



RENCANA PEMBELAJARAN SEMESTER (RPS) UNIVERSITAS DIPONEGORO

SPMI-UNDIP	RPS	S1.SK-FT-UNDIP	070
-------------------	------------	-----------------------	------------

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		SPMI-UNDIP/RPS/S1.SK-FT-UNDIP/070	Disetujui Oleh Dekan Fak. Teknik
Revisi ke 1	Tanggal 5 Juli 2022	Rencana Pembelajaran Semester	



UNIVERSITAS DIPONEGORO
FAKULTAS TEKNIK
DEPARTEMEN TEKNIK KOMPUTER
PROGRAM SARJANA

SPMI-
UNDIP/RPS/S1.SK-
FT-UNDIP/070

RENCANA PEMBELAJARAN
SEMESTER

MATA KULIAH (MK)	KODE	RUMPUN MK	BOBOT		SEMESTER	TANGGAL PENYUSUNAN
Keamanan Jaringan Komputer	PTSK6711	Pilihan	T=2	P=0	Ganjil	5 Juli 2022
OTORISASI/PENGESAHAN	DOSEN PENGEMBANG RPS		Koordinator RMK		KaPRODI	
CAPAIAN PEMBELAJARAN	CPL yang dibebankan pada MK					
	CPL 2	Memiliki kompetensi keilmuan dan keahlian di bidang teknik komputer dan bidang terkait lainnya yang menunjang profesionalitas kerja, baik secara individu maupun tim, serta kemampuan beradaptasi dan pengembangan diri di lingkungan kerja.				
	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.				
	CPL 6	Mampu menyampaikan ide dan gagasannya dengan baik dalam menghadirkan solusi dari suatu permasalahan berdasarkan pemahaman pengetahuan dan penguasaan keahlian yang kuat.				
	CPMK (Capaian Pembelajaran Mata Kuliah)					
	CPMK 2-1	Mampu untuk belajar secara mandiri untuk mengembangkan kemampuan baik di bidang teknik komputer atau di bidang terkait lainnya				
	CPMK 2-2	Mampu mengidentifikasi konsep teoritis di bidang teknik komputer untuk berbagai permasalahan komputasi, jaringan komputer, dan perangkat keras				
	CPMK 3-4	Mampu menerapkan aspek-aspek keamanan untuk komputer server dan jaringan komputer dengan berdasarkan <i>best practice</i> yang ada				
	CPMK 6-1	Mampu mengkomunikasikan ide dan gagasan dengan memperhatikan aspek komunikasi yang baik				
	CPMK 6-2	Mampu menggunakan berbagai perangkat lunak yang ada untuk membantu mempresentasikan ide dan gagasan				

Deskripsi Singkat	Mata kuliah ini berisi resiko ancaman serangan terhadap sistem melalui jaringan komputer, metode mengamankan data melalui jaringan komputer, dan langkah-langkah pendukung untuk mengamankan data melalui jaringan komputer.
Bahan Kajian Materi Pembelajaran	1. Pengantar keamanan jaringan komputer 2. Ancaman Keamanan Jaringan Modern 3. Model Ancaman keamanan jaringan modern 4. Mengamankan perangkat jaringan 5. Authentication, authorization, and accounting (AAA) 6. Implementing AAA 7. Implementing Firewall Technologies 8. Implementing intrusion prevention 9. Securing Local Area Network 10. Cryptographic systems 11. Implementing virtual private networks 12. Managing a secure network

Pustaka		1. NetAcad, Cisco Learning Institute, Network Security 2. C. Branch, Melville. 1985. Comprehensive City Planning Introduction and Explanation. APA Press. Washington D.C				
Pengampu		Team Pengajar Keamanan Jaringan Komputer				
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 serangan sistem melalui jaringan komputer	• Kemampuan mahasiswa memahami	• Ceramah • Diskusi 2x50"		Materi Kuliah 1 Pengantar pengenalan jaringan kompu1. Pendahuluan 1.1 Rencana Perkuliahan Semester 1.2 Kontrak Perkuliahan 1.3 Intro Modern Network Security Threatsan karakteristik jenis jaringan yang umum.	5

					5. Menjelaskan bagaimana LAN dan WAN saling terhubung ke internet. 6. Menjelaskan empat persyaratan dasar jaringan yang andal. 7. Menjelaskan bagaimana tren seperti BYOD, kolaborasi online, video, dan komputasi awan mengubah cara kita berinteraksi. 8. Identifikasi beberapa ancaman keamanan dasar dan solusi untuk semua jaringan. 9. Menjelaskan kesempatan kerja di bidang networking.	
2	Mahasiswa mampu menjelaskan dasar-dasar, resiko, ancaman, dan struktur keamanan jaringan komputer	• Kemampuan mahasiswa memahami • Keaktifan mahasiswa dalam diskusi	• Ceramah • Self direction learning • Small group discussion • Tanya jawab 2x50"		2. Modern Network Security Threats 2.1 Rationale for network security 2.2 Data confidentiality, integrity, availability 2.3 Risks, threats, vulnerabilities and countermeasure s 2.4 Methodolog y of a structured attack	5

3	Mahasiswa mampu menjelaskan model, kebijakan, dan desain keamanan jaringan komputer	Kemampuan mahasiswa memahami	- Ceramah - Self direction learning - Tanya jawab 2x50"		3. Modern Network Security Threats Model 3.1 Security model 3.2 Security policies, standards and guidelines 3.3 Network security design	10
4	Mahasiswa mampu menjelaskan konfigurasi mengamankan perangkat jaringan komputer	- Produk tugas kecil - Keaktifan mahasiswa dalam diskusi	- Ceramah - Self direction learning - Small group discussion - Tanya jawab 2x50"		4. Securing Network Devices 4.1 Configure secure administrative access 4.2 Configure network devices for monitoring administrative access 4.3 Secure IOS-based Routers using automated features	10
5	Mahasiswa mampu menjelaskan protokol-protokol untuk mengontrol akses ke jaringan komputer	- Kemampuan mahasiswa memahami - Keaktifan mahasiswa dalam diskusi	- Ceramah - Self direction learning - Small group discussion - Tanya jawab 2x50"		5. Authentication, Authorization, and Accounting (AAA) 5.1 Local Authentication 5.2 Enhancements to Local Authentication 5.3 Describe the purpose of AAA and the various implementation techniques	5
6	Mahasiswa mampu menjelaskan protokol-protokol untuk mengontrol akses ke jaringan komputer	- Produk tugas kecil - Keaktifan mahasiswa dalam diskusi	- Ceramah - Self direction learning - Small group discussion - Tanya jawab 2x50"		6. Implementing Authentication, Authorization, and Accounting (AAA) 6.1 Implement AAA using the local database 6.2 Implement AAA using	10

					TACACS+ and RADIUS protocols 6.3 Implement AAA Authorization and Accounting	
7	Mahasiswa mampu menjelaskan jenis Access List dan fungsinya untuk mengontrol akses ke jaringan komputer	• Kemampuan mahasiswa memahami • Keaktifan mahasiswa dalam diskusi	• Ceramah • Tanya jawab 2x50"		7.Implementing Firewall Technologies 7.1 Standard and extended ACLs 7.2 Applications of standard and extended ACLs	5
8	UTS					0

9	Mahasiswa mampu menjelaskan langkah-langkah pencegahan serangan melalui jaringan komputer dengan menggunakan IDS dan IPS	• Kemampuan mahasiswa memahami • Keaktifan mahasiswa dalam diskusi	• Ceramah • Tanya jawab 2x50"		8.Implementing Intrusion Prevention 8.1 Intrusion Prevention Systems (IPS) 8.2 purpose and operation of network-based and host-based Intrusion Prevention Systems (IPS) 8.3 How IDS and IPS signatures are used to detect malicious network traffic	5
10	Mahasiswa mampu menjelaskan konfigurasi untuk mengamankan perangkat jaringan komputer yang dikelola	• Kemampuan mahasiswa memahami	• Ceramah • Tanya jawab 2x50"		9. Securing the Local Area Network 9.1 Endpoint vulnerabilities and protection methods 9.2 Configure and verify switch security features, including port security and storm control 9.3Fundamental	10

					security considerations of Wireless, VoIP, and SANs	
11	Mahasiswa mampu menjelaskan jenis-jenis enkripsi pada komunikasi jaringan komputer	• Kemampuan mahasiswa memahami • Keaktifan mahasiswa dalam diskusi	• Ceramah • Self direction learning • Tanya jawab 2x50"		10.Cryptographic Systems (1) 10.1How the types of encryption, hashes, and digital signatures work together to provide confidentiality, integrity, and authentication	5
12	Mahasiswa mampu menjelaskan langkah-langkah untuk memastikan kesesuaian data setelah data dikirimkan melalui jaringan komputer	• Kemampuan mahasiswa memahami	• Ceramah • Tanya jawab 2x50"		11.Cryptographic Systems (2) 11.1Mechanisms to ensure data integrity, authentication, and confidentiality 11.2Mechanisms used to ensure data confidentiality and authentication using a public key	5
13	Mahasiswa mampu menjelaskan fungsi, komponen, dan konfigurasi VPN	• Kemampuan mahasiswa memahami • Keaktifan mahasiswa dalam diskusi	• Ceramah • Tanya jawab 2x50"		12.Implementing Virtual Private Networks (1) 12.1Purpose and operation of VPN types 12.2purpose and operation of GRE VPNs 12.3components and operations of IPsec VPNs	5
14	Mahasiswa mampu menjelaskan konfigurasi VPN	• Kemampuan mahasiswa memahami • Keaktifan mahasiswa dalam diskusi	• Ceramah • Tanya jawab 2x50"		13.Implementing Virtual Private Networks (2) 13.1Configure and verify a site-to-site IPsec VPN with pre-shared key authentication using CLI 13.2Configure and verify a Remote Access VPN	5

15	Mahasiswa mampu menjelaskan prinsip-prinsip, fungsi, tujuan, peran, serta struktur kebijakan dalam mengamankan jaringan komputer	• Produk tugas kecil • Keaktifan mahasiswa dalam diskusi	• Ceramah • Self direction learning • Small group discussion • Tanya jawab 2x50"		14. Managing a Secure Network 14.1Principles of secure network design 14.2Role of operations security in a network 14.3Various techniques and tools to use for network security testing 14.4Functions, goals, role, and structure of a comprehensive security policy	10
16	UAS					0

