
6	1. Mahasiswa mampu menjelaskan keterkaitan antara : kapasitas, keamanan dan kehandalan pada konsep dasar penyembunyian informasi 2. Mahasiswa dapat menggabungkan konsep penyandian	- <i>Mempelajari tentang konsep information hiding</i>	- Ceramah - diskusi tanya jawab - presentasi	150 menit	Setelah mempelajari pokok bahasan ini mahasiswa mampu menjelaskan keterkaitan antara : kapasitas, keamanan dan kehandalan pada konsep dasar	Perluasan wawasan tentang konsep steganalysis	

Minggu ke-	Kemampuan Akhir yang Diharapkan	Pokok Bahasan dan Sub Pokok Bahasan	Strategi/Metode Pembelajaran	Waktu Belajar	Pengalaman Belajar Mahasiswa	Penilaian	
						Kriteria Penilaian (Indikator)	Bobot Nilai (%)
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	dan penyembunyian informasi				penyembunyian informasi		
7	1. Mahasiswa mampu memahami cara menanamkan pola unik atau beberapa data ke dalam konten digital tanpa mengubah kualitas perseptual 2. Mahasiswa mampu memahami proses kunci perlindungan kepemilikan data elektronik yang akan dipertukarkan lewat jaringan internet	- Mempelajari tentang penambahan konten informasi intangible	Ceramah, diskusi tanya jawab	150 menit	Setelah mempelajari pokok bahasan ini mahasiswa mampu memahami cara menanamkan pola unik atau beberapa data ke dalam konten digital tanpa mengubah kualitas perseptual dengan kunci perlindungan kepemilikan data elektronik	Perluasan wawasan tentang konsep watermarking	
8	UJIAN TENGAH SEMESTER (UTS)					Bentuk tes ujian tertulis	25%
9	1. Mahasiswa mampu	Konsep tentang message	Ceramah, diskusi tanya jawab.	150 menit	Setelah	indikator • Perluasan	

Minggu ke-	Kemampuan Akhir yang Diharapkan	Pokok Bahasan dan Sub Pokok Bahasan	Strategi/Metode Pembelajaran	Waktu Belajar	Pengalaman Belajar Mahasiswa	Penilaian	
						Kriteria Penilaian (Indikator)	Bobot Nilai (%)
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	menspesifikasikan standarisasi mengaplikasikan autentifikasi code pada pesan 2. Mahasiswa mampu menjelaskan pemanfaatan WAP (Wireless Application Protocol) 3. Mahasiswa mampu menjelaskan pemanfaatan penerapan message authentication code pada komunikasi harian	authentication code	Tugas Pribadi 1 : Membuat resume tentang message authentication code pada pengiriman pesan elektronik		mempelajari pokok bahasan ini mahasiswa mampu menspesifikasikan standarisasi mengaplikasikan autentifikasi code pada pesan	wawasan tentang message authentication code • Pemahaman konsep tentang OSI layer	
10	1. Mahasiswa mampu memahami konsep dasar digital signature. 2. Mahasiswa mampu mengobservasi modul yang berkaitan dengan digital signature	Mempelajari alur dan mekanisme keamanan pada digital signature	- Ceramah, diskusi tanya jawab	150 menit	Setelah mempelajari pokok bahasan ini mahasiswa mampu memahami konsep dasar digital signature	Indikator • Perluasan wawasan tentang konsep pembuatan dan perekayasaan digital signature Bentuk non-tes; Presentasi Tugas	

Minggu ke-	Kemampuan Akhir yang Diharapkan	Pokok Bahasan dan Sub Pokok Bahasan	Strategi/Metode Pembelajaran	Waktu Belajar	Pengalaman Belajar Mahasiswa	Penilaian	
						Kriteria Penilaian (Indikator)	Bobot Nilai (%)
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
11	1. Mahasiswa dapat mengkorelasikan format enkripsi encapsulating security payload pada mode tunneling dan transport. 2. Mahasiswa dapat menerapkan mode standar keamanan protokol internet dan memberikan edukasi yang baik kepada masyarakat	Mempelajari tentang struktur fisik internet protocol security	- Ceramah, diskusi tanya jawab - Tugas 2 : Membuat resume korelasi antara Wireless dan Ad Hoc Network	150 menit	Setelah mempelajari pokok bahasan ini mahasiswa mampu mengkorelasikan format enkripsi encapsulating security payload pada mode tunneling dan transport. dan menerapkan mode standar keamanan protokol internet dan memberikan edukasi yang baik	Indikator • Perluasan wawasan tentang Internet Protocol Security	
12	1. Mahasiswa mampu memahami konsep dasar firewall 2. Mahasiswa mampu mendesain dan mengimplementasikan jenis firewall	Membahas tentang konsep dan pengaplikasian firewall	- Ceramah, diskusi tanya jawab	150 menit	Setelah mempelajari pokok bahasan ini mahasiswa mampu memahami tipe dan penempatan	Indikator • Perluasan wawasan tentang Firewall	

Minggu ke-	Kemampuan Akhir yang Diharapkan	Pokok Bahasan dan Sub Pokok Bahasan	Strategi/Metode Pembelajaran	Waktu Belajar	Pengalaman Belajar Mahasiswa	Penilaian	
						Kriteria Penilaian (Indikator)	Bobot Nilai (%)
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	3. Mahasiswa mampu memahami tipe dan penempatan fisik / logic firewall				fisik / logic firewall		
13	1. Mahasiswa mampu memahami konsep dasar intrusion detection system, denial of services dan distributed denial of services 2. Mahasiswa mampu mengimplementasikan bentuk bentuk intrusion detection system yang efektif	Mempelajari perbedaan antara denial of services dan distributed denial of services	- Ceramah, diskusi tanya jawab	150 menit	Setelah mempelajari pokok bahasan ini mahasiswa mampu konsep dasar intrusion detection system, denial of services dan distributed denial of services beserta bentuk bentuk intrusion detection system yang efektif	Indikator • Perluasan wawasan tentang Intrusion Detection System • Konsep topologi Jaringan • Bentuk non-tes; • Presentasi Tugas	
14	1. Mahasiswa mampu mengkorelasikan keterkaitan antara wireless security dan ad hoc networking	- Membahas tentang wireless security dan ad hoc networking dan bentuk	- Ceramah, diskusi tanya jawab	150 menit	Setelah mempelajari pokok bahasan ini mahasiswa mampu	Indikator • Perluasan wawasan tentang perpaduan	

Minggu ke-	Kemampuan Akhir yang Diharapkan	Pokok Bahasan dan Sub Pokok Bahasan	Strategi/Metode Pembelajaran	Waktu Belajar	Pengalaman Belajar Mahasiswa	Penilaian	
						Kriteria Penilaian (Indikator)	Bobot Nilai (%)
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	2. Mahasiswa mampu memahami bentuk bentuk pengaplikasian ad hoc networking	bentuk bentuk pengaplikasian ad hoc networking			mengkorelasikan keterkaitan antara wireless security dan ad hoc networking	wireless security dan ad hoc networking	
15	1. Mahasiswa mampu memahami konsep routing protocol dan jenis serangan pada mobile ad hoc 2. Mahasiswa mampu mengimplementasikan pengamanan ad hoc network routing protocol	Mempelajari salah satu bentuk ad hoc networking	Ceramah, Diskusi tanya jawab. Quiz	150 menit	Setelah mempelajari pokok bahasan ini mahasiswa mampu memahami konsep routing protocol dan jenis serangan dan pengamanan pada mobile ad hoc	Indikator • Perluasan wawasan tentang perpaduan wireless security dan ad hoc networking Bentuk test Quiz tertulis 1 x 45 menit	
16	UJIAN AKHIR SEMESTER(UAS)					Bentuk test Ujian Tertulis 2 x 45 Menit / Tugas Besar / Tugas Pengganti UAS	30%

PENILAIAN

A. Standar Penilaian

No.	Nilai Angka	Nilai Huruf	Angka Mutu	Mutu
1	85,00 – 100	A	4	Istimewa
2	80,00 – 84,99	A-	3,70	Sangat Memuaskan
3	75,00 – 79,99	B+	3,30	Memuaskan
4	70,00 - 74,99	B	3	Sangat Baik
5	65,00 - 69,99	B-	2,70	Baik
6	60,00 – 64,99	C+	2,30	Cukup Baik
7	55,00 – 59,99	C	2	Cukup
8	50,00 – 54,99	C-	1,70	Kurang
9	45,00 – 49,99	D	1	Sangat Kurang
10	< 44,99	E	0	Gagal
11	0,00 (Tunda)	T	0	Tunda

Keterangan: Sesuai dengan Buku Panduan Akademik Tahun 2020

B. Komponen Penilaian

Bentuk Pembelajaran Kuliah, Diskusi Tanya Jawab		
No	Komponen	Bobot (%)
1	Tugas	25%
2	Kuis	20%
3	Ujian Tengah Semester	25%
4	Ujian Akhir Semester	30%
Total		100%

Mengetahui,
Ketua Program Studi

Rizky Putra Fhonna, S.T., M.Kom
NIP. 199111192019031012

Lhokseumawe, 5 Maret 2022

Koordinator

Rahma Fitria, B.Tech(Hons)., M.Sc
NIP. 198706122020122008