RENCANA PEMBELAJARAN SEMESTER GANJIL 2018/2019
PROGRAM STUDI MANAJEMEN INFORMASI KESEHATAN
UNIVERSITAS ESA UNGGUL

Mata kuliah	**:**	Aspek Keamanan Dan Kerahasiaan Si/Sirs	**Kode MK**	**:**	MIK550
Mata kuliah prasyarat	**:**	-	**Bobot MK**	**:**	2 sks
Dosen Pengampu	**:**	1. Nauri Anggita T., SKM, MKM 2. Harfebi Fryonanda, S.Kom, M.Kom	**Kode Dosen**	**:**	7502
Alokasi Waktu	**:**	100 Menit			
Deskripsi Ringkas	**:**	Pada mata kuliah aspek kemanan dan kerahasiaan system informasi dikaji mengenai proses pengamanan pada informasi, tidak terbatas pada teknologi yang memproses, menyimpan dan mengirimkan informasi, *stakheloder* yang mengelola informasi dan proses bisnis yang menggunakan informasi terkait.			
Capaian Pembelajaran	**:**	1. Mahasiswa mampu memahami prinsip dasar keamanan informasi 2. Mahasiswa mengetahui standar dan framework *compliance* yang mengatur keamanan informasi 3. Mahasiswa dapat memberikan solusi permasalahan terkait bagaimana melindungi aset informasi 4. Mahasiswa dapat mengeksplorasi beberapa kerentanan yang membuat keamanan informasi tidak terjamin 5. Mahasiswa dapat mengeksplorasi proses perlindungan terhadap informasi dari sisi teknis maupun sisi prosedural			
Buku Acuan	**:**	1. Rhodes M and Oesley., Information Security The Complete Reference, 2nd Edition, Mc Graw Hill Education, 2013. 2. Peltier T. R., Information Security Policies and Procedures, A Practitioner's Reference, 2nd Edition, CRC Press LLC, 2004 3. Michael E. Whitman and Herbert J. Mattord., *Management of Information Security,* Fourth Edition, Stamford: 2014. 4. Johannes A. Buchman, et al., *Introduction to Public Key Infrastructures*, London: 2013. 5. International Standard (ISO/ IEC) 27001. *Information Technology – techniques – Information Security Management Systems – Requirements.* Geneva: 2013 6. Andrew Muller, et al., *Open Web Application Security (OWASP) Project Testing Guide - Release.*			

SESI	KEMAMPUAN AKHIR	MATERI PEMBELAJARAN	BENTUK PEMBELAJARAN	SUMBER PEMBELAJARAN	INDIKATOR PENILAIAN
1	Mahasiswa mampu menguraikan konsep prinsip dasar mengenai keamanan informasi	Information Security Overview & Basic Principle	1. Metode *contextual instruction* 2. Media: kelas, komputer, *LCD, whiteboard*	1. Rhodes M and Oesley., Information Security The Complete Reference, 2nd Edition, Mc Graw Hill Education, 201 chapter 1 & chapter 4 2. Michael E. Whitman and Herbert J. Mattord., *Management of Information Security,* Fourth Edition, Stamford: 2014. Chapter 1 & Chapter 2	Menguraikan konsep dan prinsip dasar dalam keamanan informasi
2	Mahasiswa mampu menjabarkan berbagai *compliance standard* dan framework yang mengatur keamanan informasi	*Compliance Standard for Information Security*	1. Media: *contextual instruction* 2. Media: kelas, komputer, LCD, *whiteboard*	1. Rhodes M and Oesley., Information Security The Complete Reference, 2nd Edition, Mc Graw Hill Education, 201 chapter 3	Menjabarkan berbagai *compliance standard* dan framework yang mengatur keamanan informasi
3	Mahasiswa mampu menguraikan Siklus hidup keamanan informasi dan implementasi dari Sistem Manajemen Keamanan Informasi	*Information Security Management System* (ISMS)	1. Media: *contextual instruction* *2.* Media: kelas, komputer, LCD, *whiteboard*	2. International Standard (ISO/ IEC) 27001. *Information Technology – techniques – Information Security Management Systems – Requirements.* Geneva: 2013	Menguraikan Siklus hidup keamanan informasi dan implementasi dari Sistem Manajemen Keamanan

SESI	KEMAMPUAN AKHIR	MATERI PEMBELAJARAN	BENTUK PEMBELAJARAN	SUMBER PEMBELAJARAN	INDIKATOR PENILAIAN
					Informasi
4	Mahasiswa dapat menguraikan proses manajemen risiko keamanan informasi, mulai dari tahap identifikasi, *assessment,* dan menetapkan kontrol yang tepat untuk mengurangi resiko	*Risk Management*	1. Media: *contextual instruction* 2. Media: kelas, komputer, LCD, *whiteboard*	1. Rhodes M and Oesley., Information Security The Complete Reference, 2nd Edition, Mc Graw Hill Education, 2013 chater 2 2. Michael E. Whitman and Herbert J. Mattord., *Management of Information Security,* Fourth Edition, Stamford: 2014. Chapter 8 & Chapter 9	Menguraikan proses manajemen risiko keamanan informasi, mulai dari tahap identifikasi, *assessment,* dan menetapkan kontrol yang tepat untuk mengurangi resiko
5	Mahasiswa mampu menguraikan prinsip yang harus ada dalam *policy*, prosedur, standar dan guideline untuk melindungi aset informasi, serta mampu membuat contoh *policy*	*Information Security Policy*	1. Media: *contextual instruction* 2. Media: kelas, komputer, LCD, *whiteboard*	1. Rhodes M and Oesley., Information Security The Complete Reference, 2nd Edition, Mc Graw Hill Education, 2013 chapter 5 2. Michael E. Whitman and Herbert J. Mattord., *Management of Information Security,* Fourth Edition, Stamford: 2014. Chapter 4 3. Peltier T. R., Information Security Policies and Procedures, A Practitioner's Reference, 2nd	Merancang Menguraikan prinsip yang harus ada dalam policy, prosedur, standar dan guideline untuk melindungi aset informasi, serta mampu mebuat *policy*

SESI	KEMAMPUAN AKHIR	MATERI PEMBELAJARAN	BENTUK PEMBELAJARAN	SUMBER PEMBELAJARAN	INDIKATOR PENILAIAN
				Edition, CRC Press LLC, 2004	
6	Mahasiswa mampu menguraikan proses dalam *vulnerability assessment* dan kegunaannya dalam keamanan informasi	*Vulnerability Assessment*	1. Media: *contextual instruction* 2. Media: kelas, komputer, LCD, *whiteboard*	1. Michael E. Whitman and Herbert J. Mattord., *Management of Information Security,* Fourth Edition, Stamford: 2014. Chapter 10	Menguraikan proses dalam vulnerability assessment, dan kegunaannya dalam keamanan informasi
7	Mahasiswa mampu mensimulasikan proses vulnerability assessment dengan menggunakan tools	*Vulnerability Assessment Practical* (Studi Kasus)	1. Media: kelas, komputer, LCD, *whiteboard* 2. *Small Group Discussion*	2. Michael E. Whitman and Herbert J. Mattord., *Management of Information Security,* Fourth Edition, Stamford: 2014. Chapter 10	Mensimulasikan proses vulnerability assessment dengan menggunakan tools
8	Mahasiswa mampu menjabarkan klasifikasi aset informasi sesuai dengan tingkat confidential dan peruntukannya	*Information Classification*	1. Media: *contextual instruction* 2. Media: kelas, komputer, LCD, *whiteboard*	1. Michael E. Whitman and Herbert J. Mattord., *Management of Information Security,* Fourth Edition, Stamford: 2014. Chapter 8	Menjabarkan klasifikasi aset informasi sesuai dengan tingkat confidential dan peruntukannya
9	Mahasiswa mampu menguraikan prinsip pemberian hak akses dan pengelolaan siklus hidup akun pengguna untuk mengakses informasi	*Information Right Management*	1. Media: *contextual instruction* 2. Media: kelas, komputer, LCD, *whiteboard*	1. Rhodes M and Oesley., Information Security The Complete Reference, 2nd Edition, Mc Graw Hill Education, 2013 chapter 9 2. Michael E. Whitman and Herbert J. Mattord., *Management of Information Security,* Fourth	Menguraikan prinsip pemberian hak akses dan pengelolaan siklus hidup akun pengguna untuk mengakses informasi

SESI	KEMAMPUAN AKHIR	MATERI PEMBELAJARAN	BENTUK PEMBELAJARAN	SUMBER PEMBELAJARAN	INDIKATOR PENILAIAN
				Edition, Stamford: 2014. Chapter 8	
10	Mahasiswa mampu menguraikan jenis-jenis skema pengamanan dengan menggunakan kunci kriptografi untuk melakukan enkripsi dan hashing	*Cryptography*	1. Media: *contextual instruction* 2. Media: kelas, komputer, LCD, *whiteboard*	1. Johannes A. Buchman, et al., *Introduction to Public Key Infrastructures*, London: 2013. Chapter 1 2. Rhodes M and Oesley., Information Security The Complete Reference, 2nd Edition, Mc Graw Hill Education, 2013 chapter 10 3. Michael E. Whitman and Herbert J. Mattord., *Management of Information Security,* Fourth Edition, Stamford: 2014. Chapter 10	Menguraikan jenis-jenis skema pengamanan dengan menggunakan kunci kriptografi untuk melakukan enkripsi dan hashing
11	Mahasiswa mampu menguraikan prinsip keamanan pada jaringan komputer dan bagaimana merancangnya	*Network Security Design*	1. Media: *contextual instruction* 2. Media: kelas, komputer, LCD, *whiteboard*	1. Rhodes M and Oesley., Information Security The Complete Reference, 2nd Edition, Mc Graw Hill Education, 2013 chapter 13 2. Mattord., *Management of Information Security,* Fourth Edition, Stamford: 2014. Chapter 10	Menguraikan prinsip keamanan pada jaringan komputer dan bagaimana merancangnya
12	Mahasiswa mampu menguraikan jenis-jenis *vulnerable* pada aplikasi (web) dan menentukan design yang aman	*Secure Application design*	1. Media: *contextual instruction* 2. Media: kelas, komputer,	1. Rhodes M and Oesley., Information Security The Complete Reference, 2nd Edition, Mc Graw Hill Education, 2013 chapter 26	Menguraikan jenis-jenis *vulnerable* pada aplikasi (web) dan menentukan

SESI	KEMAMPUAN AKHIR	MATERI PEMBELAJARAN	BENTUK PEMBELAJARAN	SUMBER PEMBELAJARAN	INDIKATOR PENILAIAN
	untuk menghindari celah		LCD, *whiteboard*	2. Andrew Muller, et al., *Open Web Application Security (OWASP) Project Testing Guide - Release*. 4.0 Edition	design yang aman untuk menghindari celah celahnya
13	Mahasiswa mampu menguraikan aktivitas operasional dalam mengelola dan memelihara perangkat teknologi informasi yang aman	*Security Operation Management*	1. Media: *contextual instruction* 2. Media: kelas, komputer, LCD, *whiteboard*	1. Rhodes M and Oesley., Information Security The Complete Reference, 2nd Edition, Mc Graw Hill Education, 2013 chapter 31 2. Michael E. Whitman and Herbert J. Mattord., *Management of Information Security,* Fourth Edition, Stamford: 2014. Chapter 11	Menguraikan aktivitas operasional dalam mengelola dan memelihara perangkat teknologi informasi yang aman
14	Mahasiswa mampu melakukan simulasi serangan dengan mencari *vulnerable* pada aplikasi atau program	*Security Flaw Practice* (Studi Kasus)	1. Media: *contextual instruction* 2. Media: kelas, komputer, LCD, *whiteboard*	1. Andrew Muller, et al., *Open Web Application Security (OWASP) Project Testing Guide - Release*. 4.0 Edition	Melakukan simulasi serangan dengan mencari *vulnerable* pada aplikasi

Jakarta, 2018

Mengetahui,
Ketua Program Studi,

Dosen Pengampu,

Nama dan tanda tangan

Nama dan tanda tangan

EVALUASI PEMBELAJARAN

SESI	PROSE-DUR	BEN-TUK	SEKOR ≥ 77 (A / A-)	SEKOR ≥ 65 (B- / B / B+)	SEKOR ≥ 60 (C / C+)	SEKOR ≥ 45 (D)	SEKOR < 45 (E)	BOBOT (%)
1	*Post test*	Tes Tulisan (UTS)	Mahasiswa mampu menguraikan konsep prinsip dasar mengenai keamanan informasi dengan benar dan lengkap serta mampu memberikan contoh penerapannya	Mahasiswa mampu menguraikan konsep prinsip dasar mengenai keamanan informasi dengan benar dan lengkap	Mahasiswa mampu menguraikan konsep prinsip dasar mengenai keamanan informasi dengan benar namun belum lengkap	Mahasiswa mampu menguraikan konsep prinsip dasar mengenai keamanan informasi namun jawaban kurang tepat	Mahasiswa tidak mampu menguraikan konsep prinsip dasar mengenai keamanan informasi	5
2	*Post test*	Tes Tulisan (UTS) & Tugas Kelompok	Mahasiswa mampu menjabarkan berbagai *compliance standard* dan framework yang mengatur keamanan informasi dengan benar dan lengkap serta memahami proses untuk	Mahasiswa mampu menjabarkan berbagai *compliance standard* dan framework yang mengatur keamanan informasi dengan benar dan lengkap	Mahasiswa mampu menjabarkan berbagai *compliance standard* dan framework yang mengatur keamanan informasi dengan benar namun belum lengkap	Mahasiswa mampu menjabarkan berbagai *compliance standard* dan framework yang mengatur keamanan informasi, namun jawaban kurang tepat	Mahasiswa tidak mampu menjabarkan berbagai *compliance standard* dan framework yang mengatur keamanan informasi	15

SESI	PROSE-DUR	BEN-TUK	SEKOR ≥ 77 (A / A-)	SEKOR ≥ 65 (B- / B / B+)	SEKOR ≥ 60 (C / C+)	SEKOR ≥ 45 (D)	SEKOR < 45 (E)	BOBOT (%)
			mendapatkan sertifikasi SMKI					
3	*Post test*	Tes Tulisan (UTS)	Mahasiswa mampu menguraikan Siklus hidup keamanan informasi dan implementasi dari Sistem Manajemen Keamanan Informasi dengan benar dan lengkap serta memahami proses untuk mendapatkan sertifikasi SMKI	Mahasiswa mampu menguraikan Siklus hidup keamanan informasi dan implementasi dari Sistem Manajemen Keamanan Informasi dengan benar dan lengkap	Mahasiswa mampu menguraikan Siklus hidup keamanan informasi dan implementasi dari Sistem Manajemen Keamanan Informasi dengan benar namun belum lengkap	Mahasiswa mampu menguraikan Siklus hidup keamanan informasi dan implementasi dari Sistem Manajemen Keamanan Informasi, namun jawaban kurang tepat	Mahasiswa tidak mampu menguraikan Siklus hidup keamanan informasi dan implementasi dari Sistem Manajemen Keamanan Informasi	5
4	*Post test*	Tes Tulisan (UTS)	Mahasiswa dapat menguraikan proses manajemen risiko keamanan informasi, mulai dari tahap identifikasi, *assessment,* dan respon terhadap risiko dengan	Mahasiswa dapat menguraikan proses manajemen risiko keamanan informasi, mulai dari tahap identifikasi, *assessment,* dan respon terhadap	Mahasiswa dapat menguraikan proses manajemen risiko keamanan informasi, mulai dari tahap identifikasi, *assessment,* dan respon terhadap risiko dengan	Mahasiswa dapat menguraikan proses manajemen risiko keamanan informasi, mulai dari tahap identifikasi,	Mahasiswa tidak dapat menguraikan proses manajemen risiko keamanan informasi, mulai dari tahap identifikasi,	5

SESI	PROSE-DUR	BEN-TUK	SEKOR ≥ 77 (A / A-)	SEKOR ≥ 65 (B- / B / B+)	SEKOR ≥ 60 (C / C+)	SEKOR ≥ 45 (D)	SEKOR < 45 (E)	BOBOT (%)
			benar dan lengkap	risiko dengan benar dan lengkap	benar, namun tidak lengkap	*assessment,* dan respon terhadap risiko, namun kurang tepat	*assessment,* dan respon terhadap risiko	
5	*Post test*	Tes Tulisan (UTS) & Tugas Individu	Mahasiswa mampu menguraikan prinsip yang harus ada dalam policy, prosedur, standar dan guideline untuk melindungi aset informasi secara benar dan lengkap serta mampu membuat *policy*	Mahasiswa mampu menguraikan prinsip yang harus ada dalam policy, prosedur, standar dan guideline untuk melindungi aset informasi secara benar dan lengkap	Mahasiswa mampu menguraikan prinsip yang harus ada dalam policy, prosedur, standar dan guideline untuk melindungi aset informasi secara benar, namun belum lengkap	Mahasiswa mampu menguraikan prinsip yang harus ada dalam policy, prosedur, standar dan guideline untuk melindungi aset informasi, namun jawaban kurang tepat	Mahasiswa tidak mampu menguraikan prinsip yang harus ada dalam policy, prosedur, standar dan guideline untuk melindungi aset informasi	10
6	*Post test*	Tes Tulisan (UTS)	Mahasiswa mampu menguraikan proses dalam vulnerability assessment, dengan benar dan lengkap serta melakukan	Mahasiswa mampu menguraikan proses dalam vulnerability assessment, dengan benar dan lengkap	Mahasiswa mampu menguraikan proses dalam vulnerability assessment dengan benar, namun belum lengkap	Mahasiswa mampu menguraikan proses dalam vulnerability assessment, namun tidak tepat	Mahasiswa tidak mampu menguraikan proses dalam vulnerability assessment	5

SESI	PROSE-DUR	BEN-TUK	SEKOR ≥ 77 (A / A-)	SEKOR ≥ 65 (B- / B / B+)	SEKOR ≥ 60 (C / C+)	SEKOR ≥ 45 (D)	SEKOR < 45 (E)	BOBOT (%)
			simulasi dengan menggunakan tools					
7	*Post test*	Tugas Individu	Mahasiswa mampu mensimulasikan proses *vulnerability assessment* dengan menggunakan tools dengan benar dan semua disimulasikan	Mahasiswa mampu mensimulasikan proses *vulnerability assessment* dengan menggunakan tools dengan benar dan sebagian besar disimulasikan	Mahasiswa mampu mensimulasikan proses *vulnerability assessment* dengan menggunakan tools dengan benar dan sebagian kecil disimulasikan	Mahasiswa mampu mensimulasikan proses *vulnerability assessment* dengan menggunakan tools, namun tidak mengerti terhadap apa yang dilakukan	Mahasiswa tidak mampu mensimulasikan proses *vulnerability assessment* dengan menggunakan tools	10
8	*Post test*	Tes Tulisan (UAS)	Mahasiswa mampu menjabarkan klasifikasi aset informasi sesuai dengan tingkat confidential dan peruntukannya dengan benar dan lengkap serta mampu melakukan simulasi penerapannya pada aset	Mahasiswa mampu menjabarkan klasifikasi aset informasi sesuai dengan tingkat confidential dan peruntukannya dengan benar dan lengkap	Mahasiswa mampu menjabarkan klasifikasi aset informasi sesuai dengan tingkat confidential dan peruntukannya dengan benar, namun belum lengkap	Mahasiswa mampu menjabarkan klasifikasi aset informasi sesuai dengan tingkat confidential dan peruntukannya , namun jawaban kurang tepat	Mahasiswa tidak mampu menjabarkan klasifikasi aset informasi sesuai dengan tingkat confidential dan peruntukannya	5

SESI	PROSE-DUR	BEN-TUK	SEKOR ≥ 77 (A / A-)	SEKOR ≥ 65 (B- / B / B+)	SEKOR ≥ 60 (C / C+)	SEKOR ≥ 45 (D)	SEKOR < 45 (E)	BOBOT (%)
			informasi					
9	*Post test*	Tes Tulisan (UTS)	Mahasiswa mampu menguraikan prinsip pemberian hak akses dan pengelolaan siklus hidup akun pengguna untuk mengakses informasi dengan benar dan lengkap serta mampu menyebutkan contoh penerapannya	Mahasiswa mampu menguraikan prinsip pemberian hak akses dan pengelolaan siklus hidup akun pengguna untuk mengakses informasi dengan benar dan lengkap	Mahasiswa mampu menguraikan prinsip pemberian hak akses dan pengelolaan siklus hidup akun pengguna untuk mengakses informasi dengan benar, namun belum lengkap	Mahasiswa mampu menguraikan prinsip pemberian hak akses dan pengelolaan siklus hidup akun pengguna untuk mengakses informasi, namun kurang tepat	Mahasiswa tidak mampu menguraikan prinsip pemberian hak akses dan pengelolaan siklus hidup akun pengguna untuk mengakses informasi	5
10	*Post test*	Tes Tulisan (UAS) & Tugas Individu	Mahasiswa mampu menguraikan jenis-jenis skema pengamanan dengan menggunakan kunci kriptografi untuk melakukan enkripsi dan hashing dengan benar dan lengkap serta	Mahasiswa mampu menguraikan jenis-jenis skema pengamanan dengan menggunakan kunci kriptografi untuk melakukan enkripsi dan hashing dengan benar dan lengkap	Mahasiswa mampu menguraikan jenis-jenis skema pengamanan dengan menggunakan kunci kriptografi untuk melakukan enkripsi dan hashing dengan benar, namun tidak lengkap	Mahasiswa mampu menguraikan jenis-jenis skema pengamanan dengan menggunakan kunci kriptografi untuk melakukan enkripsi dan	Mahasiswa tidak mampu menguraikan jenis-jenis skema pengamanan dengan menggunakan kunci kriptografi untuk melakukan enkripsi dan	10

SESI	PROSE-DUR	BEN-TUK	SEKOR ≥ 77 (A / A-)	SEKOR ≥ 65 (B- / B / B+)	SEKOR ≥ 60 (C / C+)	SEKOR ≥ 45 (D)	SEKOR < 45 (E)	BOBOT (%)
			melakukan simulasi contoh penerapannya			hashing, namun kurang tepat	hashing	
11	*Post test*	Tes Tulisan (UAS)	Mahasiswa mampu menguraikan prinsip keamanan pada jaringan komputer dengan benar dan lengkap serta mampu merancangnya	Mahasiswa mampu menguraikan prinsip keamanan pada jaringan komputer dengan benar dan lengkap	Mahasiswa mampu menguraikan prinsip keamanan pada jaringan komputer dengan benar, namun tidak lengkap	Mahasiswa mampu menguraikan prinsip keamanan pada jaringan komputer, namun kurang tepat	Mahasiswa tidak mampu menguraikan prinsip keamanan pada jaringan komputer	5
12	*Post test*	Tes Tulisan (UAS)	Mahasiswa mampu menguraikan jenis-jenis *vulnerable* pada aplikasi (web) dengan benar dan lengkap serta dan mampu menentukan design yang aman untuk menghindari celah	Mahasiswa mampu menguraikan jenis-jenis *vulnerable* pada aplikasi (web) dengan benar dan lengkap	Mahasiswa mampu menguraikan jenis-jenis *vulnerable* pada aplikasi (web) dengan benar, namun tidak lengkap	Mahasiswa mampu menguraikan jenis-jenis *vulnerable* pada aplikasi (web), namun jawaban kurang tepat	Mahasiswa tidak mampu menguraikan jenis-jenis *vulnerable* pada aplikasi (web)	5
13	*Post test*	Tes Tulisan (UAS)	Mahasiswa mampu menguraikan	Mahasiswa mampu menguraikan	Mahasiswa mampu menguraikan	Mahasiswa mampu menguraikan	Mahasiswa tidak mampu menguraikan	5

SESI	PROSE-DUR	BEN-TUK	SEKOR ≥ 77 (A / A-)	SEKOR ≥ 65 (B- / B / B+)	SEKOR ≥ 60 (C / C+)	SEKOR ≥ 45 (D)	SEKOR < 45 (E)	BOBOT (%)
			aktivitas operasional dalam mengelola dan memelihara perangkat teknologi informasi yang aman dengan benar dan lengkap serta mampu memberikan contohnya	aktivitas operasional dalam mengelola dan memelihara perangkat teknologi informasi yang aman dengan benar dan lengkap	aktivitas operasional dalam mengelola dan memelihara perangkat teknologi informasi yang aman dengan benar, namun tidak lengkap	aktivitas operasional dalam mengelola dan memelihara perangkat teknologi informasi yang aman, namun jawaban kurang tepat	aktivitas operasional dalam mengelola dan memelihara perangkat teknologi informasi yang aman	
14	*Post test*	Tugas Kelompok	Mahasiswa mampu melakukan simulasi serangan dengan mencari *vulnerable* pada sistem atau program dengan benar dan pemaparan yang jelas	Mahasiswa mampu melakukan simulasi serangan dengan mencari *vulnerable* pada sistem atau program dengan benar, dengan pemaparan cukup jelas	Mahasiswa mampu melakukan simulasi serangan dengan mencari *vulnerable* pada sistem atau program dengan benar, namun pemaparan kurang jelas	Mahasiswa mampu melakukan simulasi serangan dengan mencari *vulnerable* pada sistem atau program, namun tidak sesuai dengan sasarannya	Mahasiswa tidak mampu melakukan simulasi serangan dengan mencari *vulnerable* pada sistem atau program	10

Komponen penilaian :

1. Tugas Individu = 20%
2. Tugas Kelompok = 20%
3. UTS = 30%
4. UAS = 30%

Jakarta, September 2018

Mengetahui,
Ketua Program Studi,

Dosen Pengampu,

Dr. Hosizah, SKM, MKM

Nauri Anggita T., SKM, MKM/
Harfebi Fryonanda, S.Kom, M.Kom