TKIF262502

Keamanan Siber

INFORMASI MATA KULIAH	
SKS	3
Status MK	Pilihan
Klasifikasi MK/ Spesialisasi	Rekayasa
Prasyarat	Jaringan Komputer

CPL DAN CPMK

Capaian Pembelajaran Mata Kuliah		CPL	Metode Assessmen
CPMK1	Mahasiswa mampu membuat aplikasi mobile yang aman dengan mematuhi standar privasi data pengguna.	(a) Menjunjung Tinggi Etika dan Tanggung Jawab Profesional	Tugas-Proyek;Kuis-Pilihan Ganda
CPMK2	Mahasiswa mampu merencanakan strategi keamanan jaringan secara bertanggung jawab untuk melindungi informasi organisasi.	(a) Menjunjung Tinggi Etika dan Tanggung Jawab Profesional	Tugas-Analisis Studi Kasus;UTS-Essay
CPMK3	Mahasiswa mampu menerapkan algoritma penyandian (kriptografi) untuk menjamin kerahasiaan data sesuai kode etik profesi.	(c) Merancang dan mengimplementasikan solusi	Tugas-Latihan;Kuis-Essay
CPMK4	Mahasiswa mampu membangun sistem pembuktian identitas (autentikasi) dan tanda tangan digital untuk mencegah pemalsuan data.	(c) Merancang dan mengimplementasikan solusi	Tugas-Proyek;UTS-Essay
CPMK5	Mahasiswa mampu mengatur infrastruktur kunci publik (PKI) untuk memastikan keamanan komunikasi antar pengguna.	(a) Menjunjung Tinggi Etika dan Tanggung Jawab Profesional	Tugas-Latihan;Kuis-Essay
CPMK6	Mahasiswa mampu merancang benteng pertahanan jaringan menggunakan Firewall dan VPN untuk menjaga kedaulatan data.	(c) Merancang dan mengimplementasikan solusi	Tugas-Proyek;UAS-Proyek & Presentasi

DESKRIPSI MATAKULIAH

Matakuliah ini membahas tentang konsep dan istilah dalam sistem keamanan jaringan komputer, Model Keamanan Sistem, dan Algoritma Kriptografi

REFERENSI

[1] Mike Chapple & David Seidl, CompTIA Security+ Study Guide: Exam SY0-701, Edisi ke-9, Sybex (Wiley), 2024

[2] William Stallings, Cryptography and Network Security: Principles and Practice, Edisi ke-8 (Global Edition), Pearson, 2022.

[3]Stephen Thomas , 2000, SSL and TLS Essential Securing the Web, John Wiley and Sons

[4] Ivan Ristić, Bulletproof TLS and PKI, Edisi ke-2, Feisty Duck, 2022.

TOPIK			
Topik	**Deskripsi Topik (referensi)**	**Metode Penyampaian**	**CPMK**

Pendahuluan Keamanan & Komputasi Mobile	1.1 Konsep Keamanan Jaringan Komputer, 1.2 Arsitektur Komputasi Mobile, 1.3 Keamanan pada Perangkat Bergerak (Ref [1])	Ceramah & Tanya Jawab	CPMK1
Pengembangan Aplikasi Mobile Aman	2.1 Siklus Pengembangan Aplikasi Mobile, 2.2 Implementasi Security-by-Design, 2.3 Penyimpanan Data Lokal yang Aman (Ref [1])	Proyek & Latihan	CPMK1
Perencanaan Strategi Keamanan Jaringan	3.1 Identifikasi Aset dan Ancaman Jaringan, 3.2 Pembuatan Kebijakan Keamanan (Security Policy), 3.3 Kerangka Kerja Pertahanan Berlapis (Ref [1])	Diskusi & Studi Kasus	CPMK2
Keamanan Komunikasi Aplikasi Mobile	4.1 Protokol Komunikasi Mobile, 4.2 Keamanan API dan Backend, 4.3 Manajemen Sesi pada Perangkat Mobile (Ref [1], [2])	Latihan & Tanya Jawab	CPMK2
Manajemen Risiko & Penilaian Kerentanan	5.1 Risk Assessment Jaringan, 5.2 Strategi Mitigasi Ancaman, 5.3 Business Continuity Planning (Ref [1])	Studi Kasus & Diskusi	CPMK3
Kontrol Akses & Identitas dalam Strategi Jaringan	6.1 Model Kontrol Akses (MAC, DAC, RBAC), 6.2 Perencanaan Autentikasi Terpusat, 6.3 Strategi Keamanan Host (Ref [1])	Tanya Jawab & Latihan	CPMK3
Audit & Kepatuhan Keamanan Jaringan	7.1 Teknik Audit Jaringan, 7.2 Standar Kepatuhan Keamanan (Compliance), 7.3 Pelaporan dan Evaluasi Strategi (Ref [1])	Latihan & Diskusi	CPMK3
Ujian Tengah Semester			
Dasar-Dasar Kriptografi	8.1 Sejarah dan Konsep Kriptografi, 8.2 Prinsip Algoritma Kriptografi, 8.3 Kriptanalisis Sederhana (Ref [2])	Ceramah & Latihan	CPMK4

Algoritma Kriptografi Simetris & Asimetris	9.1 Implementasi DES/AES, 9.2 Implementasi RSA dan Diffie-Hellman, 9.3 Manajemen Kunci (Ref [2])	Latihan & Proyek	CPMK4
Integritas Data & Fungsi Hash	10.1 Konsep Fungsi Hash (MD5, SHA), 10.2 Message Authentication Code (MAC), 10.3 Implementasi Checksum untuk Integritas (Ref [2])	Latihan & Tanya Jawab	CPMK5
Mekanisme Autentikasi & Privasi	11.1 Protokol Autentikasi Jaringan, 11.2 Implementasi Enkripsi End-to-End untuk Privasi, 11.3 Tantangan Privasi di Jaringan Publik (Ref [2], [3])	Studi Kasus & Proyek	CPMK5
Tanda Tangan Digital (Digital Signature)	12.1 Konsep Non-Repudiation, 12.2 Prosedur Pembuatan Tanda Tangan Digital, 12.3 Verifikasi Sertifikat Digital (Ref [2], [3])	Latihan & Proyek	CPMK6
Protokol Komunikasi Aman (SSL/TLS)	13.1 Arsitektur SSL/TLS, 13.2 Proses Handshake dan Pertukaran Kunci, 13.3 Implementasi HTTPS pada Layanan Web (Ref [3])	Tanya Jawab & Praktik	CPMK6
Proyek Akhir Implementasi Kriptografi & Autentikasi	14.1 Integrasi Algoritma pada Sistem Jaringan, 14.2 Pengujian Mekanisme Autentikasi dan Privasi, 14.3 Dokumentasi Teknis (Ref [2], [3])	Proyek & Presentasi	CPMK6
Ujian Akhir Semester			