



Universitas Negeri Surabaya
Fakultas Teknik
Program Studi S1 Pendidikan Teknologi Informasi

Kode Dokumen

RENCANA PEMBELAJARAN SEMESTER

MATA KULIAH (MK)	KODE	Rumpun MK	BOBOT (sks)			SEMESTER	Tgl Penyusunan
Keamanan Jaringan Komputer	8320703030	Mata Kuliah Wajib Program Studi	T=3	P=0	ECTS=4.77	7	18 Januari 2025
OTORISASI	Pengembang RPS		Koordinator RMK			Koordinator Program Studi	
	Drs. Bambang Sujatmiko, M.T.				Drs. Bambang Sujatmiko, M.T.	

Model Pembelajaran	Project Based Learning
--------------------	------------------------

Capaian Pembelajaran (CP) **CPL-PRODI yang dibebankan pada MK**

CPL-6	Mampu mengambil keputusan berdasarkan data/informasi dan mampu menyelesaikan masalah di bidang teknologi informasi.
CPL-8	Menguasai konsep dan implementasi dalam mengembangkan rekayasa perangkat lunak, permainan, multimedia cerdas, dan teknik komputer jaringan.

Capaian Pembelajaran Mata Kuliah (CPMK)

CPMK - 1	Mahasiswa dapat menerapkan konsep keamanan jaringan untuk melindungi data dan informasi dalam jaringan komputer (C3)
CPMK - 2	Mahasiswa dapat menganalisis kerentanan sistem jaringan untuk mengidentifikasi potensi ancaman dan risiko (C4)
CPMK - 3	Mahasiswa dapat mengevaluasi efektivitas berbagai protokol keamanan jaringan dan alat keamanan dalam skenario yang berbeda (C5)
CPMK - 4	Mahasiswa dapat menciptakan solusi keamanan jaringan yang inovatif untuk mengatasi masalah keamanan yang spesifik (C6)
CPMK - 5	Mahasiswa dapat menerapkan teknik enkripsi dan dekripsi dalam melindungi data yang ditransmisikan melalui jaringan (C3)
CPMK - 6	Mahasiswa dapat menganalisis laporan keamanan jaringan untuk menentukan sumber dan jenis serangan (C4)
CPMK - 7	Mahasiswa dapat mengevaluasi kebijakan keamanan jaringan dan prosedur yang ada untuk memastikan mereka memenuhi standar keamanan yang diharapkan (C5)
CPMK - 8	Mahasiswa dapat menciptakan strategi pengelolaan risiko yang efektif untuk jaringan yang aman (C6)
CPMK - 9	Mahasiswa dapat menerapkan firewall dan sistem deteksi intrusi untuk melindungi jaringan dari serangan eksternal (C3)
CPMK - 10	Mahasiswa dapat menganalisis dan menyesuaikan konfigurasi keamanan jaringan untuk berbagai jenis jaringan (C4)

Matrik CPL - CPMK

	<table border="1"> <thead> <tr> <th>CPMK</th> <th>CPL-6</th> <th>CPL-8</th> </tr> </thead> <tbody> <tr><td>CPMK-1</td><td></td><td>✓</td></tr> <tr><td>CPMK-2</td><td>✓</td><td></td></tr> <tr><td>CPMK-3</td><td></td><td>✓</td></tr> <tr><td>CPMK-4</td><td>✓</td><td></td></tr> <tr><td>CPMK-5</td><td></td><td>✓</td></tr> <tr><td>CPMK-6</td><td>✓</td><td></td></tr> <tr><td>CPMK-7</td><td>✓</td><td></td></tr> <tr><td>CPMK-8</td><td>✓</td><td></td></tr> <tr><td>CPMK-9</td><td></td><td>✓</td></tr> <tr><td>CPMK-10</td><td></td><td>✓</td></tr> </tbody> </table>	CPMK	CPL-6	CPL-8	CPMK-1		✓	CPMK-2	✓		CPMK-3		✓	CPMK-4	✓		CPMK-5		✓	CPMK-6	✓		CPMK-7	✓		CPMK-8	✓		CPMK-9		✓	CPMK-10		✓
CPMK	CPL-6	CPL-8																																
CPMK-1		✓																																
CPMK-2	✓																																	
CPMK-3		✓																																
CPMK-4	✓																																	
CPMK-5		✓																																
CPMK-6	✓																																	
CPMK-7	✓																																	
CPMK-8	✓																																	
CPMK-9		✓																																
CPMK-10		✓																																

Matrik CPMK pada Kemampuan akhir tiap tahapan belajar (Sub-CPMK)

--	--

	CPMK	Minggu Ke															
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
	CPMK-1	✓	✓														
	CPMK-2			✓	✓												
	CPMK-3					✓	✓										
	CPMK-4							✓	✓								
	CPMK-5									✓							
	CPMK-6																
	CPMK-7										✓	✓					
	CPMK-8												✓	✓			
	CPMK-9														✓	✓	
CPMK-10																✓	

Deskripsi Singkat MK Mata kuliah Keamanan Jaringan Komputer mengajarkan konsep dasar keamanan jaringan komunikasi, aspek-aspek keamanan, kemungkinan ancaman dan serangan terhadap keamanan jaringan, dasar-dasar kriptografi, dan mekanisme keamanan jaringan seperti perlindungan host, firewall, IDS, VPN tool dan software yang dibutuhkan.

Pustaka	Utama :	
		<ol style="list-style-type: none"> 1. William Stallings. 2017. Cryptography and Network Security Principles and Practice Seventh Edition Global Edition. Pearson. 2. William Stallings. 2017. Network Security Essentials : Applications and Standards Sixth edition Global edition. Pearson 3. Joseph Migga Kizza. 2020. Guide to Computer Network Security Fifth Edition. Springer.
	Pendukung :	

Dosen Pengampu I Gusti Lanang Putra Eka Prisma, S.Kom., M.Kom.
I Made Suartana, S.Kom., M.Kom.

Mg Ke-	Kemampuan akhir tiap tahapan belajar (Sub-CPMK)	Penilaian		Bantuk Pembelajaran, Metode Pembelajaran, Penugasan Mahasiswa, [Estimasi Waktu]		Materi Pembelajaran [Pustaka]	Bobot Penilaian (%)
		Indikator	Kriteria & Bentuk	Luring (offline)	Daring (online)		
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
1	Pendahuluan materi, cakupan materi, penerapan dan kaitan keamanan jaringan dengan keilmuan dalam bidang informatika	<ol style="list-style-type: none"> 1. Memahami prasyarat matakuliah pengaman jaringan 2. Memahami kuliah keamanan jaringan dan kaitannya dengan matakuliah lain dan keilmuan dalam bidang informatika 3. Mengetahui penerapan keamanan jaringan dalam dunia nyata 	Kriteria: Dapat memahami Bentuk Penilaian : Penilaian Hasil Project / Penilaian Produk, Penilaian Portofolio	Pendekatan: Sainifik dengan Model Pembelajaran: Project-Based Learning 3 X 50	Diskusi kelompok tentang studi kasus keamanan jaringan, Simulasi serangan cyber dan penyusunan laporan hasil simulasi	Materi: Pengenalan keamanan jaringan, Enkripsi data, Firewall dan IDS, Manajemen akses pengguna, Deteksi intrusi Pustaka: Handbook Perkuliahan	3%
2	Pendahuluan materi, cakupan materi, penerapan dan kaitan keamanan jaringan dengan keilmuan dalam bidang informatika	<ol style="list-style-type: none"> 1. Memahami prasyrat matakuliah pengaman jaringan 2. Memahami kuliah keamanan jaringan dan kaitannya dengan matakuliah lain dan keilmuan dalam bidang informatika 3. Mengetahui penerapan keamanan jaringan dalam dunia nyata 	Kriteria: Dapat memahami Bentuk Penilaian : Penilaian Hasil Project / Penilaian Produk	Pendekatan: Sainifik dengan Model Pembelajaran: Project-Based Learning 3 X 50	Diskusi kelompok tentang studi kasus keamanan jaringan, Simulasi serangan cyber dan penyusunan laporan hasil simulasi	Materi: Pengenalan keamanan jaringan, Enkripsi data, Firewall dan IDS, Manajemen akses pengguna, Deteksi intrusi Pustaka: Handbook Perkuliahan	3%

3	Mendeteksi Permasalahan Keamanan dan kelemahan teknologi pada Jaringan Komputer	<ol style="list-style-type: none"> 1.Mengetahui permasalahan keamanan pada jaringan komputer 2.Mengetahui kelemahan-kelemahan teknologi jaringan komputer 3.Membedakan tipe-tipe serangan terhadap keamanan jaringan 4.Membedakan jenis-jenis serangan terhadap keamanan jaringan 5.Menerapkan tahapan-tahapan dalam mengetahui celah keamanan jaringan 	<p>Kriteria: Dapat menerapkan</p> <p>Bentuk Penilaian : Penilaian Hasil Project / Penilaian Produk</p>	Pendekatan: Sainifik dengan Model Pembelajaran: Project-Based Learning dan Pembelajaran berbasis masalah 3 X 50	Diskusi daring tentang studi kasus kerentanan sistem jaringan yang diberikan	<p>Materi: Pengenalan Kerentanan Sistem Jaringan, Teknik Analisis Kerentanan, Identifikasi Potensi Ancaman dan Risiko</p> <p>Pustaka: <i>Handbook Perkuliahan</i></p>	3%
4	Memahami konsep kriptografi sebagai dasar dalam mekanisme pengamanan jaringan	<ol style="list-style-type: none"> 1.Memahami cara kerja kriptografi 2.Membedakan jenis-jenis kriptografi 3.Menentukan fungsi dan peranan kriptografi dalam keamanan jaringan 	<p>Kriteria: Dapat mengevaluasi</p> <p>Bentuk Penilaian : Penilaian Hasil Project / Penilaian Produk</p>	Pendekatan: Sainifik dengan Model Pembelajaran: Project-Based Learning dan Pembelajaran berbasis masalah 3 X 50		<p>Materi: Memahami konsep kriptografi</p> <p>Pustaka: <i>William Stallings. 2017. Cryptography and Network Security Principles and Practice Seventh Edition Global Edition. Pearson.</i></p>	3%
5	Membedakan cara kerja algoritma kriptografi simetrik dan asimetrik	<ol style="list-style-type: none"> 1.Menjelaskan cara kerja kriptografi simetrik 2.Menjelaskan cara kerja kriptografi Asimetrik 3.Membedakan karakteristik kriptografi simetrik dan asimetrik 	<p>Kriteria: Dapat mengevaluasi</p> <p>Bentuk Penilaian : Penilaian Hasil Project / Penilaian Produk</p>	Pendekatan: Sainifik dengan Model Pembelajaran: Project-Based Learning dan Pembelajaran berbasis masalah 3 X 50	Penugasan Analisis Efektivitas Protokol Keamanan, Penugasan Pemilihan Alat Keamanan yang Tepat	<p>Materi: Pengenalan Protokol Keamanan Jaringan, Analisis Risiko Keamanan Jaringan, Pemilihan Alat Keamanan yang Tepat</p> <p>Pustaka: <i>Handbook Perkuliahan</i></p>	3%
6	Membedakan cara kerja algoritma kriptografi simetrik dan asimetrik	<ol style="list-style-type: none"> 1.Menjelaskan cara kerja kriptografi simetrik 2.Menjelaskan cara kerja kriptografi Asimetrik 3.Membedakan karakteristik kriptografi simetrik dan asimetrik 	<p>Kriteria: Dapat mengevaluasi</p> <p>Bentuk Penilaian : Penilaian Hasil Project / Penilaian Produk</p>	Pendekatan: Sainifik dengan Model Pembelajaran: Project-Based Learning dan Pembelajaran berbasis masalah 3 X 50	Penugasan Analisis Efektivitas Protokol Keamanan, Penugasan Pemilihan Alat Keamanan yang Tepat	<p>Materi: Pengenalan Protokol Keamanan Jaringan, Analisis Risiko Keamanan Jaringan, Pemilihan Alat Keamanan yang Tepat</p> <p>Pustaka: <i>Handbook Perkuliahan</i></p>	3%
7	Memahami permasalahan dalam keamanan jaringan meliputi asal permasalahan, cara mendeteksi permasalahan	Menganalisis permasalahan keamanan pada jaringan komputer	<p>Kriteria: Dapat menganalisis dan menerapkan</p> <p>Bentuk Penilaian : Penilaian Hasil Project / Penilaian Produk</p>	Pendekatan: Sainifik dengan Model Pembelajaran: Project-Based Learning dan Pembelajaran berbasis masalah 3 X 50	Penugasan proyek keamanan jaringan inovatif	<p>Materi: Analisis Masalah Keamanan Jaringan, Inovasi dalam Keamanan Jaringan, Rancang Bangun Solusi Keamanan</p> <p>Pustaka: <i>Handbook Perkuliahan</i></p>	3%

8	UTS	<ol style="list-style-type: none"> 1.Solusi keamanan jaringan yang inovatif 2.Kreativitas dalam pemecahan masalah keamanan 3.Efektivitas solusi yang diusulkan 	<p>Kriteria: Dapat menganalisis dan menerapkan</p> <p>Bentuk Penilaian : Aktifitas Partisipasif, Penilaian Hasil Project / Penilaian Produk</p>	UTS 3 X 50	Pengembangan Proyek Keamanan Jaringan	<p>Materi: Analisis Masalah Keamanan Jaringan, Inovasi dalam Keamanan Jaringan, Implementasi Solusi Keamanan</p> <p>Pustaka: <i>Handbook Perkuliahan</i></p>	20%
9	Memahami aspek keamanan jaringan (ancaman dan mekanisme keamanan) pada layer 2 dan 3 TCP/IP model	<ol style="list-style-type: none"> 1.Menjelaskan konsep layer 2 dan layer 3 TCP/IP dan OSI model kaitannya dengan keamanan jaringan 2.Menganalisis ancaman keamanan dan jenis serangan pada layer 2 dan 3 3. Mengimplementasikan mekanisme security pada layer 2 dan layer 3 	<p>Kriteria: Dapat menganalisis dan menerapkan</p> <p>Bentuk Penilaian : Penilaian Hasil Project / Penilaian Produk</p>	Pendekatan: Sainifik dengan Model Pembelajaran: Project-Based Learning dan Pembelajaran berbasis masalah 3 X 50	Penugasan online memungkinkan, Pembuatan proyek implementasi teknik enkripsi dan dekripsi	<p>Materi: Pengenalan teknik enkripsi dan dekripsi, Algoritma enkripsi simetris dan asimetris, Implementasi enkripsi pada jaringan komputer</p> <p>Pustaka: <i>Handbook Perkuliahan</i></p>	3%
10	Memahami konsep autentikasi sebagai mekanisme keamanan jaringan	<ol style="list-style-type: none"> 1.Menjelaskan Konsep autentikasi dan kaitannya dengan keamanan jaringan 2.Membedakan Jenis-jenis mekanisme autentikasi 3.Menerapkan mekanisme autentikasi untuk pengamanan jaringan 	<p>Kriteria: Dapat mengevaluasi</p> <p>Bentuk Penilaian : Penilaian Hasil Project / Penilaian Produk</p>	Pendekatan: Sainifik dengan Model Pembelajaran: Project-Based Learning dan Pembelajaran berbasis masalah 3 X 50	Pembuatan laporan analisis keamanan jaringan berdasarkan studi kasus yang diberikan. Mahasiswa diminta untuk mengidentifikasi sumber dan jenis serangan yang terjadi serta memberikan rekomendasi perlindungan yang sesuai.	<p>Materi: Pengenalan laporan keamanan jaringan, Teknik analisis sumber serangan, Teknik analisis jenis serangan</p> <p>Pustaka: <i>Handbook Perkuliahan</i></p>	3%
11	Memahami konsep autentikasi sebagai mekanisme keamanan jaringan	<ol style="list-style-type: none"> 1.Menjelaskan Konsep autentikasi dan kaitannya dengan keamanan jaringan 2.Membedakan Jenis-jenis mekanisme autentikasi 3.Menerapkan mekanisme autentikasi untuk pengamanan jaringan 	<p>Kriteria: Dapat mengevaluasi</p> <p>Bentuk Penilaian : Penilaian Hasil Project / Penilaian Produk</p>	Pendekatan: Sainifik dengan Model Pembelajaran: Project-Based Learning dan Pembelajaran berbasis masalah 3 X 50	Pembuatan laporan analisis keamanan jaringan berdasarkan keamanan laporan jaringan, Mahasiswa diminta untuk mengidentifikasi sumber dan jenis serangan yang terjadi serta memberikan rekomendasi perlindungan yang sesuai.	<p>Materi: Pengenalan laporan keamanan jaringan, Teknik analisis sumber serangan, Teknik analisis jenis serangan</p> <p>Pustaka: <i>Handbook Perkuliahan</i></p>	3%
12	Memahami cara kerja dan implementasi Firewall dalam pengamanan jaringan	<ol style="list-style-type: none"> 1.Menjelaskan konsep dan cara kerja firewall 2.Menerapkan Firewall dalam jaringan 	<p>Kriteria: Dapat mengevaluasi</p> <p>Bentuk Penilaian : Penilaian Hasil Project / Penilaian Produk, Penilaian Portofolio</p>	Pendekatan: Sainifik dengan Model Pembelajaran: Project-Based Learning dan Pembelajaran berbasis masalah 3 X 50	Diskusi daring tentang studi kasus pengelolaan risiko, Penugasan individu untuk merancang strategi pengelolaan risiko	<p>Materi: Identifikasi risiko, Analisis risiko, Mitigasi risiko, Implementasi strategi pengelolaan risiko</p> <p>Pustaka: <i>Handbook Perkuliahan</i></p>	5%
13	Memahami cara kerja dan implementasi Firewall dalam pengamanan jaringan	<ol style="list-style-type: none"> 1.Menjelaskan konsep dan cara kerja firewall 2.Menerapkan Firewall dalam jaringan 	<p>Kriteria: Dapat mengevaluasi</p> <p>Bentuk Penilaian : Penilaian Hasil Project / Penilaian Produk, Penilaian Praktikum</p>	Pendekatan: Sainifik dengan Model Pembelajaran: Project-Based Learning dan Pembelajaran berbasis masalah 3 X 50	Diskusi daring tentang studi kasus pengelolaan risiko, Penugasan individu untuk merancang strategi pengelolaan risiko	<p>Materi: Identifikasi risiko, Analisis risiko, Mitigasi risiko, Implementasi strategi pengelolaan risiko</p> <p>Pustaka: <i>Handbook Perkuliahan</i></p>	5%

14	Memahami jenis atau teknik-teknik dan monitoring dalam konteks pengamanan jaringan	1.Menjelaskan metode-metode pengamanan jaringan 2.Menerapkan mekanisme pengawasan dalam konteks pengamanan jaringan	Kriteria: Dapat mengevaluasi dan mengimitasi Bentuk Penilaian : Penilaian Hasil Project / Penilaian Produk, Penilaian Portofolio	Pendekatan: Sainifik dengan Model Pembelajaran: Project-Based Learning dan Pembelajaran berbasis masalah 3 X 50	Penugasan proyek online	Materi: Pengenalan Firewall, Konfigurasi Firewall, Penggunaan Sistem Deteksi Intrusi, Analisis Serangan Eksternal Pustaka: <i>Handbook Perkuliahan</i>	5%
15	Memahami jenis atau teknik-teknik dan monitoring dalam konteks pengamanan jaringan	1.Menjelaskan metode-metode pengamanan jaringan 2.Menerapkan mekanisme pengawasan dalam konteks pengamanan jaringan	Kriteria: Dapat mengevaluasi dan mengimitasi Bentuk Penilaian : Penilaian Hasil Project / Penilaian Produk	Pendekatan: Sainifik dengan Model Pembelajaran: Project-Based Learning dan Pembelajaran berbasis masalah 3 X 50	Penugasan proyek online	Materi: Pengenalan Firewall, Konfigurasi Firewall, Penggunaan Sistem Deteksi Intrusi, Analisis Serangan Eksternal Pustaka: <i>Handbook Perkuliahan</i>	5%
16	Mahasiswa diharapkan mampu menganalisis kebutuhan keamanan jaringan berdasarkan jenis jaringan yang berbeda dan dapat mengkonfigurasi sistem keamanan yang sesuai.	1.Analisis kebutuhan keamanan jaringan 2.Pemahaman risiko keamanan jaringan 3.Kemampuan mengkonfigurasi keamanan jaringan	Kriteria: Dapaqt mengimplementasikan dan meniru Bentuk Penilaian : Penilaian Hasil Project / Penilaian Produk, Tes	UAS	UAS	Materi: Konsep Keamanan Jaringan, Risiko Keamanan Jaringan, Konfigurasi Keamanan Jaringan Pustaka: <i>Handbook Perkuliahan</i>	30%

Rekap Persentase Evaluasi : Project Based Learning

No	Evaluasi	Persentase
1.	Aktifitas Partisipasif	10%
2.	Penilaian Hasil Project / Penilaian Produk	66%
3.	Penilaian Portofolio	6.5%
4.	Penilaian Praktikum	2.5%
5.	Tes	15%
		100%

Catatan

- 1. Capaian Pembelajaran Lulusan Prodi (CPL - Prodi)** adalah kemampuan yang dimiliki oleh setiap lulusan prodi yang merupakan internalisasi dari sikap, penguasaan pengetahuan dan ketrampilan sesuai dengan jenjang prodinya yang diperoleh melalui proses pembelajaran.
- 2. CPL yang dibebankan pada mata kuliah** adalah beberapa capaian pembelajaran lulusan program studi (CPL-Prodi) yang digunakan untuk pembentukan/pengembangan sebuah mata kuliah yang terdiri dari aspek sikap, ketrampilan umum, ketrampilan khusus dan pengetahuan.
- 3. CP Mata kuliah (CPMK)** adalah kemampuan yang dijabarkan secara spesifik dari CPL yang dibebankan pada mata kuliah, dan bersifat spesifik terhadap bahan kajian atau materi pembelajaran mata kuliah tersebut.
- 4. Sub-CPMK Mata kuliah (Sub-CPMK)** adalah kemampuan yang dijabarkan secara spesifik dari CPMK yang dapat diukur atau diamati dan merupakan kemampuan akhir yang direncanakan pada tiap tahap pembelajaran, dan bersifat spesifik terhadap materi pembelajaran mata kuliah tersebut.
- 5. Indikator penilaian** kemampuan dalam proses maupun hasil belajar mahasiswa adalah pernyataan spesifik dan terukur yang mengidentifikasi kemampuan atau kinerja hasil belajar mahasiswa yang disertai bukti-bukti.
- 6. Kreteria Penilaian** adalah patokan yang digunakan sebagai ukuran atau tolok ukur ketercapaian pembelajaran dalam penilaian berdasarkan indikator-indikator yang telah ditetapkan. Kreteria penilaian merupakan pedoman bagi penilai agar penilaian konsisten dan tidak bias. Kreteria dapat berupa kuantitatif ataupun kualitatif.
- 7. Bentuk penilaian:** tes dan non-tes.
- 8. Bentuk pembelajaran:** Kuliah, Responsi, Tutorial, Seminar atau yang setara, Praktikum, Praktik Studio, Praktik Bengkel, Praktik Lapangan, Penelitian, Pengabdian Kepada Masyarakat dan/atau bentuk pembelajaran lain yang setara.
- 9. Metode Pembelajaran:** Small Group Discussion, Role-Play & Simulation, Discovery Learning, Self-Directed Learning, Cooperative Learning, Collaborative Learning, Contextual Learning, Project Based Learning, dan metode lainnya yg setara.
- 10. Materi Pembelajaran** adalah rincian atau uraian dari bahan kajian yg dapat disajikan dalam bentuk beberapa pokok dan sub-pokok bahasan.
- 11. Bobot penilaian** adalah prosentasi penilaian terhadap setiap pencapaian sub-CPMK yang besarnya proposional dengan tingkat kesulitan pencapaian sub-CPMK tsb., dan totalnya 100%.
- 12. TM=Tatap Muka, PT=Penugasan terstruktur, BM=Belajar mandiri.**

RPS ini telah divalidasi pada tanggal 22 Desember 2024

Koordinator Program Studi S1
Pendidikan Teknologi Informasi

UPM Program Studi S1
Pendidikan Teknologi Informasi



Drs. Bambang Sujatmiko, M.T.
NIDN 0019056503



Martini Dwi Endah Susanti,
S.Kom., M.Kom.
NIDN 0016039305



File PDF ini digenerate pada tanggal 18 Januari 2025 Jam 15:06 menggunakan aplikasi RPS-OBE S1 Dia Unesa