# RENCANA PEMBELAJARAN SEMESTER
## KEAMANAN INFORMASI

**Oleh**
**Hario Jati Setyadi, S.Kom., M.Kom**

**KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN**
**PROGAM STUDI SISTEM INFORMASI**
**FAKULTAS TEKNIK**
**UNIVERSITAS MULAWARMAN**
**2022**

# HALAMAN PENGESAHAN

| | | |
|---|---|---|
| Revisi Ke - | : | 3 |
| Mata Kuliah | : | Kemanan Informasi |
| Kode Mata Kuliah | : | 190903603W020 |
| SKS | : | 3 |
| Semester | : | IV (Empat) / Genap |
| Program Studi | : | Sistem Informasi |
| Fakultas | : | Teknik |
| Perguruan Tinggi | : | Universitas Mulawarman |
| Dosen Penyusun / Pengampu | : | Hario Jati Setyadi, S.Kom., M.Kom. |

Samarinda, 18 Mei 2022

Menyetujui,
Koordinator Prodi Sistem Informasi.

Islamiyah, S.Kom., M.Kom
NIP. 198701162015042001

Penyusun,
Dosen Pengampu,

Hario Jati Setyadi , S.Kom., M.Kom.
NIP. 198612182019031007

Mengesahkan,
a.n Dekan
Wakil Dekan Bidang Akademik, Kemahasiswaan dan Alumni,

Dr. Ir. Tamrin, S.T., M.T., IPU.
NIP. 197002272000121001

# MATA KULIAH KEAMANAN INFORMASI

1. **Deskripsi Mata Kuliah**

   Mata kuliah ini yang membahas prinsip-prinsip dan praktek keamanan sistem informasi yang ada yang dibahas secara mendalam dan komprehensif. Topik meliputi konsep dasar keamanan sistem informasi, teknik penyerangan umum, kebijakan keamanan bersama, kriptografi, otentikasi, kontrol akses, deteksi intrusi jaringan, keamanan jaringan, masalah hukum dan etika dalam keamanan sistem informasi.

2. **Capaian Pembelajaran Lulusan (CPL)**
   - **CPL01** Mampu memahami, menganalisis, dan menilai konsep dasar dan peran sistem informasi dalam mengelola data dan memberikan rekomendasi pengambilan keputusan pada proses dan sistem organisasi.
   - **CPL04** Mampu memahami dan menerapkan kode etik dalam penggunaan informasi dan data pada perancangan, implementasi dan penggunaan suatu sistem.
   - **CPL05** Memiliki kemampuan merencanakan, menerapkan, memelihara dan meningkatkan sistem informasi untuk mencapai tujuan dan sasaran organisasi yang strategis baik jangka pendek maupun jangka panjang.

3. **Capaian Pembelajaran Mata Kuliah (CPMK)**

   Setelah mengikuti mata kuliah Basis Data :
   - **CPMK01** Mahasiswa mampu memahami konsep dasar keamanan informasi, termasuk keamanan fisik jaringan dan pentingnya pengamanan aplikasi web dan server.
   - **CPMK02** Mahasiswa mampu menjelaskan dan menerapkan etika, hukum, serta mengikuti perkembangan tren dan isu dalam keamanan informasi global.
   - **CPMK03** Mahasiswa mampu melakukan persiapan lingkungan pengujian keamanan web termasuk instalasi OS dan tools yang dibutuhkan.
   - **CPMK04** Mahasiswa mampu melakukan reconnaissance dan teknik OSINT untuk mengumpulkan informasi awal dari target pengujian.
   - **CPMK05** Mahasiswa mampu melakukan pengujian keamanan aplikasi web menggunakan pendekatan penetration testing, baik dasar maupun lanjutan.

4. **Kemampuan Khusus (KK)**

   Setelah mengikuti mata kuliah Basis Data :
   1. Mahasiswa mampu memahami target kemampuan mahasiswa yang ingin dicapai melalui mata kuliah ini.
   2. Mahasiswa memahami dengan baik tentang keamanan fisik dari jaringan komputer pada suatu sistem informasi.
   3. Mahasiswa memahami dengan baik tentang keamanan fisik dari jaringan komputer pada suatu sistem informasi.
   4. Mahasiswa memahami pentingnya pengamanan aplikasi web.

5. Mahasiswa memahami pentingnya keamanan Web Server dengan melihat kasus nyata yang terjadi di dunia nyata.
6. Mahasiswa mampu memahami Mematuhi hukum, peraturan, dan etika dalam keamanan informasi global.
7. Mahasiswa mampu Mengikuti perkembangan tren dan isu keamanan informasi.
8. Mahasiswa mampu melakukan Persiapan Lab Web Penetration dan OS yang akan di pakai
9. Mahasiswa mengenal Jenis-jenis Keamanan Web Aplikasi dan Server
10. Mahasiswa mampu melakukan reconnaissance dan OSINT untuk mencari informasi terkait suatu target
11. Mahasiswa mampu melakukan penetration testing dasar.
12. Mahasiswa mengenal berbagai kerentanan yang ada pada aplikasi web dan melakukan pengujian dasar menggunakan tools Burp Suite.
13. Mahasiswa mampu melakukan pengujian lanjutan untuk kerentanan aplikasi web yang tidak dapat ditemukan oleh tools scanner.

## Pemetaan CPL Prodi Sistem Informasi dengan CPMK

| | |
|---|---|
| **CPL01** Mampu memahami, menganalisis, dan menilai konsep dasar dan peran sistem informasi dalam mengelola data dan memberikan rekomendasi pengambilan keputusan pada proses dan sistem organisasi | **CPMK01** Mahasiswa mampu memahami konsep dasar keamanan informasi, termasuk keamanan fisik jaringan dan pentingnya pengamanan aplikasi web dan server. |
| **CPL04** Mampu memahami dan menerapkan kode etik dalam penggunaan informasi dan data pada perancangan, implementasi dan penggunaan suatu sistem | **CPMK02** Mahasiswa mampu menjelaskan dan menerapkan etika, hukum, serta mengikuti perkembangan tren dan isu dalam keamanan informasi global. |
| **CPL05** Memiliki kemampuan merencanakan, menerapkan, memelihara dan meningkatkan sistem informasi untuk mencapai tujuan dan sasaran organisasi yang strategis baik jangka pendek maupun jangka panjang. | **CPMK03** Mahasiswa mampu melakukan persiapan lingkungan pengujian keamanan web termasuk instalasi OS dan tools yang dibutuhkan. |
| | **CPMK04** Mahasiswa mampu melakukan reconnaissance dan teknik OSINT untuk mengumpulkan informasi awal dari target pengujian. |
| | **CPMK05** Mahasiswa mampu melakukan pengujian keamanan aplikasi web menggunakan pendekatan penetration testing, baik dasar maupun lanjutan. |

# RENCANA PEMBELAJARAN SEMESTER

| Mata Kuliah | Kode Mata Kuliah | Rumpun Mata Kuliah | Bobot (SKS) | Semester | Tgl. Penyusunan |
|---|---|---|---|---|---|
| Keamanan Informasi | | Komputer | 3 | 4 | 10 Juli 2024 |

| | Koordinator Mata Kuliah | | Koordinator Program Studi |
|---|---|---|---|
| **Otorisasi / Pengesahan** | Hario Jati Setyadi, M.Kom. | | Koordinator Prodi Sistem Informasi.<br>Islamiyah, S.Kom., M.Kom<br>NIP. 198701162015042001 |

| | | |
|---|---|---|
| **Capaian Pembelajaran Lulusan (CPL)** | **Capaian Pembelajaran Lulusan Program Studi (CPL-PRODI) yang Dibebankan Pada Mata Kuliah** | |
| | CPL01 | Mampu memahami, menganalisis, dan menilai konsep dasar dan peran sistem informasi dalam mengelola data dan memberikan rekomendasi pengambilan keputusan pada proses dan sistem organisasi. |
| | CPL04 | Mampu memahami dan menerapkan kode etik dalam penggunaan informasi dan data pada perancangan, implementasi dan penggunaan suatu sistem. |
| | CPL05 | Memiliki kemampuan merencanakan, menerapkan, memelihara dan meningkatkan sistem informasi untuk mencapai tujuan dan sasaran organisasi yang strategis baik jangka pendek maupun jangka panjang. |
| | **Capaian Pembelajaran Mata Kuliah (CPMK)** | |
| | • **CPMK01** Mahasiswa mampu memahami konsep dasar keamanan informasi, termasuk keamanan fisik jaringan dan pentingnya pengamanan aplikasi web dan server.<br>• **CPMK02** Mahasiswa mampu menjelaskan dan menerapkan etika, hukum, serta mengikuti perkembangan tren dan isu dalam keamanan informasi global.<br>• **CPMK03** Mahasiswa mampu melakukan persiapan lingkungan pengujian keamanan web termasuk instalasi OS dan tools yang dibutuhkan. | |

| | |
|---|---|
| | • **CPMK04** Mahasiswa mampu melakukan reconnaissance dan teknik OSINT untuk mengumpulkan informasi awal dari target pengujian.<br>• **CPMK05** Mahasiswa mampu melakukan pengujian keamanan aplikasi web menggunakan pendekatan penetration testing, baik dasar maupun lanjutan. |
| **PIP yang Diintegrasikan** | a. Integritas: Mahasiswa didorong untuk berperilaku jujur, bertanggung jawab, dan memiliki etika profesional dalam setiap aspek pembelajaran dan penerapan keamanan informasi.<br>b. Kerja sama: Mahasiswa belajar bekerja sama dalam tim, baik dalam diskusi kelas, proyek kelompok, maupun dalam simulasi kasus keamanan informasi.<br>c. Kreativitas: Mahasiswa diharapkan mampu berpikir kreatif dalam merancang solusi keamanan informasi yang inovatif dan efektif.<br>d. Tanggung jawab: Mahasiswa dilatih untuk bertanggung jawab terhadap tugas dan proyek yang diberikan, serta memahami pentingnya menjaga keamanan informasi di lingkungan profesional.<br>e. Penguasaan Alat dan Teknologi Terkini: Mahasiswa dilatih menggunakan perangkat lunak dan alat keamanan informasi terkini seperti Wireshark, Metasploit, dan Nessus untuk mengatasi tantangan keamanan modern.<br>f. Adaptasi Terhadap Teknologi Baru: Mahasiswa diajarkan untuk terus mengikuti dan mengadaptasi teknologi baru dalam keamanan informasi seperti AI-driven security dan blockchain.<br>g. Kepatuhan Terhadap Hukum dan Etika: Mahasiswa memahami dan mematuhi hukum, peraturan, dan standar industri yang berlaku terkait keamanan informasi, serta mampu mengidentifikasi dan menangani isu-isu etika dalam praktik profesional.<br>h. Keterampilan Komunikasi: Mahasiswa dilatih untuk berkomunikasi secara efektif mengenai isu-isu keamanan informasi kepada berbagai pemangku kepentingan, baik teknis maupun non-teknis.<br>i. Pemahaman Konsep Dasar: Mahasiswa mendapatkan pemahaman yang mendalam tentang konsep dasar keamanan informasi, termasuk ancaman, kerentanan, dan risiko.<br>j. Kemampuan Analisis dan Evaluasi: Mahasiswa mampu menganalisis kebutuhan dan risiko keamanan informasi serta mengevaluasi dan mengoptimalkan sistem keamanan informasi dengan teknik modern. |

| | | |
|---|---|---|
| **Deskripsi Mata Kuliah** | mata kuliah ini membahas prinsip-prinsip dan praktek keamanan sistem informasi yang ada yang dibahas secara mendalam dan komprehensif. Topik meliputi konsep dasar keamanan sistem informasi, teknik penyerangan umum, kebijakan keamanan bersama, kriptografi, otentikasi, kontrol akses, deteksi intrusi jaringan, keamanan jaringan, masalah hukum dan etika dalam keamanan sistem informasi. | |
| **Referensi** | 1. Stallings, W., & Brown, L. (2019). Computer Security: Principles and Practice. Pearson.<br>2. Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems (3rd ed.). Wiley.<br>3. Harris, S. (2019). CISSP All-in-One Exam Guide, Eighth Edition. McGraw-Hill Education.<br>4. Ferguson, N., Schneier, B., & Kohno, T. (2021). Cryptography Engineering: Design Principles and Practical Applications. Wiley.<br>5. Bishop, M. (2021). Introduction to Computer Security. Addison-Wesley.<br>6. Offensive Security. (2021). *Kali Linux Revealed: Mastering the Penetration Testing Distribution*. Offensive Security.<br>7. Conti, M., Dragoni, N., & Gottardo, S. (2020). Blockchain Security and Privacy. Springer.<br>8. Weippl, E. (2022). Security in Computing and Information Technology. Springer.<br>9. Easttom, C. (2023). Network Defense and Countermeasures: Principles and Practices. Pearson.<br>10. Juels, A., & Garay, J. (2024). Cryptographic Systems for Secure Applications. Cambridge University Press.<br>11. Stallings, W. (2023). Network Security Essentials: Applications and Standards. Pearson. | |
| **Media Pembelajaran** | **Perangkat lunak :** | **Perangkat keras :** |
| | Figma | Laptop |
| **Mata Kuliah Prayarat (Jika ada)** | Manajenen jaringan Komputer , Sistem Operasi | |

| Perte-muan ke | Sub-CPMK | Indikator | Bahan Kajian | Strategi Pembelajaran (Model dan Metode) | Pengalaman Belajar Mahasiswa | Penilaian | | | Referensi |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | Jenis | Kriteria | Bobot (%) | |
| (1) | (2) | (3) | (4) | (5) | (6) | (7) | (8) | (9) | (10) |
| 1 | Mampu memahami target kemampuan mahasiswa yang ingin dicapai melalui mata kuliah ini. | a. Menjelaskan definisi, tugas, tujuan serta manfaat pengantar keamanan bagi sistem komputer.<br>b. Menceritakan kembali sejarah perkembangan keamanan SI.<br>c. Menjelaskan metode dalam keamanan SI . | Pendahuluan pengantar sistem operasi :<br>a. Definisi Tujuan pengantar keamanan SI<br>b. Fungsi dan sasaran pengantar sistem operasi<br>c. Sejarah perkembangan keamanan SI<br>d. Konsep keamanan SI | Ceramah dan Tanya Jawab | | Tertulis, uraian subyektif | a. Mencatat semua informasi secara ringkas<br>b. Kelengkapan Kebenaran penjelasan<br>c. Kebenaran identifikasi | | 1,2,3 |
| 2. | memahami dengan baik tentang keamanan fisik dari jaringan komputer pada suatu sistem informasi | Menjelaskan keamanan pada lapisan OSI | Physical Layer Security | Ceramah dan Diskusi | Menjelaskan keamanan pada lapisan OSI Physical Layer Security | Tertulis, uraian subyektif | a. Tingkat komunikatif diskusi<br>b. Ketepatan penjelasan<br>c. Ketepatan identifikasi kasus | | |

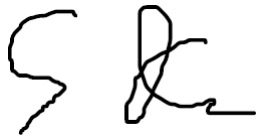
| Perte-muan ke | Sub-CPMK | Indikator | Bahan Kajian | Strategi Pembelajaran (Model dan Metode) | Pengalaman Belajar Mahasiswa | Penilaian | | | Referensi |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | Jenis | Kriteria | Bobot (%) | |
| 3 | memahami dengan baik tentang keamanan fisik dari jaringan komputer pada suatu sistem informasi | Mahasiswa mampu merancang sistem keamanan informasi yang efektif | Kontrol akses, enkripsi, otentikasi, kebijakan dan prosedur keamanan | Ceramah, Diskusi, Studi Kasus | Diskusi kasus, tugas merancang | Tertulis, uraian subyektif | a. Tingkat komunikatif diskusi<br>b. Ketepatan penjelasan<br>c. Ketepatan Analisis | | |
| 4 | memahami pentingnya pengamanan aplikasi web | a. Menjelaskkan Manfaat keamanan web<br>b. Menjelaskan kasus keamanan pada dunia nyata | Web Security, Web Firewall | Ceramah, Tanya Jawab | Tertulis, uraian subyektif | | a. Tingkat komunikatif Diskusi.<br>b. Ketepatan penjelasan Ketepatan Analisis kasus | | |
| 5 | memahami pentingnya keamanan Web Server dengan melihat kasus nyata yang terjadi di dunia nyata | a. Menjelaskan definisi Access control<br>b. Menjelaskan bagaimana proses control akses | Access Control | Ceramah, Tanya Jawab | Tertulis, uraian subyektif | | a. Tingkat komunikatif Diskusi.<br>b. Ketepatan penjelasan Ketepatan Analisis kasus | | |
| 6 | Mematuhi hukum, peraturan, dan etika dalam keamanan informasi global | Mahasiswa memahami dan mematuhi hukum dan etika dalam keamanan informasi | Hukum, peraturan, standar industri, etika profesional global | Ceramah, Diskusi | Diskusi hukum dan etika, tugas analisis | Tugas | Kepatuhan hukum dan etika | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 7 | Mengikuti perkembangan tren dan isu keamanan informasi | Mahasiswa mampu mengikuti perkembangan tren dan isu keamanan informasi | Tren terbaru, isu keamanan, adopsi teknologi baru | Diskusi, Studi Kasus | Diskusi tren terbaru, studi kasus | Tugas dan Diskusi | | | |
| 8 | **UJIAN TENGAH SEMESTER** | | | | | | | | |
| 9 | Persiapan Lab Web Penetration dan OS yang akan di pakai | Mahasiswa mampu mempersiapkan lingkungan lab untuk pengujian penetrasi web dan sistem operasi yang diperlukan | Persiapan lingkungan lab, instalasi dan konfigurasi alat dan sistem operasi | Praktikum, Ceramah | Instalasi dan konfigurasi alat dan sistem operasi | Praktikum | | | |
| 10 | Jenis-jenis Keamanan Web Aplikasi dan Server | Mahasiswa mampu menjelaskan dan menerapkan berbagai teknik keamanan web aplikasi dan server | Jenis-jenis keamanan web aplikasi, teknik keamanan server, firewall, IDS/IPS | Ceramah, Praktikum | Diskusi teknik keamanan, praktikum implementasi keamanan | Tugas dan Praktikum | | | |
| 11 | Mahasiswa mampu melakukan reconnaissance dan OSINT untuk mencari informasi terkait suatu target. | 1. Mahasiswa dapat menjelaskan konsep dan tujuan dari usability testing.<br>2. Mahasiswa mampu merancang dan melaksanakan usability testing.<br>3. Mahasiswa mampu mengumpulkan dan menganalisis data dari usability testing untuk | Usability testing: konsep, perencanaan, pelaksanaan, analisis | Ceramah, Praktikum | Praktikum merancang dan melaksanakan usability testing | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | memberikan rekomendasi | | | | | | | |
| 12 | Mahasiswa mampu melakukan penetration testing dasar. | Mahasiswa mampu melakukan penetration testing dasar | Teknik penetration testing dasar, metodologi pengujian, alat dan teknik yang digunakan dalam penetration testing | Ceramah, Praktikum | Praktikum penetration testing | Tugas, Praktikum | | | |
| 13 | Mahasiswa mengenal berbagai kerentanan yang ada pada aplikasi web dan melakukan | Mahasiswa mampu mengidentifikasi kerentanan aplikasi web dan melakukan pengujian | Kerentanan aplikasi web, pengujian dasar, penggunaan Burp Suite | Ceramah, Praktikum | Praktikum pengujian aplikasi web menggunakan Burp Suit | Tugas dan Praktikum | | | |
| | pengujian dasar menggunakan tools Burp Suite. | dasar menggunakan Burp Suite | | | | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 14-15 | Mahasiswa mampu melakukan pengujian lanjutan untuk kerentanan aplikasi web yang tidak dapat ditemukan oleh tools scanner. | Mahasiswa mampu mengidentifikasi dan mengeksploitasi kerentanan aplikasi web yang tidak terdeteksi oleh tools otomatis | Kerentanan aplikasi web lanjutan, teknik eksploitasi manual, bypass scanner tools | Ceramah, Praktikum | Praktikum pengujian manual aplikasi web | Tugas | | | |
| **16** | **Presentasi Akhir Project / Quiz 2 / UAS** | | | | | | | | |

**Samarinda, 18 Mei 2022**

| **Praktisi** | **Dosen Pengampu Mata Kuliah** | Koordinator Prodi Sistem Informasi |
|---|---|---|
|  |  |  |
| **Syaiful Andy, ST., MT.** | **Hario Jati Setyadi, S,Kom., M.Kom.** | Islamiyah, S.Kom., M.Kom |

**Tabel Revisi RPS Mata Kuliah Keamanan Informasi**

| No. | Bagian yang Berubah | Sebelum Berubah | Setelah Berubah | Pertemuan | Halaman |
|---|---|---|---|---|---|
| 1. | Capaian Pembelajaran Mata Kuliah | | | | |
| | Memahami pentingnya pengamanan aplikasi web | Memahami pentingnya pengamanan aplikasi web | Jenis-jenis Keamanan Web Aplikasi dan Server | 10 | |
| | Memahamivpentingnya pengamanan aplikasi web | Memahami pentingnya pengamanan aplikasi web | Mahasiswa mampu melakukan reconnaissance dan OSINT untuk mencari informasi terkait suatu target. | 11 | |
| | Memahami pentingnya keamanan konten dengan melihat kasus nyata yang terjadi di dunia nyata | a. Menjelaskan konsep autentifikasi dan kelola akun<br>b. MenjelaskanProses pengamanan konten dengan autentifikasi | Mahasiswa mampu melakukan penetration testing dasar. | 12 | |
| | Memahami pentingnya penggunaan metode kriptografi dalam SI | Memahami pentingnya penggunaan metode kriptografi dalam SI | Mahasiswa mengenal berbagai kerentanan yang ada pada aplikasi | 13 | |

| No. | Bagian yang Berubah | Sebelum Berubah | Setelah Berubah | Pertemuan | Halaman |
|---|---|---|---|---|---|
| | | | web dan melakukan pengujian dasar menggunakan tools Burp Suite. | | |
| | Memahami pentingnya penggunaan metode kriptografi dalam SI | Memahami pentingnya penggunaan metode kriptografi dalam SI | Mahasiswa mampu melakukan pengujian lanjutan untuk kerentanan aplikasi web yang tidak dapat ditemukan oleh tools scanner. | 14-15 | |

## RUBRIK PENILAIAN

| Kriteria Penilaian | Skor 10-40 | Skor 50-80 | Skor 90-100 |
|---|---|---|---|
| Kehadiran (10%) | Kehadiran tidak lebih dari 50% dari total pertemuan. | Kehadiran antara 50%-80% dari total pertemuan. | Kehadiran lebih dari 80% dari total pertemuan. |
| Tugas (30%) | Tugas tidak lengkap atau banyak kesalahan konsep. | Tugas lengkap dengan beberapa kesalahan kecil. | Tugas lengkap dan akurat, menunjukkan pemahaman yang baik. |
| Ujian Tengah Semester (UTS) (30%) | Hasil ujian menunjukkan pemahaman yang kurang memadai (nilai <60%). | Hasil ujian menunjukkan pemahaman yang cukup baik (nilai 60%-80%). | Hasil ujian menunjukkan pemahaman yang sangat baik (nilai >80%). |
| Ujian Akhir Semester (UAS) (30%) | Hasil ujian menunjukkan pemahaman yang sangat kurang (nilai <60%). | Hasil ujian menunjukkan pemahaman yang baik (nilai 60%-80%). | Hasil ujian menunjukkan pemahaman yang sangat baik (nilai >80%). |