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.	Dr. Resdiansyah

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	

RENCANA PEMBELAJARAN SEMESTER

PROGRAM STUDI INFORMATIKA

RENCANA PEMBELAJARAN SEMESTER			
	5	Mampu menjelaskan prinsip-prinsip confidentiality, integrity, dan availability yang terkait dengan status data dan penanggulangan keamanan siber.	
	6	Mampu menjelaskan taktik, Teknik, dan prosedur yang digunakan oleh penjahat siber.	
	7	Mampu menjelaskan bagaimana teknologi, produk, dan prosedur dapat digunakan untuk melindungi kerahasiaan / confidentiality, integritas / integrity, dan memberikan ketersediaan tinggi / high availability.	
	8	Mampu menjelaskan bagaimana para professional keamanan siber menggunakan teknologi, proses, dan prosedur untuk mempertahankan semmua komponen jaringan.	
		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	Threat Actor and Defender Operating System Overview Network Fundamental Network Infrastructure Security Threats and Attacks Network Defense Cryptography and Endpoint Protection Protocols and Log Files Analyzing Security Data		
Pustaka	**Utama**		
	Modul Cybersecurity Associate, Cisco Academy		
	Pendukung		
Media Pembelajaran	**Perangkat Lunak:**	**Perangkat Keras:**	
	Cisco Packet Tracert, Windows, Linux, Android	LCD Projector, Komputer, Router & Switch Cisco, Smartphone	
Team Teaching	-		
Mata Kuliah Prasyarat			
Indikator, Kriteria dan Bobot Penilaian	Tugas/Kuis : 20% Praktek / Latihan : 20% UTS : 30%		

RENCANA PEMBELAJARAN SEMESTER	
	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)*
1,2	1. Mahasiswa mampu mengidentifikasi dan mengklasifikasikan berbagai jenis aktor ancaman siber berdasarkan motivasi, kemampuan, dan taktik yang digunakan dalam serangan siber. 2. Mahasiswa mampu mengembangkan dan mengimplementasikan strategi pertahanan siber yang efektif untuk melindungi sistem informasi dari berbagai jenis serangan siber. 3. Mahasiswa mampu merancang dan melaksanakan rencana respon insiden yang komprehensif, termasuk identifikasi, penanganan, dan	• Ketepatan dalam mengidentifikasi dan mengklasifikasikan berbagai jenis aktor ancaman siber berdasarkan motivasi, kemampuan, dan taktik yang digunakan dalam serangan siber. • Ketepatan dalam mengembangkan dan mengimplementasikan strategi pertahanan siber yang efektif untuk melindungi sistem informasi dari berbagai jenis serangan siber. • Ketepatan dalam merancang dan melaksanakan rencana respon insiden yang komprehensif, termasuk identifikasi, penanganan, dan	Kriteria: Ketepatan dan Penguasaan Bentuk Penilaian: • Ceramah • Test dan Evaluasi	Kuliah : TM : 2 x 50’ BM : 2 x 60’ BS : 2 x 60’ Praktikum : TM : 2 x 100’ BM : 2 x 70’	Threat Actor and Defender	5,72% (2,86% logbook, 2,86% 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)*
	pemulihan dari insiden siber.	pemulihan dari insiden siber.				
3,4	1. Mahasiswa mampu menjelaskan konsep dasar sistem operasi, termasuk manajemen proses, manajemen memori, sistem file, dan perangkat keras. 2. Mahasiswa mampu menganalisis arsitektur berbagai sistem operasi dan menjelaskan perbedaan serta keunggulan masing-masing. 3. Mahasiswa mampu mengidentifikasi dan mengimplementasikan mekanisme keamanan sistem operasi untuk melindungi data dan aplikasi dari ancaman keamanan.	• Ketepatan dalam menjelaskan konsep dasar sistem operasi, termasuk manajemen proses, manajemen memori, sistem file, dan perangkat keras. • Ketepatan dalam menganalisis arsitektur berbagai sistem operasi dan menjelaskan perbedaan serta keunggulan masing-masing. • Ketepatan dalam mengidentifikasi dan mengimplementasikan mekanisme keamanan sistem operasi untuk melindungi data dan aplikasi dari ancaman keamanan..	Kriteria: Ketepatan dan Penguasaan Bentuk Penilaian: • Ceramah Test dan Evaluasi	Kuliah : TM : 2 x 50’ BM : 2 x 60’ BS : 2 x 60’ Praktikum : TM : 2 x 100’ BM : 2 x 70’	Operating System Overview	5,72% (2,86% logbook, 2,86% 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, 6	1. Mahasiswa mampu menjelaskan prinsip dasar jaringan komputer, termasuk model OSI, TCP/IP, dan topologi jaringan. 2. Mahasiswa mampu mengidentifikasi dan mengkonfigurasi berbagai perangkat jaringan seperti router, switch, dan firewall. 3. Mahasiswa mampu menganalisis fungsi dan implementasi protokol jaringan umum seperti HTTP, FTP, SMTP, DNS	• Ketepatan dalam menjelaskan prinsip dasar jaringan komputer, termasuk model OSI, TCP/IP, dan topologi jaringan. • Ketepatan dalam mengidentifikasi dan mengkonfigurasi berbagai perangkat jaringan seperti router, switch, dan firewall. • Ketepatan dalam menganalisis fungsi dan implementasi protokol jaringan umum seperti HTTP, FTP, SMTP, dan DNS.	Kriteria: Ketepatan dan Penguasaan Bentuk Penilaian: • Ceramah • Test dan Evaluasi	<u>Kuliah</u> : TM : 2 x 50’ BM : 2 x 60’ BS : 2 x 60’ <u>Praktikum</u> : TM : 2 x 100’ BM : 2 x 70’	Network Fundamental	5,72% (2,86% logbook, 2,86% praktek)
7	1. Mahasiswa mampu mengidentifikasi dan mengevaluasi kelemahan dalam infrastruktur jaringan yang dapat dieksploitasi oleh penyerang.	• Ketepatan dalam mengidentifikasi dan mengevaluasi kelemahan dalam infrastruktur jaringan yang dapat dieksploitasi oleh penyerang.	Kriteria: Ketepatan dan Penguasaan Bentuk Penilaian: • Ceramah • 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’	Network Infrastructure Security	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)*
8	**Evaluasi Tengah Semester : Melakukan validasi hasil penilaian, evaluasi dan perbaikan proses pembelajaran berikutnya**					
9, 10	1. Mahasiswa mampu merancang dan mengimplementasikan langkah-langkah keamanan untuk melindungi infrastruktur jaringan dari serangan. 2. Mahasiswa mampu menerapkan teknik segmentasi jaringan untuk membatasi pergerakan lateral penyerang dalam jaringan.	• Ketepatan dalam merancang dan mengimplementasikan langkah-langkah keamanan untuk melindungi infrastruktur jaringan dari serangan. • Ketepatan dalam menerapkan teknik segmentasi jaringan untuk membatasi pergerakan lateral penyerang dalam jaringan.	Kriteria: Ketepatan dan Penguasaan Bentuk Penilaian: • Ceramah • Test dan Evaluasi	Kuliah : TM : 2 x 50' BM : 2 x 60' BS : 2 x 60' Praktikum : TM : 2 x 100' BM : 2 x 70'	Network Infrastructure Security	5,72% (2,86% logbook, 2,86% praktek)
11	1. Mahasiswa mampu mengidentifikasi dan menjelaskan berbagai jenis ancaman siber dan serangan yang umum terjadi, seperti malware, phishing, dan DDoS. 2. Mahasiswa mampu menganalisis berbagai vektor serangan yang	• Ketepatan dalam mengidentifikasi dan menjelaskan berbagai jenis ancaman siber dan serangan yang umum terjadi, seperti malware, phishing, dan DDoS. • Ketepatan dalam menganalisis berbagai vektor serangan yang	Kriteria: Ketepatan dan Penguasaan Bentuk Penilaian: • Ceramah • 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'	Threats and Attacks	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)*
	digunakan oleh penyerang untuk mengakses sistem informasi. 3. Mahasiswa mampu mengembangkan strategi mitigasi yang efektif untuk mencegah dan mengurangi dampak serangan siber.	digunakan oleh penyerang untuk mengakses sistem informasi. • Ketepatan dalam mengembangkan strategi mitigasi yang efektif untuk mencegah dan mengurangi dampak serangan siber..				
12	1. Mahasiswa mampu menjelaskan dan mengimplementasikan teknologi pertahanan jaringan seperti IDS/IPS, firewall, dan honeypots. 2. Mahasiswa mampu merancang dan mengimplementasikan strategi pertahanan berlapis untuk melindungi jaringan dari berbagai jenis serangan. 3. Mahasiswa mampu mengembangkan rencana penanganan insiden yang efektif	• firewall, dan honeypots. • Ketepatan dalam merancang dan mengimplementasikan strategi pertahanan berlapis untuk melindungi jaringan dari berbagai jenis serangan. • Ketepatan dalam mengembangkan rencana penanganan insiden yang efektif untuk mendeteksi, merespons, dan memulihkan dari insiden keamanan jaringan.	Kriteria: Ketepatan dan Penguasaan Bentuk Penilaian: • Ceramah • 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’	Network Defense	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)*
	untuk mendeteksi, merespons, dan memulihkan dari insiden keamanan jaringan.					
13	1. Mahasiswa mampu menjelaskan prinsip dasar kriptografi dan berbagai algoritma kriptografi yang digunakan untuk melindungi data. 2. Mahasiswa mampu mengidentifikasi dan menerapkan langkah-langkah keamanan untuk melindungi endpoint dari ancaman keamanan. 3. Mahasiswa mampu mengimplementasikan teknik enkripsi untuk melindungi data dalam proses penyimpanan dan transmisi.	• Ketepatan dalam menjelaskan prinsip dasar kriptografi dan berbagai algoritma kriptografi yang digunakan untuk melindungi data. • Ketepatan dalam mengidentifikasi dan menerapkan langkah-langkah keamanan untuk melindungi endpoint dari ancaman keamanan. • Ketepatan dalam mengimplementasikan teknik enkripsi untuk melindungi data dalam proses penyimpanan dan transmisi.	Kriteria: Ketepatan dan Penguasaan Bentuk Penilaian: • Ceramah • 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’	Cryptography and Endpoint Protection	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)*
14	1. Mahasiswa mampu menganalisis dan menjelaskan fungsi dan struktur berbagai protokol jaringan yang umum digunakan. 2. Mahasiswa mampu mengumpulkan, menganalisis, dan mengelola log file untuk mendeteksi dan merespons insiden keamanan. 3. Mahasiswa mampu merancang dan mengimplementasikan sistem SIEM (Security Information and Event Management) untuk memonitor dan menganalisis aktivitas jaringan secara real-time.	• Ketepatan dalam menganalisis dan menjelaskan fungsi dan struktur berbagai protokol jaringan yang umum digunakan. • Ketepatan dalam mengumpulkan, menganalisis, dan mengelola log file untuk mendeteksi dan merespons insiden keamanan. • Ketepatan dalam merancang dan mengimplementasikan sistem SIEM (Security Information and Event Management) untuk memonitor dan menganalisis aktivitas jaringan secara real-time.	Kriteria: Ketepatan dan Penguasaan Bentuk Penilaian: • Ceramah • 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’	Protocols and Log Files	2,86% (1,43% logbook, 1,43% praktek)
15	1. Mahasiswa mampu mengidentifikasi dan menerapkan teknik pengumpulan data yang efektif untuk analisis keamanan.	• Ketepatan dalam mengidentifikasi dan menerapkan teknik pengumpulan data yang efektif untuk analisis keamanan.	Kriteria: Ketepatan dan Penguasaan Bentuk Penilaian: • Ceramah • Test dan Evaluasi	Kuliah : TM : 1 x 50’ BM : 1 x 60’ BS : 1 x 60’ Praktikum :	Analyzing Security Data	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)*
	2. Mahasiswa mampu menganalisis data keamanan untuk mengidentifikasi pola, anomali, dan indikasi serangan siber. 3. Mahasiswa mampu menyusun laporan analisis keamanan yang komprehensif dan menyampaikan temuan kepada pihak terkait dengan jelas dan efektif.	• Ketepatan dalam menganalisis data keamanan untuk mengidentifikasi pola, anomali, dan indikasi serangan siber. • Ketepatan dalam menyusun laporan analisis keamanan yang komprehensif dan menyampaikan temuan kepada pihak terkait dengan jelas dan efektif.		TM : 1 x 100’ BM : 1 x 70’		
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

RENCANA PEMBELAJARAN SEMESTER
PROGRAM STUDI INFORMATIKA

RANCANGAN TUGAS MAHASISWA	
Dokumentasi hasil observasi dan analisis permasalahan yang diangkat	Sebelum UTS
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