



**STMIK HANDAYANI MAKASSAR**  
**FAKULTAS KOMPUTER**  
**JURUSAN/PROGRAM STUDI SISTEM KOMPUTER**

**RENCANA PEMBELAJARAN SEMESTER (RPS)**

NAMA MATA KULIAH	KODE MK	Rumpun MK	BOBOT (sks)	SEMESTER	Tgl Penyusunan
Keamanan Jaringan	KB034134	Matakuliah Wajib	3	3	
OTORISASI	Nama Koordinator Pengembang RPS	Koordinator RMK	Ka PRODI		
Capaian Pembelajaran (CP)	CPL-PRODI (Capaian Pembelajaran Lulusan Program Studi)				
	S9	Menunjukkan sikap dan bertanggungjawab atas pekerjaan dibidang keahliannya secara mandiri			
	KU1	Mampu menunjukkan kinerja mandiri, bermutu, dan terukur			
	KU5	Mampu mengambil keputusan secara tepat dalam konteks penyelesaian masalah di bidang keahliannya, berdasarkan hasil analisis informasi dan data			
	C2	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.			
	C3	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.			
	C6	Mampu menyampaikan ide dan gagasannya dengan baik dalam menghadirkan solusi dari suatu permasalahan berdasarkan pemahaman pengetahuan dan penguasaan keahlian yang kuat.			
	CPMK (Capaian Pembelajaran Lulusan Yang Dibebankan Pada Mata Kuliah)				
CPMK1 - Mahasiswa akan dapat mengetahui resiko ancaman serangan melalui jaringan komputer					
CPMK2 - Mahasiswa akan dapat mengetahui metode untuk mengamankan data melalui jaringan komputer					
CPMK3 - Mahasiswa akan dapat mengetahui fungsi, tujuan, peran, serta struktur kebijakan keamanan yang komprehensif pada jaringan komputer					
Diskripsi Singkat MK	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 / Pokok Bahasan	<ol style="list-style-type: none"><li>1. Pengantar keamanan jaringan komputer</li><li>2. Ancaman Keamanan Jaringan Modern</li><li>3. Model Ancaman keamanan jaringan modern</li><li>4. Mengamankan perangkat jaringan</li><li>5. Authentication, authorization, and accounting (AAA)</li></ol>				

	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	
<b>Daftar Referensi</b>	<b>Utama:</b>	
	1. NetAcad, Cisco Learning Institute, Network Security 2. C. Branch, Melville. 1985. Comprehensive City Planning Introduction and Explanation. APA Press. Washington D.C	
	<b>Pendukung:</b>	
<b>Media Pembelajaran</b>	<b>Preangkat lunak:</b>	<b>Perangkat keras :</b>
	SO: Windows/Linux, Cisco Paket Tracer	PC/Laptop, Projektor, White Board
<b>Nama Dosen Pengampu</b>	Andy Lukman Affandy	
<b>Mata kuliah prasyarat</b>	-	

Minggu Ke-	Sub-CPMK (Kemampuan akhir yg direncanakan)	Bahan Kajian (Materi Pembelajaran)	Bentuk dan Metode Pembelajaran	Estimasi Waktu	Pengalaman Belajar Mahasiswa	Kriteria & Bentuk Penilaian	Indikator Penilaian	Bobot Penilaian (%)
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
1	Mahasiswa mampu menjelaskan jenis serangan sistem melalui jaringan komputer	<b>Pendahuluan Pengenalan Jaringan Komputer:</b> <ul style="list-style-type: none"> <li>- Kontrak Kuliah</li> <li>- Intro Modern Network Security Threatsan karakteristik jenis jaringan yang umum</li> <li>- Menjelaskan bagaimana LAN dan WAN saling terhubung ke internet.</li> <li>- Menjelaskan empat persyaratan dasar jaringan yang andal.</li> <li>- Menjelaskan bagaimana tren seperti BYOD, kolaborasi online, video, dan komputasi awan mengubah cara kita berinteraksi.</li> <li>- Identifikasi beberapa ancaman keamanan dasar dan solusi untuk semua jaringan.</li> <li>- Menjelaskan kesempatan kerja di bidang networking.</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Bentuk:</b> Kuliah</li> <li>• <b>Metode:</b> Diskusi Kelompok</li> </ul>	TM : 1x3x50' BT ; 180' BM : 180'	Dapat memberi contoh Implementasi dan bentuk Jaringan Komputer.	<ul style="list-style-type: none"> <li>• Tanya Jawab</li> <li>• Keaktifan dalam kelas</li> </ul>	Ketepatan menjelaskan dasar Jaringan komputer	5
2	Mahasiswa mampu menjelaskan dasar-dasar, resiko, ancaman, dan	<b>Resiko dan Ancaman:</b> <ul style="list-style-type: none"> <li>- Modern Network Security Threats</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Bentuk:</b> Kuliah</li> <li>• <b>Metode:</b> Diskusi</li> </ul>	TM : 1x3x50' BT ; 180' BM : 180'	Tugas resiko dan ancaman jaringan komputer, dikirim lewat email	<ul style="list-style-type: none"> <li>• Tanya Jawab</li> <li>• Keaktifan dalam kelas</li> </ul>	Ketepatan menjelaskan resiko dan ancaman jaringan komputer	10

Minggu Ke-	Sub-CPMK (Kemampuan akhir yg direncanakan)	Bahan Kajian (Materi Pembelajaran)	Bentuk dan Metode Pembelajaran	Estimasi Waktu	Pengalaman Belajar Mahasiswa	Kriteria & Bentuk Penilaian	Indikator Penilaian	Bobot Penilaian (%)
	struktur keamanan jaringan komputer	<ul style="list-style-type: none"> <li>- Rationale for network security</li> <li>- Data confidentiality, integrity, availability</li> <li>- Risks, threats, vulnerabilities and countermeasures</li> <li>- Methodology of a structured attack</li> </ul>	Kelompok					
3	Mahasiswa mampu menjelaskan model, kebijakan, dan desain keamanan jaringan komputer	<ul style="list-style-type: none"> <li>- Modern Network Security Threats Model</li> <li>- Security model</li> <li>- Security policies, standards and guidelines</li> <li>- Network security design</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Bentuk:</b> Kuliah</li> <li>• <b>Metode:</b> Diskusi Kelompok</li> </ul>	TM : 1x3x50' BT ; 180' BM : 180'	Tugas makalah model, kebijakan, dan desain keamanan jaringan.	<ul style="list-style-type: none"> <li>• Tanya Jawab</li> <li>• Keaktifan dalam kelas</li> </ul>	Ketepatan menjelaskan model, kebijakan dan desain keamanan jaringan	<b>10</b>
4	Mahasiswa mampu menjelaskan konfigurasi mengamankan perangkat jaringan komputer	<b>Konfigurasi Network Security</b> <ul style="list-style-type: none"> <li>- Securing Network Devices</li> <li>- Configure secure administrative access</li> <li>- Configure network devices for monitoring administrative access</li> <li>- Secure IOS- based Routers using automated features</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Bentuk:</b> Kuliah</li> <li>• <b>Metode:</b> Diskusi Kelompok</li> </ul>	TM : 1x3x50' BT ; 180' BM : 180'	Praktek konfigurasi keamanan jaringan komputer.	<ul style="list-style-type: none"> <li>• Keaktifan dalam kelas</li> <li>• Tugas Individu</li> </ul>	Ketepatan menjelaskan konfigurasi mengamankan perangkat jaringan.	<b>15</b>

Minggu Ke-	Sub-CPMK (Kemampuan akhir yg direncanakan)	Bahan Kajian (Materi Pembelajaran)	Bentuk dan Metode Pembelajaran	Estimasi Waktu	Pengalaman Belajar Mahasiswa	Kriteria & Bentuk Penilaian	Indikator Penilaian	Bobot Penilaian (%)
5	Mahasiswa mampu menjelaskan protokol- protokol untuk mengontrol akses ke jaringan komputer	<b>Protocol Keamanan:</b> <ul style="list-style-type: none"> <li>- Authentication, Authorization, and Accounting (AAA)</li> <li>- Local Authentication</li> <li>- Enhancements to Local Authentication</li> <li>- Describe the purpose of AAA and the various implementation techniques</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Bentuk:</b> Kuliah</li> <li>• <b>Metode:</b> Diskusi Kelompok, Simulasi</li> </ul>	TM : 1x3x50' BT ; 180' BM : 180'	Tugas mensimulasikan penerapan Protocol Keamanan	<ul style="list-style-type: none"> <li>• Quis</li> <li>• Keaktifan dalam kelas</li> <li>• Rubrik</li> <li>• Tugas Authentication</li> </ul>	Ketepatan menjelaskan Protocol Keamanan	<b>15</b>
6	Mahasiswa mampu menjelaskan protokol- protokol untuk mengontrol akses ke jaringan komputer	<b>Protocol Keamanan:</b> <ul style="list-style-type: none"> <li>- Implementing Authentication, Authorization, and Accounting (AAA)</li> <li>- Implement AAA using the local database</li> <li>- Implement AAA using TACACS+ and RADIUS protocols</li> <li>- Implement AAA Authorization and Accounting</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Bentuk:</b> Kuliah</li> <li>• <b>Metode:</b> Diskusi Kelompok, Simulasi</li> </ul>	TM : 1x3x50' BT ; 180' BM : 180'	Tugas mensimulasikan penerapan Protocol Keamanan	<ul style="list-style-type: none"> <li>• Tanya Jawab</li> <li>• Keaktifan dalam kelas</li> </ul>	Ketepatan menjelaskan Protocol Keamanan	<b>10</b>
7	Mahasiswa mampu menjelaskan jenis Access List dan fungsinya untuk mengontrol akses ke jaringan komputer	<b>Access List:</b> <ul style="list-style-type: none"> <li>- Implementing Firewall Technologies</li> <li>- Standard and extended ACLs</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Bentuk:</b> Kuliah</li> <li>• <b>Metode:</b> Diskusi Kelompok, Simulasi</li> </ul>	TM : 1x3x50' BT ; 180' BM : 180'	Tugas mensimulasikan penerapan Access List	<ul style="list-style-type: none"> <li>• Tanya Jawab</li> <li>• Keaktifan dalam kelas</li> </ul>	Ketepatan menjelaskan Access List Keamanan Jaringan	<b>10</b>

Minggu Ke-	Sub-CPMK (Kemampuan akhir yg direncanakan)	Bahan Kajian (Materi Pembelajaran)	Bentuk dan Metode Pembelajaran	Estimasi Waktu	Pengalaman Belajar Mahasiswa	Kriteria & Bentuk Penilaian	Indikator Penilaian	Bobot Penilaian (%)
		- Applications of standard and extended ACLs						
8	<b>Evaluasi Tengah Semester (Evaluasi Formatif-Evaluasi yg dimaksudkan untuk melakukan improvement proses pembelajaran berdasarkan assessment yang telah dilakukan)</b>							
9	Mahasiswa mampu menjelaskan langkah pencegahan serangan melalui jaringan komputer dengan menggunakan IDS dan IPS	<b>IDS DAN IPS</b> <ul style="list-style-type: none"> <li>- Implementing Intrusion Prevention</li> <li>- Intrusion Prevention Systems (IPS)</li> <li>- purpose and operation of network-based and host-based Intrusion Prevention Systems (IPS)</li> <li>- How IDS and IPS signatures are used to detect malicious network traffic</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Bentuk:</b> Kuliah</li> <li>• <b>Metode:</b> Diskusi Kelompok</li> </ul>	TM : 1x3x50' BT ; 180' BM : 180'	Tugas mensimulasikan penerapan IDS dan IPS	<ul style="list-style-type: none"> <li>• Tanya Jawab</li> <li>• Keaktifan dalam kelas</li> </ul>	Ketepatan menjelaskan pencegahan serangan jaringan komputer.	<b>15</b>
10	Mahasiswa mampu menjelaskan konfigurasi untuk mengamankan perangkat jaringan komputer yang dikelola	<b>PENGAMANAN PADA PERANGKAT</b> <ul style="list-style-type: none"> <li>- Securing the Local Area Network</li> <li>- Endpoint vulnerabilities and protection methods</li> <li>- Configure and verify switch security features, including port security and storm control</li> <li>- Fundamental security considerations of</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Bentuk:</b> Kuliah</li> <li>• <b>Metode:</b> Diskusi Kelompok</li> </ul>	TM : 1x3x50' BT ; 180' BM : 180'	Tugas mensimulasikan mengamankan perangkat jaringan komputer	<ul style="list-style-type: none"> <li>• Tanya Jawab</li> <li>• Keaktifan dalam kelas</li> </ul>	Ketepatan menjelaskan langkah mengamankan perangkat jaringan komputer.	<b>15</b>

Minggu Ke-	Sub-CPMK (Kemampuan akhir yg direncanakan)	Bahan Kajian (Materi Pembelajaran)	Bentuk dan Metode Pembelajaran	Estimasi Waktu	Pengalaman Belajar Mahasiswa	Kriteria & Bentuk Penilaian	Indikator Penilaian	Bobot Penilaian (%)
		Wireless, VoIP, and SANs						
11	Mahasiswa mampu menjelaskan jenis-jenis enkripsi pada komunikasi jaringan komputer	<b>Enkripsi:</b> <ul style="list-style-type: none"> <li>- Cryptographic Systems (1)</li> <li>- How the types of encryption, hashes, and digital signatures work together to provide confidentiality, integrity, and authentication</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Bentuk:</b> Kuliah</li> <li>• <b>Metode:</b> Diskusi Kelompok</li> </ul>	TM : 1x3x50' BT ; 180' BM : 180'	Tugas mensimulasikan mengamankan jaringan enkripsi dan deskripsi.	<ul style="list-style-type: none"> <li>• Quis</li> <li>• Tanya Jawab</li> <li>• Keaktifan dalam kelas</li> <li>• Tugas Individu</li> </ul>	Ketepatan menjelaskan cara enkripsi dan deskripsi	<b>15</b>
12	Mahasiswa mampu menjelaskan langkahlangkah untuk memastikan kesesuiandata setelah data dikirimkan melalui jaringan komputer	<b>INTEGRITY DATA:</b> <ul style="list-style-type: none"> <li>- Cryptographic Systems (2)</li> <li>- Mechanisms to ensure data integrity, authentication, and confidentiality</li> <li>- Mechanisms used to ensure data confidentiality and authentication using a public key</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Bentuk:</b> Kuliah</li> <li>• <b>Metode:</b> Diskusi Kelompok</li> </ul>	TM : 1x3x50' BT ; 180' BM : 180'	Tugas makalah penerapan Integrity data.	<ul style="list-style-type: none"> <li>• Tanya Jawab</li> <li>• Keaktifan dalam kelas</li> </ul>	Ketepatan menjelaskan menerapkan Integrity data	<b>10</b>
13-14	Mahasiswa mampu Menjelaskan fungsi, komponen, dan konfigurasi VPN	<b>VPN:</b> <ul style="list-style-type: none"> <li>- ImplementingVirtual Private Networks (1)</li> <li>- Purpose and operation of VPN types</li> <li>- purpose and operation of GREVPNs</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Bentuk:</b> Kuliah</li> <li>• <b>Metode:</b> Diskusi Kelompok</li> </ul>	TM : 2x3x50' BT ; 180' BM : 180'	Tugas mensimulasikan dan konfigurasi VPN.	<ul style="list-style-type: none"> <li>• Tanya Jawab</li> <li>• Keaktifan dalam kelas</li> </ul>	Ketepatan menjelaskan menerapkan VPN	<b>10</b>

Minggu Ke-	Sub-CPMK (Kemampuan akhir yg direncanakan)	Bahan Kajian (Materi Pembelajaran)	Bentuk dan Metode Pembelajaran	Estimasi Waktu	Pengalaman Belajar Mahasiswa	Kriteria & Bentuk Penilaian	Indikator Penilaian	Bobot Penilaian (%)
		- components and operations of IPsec VPNs						
15	Mahasiswa mampu menjelaskan Prinsip-prinsip, fungsi, tujuan, peran, serta struktur kebijakan dalam mengamankan jaringan komputer	<b>Struktur Kebijakan:</b> <ul style="list-style-type: none"> <li>- Managing a Secure Network</li> <li>- Principles of secure network design</li> <li>- Role of operations security in a network</li> <li>- Various techniques and tools to use for network security testing</li> <li>- Functions, goals, role, and structure of a comprehensive security policy</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Bentuk:</b> Kuliah</li> <li>• <b>Metode:</b> Diskusi Kelompok</li> </ul>	TM : 1x3x50' BT ; 180' BM : 180'	Tugas mensimulasikan dan konfigurasi struktur kebijakan dalam pengamanan.	<ul style="list-style-type: none"> <li>• Tanya Jawab</li> <li>• Keaktifan dalam kelas</li> </ul>	Ketepatan menjelaskan menerapkan struktur kebijakan	<b>10</b>
16	<b>Evaluasi Akhir Semester (Evaluasi yg dimaksudkan untuk mengetahui capaian akhir hasil belajar mahasiswa)</b>							

**Catatan:**

.....

.....

.....