

RENCANA PEMBELAJARAN MATA KULIAH

NAMA MK : Keamanan Siber
KODE MK : TI213511
SEMESTER : VII
NAMA DOSEN / TIM : I Wayan Ardiyasa, S.Kom., M.MSI
Gde Sastrawangsa, ST., MT.

DAFTAR ISI

I.	Capaian Pembelajaran (Learning Outcomes) Prodi.....	1
	1. Capaian Pembelajaran Lulusan (CPL) / Programme Learning Outcomes (PLO)	1
	2. Capaian Pembelajaran Lulusan (CPL) yang dibebankan Pada MK.....	1
II.	Rencana Pembelajaran Semester	3
III.	Rencana Penilaian / Asesmen & Evaluasi (RAE), dan Rencana Tugas.....	17
	1. I Wayan Ardiyasa, S.Kom., M.MSI	17
	2. Gde Sastrawangsa, S.T., M.T.	17
IV.	Portofolio penilaian & evaluasi proses dan hasil belajar setiap mahasiswa.....	20
A.	Rencana Tugas & Rubrik Penilaian	21

Capaian Pembelajaran (Learning Outcomes) Prodi

1. Capaian Pembelajaran Lulusan (CPL) / Programme Learning Outcomes (PLO)

KODE CPL	DESKRIPSI CPL
CPL01	Mampu menerapkan konsep-konsep dasar komputer yang dibutuhkan dalam merancang dan mengimplementasikan solusi teknologi Informasi dan komunikasi
CPL02	Memiliki kemampuan mengidentifikasi, merancang dan memecahkan permasalahan kebutuhan sistem dan informasi dari suatu organisasi
CPL03	Mampu menerapkan solusi berbasis teknologi Informasi dan komunikasi dari sudut pandang bisnis dan manajemen secara efektif pada suatu organisasi
CPL04	Memiliki kemampuan dalam menganalisis, mengembangkan ide dan menyelesaikan masalah yang dituangkan dalam bentuk suatu tulisan karya ilmiah sesuai dengan bidang sistem informasi
CPL05	Memiliki kemampuan dalam menganalisis, mengembangkan ide dan menyelesaikan masalah yang dituangkan dalam bentuk suatu tulisan karya ilmiah sesuai dengan bidang sistem informasi
CPL06	Memiliki tanggung jawab dan kemampuan dalam pengambilan keputusan yang tepat terhadap suatu masalah tertentu
CPL07	Mampu berkarya dengan berdasarkan agama, moral dan etika serta seni dan budaya lokal sesuai bidang keprofesian teknologi Informasi dan komunikasi
CPL08	Memiliki kemampuan berkomunikasi dan bekerjasama secara efektif dengan berbagai kalangan.
CPL09	Memiliki kemampuan untuk mengidentifikasi kebutuhan dan sumberdaya untuk menjadi wirausaha khususnya dalam bidang teknologi Informasi dan komunikasi

2. Capaian Pembelajaran Lulusan (CPL) yang dibebankan Pada MK

CPL-PRODI yang dibebankan pada MK	
CPL06	Memiliki kemampuan dan pengetahuan secara konsep dan teori tentang arsitektur dan kebutuhan infrastruktur teknologi informasi yang mencakup sistem dan jaringan komputer, integrasi sistem, sistem enterprise dan sistem database untuk kebutuhan organisasi/perusahaan didalam mengelola sistem informasi.
CPL07	Memiliki kemampuan dan pengetahuan secara konsep dan teknis untuk melakukan analisa kelemahan suatu sistem serta mampu mengamankannya untuk

	meminimalisir potensi pelanggaran terhadap suatu sistem dan mampu mengambil keputusan secara cepat dan tepat untuk proses monitoring dan evaluasi.
Capaian Pembelajaran Mata Kuliah (CPMK)	
CPMK-06-17	Mampu menjelaskan dan menguasai Teknik pengamanan sistem dan jaringan komputer untuk mengidentifikasi dan mencegah serangan cyber dengan mengimplementasikan aspek-aspek keamanan informasi.
CPMK-07-4	Mampu menjelaskan dan menguasai konsep dasar teori jaringan Mahasiswa mampu memahami konsep Jaringan Komputer, Mengetahui Perangkat- perangkat Jaringan, Protokol Jaringan, OSI dan TCP/IP Model, konsep IP adres dan kelas-kelas dalam IP Adres, Routing dengan media Virtual seperti menggunakan Packet Tracer, memahami Jaringan Nirkabel, mengetahui serangan dalam jaringan dan mengetahui Firewall

INSTITUT TEKNOLOGI DAN BISNIS STIKOM BALI
FAKULTAS INFORMATIKA DAN KOMPUTER
PROGRAM STUDI TEKNOLOGI INFORMASI

No. Dok	: FM/01/12/WRI/ITBSTIKOM
No. Revisi	: 00
Tgl. Berlaku	: 18 Agustus 2021
Halaman	: 3

Rencana Pembelajaran Semester

RENCANA PEMBELAJARAN SEMESTER							
MATA KULIAH (MK)	KODE	Rumpun MK	BOBOT (sks)		SEMESTER	Tgl. Penyusunan	Versi Dok.
Keamanan Siber	TI213511	Mata Kuliah Wajib Prodi (MKWP)	Teori = 4	P = 0	VII	21 Juni 2024	02
OTORISASI / PENGESAHAN	Dosen Pengembang RPS		Ka PRODI				
	I Wayan Ardiyasa, S.Kom., M.MSI						
	Gde Sastrawangsa, ST., MT.		I Wayan Ardiyasa, S.Kom., M.MSI.				
Capaian Pembelajaran	CPL-PRODI yang dibebankan pada MK						
	CPL06	Memiliki kemampuan dan pengetahuan secara konsep dan teori tentang arsitektur dan kebutuhan infrastruktur teknologi informasi yang mencakup sistem dan jaringan komputer, integrasi sistem, sistem enterprise dan sistem database untuk kebutuhan organisasi/perusahaan didalam mengelola sistem informasi.					

INSTITUT TEKNOLOGI DAN BISNIS STIKOM BALI
FAKULTAS INFORMATIKA DAN KOMPUTER
PROGRAM STUDI TEKNOLOGI INFORMASI

No. Dok	: FM/01/12/WRI/ITBSTIKOM
No. Revisi	: 00
Tgl. Berlaku	: 18 Agustus 2021
Halaman	: 4

	CPL07	Memiliki kemampuan dan pengetahuan secara konsep dan teknis untuk melakukan analisa kelemahan suatu sistem seta mampu mengamankannya untuk meminimalisir potensi pelanggaran terhadap suatu sistem dan mampu mengambil keputusan secara cepat dan tepat untuk proses monitoring dan evaluasi									
Capaian Pembelajaran Mata Kuliah (CPMK)											
	CPMK-06-17	Mampu menjelaskan dan menguasai teknik pengamanan sistem dan jaringan komputer untuk mengidentifikasi dan mencegah serangan cyber dengan mengimplementasikan aspek-aspek keamanan informasi									
	CPMK-07-4	Mampu menjelaskan dan menguasai konsep dasar teori jaringan mahasiswa mampu memahami konsep jaringan komputer, mengetahui perangkat-perangkat jaringan, protokol jaringan, OSI dan TCP/IP model, konsep IP Address dan kelas-kelas dalam IP Address, Routing dengan media virtual seperti menggunakan packet tracer, memahami jaringan nirkabel, mengetahui serangan dalam jaringan dan mengetahui firewall.									
Peta CPL – CP MK		CPL01	CPL02	CPL03	CPL04	CPL05	CPL06	CPL07	CPL08	CPL09	
	CPMK-06-17						√				
	CPMK-07-4							√			
Deskripsi Singkat MK	Keamanan siber adalah matakuliah yang mempelajari tentang konsep dan teknik untuk pengamanan aplikasi, sistem dan jaringan komputer serta data digital dari kejahatan cyber yang dapat mengganggu proses bisnis dan mengakibatkan kerugian.										
Bahan Kajian: Materi pembelajaran	<ul style="list-style-type: none"> • Pengenalan Keamanan Siber • Kriptografi • Steganografi • Vulnerability Assesment • Hardening System • Email Security • Malware Analyst • Web Application Security 										

INSTITUT TEKNOLOGI DAN BISNIS STIKOM BALI
FAKULTAS INFORMATIKA DAN KOMPUTER
PROGRAM STUDI TEKNOLOGI INFORMASI

No. Dok	: FM/01/12/WRI/ITBSTIKOM
No. Revisi	: 00
Tgl. Berlaku	: 18 Agustus 2021
Halaman	: 5

	<ul style="list-style-type: none"> • Wireless Security • Firewall & IDS • IT & Cyberlaw
Pustaka	<p>Utama:</p> <p>Tuliskan referensi utama dalam susunan berurut</p> <ol style="list-style-type: none"> 1. Sadikin, R. (2012). Kriptografi Untuk Keamanan Jaringan dan Implementasinya dalam bahasa java. Yogyakarta: Andi 2. Weidman, G. (2014). Penetration Testing A Hands-On Introduction to Hacking. 3. Situmeang, M.S (2020). <i>Cyber Law</i>, Bandung: Cakra 2020 <p>Referensi Pendukung :</p> <ol style="list-style-type: none"> 1. Artikel Keamanan Informasi : http://www.conferencezone.org/index.php/cz/article/view/570/547 2. Artikel tentang Kriptografi : https://ejournal.utp.ac.id/index.php/JSS/article/view/1601/520521268 3. Artikel Scanning Vulnerability : https://jtdt.org/jtdt/article/view/190/106 4. Artikel Hardening Sistem : https://journal.mediapublikasi.id/index.php/oktal/article/view/882/604 5. Artikel Email Security. http://teknologipintar.org/index.php/teknologipintar/article/view/397/383 6. Artikel tentang Malware : http://jurnal.unmuhjember.ac.id/index.php/JUSTINDO/article/view/1037/832 7. Artikel Keamanan Web : http://ijcs.net/ijcs/index.php/ijcs/article/view/3736/525 8. Artikel Keamanan Wireless : https://www.unisbank.ac.id/ojs/index.php/fti1/article/view/33/28 9. Artikel IDS : https://iocscience.org/ejournal/index.php/mantik/article/view/120/81
Dosen Pengampu	Terlampir
Matakuliah syarat	-

INSTITUT TEKNOLOGI DAN BISNIS STIKOM BALI
FAKULTAS INFORMATIKA DAN KOMPUTER
PROGRAM STUDI TEKNOLOGI INFORMASI

No. Dok	: FM/01/12/WRI/ITBSTIKOM
No. Revisi	: 00
Tgl. Berlaku	: 18 Agustus 2021
Halaman	: 6

Pertemuan Ke-	Kemampuan akhir tiap tahapan belajar (Sub-CPMK)	Penilaian		Bantuk Pembelajaran; Metode Pembelajaran; Penugasan Mahasiswa; [Estimasi Waktu]		Materi Pembelajaran [Pustaka]	Bobot Penilaian (%)
		Indikator	Kriteria & Teknik	Tatap Muka (5)	Daring (6)		
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
1	CPMK-06-17 Mampu menjelaskan dan menguasai teknik pengamanan sistem dan jaringan komputer untuk mengidentifikasi dan mencegah serangan cyber dengan mengimplementasikan aspek-aspek keamanan informasi	1.1 Pengenalan Keamanan Siber 1.2 Aspek-aspek keamanan informasi 1.3 Jenis-jenis ancaman, serangan dan asset 1.4 Strategi keamanan komputer 1.5 Attack surfack dan Atttack tree	Kriteria: <ul style="list-style-type: none"> • Komponen sikap • Komponen pengetahuan • Komponen keterampilan umum • Komponen keterampilan khusus Teknik: <ul style="list-style-type: none"> • Tes Lisan – Mampu menjelaskan tentang konsep network penetration testing dan fase-fasenya. 	<ul style="list-style-type: none"> • Kuliah [TM:1x(3x50)]-Pert.1 • Diskusi [TM:1x(1x50)]-Pert.1 	<ul style="list-style-type: none"> • Ms.Teams • eLearning http://elearning.stikom-bali.ac.id/ • Studi Independen: Topik Keamanan Siber [1x(4x119)]-Pert.1 	Materi Pembelajaran <ul style="list-style-type: none"> • Pengenalan Keamanan Siber Pustaka: <ul style="list-style-type: none"> • Bill Nelson, A. P. (2018). Guide to Computer Forensics And Investigations. USA. (Chapter 1) 	
2,3	CPMK-06-17 Mampu menjelaskan dan menguasai teknik pengamanan sistem dan	1.1 Pengenalan kriptografi dan keamanan jaringan 1.2 Kriptografi klasik	Kriteria: <ul style="list-style-type: none"> • Komponen sikap • Komponen pengetahuan 	<ul style="list-style-type: none"> • Kuliah [TM:2x(3x50)]-Pert.2,3 • Diskusi 	<ul style="list-style-type: none"> • Ms.Teams • eLearning http://elearning.stikom-bali.ac.id/ 	Materi Pembelajaran <ul style="list-style-type: none"> • Kriptografi Pustaka: <ul style="list-style-type: none"> • Sadikin, R. (2012). Kriptografi Untuk 	10

INSTITUT TEKNOLOGI DAN BISNIS STIKOM BALI
FAKULTAS INFORMATIKA DAN KOMPUTER
PROGRAM STUDI TEKNOLOGI INFORMASI

No. Dok	: FM/01/12/WRI/ITBSTIKOM
No. Revisi	: 00
Tgl. Berlaku	: 18 Agustus 2021
Halaman	: 7

	jaringan komputer untuk mengidentifikasi dan mencegah serangan cyber dengan mengimplementasikan aspek-aspek keamanan informasi	1.3 Kriptografi Modern 1.4 Proses Enkripsi dan Dekripsi 1.5 Kunci Private 1.6 kunci public 1.7 Fungsi hash 1.8 Digital signature 1.9 Steganografi	<ul style="list-style-type: none"> Komponen keterampilan umum Komponen keterampilan khusus <p>Teknik: Tugas 1 – Studi Kasus Kriptografi dan Steganografi</p>	<p>[TM:2x(1x50)]-Pert.2,3</p> <ul style="list-style-type: none"> Tugas 1 [PT+BM:(1+1)x(1x60)]-Pert.3 	<ul style="list-style-type: none"> Studi Independen: Topik Kriptografi [1x(4x119)]-Pert.2 Penugasan Terstruktur, Topik Kriptografi dan steganografi [1x(4x119)]-Pert.3 	Keamanan Jaringan dan Implementasinya dalam bahasa java. Yogyakarta: Andi.	
4	CPMK-06-17 Mampu menjelaskan dan menguasai teknik pengamanan sistem dan jaringan komputer untuk mengidentifikasi dan mencegah serangan cyber dengan mengimplementasikan aspek-aspek keamanan informasi	1.1 Pengenalan finding Vulnerability 1.2 Teknik scanning 1.3 Jenis vulnerability 1.4 Penggunaan tools Nessus dan nmap	<p>Kriteria:</p> <ul style="list-style-type: none"> Komponen sikap Komponen pengetahuan Komponen keterampilan umum Komponen keterampilan khusus <p>Teknik:</p> <ul style="list-style-type: none"> Kuis 1: 	<ul style="list-style-type: none"> Kuliah [TM:1x(3x50)]-Pert. 4 Diskusi [TM:1x(1x50)]-Pert.4 Kuis 1: [PT+BM:(1+1)x(1x60)]-Pert.4 	<ul style="list-style-type: none"> Ms.Teams eLearning http://elearning.stikom-bali.ac.id/ Studi Independen: Topik Scanning Vulnerability [1x(4x119)]-Pert.4 	<p>Materi Pembelajaran</p> <ul style="list-style-type: none"> Finding Vulnerability Pustaka: Weidman, G. (2014). Penetration Testing A Hands-On Introduction to Hacking. 	5

INSTITUT TEKNOLOGI DAN BISNIS STIKOM BALI
FAKULTAS INFORMATIKA DAN KOMPUTER
PROGRAM STUDI TEKNOLOGI INFORMASI

No. Dok	: FM/01/12/WRI/ITBSTIKOM
No. Revisi	: 00
Tgl. Berlaku	: 18 Agustus 2021
Halaman	: 8

	<p>CPMK-07-4 Mampu menjelaskan dan menguasai konsep dasar teori jaringan mahasiswa mampu memahami konsep jaringan komputer, mengetahui perangkat-perangkat jaringan, protokol jaringan, OSI dan TCP/IP model, konsep IP Address dan kelas-kelas dalam IP Address, Routing dengan media virtual seperti menggunakan packet tracer, memahami jaringan nirkabel, mengetahui serangan dalam jaringan dan mengetahui firewall.</p>		<ul style="list-style-type: none"> • Menjelaskan tentang jenis-jenis kriptografi • Menjelaskan tentang jenis algoritma kriptografi • Menjelaskan implementasi teknologi kriptografi • Memahami teknik enkripsi dan dekripsi kriptografi 				
5	<p>CPMK-06-17 Mampu menjelaskan dan</p>	1.1. Pengenalan keamanan sistem	<p>Kriteria:</p> <ul style="list-style-type: none"> • Komponen sikap 	<ul style="list-style-type: none"> • Kuliah 	<ul style="list-style-type: none"> • Ms.Teams • eLearning 	<p>Materi Pembelajaran</p> <ul style="list-style-type: none"> • Hardening Sistem 	

INSTITUT TEKNOLOGI DAN BISNIS STIKOM BALI
FAKULTAS INFORMATIKA DAN KOMPUTER
PROGRAM STUDI TEKNOLOGI INFORMASI

No. Dok	: FM/01/12/WRI/ITBSTIKOM
No. Revisi	: 00
Tgl. Berlaku	: 18 Agustus 2021
Halaman	: 9

	menguasai teknik pengamanan sistem dan jaringan komputer untuk mengidentifikasi dan mencegah serangan cyber dengan mengimplementasikan aspek-aspek keamanan informasi	1.2 Teknik hardening 1.2. Windows dan Linux Hardening 1.3. Patch management 1.4 Network Access Quarantine Control 1.5 Security Auditing and Event Logs	<ul style="list-style-type: none"> • Komponen pengetahuan • Komponen keterampilan umum • Komponen keterampilan khusus 	<ul style="list-style-type: none"> • [TM:1x(3x50)]-Pert.5 • Diskusi [TM:1x(1x50)]-Pert.5 	<ul style="list-style-type: none"> • http://elearning.stikom-bali.ac.id/ • Studi Independen: Topik Hardening Sistem [1x(4x119)]-Pert.5 	<p>Pustaka: Hassell, J. (2006). Hardening Windows Secpnd Edition. Springer.</p>	
6	CPMK-06-17 Mampu menjelaskan dan menguasai teknik pengamanan sistem dan jaringan komputer untuk mengidentifikasi dan mencegah serangan cyber dengan mengimplementasikan aspek-aspek keamanan informasi	1.1. Pengertian Email 1.2. Masalah keamanan Email 1.3. Komponen Sistem email 1.4. Jenis kejahatan email	<p>Kriteria:</p> <ul style="list-style-type: none"> • Komponen sikap • Komponen pengetahuan • Komponen keterampilan umum • Komponen keterampilan khusus 	<ul style="list-style-type: none"> • Kuliah [TM:1x(3x50)]-Pert.6 • Diskusi [TM:1x(1x50)]-Pert.6 	<ul style="list-style-type: none"> • Ms.Teams • eLearning • http://elearning.stikom-bali.ac.id/ • Studi Independen: Topik email security [1x(4x119)]-Pert.6 	<p>Materi Pembelajaran</p> <ul style="list-style-type: none"> • Email Security <p>Pustaka: Raharjo, B. (2017). Keamanan Informasi. Bandung.</p>	
7	CPMK-06-17 Mampu menjelaskan dan menguasai teknik pengamanan sistem dan jaringan komputer untuk mengidentifikasi dan mencegah serangan	1.1 Pendahuluan dan pengenalan tentang malware 1.2 Teknik analysis malware 1.3 Jenis malware	<p>Kriteria:</p> <ul style="list-style-type: none"> • Komponen sikap • Komponen pengetahuan • Komponen keterampilan umum 	<ul style="list-style-type: none"> • Kuliah [TM:1x(3x50)]-Pert.7 • Diskusi [TM:1x(1x50)]-Pert.7 	<ul style="list-style-type: none"> • Ms.Teams • eLearning http://elearning.stikom-bali.ac.id/ • Studi Independen: Topik malware 	<p>Materi Pembelajaran</p> <ul style="list-style-type: none"> • Malware Analyst <p>Pustaka: Sikroski, M., & Honig, A. (2012). Pratical Malware Analysis The Hands-On Guide to</p>	

INSTITUT TEKNOLOGI DAN BISNIS STIKOM BALI
FAKULTAS INFORMATIKA DAN KOMPUTER
PROGRAM STUDI TEKNOLOGI INFORMASI

No. Dok	: FM/01/12/WRI/ITBSTIKOM
No. Revisi	: 00
Tgl. Berlaku	: 18 Agustus 2021
Halaman	: 10

	cyber dengan mengimplementasikan aspek-aspek keamanan informasi	1.4 Dasar Teknik analisis static 1.5 Malware analisis virtual mesin 1.6 Dasar Dynamic analisis 1.7	<ul style="list-style-type: none"> Komponen keterampilan khusus 		analisis [1x(4x119)]- Pert.7	Dissecting Malicious Software.	
UTS / Evaluasi Tengah Semester							25
8	CPMK-06-17 Mampu menjelaskan dan menguasai teknik pengamanan sistem dan jaringan komputer untuk mengidentifikasi dan mencegah serangan cyber dengan mengimplementasikan aspek-aspek keamanan informasi	1.1 Pengenalan WWW 1.2 Jenis serangan aplikasi berbasis web 1.3 Scanning vulnerability menggunakan Acunetix, W3AF, wpscan 1.4 Keamanan Server WWW 1.5 Kontrol akses 1.6 SSL 1.7 Keamanan Program CGI 1.8 Keamanan client WWW	Kriteria: <ul style="list-style-type: none"> Komponen sikap Komponen pengetahuan Komponen keterampilan umum Komponen keterampilan khusus. 	<ul style="list-style-type: none"> Kuliah [TM:1x(3x50)]- Pert.8 Diskusi [TM:1x(1x50)]- Pert.8 	<ul style="list-style-type: none"> Ms.Teams eLearning http://elearning.stikom-bali.ac.id/ Studi Independen: Topik keamanan web [1x(4x119)]- Pert.8 	Materi Pembelajaran <ul style="list-style-type: none"> Web Application Pustaka: Raharjo, B. (2017). Keamanan Informasi. Bandung (chapter 63)	

INSTITUT TEKNOLOGI DAN BISNIS STIKOM BALI
FAKULTAS INFORMATIKA DAN KOMPUTER
PROGRAM STUDI TEKNOLOGI INFORMASI

No. Dok	: FM/01/12/WRI/ITBSTIKOM
No. Revisi	: 00
Tgl. Berlaku	: 18 Agustus 2021
Halaman	: 11

9	<p>CPMK-06-17 Mampu menjelaskan dan menguasai teknik pengamanan sistem dan jaringan komputer untuk mengidentifikasi dan mencegah serangan cyber dengan mengimplementasikan aspek-aspek keamanan informasi</p> <p>CPMK-07-4 Mampu menjelaskan dan menguasai konsep dasar teori jaringan mahasiswa mampu memahami konsep jaringan komputer, mengetahui perangkat-perangkat jaringan, protokol jaringan, OSI dan TCP/IP model, konsep IP Address dan kelas-kelas dalam IP Address, Routing</p>	<p>1.1 Pengenalan jaringan wireless 1.2 Kelemahan jaringan wireless 1.3 Wifi Security 1.4 Jenis-jenis serangan jaringan wireless 1.5 Teknik pengamanan jaringan wireless 1.6 Pengujian keamanan wireless</p>	<p>Kriteria:</p> <ul style="list-style-type: none"> • Komponen sikap • Komponen pengetahuan • Komponen keterampilan umum • Komponen keterampilan khusus <p>Teknik:</p> <ul style="list-style-type: none"> • Tugas 2 : • Bagaimana Implementasi keamanan jaringan nirkabel pada perangkat Access Point. 	<ul style="list-style-type: none"> • Kuliah [TM:1x(3x50)]-Pert.9 • Diskusi [TM:1x(1x50)]-Pert.9 • Tugas 2: [PT+BM:(1+1)x(1x60)]-Pert.9 	<ul style="list-style-type: none"> • Ms.Teams • eLearning • http://elearning.stikom-bali.ac.id/ • Studi Independen: Topik keamanan wireless [1x(4x119)]-Pert.9 	<p>Materi Pembelajaran</p> <ul style="list-style-type: none"> • Wireless Security <p>Pustaka:</p> <ul style="list-style-type: none"> • Hakima Chaousgi, M. L.-M. (n.d.). Wireless and Mobile Network Security. Wiley. 	10
---	---	---	--	--	--	---	-----------

INSTITUT TEKNOLOGI DAN BISNIS STIKOM BALI
FAKULTAS INFORMATIKA DAN KOMPUTER
PROGRAM STUDI TEKNOLOGI INFORMASI

No. Dok	: FM/01/12/WRI/ITBSTIKOM
No. Revisi	: 00
Tgl. Berlaku	: 18 Agustus 2021
Halaman	: 12

	dengan media virtual seperti menggunakan packet tracer, memahami jaringan nirkabel, mengetahui serangan dalam jaringan dan mengetahui firewall.						
10	CPMK-07-4 Mampu menjelaskan dan menguasai konsep dasar teori jaringan mahasiswa mampu memahami konsep jaringan komputer, mengetahui perangkat-perangkat jaringan, protokol jaringan, OSI dan TCP/IP model, konsep IP Address dan kelas-kelas dalam IP Address, Routing	1.1 Pengertian firewall dan IDS 1.2 Jenis-jenis firewall dan IDS 1.3 Menerapkan IDS dengan snort 1.4 Menutup servis dengan firewall 1.5 Mekanisme pertahanan DDoS 1.6 Advanced Policy Firewall (APF)	Kriteria: <ul style="list-style-type: none"> • Komponen sikap • Komponen pengetahuan • Komponen keterampilan umum • Komponen keterampilan khusus 	<ul style="list-style-type: none"> • Kuliah [TM:1x(3x50)]- Pert.10 • Diskusi [TM:1x(1x50)]- Pert.10 	<ul style="list-style-type: none"> • Ms.Teams • eLearning • http://elearning.stikom-bali.ac.id/ • Studi Independen: Topik IDS [1x(4x119)]- Pert.10 	Materi Pembelajaran <ul style="list-style-type: none"> • Firewall & IDS Pustaka: Pribadi, H. (2008). Firewall Melindungi Jaringan dari DDoS Menggunakan Linux + Mikrotik. Andi Publisher	

INSTITUT TEKNOLOGI DAN BISNIS STIKOM BALI
FAKULTAS INFORMATIKA DAN KOMPUTER
PROGRAM STUDI TEKNOLOGI INFORMASI

No. Dok	: FM/01/12/WRI/ITBSTIKOM
No. Revisi	: 00
Tgl. Berlaku	: 18 Agustus 2021
Halaman	: 13

	dengan media virtual seperti menggunakan packet tracer, memahami jaringan nirkabel, mengetahui serangan dalam jaringan dan mengetahui firewall.						
11	CPMK-06-17 Mampu menjelaskan dan menguasai teknik pengamanan sistem dan jaringan komputer untuk mengidentifikasi dan mencegah serangan cyber dengan mengimplementasikan aspek-aspek keamanan informasi.	1.1 Pengertian Cyber Law 1.2 Sumber hukum cyberlaw 1.3 Cybercrime 1.4 Cybercrime sebagai kejahatan transnasional 1.5 Penangan Cybercrime 1.6 Kaitan dengan HaKi dan Cyber Law 1.7 Pelindungan konsumen dalam transaksi e-Commerce	Kriteria: <ul style="list-style-type: none"> • Komponen sikap • Komponen pengetahuan • Komponen keterampilan umum • Komponen keterampilan khusus Teknik: <ul style="list-style-type: none"> • Kuis 2 : • Bagaimana firewall dan IDS mampu mendeteksi serangan? 	<ul style="list-style-type: none"> • Kuliah [TM:1x(3x50)]-Pert.11 • Diskusi [TM:1x(1x50)]-Pert.11 • Kuis 2: [PT+BM:(1+1)x(1x60)]-Pert.11 	<ul style="list-style-type: none"> • Ms.Teams • eLearning • http://elearning.stikom-bali.ac.id/ • Studi Independen: Topik cyber law [1x(4x119)]-Pert.11 	Materi Pembelajaran <ul style="list-style-type: none"> • IT & Cyberlaw Pustaka: Situmeang, M.S (2020). <i>Cyber Law</i> , Bandung: Cakra 2020	5

INSTITUT TEKNOLOGI DAN BISNIS STIKOM BALI
FAKULTAS INFORMATIKA DAN KOMPUTER
PROGRAM STUDI TEKNOLOGI INFORMASI

No. Dok	: FM/01/12/WRI/ITBSTIKOM
No. Revisi	: 00
Tgl. Berlaku	: 18 Agustus 2021
Halaman	: 14

			<ul style="list-style-type: none"> • Sebutkan dan jelaskan model atau teknik filter packet pada firewall? • Apa tools untuk IDS dan Firewall? 				
12,13,14	<p>CPMK-06-17 Mampu menjelaskan dan menguasai teknik pengamanan sistem dan jaringan komputer untuk mengidentifikasi dan mencegah serangan cyber dengan mengimplementasikan aspek-aspek keamanan informasi</p> <p>CPMK-07-4 Mampu menjelaskan dan menguasai konsep dasar teori jaringan mahasiswa mampu memahami konsep jaringan komputer, mengetahui perangkat-</p>	1.1 Ketepatan didalam mengidentifikasi, menganalisa, merancang, serta mengimplentasikan suatu teknik keamanan cyber dalam hal sistem informasi dan jaringan komputer yang digunakan didalam mengelola data dan informasi.	<p>Kriteria:</p> <ul style="list-style-type: none"> • Komponen sikap • Komponen pengetahuan • Komponen keterampilan umum • Komponen keterampilan khusus <p>Teknik:</p> <ul style="list-style-type: none"> • Presentasi kelompok 	<ul style="list-style-type: none"> • Diskusi [TM:3x(4x50)] 	<ul style="list-style-type: none"> • Ms.Teams • eLearning • http://elearning.stikom-bali.ac.id/ • Analisa dan Desain project untuk pengamanan sistem dan jaringan komputer [1x(4x119)]-Pert.12 • Implemetnasi project untuk pengamanan sistem dan jaringan komputer 		

INSTITUT TEKNOLOGI DAN BISNIS STIKOM BALI
FAKULTAS INFORMATIKA DAN KOMPUTER
PROGRAM STUDI TEKNOLOGI INFORMASI

No. Dok	: FM/01/12/WRI/ITBSTIKOM
No. Revisi	: 00
Tgl. Berlaku	: 18 Agustus 2021
Halaman	: 15

	perangkat jaringan, protokol jaringan, OSI dan TCP/IP model, konsep IP Address dan kelas-kelas dalam IP Address, Routing dengan media virtual seperti menggunakan packet tracer, memahami jaringan nirkabel, mengetahui serangan dalam jaringan dan mengetahui firewall.				<p>[1x(4x119)]- Pert.13</p> <ul style="list-style-type: none"> • Presentasi project untuk pengamanan sistem dan jaringan komputer <p>[1x(4x119)]- Pert.14</p>			
UAS / Evaluasi Akhir Semester								30


Catatan sesuai dengan SN Dikti Permendikbud No 3/2020:

1. Capaian Pembelajaran Lulusan PRODI (CPL-PRODI) adalah kemampuan yang dimiliki oleh setiap lulusan PRODI yang merupakan internalisasi dari sikap, penguasaan pengetahuan dan ketrampilan sesuai dengan jenjang prodinya yang diperoleh melalui proses pembelajaran.
2. CPL yang dibebankan pada mata kuliah adalah beberapa capaian pembelajaran lulusan program studi (CPL-PRODI) yang digunakan untuk pembentukan/pengembangan sebuah mata kuliah yang terdiri dari aspek sikap, ketrampilan umum, ketrampilan khusus dan pengetahuan.
3. CP Mata kuliah (CPMK) adalah kemampuan yang dijabarkan secara spesifik dari CPL yang dibebankan pada mata kuliah, dan bersifat spesifik terhadap bahan kajian atau materi pembelajaran mata kuliah tersebut.
4. Sub-CP Mata kuliah (Sub-CPMK) adalah kemampuan yang dijabarkan secara spesifik dari CPMK yang dapat diukur atau diamati dan merupakan kemampuan akhir yang direncanakan pada tiap tahap pembelajaran, dan bersifat spesifik terhadap materi pembelajaran mata kuliah tersebut.

INSTITUT TEKNOLOGI DAN BISNIS STIKOM BALI
FAKULTAS INFORMATIKA DAN KOMPUTER
PROGRAM STUDI TEKNOLOGI INFORMASI

No. Dok	: FM/01/12/WRI/ITBSTIKOM
No. Revisi	: 00
Tgl. Berlaku	: 18 Agustus 2021
Halaman	: 16

5. Indikator penilaian kemampuan dalam proses maupun hasil belajar mahasiswa adalah pernyataan spesifik dan terukur yang mengidentifikasi kemampuan atau kinerja hasil belajar mahasiswa yang disertai bukti-bukti.
6. Kreteria Penilaian adalah patokan yang digunakan sebagai ukuran atau tolok ukur ketercapaian pembelajaran dalam penilaian berdasarkan indikator-indikator yang telah ditetapkan. Kreteria penilaian merupakan pedoman bagi penilai agar penilaian konsisten dan tidak bias. Kreteria dapat berupa kuantitatif ataupun kualitatif.
7. Teknik penilaian: tes dan non-tes.
8. Bentuk pembelajaran: Kuliah, Responsi, Tutorial, Seminar atau yang setara, Praktikum, Praktik Studio, Praktik Bengkel, Praktik Lapangan, Penelitian, Pengabdian Kepada Masyarakat dan/atau bentuk pembelajaran lain yang setara.
9. Metode Pembelajaran: *Small Group Discussion, Role-Play & Simulation, Discovery Learning, Self-Directed Learning, Cooperative Learning, Collaborative Learning, Contextual Learning, Project Based Learning*, dan metode lainnya yg setara.
10. Materi Pembelajaran adalah rincian atau uraian dari bahan kajian yg dapat disajikan dalam bentuk beberapa pokok dan sub-pokok bahasan.
11. Bobot penilaian adalah prosentasi penilaian terhadap setiap pencapaian sub-CPMK yang besarnya proposional dengan tingkat kesulitan pencapaian sub-CPMK tsb., dan totalnya 100%.
12. **TM**=Tatap Muka, **PT**=Penugasan Terstruktur, **BM**=Belajar Mandiri.

	RENCANA ASESMEN & EVALUASI Program Studi Sistem Informasi MK : Information System Security	No. Dok	: FM/02/12/WRI/ITBSTIKOM
		No. Revisi	: 00
		Tgl. Berlaku	: 18 Agustus 2021
		Halaman	: 17

Rencana Penilaian / Asesmen & Evaluasi (RAE), dan Rencana Tugas

Kode: TI213511	Bobot sks (T/P): T:4/P:	Rumpun MK: Praktik Profesional (BK10)	Smt: VII
OTORISASI	Penyusun RA & E 1. I Wayan Ardiyasa, S.Kom., M.MSI 2. Gde Sastrawangsa, S.T., M.T.	Ka PRODI I Wayan Ardiyasa, S.Kom., M.MSI.	

Pert. ke (1)	Sub CP-MK (2)	Bentuk Asesmen (Penilaian) (3)	Bobot (%) (4)
3	CPMK-06-17 Mampu menjelaskan dan menguasai teknik pengamanan sistem dan jaringan komputer untuk mengidentifikasi dan mencegah serangan cyber dengan mengimplementasikan aspek-aspek keamanan informasi	Tugas 1 – Studi Kasus Kriptografi dan Keamanan Jaringan. 1. Keakuratan implementasi teknik kriptografi. 2. Kejelasan dan kelengkapan dokumentasi dan laporan. 3. Pemahaman konseptual terhadap prinsip kriptografi dan keamanan jaringan. 4. Kreativitas dan efektivitas dalam menyusun solusi keamanan yang holistik. 5. Kemampuan untuk mengidentifikasi dan menjelaskan kelebihan dan kekurangan setiap teknik yang digunakan. 6. Ketepatan dan keefektifan dalam menggunakan teknik steganografi untuk menyembunyikan informasi.	10
4	CPMK-06-17 Mampu menjelaskan dan menguasai teknik pengamanan sistem dan jaringan komputer untuk mengidentifikasi dan mencegah serangan cyber dengan mengimplementasikan aspek-aspek keamanan informasi CPMK-07-4 Mampu menjelaskan dan menguasai konsep dasar teori jaringan mahasiswa mampu memahami konsep jaringan komputer, mengetahui perangkat-perangkat jaringan, protokol jaringan, OSI dan TCP/IP model, konsep	Kuis 1: 1. Menjelaskan tentang jenis-jenis kriptografi 2. Menjelaskan tentang jenis algoritma kriptografi 3. Menjelaskan implementasi teknologi kriptografi 4. Memahami teknik enkripsi dan dekripsi kriptografi	5

Pert. ke (1)	Sub CP-MK (2)	Bentuk Asesmen (Penilaian) (3)	Bobot (%) (4)
	IP Address dan kelas-kelas dalam IP Address, Routing dengan media virtual seperti menggunakan packet tracer, memahami jaringan nirkabel, mengetahui serangan dalam jaringan dan mengetahui firewall.		
UTS	Evaluasi Tengah Semester	Tes Tertulis	25
9	<p>CPMK-06-17 Mampu menjelaskan dan menguasai teknik pengamanan sistem dan jaringan komputer untuk mengidentifikasi dan mencegah serangan cyber dengan mengimplementasikan aspek-aspek keamanan informasi</p> <p>CPMK-07-4 Mampu menjelaskan dan menguasai konsep dasar teori jaringan mahasiswa mampu memahami konsep jaringan komputer, mengetahui perangkat-perangkat jaringan, protokol jaringan, OSI dan TCP/IP model, konsep IP Address dan kelas-kelas dalam IP Address, Routing dengan media virtual seperti menggunakan packet tracer, memahami jaringan nirkabel, mengetahui serangan dalam jaringan dan mengetahui firewall.</p>	<p>Tugas 2 – Implementasi keamanan jaringan nirkabel pada perangkat Access Point.</p> <ol style="list-style-type: none"> 1. Keakuratan Analisis Melakukan analisa dan deteksi celah keamanan pada wireless. 2. Kejelasan dan Kelengkapan Rencana Hardening: Kualitas rencana yang menyeluruh dan dapat diterapkan. 3. Efektivitas Implementasi: Seberapa baik teknik pengamanan mengurangi risiko keamanan. 4. Kemampuan dalam Testing dan Evaluasi: Efektivitas pengujian dalam menemukan kelemahan pasca-hardening. 5. Kualitas Dokumentasi: Kejelasan, kelengkapan, dan keakuratan dokumentasi proses dan hasil. 	10
11	<p>CPMK-06-17 Mampu menjelaskan dan menguasai teknik pengamanan sistem dan jaringan komputer untuk mengidentifikasi dan mencegah serangan cyber dengan mengimplementasikan aspek-aspek keamanan informasi</p>	<ul style="list-style-type: none"> • Kuis 2 – • Bagaimana firewall dan IDS mampu mendeteksi serangan? • Sebutkan dan jelaskan model atau teknik filter packet pada firewall? • Apa tools untuk IDS dan Firewall? 	5
UAS	Evaluasi Akhir Semester	Tes Tertulis	30
Sub Total Bobot			85
Persentase Kehadiran			15
Total Bobot Penilaian			100



RENCANA ASESMEN & EVALUASI
Program Studi Sistem Informasi
MK : Information System Security

No. Dok	: FM/02/12/WRI/ITBSTIKOM
No. Revisi	: 00
Tgl. Berlaku	: 18 Agustus 2021
Halaman	: 19

Pert. ke (1)	Sub CP-MK (2)	Bentuk Asesmen (Penilaian) (3)	Bobot (%) (4)
12,13,14	<p>CPMK-06-17 Mampu menjelaskan dan menguasai teknik pengamanan sistem dan jaringan komputer untuk mengidentifikasi dan mencegah serangan cyber dengan mengimplementasikan aspek-aspek keamanan informasi</p> <p>CPMK-07-4 Mampu menjelaskan dan menguasai konsep dasar teori jaringan mahasiswa mampu memahami konsep jaringan komputer, mengetahui perangkat-perangkat jaringan, protokol jaringan, OSI dan TCP/IP model, konsep IP Address dan kelas-kelas dalam IP Address, Routing dengan media virtual seperti menggunakan packet tracer, memahami jaringan nirkabel, mengetahui serangan dalam jaringan dan mengetahui firewall.</p>	1.	50
	50		
Total bobot penilaian			100
Total Akhir Nilai Presentasi Proyek (TANPP)			100

Nilai Akhir Mata Kuliah=50%(TANP)+50%(TANPP)

Portofolio penilaian & evaluasi proses dan hasil belajar setiap mahasiswa

Pert. ke	CPL	CPMK	Bentuk Penilaian (Bobot%)*		Bobot (%) CPMK	Nilai Mhs (0-100)	$\Sigma((\text{Nilai Mhs}) \times (\text{Sub-Bobot\%}))$	Ketercapaian CPL pd MK (%)	Diskripsi Evaluasi & Tindak lanjut perbaikan
			(4)	(5)					
3, 11	CPL06	CPMK-06-17	Tugas 1 Kuis 2 Kehadiran	10 5 7.5	22.5				
4,9, UTS, UAS	CPL06, CPL07	CPMK-06-19 CPMK-07-4	Kuis 1, Tugas 2 UTS UAS Kehadiran	5 10 25 30 7.5	77.5				
12, 13, 14	CPL06, CPL07	CPMK-06-19 CPMK-07-4			100				

Lampiran

A. Rencana Tugas & Rubrik Penilaian

1. Rencana Tugas 1 : Studi Kasus Kriptografi dan Keamanan Jaringan

a. **Tujuan Tugas:** Mengasah pemahaman mahasiswa mengenai prinsip dan aplikasi kriptografi, termasuk teknik enkripsi dan dekripsi, penggunaan kunci publik dan privat, serta aplikasi fungsi hash dan digital signature dalam konteks keamanan jaringan. Mahasiswa diharapkan dapat menerapkan teori ke dalam skenario praktis, mengembangkan keterampilan pemecahan masalah, dan menunjukkan pemahaman mereka tentang pentingnya keamanan informasi.

b. Uraian Tugas

i. **Obyek Tugas:** Mahasiswa akan diberikan skenario di mana mereka harus mengamankan transfer data antara dua pihak menggunakan teknik kriptografi yang sesuai. Data termasuk dokumen-dokumen sensitif yang membutuhkan kerahasiaan, integritas, dan autentikasi.

ii. Lingkup Tugas:

- 1) Mengimplementasikan kriptografi klasik (misalnya Caesar Cipher) untuk mengenkripsi pesan sederhana.
- 2) Menggunakan kriptografi modern (misalnya AES) untuk mengenkripsi dokumen.
- 3) Menerapkan kunci publik dan privat untuk enkripsi dan dekripsi dokumen.
- 4) Menggunakan fungsi hash untuk memverifikasi integritas dokumen.
- 5) Membuat dan mengimplementasikan digital signature untuk autentikasi dokumen.
- 6) Menyembunyikan informasi menggunakan teknik steganografi dalam gambar.

iii. Metode/Mekanisme tugas: Tugas merupakan tugas individu. Mahasiswa harus:

- 1) Menyusun algoritma untuk setiap teknik yang disebutkan.
- 2) Mengimplementasikan algoritma tersebut dalam bentuk kode atau menggunakan tools kriptografi yang tersedia.
- 3) Menyiapkan dokumentasi yang menjelaskan setiap langkah proses, termasuk pilihan algoritma, alasan penggunaan, dan potensi kelemahan.
- 4) Membuat laporan yang mencakup demonstrasi aplikasi dari setiap teknik, dilengkapi dengan screenshot atau tautan ke kode sumber.

iv. Luaran Tugas:

- 1) Kode sumber untuk setiap teknik kriptografi yang diimplementasikan.
- 2) Dokumentasi yang mendetail termasuk penjelasan teori, kode, dan analisis hasil.

- 3) Laporan akhir yang menyajikan solusi keamanan secara keseluruhan, termasuk bagaimana setiap teknik kriptografi berkontribusi terhadap keamanan data dalam skenario yang diberikan.

c. Kriteria Penilaian:

i. Parameter Penilaian:

- 1) Keakuratan implementasi teknik kriptografi.
- 2) Kejelasan dan kelengkapan dokumentasi dan laporan.
- 3) Pemahaman konseptual terhadap prinsip kriptografi dan keamanan jaringan.
- 4) Kreativitas dan efektivitas dalam menyusun solusi keamanan yang holistik.
- 5) Kemampuan untuk mengidentifikasi dan menjelaskan kelebihan dan kekurangan setiap teknik yang digunakan.
- 6) Ketepatan dan keefektifan dalam menggunakan teknik steganografi untuk menyembunyikan informasi.

ii. Skala Penilaian:

- 1) $85 < \text{Nilai} \leq 100$: A
- 2) $80 < \text{Nilai} \leq 85$: AB
- 3) $70 < \text{Nilai} \leq 80$: B
- 4) $65 < \text{Nilai} \leq 70$: BC
- 5) $55 < \text{Nilai} \leq 65$: C
- 6) $40 < \text{Nilai} \leq 55$: D
- 7) $0 \leq \text{Nilai} \leq 40$: E

2. Rencana Tugas 2: Implementasi keamanan jaringan nirkabel pada perangkat Access Point.

a. Tujuan Tugas:

Tujuan dari tugas ini adalah untuk memperkuat keamanan jaringan nirkabel melalui konfigurasi dan pengaturan yang tepat pada perangkat Access Point (AP). Mahasiswa akan menganalisis potensi risiko keamanan, menerapkan strategi pengamanan, dan mengevaluasi efektivitas langkah-langkah tersebut. Tugas ini bertujuan mengembangkan kemampuan mahasiswa dalam menerapkan keamanan jaringan praktis dan memahami implikasi keamanan dalam konfigurasi jaringan nirkabel.

b. Uraian Tugas:

i. Obyek Tugas: Perangkat Access Point yang digunakan dalam jaringan nirkabel di lingkungan yang mirip dengan lingkungan kantor kecil atau rumah.

ii. Lingkup Tugas:

- 1) Analisis keamanan jaringan nirkabel saat ini pada Access Point.
- 2) Penerapan pengaturan keamanan yang diperkuat seperti WPA3, MAC address filtering, SSID hiding, dan pengaturan firewall.
- 3) Evaluasi kinerja jaringan setelah implementasi keamanan untuk menentukan dampaknya terhadap kinerja dan aksesibilitas.

iii. Metode/Mekanisme tugas: Tugas merupakan tugas individu. Mahasiswa harus melakukan:

- 1) Analisis Risiko: Melakukan audit pada pengaturan keamanan AP saat ini dan mengidentifikasi kelemahan atau celah keamanan.
- 2) Rencana Pengamanan: Menyusun strategi pengamanan yang mencakup pengaturan teknis pada AP.
- 3) Implementasi: Melakukan konfigurasi keamanan pada AP sesuai dengan strategi yang telah disusun.
- 4) Testing dan Evaluasi: Menguji jaringan untuk mengevaluasi keefektifan pengaturan keamanan dan mengidentifikasi potensi degradasi kinerja.
- 5) Dokumentasi: Menyusun laporan yang mendetail mengenai prosedur, hasil pengujian, dan rekomendasi keamanan.

iv. Luaran Tugas:

- 1) Laporan analisis risiko keamanan jaringan nirkabel.
- 2) Dokumentasi rencana pengamanan dan konfigurasi.
- 3) Hasil evaluasi keefektifan keamanan.
- 4) Dokumentasi lengkap termasuk langkah-langkah yang diambil, analisis hasil, dan rekomendasi.

c. Kriteria Penilaian:

i. Parameter Penilaian:

- 1) Keakuratan Analisis Keamanan: Kemampuan untuk mengidentifikasi dan memprioritaskan risiko keamanan.
- 2) Kejelasan dan Kelengkapan Rencana Pengamanan: Kualitas rencana yang detail dan dapat diimplementasikan.
- 3) Efektivitas Implementasi: Seberapa baik pengaturan keamanan mengurangi risiko yang diidentifikasi.
- 4) Kemampuan dalam Testing dan Evaluasi: Efektivitas pengujian dalam menemukan kelemahan pasca-implementasi.
- 5) Kualitas Dokumentasi: Kejelasan, kelengkapan, dan keakuratan dokumentasi proses dan hasil.

ii. Skala Penilaian:

- 1) $85 < \text{Nilai} \leq 100$: A
- 2) $80 < \text{Nilai} \leq 85$: AB
- 3) $70 < \text{Nilai} \leq 80$: B
- 4) $65 < \text{Nilai} \leq 70$: BC
- 5) $55 < \text{Nilai} \leq 65$: C
- 6) $40 < \text{Nilai} \leq 55$: D
- 7) $0 \leq \text{Nilai} \leq 40$: E

1. Rencana Kuis 1:

a. Tujuan Kuis :

Memberikan pemahaman tentang teknik kriptografi dan steganografi yang bisa diimplementasikan didalam segala jenis aspek didalam kehidupan manusia untuk mengamankan data maupun informasi dari attacker.

b. Uraian Kuis

i. **Obyek Kuis:** Teknik Kriptografi dan steganografi didalam implementasinya pada teknologi yang digunakan.

ii. **Lingkup Kuis:**

- 1) Menjelaskan tentang jenis-jenis kriptografi
- 2) Menjelaskan tentang jenis algoritma kriptografi
- 3) Menjelaskan implementasi teknologi kriptografi
- 4) Memahami teknik enkripsi dan dekripsi kriptografi

iii. **Metode/Mekanisme kuis:** Kuis merupakan dikerjakan secara individu didalam kelas.

- 1) Soal pilihan ganda dengan minimal jumlah soal sebanyak 20 soal.
- 2) Setiap soal memiliki 4 pilihan jawaban.
- 3) Hanya ada 1 jawaban yang benar untuk setiap soal.

iv. **Luaran Kuis:** Jawaban kuis yang sudah diisi oleh mahasiswa.

c. Kriteria Penilaian

i. **Parameter Penilaian: Ketepatan jawaban 100%**

ii. **Skala penilaian**

- 1) $85 < \text{Nilai} \leq 100$: A
- 2) $80 < \text{Nilai} \leq 85$: AB
- 3) $70 < \text{Nilai} \leq 80$: B
- 4) $65 < \text{Nilai} \leq 70$: BC
- 5) $55 < \text{Nilai} \leq 65$: C
- 6) $40 < \text{Nilai} \leq 55$: D
- 7) $0 \leq \text{Nilai} \leq 40$: E

2. Rencana Kuis 2:

a. Tujuan Kuis:

Memberikan mahasiswa teknik analisis dan evaluasi penggunaan firewall dan IDS

b. Uraian Kuis

i. **Obyek Kuis:** Bagaimana implementasi firewall dan IDS pada sistem dan jaringan computer.

ii. **Lingkup Kuis:**

- 1) Bagaimana firewall dan IDS mampu mendeteksi serangan?
- 2) Sebutkan dan jelaskan model atau teknik filter packet pada firewall?
- 3) Apa tools untuk IDS dan Firewall?

iii. **Metode/Mekanisme Kuis:** Tugas merupakan tugas individu

- 1) Soal pilihan ganda dengan minimal jumlah soal sebanyak 20 soal.
- 2) Setiap soal memiliki 4 pilihan jawaban.
- 3) Hanya ada 1 jawaban yang benar untuk setiap soal.

c. Kriteria Penilaian

i. **Luaran Kuis:** Jawaban kuis yang sudah diisi oleh mahasiswa.

ii. **Parameter Penilaian:** Ketepatan jawaban 100%

iii. **Skala Penilaian:**

- 1) $85 < \text{Nilai} \leq 100$: A
- 2) $80 < \text{Nilai} \leq 85$: AB
- 3) $70 < \text{Nilai} \leq 80$: B
- 4) $65 < \text{Nilai} \leq 70$: BC
- 5) $55 < \text{Nilai} \leq 65$: C
- 6) $40 < \text{Nilai} \leq 55$: D
- 7) $0 \leq \text{Nilai} \leq 40$: E

3. Rencana Project: Hardening Sistem untuk Aplikasi E-commerce

a. Tujuan Project:

Tujuan dari tugas ini adalah untuk memperkuat keamanan sistem yang mendukung aplikasi e-commerce. Mahasiswa akan mengidentifikasi potensi kerentanan dan menerapkan teknik hardening yang efektif untuk melindungi sistem dari ancaman keamanan yang mungkin terjadi. Tugas ini bertujuan mengembangkan pemahaman mahasiswa tentang pentingnya keamanan aplikasi dalam lingkungan bisnis yang terhubung dan cara-cara praktis untuk mengimplementasikan keamanan yang kuat.

b. Uraian Project:

i. **Obyek Project:** Aplikasi e-commerce yang menyediakan layanan transaksi online, termasuk pembayaran, pengelolaan inventori, dan manajemen data pelanggan.

ii. Lingkup Project:

- 1) Analisis kerentanan sistem yang mungkin ada dalam aplikasi e-commerce.
- 2) Pengembangan strategi untuk hardening server web, basis data, dan infrastruktur jaringan.
- 3) Penerapan langkah-langkah keamanan seperti firewall, enkripsi, dan otentikasi dua faktor.

iii. **Metode/Mekanisme Project:** Tugas merupakan tugas kelompok. Mahasiswa harus:

- 1) Analisis Sistem: Melakukan audit keamanan pada aplikasi e-commerce untuk mengidentifikasi kelemahan atau kerentanan dalam sistem.
- 2) Penyusunan Rencana Hardening: Menyusun rencana hardening yang menyeluruh berdasarkan hasil analisis.
- 3) Implementasi: Menerapkan teknik hardening pada aplikasi e-commerce sesuai dengan rencana yang telah disusun.
- 4) Testing dan Evaluasi: Menguji sistem untuk memastikan bahwa langkah-langkah hardening telah diterapkan dengan benar dan efektif.
- 5) Dokumentasi: Menyusun dokumentasi yang menjelaskan proses dan hasil dari hardening sistem, termasuk langkah-langkah yang diambil dan justifikasi untuk setiap keputusan.

iv. Luaran Project

- 1) Dokumen analisis kerentanan yang mendetail.
- 2) Rencana hardening yang lengkap.
- 3) Laporan implementasi dan hasil testing.
- 4) Dokumentasi lengkap dari seluruh proses.

- 5) Publikasi Tugas/ Project (luaran) melalui platform Medium (<https://medium.com/>)

c. Parameter Penilaian Project

i. Kriteria Penilaian

- 1) Keakuratan Analisis Kerentanan: Kemampuan untuk mengidentifikasi dan memprioritaskan kerentanan dalam aplikasi.
- 2) Kejelasan dan Kelengkapan Rencana Hardening: Kualitas rencana yang menyeluruh dan dapat diterapkan.
- 3) Efektivitas Implementasi: Seberapa baik teknik hardening mengurangi risiko keamanan.
- 4) Kemampuan dalam Testing dan Evaluasi: Efektivitas pengujian dalam menemukan kelemahan pasca-hardening.
- 5) Kualitas Dokumentasi: Kejelasan, kelengkapan, dan keakuratan dokumentasi proses dan hasil.

ii. Skala Penilaian:

- 1) $85 < \text{Nilai} \leq 100$: A
- 2) $80 < \text{Nilai} \leq 85$: AB
- 3) $70 < \text{Nilai} \leq 80$: B
- 4) $65 < \text{Nilai} \leq 70$: BC
- 5) $55 < \text{Nilai} \leq 65$: C
- 6) $40 < \text{Nilai} \leq 55$: D
- 7) $0 \leq \text{Nilai} \leq 40$: E

1. Rubrik Tugas 1:

BOBOT PENILAIAN	KRITERIA PENILAIAN	0 <= Nilai <= 40 : E	40 < Nilai <= 55 : D	55 < Nilai <= 65 : C	65 < Nilai <= 70 : BC	70 < Nilai <= 80 : B	80 < Nilai <= 85 : AB	85 < Nilai <= 100 : A	NILAI MHS
Keakuratan Implementasi Teknik Kriptografi : 20%	Pengetahuan Keterampilan Khusus	Implementasi salah atau tidak berfungsi sama sekali.	Implementasi memiliki banyak kesalahan dan hanya sebagian yang berfungsi.	Teknik diimplementasikan dengan cara yang dasar dan memiliki kesalahan yang cukup signifikan.	Ada beberapa kesalahan yang mempengaruhi fungsi dari kriptografi.	Teknik kriptografi diimplementasikan dengan benar, beberapa kesalahan kecil.	Implementasi hampir sempurna dengan kesalahan minimal.	Teknik kriptografi diimplementasikan dengan sangat akurat, tanpa kesalahan.	
Kejelasan dan Kelengkapan Dokumentasi dan Laporan: 10%	Pengetahuan Keterampilan Khusus	Dokumentasi sangat kurang atau hampir tidak ada.	Dokumentasi minim dan banyak kekurangan detail.	Dokumentasi kurang jelas dan tidak lengkap.	Dokumentasi umumnya baik tapi kekurangan beberapa detail penting.	Dokumentasi cukup jelas dan lengkap namun ada beberapa bagian yang tidak jelas.	Dokumentasi jelas dan lengkap dengan detail minor yang kurang.	Dokumentasi sangat jelas, lengkap, dan rinci.	
Pemahaman Konseptual terhadap Prinsip Kriptografi dan Keamanan Jaringan: 10%	Pengetahuan Keterampilan Khusus	Tidak menunjukkan pemahaman.	Pemahaman yang sangat terbatas.	Pemahaman minimal dan banyak kesalahan konseptual.	Pemahaman dasar dan beberapa kesalahan konseptual.	Pemahaman yang cukup dan penjelasan umum yang baik.	Pemahaman yang baik dan penjelasan yang jelas tentang sebagian besar konsep.	Pemahaman mendalam dan dapat menjelaskan dengan detail semua konsep.	

BOBOT PENILAIAN	KRITERIA PENILAIAN	0 <= Nilai <= 40 : E	40 < Nilai <= 55 : D	55 < Nilai <= 65 : C	65 < Nilai <= 70 : BC	70 < Nilai <= 80 : B	80 < Nilai <= 85 : AB	85 < Nilai <= 100 : A	NILAI MHS
Kreativitas dan Efektivitas dalam Menyusun Solusi Keamanan yang Holistik: 20%	Pengetahuan Keterampilan Khusus	Solusi tidak praktis atau tidak ada kreativitas.	Solusi tidak kreatif dan kurang efektif.	Kurang kreativitas dan efektivitas dalam solusi.	Solusi memiliki beberapa aspek kreatif namun tidak sepenuhnya efektif.	Solusi cukup kreatif dan efektif namun bisa lebih holistik.	Solusi kreatif dan efektif dengan beberapa peningkatan yang mungkin.	Solusi sangat kreatif, efektif, dan lengkap.	
Kemampuan untuk Mengidentifikasi dan Menjelaskan Kelebihan dan Kekurangan Setiap Teknik yang Digunakan: 20%	Pengetahuan Keterampilan Khusus	Tidak mampu mengidentifikasi atau menjelaskan kelebihan atau kekurangan.	Penjelasan sangat minimal dan kurang detail.	Menunjukkan pemahaman dasar kelebihan dan kekurangan namun kurang detail.	Penjelasan cukup tapi masih ada ruang untuk detail yang lebih spesifik.	Penjelasan baik mengenai kelebihan dan kekurangan dengan beberapa detail yang kurang.	Penjelasan sangat baik dengan beberapa minor oversight pada detail.	Penjelasan sangat detail dan lengkap mengenai kelebihan dan kekurangan.	
Ketepatan dan Keefektifan dalam Menggunakan Teknik Steganografi untuk Menyembunyikan Informasi: 20%	Pengetahuan Keterampilan Khusus	Tidak efektif; informasi mudah terdeteksi atau rusak.	Penggunaan steganografi dengan efektivitas yang rendah; beberapa informasi dapat terdeteksi.	Penggunaan steganografi cukup efektif tetapi masih ada ruang untuk penyempurnaan.	Efektifitas cukup namun masih dapat ditingkatkan.	Penggunaan steganografi efektif dengan hasil yang aman.	Sangat efektif dengan minimal risiko deteksi.	Penggunaan steganografi sangat efektif dan benar-benar menyembunyikan informasi tanpa deteksi.	

2. Rubrik Tugas 2

BOBOT PENILAIAN	KRITERIA PENILAIAN	0 <= Nilai <= 40 : E	40 < Nilai <= 55 : D	55 < Nilai <= 65 : C	65 < Nilai <= 70 : BC	70 < Nilai <= 80 : B	80 < Nilai <= 85 : AB	85 < Nilai <= 100 : A	NILAI MHS
Keakuratan Analisis Keamanan: 20%	Pengetahuan Keterampilan Khusus	Tidak mengidentifikasi risiko atau analisis sangat tidak akurat.	Mengidentifikasi sedikit risiko; banyak kesalahan dalam analisis.	Mengidentifikasi beberapa risiko utama; analisis kurang detail.	Analisis cukup akurat, tapi masih ada beberapa risiko yang terlewat.	Analisis risiko yang baik dan cukup detail.	Analisis sangat akurat, hanya sedikit risiko minor yang terlewat.	Analisis risiko yang sangat akurat dan mendalam; semua risiko diidentifikasi.	
Kejelasan dan Kelengkapan Rencana Pengamanan: 20%	Pengetahuan Keterampilan Khusus	Rencana sangat tidak jelas atau tidak praktis; banyak aspek penting yang terlewat.	Rencana kurang jelas dan kurang lengkap; hanya mencakup beberapa aspek.	Rencana cukup jelas dan cukup lengkap; beberapa aspek penting masih terlewat.	Rencana cukup detail dan mencakup kebanyakan aspek keamanan.	Rencana baik, lengkap, dan logis; mencakup semua aspek penting.	Rencana sangat lengkap dan detail; hampir sempurna.	Rencana sangat detail dan sangat lengkap; mencakup semua aspek keamanan dengan sempurna.	
Efektivitas Implementasi: 25%	Pengetahuan Keterampilan Khusus	Implementasi tidak efektif; keamanan tidak ditingkatkan atau bahkan memburuk.	Implementasi sedikit efektif; hanya sedikit peningkatan keamanan.	Implementasi cukup efektif; beberapa peningkatan keamanan yang nyata.	Implementasi efektif; keamanan jaringan jelas ditingkatkan.	Implementasi sangat efektif; peningkatan keamanan yang signifikan.	Implementasi hampir sempurna; keamanan jaringan sangat ditingkatkan.	Implementasi sempurna; keamanan jaringan optimal dan semua risiko diatasi.	
Kemampuan dalam Testing dan Evaluasi: 25%	Pengetahuan Keterampilan Khusus	Tidak melakukan pengujian atau pengujian yang	Pengujian minim dan tidak efektif, banyak	Pengujian cukup, tetapi tidak semua masalah	Pengujian efektif; kebanyakan masalah	Pengujian sangat baik; mengidentifikasi hampir semua	Pengujian sangat efektif dan menyeluruh;	Pengujian luar biasa; semua masalah keamanan	

BOBOT PENILAIAN	KRITERIA PENILAIAN	0 <= Nilai <= 40 : E	40 < Nilai <= 55 : D	55 < Nilai <= 65 : C	65 < Nilai <= 70 : BC	70 < Nilai <= 80 : B	80 < Nilai <= 85 : AB	85 < Nilai <= 100 : A	NILAI MHS
		sangat tidak memadai.	masalah yang tidak terdeteksi.	keamanan terdeteksi.	keamanan terdeteksi.	masalah keamanan.	semua masalah kecil teridentifikasi.	teridentifikasi dan diatasi.	
Kualitas Dokumentasi: 10%	Pengetahuan Keterampilan Khusus	Dokumentasi sangat minim dan tidak jelas, tidak membantu pemahaman.	Dokumentasi kurang lengkap dan tidak selalu jelas.	Dokumentasi cukup lengkap dan cukup jelas.	Dokumentasi cukup baik dan relatif lengkap, detail masih bisa ditingkatkan.	Dokumentasi sangat baik, jelas dan cukup rinci.	Dokumentasi sangat rinci dan sangat jelas, hampir sempurna.	Dokumentasi luar biasa dalam kejelasan, kelengkapan, dan detail, sangat mendukung pemahaman.	

3. Rubrik Kuis 1

BOBOT PENILAIAN	KRITERIA PENILAIAN	0 <= Nilai <= 40 : E	40 < Nilai <= 55 : D	55 < Nilai <= 65 : C	65 < Nilai <= 70 : BC	70 < Nilai <= 80 : B	80 < Nilai <= 85 : AB	85 < Nilai <= 100 : A	NILAI MHS
Ketepatan jawaban 100%.	Pengetahuan Keterampilan Khusus	Sesuai kunci jawaban	Sesuai kunci jawaban	Sesuai kunci jawaban	Sesuai kunci jawaban	Sesuai kunci jawaban	Sesuai kunci jawaban	Sesuai kunci jawaban	

4. Rubrik Kuis 2

BOBOT PENILAIAN	KRITERIA PENILAIAN	0 <= Nilai <= 40 : E	40 < Nilai <= 55 : D	55 < Nilai <= 65 : C	65 < Nilai <= 70 : BC	70 < Nilai <= 80 : B	80 < Nilai <= 85 : AB	85 < Nilai <= 100 : A	NILAI MHS
Ketepatan jawaban 100%.	Pengetahuan Keterampilan Khusus	Sesuai kunci jawaban	Sesuai kunci jawaban	Sesuai kunci jawaban	Sesuai kunci jawaban	Sesuai kunci jawaban	Sesuai kunci jawaban	Sesuai kunci jawaban	

5. Rubrik Project:

BOBOT PENILAIAN	KRITERIA PENILAIAN	0 <= Nilai <= 40 : E	40 < Nilai <= 55 : D	55 < Nilai <= 65 : C	65 < Nilai <= 70 : BC	70 < Nilai <= 80 : B	80 < Nilai <= 85 : AB	85 < Nilai <= 100 : A	NILAI MHS
Keakuratan Analisis Kerentanan: 20%	Pengetahuan Keterampilan Khusus	Tidak mengidentifikasi kerentanan utama atau memiliki pemahaman yang salah.	Mengidentifikasi beberapa kerentanan tetapi dengan banyak kesalahan.	Mengidentifikasi kerentanan yang relevan, tetapi dengan beberapa kekurangan analisis.	Analisis yang cukup akurat tetapi masih ada kekurangan detail.	Analisis yang baik dan cukup detail tentang kerentanan utama.	Analisis yang sangat baik dan mendetail, kecil kemungkinan meninggalkan kerentanan penting.	Analisis yang luar biasa, lengkap dan mendalam mengenai semua kerentanan penting.	
Kejelasan dan Kelengkapan Rencana Hardening: 20%	Pengetahuan Keterampilan Khusus	Rencana tidak jelas atau tidak logis, dengan banyak kekurangan dalam keamanan.	Rencana kurang detail dan tidak menyeluruh, hanya mencakup beberapa	Rencana cukup jelas tetapi tidak menyeluruh, beberapa area keamanan penting tidak tercakup.	Rencana cukup lengkap namun masih ada beberapa aspek yang bisa diperbaiki.	Rencana baik dan mencakup sebagian besar area keamanan penting dengan cukup detail.	Rencana sangat lengkap dan terstruktur dengan baik, hampir mencakup semua aspek.	Rencana sangat detail dan menyeluruh, mencakup semua aspek keamanan yang penting	

BOBOT PENILAIAN	KRITERIA PENILAIAN	0 <= Nilai <= 40 : E	40 < Nilai <= 55 : D	55 < Nilai <= 65 : C	65 < Nilai <= 70 : BC	70 < Nilai <= 80 : B	80 < Nilai <= 85 : AB	85 < Nilai <= 100 : A	NILAI MHS
			aspek keamanan.					dengan sangat baik.	
Efektivitas Implementasi: 25%	Pengetahuan Keterampilan Khusus	Implementasi gagal mengurangi risiko dan mungkin memperburuk kerentanan.	Implementasi sedikit mengurangi risiko tetapi masih banyak kekurangan.	Implementasi cukup efektif, mengurangi beberapa risiko tetapi masih ada kekurangan.	Implementasi cukup baik, namun masih ada ruang untuk peningkatan efektivitas.	Implementasi baik dan mengurangi sebagian besar risiko yang diidentifikasi.	Implementasi sangat baik dan efektif, meninggalkan sangat sedikit risiko.	Implementasi luar biasa dan optimal, mengeliminasi atau mengurangi risiko keamanan secara signifikan.	
Kemampuan dalam Testing dan Evaluasi: 25%	Pengetahuan Keterampilan Khusus	Tidak melakukan pengujian atau evaluasi, atau melakukan pengujian yang salah.	Pengujian minimal dan tidak efektif dalam mengungkap masalah.	Pengujian cukup tapi tidak mencakup semua aspek atau gagal mengungkap beberapa masalah.	Pengujian cukup efektif, mengungkap kebanyakan masalah tetapi masih ada yang terlewat.	Pengujian yang baik dan efektif, mengungkap sebagian besar masalah keamanan.	Pengujian sangat efektif, hanya meninggalkan masalah kecil yang tidak terungkap.	Pengujian luar biasa, mengungkap semua masalah keamanan potensial.	

BOBOT PENILAIAN	KRITERIA PENILAIAN	0 <= Nilai <= 40 : E	40 < Nilai <= 55 : D	55 < Nilai <= 65 : C	65 < Nilai <= 70 : BC	70 < Nilai <= 80 : B	80 < Nilai <= 85 : AB	85 < Nilai <= 100 : A	NILAI MHS
Kualitas Dokumentasi: 10%	Pengetahuan Keterampilan Khusus	Dokumentasi sangat minim, tidak jelas atau salah.	Dokumentasi ada tetapi sering tidak jelas dan tidak lengkap.	Dokumentasi cukup jelas dan lengkap namun masih ada beberapa kekurangan.	Dokumentasi umumnya baik dan relatif lengkap tetapi bisa lebih detail.	Dokumentasi baik, jelas, dan cukup lengkap dengan detail yang memadai.	Dokumentasi sangat baik, sangat jelas, dan hampir sempurna.	Dokumentasi luar biasa dalam kejelasan, kelengkapan, dan detail, sangat mendukung pemahaman.	

6. Rubrik Presentasi:

BOBOT PENILAIAN	KRITERIA PENILAIAN	0 <= Nilai <= 40 : E	40 < Nilai <= 55 : D	55 < Nilai <= 65 : C	65 < Nilai <= 70 : BC	70 < Nilai <= 80 : B	80 < Nilai <= 85 : AB	85 < Nilai <= 100 : A	NILAI MHS1, dst
Pengelolaan Presentasi: 20%	Pengetahuan Keterampilan Umum	Tidak ada struktur; acak-acakan	Kurang terstruktur; banyak kesalahan	Cukup terstruktur; beberapa kesalahan	Terstruktur dengan sedikit kesalahan	Terstruktur dengan kesalahan minor	Hampir sempurna; satu atau dua kesalahan kecil	Terstruktur dengan sangat baik	
Pengenalan Penyaji: 10%	Sikap Keterampilan Umum	Tidak memperkenalkan diri atau tim	Pengenalan sangat singkat dan tidak jelas	Pengenalan cukup namun kurang menarik	Pengenalan jelas dengan sedikit kesalahan	Pengenalan menarik dengan kesalahan minor	Pengenalan menarik dan hampir tanpa kesalahan	Pengenalan menarik dan sangat baik	

BOBOT PENILAIAN	KRITERIA PENILAIAN	0 <= Nilai <= 40 : E	40 < Nilai <= 55 : D	55 < Nilai <= 65 : C	65 < Nilai <= 70 : BC	70 < Nilai <= 80 : B	80 < Nilai <= 85 : AB	85 < Nilai <= 100 : A	NILAI MHS1, dst
Penyampaian: 30%	Sikap Keterampilan Umum	Tidak jelas; banyak kesalahan	Kurang jelas; banyak kesalahan	Cukup jelas; beberapa kesalahan	Jelas dengan sedikit kesalahan	Jelas dengan kesalahan minor	Hampir baik; satu atau dua kesalahan kecil	Penyampaian jelas dan sangat baik	
Menjawab Pertanyaan: 40%	Sikap Pengetahuan Keterampilan Khusus	Tidak menjawab atau jawaban salah	Jawaban kurang tepat; banyak kesalahan	Jawaban cukup; beberapa kesalahan	Jawaban jelas dengan sedikit kesalahan	Jawaban tepat dengan kesalahan minor	Hampir tepat; satu atau dua kesalahan kecil	Menjawab dengan tepat dan sangat baik	