	INSTITUT SAINS DAN TEKNOLOGI NASIONAL **PROGRAM STUDI MAGISTER TEKNIK ELEKTRO** **Master of Science in Cybersecurity and Defense - MSCD**	RPS-MKE-CS-001

RENCANA PEMBELAJARAN SEMESTER (RPS)

Mata Kuliah	Kode MK	Rumpun MK	Bobot SKS		Semester	Tgl. Penyusunan
Advanced Network Security Specialization	MTE-CS-001	Operating Systems Security	T = 2 SKS	P = 0 SKS	1	1 Maret 2025

OTORISASI	Pengembang RPS	Koordinator Rumpun MK	Kaprodi
	(Dr. Ir. Kuntjoro Pinardi MSc)	(Dr. Ir. Kuntjoro Pinardi MSc)	

Capaian Pembelajaran (CP)	CPL/SO-Prodi yang dibebankan pada MK – Student Outcome (SO)	
	CPL/SO 1	Mastery of Cybersecurity and Defense Technologies
	CPL/SO 3	Data-Driven Innovation and Analytics
	CPL/SO 4	Project Management and Practical Application
	CPL/SO 5	Ethics, Sustainability, and Social Responsibility
	CPL/SO 6	Communication, Certification, and Lifelong Learning
	Capaian Pembelajaran Mata Kuliah (CO) or Course Objective (CO)	
	Understand the security fundamentals of operating systems, including authentication, access control, and encryption.	

	Develop practical skills in system administration and security configuration for Windows and Linux environments.
	Analyze vulnerabilities and security threats in operating systems and propose mitigation strategies.
	Apply industry-standard security frameworks and tools to enhance operating system security.

Korelasi CO dan CPL/SO

CO	SO1	SO2	SO3	SO4	SO5	SO6
CO1	X				X	
CO2	X		X			
CO3	X			X		
CO4			X			X

Kemampuan akhir tiap tahapan belajar (Sub-CO) – Course Outcome

Sub-CO1	Explain authentication, access control, and encryption techniques in operating systems.
Sub-CO2	Configure security settings and harden operating systems against cyber threats.
Sub-CO3	Analyze and assess operating system vulnerabilities using security tools.
Sub-CO4	Implement security policies and apply forensic analysis in response to security incidents.
Sub-CO5	Security frameworks, such as CIS benchmarks and NIST guidelines, are applied in system security management.

Korelasi CO terhadap Sub-CO

Sub-CO	CO1	CO2	CO3	CO4
Sub-CO1	X			
Sub-CO2		X		
Sub-CO3			X	
Sub-CO4			X	
Sub-CO5				X
Sub-CO6				X

Korelasi CPL/SO dan Sub-COTerhadap Bobot Penilaian

Sub-CO	SO1 (%)	SO2 (%)	SO3 (%)	SO4 (%)	SO5 (%)	SO6 (%)	Total Weight (%)	Number of Weeks
Sub-CO1	10	0	0	0	5	0	15	2
Sub-CO2	10	0	5	0	0	0	15	2
Sub-CO3	10	0	5	0	0	0	15	2
Sub-CO4	0	0	0	10	0	5	15	2
Sub-CO5	0	0	0	10	0	10	20	3
Sub-CO6	0	0	0	0	0	20	20	3
TOTAL	30	0	10	20	5	35	100	14

Deskripsi singkat MK	This course thoroughly examines operating system security principles, covering authentication, access control, encryption, security configurations, system administration, and vulnerability management. Students will develop hands-on skills in securing Linux and Windows systems, identifying security threats, and applying security best practices aligned with industry frameworks.	
Bahan Kajian: Materi Pembelajaran	The Operating Systems Security course provides in-depth knowledge of securing Linux and Windows environments, focusing on authentication, access control, encryption, system hardening, and vulnerability assessment. Students will learn to configure security settings, analyze risks using security tools, and implement security frameworks such as CIS benchmarks and NIST guidelines. The course emphasizes forensic analysis, incident response, and compliance with industry standards. Through hands-on labs and case studies, students develop practical skills in system security management, ensuring resilience against cyber threats. By the end of the course, they will be proficient in securing operating systems and responding to security incidents effectively.	
Pustaka	**Utama:**	**Pendukung:**

	1. IBM & ISC2. (2023). *Cybersecurity Specialist Training Guide*.	1. Semua *e-book* dan jurnal-jurnal terkait dengan materi setiap pertemuan 2. Garfinkel, S., & Spafford, G. (2020). *Practical UNIX and Internet Security* (3rd ed.). O'Reilly Media.
Dosen Pengampu:	Dr. Ir. Kuntjoro Pinardi, MSc	
MK Prasyarat:	None	

Advanced Network Security Course Plan (14 Weeks)

Week	Sub-CO	Learning Activities and Assignments	Learning Materials & References	Assessment & Criteria	Online Learning Mode	Weight (%)
1	**Sub-CO1**	Introduction to Operating System Security: Principles & Concepts	IBM ISC2 Cybersecurity Guide, Modern OS Book	Discussion participation	Online lecture & discussion	7%
2	**Sub-CO1**	Authentication, Access Control, and Encryption in OS	NIST Guidelines, Modern OS Book	Report writing	Online lecture, independent study	7%
3	**Sub-CO2**	System Hardening: Security Configurations for Windows & Linux	CIS Benchmarks, Security Hardening Guides	Lab exercises	Online lecture, hands-on lab	8%

4	**Sub-CO2**	Secure Boot, BIOS/UEFI, and Firmware Protection	Security Compliance Reports	Practical security configuration	Online lecture, case study discussion	8%
5	**Sub-CO3**	OS Vulnerabilities and Exploitation Analysis	IBM ISC2 Cybersecurity Guide	Research report	Online lecture, case study discussion	5%
6	**Sub-CO3**	Malware Analysis and Threat Detection in OS	Threat Intelligence Reports	Threat assessment report	Online lecture, lab session	5%
7	**Sub-CO4**	Incident Response and Digital Forensics	Cybersecurity Case Studies	Incident response report	Online lecture, forensic lab	5%
8	**Sub-CO4**	Security Logging, Monitoring, and SIEM Integration	Log Analysis Frameworks	Security monitoring project	Online lecture, hands-on lab	5%
9	**Sub-CO5**	OS Security Policies: Compliance and Legal Regulations	ISO 27001, NIST Guidelines	Policy compliance audit	Online lecture, report writing	5%
10	**Sub-CO5**	Patch Management and Security Updates	Patch Management Frameworks	Patch deployment assessment	Online lecture, practical session	5%
11	**Sub-CO6**	Security Automation & AI in OS Security	AI-Based Security Tools	Security automation report	Online lecture, case	5%

					study discussion	
12	**Sub-CO6**	Cloud & Virtualized OS Security	Cloud Security Frameworks	Cloud OS security implementation	Online lecture, hands-on cloud lab	5%
13	**Capstone**	Capstone Project: OS Security Audit & Implementation	Research & Industry Reports	Final project presentation	Online mentoring, project work	15%
14	**Final Exam**	Comprehensive Exam on OS Security	Course Review Materials	Exam performance	Online proctored exam	15%

Rubric for Presentation Assessment (Perception-Based)

Aspect Assessed	Very Poor	Poor	Adequate	Good	Excellent
	< 20	21 – 40	41 – 60	61 – 80	> 80
Communication Skills (15%)					
Mastery of Content (15%)					
Ability to Answer Questions (15%)					
Use of Visual Aids (5%)					
Accuracy in Problem-Solving (50%)					
FINAL SCORE					

Rubric for Observation-Based Assessment

Aspect Assessed	Very Poor	Poor	Adequate	Good	Excellent
	< 20	21 – 40	41 – 60	61 – 80	> 80
Fieldwork Engagement (20%)					
Mastery of Subject Matter (20%)					
Ability to Select Relevant Observation Data (30%)					
Ability to Correlate Observations with Project Solutions (30%)					
FINAL SCORE					

Rubric for Oral Exam and Class Participation Assessment

Aspect Assessed	Very Poor	Poor	Adequate	Good	Excellent
	< 20	21 – 40	41 – 60	61 – 80	> 80
Class Activity/Participation (20%)					
Mastery of Subject Matter (35%)					
Accuracy in Answering Questions (45%)					
FINAL SCORE					

Rubric for Performance-Based Assessment and Written Test

Aspect Assessed	Very Poor	Poor	Adequate	Good	Excellent
	< 20	21 – 40	41 – 60	61 – 80	> 80
Ability to Develop a Comprehensive Performance Plan (20%)					
Mastery of Subject Matter (35%)					
Ability to Solve Cases or Projects Based on Performance Plan (45%)					
FINAL SCORE					