|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | **POLITEKNIK NEGERI MALANG**  **JURUSAN TEKNIK INFORMATIKA**  **PROGRAM STUDI : D 4 TEKNIK INFORMATIKA** | | | | | | | | | | | | | | |
| **RENCANA PEMBELAJARAN SEMESTER (RPS)** | | | | | | | | | | | | | | | | |
| **MATA KULIAH** | | **KODE** | | **RUMPUN MATA KULIAH** | | | | | **BOBOT (sks)/jam** | | **SEMESTER** | | **TGL. PENYUSUNAN** | | | |
| Keamanan Sistem dan Jaringan Komputer | | RTI165005 | | Jarkom dan Multimedia | | | | | 3 sks/6 jam | | 5 | | 2 Agustus 2016 | | | |
| **OTORISASI** | | **Dosen Pengembang RPS** | | | | | | | **Koordinator RMK** | | **Ka PRODI** | | | | | |
| Deddy Kusbianto PA, Ir., M.Mkom | | | | | | | Deddy Kusbianto PA, Ir., M.Mkom | | Ir. Deddy Kusbianto PA., MMKom. | | | | | |
| **Capaian Pembelajaran (CP)** | | **Capaian Pembelajaran Lulusan Program Studi (CPL-Prodi)** | | | | | | | | |  | | | | | |
| Mampu mengidentifikasi celah keamanan dalam jaringan komputer, menjelaskan masalah keamanan komputer, menggunakan tool keamanan standar untuk menemukan dan memperbaiki celah keamanan dalam jaringan computer, memahami beberapa algoritma kriptografi dan protocol yang mendasari aplikasi kemanan jaringan, serta memahami system level security. | | | | | | | | | | | | | | |
| **Capaian Pembelajaran Lulusan yang dibebankan pada mata kuliah (CPL-MK)** | | | | | | | | | | | |  | | |
| Mahasiswa mengetahui, memahami, menguasai dan mampu mengimplementasikan teori, konsep, dan prinsip keamanan jaringan komputer dalam rangka meningkatkan pelayanan pemakaian jaringan komputer. | | | | | | | | | | | | | | |
| **Diskripsi Singkat Mata Kuliah** | | Mahasiswa mampu mengidentifikasi celah keamanan dalam jaringan computer, menjelaskan masalah keamanan komputer, menggunakan tool keamanan standar untuk menemukan dan memperbaiki celah keamanan dalam jaringan computer, memahami beberapa algoritma kriptografi dan protocol yang mendasari aplikasi kemanan jaringan, dan memahami system level security | | | | | | | | | | | | | | |
| **Materi Pembelajaran / Pokok Bahasan** | | Konsep keamanan dan terminology yang berhubungan, Keamanan jaringan TCP/IP dan OSI, Masalah kontrol akses, Keamanan sistem operasi (windows dan linux), Keamanan level network, Keamanan komunikasi, Tool keamanan, Serangan keamanan dan respon, Kriptografi, Proteksi Virus dan Malware, Keamanan level aplikasi | | | | | | | | | | | | | | |
| **Pustaka** | | **Utama :** | | |  | | | | | | | | | | | |
| |  |  | | --- | --- | | 1. | Ananta, Ahmadi Yuli, 2007, Praktikum Aplikasi Mobile, Modul Ajar, Polinema, Malang. | | 2. | Nirav Mehta, 2008, Mobile Web Development, Packt Publishing. | | | | | | | | | | | | | | | |
| **Pendukung :** | | |  | | | | | | | | | | | |
| |  |  | | --- | --- | |  | Sing Li and Jonathan Knudsen, 2009, Beginning J2ME: From Novice to Professional, Third Edition, Apress. | | | | | | | | | | | | | | | |
| **Media Pembelajaran** | | **Software :** | | | | | **Hardware :** | | | | | | | | | |
| 1. Server Apache 2. Server Mysql 3. Browser Internet | | | | | Komputer | | | | | | | | | |
| **Nama Dosen Pengampu** | | Deddy Kusbianto PA, Ir., M.Mkom  Meyti Eka Apriani, ST., MT.  Odhitya Desta Triswidrananta, S.Pd., M.Pd.  Vivi Nur Wijayaningrum, S.Kom | | | | | | | | | | | | | | |
| **Matakuliah Syarat** | |  | | | | | | | | | | | | | | |
| **Minggu Ke** | **Kemampuan Akhir Yang Direncanakan**  **(Sub-CP-MK)** | | **Bahan kajian**  **(Materi Pembelajaran)** | | | **Bentuk dan Metode Pembelajaran** | | **Estimasi Waktu** | | **Pengalaman Belajar Mahasiswa** | | **Kriteria & Bentuk Penilaian** | | | **Indikator Penilaian** | **Bobot Penilaian (%)** |
| **(1)** | **(2)** | | **(3)** | | | **(4)** | | **(5)** | | **(6)** | | **(7)** | | | **(8)** | **(9)** |
| 1-2 | * Mahasiswa dapat menjelaskan konsep keamanan komputer dan jaringan serta membedakan jenis-jenis serangan yang dapat mengganggu operasional sistem | | * Pendahuluan, Definisi dan Tujuan * Trend Keamanan * Arsitektur Keamanan OSI * Aspek Keamanan | | | Ceramah, praktek dan diskusi | | 6 X 45” | | Latihan dan tugas | | Penyelesaian tugas jobsheet | | | * Mahasiswa mampu menyebutkan 5 tujuan keamanan komputer * Mahasiswa mampu menyebutkan dan menjelaskan prediksi ancaman cyber * Mahasiswa mampu menyebutkan dan menjelaskan fokus keamanan arsitektur OSI dan rekomendasi ITU-T X.800 terhadap layanan-layanan keamanan * Mahasiswa mampu menyebutkan dan menjelaskan lima aspek keamanan komputer | 1.5% |
| 3-4 | * Mahasiswa dapat memahami kebijakan keamanan jaringan komputer, dan pembagian level akses terhadap sistem yang menggunakan sistem pengamanan berlapis | | * Pendahuluan, Definisi dan Tujuan * Komponen Kebijakan Keamanan * Model Kebijakan Keamanan yang Baik * Prinsip-prinsip Dasar Kebijakan Keamanan Informasi | | | Ceramah, praktek dan diskusi | | 6 X 45” | | Latihan dan tugas | | Penyelesaian tugas jobsheet | | | * Mahasiswa mampu menyebutkan dan menjelaskan tujuan pengamanan jaringan komputer, * Mahasiswa mampu menyebutkan dan menjelaskan definisi kebijakan keamanan komputer * Mahasiswa mampu menyebutkan dan menjelaskan tujuan utama pembuatan kebijakan keamanan * Sebutkan dan jelaskan tujuan spesifik pembuatan kebijakan keamanan * Mahasiswa mampu menyebutkan dan menjelaskan dukungan komponen-komponen pembuat kebijakan keamanan * Mahasiswa mampu menyebutkan dan menjelaskan model kebijakan keamanan yang baik memiliki karakteristik * Mahasiswa mampu menyebutkan dan menjelaskan prinsip-prinsip dasar yang dapat digunakan sebagai panduan bagi pengambilan keputusan untuk membuat kebijakan | 1.5% |
| 5 | KUIS | |  | | | KUIS | | 6 X 45” | | KUIS | | KUIS | | | KUIS | 1.5% |
| 6-7 | Mahasiswa dapat mengerti perbedaan jenis program jahat, serta antisipasi dan deteksi penanggulangannya | | * Pendahuluan dan Definisi * Tipe Malicious Logic * Program Anti virus | | | Ceramah, praktek dan diskusi | | 6 X 45” | | Latihan dan tugas | | Penyelesaian tugas jobsheet | | | * Mahasiswa mampu menyebutkan dan menjelaskan definisi code jahat (*malicious code*)? * Mahasiswa mampu memberikan solusi apabila di komputer terjangkit code jahat | 1.5% |
| 8-9 | Mahasiswa dapat memahami algoritma beberapa jenis kritographi yang digunakan untuk menjamin keamanan data | | * Pendahuluan dan Definisi * Kunci Enkripsi dan Dekripsi * Algoritma Simetris * Algoritma Asimetris | | | Ceramah, praktek dan diskusi | | 6 X 45” | | Latihan dan tugas | | Penyelesaian tugas jobsheet | | | * Mahasiswa mampu menyebutkan dan menjelaskan dua jenis algoritma kriptografi berdasarkan jenis kunci yang digunakan. * Mahasiswa mampu menyebutkan dan menjelaskan perbedaan berdasarkan besar data yang diolah dalam satu kali proses pada algoritma kriptografi. * Mahasiswa mampu menyebutkan dan menjelaskan prinsip-prinsip yang mendasari kriptografi. * Mahasiswa mampu menyebutkan dan menjelaskan apa yang dimaksudkan dengan Algoritma Simetris * Mahasiswa mampu menyebutkan dan menjelaskan apa yang dimaksudkan dengan Algoritma Asimetris | 15% |
| 10 | UTS/KUIS 2 | |  | | | UTS/KUIS 2 | | 6 X 45” | | UTS/KUIS 2 | | UTS/KUIS 2 | | | UTS/KUIS 2 | 1.5% |
| 11-12 | Mahasiswa dapat menjelaskan ancaman yang sering terjadi pada aplikasi komputer berbasis web dan teknik pengelolaan yang baik untuk terhindar dari kegagalan sistem | | * Pendahuluan dan Mengenal Keamanan Wireless Metode WEP * Mengenal Keamanan Wireless Metode WPA * Jenis Penghalang Wi-Fi Dan Solusinya * Mengamankan jaringan wireless | | | Ceramah dan praktek | | 6 X 45” | | Latihan dan tugas | | Penyelesaian tugas jobsheet | | | * Mahasiswa mampu menyebutkan dan menjelaskan metode keamanan apa yang dipakai pada perangkat peralatan wireless Metode WEP * Mahasiswa mampu menyebutkan dan menjelaskan metode keamanan apa yang dipakai pada perangkat peralatan wireless Metode WPA * Mahasiswa mampu menyebutkan dan menjelaskan apa permasalahan yang menghalangi kecepatan data koneksi broadband pada perangkat peralatan wireless * Mahasiswa mampu menyebutkan dan menjelaskan tips apa saja dalam rangkah mengamankan perangkat peralatan wireless | 1.5% |
| 13-14 | Mahasiswa dapat menjelaskan ancaman yang sering terjadi pada aplikasi komputer berbasis web dan teknik pengelolaan yang baik untuk terhindar dari kegagalan sistem | | * Pendahuluan dan Definisi * Keamanan Server WWW * Keamanan client WWW | | | Ceramah dan praktek | | 6 X 45” | | Latihan dan tugas | | Penyelesaian tugas jobsheet | | | * Mahasiswa mampu menyebutkan dan menjelaskan dua sisi dari Arsitektur sistem Web. * Mahasiswa mampu menyebutkan dan menjelaskan asumsi sistem Web, dilihat dari sisi penyedia jasa (webmaster) * Mahasiswa mampu menyebutkan dan menjelaskan asumsi sistem Web, dilihat dari sisi sisi pengguna | 1.5% |
| 15 | KUIS 3 | |  | | | KUIS 3 | | 6 X 45” | | KUIS 3 | | KUIS 3 | | | KUIS 3 | 20% |
| 16,17,18 | Mahasiswa dapat menjelaskan konsep pengamanan yang spesifik menggunakan IDS dan IPS beserta tools dan perangkat yang digunakan | | * Pendahuluan dan Definisi * Intrution detection System * Intrution Prevention System. | | | Ceramah dan praktek | | 6 X 45” | | Latihan dan tugas | | Penyelesaian tugas jobsheet | | | * Mahasiswa mampu menyebutkan dan menjelaskan fungsi dari Intrution detection System dalam sistem jaringan computer * Mahasiswa mampu menyebutkan dan menjelaskan jenis-jenis, karakteristik dan cara kerja dari Intrution detection System. * Mahasiswa mampu menyebutkan dan menjelaskan jenis-jenis, karakteristik dan cara kerja dari Intrution Prevention System. | 1.5% |
| 19 | UAS | | * UAS | | | UAS | | 6 X 45” | | UAS | | UAS | | | UAS | 1.5% |

**Keterangan :**

……………………………………………..

……………………………………………..