MODUL AJAR

Mata Pelajaran	: Administrasi Sistem Jaringan Komputer (ASJK)
Kelas / Semester	: XI TJKT (Teknik Jaringan Komputer dan Telekomunikasi) / Ganjil
Tahun Pelajaran	: 2025/2026
Alokasi Waktu	: 16 JP (4 Pertemuan @ 4 JP)
Nama Guru	: Mukadar, S.Kom
Sekolah	: SMKN 1 Sampang

A. Informasi Umum

1. Identitas Modul:

- **Nama Modul:** "Network Administrator Muda: Mengamankan Jaringan Lokal SMKN 1 Sampang"
- **Kode Modul:** ASJK-XI-01-2025

2. Kompetensi Awal:

- Siswa telah memahami dasar-dasar jaringan komputer (TCP/IP, subnetting, perangkat jaringan).
- Siswa mampu menginstalasi sistem operasi server (Debian/Ubuntu Server).

3. Profil Pelajar Pancasila:

- **Bernalar Kritis:** Menganalisis log dan merancang solusi keamanan.
- **Kreatif:** Merancang skrip otomatisasi dan solusi mitigasi yang inovatif.
- **Bergotong-royong:** Bekerja dalam tim *helpdesk* dan *security*.
- **Mandiri:** Menyelesaikan tantangan troubleshooting secara mandiri.

4. Sarana dan Prasarana:

- Lab Jaringan dengan PC yang telah terinstal VirtualBox/VMware.
- Image OS Debian/Ubuntu Server dan Windows Client.
- Koneksi internet untuk mencari referensi dan dokumentasi.
- Poster/Infografis tentang Command Line Linux dan DHCP/DNS.
- *Tools:* nmap, wireshark, ssh, fail2ban.

5. **Target Peserta Didik:** Siswa reguler kelas XI TJKT. Pendekatan diferensiasi akan diterapkan untuk siswa yang lebih cepat dan yang perlu pendampingan lebih.

B. Kompetensi dan Tujuan Pembelajaran

- **Capaian Pembelajaran (CP):**

- *Pada akhir fase F*, peserta didik mampu menerapkan prinsip-prinsip administrasi sistem dan jaringan untuk mengelola, memelihara, dan mengamankan infrastruktur jaringan skala kecil hingga menengah, serta mampu berkomunikasi efektif dalam memberikan layanan dukungan teknis.

- **Tujuan Pembelajaran (TP):**

- Setelah mengikuti proses pembelajaran, peserta didik dapat:
 1. Menganalisis kebutuhan konfigurasi layanan DHCP dan DNS untuk sebuah jaringan lokal.
 2. Mengimplementasikan dan mengkonfigurasi layanan DHCP dan DNS pada server Linux.
 3. Menganalisis potensi kerentanan keamanan pada layanan jaringan menggunakan tools *scanning*.
 4. Mengimplementasikan kebijakan keamanan dasar (firewall ufw, fail2ban) untuk mengamankan server.
 5. Membuat dokumentasi teknis dan presentasi yang merefleksikan proses pemecahan masalah dan hasil yang dicapai.

C. Pemahaman Bermakna (Meaningful Learning)

- Peserta didik akan memahami bahwa tugas seorang Network Administrator adalah memastikan konektivitas yang lancar dan aman, sebuah peran yang sangat krusial di dunia nyata.
- Proyek ini bermakna karena langsung diterapkan pada simulasi jaringan sekolah mereka sendiri (**Kontekstual**). Keberhasilan mereka berdampak langsung pada "kelancaran operasional" simulasi.
- Materi ini menjadi fondasi untuk kompetensi keamanan jaringan yang lebih advanced.

D. Pertanyaan Pemantik (Deep Learning & Joyful Learning)

- **Deep Learning:** "Bagaimana jika suatu hari, jaringan internet SMKN 1 Sampang down? Apa langkah pertama yang akan kalian ambil sebagai calon administrator? Layanan apa yang paling kritis untuk diperiksa?"
- **Joyful Learning:** "Bersiaplah menjadi pahlawan jaringan! Tim kalian adalah tim IT support baru yang bertugas melindungi jaringan sekolah dari serangan *hacker* yang akan datang dalam 60 menit! Apakah kalian siap membangun pertahanan?"

E. Kegiatan Pembelajaran

PERTEMUAN 1 (4 JP): Perancangan Jaringan dan Konfigurasi Dasar (Meaningful Setup)

- **Kegiatan Awal (15 menit):**
 - **Ice Breaker (Joyful):** Game "Network Puzzle": Siswa menyusun kartu yang berisi urutan proses DHCP (DORA Process - Discover, Offer, Request, Acknowledge).
 - Guru menyampaikan *storyline*: "Kalian ditugaskan menjadi admin jaringan untuk merancang ulang lab ini. Setiap tim bertanggung jawab atas satu subnet."
 - Penyampaian tujuan dan motivasi.
- **Kegiatan Inti (150 menit):**
 - **Stimulasi (Meaningful):** Guru menunjukkan video singkat tentang chaos tanpa DHCP (IP conflict, manual configuration).
 - **Problem Statement (Deep Learning):** "Rancanglah skema IP addressing untuk 20 PC client di lab kalian dengan range IP tertentu. Kemudian, implementasikan pada virtual server kalian."
 - **Eksplorasi & Kolaborasi:** Siswa berdiskusi dalam tim untuk membuat desain jaringan sederhana. Mereka mencari referensi konfigurasi DHCP di internet (dokumentasi online).
 - **Assimilation & Creation:** Masing-masing tim mengimplementasikan konfigurasi DHCP pada server virtual mereka. Guru berkeliling sebagai fasilitator.
- **Kegiatan Penutup (15 menit):**
 - **Refleksi:** Beberapa siswa mempresentasikan desain jaringan mereka dan menjelaskan alasan pemilihan IP range.

- Guru memberikan umpan balik dan mengaitkan dengan pertemuan selanjutnya (DNS).

PERTEMUAN 2 (4 JP): Membuat Jaringan yang "Ramah" (Joyful Naming)

- **Kegiatan Awal (10 menit):**

- Refleksi singkat masalah di Pertemuan 1.
- **Pemantik (Joyful):** "Siapa yang hafal alamat IP Google? Lalu, siapa yang ingat google.com? Mana yang lebih mudah? Hari ini kita akan membuat jaringan kita semudah itu!"

- **Kegiatan Inti (160 menit):**

- **Stimulasi:** Demonstrasi guru: akses server lain menggunakan IP vs menggunakan nama host (e.g., ssh admin@server01).
- **Problem Statement (Deep Learning):** "Client tidak boleh lagi mengingat alamat IP server. Buatlah layanan DNS sehingga setiap device di jaringan dapat dikenali dengan nama, bukan hanya angka."
- **Eksplorasi & Kolaborasi:** Siswa research perbedaan DNS Forwarder dan DNS Authoritative. Mereka berdiskusi untuk memberi nama yang kreatif dan kontekstual untuk setiap server dan client (e.g., gateway.smk1sampang.sch.id, www.tjkt.sch.id).
- **Assimilation & Creation:** Tim mengkonfigurasi layanan DNS (BIND9 atau dnsmasq) dan menguji dengan command nslookup dan ping menggunakan nama.

- **Kegiatan Penutup (10 menit):**

- Kuis cepat (quizzz/live worksheet) tentang record DNS (A, CNAME, MX).
- Refleksi tentang pentingnya DNS dalam pengalaman browsing sehari-hari.

PERTEMUAN 3 (4 JP): Serangan dan Pertahanan (Deep Learning Challenge)

- **Kegiatan Awal (15 menit):**

- **Pemantik (Joyful & Meaningful):** "Tim Security telah mendapatkan informasi bahwa akan ada serangan pada jaringan kita dalam 30 menit! Tugas kalian adalah melakukan *hardening!*"
- Siswa menonton video singkat tentang dampak cyber attack pada dunia nyata.

- **Kegiatan Inti (150 menit):**
 - **Stimulasi:** Guru melakukan demo *scanning* dengan nmap ke server yang tidak dikonfigurasi keamanannya, menunjukkan port-port yang terbuka dan berbahaya.
 - **Problem Statement (Deep Learning):** "Lakukan scanning terhadap server milik tim lain. Identifikasi 3 kerentanan terbesar. Kemudian, amankan server kalian sendiri berdasarkan temuan tersebut!"
 - **Eksplorasi & Kolaborasi:** Tim berganti peran menjadi "**Penyerang**" (menggunakan nmap, telnet) dan "**Pertahanan**" (mencari cara menutup port, menginstall fail2ban, mengkonfigurasi firewall ufw).
 - **Assimilation & Creation:** Siswa membuat log temuan keamanan dan langkah-langkah mitigasi yang mereka terapkan. Ini adalah puncak dari berpikir kritis dan pemecahan masalah.

- **Kegiatan Penutup (15 menit):**
 - Diskusi kelas: "Port dan service apa saja yang *seharusnya* terbuka untuk sebuah server jaringan?".
 - Guru menekankan etika hacking (*penetration testing* hanya dilakukan dengan izin).

PERTEMUAN 4 (4 JP): Implementasi, Troubleshooting, dan Demonstrasi (Meaningful Showcase)

- **Kegiatan Awal (10 menit):**
 - Briefing untuk persiapan presentasi dan simulasi *helpdesk*.

- **Kegiatan Inti (160 menit):**
 - **Simulasi Helpdesk (Joyful & Meaningful):** Guru memberikan "**Tiket Gangguan**" kepada setiap tim (e.g., "Client tidak bisa mendapatkan IP", "Tidak bisa akses website internal").
 - **Problem Solving (Deep Learning):** Tim harus melakukan troubleshooting berdasarkan tiket tersebut dengan metode yang terstruktur (cek fisik, cek log, cek konfigurasi).
 - **Creation & Demonstration:** Setiap tim mempresentasikan desain jaringan lengkap mereka, konfigurasi yang telah dibuat, dan menceritakan pengalaman

saat menjadi "penyerang" dan "bertahan". Mereka juga menunjukkan penyelesaian tiket gangguan.

- **Kegiatan Penutup (10 menit):**

- **Refleksi Akhir:** Siswa menuliskan pada selembar kertas: "Satu hal paling berharga yang saya pelajari adalah..." dan "Satu hal yang masih ingin saya pelajari lebih dalam adalah...".
- Guru memberikan apresiasi kepada seluruh tim dan menginformasikan materi selanjutnya.

F. Asesmen / Penilaian

1. Asesmen Formatif:

- **Kinerja (Observasi):** Keaktifan dalam diskusi, ketrampilan dalam menggunakan CLI, prosedur troubleshooting. (Rubrik)
- **Kuis:** Quizizz pada setiap akhir pertemuan untuk mengingat konsep kunci.

2. Asesmen Sumatif:

- **Proyek (Produk):** Konfigurasi server yang berfungsi (DHCP, DNS, Keamanan). (Rubrik: Kelengkapan, Fungsionalitas, Efisiensi)
- **Laporan & Presentasi (Portofolio):** Kualitas dokumentasi teknis dan presentasi. (Rubrik: Kelengkapan, Struktur, Analisis)
- **Sikap:** Kolaborasi dalam tim dan kemandirian belajar. (Rubrik Pengamatan)

G. Pengayaan dan Remedial

- **Pengayaan:** Siswa yang cepat dapat mencoba konfigurasi yang lebih kompleks: 1) Membuat DNS Master-Slave, 2) Mengkonfigurasi VLAN dan DHCP Relay, 3) Melakukan analisis packet yang lebih mendalam dengan Wireshark.
- **Remedial:** Siswa yang mengalami kesulitan akan diberikan pendampingan one-on-one atau dalam kelompok kecil dengan menggunakan lembar kerja yang lebih terstruktur dan simulasi yang disederhanakan.

H. Referensi dan Lampiran

- **Buku Teks:** "Jaringan Komputer" oleh Abdul Kadir, "Debian Server Handbook".
- **Online:** Dokumentasi Debian, DigitalOcean Tutorials, Cisco Networking Academy.