UNIVERSITAS NEGERI MANADO
FAKULTAS TEKNIK
PROGRAM STUDI TEKNIK INFORMATIKA

RENCANA PEMBELAJARAN SEMESTER (RPS)

Nama Mata Kuliah	Kode	Rumpun MK	Bobot		Semester	Tahun Ajaran
Network Intrusion Detection	5662668	Sistem Terdistribusi	T = 1	P = 1		Ganjil 2025/2026

Otorisasi/Pengesahan	Pengembang RPS	Koordinator MK	Koordinator Prodi
	Tim Pengembang RPS Prodi TI	Kristofel Santa, S.ST, M.MT	**Kristofel Santa, S.ST, M.MT**

Capaian Pembelajaran Mata Kuliah	Capaian Pembelajaran Lulusan Program Studi (CPL Prodi) yang Dibebankan pada Mata Kuliah	
	CPL-1	Mampu menerapkan pengetahuan di bidang informatika untuk menyelesaikan permasalahan kompleks.
	CPL-2	Mampu menganalisis kebutuhan sistem informasi dan merancang solusi berbasis teknologi.
	CPL-3	Mampu merancang dan mengimplementasikan sistem keamanan jaringan dan informasi.
	CPL-4	Mampu berkomunikasi efektif, bekerja dalam tim, dan menjunjung tinggi etika profesi.
	CPL-5	Mampu belajar secara mandiri dan beradaptasi terhadap perkembangan teknologi informasi terkini.
	Capaian Pembelajaran Mata Kuliah (CPMK)	
	CPMK-1	Mahasiswa mampu menjelaskan konsep dasar serangan jaringan dan sistem deteksi intrusi (IDS).
	CPMK-2	Mahasiswa mampu mengidentifikasi jenis-jenis serangan berdasarkan pola lalu lintas jaringan.
	CPMK-3	Mahasiswa mampu mengkonfigurasi dan menggunakan tools IDS seperti Snort atau Suricata.
	CPMK-4	Mahasiswa mampu menganalisis log hasil IDS dan memberikan rekomendasi mitigasi.

	CPMK-5	Mahasiswa mampu mengembangkan sistem deteksi intrusi berbasis aturan dan pembelajaran mesin.				
	Kemampuan Akhir Tiap Tahapan Belajar (Sub-CPMK)					
	Sub-CPMK-1	Menjelaskan konsep dasar serangan jaringan, jenis ancaman, dan mekanisme IDS				
	Sub-CPMK-2	Mengklasifikasikan serangan berdasarkan lalu lintas jaringan dan pola signature.				
	Sub-CPMK-3	Menggunakan dan mengkonfigurasi IDS berbasis signature (Snort) dan anomaly-based.				
	Sub-CPMK-4	Menganalisis log IDS dan mendeteksi anomali atau serangan secara manual maupun otomatis.				
	Sub-CPMK-5	Mendesain IDS berbasis AI atau machine learning sederhana				
	Korelasi CPMK terhadap Sub-CPMK					
		Sub-CPMK-1	Sub-CPMK-2	Sub-CPMK-3	Sub-CPMK-4	Sub-CPMK-5
	CPMK-1	Menjelaskan konsep dasar serangan jaringan, jenis ancaman, dan mekanisme IDS				
	CPMK-2		Mengklasifikasikan serangan berdasarkan lalu lintas jaringan dan pola signature			
	CPMK-3			Menggunakan dan mengkonfigurasi IDS berbasis signature (Snort) dan anomaly-based		
	CPMK-4				Menganalisis log IDS dan	

<table>
<tr><td></td><td></td><td></td><td></td><td></td><td>mendeteksi anomali atau serangan secara manual maupun otomatis</td><td></td></tr>
<tr><td></td><td>CPMK-5</td><td></td><td></td><td></td><td></td><td>Mendesain IDS berbasis AI atau machine learning sederhana</td></tr>
<tr><td>Deskripsi Singkat Mata Kuliah</td><td colspan="6">Mata kuliah ini membahas konsep, teknik, dan implementasi sistem deteksi intrusi dalam jaringan komputer. Mahasiswa akan mempelajari dasar-dasar serangan jaringan, jenis-jenis IDS, konfigurasi tools seperti Snort dan Suricata, serta penggunaan metode analitik dan machine learning untuk deteksi dan mitigasi serangan. Mata kuliah ini menggabungkan teori dan praktik untuk meningkatkan kemampuan analisis dan pemecahan masalah dalam keamanan jaringan.</td></tr>
<tr><td rowspan="14">Bahan Kajian Materi Pembelajaran</td><td colspan="6">Pengantar Keamanan Jaringan, Definisi IDS, Tipe-tipe IDS, Karakteristik Serangan Jaringan</td></tr>
<tr><td colspan="6">Arsitektur IDS, Komponen IDS, Posisi IDS dalam Topologi Jaringan</td></tr>
<tr><td colspan="6">Kategori Serangan Jaringan: DoS, DDoS, Spoofing, MITM, Malware, dan Exploit</td></tr>
<tr><td colspan="6">Tanda-tanda Serangan (Signatures) dan Pola Lalu Lintas Jaringan yang Mencurigakan</td></tr>
<tr><td colspan="6">Studi Kasus Analisis Data Serangan Berdasarkan Signature dan Behavior</td></tr>
<tr><td colspan="6">Instalasi dan Konfigurasi Dasar Snort</td></tr>
<tr><td colspan="6">Pembuatan dan Penggunaan Rule di Snort</td></tr>
<tr><td colspan="6">Studi Kasus: Simulasi Serangan dan Deteksi dengan Snort</td></tr>
<tr><td colspan="6">IDS berbasis Anomali: Konsep Dasar dan Contoh Implementasi</td></tr>
<tr><td colspan="6">Format Log IDS (Snort, Suricata), Teknik Pembacaan dan Interpretasi Log</td></tr>
<tr><td colspan="6">Deteksi Anomali melalui Log Analisis Menggunakan Tools (Wireshark, Zeek, ELK Stack)</td></tr>
<tr><td colspan="6">Studi Kasus: Investigasi Serangan Berdasarkan Log IDS</td></tr>
<tr><td colspan="6">Pengenalan Machine Learning untuk Intrusion Detection</td></tr>
<tr><td colspan="6">Dataset IDS (KDD99, NSL-KDD, CICIDS2017), Teknik Feature Selection</td></tr>
</table>

	Implementasi IDS ML Sederhana (misalnya dengan Decision Tree atau KNN menggunakan Python/Scikit-learn)
	Presentasi Proyek Mini dan Ujian Akhir
Bahan Pustaka	1. Northcutt, S. & Novak, J. (2002). *Network Intrusion Detection: An Analyst's Handbook*. New Riders. 2. Scarfone, K., & Mell, P. (2007). *Guide to Intrusion Detection and Prevention Systems (IDPS)*, NIST. 3. Bejtlich, R. (2005). *The Tao of Network Security Monitoring: Beyond Intrusion Detection*. Addison-Wesley. 4. Bace, R. (2000). *Intrusion Detection*. Macmillan Technical Publishing 5. Choraś, M. (2013). *Advanced Intrusion Detection Systems*. Springer. 6. Kshetri, N. (2020). *Artificial Intelligence in Cybersecurity*. IT Professional, IEEE. 7. Modi, C. et al. (2013). *A survey of intrusion detection techniques in Cloud*. Journal of Network and Computer Applications. 8. Snort.org – Official Documentation and Rule Development Guide. 9. Suricata.io – Suricata IDS Documentation. 10. CICIDS2017, NSL-KDD Dataset Documentation (https://www.unb.ca/cic/datasets/)
Dosen Pengampu	Kristofel Santa, S.ST, M.MT
Mata Kuliah Prasyarat	-

Mg ke-	**Kemampuan Akhir Tiap Tahapan Belajar (Sub-CPMK)**	**Penilaian**		**Bentuk Pembelajaran; Metode Pembelajaran; Penugasan Mahasiswa; Estimasi Waktu**		**Materi Pembelajaran**	**Bobot Penilaian (%)**
		Indikator	**Bentuk Penilaian**	**Luring**	**Daring**		
(1)	**(2)**	**(3)**	**(4)**	**(5)**	**(6)**	**(7)**	**(8)**
1	Menjelaskan konsep dasar IDS dan ancaman jaringan	Menjelaskan definisi dan fungsi IDS	Jawaban ≥70% benar Teknik: Tes awal	a. Ceramah pengantar konsep dasar b. Tanya jawab (diskusi kasus	Membuat rangkuman dari video pengantar IDS	[1], [2], [3]	5%

				nyata serangan) c. Quiz klasikal			
2	Menjelaskan komponen dan arsitektur IDS	Menguraikan komponen dan arsitektur IDS	Struktur lengkap dan akurat Teknik: Quiz	a. Kuliah interaktif b. Case method: studi arsitektur open-source IDS c. Penugasan bagan arsitektur	Forum diskusi tentang arsitektur IDS	[1], [3]	5%
3	Mengklasifikasikan jenis serangan jaringan	Mengelompokkan serangan berdasarkan tipe	Klasifikasi tepat ≥70% Teknik: Quiz	a. Kuliah deskriptif b. Diskusi kasus: klasifikasi serangan malware/DDOS c. Tugas klasifikasi serangan	Tugas membuat infografis jenis serangan	[4], [5]	5%
4	Menganalisis pola signature serangan	Menjelaskan konsep signature	Pola sesuai signature Teknik: Diskusi	a. Kuliah singkat tentang IDS berbasis signature b. Case method: identifikasi pola dari rule Snort c. Tugas menandai pola signature	Penugasan membaca dan menganalisis file rule	[1], [5]	5%
5	Studi kasus analisis data serangan	Mengidentifikasi anomali dari log PCAP	Temuan minimal 2 serangan Teknik: Observasi	a. Kuliah teknis dasar analisis trafik b. Case method: analisis file PCAP c. Penugasan laporan analisis	Penugasan identifikasi log mencurigakan	[5], [6]	5%

				serangan			
6	Menggunakan dan mengkonfigurasi Snort dasar	Konfigurasi Snort berhasil dijalankan	Snort aktif & output log Teknik: Praktikum	a. Kuliah: instalasi dan sintaks dasar b. Praktikum konfigurasi Snort c. Penugasan dokumentasi konfigurasi	Instalasi Snort secara mandiri & kirim log	[5], [6]	15%
7	Membuat dan menerapkan rule Snort	Rule mendeteksi paket	Deteksi berhasil & sesuai rule Teknik: Observasi	a. Kuliah singkat rule engine b. Project based: menulis dan uji rule buatan sendiri c. Penugasan upload konfigurasi	Menulis dan menguji rule sederhana	[8], [9]	5%
8	Simulasi serangan & deteksi IDS	Snort mendeteksi serangan	Output log menunjukkan deteksi Teknik: Praktik	a. Praktikum simulasi serangan dengan tools b. Case method: pengujian IDS c. Laporan simulasi deteksi	Tidak ada (fokus luring)	[1], [8]	5%
	UTS						
9	Menjelaskan IDS berbasis anomaly	Menjelaskan perbedaan signature vs anomaly	Penjelasan logis dan jelas Teknik: Tugas	a. Ceramah komparatif b. Diskusi kasus IDS anomaly pada sistem besar c. Presentasi mini	Tugas esai tentang IDS anomaly-based	[5], [6]	5%

				tugas daring			
10	Membaca dan memahami log IDS	Membaca dan menjelaskan struktur log	Interpretasi akurat Teknik: Praktik	a. Kuliah: struktur log b. Praktikum membaca dan menjelaskan isi log c. Tugas review log harian	Penugasan membaca log format Suricata	[8], [9]	5%
11	Menganalisis log untuk deteksi serangan	Menyimpulkan pola dari log	Temuan logis dan didukung data Teknik: Analisis	a. Kuliah lanjutan log analitik b. Case method: eksplorasi data IDS c. Tugas analisis file log	Penugasan analisis log menggunakan dataset	[9], [10]	10%
12	Investigasi berdasarkan log IDS	Menyusun proses investigasi	Investigasi valid dan sistematis Teknik: Laporan	a. Kuliah investigasi digital b. Case method: penyelidikan berbasis log c. Penugasan: kronologi serangan	Penugasan studi kasus log serangan	[6], [10]	5%
13	Mendesain IDS berbasis ML (konsep & dataset)	Mendesain pendekatan IDS-ML	Dataset dan desain logis Teknik: Presentasi	a. Kuliah model ML pada IDS b. Project based learning: desain arsitektur ML sederhana c. Tugas desain sistem IDS ML	Penugasan desain awal sistem ML + dataset	[6], [7], [10]	10%

14	Seleksi fitur dan preprocessing data	Memilih fitur penting dan bersihkan data	Fitur relevan & proses benar Teknik: Praktikum	a. Kuliah teknik preprocessing b. Praktikum cleaning data NSL-KDD c. Tugas eksplorasi fitur dataset	Penugasan preprocessing dataset IDS	[6], [10]	5%
15	Seleksi fitur dan preprocessing data	Model berjalan dan akurat ≥70%	Evaluasi model Teknik: Uji praktik	a. Ceramah evaluasi model b. Praktikum build & test model klasifikasi c. Tugas validasi hasil deteksi	Tugas evaluasi dan dokumentasi model	[6], [7]	5%
16	Evaluasi akhir (Proyek & Ujian)	Menyelesaikan proyek & menjawab ujian	Penilaian Proyek + Ujian Akhir Teknik: Presentasi + Tes	a. Presentasi proyek mini IDS b. Ujian akhir teori & praktik c. Penilaian akhir proyek	Kirim dokumentasi proyek final	Semua	5%
	UAS						

SISTEM PENILAIAN DAN SISTEM EVALUASI

A. Sistem Penilaian

1. Sistem penilaian menggunakan penilaian acuan pokok pada RPS.
2. Komponen, bobot, dan rentang penilaian sebagai berikut:

- Komponen: nilai kompetensi (CPMK) sebesar 90% dan nilai kehadiran sebesar 10%.

- Nilai akhir mata kuliah = jumlah nilai CPMK + nilai kehadiran.
- Bobot masing-masing CPMK dan kehadiran dapat dilihat pada tabel berikut:

No.	**Kompetensi dan Kehadiran**	**Bobot Penilaian**						**Target Pengukuran**	
		Tugas (10%)	**Quiz (10%)**	**UTS (15%)**	**UAS (15%)**	**Project (50%)**	**Kehadiran**	**Maksimal**	**Konversi**
1.	CPMK-1	3%	2%	3%	3%	-	-	100	≥ 70 = Lulus
2.	CPMK-2	2%	2%	3%	3%	10%	-	100	≥ 70 = Lulus
3.	CPMK-3	2%	2%	3%	3%	10%	-	100	≥ 70 = Lulus
4.	CPMK-4	2%	2%	3%	3%	10%	-	100	≥ 70 = Lulus
5.	CPMK=5	1%	2%	3%	3%	20%	-	100	≥ 70 = Lulus
6.	Kehadiran	-	-	-	-	-	0%	100	≥ 80 = Lulus
TOTAL		**10%**	**10%**	**15%**	**15%**	**50%**	**0%**	**100%**	

- Rentang penilaian huruf mengikuti tabel berikut.

No.	**Rentang Nilai Angka Skala 100**	**Nilai Angka Skala 4**	**Nilai Huruf**
1.	80,00 – 100,00	4,00	A
2.	68,00 – 79,99	3,00	B
3.	56,00 – 67,99	2,00	C
4.	45,00 – 55,99	1,00	D
5.	00,00 – 44,99	0,00	E

B. Sistem Evaluasi

1. Mahasiswa dinyatakan lulus dalam mata kuliah ini bila nilai minimal D.
2. Nilai kehadiran mahasiswa dalam perkuliahan harus lebih dari 75%, bila kurang dari nilai tersebut maka nilai otomatis E.