SMK ISLAMIYAH ADIWERNA

Jl. Raya Singkil No. 234, Adiwerna, Tegal, Jawa Tengah 52194

MODUL AJAR

SISTEM KEAMANAN JARINGAN

Mata Pelajaran	: KONSENTRASI KEAHLIAN
Kelas / Semester	: XI / 1
Tahun Ajaran	: 2025/2026
Alokasi Waktu	: 6 JP
Fase	: F
Penyusun	: Noval Ali Chaedar, S.Kom
Jurusan	: Teknik Komputer dan Jaringan

A. INFORMASI UMUM

1. Kompetensi Awal

DASAR DASAR KEAMANAN KOMPUTER

2. Profil Pelajar Pancasila

Berkebinekaan Global | Bernalar Kritis | Bergotong Royong | Kreatif | Beriman, Bertakwa kepada Tuhan YME, dan Berakhlak Mulia | Mandiri

3. Model Pembelajaran

Problem Based Learning (PBL)

4. Sarana & Prasarana

□□ Hardware: 3 PC + Switch + Router □□ Software: pfSense, Wireshark, Nmap, WireGuard □□ Online: TryHackMe, HackTheBox (free room) □□ Referensi: CISSP Guide, NIST SP 800-53

5. Target Peserta Didik

Setelah mengikuti pembelajaran ini, peserta didik mampu: Menjelaskan konsep dasar keamanan komputer dan ancaman siber Mengidentifikasi jenis-jenis malware dan cara penyebarannya Menerapkan praktik keamanan dasar pada perangkat komputer Memahami pentingnya password yang kuat dan autentikasi dua faktor Menganalisis risiko phishing dan social engineering

B. TUJUAN PEMBELAJARAN

1. Capaian Pembelajaran (CP)

Mengimplementasikan sistem keamanan jaringan dasar

2. Alur Tujuan Pembelajaran (ATP)

PERTEMUAN 1 (Konsep Dasar) PERTEMUAN 2 (Ancaman & Kerentanan) PERTEMUAN 3 (Implementasi & Evaluasi)

3. Tujuan Pembelajaran

- Pertemuan 1: Konsep Dasar Keamanan
- Pertemuan 2: Ancaman & Kerentanan
- Pertemuan 3: Implementasi & Evaluasi

4. Pemahaman Bermakna

"Keamanan jaringan bukanlah produk tunggal, melainkan proses berkelanjutan yang melibatkan orang, proses, dan teknologi untuk melindungi aset informasi dari ancaman siber yang terus berkembang."

5. Pertanyaan Pemantik

- Fakta: Apa perbedaan keamanan jaringan dengan keamanan komputer biasa?
- Konsep: Bagaimana CIA Triad diterapkan dalam lingkungan jaringan?
- Praktik: Mengapa "Defense in Depth" lebih efektif daripada satu lapis perlindungan?
- Perspektif: Bagaimana peran manusia menjadi faktor terlemah dalam keamanan jaringan?

C. KEGIATAN PEMBELAJARAN

Pertemuan 1 (90 menit)

Pendahuluan

PERTEMUAN 1: KONSEP DASAR KEAMANAN JARINGAN

Pendahuluan (15 Menit)

□□ Tujuan: Mengaktifkan pengetahuan awal

□ Kegiatan:

1. Salam & presensi digital (QR Code)
2. Pertanyaan pemantik: "Siapa yang pernah kena WiFi diretas?"
3. Kuis diagnostik 5 menit (Mentimeter)

Kegiatan Inti

1□ EXPLORASI (20 Menit) - CIA Triad & Model Keamanan

□□ Aktivitas: Galeri Walk - 4 stasiun CIA Triad

□□ Media: Infografis + Video NIST Framework (3')

2□ ELABORASI (25 Menit) - Komponen Sistem Keamanan

□□ Kelompok: Mapping 7 lapis keamanan jaringan

□□ Worksheet: Identify → Firewall, IDS, VPN, dll

3□ KONFRONTASI (15 Menit) - Analisis Kebutuhan

□□ Case Study: "Sekolah diretas via WiFi tamu"

□□ Output: Rekomendasi keamanan

Penutup

Penutup (15 Menit)

□ Refleksi: "Apa 1 hal baru yang dipelajari?"

□ PR: Identifikasi 3 perangkat keamanan di rumah

□ Penilaian: Observasi kelompok (Rubrik)

Pertemuan 2 (90 menit)

Pendahuluan

PERTEMUAN 2: ANCAMAN & KERENTANAN JARINGAN

Pendahululan (10 Menit)

- Review PR Pertemuan 1 (Think-Pair-Share)
- Presentasi 2 kelompok terbaik
- Preview: "Hari ini kita jadi hacker etis!"

Kegiatan Inti

Kegiatan Inti (65 Menit)

1. EXPLORASI (20 Menit) - Klasifikasi Ancaman
   - Aktivitas: "Threat Hunting Game"
   - Kartu ancaman → Kelompok klasifikasi (MITRE ATT&CK)

2. ELABORASI (25 Menit) - Kerentanan Umum
   - Lab: Scan vulnerability lokal (Nmap demo)
   - Diskusi: CVSS Scoring untuk kerentanan

3. KONFRONTASI (20 Menit) - Vektor Serangan
   - Simulasi: Wireshark capture → Analisis packet
   - ⚠ Identifikasi: ARP Poisoning, DNS Spoofing

Penutup

Penutup (15 Menit)

- Exit Ticket: "3 ancaman terbesar jaringan sekolah?"
- PR: Riset 1 CVE terkini
- Penilaian: Worksheet + Lab report

Pertemuan 3 (90 menit)

Pendahuluan

PERTEMUAN 3: IMPLEMENTASI & EVALUASI (90 MENIT)

Pendahuluan (10 Menit)

- Review ancaman dari PR

- Demo live: Firewall block attack
- Safety briefing lab network

Kegiatan Inti

Kegiatan Inti (65 Menit)

1. EXPLORASI (20') - Kontrol Akses Dasar
   - Praktik: pfSense/iptables basic rules
   - Lab: Block port 23, allow SSH only

2. ELABORASI (25') - Enkripsi Dasar
   - Praktik: Generate SSL cert + HTTPS redirect
   - Lab: WireGuard VPN tunnel (client-server)

3. KONFRONTASI (20') - Evaluasi Efektivitas
   - Penetration Testing sederhana
   - Tools: nmap, nikto → Report findings

Penutup

Penutup (15 Menit)

- Presentasi hasil lab (3 kelompok)
- Refleksi: "Apa yang akan diterapkan di jaringan rumah?"
- Portofolio: Kumpulan lab report

D. ASESMEN

Tipe	Jenis	Bentuk	Instrumen
Formatif	Pengetahuan	Tes Tulis	Pertemuan : 1 Instrumen : Observasi + Worksheet Bobot : 20% Pertemuan : 2 Instrumen : Lab Report + Exit Ticket Bobot : 30% Pertemuan : 3 Instrumen : Portofolio + Presentasi Bobot : 50% Rubrik Penilaian Praktik 5 (Excellent): Konfigurasi sempurna, zero vulnerability 4 (Good): 1-2 minor issue, functional 3 (Fair): Basic function, multiple issues 2 (Poor): Tidak berfungsi 1 (Fail): Tidak ada hasil