Modul Ajar

A. Materi : Sistem keamanan jaringan dan kemungkinan potensi ancaman dan serangannya

Identitas Modul

- **Mata Pelajaran :** Keamanan jaringan
- **Fase :** F
- **Penyusun :** Suci Mulyani
- **Tahun Ajaran :** 2024/2025

Kompetensi Awal

- Pemahaman Dasar tentang Jaringan Komputer
- Pengertian Keamanan dalam Teknologi Informasi
- Dasar-dasar Sistem Operasi Jaringan dan Akses Pengguna
- Pengertian Ancaman dan Serangan Siber
- Kesadaran akan Risiko dan Praktik Keamanan Dasar

Profil Pelajar Pancasila

1. **Beriman, Bertakwa kepada Tuhan YME, dan Berakhlak Mulia.**
   Integritas dalam Penggunaan Teknologi: Siswa diajarkan untuk menggunakan teknologi dan pengetahuan keamanan jaringan secara bertanggung jawab dan etis.
2. **Berkebinekaan Global.**
   Kesadaran Keberagaman dalam Keamanan Siber: Siswa memahami bahwa ancaman siber bersifat global dan dapat berasal dari berbagai penjuru dunia, sehingga penting untuk selalu menjaga keterbukaan dan kehati-hatian dalam berinteraksi secara digital.
3. **Gotong royong.**
   Kolaborasi dan Pembagian Tugas: Dalam simulasi keamanan jaringan, siswa berbagi peran untuk mencapai tujuan bersama dalam menjaga keamanan infrastruktur jaringan.
4. **Mandiri.**
   Kemandirian dalam Menyelesaikan Tantangan: Siswa belajar untuk menyelesaikan masalah keamanan secara mandiri dan membuat keputusan tepat dalam menghadapi ancaman siber
5. **Bernalar kritis.**
   Analisis Ancaman Jaringan: Siswa diajarkan untuk berpikir kritis dalam menganalisis berbagai ancaman jaringan, memahami pola serangan, dan menentukan tindakan yang tepat.

Sarana dan Prasarana

- Ruang kelas atau laboratorium komputer
- Komputer/Laptop untuk Setiap Siswa
  Dengan spesifikasi minimum
  - Prosesor minimal Intel i3/AMD Ryzen 3 atau lebih tinggi.
  - RAM minimal 4GB (direkomendasikan 8GB untuk performa lebih baik).
  - Penyimpanan minimal 256GB.
- Perangkat Jaringan (Router dan Switch,Access point,Firewall)
- Perangkat lunak keamanan jaringan (firewall software,network monitoring tools,IDS/IPS software, virtual machine software,SIEM)
- Internet dan Intranet (Jaringan Lokal)

- Papan Tulis atau Smartboard
- Proyektor dan Layar
- Sumber Belajar dan Referensi
- Akses ke Platform Pembelajaran Online (Google Classroom, Moodle, atau Microsoft Teams.)

Target Peserta Didik

- Peserta didik SMK khususnya jurusan **Teknik Komputer dan Jaringan** atau **Teknik Informatika**.

Strategi Pembelajaran

- **Pembelajaran Ekspositori:** Guru menjelaskan materi secara sistematis dengan menggunakan media presentasi.
- **Diskusi Kelompok:** Peserta didik dibagi menjadi beberapa kelompok untuk mendiskusikan kasus atau soal terkait perencanaan jaringan.
- **Praktikum:** Peserta didik melakukan simulasi perancangan jaringan menggunakan software simulasi jaringan (misalnya Cisco Packet Tracer).
- **Penugasan:** Peserta didik diberikan tugas individu atau kelompok untuk membuat desain jaringan sederhana.

Capaian Pembelajaran

Pada akhir fase F, peserta didik mampu:

- Memahami konsep dasar keamanan jaringan
- Mengidentifikasi jenis-jenis ancaman dan serangan jaringan
- Menguasai Teknik dasar pencegahan dan perlindungan jaringan
- Menerapkan alat dan teknik untuk memantau dan merespon ancaman jaringan
- Menerapkan Tindakan mitigasi dan respon terhadap insiden keamanan
- Mengembangkan kesadaran etika dan tanggung jawab dalam keamanan siber

Tujuan Pembelajaran

- Siswa memahami konsep dasar keamanan jaringan dan perangkat yang digunakan untuk melindungi jaringan.
- Siswa mampu mengidentifikasi berbagai jenis ancaman dan serangan yang dapat mengganggu jaringan.
- Siswa memahami cara mitigasi dan respons terhadap ancaman dan serangan jaringan.
- Siswa dapat melakukan konfigurasi dasar pada perangkat keamanan jaringan.

Alur Tujuan Pembelajaran

- Pengantar Keamanan Jaringan
- Identifikasi Ancaman dan Serangan Jaringan
- Perlindungan dan Pencegahan Jaringan
- Teknik Deteksi dan Respons terhadap Ancaman
-

Kegiatan Pembelajaran

Pertemuan 1: Pengenalan Jaringan Komputer.

- **Pengantar Keamanan Jaringan**
  Mengapa keamanan jaringan penting, dan bagaimana pengaruhnya terhadap integritas data.

- **Elemen Keamanan Jaringan**
  Tiga aspek utama: Kerahasiaan (Confidentiality), Integritas (Integrity), dan Ketersediaan (Availability).
- **Perangkat Keamanan Jaringan**
  - Firewall: Membatasi akses masuk dan keluar jaringan.
  - IDS/IPS: Memantau dan mencegah serangan berdasarkan pola.
  - VPN: Mengamankan koneksi dan menjaga privasi data.

Aktivitas: Diskusi kelas tentang contoh nyata serangan jaringan dan pengenalan perangkat keamanan dasar.

Pertemuan 2: Pengalamatan IP

- **Malware**: Virus, worm, trojan, ransomware, dan spyware.
- **Serangan Berbasis Jaringan**: DDoS, MitM (Man-in-the-Middle).
- **Serangan Berbasis Aplikasi Web**: SQL Injection, Cross-Site Scripting (XSS).
- **Ancaman Internal**: Serangan dari dalam organisasi, seperti kebocoran data.

Aktivitas: Analisis kasus serangan jaringan dan diskusi kelompok tentang cara penyerang mendapatkan akses.

Pertemuan 3: Praktikum Simulasi Jaringan

- **Keamanan Perimeter**: Konfigurasi firewall, IDS, dan IPS.
- **Enkripsi Data**: SSL/TLS, enkripsi dalam aplikasi web dan perangkat lunak.
- **Manajemen Akses**: Penerapan otentikasi dua faktor (2FA) dan kebijakan kata sandi yang kuat.
- **Pemantauan Jaringan**: Penggunaan alat SIEM (Security Information and Event Management) untuk mendeteksi ancaman.

Aktivitas: Latihan konfigurasi firewall dan simulasi deteksi ancaman menggunakan perangkat lunak pemantauan jaringan.

Pertemuan 4: Mitigasi dan Respons Serangan

- **Penyusunan Kebijakan Keamanan Jaringan**: Prosedur mitigasi dan protokol respons.
- **Manajemen Patch dan Update**: Mengelola pembaruan perangkat lunak dan perangkat keras untuk mengurangi kerentanan.
- **Latihan Tanggap Darurat**: Mengasah keterampilan siswa dalam mengatasi serangan dengan simulasi.

Aktivitas: Simulasi respons serangan dengan studi kasus, di mana siswa belajar menerapkan kebijakan keamanan dan teknik mitigasi.

Pertemuan 5: **Evaluasi**

- **Tugas Akhir**: Analisis kasus studi tentang serangan jaringan dan membuat rencana mitigasi.
- **Ujian Praktik**: Konfigurasi firewall dan IDS pada simulasi jaringan untuk mengamankan lalu lintas data.
- **Refleksi Pembelajaran**: Diskusi kelompok tentang tantangan keamanan jaringan di masa depan dan pemahaman siswa tentang keamanan siber.

Pernyataan Pematik

- "Bagaimana cara merancang jaringan yang handal dan efisien untuk sebuah kantor kecil?"
- "Apa yang dimaksud dengan subnetting dan mengapa penting dalam perencanaan jaringan?"

Jenis Asesmen

- **Asesmen formatif:** Kuis, tugas individu, diskusi kelompok.
- **Asesmen sumatif:** Ujian akhir, presentasi proyek.

Lampiran

- Rubrik penilaian proyek.
- Daftar perangkat jaringan yang digunakan.
- Contoh topologi jaringan.

Referensi :

- **NIST:** National Institute of Standards and Technology (nist.gov)
- **CERT:** Computer Emergency Readiness Team (cert.org)
- **OWASP:** Open Web Application Security Project (owasp.org)