|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | **POLITEKNIK MEDICA FARMA HUSADA MATARAM,**  **PRODI D4 TEKNOLOGI REKAYASA PERANGKAT LUNAK** | | | | | | | | | | | | | | | | | **Kode Dokumen** | |
| **RENCANA PEMBELAJARAN SEMESTER** | | | | | | | | | | | | | | | | | | | | |
| **MATA KULIAH (MK)** | | | | | | **KODE** | | | **Rumpun MK** | | | | | **BOBOT (sks)** | | | **SEMESTER** | | **Tgl Penyusunan** | |
| **KEAMANAN KOMPUTER DAN JARINGAN** | | | | | | RPL701 | | |  | | | | | **T=3** | | **P=0** |  | |  | |
| **OTORISASI** | | | | | | **Pengembang RPS** | | | | | **Koordinator** | | | | | | **Ketua PRODI** | | | |
|  | | | | |  | | | | | | **Hendra Setiawan, M.Kom.** | | | |
| **Capaian Pembelajaran (CP)** | | **CPL-PRODI yang dibebankan pada MK** | | | | | | | | |  | | | | | | | | | |
| CPL -1 | | | Memiliki pengetahuan komprehensip tentang teori, prinsip dan konsep dasar rekayasa perangkat lunak | | | | | | | | | | | | | | | |
| CPL -2 | | | Menguasai konsep pengembangan rekayasa perangkat lunak | | | | | | | | | | | | | | | |
| CPL -3 | | | Mampu beradaptasi terhadap penggunaan metode baru pada konteks permasalahan yang dinamis | | | | | | | | | | | | | | | |
| CPL -4 | | | Mampu menyajikan solusi atas permasalahan pada dunia industri dan masyarakat berdasarkan pengetahuan bidang rekayasa perangkat lunak | | | | | | | | | | | | | | | |
| CPL -5 | | | Mampu merancang, mengimplemntasikan dan mengevaluasi solusi inovatif terhadap pengembangan teknologi rekayasa perangkat lunak | | | | | | | | | | | | | | | |
| CPL -6 | | | Mampu berkolaborasi dengan berbagai pihak dari disiplin ilmu lain yang relevan secara efektif | | | | | | | | | | | | | | | |
| CPL -7 | | | Mampu berkomunikasi secara efektif untuk menyampaikan solusi dalam menjalankan profesinya | | | | | | | | | | | | | | | |
| CPL -8 | | | Memiliki komitmen terhadap prinsip dan nilai profesional sebagai landasan hidup dalamkonteks individu maupun organisasi | | | | | | | | | | | | | | | |
| CPL -9 | | | Memiliki jiwa pembelajar sepanjang hayat yang kreatif dan inovatif | | | | | | | | | | | | | | | |
|
| **Capaian Pembelajaran Mata Kuliah (CPMK)** | | | | | | | | |  | | | | | | | | | |
| CPMK -1 | | | Mahasiswa dapat menjelaskan prinsip dasar keamanan komputer, termasuk ancaman yang umum seperti malware, serangan phishing, dan serangan denial-of-service (DoS). | | | | | | | | | | | | | | | |
| CPMK -2 | | | Mahasiswa mampu mengidentifikasi potensi ancaman keamanan yang dapat mempengaruhi sistem komputer dan jaringan, serta memahami kerentanan yang mungkin ada. | | | | | | | | | | | | | | | |
| CPMK -3 | | | Mahasiswa dapat mengimplementasikan teknik dan alat perlindungan keamanan seperti firewall, antivirus, enkripsi data, serta kebijakan pengelolaan kata sandi untuk memitigasi risiko keamanan. | | | | | | | | | | | | | | | |
| CPMK -4 | | | Mahasiswa dapat menganalisis kasus keamanan yang ada, termasuk insiden keamanan yang terjadi, dan mengusulkan strategi perbaikan atau pencegahan lebih lanjut. | | | | | | | | | | | | | | | |
| CPMK -5 | | | Mahasiswa memahami pentingnya kepatuhan terhadap kebijakan keamanan dan etika dalam penggunaan sistem komputer serta jaringan. | | | | | | | | | | | | | | | |
| CPMK -6 | | | Mahasiswa memahami hukum dan regulasi yang terkait dengan keamanan komputer, termasuk privasi data dan kewajiban yang terkait. | | | | | | | | | | | | | | | |
| CPMK -7 | | | Mahasiswa mampu melakukan investigasi terhadap insiden keamanan, termasuk pengumpulan bukti digital dan analisis forensik. | | | | | | | | | | | | | | | |
| CPMK -8 | | | Mahasiswa memiliki pemahaman tentang teknologi keamanan lanjutan seperti pengujian penetrasi (penetration testing), deteksi intrusi (intrusion detection), dan manajemen risiko keamanan. | | | | | | | | | | | | | | | |
| CPL->Sub-CPMK | | | | | | | | | | | | | | | | | | |
|  | |  | | | | | | | | | | | | | | | | |
|  | |  | | | | | | | | | | | | | | | | |
| Korelasi CPMK Terhadap Sub-CPMK | | | | | | | | | | | | | | | | | | |
|  | |  | Sub-CPMK 1 | | | | Sub-CPMK 2 | | Sub-CPMK 3 | | | Sub-CPMK 4 | | | Sub-CPMK 5 | | | Sub-CPMK 6 | | |
|  | | CPMK |  | | | |  | |  | | |  | | |  | | |  | | |
| **Deskripsi Singkat MK** | | Keamanan komputer dan jaringan mengacu pada praktik, teknologi, dan kebijakan yang digunakan untuk melindungi sistem komputer dan jaringan dari ancaman, akses tidak sah, dan kerusakan. Tujuan utamanya adalah memastikan kerahasiaan, integritas, dan ketersediaan data. | | | | | | | | | | | | | | | | | | |
| **Bahan Kajian / Materi Pembelajaran** | | 1. Dasar-dasar Keamanan Komputer 2. Teknik Perlindungan Keamanan 3. Keamanan Jaringan 4. Keamanan Aplikasi 5. Manajemen Keamanan 6. Pengujian Keamanan 7. Teknologi Keamanan Lanjutan | | | | | | | | | | | | | | | | | | |
| **Pustaka** | | **Utama :** | | | |  | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | |
| **Pendukung :** | | | |  | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | |
| **Dosen Pengampu** | |  | | | | | | | | | | | | | | | | | | |
| **Matakuliah syarat** | | - | | | | | | | | | | | | | | | | | | |
| **Mg Ke-** | **Sub-CPMK**  **(Kemampuan akhir tiap tahapan belajar)** | | | | **Penilaian** | | | | | **Bantuk Pembelajaran,**  **Metode Pembelajaran,**  **Penugasan Mahasiswa,**  **[ Estimasi Waktu]** | | | | | | | **Materi Pembelajaran**  **[ Pustaka ]** | | | **Bobot Penilaian (%)** |
| **Indikator** | | | **Kriteria & Bentuk** | | **Luring (*offline*)** | | | **Daring (*online*)** | | | |
| **(1)** | **(2)** | | | | **(3)** | | | **(4)** | | **(5)** | | | **(6)** | | | | **(7)** | | | **(8)** |
| **1** | Konsep dasar, ancaman keamanan | | | | Mampu menjelaskan konsep dasar, ancaman keamanan | | | Kriteria:  Ketepatan dan  penguasaan materi  Bentuk test:  -tes lisan | | Ceramah & Diskusi  (TM : 1X (2X59))  Pemberian Tugas dengan contoh kasus | | | Video Pembelajaran  Via Zoom Meeting  LMS | | | | Pengenalan Keamanan Komputer | | | **5%** |
| **2** | Algoritma kunci publik, enkripsi, deskripsi | | | | Mampu mengembakan konsep algoritma kunci public, enkripsi, diskripsi | | | Kriteria:  Ketepatan dan  penguasaan materi  Bentuk test:  -tes lisan  Bentuk non tes:  - presentasi | | Ceramah & Diskusi  (TM : 1X (2X59))  Pemberian Tugas dengan contoh kasus | | | Video Pembelajaran  Via Zoom Meeting  LMS | | | | kriptografi | | | **5%** |
| **3** | Generasi kunci, distribusi, manajemen siklus hidup | | | | Mampu menjelaskan konsep generasi kunci, distribusi, manejemen siklus hidup | | | Kriteria:  Ketepatan dan  penguasaan materi  Bentuk non test:  -Presentasi | | Ceramah & Diskusi  (TM : 1X (2X59))  Pemberian Tugas dengan contoh kasus | | | Video Pembelajaran  Via Zoom Meeting  LMS | | | | Manajemen Kunci | | | **7,5 %** |
| **4** | Proteksi data, firewall, IDS/IPS | | | | Mampu mengembakan konsep proteksi data, firewall, IDS/IPS | | | Kriteria:  Ketepatan dan  penguasaan  Bentuk non test:  -Presentasi | | Ceramah & Diskusi  (TM : 1X (2X59))  Pemberian Tugas dengan contoh kasus | | | Video Pembelajaran  Via Zoom Meeting  LMS | | | | Keamanan Jaringan | | | **7,5 %** |
| **5** | Metodologi penetrasi, teknik serangan | | | | Mampu menjelaskan metodologi penetrasi teknik serangan | | | Kriteria:  Ketepatan dan  penguasaan  Bentuk non test:  -Presentasi | | Ceramah & Diskusi  (TM : 1X (2X59))  Pemberian Tugas dengan contoh kasus | | | Video Pembelajaran  Via Zoom Meeting  LMS | | | | Serangan dan Penetrasi | | | **7,5 %** |
| **6** | Deteksi malware, teknik proteksi | | | | Mampu menjelaskan konsep Deteksi malware, teknik proteksi | | | Kriteria:  Ketepatan dan  penguasaan  Bentuk non test:  -Presentasi | | Ceramah & Diskusi  (TM : 1X (2X59))  Pemberian Tugas dengan contoh kasus | | | Video Pembelajaran  Via Zoom Meeting  LMS | | | | Proteksi Malware | | | **7,5 %** |
| **7** | OWASP Top 10, teknik penetrasi aplikasi web | | | | Mampu menjelaskan OWASP top 10, teknik penetrasi aplikasi web | | | Kriteria:  Ketepatan dan  penguasaan  Bentuk non test:  -Presentasi | | Ceramah & Diskusi  (TM : 1X (2X59))  Pemberian Tugas dengan contoh kasus | | | Video Pembelajaran  Via Zoom Meeting  LMS | | | | Keamanan Aplikasi web | | | **7,5 %** |
| **8** | **Evaluasi Tengah Semester / Ujian Tengan Semester** | | | | | | | | | | | | | | | | | | |  |
| **9,10** | 1. Audit sistem, peraturan dan kepatuhan 2. Proteksi WiFi, teknik serangan WiFi | | | | Mampu mengembakan konsep audit system, peraturan dan kepatuhan. Menjelaskan proteksi wifi, teknik serangan wifi | | | Kriteria:  Ketepatan dan  penguasaan  Bentuk non test:  -Presentasi | | Ceramah & Diskusi  (TM : 1X (2X59))  Pemberian Tugas dengan contoh kasus | | | Video Pembelajaran  Via Zoom Meeting  LMS | | | | 1. Audit Keamanan 2. Keamanan Wireless | | | **15%** |
| **11,12** | 1. Identifikasi risiko, analisis dampak, mitigasi 2. Rencana pemulihan, tes bencana | | | | Mampu menganalisa konsep identifikasi dampak, mitigasi dan menjelaskan rencana pemulihan, tes bencana | | | Kriteria:  Ketepatan dan  penguasaan  Bentuk non test:  -Presentasi | | Ceramah & Diskusi  (TM : 1X (2X59))  Pemberian Tugas dengan contoh kasus | | | Video Pembelajaran  Via Zoom Meeting  LMS | | | | 1. Analisis Risiko 2. Pemulihan dan Kontinuitas Bisnis | | | **15%** |
| **13** | Privasi, kebijakan, hukum cyber | | | | Mampu menjelasakan konsep privasi,kebijakan,hukum cyber | | | Kriteria:  Ketepatan dan  penguasaan  Bentuk non test:  -Presentasi | | Ceramah & Diskusi  (TM : 1X (2X59))  Pemberian Tugas dengan contoh kasus | | | Video Pembelajaran  Via Zoom Meeting  LMS | | | | Etika dan Hukum dalam Keamanan Komputer | | | **7,5 %** |
| **14,15** | 1. Kasus studi, diskusi kelompok | | | | Mampu menjelaskan konsep kasus studi, diskusi kelompok | | | Kriteria:  Ketepatan dan  penguasaan  Bentuk non test:  -Presentasi | | Ceramah & Diskusi  (TM : 1X (2X59))  Pemberian Tugas dengan contoh kasus | | | Video Pembelajaran  Via Zoom Meeting  LMS | | | | 1. Studi Kasus dan Diskusi 2. Presentasi Proyek Akhir | | | **15%** |
| **16** | **Evaluasi Akhir Semester / Ujian Akhir Semester** | | | | | | | | | | | | | | | | | | |  |
| **BOBOT PENILAIAN** | | | | | | **Kehadiran dan Partisipasi dalam kelas : 10%**  **Hasil Praktikum dan Penugasan : 30%**  **Ujian Tengah Semester : 30%**  **Ujian Akhir Semester : 30%**  **Jumlah : 100%** | | | | | | | | | | | | | | | | |