RENCANA PEMBELAJARAN SEMESTER (RPS)
PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNOLOGI DAN DESAIN

SPT-I/02/BPP-LSE/POB-01/F-01

Issue/Revisi : R1

Mata Kuliah	*Cyber Security*	Tanggal	04 Agustusi 2025
Kode MK	INF323	Rumpun MK	MKWP
Bobot (sks)	T (Teori) : 2 P (Praktik/Praktikum) :	Semester	5
Dosen Pengembang RPS,  Hendi Hermawan, S.T., M.T.I.	Koordinator Keilmuan,  Mohammad Nasucha, S.T., M.Sc., Ph.D.	Kepala Program Studi,  Dr. Ida Nurhaida, S.T., M.T.	Dekan,  Danto Sukmajati,S.T., M.Sc., Ph.D.

RENCANA PEMBELAJARAN SEMESTER		
Capaian Pembelajaran (CP)	**CPL – PRODI yang dibebankan pada MK**	
	CPL04	Memiliki kompetensi dalam menganalisis (C4) persoalan computing, mengidentifikasi solusinya serta mengelola (C3) proyek teknologi di bidang informatika (bahan kajian) dengan mempertimbangkan perkembangan ilmu transdisiplin.
	CPL05	Menguasai konsep teoritis (C2) dalam bidang Informatika/Ilmu Komputer untuk mendukung perancangan dan pengembangan aplikasi teknologi yang sesuai dengan kebutuhan industri dan masyarakat.
	CPL08	Memiliki kemampuan untuk menentukan (C2) dan mengimplementasikan solusi (C3) berbasis computing yang sesuai dengan kebutuhan pengguna.
	Capaian Pembelajaran Mata Kuliah (CPMK)	

RENCANA PEMBELAJARAN SEMESTER

CPMK041	Mampu menganalisis(C4) persoalan computing serta mengidentifikasi solusi setidaknya secara konseptual.
CPMK051	Mampu menguasai konsep teoritis (C2) dalam bidang Informatika/Ilmu Komputer untuk mendukung perancangan aplikasi teknologi yang sesuai dengan kebutuhan industri dan masyarakat.
CPMK083	Mampu mengimplementasikan solusi berbasis computing yang sesuai dengan kebutuhan pengguna (C3)
Kemampuan Akhir Tiap Tahap Belajar (SCPMK)	
SCPMK0419	Mampu menganalisis persoalan computing serta mengidentifikasi solusi setidaknya secara konseptual **yang terkait dengan keamanan siber.**
SCPMK0519	Mampu menguasai konsep teoritis dalam bidang Informatika/Ilmu Komputer untuk mendukung perancangan aplikasi teknologi yang sesuai dengan kebutuhan industri dan masyarakat **yang terkait dengan keamanan siber.**
SCPMK0835	Mampu mengimplementasikan metode/algoritma yang sesuai dengan kebutuhan computing pengguna **yang terkait dengan keamanan siber.**
Korelasi CPMK terhadap SCPMK	

	SCPMK0419	SCPMK0519	SCPMK0835
CPMK041	√		
CPMK051		√	
CPMK083			√

Kode CPL	Kode CPMK	Kode SCPMK	Indikator	Metode Penilaian	Bobot
CPL04	CPMK041	SCPMK0419	Mampu menganalisis persoalan computing serta mengidentifikasi solusi setidaknya secara konseptual yang terkait dengan keamanan siber.	Kuis / Diskusi, Praktikum, UTS	20%

Universitas Pembangunan Jaya	**RENCANA PEMBELAJARAN SEMESTER (RPS)** **PROGRAM STUDI INFORMATIKA** **FAKULTAS TEKNOLOGI DAN DESAIN**	**SPT-I/02/BPP-LSE/POB-01/F-01** Issue/Revisi : R1

RENCANA PEMBELAJARAN SEMESTER

CPL05	CPMK051	SCPMK0519	Mampu menguasai konsep teoritis dalam bidang Informatika/Ilmu Komputer untuk mendukung perancangan aplikasi teknologi yang sesuai dengan kebutuhan industri dan masyarakat yang terkait dengan keamanan siber.	Kuis, Praktikum,Laporan Studi Kasus, UTS	40%
CPL08	CPMK083	SCPMK0835	Mampu mengimplementasikan metode/algoritma yang sesuai dengan kebutuhan computing pengguna yang terkait dengan keamanan siber.	Proyek akhir, UAS	40%

Deskripsi Singkat MK	Mata kuliah ini memfasilitasi mahasiswa dalam dasar-dasar jaringan komputer yang mencakup topologi, media transmisi, model referensi OSI dan TCP/IP, perangkat jaringan, pengalamatan IP, hingga konfigurasi dasar perangkat jaringan menggunakan Cisco IOS. Mahasiswa juga akan dikenalkan pada simulasi menggunakan Cisco Packet Tracer serta keterampilan pemecahan masalah jaringan.
Bahan Kajian : Materi Pembelajaran/Pokok Bahasan	1. Pengantar ancaman, kerentanan, dan serangan siber 2. Serangan umum: rekayasa sosial, serangan aplikasi, serangan nirkabel dan perangkat mobile 3. Prinsip dasar keamanan jaringan 4. Pengantar Cisco IOS dan konfigurasi dasar perangkat jaringan 5. Kerentanan TCP/IP dan analisis struktur header IP, TCP, dan UDP 6. Serangan berbasis layanan IP dan aplikasi jaringan 7. Langkah mitigasi terhadap serangan jaringan 8. Perangkat dan ancaman jaringan nirkabel serta penanganannya 9. Infrastruktur keamanan jaringan dan penerapan Zone-Based Policy Firewall 10. Sistem Operasi Windows: arsitektur, konfigurasi, monitoring, dan keamanan 11. Sistem Operasi Linux: dasar CLI, manajemen file, permission, log, dan deteksi malware 12. Perlindungan sistem dan endpoint: antimalware, HIPS, dan keamanan aplikasi 13. Prinsip CIA, states of data, dan metode countermeasure dalam cybersecurity 14. Studi kasus insiden nyata, investigasi insiden, response plan, lesson learned
Pustaka	**Utama**
	Cisco Networking Academy. (2023). *Endpoint Security - Scope and Sequence v1.0*. Cisco. https://www.netacad.com/courses/endpoint-security
	Pendukung

RENCANA PEMBELAJARAN SEMESTER

<table>
<tr><td></td><td colspan="2">Ciampa, M. (2022). CompTIA Security+ Guide to Network Security Fundamentals (7th ed.). Cengage Learning.</td></tr>
<tr><td rowspan="2">Media Pembelajaran</td><td>Perangkat Lunak:</td><td>Perangkat Keras:</td></tr>
<tr><td>Cisco Packet Tracer, Wireshark, PowerPoint, Collabor / LMS</td><td>Desktop PC / Laptop, Internet, LCD Projector, Cisco Router & Switch</td></tr>
<tr><td>Dosen Pengampu</td><td colspan="2">Hendi Hermawan, S.T., M.T.I.</td></tr>
<tr><td>Mata Kuliah Prasyarat</td><td colspan="2"></td></tr>
<tr><td>Indikator, Kriteria, dan Bobot Penilaian</td><td colspan="2">
<table>
<tr><td rowspan="2">SCPMK</td><td colspan="5">Penilaian dan Bobot</td><td rowspan="2">Total Bobot Penilaian</td></tr>
<tr><td>Diskusi</td><td>UTS</td><td>Praktikum</td><td>Studi Kasus</td><td>Proyek Akhir / UAS</td></tr>
<tr><td>SCPMK0411</td><td>3.3%</td><td>10%</td><td>-</td><td>-</td><td>-</td><td>20.3%</td></tr>
<tr><td>SCPMK0511</td><td>3.3%</td><td>10%</td><td>15%</td><td>15%</td><td>-</td><td>40.3%</td></tr>
<tr><td>SCPMK0831</td><td>3.4%</td><td>-</td><td>-</td><td>-</td><td>40%</td><td>40.4%</td></tr>
<tr><td>Total per penilaian</td><td>10%</td><td>20%</td><td>15%</td><td>15%</td><td>40%</td><td>100%</td></tr>
</table>
</td></tr>
</table>

Minggu ke-	Sub CP-MK (Kemampuan Akhir yang Diharapkan)	Penilaian		Bentuk Pembelajaran: Metode Pembelajaran; Penugasan Mahasiswa (Estimasi Waktu)		Materi Pembelajaran (Pustaka)	Bobot Penilaian (%)
		Indikator	Kriteria & Bentuk Penilaian				
(1)	*(2)*	*(3)*	*(4)*	*Luring (5)*	*Daring (6)*	*(7)*	
1	**SCPMK0511** Mampu menguasai konsep teoritis dalam bidang Informatika/Ilmu	Mahasiswa mampu menjelaskan konsep ancaman, kerentanan,	**Kriteria penilaian:** Ketepatan konsep dan penggunaan istilah	**Bentuk pembelajaran:** Tatap muka di kelas	-	Pengantar ancaman, kerentanan, dan serangan siber	2.9%

Minggu ke-	Sub CP-MK (Kemampuan Akhir yang Diharapkan)	Penilaian		Bentuk Pembelajaran: Metode Pembelajaran; Penugasan Mahasiswa (Estimasi Waktu)		Materi Pembelajaran (Pustaka)	Bobot Penilaian (%)
		Indikator	Kriteria & Bentuk Penilaian				
(1)	*(2)*	*(3)*	*(4)*	*Luring (5)*	*Daring (6)*	*(7)*	
	Komputer untuk mendukung perancangan aplikasi teknologi yang sesuai dengan kebutuhan industri dan masyarakat yang terkait dengan keamanan siber.	dan jenis-jenis serangan siber.	dalam diskusi serta jawaban tertulis. **Bentuk penilaian:** diskusi	**Metode pembelajaran:** Ceramah Partisipasi (kemampuan literasi) **Estimasi waktu:** TM = 3 x 50' BM = 3 x 60' BS = 3 x 60'			
2	**SCPMK0411** Mampu menganalisis persoalan computing serta mengidentifikasi solusi setidaknya secara konseptual yang terkait dengan keamanan siber.	Mahasiswa mampu mengidentifikasi jenis serangan umum seperti rekayasa sosial, serangan aplikasi, serta serangan nirkabel dan perangkat mobile.	**Kriteria penilaian:** Ketepatan klasifikasi serangan dan pemahaman vektor ancaman **Bentuk penilaian:** diskusi	**Bentuk pembelajaran:** Tatap muka di kelas **Metode pembelajaran:** Studi kasus, demonstrasi, pemutaran video, diskusi kelompok **Estimasi waktu:** TM = 3 × 50' BM = 3 × 60' BS = 3 × 60'	-	Serangan umum: rekayasa sosial, serangan aplikasi, serangan nirkabel dan perangkat mobile	2.9%
3	**SCPMK0511** Mampu menguasai konsep teoritis dalam bidang Informatika/Ilmu	Mahasiswa mampu menjelaskan prinsip dasar keamanan	**Kriteria penilaian:** Ketepatan pemahaman konsep	**Bentuk pembelajaran:**	-	Prinsip dasar keamanan jaringan (CIA,	2.9%

Minggu ke-	Sub CP-MK (Kemampuan Akhir yang Diharapkan)	Penilaian		Bentuk Pembelajaran: Metode Pembelajaran; Penugasan Mahasiswa (Estimasi Waktu)		Materi Pembelajaran (Pustaka)	Bobot Penilaian (%)
		Indikator	Kriteria & Bentuk Penilaian				
(1)	*(2)*	*(3)*	*(4)*	*Luring (5)*	*Daring (6)*	*(7)*	
	Komputer untuk mendukung perancangan aplikasi teknologi yang sesuai dengan kebutuhan industri dan masyarakat yang terkait dengan keamanan siber.	jaringan dan hubungannya dengan ancaman siber.	dan argumentasi logis **Bentuk penilaian:** diskusi, refleksi kelompok	Tatap muka di kelas **Metode pembelajaran:** Ceramah interaktif, presentasi kelompok, diskusi kasus **Estimasi waktu:** TM = 3 × 50' BM = 3 × 60' BS = 3 × 60'		defense in depth, least privilege, access control)	
4	**SCPMK0831** Mampu mengimplementasikan metode/algoritma yang sesuai dengan kebutuhan computing pengguna yang terkait dengan keamanan siber.	Mahasiswa mampu mengoperasikan Cisco IOS dan melakukan konfigurasi dasar perangkat jaringan.	**Kriteria penilaian:** Ketepatan konfigurasi dan penguasaan dasar perintah CLI **Bentuk penilaian:** studi kasus		**Bentuk pembelajaran:** Ceramah dan simulasi lab **Metode pembelajaran:** Daring sinkron dan asinkron Media: Video tutorial,	Pengantar Cisco IOS, konfigurasi dasar (hostname, IP, password), CLI dasar	2.9%

Minggu ke-	Sub CP-MK (Kemampuan Akhir yang Diharapkan)	Penilaian		Bentuk Pembelajaran: Metode Pembelajaran; Penugasan Mahasiswa (Estimasi Waktu)		Materi Pembelajaran (Pustaka)	Bobot Penilaian (%)
		Indikator	Kriteria & Bentuk Penilaian				
(1)	*(2)*	*(3)*	*(4)*	*Luring (5)*	*Daring (6)*	*(7)*	
					simulasi Packet Tracer Penugasan melalui LMS Estimasi waktu: TM = 3 × 50’ BM = 3 × 60’ BS = 3 × 60’		
5	**SCPMK0411** Mampu menganalisis persoalan computing serta mengidentifikasi solusi setidaknya secara konseptual yang terkait dengan keamanan siber.	Mahasiswa mampu menganalisis struktur header IP, TCP, dan UDP serta menjelaskan kerentanannya terhadap serangan.	**Kriteria penilaian:** Analisis tepat terhadap struktur dan kerentanan protokol **Bentuk penilaian:** diskusi	**Bentuk pembelajaran:** Tatap muka **Metode pembelajaran:** Ceramah interaktif, presentasi kelompok, diskusi kasus **Estimasi waktu:** TM = 3 × 50’ BM = 3 × 60’ BS = 3 × 60’	-	Struktur dan kerentanan header IP, TCP, UDP; sniffing, spoofing, session hijacking	2.9%

Minggu ke-	Sub CP-MK (Kemampuan Akhir yang Diharapkan)	Penilaian		Bentuk Pembelajaran: Metode Pembelajaran; Penugasan Mahasiswa (Estimasi Waktu)		Materi Pembelajaran (Pustaka)	Bobot Penilaian (%)
		Indikator	Kriteria & Bentuk Penilaian				
(1)	*(2)*	*(3)*	*(4)*	*Luring (5)*	*Daring (6)*	*(7)*	
6	**SCPMK0411** Mampu menganalisis persoalan computing serta mengidentifikasi solusi setidaknya secara konseptual yang terkait dengan keamanan siber.	Mahasiswa mampu menjelaskan bentuk serangan berbasis layanan jaringan dan aplikasi serta mengusulkan mitigasinya.	**Kriteria penilaian:** Kemampuan menganalisis kerentanan layanan dan solusi mitigasi yang logis. **Bentuk penilaian:** diskusi	**Bentuk pembelajaran:** Tatap muka **Metode pembelajaran:** Diskusi **Estimasi waktu:** TM = 3 × 50' BM = 3 × 60' BS = 3 × 60'	-	Layanan IP (DNS, DHCP, FTP), serangan berbasis aplikasi (SQLi, XSS), DoS, mitigasi dasar	2.9%
7	**SCPMK0411** Mampu menganalisis persoalan computing serta mengidentifikasi solusi setidaknya secara konseptual yang terkait dengan keamanan siber.	Mahasiswa mampu mengidentifikasi dan merancang langkah mitigasi terhadap berbagai jenis serangan jaringan.	**Kriteria penilaian:** Analisis tepat terhadap struktur dan kerentanan protokol. **Bentuk penilaian:** diskusi	**Bentuk pembelajaran:** Ceramah **Metode pembelajaran:** Analisis skenario, diskusi kelompok, visualisasi alur mitigasi **Estimasi waktu:** TM = 3 × 50'	-	Langkah mitigasi serangan jaringan: firewall, ACL, IDS/IPS dasar	2.9%

Minggu ke-	Sub CP-MK (Kemampuan Akhir yang Diharapkan)	Penilaian		Bentuk Pembelajaran: Metode Pembelajaran; Penugasan Mahasiswa (Estimasi Waktu)		Materi Pembelajaran (Pustaka)	Bobot Penilaian (%)
		Indikator	Kriteria & Bentuk Penilaian				
(1)	*(2)*	*(3)*	*(4)*	*Luring (5)*	*Daring (6)*	*(7)*	
				BM = 3 × 60' BS = 3 × 60'			
8	**Evaluasi Tengah Semester : Melakukan validasi hasil penilaian, evaluasi dan perbaikan proses pembelajaran berikutnya (20%)**						
9	**SCPMK0411** Mampu menganalisis persoalan computing serta mengidentifikasi solusi setidaknya secara konseptual yang terkait dengan keamanan siber.	Mahasiswa mampu mengidentifikasi ancaman pada jaringan nirkabel serta menentukan solusi penanganan yang sesuai.	**Kriteria penilaian:** Ketepatan klasifikasi ancaman dan relevansi solusi yang diajukan **Bentuk penilaian:** diskusi	**Bentuk pembelajaran:** Tatap muka **Metode pembelajaran:** Diskusi **Estimasi waktu:** TM = 3 × 50' BM = 3 × 60' BS = 3 × 60'	-	Ancaman WLAN, penanganan serangan wireless, keamanan Wi-Fi dasar	2.9%
10	**SCPMK0831** Mampu mengimplementasikan metode/algoritma yang sesuai dengan kebutuhan computing pengguna yang terkait dengan keamanan siber.	Mahasiswa mampu mengimplementasikan Zone-Based Policy Firewall serta memahami fungsi dan kegunaan perangkat serta layanan keamanan jaringan.	**Kriteria penilaian:** Keakuratan konfigurasi dan kelengkapan sistem keamanan yang diterapkan **Bentuk penilaian:** Praktikum	**Bentuk pembelajaran:** Praktikum **Metode pembelajaran:** Simulasi lab **Estimasi waktu:** TM = 3 × 50'	-	ZBPF, IDS/IPS, UTM, VPN, fungsi perangkat dan layanan keamanan jaringan	2.9%

Minggu ke-	Sub CP-MK (Kemampuan Akhir yang Diharapkan)	Penilaian		Bentuk Pembelajaran: Metode Pembelajaran; Penugasan Mahasiswa (Estimasi Waktu)		Materi Pembelajaran (Pustaka)	Bobot Penilaian (%)
		Indikator	Kriteria & Bentuk Penilaian				
(1)	*(2)*	*(3)*	*(4)*	*Luring (5)*	*Daring (6)*	*(7)*	
				BM = 3 × 60' BS = 3 × 60'			
11	**SCPMK0511** Mampu menguasai konsep teoritis dalam bidang Informatika/Ilmu Komputer untuk mendukung perancangan aplikasi teknologi yang sesuai dengan kebutuhan industri dan masyarakat yang terkait dengan keamanan siber.	Mahasiswa mampu menjelaskan arsitektur sistem operasi Windows serta menerapkan konfigurasi dan monitoring keamanan sistem.	**Kriteria penilaian:** Ketepatan pemahaman arsitektur dan hasil konfigurasi/monitoring **Bentuk penilaian:** diskusi	**Bentuk pembelajaran:** Diskusi **Metode pembelajaran:** Praktikum lab, observasi konfigurasi sistem Windows, demonstrasi tools admin **Estimasi waktu:** TM = 3 × 50' BM = 3 × 60' BS = 3 × 60'	-	Windows OS architecture, Windows tools (Task Manager, Event Viewer, MMC), pengamanan dasar sistem	2.9%
12	**SCPMK0831** Mampu mengimplementasikan metode/algoritma yang sesuai dengan kebutuhan computing pengguna yang terkait dengan keamanan siber.	Mahasiswa mampu menggunakan sistem operasi Linux untuk konfigurasi sistem dasar, pengelolaan file, dan deteksi malware.	**Kriteria penilaian:** Ketepatan penggunaan perintah Linux dan hasil pengamatan sistem		**Bentuk pembelajaran:** Ceramah dan simulasi lab **Metode**	Dasar-dasar CLI Linux, struktur file system, permission, top, ps, netstat,	2.9%

Minggu ke-	Sub CP-MK (Kemampuan Akhir yang Diharapkan)	Penilaian		Bentuk Pembelajaran: Metode Pembelajaran; Penugasan Mahasiswa (Estimasi Waktu)		Materi Pembelajaran (Pustaka)	Bobot Penilaian (%)
		Indikator	Kriteria & Bentuk Penilaian				
(1)	*(2)*	*(3)*	*(4)*	*Luring (5)*	*Daring (6)*	*(7)*	
			Bentuk penilaian: studi kasus		**pembelajaran:** Daring sinkron dan asinkron Media: Video tutorial, simulasi Packet Tracer Penugasan melalui LMS Estimasi waktu: TM = 3 × 50' BM = 3 × 60' BS = 3 × 60'	malware scanning tools	
13	**SCPMK0831** Mampu mengimplementasikan metode/algoritma yang sesuai dengan kebutuhan computing pengguna yang terkait dengan keamanan siber.	Mahasiswa mampu menerapkan perlindungan sistem dan endpoint menggunakan teknik antimalware, HIPS, dan pengamanan aplikasi.	**Kriteria penilaian:** Ketepatan identifikasi ancaman dan konfigurasi mitigasi. **Bentuk penilaian:** Praktikum	**Bentuk pembelajaran:** Efektivitas konfigurasi perlindungan dan ketepatan penggunaan tools **Metode pembelajaran:**	-	Antimalware, endpoint protection, Host-based IPS, sandboxing, application control	2.9%

Minggu ke-	Sub CP-MK (Kemampuan Akhir yang Diharapkan)	Penilaian		Bentuk Pembelajaran: Metode Pembelajaran; Penugasan Mahasiswa (Estimasi Waktu)		Materi Pembelajaran (Pustaka)	Bobot Penilaian (%)
		Indikator	Kriteria & Bentuk Penilaian				
(1)	*(2)*	*(3)*	*(4)*	*Luring (5)*	*Daring (6)*	*(7)*	
				Simulasi deteksi malware, konfigurasi endpoint security, uji aplikasi monitoring **Estimasi waktu:** TM = 3 × 50' BM = 3 × 60' BS = 3 × 60'			
14	**SCPMK0411** Mampu menganalisis persoalan computing serta mengidentifikasi solusi setidaknya secara konseptual yang terkait dengan keamanan siber.	Mahasiswa mampu menganalisis dan mempresentasikan simulasi insiden keamanan berdasarkan studi kasus.	**Kriteria penilaian:** Ketepatan penggambaran prinsip dan penerapan countermeasure dalam skenario **Bentuk penilaian:** Proyek akhir tahap 1	**Bentuk pembelajaran:** Simulasi topologi tim **Metode pembelajaran:** Kerja kelompok **Estimasi waktu:** TM = 3 × 50' BM = 3 × 60' BS = 3 × 60'	-	Studi kasus insiden nyata, investigasi insiden, response plan, lesson learned	2.9%

Minggu ke-	Sub CP-MK (Kemampuan Akhir yang Diharapkan)	Penilaian		Bentuk Pembelajaran: Metode Pembelajaran; Penugasan Mahasiswa (Estimasi Waktu)		Materi Pembelajaran (Pustaka)	Bobot Penilaian (%)
		Indikator	Kriteria & Bentuk Penilaian				
(1)	*(2)*	*(3)*	*(4)*	*Luring (5)*	*Daring (6)*	*(7)*	
15	**SCPMK0411** Mampu menganalisis persoalan computing serta mengidentifikasi solusi setidaknya secara konseptual yang terkait dengan keamanan siber.	Mahasiswa mampu menganalisis dan mempresentasikan simulasi insiden keamanan berdasarkan studi kasus.	**Kriteria penilaian:** Ketepatan penggunaan metode troubleshooting. **Bentuk penilaian:** Proyek akhir tahap 2	**Bentuk pembelajaran:** Simulasi topologi tim **Metode pembelajaran:** Kerja kelompok **Estimasi waktu:** TM = 3 × 50’ BM = 3 × 60’ BS = 3 × 60’	-	Studi kasus insiden nyata, investigasi insiden, response plan, lesson learned	2.9%
16	**Evaluasi Akhir Semester: Melakukan validasi penilaian akhir dan menentukan kelulusan mahasiswa (40%)**						