RENCANA PEMBELAJARAN SEMESTER (RPS)

UNIVERSITAS DIPONEGORO

SPMI-UNDIP	RPS	S1.SK-FT-UNDIP	081

Revisi ke		1
Tanggal		5 Juli 2022
Dikaji Ulang Oleh		Ketua Program Studi Teknik Komputer
Dikendalikan Oleh		GPM Teknik Komputer
Disetujui Oleh		Dekan Fakultas Teknik

	UNIVERSITAS DIPONEGORO **FAKULTAS TEKNIK** **DEPARTEMEN TEKNIK KOMPUTER** **PROGRAM SARJANA**	**SPMI-UNDIP/RPS/S1.SK-FT-UNDIP/081**

RENCANA PEMBELAJARAN SEMESTER

MATA KULIAH (MK)	KODE	RUMPUN MK	BOBOT		SEMESTER	TANGGAL PENYUSUNAN
Keamanan Sistem Informasi	PTSK6607	**Pilihan**	**T=2**	**P=0**	**Genap**	**5 Juli 2022**
OTORISASI/PENGESAHAN	**DOSEN PENGEMBANG RPS**		**Koordinator RMK**		**KaPRODI**	

CAPAIAN PEMBELAJARAN	**CPL yang dibebankan pada MK**	
	CPL 3	Memiliki pemahaman keilmuan dan penguasaan keterampilan di bidang teknik komputer, meliputi sistem tertanam dan robotika, jaringan dan keamanan komputer, rekayasa perangkat lunak, multimedia, game, dan kecerdasan buatan yang ditopang oleh profesionalitas, pengetahuan sains dasar dan rekayasa yang kuat.
	CPMK (Capaian Pembelajaran Mata Kuliah)	
	CPMK 3.4	Mampu menerapkan aspek-aspek keamanan untuk komputer server dan jaringan komputer dengan berdasarkan best practice yang ada
Deskripsi Singkat	Mata kuliah ini berisi konsep dasar alur komunikasi jaringan komputer, protokol, layer, pengalamatan, topologi, konfigurasi dan pengujian jaringan komputer.	
Bahan Kajian Materi Pembelajaran	1. Pendahuluan 2. Foot printing & Reconnaissance 3. Scanning Networks 4. Enumeration 5. System Hacking 6. Trojan & Backdoors 7. Virus & Worms 8. Sniffers 9. Social Engineering 10. Denial of Service 11. Session Hijacking 12. Hacking Web Application 13. SQL Injection 14. Firewall	

Pustaka		**Utama:** **1. Black, U.D., 1994, Data Network, Prentice-Hall, Englewoods Cliffs, New Jersey** **2. Ethical Hacker V.4**				
Pengampu		**Team Pengajar Keamanan Sistem Informasi**				
Prasyarat		**-**				
Media Pembelajaran		**Papan Tulis, LCD Projector, Laptop, dan Power Point**				
Mg ke-	**Sub-CPMK (sebagai kemampuan akhir yang diharapkan)**	**Penilaian**	**Bentuk pembelajaran; Metode Pembelajaran; Penugasan; [Estimasi Waktu]**		**Materi Pembelajaran**	**Bobot (%)**
		Indikator, Kriteria, dan Bentuk	**Tatap Muka/Luring**	**Daring**		
(1)	**(2)**	**(3)**	**(4)**	**(5)**	**(6)**	**(7)**
1	Mahasiswa mampu menjelaskan jenis perangkat, sistem operasi, dan teknologi virtualisasi mesin komputer paling sedikit 80% tepat.	• Dapat mengetahui perangkat yang akan digunakan pada simulasi keamanan sistem informasi • Dapat mengetahui teknologi virtual machine • Dapat mengetahui jenis-jenis sistem operasi komputer • Dapat mengetahui jenis-jenis attacker / hacker	• Ceramah • Diskusi 2x50		Pendahuluan 1.1 Pre-Configure 1.2 Virtual Machine 1.3 Attacker / Hacker	
2	Mahasiswa mampu menjelaskan langkah-langkah dan metodologi serangan keamanan sistem informasi footprinting setidaknya 80% benar	• Dapat mengetahui langkah-langkah yang dilakukan attacker dalam menyerang keamanan system informasi • Dapat mengetahui metodologi dan fungsi footprinting attack pada sistem informasi • Dapat mengetahui peralatan yang digunakan untuk melakukan footprinting sistem informasi	• Ceramah • Discovery learning • Diskusi 2x50		Foot printing & Reconnaissance 2.1 Foot printing a target network 2.2 Collect confidential Information 2.3 Extract Confidential Information 2.4 Mirroring Website	
3	Mahasiswa mampu menjelaskan langkahlangkah dan metodologi serangan keamanan sistem informasi scanning network setidaknya 80% benar	• Dapat mengetahui langkah-langkah yang dilakukan attacker dalam menyerang keamanan sistem informasi • Dapat mengetahui metodologi dan fungsi scanning network attack pada sistem informasi • Dapat mengetahui	• Simulasi • Diskusi 2x50		Scanning Networks 3.1 Use Scanner Network 3.2 Monitor and Exploit 3.3 Explore and Audit	

		peralatan yang digunakan untuk melakukan scanning network sistem informasi				
4	Mahasiswa mampu menjelaskan langkahlangkah dan metodologi serangan keamanan sistem informasi enumeration setidaknya 80% benar.	• Dapat mengetahui langkah-langkah yang dilakukan attacker dalam menyerang keamanan sistem informasi • Dapat mengetahui metodologi dan fungsi enumeration attack pada sistem informasi • Dapat mengetahui peralatan yang digunakan untuk melakukan enumeration sistem informasi	• Simulasi • Diskusi 2x50		Enumeration 4.1 NetBIOS 4.2 Password 4.3 Networks	
5	Mahasiswa mampu menjelaskan langkahlangkah dan metodologi serangan keamanan sistem informasi system hijacking setidaknya 80% benar.	• Dapat mengetahui langkah-langkah yang dilakukan attacker dalam menyerang keamanan sistem informasi • Dapat mengetahui metodologi dan fungsi system hacking attack pada sistem informasi • Dapat mengetahui peralatan yang digunakan untuk melakukan system hacking sistem informasi	• Simulasi • Diskusi 2x50		System Hacking 5.1 Extract Password 5.2 Hide file	
6	Mahasiswa mampu menjelaskan jenis dan karakteristik perangkat lunak berbahaya jenis trojan dan backdoor setidaknya 80% benar.	• Dapat mengetahui jenisjenis perangkat lunak berbahaya • Dapat memahami karakteristik perangkat lunak berbahaya jenis trojan dan backdoors	• Simulasi • Diskusi 2x50		Trojan & Backdoors 6.1 Create fake server 6.2 Trojan 6.3 Backdoors	
7	Mahasiswa mampu menjelaskan jenis dan karakteristik perangkat lunak berbahaya jenis virus dan worm setidaknya 80% benar.	• Dapat mengetahui jenisjenis perangkat lunak berbahaya • Dapat memahami karakteristik perangkat lunak berbahaya jenis virus & worms	• Simulasi • Diskusi 2x50		Virus & Worms 7.1 Create Virus 7.2 Create Worms 7.3 Scanning	
8	**UTS**					

9	Mampu menjelaskan Langkah-langkah dan metodologi serangan keamanan system informasi sniffing setidaknya 80% benar.	• Dapat mengetahui langkah-langkah yang dilakukan attacker dalam menyerang keamanan sistem informasi • Dapat mengetahui metodologi dan fungsi sniffing attack pada sistem informasi • Dapat mengetahui peralatan yang digunakan untuk melakukan sniffing sistem informasi	• Simulasi • Diskusi 2x50		Sniffers 8.1 Network sniffing 8.2 Man-in-the-middle attack	
10	Mahasiswa mampu menjelaskan Langkah-langkah dan metodologi serangan keamanan sistem informasi social engineering setidaknya 80% benar.	• Dapat mengetahui langkah-langkah yang dilakukan attacker dalam menyerang keamanan sistem informasi • Dapat mengetahui metodologi dan fungsi social engineering attack pada sistem informasi • Dapat mengetahui peralatan yang digunakan untuk melakukan social engineering sistem informasi	Cooperative learning 2x50		Social Engineering 9.1 Phishing Attack	
11	Mahasiswa mampu Menjelaskan Langkah-langkah dan metodologi serangan keamanan sistem informasi Denial of Service setidaknya 80% benar	• Dapat mengetahui langkah-langkah yang dilakukan attacker dalam menyerang keamanan sistem informasi • Dapat mengetahui metodologi dan fungsi Denial of Service attack pada sistem informasi • Dapat mengetahui peralatan yang digunakan untuk melakukan denial of service sistem informasi	Contextual instruction 2x50		Denial of Service 10.1 Denial of Service Attack 10.2 Zombies 10.3 HTTP Flooding	
12	Mahasiswa mampu Menjelaskan Langkah-langkah dan metodologi serangan keamanan sistem informasi Session Hijacking setidaknya 80% benar.	• Dapat mengetahui langkah-langkah yang dilakukan attacker dalam menyerang keamanan sistem informasi • Dapat mengetahui metodologi dan fungsi session hijacking attack pada sistem informasi • Dapat mengetahui peralatan yang digunakan untuk melakukan session hijacking sistem informasi	Contextual instruction 2x50		Session Hijacking 11.1 Intercept & Modify web traffic 11.2 Hacking Webserver	
13	Mahasiswa mampu menjelaskan Langkah-langkah dan metodologi serangan keamanan sistem informasi hacking web application setidaknya 80% benar.	• Dapat mengetahui langkah-langkah yang dilakukan attacker dalam menyerang keamanan sistem informasi • Dapat mengetahui metodologi dan fungsi hacking web attack pada sistem informasi • Dapat mengetahui peralatan yang digunakan untuk melakukan hacking web sistem informasi	• Simulasi • Diskusi 2x50		Hacking Web Application 12.1 Tampering 12.2 Cross-Site Scripting (XSS) 12.3 Web App Vulnerability Scanning	
14	Mahasiswa mampu menjelaskan Langkah-langkah dan metodologi serangan keamanan sistem informasi SQL Injection	• Dapat mengetahui langkah-langkah yang dilakukan attacker dalam menyerang keamanan sistem informasi • Dapat mengetahui metodologi dan fungsi SQL injection attack pada sistem informasi	Contextual instruction 2x50		SQL Injection 13.1 Scanning 13.2 SQL Attack	

	setidaknya 80% benar.	• Dapat mengetahui peralatan yang digunakan untuk melakukan SQL injection sistem informasi				
15	Mahasiswa mampu menjelaskan perangkat lunak pendukung keamanan sistem informasi setidaknya 80% benar.	• Dapat mengetahui format isi data pada komunikasi antar komputer • Dapat mengetahui peralatan yang digunakan untuk mendeteksi isi paket data dalam komunikasi antar komputer	• Simulasi • Diskusi 2x50		Firewall 14.1 Firewall 14.2 Intruder Detection System (IDS) 14.3 Honey Port	
16	**UAS**					