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

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

Issue/Revisi : R2

Mata Kuliah	Ethical Hacking	Tanggal	26 Agustus 2025
Kode MK	INF318	Rumpun MK	MKWP
Bobot (sks)	T (Teori) : 2 P (Praktik/Praktikum) : 1	Semester	6
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**	
	CPL01	Memperhatikan (A1) dan menghargai (A3) prinsip-prinsip ketakwaan kepada Tuhan Yang Maha Esa, prinsip-prinsip ketaatan terhadap hukum, dan prinsip-prinsip kedisiplin dalam kehidupan bermasyarakat dan bernegara.
	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.
	Capaian Pembelajaran Mata Kuliah (CPMK)	
	CPMK012	Memperhatikan (A1) dan menghargai (A3) prinsip-prinsip ketaatan terhadap hukum.

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.
Kemampuan Akhir Tiap Tahap Belajar (SCPMK)	
SCPMK0124	Mampu memahami prinsip-prinsip ketaatan terhadap hukum **yang terkait dengan peretasan etis dan pengujian keamanan siber.**
SCPMK0419	Mampu menganalisis persoalan computing serta mengidentifikasi solusi setidaknya secara konseptual **yang terkait dengan peretasan etis dan pengujian 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 peretasan etis dan pengujian keamanan siber.**
Korelasi CPMK terhadap SCPMK	

	SCPMK0124	SCPMK0419	SCPMK0519
CPMK012	√		
CPMK041		√	
CPMK051			√

Kode CPL	Kode CPMK	Kode SCPMK	Indikator	Metode Penilaian	Bobot
CPL01	CPMK012	SCPMK0124	Mampu memahami prinsip-prinsip ketaatan terhadap hukum **yang terkait dengan peretasan etis dan pengujian keamanan siber.**	Diskusi, Praktikum, UTS	20%
CPL04	CPMK041	SCPMK0419	Mampu menganalisis persoalan computing serta mengidentifikasi solusi setidaknya secara konseptual **yang terkait dengan peretasan etis dan pengujian keamanan siber.**	Praktikum,Laporan Studi Kasus, UTS	40%

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 : R2

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 peretasan etis dan pengujian keamanan siber.**	Proyek akhir, UAS	40%	

Deskripsi Singkat MK	Mata kuliah ini memfasilitasi mahasiswa dalam keterampilan untuk mengidentifikasi secara proaktif berbagai kerentanan sebelum ditemukan oleh penjahat siber. Mahasiswa akan terampil dalam menentukan ruang lingkup, melaksanakan, dan membuat laporan asesmen kerentanan serta merekomendasikan strategi mitigasi melalui praktik nyata yang berbasis narasi gamifikasi.	
Bahan Kajian : Materi Pembelajaran/Pokok Bahasan	1. Pengantar Ethical Hacking dan Penetration Testing 2. Perencanaan dan Penentuan Cakupan Penetration Testing 3. Pengumpulan Informasi dan Pemindaian Kerentanan 4. Serangan Social Engineering 5. Eksploitasi Jaringan Kabel dan Nirkabel 6. Eksploitasi Kerentanan Berbasis Aplikasi 7. Keamanan Cloud, Mobile, dan IoT 8. Teknik Pasca-Eksploitasi 9. Pelaporan dan Komunikasi 10. Analisis Alat dan Kode	
Pustaka	**Utama**	
	Cisco (2024). Ethical Hacker v1.0 Course Overview and Scope and Sequence. Cisco NetAcad.	
	Pendukung	
	Matt Walker (2023). CEH Certified Ethical Hacker Study Guide, 4th Edition. McGraw Hill.	
Media Pembelajaran	**Perangkat Lunak:**	**Perangkat Keras:**
	Oracle VirtualBox, Linux, Web Browser	Desktop PC / Laptop, Internet, LCD Projector,

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

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

Issue/Revisi : R2

RENCANA PEMBELAJARAN SEMESTER	
Dosen Pengampu	Hendi Hermawan, S.T., M.T.I.
Mata Kuliah Prasyarat	
Indikator, Kriteria, dan Bobot Penilaian	

Komponen Penilaian	Bobot
Partisipasi diskusi kelas (*case method*) – aspek afektif	-
Presentasi Akhir (*problem/project based learning*) – aspek psikomotorik	50%
Tugas - aspek kognitif	10%
Kuis - aspek kognitif	-
Ujian tertulis (UTS / UAS) - aspek kognitif	40%

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	**SCPMK0121** Mampu memahami prinsip-prinsip ketaatan terhadap hukum yang terkait dengan peretasan etis dan pengujian keamanan siber.	Menjelaskan konsep dasar ethical hacking serta prinsip hukum terkait.	**Kriteria penilaian:** Ketepatan dan pemahaman materi **Bentuk penilaian:** diskusi	**Bentuk pembelajaran:** Tatap muka di kelas **Metode pembelajaran:** Ceramah Partisipasi (kemampuan literasi) **Estimasi waktu:** TM = 3 x 50’	-	Pengantar Ethical Hacking dan Penetration Testing	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 x 60' BS = 3 x 60'			
2	**SCPMK0121** Mampu memahami prinsip-prinsip ketaatan terhadap hukum yang terkait dengan peretasan etis dan pengujian keamanan siber.	Menjelaskan pentingnya perencanaan dalam penetration testing	**Kriteria penilaian:** Ketepatan dan pemahaman materi **Bentuk penilaian:** diskusi	**Bentuk pembelajaran:** Tatap muka di kelas **Metode pembelajaran:** Ceramah interaktif, diskusi kasus **Estimasi waktu:** TM = 3 × 50' BM = 3 × 60' BS = 3 × 60'	-	Perencanaan dan Penentuan Cakupan Penetration Testing	2.9%
3	**SCPMK0411** Mampu menganalisis persoalan computing serta mengidentifikasi solusi setidaknya secara konseptual yang terkait dengan peretasan etis dan pengujian keamanan siber.	Mengidentifikasi informasi awal, pemetaan risiko, serta merancang cakupan penetration test	**Kriteria penilaian:** Ketepatan dan pemahaman materi **Bentuk penilaian:** diskusi, praktikum	**Bentuk pembelajaran:** Tatap muka di kelas **Metode pembelajaran:** Ceramah interaktif, presentasi kelompok, diskusi kasus	-	Perencanaan dan Penentuan Cakupan Penetration Testing	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)*	
				Estimasi waktu: TM = 3 × 50' BM = 3 × 60' BS = 3 × 60'			
4	**SCPMK0411** Mampu menganalisis persoalan computing serta mengidentifikasi solusi setidaknya secara konseptual yang terkait dengan peretasan etis dan pengujian keamanan siber.	Melakukan pengumpulan informasi dan pemetaan profil target secara pasif dan aktif	**Kriteria penilaian:** Ketepatan dan pemahaman materi **Bentuk penilaian:** studi kasus		**Bentuk pembelajaran:** Ceramah dan simulasi lab **Metode pembelajaran:** Daring sinkron dan asinkron Media: Video tutorial, simulasi Packet Tracer Penugasan melalui LMS Estimasi waktu: TM = 3 × 50'	Pengumpulan Informasi dan Pemindaian Kerentanan	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'		
5	**SCPMK0411** Mampu menganalisis persoalan computing serta mengidentifikasi solusi setidaknya secara konseptual yang terkait dengan peretasan etis dan pengujian keamanan siber.	Melakukan pemindaian kerentanan serta menganalisis hasil scan	**Kriteria penilaian:** Ketepatan dan pemahaman materi **Bentuk penilaian:** studi kasus	**Bentuk pembelajaran:** Tatap muka **Metode pembelajaran:** Ceramah interaktif, presentasi kelompok, diskusi kasus **Estimasi waktu:** TM = 3 × 50' BM = 3 × 60' BS = 3 × 60'	-	Pengumpulan Informasi dan Pemindaian Kerentanan	2.9%
6	**SCPMK0411** Mampu menganalisis persoalan computing serta mengidentifikasi solusi setidaknya secara konseptual yang terkait dengan peretasan etis dan pengujian keamanan siber.	Menganalisis kerentanan social engineering serta menyusun mitigasinya.	**Kriteria penilaian:** Ketepatan dan pemahaman materi **Bentuk penilaian:** diskusi	**Bentuk pembelajaran:** Tatap muka **Metode pembelajaran:** Diskusi **Estimasi waktu:**	-	Serangan Social Engineering	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)*	
				TM = 3 × 50' BM = 3 × 60' BS = 3 × 60'			
7	**SCPMK0411** Mampu menganalisis persoalan computing serta mengidentifikasi solusi setidaknya secara konseptual yang terkait dengan peretasan etis dan pengujian keamanan siber.	Mahasiswa mampu melakukan eksploitasi pada jaringan kabel dan nirkabel serta memahami metode pertahanannya	**Kriteria penilaian:** Ketepatan dan pemahaman materi **Bentuk penilaian:** diskusi dan praktikum	**Bentuk pembelajaran:** Ceramah **Metode pembelajaran:** diskusi **Estimasi waktu:** TM = 3 × 50' BM = 3 × 60' BS = 3 × 60'	-	Eksploitasi Jaringan Kabel dan Nirkabel	2.9%
8	**Evaluasi Tengah Semester : Melakukan validasi hasil penilaian, evaluasi dan perbaikan proses pembelajaran berikutnya (20%)**						
9	**SCPMK0511** Mampu menguasai konsep teoritis dalam bidang Informatika/Ilmu Komputer untuk mendukung perancangan aplikasi teknologi yang sesuai dengan kebutuhan industri dan masyarakat yang	Menjelaskan prinsip keamanan pada cloud computing, perangkat mobile, dan IoT	**Kriteria penilaian:** Ketepatan dan pemahaman materi **Bentuk penilaian:** diskusi dan praktikum	**Bentuk pembelajaran:** Tatap muka **Metode pembelajaran:** Diskusi dan praktikum	-	Keamanan Cloud, Mobile, dan IoT	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)*	
	terkait dengan peretasan etis dan pengujian keamanan siber.			**Estimasi waktu:** TM = 3 × 50' BM = 3 × 60' BS = 3 × 60'			
10	**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 peretasan etis dan pengujian keamanan siber.	Menjelaskan teknik-teknik pasca eksploitasi, mempertahankan akses, serta gerakan lateral	**Kriteria penilaian:** Ketepatan dan pemahaman materi **Bentuk penilaian:** diskusi dan praktikum	**Bentuk pembelajaran:** Tatap muka **Metode pembelajaran:** Diskusi dan praktikum **Estimasi waktu:** TM = 3 × 50' BM = 3 × 60' BS = 3 × 60'	-	Teknik Pasca-Eksploitasi	2.9%
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.	Menyusun laporan hasil penetration test, memberikan rekomendasi mitigasi dan komunikasi hasil secara efektif	**Kriteria penilaian:** Ketepatan dan pemahaman materi **Bentuk penilaian:** diskusi dan praktikum	**Bentuk pembelajaran:** Tatap muka **Metode pembelajaran:** Diskusi dan praktikum	-	Pelaporan dan Komunikasi	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)*	
				Estimasi waktu: TM = 3 × 50' BM = 3 × 60' BS = 3 × 60'			
12	**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 peretasan etis dan pengujian keamanan siber.	Mengidentifikasi dan menganalisis alat penetration testing berdasarkan fungsinya, serta menganalisis kode eksploitasi secara teoritis	**Kriteria penilaian:** Ketepatan dan pemahaman **Bentuk penilaian:** studi kasus		**Bentuk pembelajaran:** Ceramah dan simulasi lab **Metode 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'	Dasar-dasar CLI Linux, struktur file system, permission, top, ps, netstat, malware scanning tools	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)*	
13-15	**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 peretasan etis dan pengujian keamanan siber.	Mengembangkan proyek akhir ethical hacking secara terintegrasi dengan konsep-konsep yang telah dipelajari sebelumnya	**Kriteria penilaian:** Ketepatan dan pemahaman **Bentuk penilaian:** Proyek akhir	**Bentuk pembelajaran:** Tatap muka **Metode pembelajaran:** diskusi, praktikum **Estimasi waktu:** TM = 3 × 50’ BM = 3 × 60’ BS = 3 × 60’	-	Proyek akhir Integrasi seluruh materi	8.7%
16	**Evaluasi Akhir Semester: Melakukan validasi penilaian akhir dan menentukan kelulusan mahasiswa (40%)**						