MODUL AJAR KEAMANAN JARINGAN

I. INFORMASI UMUM

A. Identitas Modul

- Mata Pelajaran : Teknik Komputer dan Jaringan Telekomunikasi
- Fase/Kelas : F / XI
- Topik : Kebijakan Penggunaan Jaringan dan Ancaman
- Tahun Ajaran : 2024/2025
- Penyusun : Sri Ayatmi
- Alokasi Waktu : 2 x 45 menit

B. Kompetensi Awal

Peserta didik telah mempelajari pengenalan jaringan komputer, perangkat, dan fungsi dasar jaringan.

C. Profil Pelajar Pancasila

- Beriman, bertakwa, dan berakhlak mulia
- Mandiri
- Bernalar kritis
- Bergotong royong

D. Sarana dan Prasarana

- Laptop/PC
- Internet
- Proyektor
- Modul ajar dan LKPD
- Video pembelajaran

E. Target Peserta Didik

- Peserta didik umum
- Peserta didik dengan kebutuhan individual
- Peserta kemampuan tinggi (HOTS)

II. KOMPONEN INTI

A. Capaian Pembelajaran

Peserta didik mampu memahami kebijakan penggunaan jaringan, serta memahami kemungkinan ancaman dan serangan terhadap keamanan jaringan.

B. Tujuan Pembelajaran

Setelah mengikuti pembelajaran, peserta didik mampu:

1. Menjelaskan kebijakan penggunaan jaringan
2. Mengidentifikasi potensi ancaman keamanan jaringan
3. Mendeskripsikan alur terjadinya serangan jaringan
4. Menjelaskan kaitan kebijakan dengan ancaman
5. Menerapkan perilaku aman saat menggunakan jaringan

C. Pemahaman Bermakna

Keamanan jaringan sangat penting untuk menjaga data, perangkat, dan layanan berjalan aman. Pengguna harus mengikuti kebijakan dan memahami ancaman agar tidak menjadi celah serangan.

D. Pertanyaan Pematik

1. Mengapa sekolah harus memiliki kebijakan penggunaan jaringan?
2. Bagaimana serangan jaringan bisa terjadi?
3. Apakah ancaman hanya datang dari luar?

E. Kegiatan Pembelajaran (ATP)

Model Problem Based Learning (PBL)

1. Pendahuluan (10 menit)
    - Salam dan doa
    - Apersepsi: contoh kasus WIFI sekolah diretas
    - Menyampaikan tujuan pembelajaran
    - Ice breaking
2. Kegiatan Inti (70 menit)

    Fase 1 Mengidentifikasi Masalah
    - Guru menampilkan video kasus serangan jaringan
    - Peserta didik mengidentifikasi masalah.

    Fase 2 Mengorganisasi Peserta Didik
    - Pembentukan kelompok
    - Pemberian LKPD
    - Penjelasan tugas analisis ancaman

    Fase 3 Penyelidikan dan Diskusi

    Kelompok menganalisis

    - Kebijakan jaringan
    - Ancaman
    - Proses serangan
    - Dampaknya

    Fase 4 Presentasi Hasil

    Kelompok menyampaikan hasil analisis

    Fase 5 Evaluasi dan Refleksi

    Peserta didik mengerjakan soal formatif dan menyimpulkan.

3. Penutup (10 menit)
    - Refleksi pembelajaran
    - Guru memberikan penguatan
    - Informasi materi pertemuan selanjutnya
    - Doa penutup

III. BAHAN BACAAN (Materi Inti)

1. Pengertian Keamanan jaringan

Keamanan jaringan adalah Tindakan untuk melindungi jaringan dari ancaman, serangan, dan akses tidak sah guna menjaga kerahasiaan, integritas, dan ketersediaan data.

2. Kebijakan Penggunaan Jaringan

Kebijakan penggunaan jaringan adalah aturan penggunaan jaringan agar aman dan bertanggung jawab.

Tujuan Kebijakan

- Melindungi data
- Mencegah penyalahgunaan
- Menjaga stabilitas jaringan
- Mengurangi risiko serangan

Contoh Kebijakan

- Tidak berbagi password WIFI
- Menggunakan password kuat
- Tidak menginstal program illegal
- Tidak membuka situs berbahaya
- Tidak memodifikasi perangkat jaringan

3. Potensi Ancaman Keamanan Jaringan
   a. Ancaman Fisik
      - Pencurian perangkat
      - Kerusakan perangkat
      - Listrik tidak stabil
   b. Ancaman Malware
      - Virus
      - Worm
      - Trojan
      - Ransomware
   c. Social Engineering
      - Phishing
      - Scamming
      - Link palsu
   d. Serangan Berbasis Jaringan
      - DoS/DDoS
      - Sniffing
      - Spoofing
      - Man-in-the-Middle (MitM)
   e. Ancaman Internal
      - Password
      - Pengunduhan file berbahaya
      - Pengguna nakal
4. Alur Terjadinya Serangan (Attack Flow)
   a. Reconnaissance (pengumpulan informasi)
   b. Scanning (mencari celah)
   c. Gaining access (menembus sistem)
   d. Maintaining Access (membuat backdoor)

e. Covering Tracks (menghapus jejak)

5. Cara Pencegahan Serangan
   - Menggunakan password kuat
   - Update sistem
   - Menggunakan firewall
   - Antivirus
   - Edukasi keamanan
   - Enkripsi WIFI (WPA2/WPA3)
   - Backup data
6. Hubungan Kebijakan Jaringan dengan Ancaman
   - Kebijakan baik/serangan minim
   - Kebijakan buruk/celah terbuka
     contohnya password kuat untuk mencegah brute force dan larangan instal illegal untuk mencegah malware

IV. LAMPIRAN

A. LKPD (Lembar Kerja Peserta Didik)

Instruksi: kerjakan secara berkelompok

1. Jelaskan apa yang dimaksud kebijakan penggunaan jaringan.
2. Sebutkan 5 ancaman keamanan jaringan.
3. Jelaskan alur serangan jaringan.
4. Berikan contoh kebijakan jaringan yang ada di sekolah.
5. Apa hubungan kebijakan dan ancaman?

B. Penilaian

Rubrik Penilaian

Skor	**Deskripsi**
4	Sangat baik, analisis lengkap
3	Baik, analisis sesuai
2	Cukup, namun kurang detail
1	Perlu perbaikan

C. Glosarium

- Malware: Program berbahaya
- Phishing: Mencuri data
- Spoofing: Pemalsuan identitas
- Backdoor: Akses tersembunyi
- DDoS: Serangan pelumpuhan server