KEMENTERIAN PENDIDIKAN TINGGI, SAINS, DAN TEKNOLOGI
POLITEKNIK NEGERI PADANG
JURUSAN TEKNOLOGI INFORMASI

RENCANA PEMBELAJARAN SEMESTER

(RPS)

MATA KULIAH

Keamanan Sistem Informasi

Rencana Pembelajaran Semester ini terdiri atas dua bagian: Mata Kuliah Teori (2 SKS) dan Mata Kuliah Praktikum (1 SKS).

Program Studi D3 – Manajemen Informatika
Politeknik Negeri Padang
2026

BAGIAN I — MATA KULIAH TEORI

1. Identitas Mata Kuliah

Komponen	Keterangan
Program Studi	D3 – Manajemen Informatika
Nama Mata Kuliah	Keamanan Sistem Informasi
Kode Mata Kuliah	ISY3210
Semester	4 (Empat)
Bobot SKS	2 SKS (Teori)
Nama Dosen Pengampu	Ir. H.A. Mooduto, M.Kom.

2. Deskripsi Singkat Mata Kuliah

Mata kuliah ini membekali mahasiswa dengan pemahaman konseptual dan analitis tentang keamanan informasi dalam organisasi. Materi mencakup prinsip dasar keamanan informasi (CIA Triad), ancaman dan kerentanan sistem, kriptografi, manajemen risiko keamanan, kebijakan dan standar keamanan, keamanan jaringan dan aplikasi, aspek hukum dan etika, serta tren terkini dalam keamanan siber. Pembelajaran dilaksanakan melalui pendekatan teoritis, studi kasus, diskusi interaktif, dan analisis kebijakan untuk membangun kompetensi analitis sesuai KKNI Level 5. Mata kuliah ini dirancang untuk menghasilkan lulusan yang mampu memahami, menganalisis, dan merancang solusi keamanan informasi dasar bagi organisasi skala kecil dan menengah.

3. Capaian Pembelajaran Lulusan (CPL) yang Dibebankan

Mata kuliah Keamanan Sistem Informasi berkontribusi terhadap pencapaian dua CPL Program Studi sebagai berikut:

Kode CPL	Deskripsi Capaian Pembelajaran Lulusan
CPL-2	Mampu menguasai konsep teoretis bidang manajemen informatika secara umum dan khusus untuk menyelesaikan masalah secara prosedural sesuai dengan lingkup pekerjaannya.
CPL-6	Mampu mengelola dan memelihara infrastruktur teknologi informasi (jaringan, server, sistem cloud) serta menerapkan prinsip keamanan informasi untuk mendukung keberlangsungan operasional organisasi.

4. Capaian Pembelajaran Mata Kuliah (CPMK)

Setelah menyelesaikan mata kuliah ini, mahasiswa mampu:

Kode CPMK	Deskripsi Capaian Pembelajaran Mata Kuliah
CPMK 1	Menjelaskan konsep dasar keamanan informasi, ancaman, kerentanan, serta standar dan framework keamanan informasi yang berlaku.
CPMK 2	Menganalisis penerapan teknik kriptografi untuk pengamanan data dan autentikasi dalam berbagai skenario organisasi.
CPMK 3	Melakukan analisis risiko keamanan informasi dan merancang kontrol keamanan serta kebijakan keamanan yang sesuai.
CPMK 4	Menganalisis implementasi keamanan pada jaringan dan aplikasi serta mengevaluasi aspek hukum dan etika dalam keamanan informasi.

5. Kemampuan yang Diharapkan (Sub-CPMK)

Kode Sub-CPMK	Deskripsi Kemampuan Akhir (Sub-CPMK)
Sub-CPMK 1.1	Menjelaskan prinsip kerahasiaan, integritas, dan ketersediaan (CIA Triad) dalam keamanan informasi
Sub-CPMK 1.2	Mengidentifikasi berbagai jenis ancaman, kerentanan, dan serangan keamanan informasi
Sub-CPMK 1.3	Menjelaskan standar dan framework keamanan informasi (ISO 27001, NIST Cybersecurity Framework)
Sub-CPMK 2.1	Menjelaskan konsep dan perbedaan kriptografi simetris dan asimetris
Sub-CPMK 2.2	Menganalisis penerapan fungsi hash dan digital signature untuk integritas data dan autentikasi
Sub-CPMK 2.3	Mengevaluasi implementasi infrastruktur kunci publik (PKI) dalam organisasi
Sub-CPMK 3.1	Melakukan analisis risiko keamanan informasi menggunakan metode kualitatif
Sub-CPMK 3.2	Merancang kontrol keamanan administratif, teknis, dan fisik berdasarkan hasil analisis risiko
Sub-CPMK 3.3	Menyusun kebijakan keamanan informasi sederhana untuk organisasi skala kecil
Sub-CPMK 4.1	Menganalisis mekanisme keamanan jaringan (firewall, IDS/IPS, VPN, protokol aman)
Sub-CPMK 4.2	Mengidentifikasi kerentanan keamanan aplikasi berdasarkan OWASP Top 10
Sub-CPMK 4.3	Menjelaskan aspek hukum, etika, dan kepatuhan dalam keamanan informasi (UU ITE, perlindungan data pribadi)

6. Tabel Korelasi CPL – CPMK dengan Bobot Kontribusi

CPMK	CPL-2 (50%)	CPL-6 (50%)	Total
CPMK 1	12,5%	12,5%	**25%**
CPMK 2	12,5%	12,5%	**25%**
CPMK 3	12,5%	12,5%	**25%**
CPMK 4	12,5%	12,5%	**25%**
Total	**50%**	**50%**	**100%**

▪ *Simbol dan angka persen menunjukkan bobot kontribusi langsung setiap CPMK terhadap masing-masing CPL.*

- *Total kontribusi mata kuliah terhadap CPL-2 = 50%, terhadap CPL-6 = 50%.*

7. Tabel Korelasi CPL – Sub-CPMK

Sub-CPMK	CPL-2	CPL-6
Sub-CPMK 1.1	√	√
Sub-CPMK 1.2	√	√
Sub-CPMK 1.3	√	√
Sub-CPMK 2.1	√	√
Sub-CPMK 2.2	√	√
Sub-CPMK 2.3	√	√
Sub-CPMK 3.1	√	√
Sub-CPMK 3.2	√	√
Sub-CPMK 3.3	√	√
Sub-CPMK 4.1	√	√
Sub-CPMK 4.2	√	√
Sub-CPMK 4.3	√	√

8. Daftar Referensi

1. Stallings, W. (2020). Cryptography and Network Security: Principles and Practice (8th ed.). Pearson.

2. Whitman, M. E., & Mattord, H. J. (2021). Principles of Information Security (7th ed.). Cengage Learning.

3. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. International Organization for Standardization.

4. NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). National Institute of Standards and Technology.

5. OWASP Foundation. (2021). OWASP Top Ten - 2021. The Open Web Application Security Project.

6. Easttom, C. (2021). Computer Security Fundamentals (5th ed.). Pearson.

7. Vacca, J. R. (2020). Computer and Information Security Handbook (3rd ed.). Morgan Kaufmann.

8. Kim, D., & Solomon, M. G. (2021). Fundamentals of Information Systems Security (4th ed.). Jones & Bartlett Learning.

9. Bahan Kajian

1. Konsep Dasar Keamanan Informasi: CIA Triad (Confidentiality, Integrity, Availability), ancaman (threats), kerentanan (vulnerabilities), serangan (attacks), aset informasi, dan siklus hidup keamanan.

2. Kriptografi: kriptografi simetris (AES, DES) dan asimetris (RSA), fungsi hash (SHA, MD5), digital signature, infrastruktur kunci publik (PKI), dan manajemen kunci.

3. Manajemen Risiko Keamanan: identifikasi aset, analisis risiko (kualitatif dan kuantitatif), perlakuan risiko (risk treatment), matriks risiko, dan pemilihan kontrol.

4. Standar dan Framework Keamanan: ISO 27001, NIST Cybersecurity Framework, COBIT, dan PCI DSS.

5. Kebijakan Keamanan Informasi: struktur kebijakan, jenis kebijakan (EISP, ISSP, SysSP), prosedur, standar, dan pedoman.

6. Keamanan Jaringan: firewall, IDS/IPS, VPN, SSL/TLS, IPSec, segmentasi jaringan, dan arsitektur jaringan aman.

7. Keamanan Aplikasi: OWASP Top 10, secure coding principles, vulnerability assessment, dan penetration testing.

8. Aspek Hukum dan Etika: UU ITE, perlindungan data pribadi, hak kekayaan intelektual, cyber crime, dan etika profesional.

10. Rencana Pembelajaran per Pertemuan

Pert. Ke-	Sub-CPMK	Topik Bahasan	Metode Pembelajaran	Pengalaman Belajar Mahasiswa	Waktu (menit)	Kriteria & Indikator Penilaian	Bobot (%)	CPL
1	[1.1] Menjelaskan prinsip CIA Triad	Konsep dasar keamanan informasi: definisi, tujuan, pentingnya, prinsip CIA (Confidentiality, Integrity, Availability)	Ceramah interaktif, diskusi kelompok, studi kasus	Mendiskusikan contoh pelanggaran CIA di kehidupan sehari-hari; menganalisis studi kasus kebocoran data (mis. Tokopedia, Facebook)	100	Kriteria: ketepatan analisis, kedalaman pemahaman. Indikator: mampu mengidentifikasi pelanggaran CIA dalam kasus nyata, menjelaskan dampak, dan memberikan rekomendasi dasar	**2%**	CPL-2, CPL-6
2	[1.2] Mengidentifikasi ancaman dan kerentanan	Ancaman, kerentanan, serangan keamanan: malware, phishing, DDoS, social engineering, ransomware	Presentasi, analisis kasus, diskusi interaktif	Menganalisis kasus serangan siber terkini (ransomware, phishing); membuat peta ancaman untuk organisasi fiktif (UKM, rumah sakit, bank)	100	Kriteria: ketepatan identifikasi ancaman, kedalaman analisis. Indikator: mampu mengidentifikasi 5+ jenis ancaman, menjelaskan modus operandi, dan memetakan dampaknya	**2%**	CPL-2, CPL-6
3	[1.3] Menjelaskan standar keamanan informasi	Standar dan framework: ISO 27001, NIST Cybersecurity Framework, COBIT, PCI DSS	Ceramah, diskusi, analisis perbandingan	Membandingkan struktur dan pendekatan ISO 27001 vs NIST Framework; mengidentifikasi klausul relevan untuk organisasi tertentu	100	Kriteria: pemahaman standar, kemampuan membandingkan. Indikator: mampu menjelaskan struktur ISO 27001 (14 domain), membandingkan dengan NIST (5 fungsi), dan merekomendasikan standar yang sesuai	**2,5%**	CPL-2, CPL-6
4	[2.1] Menjelaskan konsep kriptografi simetris dan asimetris	Dasar kriptografi: algoritma simetris (AES, DES), asimetris (RSA), perbandingan, kelebihan dan kekurangan	Ceramah, demonstrasi (simulasi), studi kasus	Menganalisis skenario penggunaan kriptografi dalam e-commerce, email, dan perbankan; membandingkan performa dan keamanan berbagai algoritma	100	Kriteria: pemahaman konsep, kemampuan analisis perbandingan. Indikator: mampu menjelaskan perbedaan kriptografi simetris dan asimetris, memberikan contoh implementasi, dan menganalisis kelebihan/kekurangan	**2%**	CPL-2, CPL-6

Pert. Ke-	Sub-CPMK	Topik Bahasan	Metode Pembelajaran	Pengalaman Belajar Mahasiswa	Waktu (menit)	Kriteria & Indikator Penilaian	Bobot (%)	CPL
5	[2.2] Menganalisis penerapan hash dan digital signature	Fungsi hash (SHA, MD5), digital signature, integritas data, autentikasi, studi kasus implementasi	Ceramah, diskusi, analisis kasus	Menganalisis penggunaan hash untuk verifikasi integritas file/download; mengevaluasi implementasi digital signature dalam kontrak dan dokumen elektronik	100	Kriteria: ketepatan analisis, pemahaman aplikasi. Indikator: mampu menjelaskan cara kerja hash dan digital signature, memberikan contoh aplikasi, dan menganalisis potensi kerentanan	**2%**	CPL-2, CPL-6
6	[2.3] Mengevaluasi implementasi PKI	Infrastruktur Kunci Publik (PKI), Certificate Authority (CA), sertifikat digital, SSL/TLS, aplikasi PKI	Ceramah, studi kasus, diskusi	Menganalisis hierarki trust dalam PKI; mengevaluasi implementasi SSL/TLS pada website (analisis sertifikat)	100	Kriteria: pemahaman konsep PKI, kemampuan evaluasi. Indikator: mampu menjelaskan komponen PKI (CA, RA, sertifikat), menganalisis rantai kepercayaan, dan mengevaluasi keamanan implementasi	**2%**	CPL-2, CPL-6
7	[3.1] Melakukan analisis risiko keamanan informasi	Manajemen risiko: identifikasi aset, penilaian risiko (likelihood, impact), matriks risiko, risk treatment	Workshop, studi kasus, diskusi kelompok	Melakukan analisis risiko untuk organisasi fiktif (UKM, rumah sakit); membuat matriks risiko dan prioritas penanganan	100	Kriteria: kelengkapan identifikasi, ketepatan penilaian. Indikator: mampu mengidentifikasi aset, menilai risiko (likelihood × impact), membuat matriks risiko, dan menentukan prioritas penanganan	**2,5%**	CPL-2, CPL-6
8	UJIAN TENGAH SEMESTER	Materi pertemuan 1–7	Ujian tertulis	Mengerjakan soal ujian teori dan studi kasus komprehensif	100	Kriteria: ketepatan jawaban, kedalaman analisis. Indikator: mampu menjawab soal dengan tepat, menganalisis kasus, dan mengintegrasikan konsep	**30%**	CPL-2, CPL-6
9	[3.2] Merancang kontrol keamanan	Kontrol keamanan: administratif, teknis, fisik; pemilihan kontrol berdasarkan hasil analisis risiko	Diskusi, studi kasus, brainstorming	Merancang kontrol keamanan untuk mitigasi risiko yang telah diidentifikasi; mengevaluasi efektivitas kontrol yang	100	Kriteria: relevansi kontrol, kelengkapan aspek. Indikator: mampu merancang kontrol administratif, teknis, dan fisik yang relevan dengan risiko,	**2%**	CPL-2, CPL-6

Pert. Ke-	Sub-CPMK	Topik Bahasan	Metode Pembelajaran	Pengalaman Belajar Mahasiswa	Waktu (menit)	Kriteria & Indikator Penilaian	Bobot (%)	CPL
				diusulkan		serta mengevaluasi efektivitasnya		
10	[3.3] Menyusun kebijakan keamanan informasi	Kebijakan keamanan informasi: struktur, konten, implementasi; jenis kebijakan (EISP, ISSP, SysSP)	Simulasi, diskusi, analisis dokumen	Menyusun kebijakan keamanan sederhana (Acceptable Use Policy, Password Policy); menganalisis contoh kebijakan dari organisasi nyata	100	Kriteria: kelengkapan konten, kejelasan bahasa, kesesuaian standar. Indikator: mampu menyusun kebijakan dengan struktur lengkap (tujuan, ruang lingkup, kebijakan, sanksi), bahasa jelas, dan mengacu pada standar	**2,5%**	CPL-2, CPL-6
11	[4.1] Menganalisis keamanan jaringan	Keamanan jaringan: firewall, IDS/IPS, VPN, protokol aman (SSL/TLS, IPSec, SSH)	Ceramah, studi kasus, analisis konfigurasi	Menganalisis konfigurasi firewall pada skenario jaringan tertentu; mengevaluasi keamanan implementasi VPN dan protokol jaringan	100	Kriteria: pemahaman konsep keamanan jaringan, kemampuan analisis. Indikator: mampu menjelaskan fungsi firewall, IDS/IPS, VPN, menganalisis konfigurasi, dan mengevaluasi keamanan protokol	**2%**	CPL-2, CPL-6
12	[4.1] Lanjutan analisis keamanan jaringan	Arsitektur jaringan aman, segmentasi jaringan, DMZ, Zero Trust Architecture	Studi kasus, analisis desain, diskusi	Menganalisis desain arsitektur jaringan organisasi; mengevaluasi penerapan Zero Trust Architecture dan segmentasi jaringan	100	Kriteria: ketepatan analisis arsitektur, pemahaman konsep modern. Indikator: mampu menganalisis kelemahan arsitektur jaringan, merekomendasikan perbaikan, dan menjelaskan konsep Zero Trust	**2%**	CPL-2, CPL-6
13	[4.2] Mengidentifikasi kerentanan keamanan aplikasi	Keamanan aplikasi: OWASP Top 10, kerentanan umum (injection, XSS, broken authentication)	Ceramah, studi kasus, analisis kode	Menganalisis kerentanan pada aplikasi web fiktif berdasarkan OWASP Top 10; mengevaluasi praktik secure coding	100	Kriteria: ketepatan identifikasi kerentanan, pemahaman OWASP. Indikator: mampu mengidentifikasi 5+ kerentanan OWASP, menjelaskan dampak, dan merekomendasikan perbaikan	**2%**	CPL-2, CPL-6

Pert. Ke-	Sub-CPMK	Topik Bahasan	Metode Pembelajaran	Pengalaman Belajar Mahasiswa	Waktu (menit)	Kriteria & Indikator Penilaian	Bobot (%)	CPL
14	[4.3] Menjelaskan aspek hukum dan etika	Aspek hukum: UU ITE, perlindungan data pribadi (UU PDP), cyber crime, hak kekayaan intelektual; etika profesional	Ceramah, diskusi, analisis kasus hukum	Menganalisis kasus pelanggaran UU ITE dan cyber crime; mendiskusikan dilema etika dalam keamanan informasi (whistleblowing, ethical hacking)	100	Kriteria: pemahaman aspek hukum, kemampuan analisis etika. Indikator: mampu menjelaskan ketentuan UU ITE dan UU PDP, menganalisis kasus hukum, dan mengevaluasi dilema etika	**2%**	CPL-2, CPL-6
15	[4.3] Lanjutan aspek hukum dan kepatuhan	Kepatuhan (compliance), audit keamanan, tanggung jawab profesional, tren terkini keamanan informasi	Presentasi kelompok, diskusi panel	Mempresentasikan analisis tren keamanan terkini (AI security, IoT security, cloud security); mendiskusikan implikasi kepatuhan dan audit keamanan	100	Kriteria: kualitas presentasi, kedalaman analisis tren. Indikator: mampu mempresentasikan analisis tren keamanan dengan sistematis, menjelaskan implikasi, dan menjawab pertanyaan	**2%**	CPL-2, CPL-6
16	UJIAN AKHIR SEMESTER	Materi pertemuan 9–15	Ujian tertulis	Mengerjakan soal ujian teori dan studi kasus komprehensif	100	Kriteria: ketepatan jawaban, kemampuan analisis integratif. Indikator: mampu menjawab soal dengan tepat, menganalisis kasus kompleks, dan mengintegrasikan seluruh konsep	**30%**	CPL-2, CPL-6

Total Bobot Penilaian: Tugas per pertemuan (14 pertemuan × 2% atau 2,5%) = 30% + Partisipasi = 10% + UTS = 30% + UAS = 30% → Total = 100%

Ditetapkan di: Padang
Tanggal: 23 Februari 2026

Dosen Pengampu,

Ir. H.A. Mooduto, M.Kom.
NIP. 196605101994031003

BAGIAN II — MATA KULIAH PRAKTIKUM

1. Identitas Mata Kuliah

Komponen	Keterangan
Program Studi	D3 – Manajemen Informatika
Nama Mata Kuliah	Keamanan Sistem Informasi (Praktikum)
Kode Mata Kuliah	ISY3210
Semester	4 (Empat)
Bobot SKS	1 SKS (Praktikum)
Nama Dosen Pengampu	1. Ir. H.A. Mooduto, M.Kom. 2. Ideva Gaputra, S.Kom., M.Kom.

2. Deskripsi Singkat Mata Kuliah

Mata kuliah praktikum ini merupakan pelengkap dari mata kuliah teori Keamanan Sistem Informasi yang memberikan pengalaman langsung kepada mahasiswa dalam mengimplementasikan berbagai konsep dan teknik keamanan informasi. Mahasiswa akan melakukan praktik konfigurasi perangkat keamanan, implementasi kriptografi, analisis kerentanan, simulasi serangan dan pertahanan, serta penyusunan kebijakan keamanan. Praktikum dilaksanakan di laboratorium komputer dengan panduan modul dan pendampingan instruktur. Setiap pertemuan dirancang untuk mengembangkan keterampilan teknis yang relevan dengan kebutuhan industri dan sesuai dengan KKNI Level 5.

3. Capaian Pembelajaran Lulusan (CPL) yang Dibebankan

Mata kuliah Keamanan Sistem Informasi (Praktikum) berkontribusi terhadap pencapaian dua CPL Program Studi sebagai berikut:

Kode CPL	Deskripsi Capaian Pembelajaran Lulusan
CPL-2	Mampu menguasai konsep teoretis bidang manajemen informatika secara umum dan khusus untuk menyelesaikan masalah secara prosedural sesuai dengan lingkup pekerjaannya.
CPL-6	Mampu mengelola dan memelihara infrastruktur teknologi informasi (jaringan, server, sistem cloud) serta menerapkan prinsip keamanan informasi untuk mendukung keberlangsungan operasional organisasi.

4. Capaian Pembelajaran Mata Kuliah (CPMK)

Setelah menyelesaikan mata kuliah praktikum ini, mahasiswa mampu:

Kode CPMK	Deskripsi Capaian Pembelajaran Mata Kuliah
CPMK 1	Mengimplementasikan teknik kriptografi untuk pengamanan data dan komunikasi.
CPMK 2	Melakukan analisis risiko keamanan dan menyusun dokumen kebijakan keamanan sederhana.
CPMK 3	Mengkonfigurasi perangkat keamanan jaringan (firewall, IDS, VPN) dan menganalisis keamanannya.
CPMK 4	Melakukan pengujian keamanan aplikasi web dan mengidentifikasi kerentanan berdasarkan OWASP Top 10.

5. Kemampuan yang Diharapkan (Sub-CPMK)

Kode Sub-CPMK	Deskripsi Kemampuan Akhir (Sub-CPMK)
Sub-CPMK 1.1	Menggunakan tools kriptografi (OpenSSL, GnuPG) untuk mengenkripsi dan mendekripsi file
Sub-CPMK 1.2	Membuat dan memverifikasi digital signature menggunakan OpenSSL
Sub-CPMK 1.3	Mengimplementasikan hash untuk verifikasi integritas file
Sub-CPMK 2.1	Melakukan identifikasi aset dan analisis risiko menggunakan metode kualitatif
Sub-CPMK 2.2	Menyusun kebijakan keamanan (Acceptable Use Policy, Password Policy)
Sub-CPMK 3.1	Mengkonfigurasi firewall (iptables) dengan aturan yang sesuai
Sub-CPMK 3.2	Menginstal dan mengkonfigurasi IDS (Snort) untuk mendeteksi serangan
Sub-CPMK 3.3	Mengkonfigurasi VPN server dan client menggunakan OpenVPN
Sub-CPMK 3.4	Menganalisis keamanan jaringan menggunakan tools seperti Wireshark dan Nmap
Sub-CPMK 4.1	Melakukan vulnerability scanning menggunakan tools (Nessus, OWASP ZAP)
Sub-CPMK 4.2	Mengidentifikasi kerentanan OWASP Top 10 pada aplikasi web
Sub-CPMK 4.3	Membuat laporan hasil pengujian keamanan dan rekomendasi perbaikan

6. Tabel Korelasi CPL – CPMK dengan Bobot Kontribusi

CPMK	CPL-2 (50%)	CPL-6 (50%)	Total
CPMK 1	12,5%	12,5%	**25%**
CPMK 2	12,5%	12,5%	**25%**
CPMK 3	12,5%	12,5%	**25%**
CPMK 4	12,5%	12,5%	**25%**
Total	**50%**	**50%**	**100%**

- *Simbol dan angka persen menunjukkan bobot kontribusi langsung setiap CPMK terhadap masing-masing CPL.*
- *Total kontribusi mata kuliah terhadap CPL-2 = 50%, terhadap CPL-6 = 50%.*

7. Tabel Korelasi CPL – Sub-CPMK

Sub-CPMK	CPL-2	CPL-6
Sub-CPMK 1.1	√	√
Sub-CPMK 1.2	√	√
Sub-CPMK 1.3	√	√
Sub-CPMK 2.1	√	√
Sub-CPMK 2.2	√	√
Sub-CPMK 3.1	√	√
Sub-CPMK 3.2	√	√
Sub-CPMK 3.3	√	√
Sub-CPMK 3.4	√	√
Sub-CPMK 4.1	√	√
Sub-CPMK 4.2	√	√
Sub-CPMK 4.3	√	√

8. Daftar Referensi

1. Stallings, W. (2020). Cryptography and Network Security: Principles and Practice (8th ed.). Pearson.

2. Whitman, M. E., & Mattord, H. J. (2021). Principles of Information Security (7th ed.). Cengage Learning.

3. Easttom, C. (2021). Computer Security Fundamentals (5th ed.). Pearson.

4. OWASP Foundation. (2021). OWASP Top Ten - 2021. The Open Web Application Security Project.

5. Messier, R. (2021). Network Security with OpenSSL. O'Reilly Media.

6. Oracle. (2022). MySQL Security Guide. Oracle Corporation.

7. Snort Project. (2023). Snort User Manual. Cisco Systems.

8. OpenVPN. (2023). OpenVPN Documentation. OpenVPN Inc.

9. Bahan Kajian

1. Kriptografi Terapan: enkripsi/dekripsi file dengan OpenSSL/GnuPG, pembuatan key pair, digital signature, hash.

2. Analisis Risiko: identifikasi aset, penilaian risiko, matriks risiko.

3. Kebijakan Keamanan: penyusunan dokumen kebijakan (AUP, Password Policy).

4. Keamanan Jaringan: konfigurasi firewall iptables, instalasi dan konfigurasi Snort IDS, konfigurasi OpenVPN, analisis traffic dengan Wireshark, scanning dengan Nmap.

5. Keamanan Aplikasi: vulnerability scanning dengan Nessus/OWASP ZAP, identifikasi kerentanan OWASP Top 10.

6. Pelaporan: penyusunan laporan hasil pengujian keamanan.

10. Rencana Pembelajaran per Pertemuan

Pert. Ke-	Sub-CPMK	Topik Bahasan	Metode Pembelajaran	Pengalaman Belajar Mahasiswa	Waktu (menit)	Kriteria & Indikator Penilaian	Bobot (%)	CPL
1	[1.1] Menggunakan tools kriptografi (OpenSSL) untuk enkripsi/dekripsi file	Pengenalan OpenSSL, enkripsi simetris (AES) dan asimetris (RSA)	Demonstrasi, praktik mandiri, workshop	Menginstal OpenSSL; melakukan enkripsi dan dekripsi file menggunakan AES; membuat key pair RSA dan melakukan enkripsi/dekripsi	170	Kriteria: keberhasilan enkripsi/dekripsi, ketepatan penggunaan perintah. Indikator: semua file berhasil dienkripsi dan didekripsi, perintah sesuai	**2%**	CPL-2, CPL-6
2	[1.2] Membuat dan memverifikasi digital signature	Digital signature dengan OpenSSL, fungsi hash	Demonstrasi, praktik	Menghitung hash file (SHA-256); membuat digital signature; memverifikasi signature	170	Kriteria: keberhasilan pembuatan dan verifikasi signature. Indikator: signature berhasil dibuat dan diverifikasi, hash konsisten	**2%**	CPL-2, CPL-6
3	[1.3] Mengimplementasikan hash untuk verifikasi integritas	Hash file, verifikasi integritas, studi kasus	Praktik, studi kasus	Menghitung hash file sebelum dan sesudah modifikasi; membandingkan hash untuk deteksi perubahan	170	Kriteria: ketepatan perhitungan hash, kemampuan deteksi perubahan. Indikator: hash berubah setelah modifikasi, laporan analisis lengkap	**2,5%**	CPL-2, CPL-6
4	[2.1] Melakukan identifikasi aset dan analisis risiko	Identifikasi aset, penilaian risiko, matriks risiko	Simulasi, studi kasus, diskusi	Mengidentifikasi aset organisasi fiktif; menilai likelihood dan impact; membuat matriks risiko	170	Kriteria: kelengkapan identifikasi, ketepatan penilaian. Indikator: 10+ aset teridentifikasi, matriks risiko jelas	**2%**	CPL-2, CPL-6
5	[2.2] Menyusun kebijakan keamanan	Struktur kebijakan, Acceptable Use Policy, Password Policy	Workshop, penyusunan dokumen	Menyusun draf kebijakan AUP; menyusun kebijakan password	170	Kriteria: kelengkapan struktur, kejelasan bahasa, kesesuaian standar. Indikator: kebijakan lengkap (tujuan, ruang lingkup, sanksi)	**2%**	CPL-2, CPL-6
6	[3.1] Mengkonfigurasi firewall (iptables)	Dasar iptables, aturan filtering, NAT	Demonstrasi, praktik	Mengkonfigurasi aturan dasar iptables; memblokir port tertentu; mengatur forwarding	170	Kriteria: keberhasilan konfigurasi, aturan bekerja sesuai. Indikator: port yang diblokir tidak dapat diakses, aturan persist	**2%**	CPL-2, CPL-6

Pert. Ke-	Sub-CPMK	Topik Bahasan	Metode Pembelajaran	Pengalaman Belajar Mahasiswa	Waktu (menit)	Kriteria & Indikator Penilaian	Bobot (%)	CPL
7	[3.2] Menginstal dan mengkonfigurasi IDS (Snort)	Instalasi Snort, konfigurasi rules, deteksi serangan	Demonstrasi, praktik	Menginstal Snort; mengkonfigurasi rules sederhana; menguji deteksi serangan (ping, port scan)	170	Kriteria: instalasi berhasil, deteksi serangan tepat. Indikator: Snort berjalan, alert muncul saat serangan	**2,5%**	CPL-2, CPL-6
8	UJIAN TENGAH SEMESTER	Praktikum mencakup pertemuan 1–7	Ujian praktik	Menyelesaikan tugas praktik individu (enkripsi, firewall, Snort)	170	Kriteria: ketepatan dan kecepatan penyelesaian. Indikator: semua tugas selesai dengan benar	**30%**	CPL-2, CPL-6
9	[3.3] Mengkonfigurasi VPN (OpenVPN)	Konsep VPN, instalasi OpenVPN, konfigurasi server-client	Demonstrasi, praktik	Menginstal OpenVPN server; membuat sertifikat; mengkonfigurasi client dan koneksi	170	Kriteria: koneksi VPN berhasil, enkripsi aktif. Indikator: client dapat terhubung, traffic terenkripsi	**2%**	CPL-2, CPL-6
10	[3.4] Menganalisis keamanan jaringan dengan Wireshark dan Nmap	Packet analysis dengan Wireshark, scanning dengan Nmap	Demonstrasi, praktik	Menggunakan Wireshark untuk menganalisis traffic; melakukan port scanning dengan Nmap; mengidentifikasi port terbuka dan layanan	170	Kriteria: kemampuan analisis traffic, ketepatan identifikasi. Indikator: menjelaskan isi packet, mengidentifikasi layanan	**2,5%**	CPL-2, CPL-6
11	[4.1] Melakukan vulnerability scanning dengan Nessus	Instalasi Nessus, konfigurasi scan, analisis hasil	Demonstrasi, praktik	Menginstal Nessus; melakukan basic network scan; menganalisis laporan kerentanan	170	Kriteria: scan berhasil, analisis laporan tepat. Indikator: menjelaskan temuan dan tingkat keparahan	**2%**	CPL-2, CPL-6
12	[4.1] Melakukan vulnerability scanning dengan OWASP ZAP	OWASP ZAP untuk aplikasi web, spider, active scan	Demonstrasi, praktik	Mengkonfigurasi OWASP ZAP; melakukan spidering dan active scan; menganalisis hasil	170	Kriteria: scan berhasil, identifikasi kerentanan tepat. Indikator: menjelaskan temuan dan rekomendasi	**2%**	CPL-2, CPL-6
13	[4.2] Mengidentifikasi kerentanan OWASP Top 10 pada aplikasi web	OWASP Top 10, contoh kerentanan (SQLi, XSS)	Praktik, studi kasus	Menguji aplikasi web rentan (DVWA); mengidentifikasi SQL injection, XSS; mencatat langkah-langkah	170	Kriteria: keberhasilan identifikasi kerentanan. Indikator: menemukan minimal 3 jenis kerentanan	**2%**	CPL-2, CPL-6
14	[4.3] Membuat laporan hasil pengujian	Struktur laporan, rekomendasi perbaikan	Workshop, penyusunan laporan	Menyusun laporan dari hasil scanning dan identifikasi; memberikan rekomendasi	170	Kriteria: kelengkapan laporan, kejelasan rekomendasi. Indikator: laporan mencakup	**2%**	CPL-2, CPL-6

Pert. Ke-	Sub-CPMK	Topik Bahasan	Metode Pembelajaran	Pengalaman Belajar Mahasiswa	Waktu (menit)	Kriteria & Indikator Penilaian	Bobot (%)	CPL
	keamanan			perbaikan		metodologi, temuan, rekomendasi		
15	Review dan integrasi semua praktikum	Simulasi proyek keamanan terintegrasi	Proyek kelompok, presentasi	Mengerjakan proyek keamanan (studi kasus); mempresentasikan hasil	170	Kriteria: kualitas proyek, presentasi, kerja tim. Indikator: proyek lengkap, presentasi jelas	**2%**	CPL-2, CPL-6
16	UJIAN AKHIR SEMESTER	Praktikum mencakup pertemuan 9–15	Ujian praktik	Menyelesaikan tugas praktik komprehensif (VPN, scanning, laporan)	170	Kriteria: ketepatan dan kelengkapan. Indikator: semua tugas selesai dengan benar	**30%**	CPL-2, CPL-6

Total Bobot Penilaian: Tugas per pertemuan (14 pertemuan × 2% atau 2,5%) = 30% + Partisipasi = 10% + UTS = 30% + UAS = 30% → Total = 100%

Ditetapkan di: Padang
Tanggal: 23 Februari 2026

A/n Dosen Pengampu,

Ir. H.A. Mooduto, M.Kom.
NIP. 196605101994031003