RENCANA PEMBELAJARAN SEMESTER
PROGRAM STUDI INFORMATIKA

Issue/Revisi	: R0	Tanggal	: 22 Januari 2020
Mata Kuliah	: Sistem Keamanan Jaringan Komputer	Kode MK	: INF504
Rumpun MK	: MKMI	Semester	: 6
Dosen Pengampu	: Hendi Hermawan, S.T., M.T.I.	Bobot (sks)	: 3 sks

Dosen Pengampu	Kaprodi	Dekan
Hendi Hermawan, S.T., M.T.I.	Safitri Jaya, S.Kom, M.T.I.	Ir. Resdiansyah, S.T, M.T., Ph.D

RENCANA PEMBELAJARAN SEMESTER		
Capaian Pembelajaran (CP)	**CPL - PRODI**	
	1	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.
	2	Mampu mengambil keputusan secara tepat dalam konteks penyelesaian masalah di bidang keahliannya, berdasarkan hasil analisis informasi dan data.
	3	Menunjukkan sikap bertanggungjawab atas pekerjaan di bidang keahliannya secara mandiri.
	4	Menguasai pengetahuan mengenai jaringan komputer secara umum maupun jaringan komputer beserta mekanisme protokol komunikasinya.
	CP-MK	
	1	Mampu memahami dasar-dasar agar dapat online secara aman.
	2	Mampu memahami berbagai jenis malware dan serangannya, dan bagaimana organisasi melindungi diri terhadap serangan ini.
	3	Mampu mengeksplorasi pilihan berkarir di bidang keamanan siber.
	4	Mampu menjelaskan prinsip-prinsip confidentiality, integrity,

RENCANA PEMBELAJARAN SEMESTER		
		dan availability yang terkait dengan status data dan penanggulangan keamanan siber.
	5	Mampu menjelaskan taktik, Teknik, dan prosedur yang digunakan oleh penjahat siber.
	6	Mampu menjelaskan bagaimana teknologi, produk, dan prosedur dapat digunakan untuk melindungi kerahasiaan / confidentiality, integritas / integrity, dan memberikan ketersediaan tinggi / high availability.
	7	Mampu menjelaskan bagaimana para professional keamanan siber menggunakan teknologi, proses, dan prosedur untuk mempertahankan semmua komponen jaringan.
	8	Mampu menjelaskan tujuan hokum yang terkait dengan keamanan siber.
Deskripsi Singkat MK	Mata kuliah ini dirancang agar mahasiswa dapat mempertimbangkan berkarir dengan spesialisasi keamanan siber. Kuliah ini akan mengeksplorasi cara-cara agar dapat online secara aman, mempelajari berbagai jenis malware dan serangannya, mengekplorasi karakteristik dan taktik yang digunakan oleh penjahat siber, langkah-langkah yang digunakan oleh organisasi untuk mengurangi serangan, dan meneliti peluang karir dibidang keamanan Siber.	
Materi Pemebelajaran/Pokok Bahasan	The Need for Cybersecurity Attacks, Concepts and Techniques Protecting Your Data and Privacy Protecting the Organization Will Your Future be in Cybersecurity? Cybersecurity: A World of Wizar The Cybersecurity Sorcery Cube dry, Criminals, and Heroes Cybersecurity Threats, Vulnerabilities and Attacks The Art of Protecting Secrets The Art of Ensuring Integrity The Realm of Five Nines Fortifying the Kingdom Joining the Order of Cyber Hero's	
Pustaka	**Utama**	
	Modul Introduction to Cybersecurity v2.1, Cisco Academy Modul Cybersecurity Essentials 1.0, Cisco Academy	
	Pendukung	
Media Pembelajaran	**Perangkat Lunak:**	**Perangkat Keras:**
	Cisco Packet Tracert, Windows, Linux, Android	LCD Projector, Komputer, Router & Switch Cisco, Smartphone
Team Teaching	-	

RENCANA PEMBELAJARAN SEMESTER
PROGRAM STUDI INFORMATIKA

RENCANA PEMBELAJARAN SEMESTER	
Mata Kuliah Prasyarat	
Indikator, Kriteria dan Bobot Penilaian	Tugas/Kuis : 20% Praktek / Latihan : 20% UTS : 30% UAS / Final Project : 30%

RENCANA PEMBELAJARAN SEMESTER

PROGRAM STUDI INFORMATIKA

RANCANGAN PEMBELAJARAN SEMESTER						
Minggu ke-	**Sub CP-MK (Kemampuan Akhir yang Diharapkan)**	**Indikator**	**Kriteria & Bentuk Penilaian**	**Metode Pembelajaran (Estimasi Waktu)**	**Materi Pembelajaran (Pustaka)**	**Bobot Penilaian (%)**
(1)	*(2)*	*(3)*	*(4)*	*(5)*	*(6)*	*(7)*
1	1. Mampu mendefinisikan karakteristik dan nilai data-data pribadi. 2. Mampu menjelaskan mengapa data pribadi dapat menguntungkan bagi para peretas. 3. Mampu menjelaskan jenis data yang digunakan oleh pemerintah dan organisasi. 4. Mampu menjelaskan dampak pelanggaran keamanan. 5. Mampu menjelaskan karakteristik dan motivasi penyerangan siber serta masalah hokum dan etika sebagai tenaga professional keamanan siber. 6. Mampu menjelaskan karakteristik dan tujuan perang siber.	• Ketepatan dalam mendefinisikan karakteristik dan nilai data-data pribadi. • Ketepatan dalam menjelaskan mengapa data pribadi dapat menguntungkan bagi para peretas. • Ketepatan dalam menjelaskan jenis data yang digunakan oleh pemerintah dan organisasi. • Ketepatan dalam menjelaskan dampak pelanggaran keamanan. • Ketepatan dalam menjelaskan karakteristik dan motivasi penyerangan siber serta masalah hokum dan etika sebagai tenaga professional keamanan	Kriteria: Ketepatan dan Penguasaan Bentuk Penilaian: • Diskusi • Test dan Evaluasi	Kuliah : TM : 1 x 50’ BM : 1 x 60’ BS : 1 x 60’ Praktikum : TM : 1 x 100’ BM : 1 x 70’	The Need for Cybersecurity	2,86% (1,43% logbook, 1,43% praktek)

RENCANA PEMBELAJARAN SEMESTER

PROGRAM STUDI INFORMATIKA

RANCANGAN PEMBELAJARAN SEMESTER						
Minggu ke-	**Sub CP-MK (Kemampuan Akhir yang Diharapkan)**	**Indikator**	**Kriteria & Bentuk Penilaian**	**Metode Pembelajaran (Estimasi Waktu)**	**Materi Pembelajaran (Pustaka)**	**Bobot Penilaian (%)**
(1)	*(2)*	*(3)*	*(4)*	*(5)*	*(6)*	*(7)*
		siber. • Ketepatan dalam menjelaskan karakteristik dan tujuan perang siber.				
2	1. Mampu menjelaskan cara eksploitasi kerentanan keamanan. 2. Mampu mengidentifikasikan contoh kerentanan keamanan. 3. Mampu menjelaskan jenis malware dan gejalanya. 4. Mampu menjelaskan metode infiltrasi. 5. Mampu menjelaskan metode yang digunakan untuk memboikot layanan. 6. Mampu menjelaskan serangan kombinasi. 7. Mampu menjelaskan pentingnya pengurangan dampak.	• Ketepatan dalam menjelaskan cara eksploitasi kerentanan keamanan. • Ketepatan dalam mengidentifikasikan contoh kerentanan keamanan. • Ketepatan dalam menjelaskan jenis malware dan gejalanya. • Ketepatan dalam menjelaskan metode infiltrasi. • Ketepatan dalam menjelaskan metode yang digunakan untuk memboikot layanan. • Ketepatan dalam menjelaskan serangan kombinasi. • Ketepatan dalam menjelaskan pentingnya pengurangan dampak.	Kriteria: Ketepatan dan Penguasaan Bentuk Penilaian: • Diskusi • Test dan Evaluasi	<u>Kuliah</u> : TM : 1 x 50’ BM : 1 x 60’ BS : 1 x 60’ <u>Praktikum</u> : TM : 1 x 100’ BM : 1 x 70’	Attacks, Concepts and Techniques	2,86% (1,43% logbook, 1,43% praktek)

RENCANA PEMBELAJARAN SEMESTER

PROGRAM STUDI INFORMATIKA

RANCANGAN PEMBELAJARAN SEMESTER

Minggu ke-	Sub CP-MK (Kemampuan Akhir yang Diharapkan)	Indikator	Kriteria & Bentuk Penilaian	Metode Pembelajaran (Estimasi Waktu)	Materi Pembelajaran (Pustaka)	Bobot Penilaian (%)
(1)	*(2)*	*(3)*	*(4)*	*(5)*	*(6)*	*(7)*
3	1. Mampu mengaktifkan dan memperbaharui firewall. 2. Mampu menggunakan antivirus dan antispyware. 3. Mampu mengelola system operasi dan browser. 4. Mampu melindungi semua perangkat.	• Ketepatan dalam mengaktifkan dan memperbaharui firewall. • Ketepatan dalam menggunakan antivirus dan antispyware. • Ketepatan dalam mengelola system operasi dan browser. • Ketepatan dalam melindungi semua perangkat.	Kriteria: Ketepatan dan Penguasaan Bentuk Penilaian: • Diskusi • Test dan Evaluasi	Kuliah : TM : 1 x 50’ BM : 1 x 60’ BS : 1 x 60’ Praktikum : TM : 1 x 100’ BM : 1 x 70’	Protecting Your Data and Privacy	2,86% (1,43% logbook, 1,43% praktek)
4	1. Mampu mengidentifikasikan fungsi CSIRT dalam Cisco. 2. Mampu menjelaskan tujuan buku panduan keamanan. 3. Mampu mengidentifikasikan alat bantu yang digunakan untuk pencegahan dan deteksi insiden. 4. Mampu mendefinisikan IDS dan IPS.	• Ketepatan dalam mengidentifikasikan fungsi CSIRT dalam Cisco. • Ketepatan dalam menjelaskan tujuan buku panduan keamanan. • Ketepatan dalam mengidentifikasikan alat bantu yang digunakan untuk pencegahan dan deteksi insiden. • Ketepatan dalam mendefinisikan IDS dan IPS.	Kriteria: Ketepatan dan Penguasaan Bentuk Penilaian: • Diskusi • Test dan Evaluasi	Kuliah : TM : 1 x 50’ BM : 1 x 60’ BS : 1 x 60’ Praktikum : TM : 1 x 100’ BM : 1 x 70’	Protecting the Organization	2,86% (1,43% logbook, 1,43% praktek)

RENCANA PEMBELAJARAN SEMESTER

PROGRAM STUDI INFORMATIKA

RANCANGAN PEMBELAJARAN SEMESTER

Minggu ke-	Sub CP-MK (Kemampuan Akhir yang Diharapkan)	Indikator	Kriteria & Bentuk Penilaian	Metode Pembelajaran (Estimasi Waktu)	Materi Pembelajaran (Pustaka)	Bobot Penilaian (%)
(1)	*(2)*	*(3)*	*(4)*	*(5)*	*(6)*	*(7)*
5	1. Mampu menjelaskan masalah hukum dalam bidang keamanan siber. 2. Mampu menjelaskan etika-etika dalam keamanan siber. 3. Mampu menjelaskan etika yang dihadapi tenaga professional keamanan siber.	• Ketepatan dalam menjelaskan masalah hukum dalam bidang keamanan siber. • Ketepatan dalam menjelaskan etika-etika dalam keamanan siber. • Ketepatan dalam menjelaskan etika yang dihadapi tenaga professional keamanan siber.	Kreteria: Ketepatan Bentuk Penilaian: • Diskusi • Test dan Evaluasi	Kuliah : TM : 1 x 50’ BM : 1 x 60’ BS : 1 x 60’ Praktikum : TM : 1 x 100’ BM : 1 x 70’	Will Your Future be in Cybersecurity?	2,86% (1,43% logbook, 1,43% praktek)
6	1. Mampu menjelaskan karakteristik umum yang terdiri dari dunia keamanan siber 2. Mampu membedakan karakteristik penjahat cyber dan profesional 3. Mampu membandingkan bagaimana ancaman keamanan siber memengaruhi individu, bisnis, dan organisasi. 4. Mampu menjelaskan faktor-faktor yang menyebabkan penyebaran dan pertumbuhan kejahatan	• Ketepatan dalam menjelaskan karakteristik umum yang terdiri dari dunia keamanan siber. • Ketepatan dalam membedakan karakteristik penjahat cyber dan profesional. • Ketepatan dalam membandingkan bagaimana ancaman keamanan siber memengaruhi individu, bisnis, dan organisasi. • Ketepatan dalam menjelaskan faktor-faktor yang	Kriteria: Ketepatan Bentuk Penilaian: • Diskusi • Test dan Evaluasi	Kuliah : TM : 1 x 50’ BM : 1 x 60’ BS : 1 x 60’ Praktikum : TM : 1 x 100’ BM : 1 x 70’	Cybersecurity: A World of Wizardry, Criminals, and Heroes	2,86% (1,43% logbook, 1,43% praktek)

RANCANGAN PEMBELAJARAN SEMESTER

Minggu ke-	Sub CP-MK (Kemampuan Akhir yang Diharapkan)	Indikator	Kriteria & Bentuk Penilaian	Metode Pembelajaran (Estimasi Waktu)	Materi Pembelajaran (Pustaka)	Bobot Penilaian (%)
(1)	*(2)*	*(3)*	*(4)*	*(5)*	*(6)*	*(7)*
	dunia maya. 5. Mampu menjelaskan organisasi dan upaya yang dilakukan untuk memperluas tenaga kerja keamanan siber.	menyebabkan penyebaran dan pertumbuhan kejahatan dunia maya. • Ketepatan dalam menjelaskan organisasi dan upaya yang dilakukan untuk memperluas tenaga kerja keamanan siber.				
7	1. Mampu menjelaskan bagaimana prinsip kerahasiaan, integritas, dan ketersediaan terkait dengan status data dan penanggulangan keamanan siber. 2. Mampu menjelaskan tiga dimensi McCumber Cube. 3. Mampu menjelaskan prinsip kerahasiaan, integritas, dan ketersediaan. 4. Mampu membedakan tiga status data. 5. Mampu membandingkan jenis tindakan pencegahan keamanan siber.	• Ketepatan dalam menjelaskan bagaimana prinsip kerahasiaan, integritas, dan ketersediaan terkait dengan status data dan penanggulangan keamanan siber. • Ketepatan dalam menjelaskan tiga dimensi McCumber Cube. • Ketepatan dalam menjelaskan prinsip kerahasiaan, integritas, dan ketersediaan. • Ketepatan dalam membedakan tiga status data. • Ketepatan dalam	Kriteria: Ketepatan Bentuk Penilaian: • Diskusi • Test dan Evaluasi	<u>Kuliah</u> : TM : 1 x 50’ BM : 1 x 60’ BS : 1 x 60’ <u>Praktikum</u> : TM : 1 x 100’ BM : 1 x 70’	The Cybersecurity Sorcery Cube	2,86% (1,43% logbook, 1,43% praktek)

RENCANA PEMBELAJARAN SEMESTER

PROGRAM STUDI INFORMATIKA

RANCANGAN PEMBELAJARAN SEMESTER

Minggu ke-	Sub CP-MK (Kemampuan Akhir yang Diharapkan)	Indikator	Kriteria & Bentuk Penilaian	Metode Pembelajaran (Estimasi Waktu)	Materi Pembelajaran (Pustaka)	Bobot Penilaian (%)
(1)	*(2)*	*(3)*	*(4)*	*(5)*	*(6)*	*(7)*
	6. Mampu menjelaskan ISO Cybersecurity Model.	membandingkan jenis tindakan pencegahan keamanan siber. • Ketepatan dalam menjelaskan ISO Cybersecurity Model.				
8	**Evaluasi Tengah Semester : Melakukan validasi hasil penilaian, evaluasi dan perbaikan proses pembelajaran berikutnya**					
9	1. Mampu membedakan jenis malware dan kode berbahaya. 2. Mampu membandingkan berbagai metode yang digunakan dalam rekayasa sosial. 3. Mampu membandingkan berbagai jenis serangan siber.	• Ketepatan dalam membedakan jenis malware dan kode berbahaya. • Ketepatan dalam membandingkan berbagai metode yang digunakan dalam rekayasa sosial. • Ketepatan dalam membandingkan berbagai jenis serangan siber.	Kriteria: Ketepatan Bentuk Penilaian: • Diskusi • Test dan Evaluasi	Kuliah : TM : 1 x 50’ BM : 1 x 60’ BS : 1 x 60’ Praktikum : TM : 1 x 100’ BM : 1 x 70’	Cybersecurity Threats, Vulnerabilities and Attacks	2,86% (1,43% logbook, 1,43% praktek)
10	1. Mampu menjelaskan bagaimana teknologi, produk, dan prosedur digunakan untuk melindungi kerahasiaan. 2. Mampu menjelaskan bagaimana teknik enkripsi melindungi kerahasiaan.	• Ketepatan dalam menjelaskan bagaimana teknologi, produk, dan prosedur digunakan untuk melindungi kerahasiaan. • Ketepatan dalam menjelaskan	Kriteria: Ketepatan dan Penguasaan Bentuk Penilaian: • Diskusi • Test dan Evaluasi	Kuliah : TM : 1 x 50’ BM : 1 x 60’ BS : 1 x 60’ Praktikum : TM : 1 x 100’ BM : 1 x 70’	The Art of Protecting Secrets	2,86% (1,43% logbook, 1,43% praktek)

RANCANGAN PEMBELAJARAN SEMESTER

Minggu ke-	Sub CP-MK (Kemampuan Akhir yang Diharapkan)	Indikator	Kriteria & Bentuk Penilaian	Metode Pembelajaran (Estimasi Waktu)	Materi Pembelajaran (Pustaka)	Bobot Penilaian (%)
(1)	*(2)*	*(3)*	*(4)*	*(5)*	*(6)*	*(7)*
	3. Mampu menjelaskan bagaimana teknik kontrol akses melindungi kerahasiaan. 4. Mampu menjelaskan konsep mengaburkan data.	bagaimana teknik enkripsi melindungi kerahasiaan. • Ketepatan dalam menjelaskan bagaimana teknik kontrol akses melindungi kerahasiaan. • Ketepatan dalam menjelaskan konsep mengaburkan data.				
11	1. Mampu menjelaskan bagaimana teknologi, produk, dan prosedur digunakan untuk memastikan integritas. 2. Mampu menjelaskan proses yang digunakan untuk memastikan integritas. 3. Mampu menjelaskan tujuan tanda tangan digital. 4. Mampu menjelaskan tujuan sertifikat digital. 5. Mampu menjelaskan perlunya integritas database.	• Ketepatan dalam menjelaskan bagaimana teknologi, produk, dan prosedur digunakan untuk memastikan integritas. • Ketepatan dalam menjelaskan proses yang digunakan untuk memastikan integritas. • Ketepatan dalam menjelaskan tujuan tanda tangan digital. • Ketepatan dalam menjelaskan tujuan sertifikat digital. • Ketepatan dalam menjelaskan perlunya	Kriteria: Ketepatan dan Penguasaan Bentuk Penilaian: • Diskusi • Test dan Evaluasi	<u>Kuliah</u> : TM : 1 x 50’ BM : 1 x 60’ BS : 1 x 60’ <u>Praktikum</u> : TM : 1 x 100’ BM : 1 x 70’	The Art of Ensuring Integrity	2,86% (1,43% logbook, 1,43% praktek)

RANCANGAN PEMBELAJARAN SEMESTER

Minggu ke-	Sub CP-MK (Kemampuan Akhir yang Diharapkan)	Indikator	Kriteria & Bentuk Penilaian	Metode Pembelajaran (Estimasi Waktu)	Materi Pembelajaran (Pustaka)	Bobot Penilaian (%)
(1)	*(2)*	*(3)*	*(4)*	*(5)*	*(6)*	*(7)*
		integritas database.				
12	1. Mampu menjelaskan bagaimana teknologi, produk, dan prosedur memberikan ketersediaan tinggi. 2. Mampu menjelaskan konsep ketersediaan tinggi. 3. Mampu menjelaskan bagaimana ukuran ketersediaan tinggi digunakan untuk meningkatkan ketersediaan. 4. Mampu menjelaskan bagaimana rencana respons insiden meningkatkan ketersediaan tinggi. 5. Mampu menjelaskan bagaimana perencanaan pemulihan bencana memainkan peran penting dalam menerapkan ketersediaan tinggi.	• Ketepatan dalam menjelaskan bagaimana teknologi, produk, dan prosedur memberikan ketersediaan tinggi. • Ketepatan dalam menjelaskan konsep ketersediaan tinggi. • Ketepatan dalam menjelaskan bagaimana ukuran ketersediaan tinggi digunakan untuk meningkatkan ketersediaan. • Ketepatan dalam menjelaskan bagaimana rencana respons insiden meningkatkan ketersediaan tinggi. • Ketepatan dalam menjelaskan bagaimana	Kriteria: Ketepatan dan Penguasaan Bentuk Penilaian: • Diskusi • Test dan Evaluasi	Kuliah : TM : 1 x 50’ BM : 1 x 60’ BS : 1 x 60’ Praktikum : TM : 1 x 100’ BM : 1 x 70’	The Realm of Five Nines	2,86% (1,43% logbook, 1,43% praktek)

RENCANA PEMBELAJARAN SEMESTER

PROGRAM STUDI INFORMATIKA

RANCANGAN PEMBELAJARAN SEMESTER						
Minggu ke-	**Sub CP-MK (Kemampuan Akhir yang Diharapkan)**	**Indikator**	**Kriteria & Bentuk Penilaian**	**Metode Pembelajaran (Estimasi Waktu)**	**Materi Pembelajaran (Pustaka)**	**Bobot Penilaian (%)**
(1)	*(2)*	*(3)*	*(4)*	*(5)*	*(6)*	*(7)*
		perencanaan pemulihan bencana memainkan peran penting dalam menerapkan ketersediaan tinggi.				
13	1. Mampu menjelaskan bagaimana para profesional keamanan siber menggunakan teknologi, proses dan prosedur untuk mempertahankan semua komponen jaringan. 2. Mampu menjelaskan bagaimana proses dan prosedur melindungi sistem. 3. Mampu menjelaskan cara melindungi server di jaringan. 4. Mampu menjelaskan bagaimana menerapkan langkah-langkah keamanan untuk melindungi perangkat jaringan. 5. Mampu menjelaskan bagaimana langkah-langkah keamanan fisik	• Ketepatan dalam menjelaskan bagaimana para profesional keamanan siber menggunakan teknologi, proses dan prosedur untuk mempertahankan semua komponen jaringan. • Ketepatan dalam menjelaskan bagaimana proses dan prosedur melindungi sistem. • Ketepatan dalam menjelaskan cara melindungi server di jaringan. • Ketepatan dalam menjelaskan bagaimana menerapkan langkah-langkah keamanan untuk melindungi	Kriteria: Ketepatan dan Penguasaan Bentuk Penilaian: • Diskusi • Test dan Evaluasi	Kuliah : TM : 1 x 50’ BM : 1 x 60’ BS : 1 x 60’ Praktikum : TM : 1 x 100’ BM : 1 x 70’	Protecting a Cybersecurity Domain	2,86% (1,43% logbook, 1,43% praktek)

RANCANGAN PEMBELAJARAN SEMESTER

Minggu ke-	Sub CP-MK (Kemampuan Akhir yang Diharapkan)	Indikator	Kriteria & Bentuk Penilaian	Metode Pembelajaran (Estimasi Waktu)	Materi Pembelajaran (Pustaka)	Bobot Penilaian (%)
(1)	*(2)*	*(3)*	*(4)*	*(5)*	*(6)*	*(7)*
	diterapkan untuk melindungi peralatan jaringan.	perangkat jaringan. • Ketepatan dalam menjelaskan bagaimana langkah-langkah keamanan fisik diterapkan untuk melindungi peralatan jaringan.				
14	1. Mampu menjelaskan tujuan hukum yang terkait dengan keamanan siber. 2. Mampu menjelaskan bagaimana domain keamanan siber digunakan dalam triad CIA. 3. Mampu menjelaskan bagaimana etika memberikan panduan. 4. Mampu menjelaskan cara mengambil langkah selanjutnya untuk menjadi profesional keamanan siber.	• Ketepatan dalam menjelaskan tujuan hukum yang terkait dengan keamanan siber. • Ketepatan dalam menjelaskan bagaimana domain keamanan siber digunakan dalam triad CIA. • Ketepatan dalam menjelaskan bagaimana etika memberikan panduan. • Ketepatan dalam menjelaskan cara mengambil langkah selanjutnya untuk menjadi profesional keamanan siber.	Kriteria: Ketepatan dan Penguasaan Bentuk Penilaian: • Diskusi • Test dan Evaluasi	<u>Kuliah</u> : TM : 1 x 50’ BM : 1 x 60’ BS : 1 x 60’ <u>Praktikum</u> : TM : 1 x 100’ BM : 1 x 70’	Becoming a Cybersecurity Specialist	2,86% (1,43% logbook, 1,43% praktek)

Universitas Pembangunan Jaya

RENCANA PEMBELAJARAN SEMESTER
PROGRAM STUDI INFORMATIKA

RANCANGAN PEMBELAJARAN SEMESTER

Minggu ke-	Sub CP-MK (Kemampuan Akhir yang Diharapkan)	Indikator	Kriteria & Bentuk Penilaian	Metode Pembelajaran (Estimasi Waktu)	Materi Pembelajaran (Pustaka)	Bobot Penilaian (%)
(1)	*(2)*	*(3)*	*(4)*	*(5)*	*(6)*	*(7)*
15	1. Mampu memahami permasalahan yang terdapat pada studi kasus. 2. Mampu memecahkan masalah yang terdapat pada studi kasus. 3. Mampu mempresentasikan solusi dari permasalahan yang telah dirumuskan.	• Ketepatan dalam memahami permasalahan yang terdapat pada studi kasus. • Ketepatan dalam memecahkan masalah yang terdapat pada studi kasus. • Ketepatan dalam mempresentasikan solusi dari permasalahan yang telah dirumuskan.	Kriteria: Ketepatan dan Penguasaan Bentuk Penilaian: • Diskusi • Test dan Evaluasi	Belajar Mandiri [BM: 1x (3x60")] Kuliah dan Diskusi [TM: 1x (1x50")] Presentasi BT: 1x(1x50") Tugas BM: 1x(3x60")		7,1
16	**Evaluasi Akhir Semester: Melakukan validasi penilaian akhir dan menentukan kelulusan mahasiswa**					

Catatan:
(1) TM: Tatap Muka, BT: Belajar Terstruktur, BM: Belajar Mandiri;

RENCANA PEMBELAJARAN SEMESTER

PROGRAM STUDI INFORMATIKA

RANCANGAN TUGAS MAHASISWA					
Mata Kuliah	Pengantar Keamanan Siber				
Kode MK	INF-	sks:	3	Semester:	4
Dosen Pengampu	Hendi Hermawan, S.T., M.T.I.				
BENTUK TUGAS					
Final Project / UAS					
JUDUL TUGAS					
Final Project: Studi Kasus Permasalahan Keamanan Siber					
SUB CAPAIAN PEMBELAJARAN MATA KULIAH					
Memecahkan permasalah dan memberikan solusi terkait dari keamanan siber yang sedang berkembang dimasyarakat					
DESKRIPSI TUGAS					
Final Project ini merupakan sebuah project yang mewajibkan mahasiswa untuk mencari permasalahan keamanan siber yang sedang berkembang dimasyarakat dimana dapat permasalahan tersebut dapat merugikan masyarakat baik secara pribadi maupun bagi masyarakat sekitar. Masalah yang didapat oleh mahasiswa perlu dicarikan solusinya agar dapat menimimalisir bahkan meniadakan kerugian yang ditimbulkannya.					
METODE PENGERJAAN TUGAS					
1. Melakukan observasi terhadap permasalahan keamanan siber yang sedang berkembang dimasyarakat. 2. Melakukan analisis dari permasalahan yang diangkat untuk dicarikan solusinya. 3. Solusi yang didapat didokumentasikan dengan baik. 4. Hasil dokumentasi, dipresentasikan didepan kelas.					
BENTUK DAN FORMAT LUARAN					
a. Obyek Garapan: Studi Kasus Permasalahan Keamanan Siber b. Bentuk luaran: 1. Dokumentasi solusi dari permasalahan yang diangkat.					
INDIKATOR, KRITERIA DAN BOBOT PENILAIAN					
a. Dokumentasi (bobot 20%) b. Analisis Permasalahan (bobot 30%) c. Solusi yang ditawarkan (bobot 30%) d. Presentasi (bobot 20%)					
JADWAL PELAKSANAAN					
Dokumentasi hasil observasi dan analisis	Sebelum UTS				

RANCANGAN TUGAS MAHASISWA	
permasalahan yang diangkat	
Dokumentasi solusi yang ditawarkan untuk memecahkan permasalahan yang diangkat	Setelah UTS
LAIN-LAIN	
-	
DAFTAR RUJUKAN	
Modul Introduction to Cybersecurity v2.1, Cisco Academy Modul Cybersecurity Essentials 1.0, Cisco Academy	

Jenjang/Grade	Angka/Skor	Angka Mutu	Deskripsi/Indikator Kerja
A (Sangat Baik)	A : 90.0 – 100	4	Mahasiswa terlibat sepenuhnya dalam diskusi, bermotivasi tinggi, melakukan persiapan dengan membaca materi sebelumnya, mengajukan gagasan dan pertanyaan substantif serta kritis, juga mendengarkan dan merespon secara terbuka terhadap kontribusi mahasiswa lain seraya memperlakukan sesama dengan setara dan adil
	A- : 80.00 – 89.99	3.7	
B (Baik)	B+ : 75.00 – 79.99	3.3	Mahasiswa terlibat sepenuhnya dalam diskusi, mengajukan gagasan dan pertanyaan substantif serta kritis, juga mendengarkan dan merespon secara terbuka terhadap kontribusi mahasiswa lain
	B : 70.00 – 74.99	3.0	
	B - : 65.00 – 69.99	2.7	
C (Cukup)	C+ : 60.00 - 64.99	2.3	Mahasiswa mengajukan gagasan dan pertanyaan, mendengarkan dan merespon secara terbuka terhadap kontribusi mahasiswa lain
	C : 55.00 – 59.99	2.0	
D (Kurang)	C- : 50.00 – 54.99	1.7	Mahasiswa tidak mengajukan gagasan dan pertanyaan, hanya mendengarkan dan tidak merespon secara terbuka terhadap kontribusi mahasiswa lain
	D : 40.00 – 49.99	1	
E (Sangat Kurang / Tidak Lulus)	<40.00	0	Mahasiswa tidak memenuhi kaidah – kaidah yang ditetapkan di atas