

MODUL AJAR FASE F

SISTEM KEAMANAN JARINGAN

3

TUJUAN
PEMBELAJARAN



Modul 3

TP : Secure Socket Layer (SSL)



Idiarso, S.Kom

SISTEM INFORMASI
JARINGAN DAN APLIKASI



Modul Ajar 3
Konsentrasi Keahlian
Sistem Informasi jaringan dan Aplikasi
Konsep Keamanan jaringan

Konsentrasi Keahlian	: Sistem Informasi Jaringan dan Aplikasi
Mata Pelajaran Fase	: Sistem Keamanan Jaringan
Fase	: F
Nama Penyususn	: Idiarso, S.Kom
Instansi	: SMKN 1 Punggelan
Jumlah Jam	: 36 JP (5 x Pertemuan)

1. TUJUAN PEMBELAJARAN

Memahami konsep dan implementasi Secure Socket Layer (SSL) dalam konteks keamanan jaringan.

Indikator Ketercapaian Tujuan Pembelajaran

- Menggambarkan pengertian dan tujuan dari SSL.
- Membedakan antara HTTP dan HTTPS serta keuntungan penggunaan SSL.
- Menjelaskan langkah-langkah dalam mengimplementasikan SSL pada sebuah situs web.
- Menganalisis risiko keamanan yang terkait dengan SSL dan langkah-langkah untuk mengurangi risiko tersebut.
- Memahami konsep sertifikat digital dan otoritas sertifikat (Certificate Authorities).
- Mampu melakukan konfigurasi SSL pada server dan menguji koneksi yang aman menggunakan alat-alat seperti OpenSSL.

Materi yang akan dibahas dalam pertemuan-pertemuan terkait SSL:

Pertemuan 1:

- Pengantar keamanan jaringan dan pentingnya SSL.
- Pengertian dasar tentang SSL dan fungsinya.
- Perbedaan antara HTTP dan HTTPS.

Pertemuan 2:

- Langkah-langkah implementasi SSL pada sebuah situs web.
- Jenis-jenis sertifikat digital dan peran Certificate Authorities.
- Proses penerbitan dan verifikasi sertifikat SSL.

Pertemuan 3:

- Manajemen sertifikat SSL dan tata kelola keamanan.
- Risiko dan ancaman terkait dengan SSL.
- Langkah-langkah untuk mengurangi risiko keamanan SSL.

Pertemuan 4:

- Konfigurasi SSL pada server menggunakan alat seperti OpenSSL.
- Pengujian koneksi yang aman dan verifikasi sertifikat.
- Troubleshooting masalah terkait SSL.

Pertemuan 5:

- Diskusi dan analisis kasus nyata terkait SSL dalam konteks bisnis atau industri.
- Identifikasi kerentanan SSL dan rekomendasi perbaikan.

1. LANGKAH PEMBELAJARAN

Pertemuan 1 (4x45 menit)

Pendahuluan:

- 1) Guru memperkenalkan materi SSL dengan memberikan penjelasan singkat tentang keamanan dalam komunikasi online dan pentingnya penggunaan SSL dalam melindungi data.
- 2) Peserta didik diberikan pertanyaan pemandik untuk membangkitkan pemahaman awal mereka:
 - a. Apa yang kalian ketahui tentang keamanan dalam komunikasi online?
 - b. Mengapa penting untuk melindungi data saat melakukan transmisi online?

Inti:

- 1) Guru menjelaskan konsep dasar SSL, termasuk definisi, tujuan, dan cara kerjanya dalam melindungi data saat ditransmisikan melalui internet.
- 2) Peserta didik diajak untuk menjelajahi sumber daya online yang membahas tentang SSL, seperti artikel, panduan, atau tutorial.
- 3) Peserta didik dibagi menjadi kelompok-kelompok kecil untuk melakukan diskusi tentang manfaat penggunaan SSL dalam lingkungan bisnis dan dampaknya terhadap kepercayaan pelanggan.
- 4) Setiap kelompok diminta untuk membuat rangkuman diskusi mereka dalam bentuk peta konsep atau diagram yang mencakup konsep-konsep kunci tentang SSL.
- 5) Kelompok-kelompok mempresentasikan rangkuman mereka kepada seluruh kelas, sambil memberikan kesempatan bagi peserta didik lain untuk memberikan tanggapan dan bertanya.

Penutup:

Guru mengadakan sesi tanya jawab untuk memastikan pemahaman peserta didik tentang materi SSL.

- 2) Peserta didik diberi kesempatan untuk merenungkan pembelajaran hari ini dan memberikan refleksi singkat tentang pemahaman mereka.
- 3) Guru memberikan pengumuman tentang materi yang akan dibahas pada pertemuan berikutnya dan memberikan tugas persiapan terkait materi tersebut.

4) Pembelajaran ditutup dengan doa.

Catatan penting:

- a. Penjelasan Tujuan Pembelajaran: Modul ajar ini menyertakan penjelasan singkat tentang tujuan pembelajaran yang ingin dicapai, yaitu pemahaman peserta didik tentang konsep dasar SSL, manfaatnya dalam bisnis, dan dampaknya terhadap kepercayaan pelanggan.
 - b. Penyediaan Sumber Referensi: Peserta didik diberikan arahan untuk menjelajahi sumber daya online terkait SSL, sehingga mereka dapat mencari informasi yang relevan dan memperluas pemahaman mereka tentang topik tersebut.
 - c. Aktivitas Diskusi Kelompok yang Terstruktur: Modul ajar ini mencakup aktivitas diskusi kelompok yang terstruktur, di mana peserta didik diberi kesempatan untuk berbagi pemikiran, ide, dan perspektif mereka tentang SSL. Aktivitas ini mendorong interaksi dan kolaborasi antar peserta didik.
 - d. Evaluasi Pemahaman: Modul ajar ini mencakup sesi tanya jawab dan refleksi singkat, yang memberikan kesempatan bagi guru untuk mengevaluasi pemahaman peserta didik dan memastikan bahwa mereka telah memahami konsep SSL yang diajarkan.
 - e. Penggunaan Media yang Variatif: Modul ajar ini dapat diperkaya dengan penggunaan media yang beragam, seperti presentasi slide, video tutorial, atau demonstrasi langsung, untuk membantu visualisasi konsep SSL dan meningkatkan pengalaman pembelajaran peserta didik.
-

Pertemuan 2 (4x45 menit)

Pendahuluan:

- 1) Guru menyampaikan ulasan singkat tentang materi SSL yang telah dibahas pada pertemuan sebelumnya.
- 2) Peserta didik diberikan kesempatan untuk berbagi pengalaman atau pemahaman tambahan yang mereka dapatkan setelah menjelajahi sumber daya tentang SSL.

Inti:

- 1) Guru membahas secara lebih mendalam tentang komponen-komponen SSL,

termasuk sertifikat digital, enkripsi, dan protokol yang digunakan dalam SSL.

- 2) Peserta didik diberikan contoh konkret tentang bagaimana SSL bekerja dalam skenario nyata, seperti saat melakukan transaksi perbankan online atau mengakses situs web yang menggunakan protokol HTTPS.
- 3) Peserta didik diberi kesempatan untuk melakukan praktik simulasi dalam pengaturan SSL, seperti mengkonfigurasi sertifikat digital atau menerapkan enkripsi pada koneksi jaringan.
- 4) Guru memfasilitasi diskusi kelompok tentang tantangan dan manfaat dalam menerapkan SSL dalam berbagai konteks, seperti di situs web, aplikasi seluler, atau jaringan perusahaan.
- 5) Peserta didik diberikan tugas individu untuk meneliti dan melaporkan tentang tren terkini dalam pengembangan SSL, termasuk inovasi atau teknologi terbaru yang relevan.

Penutup:

- 1) Guru menyimpulkan materi yang telah dibahas pada pertemuan tersebut dan memberikan kesempatan bagi peserta didik untuk bertanya atau memberikan tanggapan.
 - 2) Peserta didik diminta untuk merefleksikan pemahaman mereka tentang SSL setelah pembelajaran hari ini dan mencatat hal-hal yang perlu mereka eksplorasi lebih lanjut.
 - 3) Guru memberikan pengumuman tentang tugas persiapan untuk pertemuan selanjutnya terkait dengan SSL.
 - 4) Pembelajaran ditutup dengan doa.
-

Catatan penting:

- a. Pembahasan Komponen-komponen SSL: Modul ajar memberikan penjelasan yang lebih mendalam tentang komponen-komponen SSL, termasuk sertifikat digital, enkripsi, dan protokol yang digunakan. Hal ini membantu peserta didik memahami bagaimana SSL bekerja secara lebih rinci.
- b. Praktik Simulasi: Peserta didik diberikan kesempatan untuk melakukan praktik simulasi terkait pengaturan SSL. Hal ini membantu mereka memperoleh pengalaman praktis dalam mengimplementasikan SSL dan memperkuat pemahaman mereka tentang konsep yang telah diajarkan.
- c. Diskusi Kelompok: Melalui diskusi kelompok, peserta didik dapat berbagi pemikiran, tantangan, dan manfaat terkait

- d. ait penerapan SSL dalam berbagai konteks. Diskusi ini memungkinkan mereka untuk memperluas perspektif dan memperdalam pemahaman tentang keamanan komunikasi online.
 - e. Penelitian Tren Terkini: Peserta didik diberikan tugas untuk meneliti tren terkini dalam SSL. Ini membantu mereka tetap terinformasi tentang perkembangan terbaru dalam teknologi SSL dan mengembangkan kemampuan riset mereka.
-

Pertemuan 3 (4x45 menit)

Pendahuluan:

- 1) Guru menyampaikan ulasan singkat tentang materi SSL yang telah dibahas pada pertemuan sebelumnya.
- 2) Peserta didik diberikan kesempatan untuk berbagi hasil penelitian mereka tentang tren terkini dalam pengembangan SSL.

Inti:

- 1) Guru membahas tentang penggunaan SSL dalam berbagai aplikasi dan layanan online, seperti e-commerce, perbankan online, layanan email, dan media sosial.
- 2) Peserta didik diberikan contoh konkret tentang manfaat dan keuntungan menggunakan SSL dalam setiap aplikasi dan layanan tersebut.
- 3) Guru memfasilitasi diskusi kelompok tentang tantangan dan risiko yang mungkin terjadi dalam implementasi SSL dan bagaimana mengatasi masalah tersebut.
- 4) Peserta didik diberi tugas untuk melakukan analisis keamanan pada sebuah situs web atau aplikasi yang menggunakan SSL, dengan mengidentifikasi potensi kerentanan dan memberikan rekomendasi untuk meningkatkan keamanannya.
- 5) Guru memberikan penjelasan tentang jenis-jenis serangan yang dapat terjadi terhadap SSL, seperti serangan Man-in-the-Middle (MitM) atau serangan SSL Stripping. Peserta didik diberikan pemahaman tentang cara mendekripsi dan mencegah serangan-serangan tersebut.

Penutup:

- 1) Guru menyimpulkan materi yang telah dibahas pada pertemuan tersebut dan memberikan kesempatan bagi peserta didik untuk bertanya atau memberikan tanggapan.

2) Peserta didik diminta untuk merefleksikan pemahaman mereka tentang penggunaan SSL dalam aplikasi dan layanan online, serta bagaimana melindungi dari serangan-serangan terhadap SSL.

3) Guru memberikan pengumuman tentang tugas persiapan untuk pertemuan selanjutnya terkait dengan penerapan SSL pada proyek kecil.

4) Pembelajaran ditutup dengan doa.

Pada pertemuan ketiga ini, fokusnya adalah penggunaan SSL dalam berbagai aplikasi dan layanan online, serta pemahaman tentang serangan-serangan yang mungkin terjadi terhadap SSL. Peserta didik juga diberikan kesempatan untuk melakukan analisis keamanan pada sebuah situs web atau aplikasi yang menggunakan SSL.

Catatan penting:

- a. Penerapan SSL dalam Aplikasi dan Layanan: Modul ajar membahas penggunaan SSL dalam berbagai aplikasi dan layanan online yang relevan bagi peserta didik. Hal ini membantu mereka memahami bagaimana SSL dapat digunakan untuk melindungi data dan privasi dalam konteks yang lebih spesifik.
 - b. Diskusi tentang Tantangan dan Risiko: Diskusi kelompok memungkinkan peserta didik untuk berbagi pemikiran tentang tantangan dan risiko dalam implementasi SSL, serta mencari solusi untuk mengatasi masalah tersebut. Ini memperluas pemahaman mereka tentang aspek praktis dalam penerapan SSL.
 - c. Analisis Keamanan dan Pencegahan Serangan: Peserta didik diberikan tugas untuk melakukan analisis keamanan pada situs web atau aplikasi yang menggunakan SSL. Hal ini melibatkan mereka secara aktif dalam menerapkan pengetahuan dan keterampilan mereka untuk mengidentifikasi kerentanan dan memberikan rekomendasi untuk meningkatkan keamanan.
-

Pertemuan 4 (4x45 menit)

Pendahuluan:

- 1) Guru menyampaikan ringkasan tentang materi SSL yang telah dibahas pada pertemuan sebelumnya.
- 2) Peserta didik diberikan kesempatan untuk bertanya atau memberikan tanggapan terkait pemahaman mereka tentang penggunaan SSL dan analisis keamanan pada situs web atau aplikasi.

Inti:

- 1) Guru membahas tentang penerapan SSL pada proyek kecil yang melibatkan peserta didik secara langsung. Guru menjelaskan langkah-langkah yang perlu dilakukan untuk mengimplementasikan SSL pada proyek tersebut.
- 2) Peserta didik diberi tugas untuk melakukan implementasi SSL pada proyek kecil mereka. Mereka akan mempraktikkan penggunaan sertifikat SSL, konfigurasi server, dan menguji keamanan serta fungsionalitas SSL pada proyek tersebut.
- 3) Guru memberikan panduan langkah-demi-langkah dan bahan referensi yang diperlukan untuk membantu peserta didik dalam melakukan implementasi SSL.
- 4) Peserta didik diminta untuk membuat laporan yang berisi dokumentasi langkah-langkah implementasi SSL pada proyek kecil mereka, beserta evaluasi keamanan dan kinerja yang mereka amati selama proses implementasi.
- 5) Guru memfasilitasi sesi diskusi di mana peserta didik dapat berbagi pengalaman, tantangan, dan hasil dari implementasi SSL pada proyek mereka.

Penutup:

- 1) Guru menyimpulkan materi yang telah dibahas pada pertemuan tersebut dan memberikan kesempatan bagi peserta didik untuk bertanya atau memberikan tanggapan terkait implementasi SSL pada proyek kecil.
- 2) Peserta didik diminta untuk merefleksikan pengalaman mereka dalam implementasi SSL dan manfaat yang mereka peroleh dari penggunaan SSL pada proyek tersebut.
- 3) Guru memberikan penugasan persiapan untuk pertemuan selanjutnya terkait dengan pertanyaan dan studi kasus terkait SSL.
- 4) Pembelajaran ditutup dengan doa.

Pada pertemuan keempat ini, fokusnya adalah pada penerapan praktis SSL dalam proyek kecil yang melibatkan peserta didik secara langsung. Mereka akan melakukan implementasi SSL, menguji keamanan dan fungsionalitasnya, serta membuat laporan dokumentasi.

Catatan penting:

- a. **Implementasi SSL pada Proyek Kecil:** Modul ajar memberikan pengalaman praktis kepada peserta didik dengan melibatkan mereka dalam implementasi SSL pada proyek kecil. Hal ini membantu mereka mengaplikasikan pengetahuan teoritis menjadi tindakan nyata.
 - b. **Evaluasi Keamanan dan Kinerja:** Peserta didik diminta untuk mengamati dan mengevaluasi keamanan serta kinerja SSL selama proses implementasi. Ini membantu mereka mengembangkan kemampuan dalam menganalisis dan mengoptimalkan penggunaan SSL.
 - c. **Sesi Diskusi dan Berbagi Pengalaman:** Guru memfasilitasi sesi diskusi di mana peserta didik dapat berbagi pengalaman, tantangan, dan hasil dari implementasi SSL pada proyek mereka. Hal ini memungkinkan mereka belajar dari pengalaman satu sama lain dan memperluas pemahaman mereka tentang penerapan SSL.
 - d. **Dengan perbaikan ini, diharapkan pertemuan keempat tentang SSL memberikan pengalaman nyata bagi peserta didik dalam implementasi SSL pada proyek kecil, serta memperkuat pemahaman mereka tentang keamanan dan kinerja SSL.**
-

Pertemuan 5 (4x45 menit)

Pendahuluan:

- 1) Guru menyampaikan ringkasan tentang materi implementasi SSL pada proyek kecil yang telah dibahas pada pertemuan sebelumnya.
- 2) Peserta didik diberikan kesempatan untuk bertanya atau memberikan tanggapan terkait pengalaman mereka dalam implementasi SSL.

Inti:

- 1) Guru membahas studi kasus terkait keamanan SSL pada lingkungan bisnis dan industri. Guru menjelaskan tentang risiko yang terkait dengan SSL, seperti serangan SSL stripping, serangan Man-in-the-Middle, dan kerentanan terhadap protokol SSL tertentu.
- 2) Peserta didik diberi tugas untuk menganalisis studi kasus yang diberikan dan mengidentifikasi kerentanan serta langkah-langkah yang dapat diambil untuk meningkatkan keamanan SSL dalam konteks bisnis atau industri tersebut.
- 3) Guru memberikan panduan dan bahan referensi yang diperlukan untuk membantu peserta didik dalam menganalisis studi kasus dan mengidentifikasi langkah-langkah perbaikan.
- 4) Peserta didik diminta untuk membuat laporan analisis studi kasus yang berisi identifikasi kerentanan SSL dan rekomendasi untuk meningkatkan keamanan.
- 5) Guru memfasilitasi sesi diskusi di mana peserta didik dapat berbagi hasil analisis mereka, memberikan masukan, dan bertukar pemikiran terkait langkah-langkah perbaikan SSL.

Penutup:

- 1) Guru menyimpulkan materi yang telah dibahas pada pertemuan tersebut dan mengaitkannya dengan pengalaman nyata dalam lingkungan bisnis atau industri.
- 2) Peserta didik diminta untuk merefleksikan analisis studi kasus dan rekomendasi yang mereka buat, serta mempertimbangkan implikasi keamanan SSL dalam dunia nyata.

3) Guru memberikan penugasan persiapan untuk pertemuan selanjutnya terkait dengan topik keamanan jaringan terkait SSL.

4) Pembelajaran ditutup dengan doa.

Pada pertemuan kelima ini, fokusnya adalah pada studi kasus terkait keamanan SSL dalam lingkungan bisnis atau industri. Peserta didik akan menganalisis kerentanan SSL dan mengusulkan langkah-langkah perbaikan.

Catatan penting:

- a. Studi Kasus Keamanan SSL: Modul ajar memberikan studi kasus yang relevan dengan lingkungan bisnis atau industri untuk membantu peserta didik memahami risiko dan tantangan yang terkait dengan keamanan SSL di dunia nyata.
 - b. Analisis dan Rekomendasi: Peserta didik diajak untuk menganalisis studi kasus dan mengidentifikasi kerentanan SSL, serta memberikan rekomendasi untuk meningkatkan keamanan. Hal ini melibatkan pemikiran kritis dan penerapan pengetahuan SSL secara praktis.
 - c. Sesi Diskusi dan Pertukaran Pemikiran: Guru memfasilitasi sesi diskusi di mana peserta didik dapat berbagi hasil analisis mereka dan bertukar pemikiran terkait langkah-langkah perbaikan SSL. Hal ini memungkinkan kolaborasi dan pembelajaran antar peserta didik.
-
-

2. ASESMEN

Asesmen Awal	: a. Menjelaskan pengertian animasi b. Mendeskripsikan perkembangan proses produksi animasi mulai dari teknologi konvensional sampai dengan teknologi modern
Asesmen Proses	: Observasi diskusi sesuai LKPD 1 dan LKPD 2
Asesmen Akhir	: Observasi film animasi dan proses produksinya 2 dari luar negeri dan 2 dari dalam negeri dipandu dengan LKPD 3

LEMBAR KERJA PESERTA DIDIK (LKPD)

LEMBAR KERJA PESERTA DIDIK 1

LEMBAR KERJA PESERTA DIDIK 1

Pertemuan 1: Pengenalan Secure Socket Layer (SSL)

1. Berkelompoklah menjadi 8 (delapan) kemudian tulis nama dan nomor absen peserta didik di kelompokmu.
2. Buka HP masing-masing dan carilah materi tentang Secure Socket Layer (SSL) di internet. Cari informasi tentang pengertian SSL, tujuan penggunaannya, dan manfaat keamanan yang diberikan oleh SSL dalam konteks jaringan dan bisnis.
3. Diskusikan bersama kelompokmu tentang konsep SSL berikut ini:
 - a. Pengertian SSL dan cara kerjanya.
 - b. Perbedaan antara HTTP dan HTTPS.
 - c. Keuntungan penggunaan SSL dalam bisnis dan keamanan jaringan.
4. Tuangkan hasil diskusi kelompokmu dalam bentuk presentasi yang diupload melalui form di google classroom!. Gambarkan hubungan antara konsep-konsep yang telah dibahas dalam diskusi.
5. Sertakan gambar dan langkah langkah pengerjaan tugas tersebut.
6. Buatlah laporan hasil diskusi kelompokmu dengan menyertakan foto peta konsep dan deskripsi singkat tentang konsep-konsep yang telah dibahas. Laporan ini dapat berupa dokumen tertulis, presentasi PowerPoint, atau animasi sesuai dengan kreativitas kelompokmu.
7. Presentasikan laporan kelompokmu di depan kelas secara bergiliran. Jelaskan konsep-konsep yang telah dibahas dan sampaikan hasil diskusi kelompokmu kepada peserta didik lain.
8. Simpan hasil karya dan laporan sebagai portofolio untuk pertemuan selanjutnya.

Catatan: Jangan lupa mencantumkan sumber materi yang digunakan dalam pencarian informasi tentang SSL.

LEMBAR KERJA PESERTA DIDIK 2

LEMBAR KERJA PESERTA DIDIK 2

Pertemuan 2: Implementasi Secure Socket Layer (SSL)

1. Berkelompoklah menjadi 8 (delapan) dan tulis nama serta nomor absen peserta didik di kelompokmu.
2. Buka HP masing-masing dan carilah informasi tentang implementasi Secure Socket Layer (SSL) pada sebuah situs web. Cari tahu langkah-langkah yang perlu dilakukan untuk mengaktifkan SSL pada sebuah situs web dan mengamankan koneksi.
3. Diskusikan bersama kelompokmu tentang langkah-langkah implementasi SSL berikut ini:
 - a. Penggunaan sertifikat digital dalam SSL.
 - b. Proses penerbitan dan verifikasi sertifikat SSL.
 - c. Konfigurasi SSL pada server.
 - d. Menguji koneksi yang aman menggunakan alat seperti OpenSSL.
4. Tuangkan hasil diskusi kelompokmu dalam bentuk dalam bentuk presentasi yang diupload melalui form di google classrooml . Gambarkan hubungan antara konsep-konsep yang telah dibahas dalam diskusi.
5. Sertakan gambar dan langkah langkah penggerjaan tugas tersebut
6. Buatlah laporan hasil diskusi kelompokmu dengan menyertakan foto peta konsep dan deskripsi singkat tentang langkah-langkah implementasi SSL yang telah dibahas. Laporan ini dapat berupa dokumen tertulis, presentasi PowerPoint, atau animasi sesuai dengan kreativitas kelompokmu.
7. Presentasikan laporan kelompokmu di depan kelas secara bergiliran. Jelaskan langkah-langkah implementasi SSL dan sampaikan hasil diskusi kelompokmu kepada peserta didik lain.
8. Simpan hasil karya dan laporan sebagai portofolio untuk pertemuan selanjutnya.

Catatan: Jangan lupa mencantumkan sumber materi yang digunakan dalam pencarian informasi tentang implementasi SSL pada situs web.

LEMBAR KERJA PESERTA DIDIK 3

Pertemuan 3: Keamanan Data dan Enkripsi menggunakan SSL

1. Berkumpul dan tuliskan nama serta nomor absen peserta didik di kelompokmu.
2. Buka HP masing-masing dan carilah informasi tentang keamanan data dan enkripsi menggunakan SSL. Jelaskan mengapa keamanan data sangat penting dalam komunikasi online dan bagaimana SSL digunakan untuk melindungi data sensitif.
3. Diskusikan bersama kelompokmu tentang konsep enkripsi data dan bagaimana SSL memfasilitasi enkripsi pada koneksi web. Jelaskan langkah-langkah yang terlibat dalam proses enkripsi menggunakan SSL, termasuk:
 - a. Pemilihan algoritma enkripsi yang kuat.
 - b. Pertukaran kunci enkripsi.
 - c. Proses enkripsi dan dekripsi data.
4. Buatlah contoh skenario di mana pengguna mengakses situs web yang menggunakan SSL untuk melindungi data pengguna. Jelaskan bagaimana proses enkripsi dan dekripsi data berlangsung dalam skenario tersebut.
5. Gunakan kertas plano dan spidol untuk membuat peta konsep yang menggambarkan konsep keamanan data dan enkripsi menggunakan SSL. Tampilkan hubungan antara konsep-konsep yang telah dibahas dalam diskusi kelompokmu.
6. Fotolah peta konsep yang telah dibuat oleh kelompokmu dan tempelkan di tempat yang telah disepakati sebagai bagian dari "window shopping" di mana peserta didik lain dapat mengunjungi dan memberikan tanggapan.
7. Buatlah laporan hasil diskusi kelompokmu dengan menyertakan foto peta konsep dan deskripsi singkat tentang konsep keamanan data dan enkripsi menggunakan SSL. Laporan ini dapat berupa dokumen tertulis, presentasi PowerPoint, atau animasi sesuai dengan kreativitas kelompokmu.
8. Presentasikan laporan kelompokmu di depan kelas secara bergiliran. Jelaskan konsep keamanan data dan enkripsi menggunakan SSL serta sampaikan hasil diskusi kelompokmu kepada peserta didik lain.
9. Simpan hasil karya dan laporan sebagai portofolio untuk pertemuan selanjutnya.

Pastikan untuk menjelaskan konsep keamanan data dan enkripsi menggunakan SSL dengan jelas dan sederhana. Berikan contoh yang relevan dan nyata untuk membantu peserta didik memahami konsep tersebut. Sesuaikan LKPD dengan tingkat pemahaman dan kemampuan peserta didik Anda.

MODUL AJAR FASE F

SISTEM KEAMANAN JARINGAN



Idiarso, S.Kom

SISTEM INFORMASI
JARINGAN DAN APLIKASI

LAMPIRAN

RUBRIK PENILAIAN

Asesmen Proses

No	Kelompok	Keterbacaan Materi		Karya berupa Peta Konsep		Kreativitas		Laporan Diskusi		Presentasi	
		Ya	Tdk	Ya	Tdk	Ya	Tdk	Ya	Tdk	Ya	Tdk

Asesmen Akhir : Budi

Nama Siswa:					
No	Kreteria Ketuntasan	KETERCAPAIAN			
		Kurang kompeten (1)	Cukup Kompeten (2)	Kompeten (3)	
1	Memahami Konsep Keamanan Data: Peserta didik mampu menjelaskan konsep dasar keamanan data, termasuk pentingnya keamanan data dalam komunikasi online dan potensi risiko yang dapat terjadi tanpa keamanan yang memadai.		v		
2	Memahami Enkripsi Data: Peserta didik mampu menjelaskan konsep enkripsi data dan bagaimana enkripsi digunakan untuk melindungi data sensitif. Mereka juga memahami langkah-langkah yang terlibat dalam proses enkripsi, seperti pemilihan algoritma enkripsi, pertukaran kunci enkripsi, dan proses enkripsi dan dekripsi data.			v	
3	Memahami Penggunaan SSL: Peserta didik mampu menjelaskan penggunaan SSL (Secure Socket Layer) dalam koneksi web dan bagaimana SSL memfasilitasi enkripsi data. Mereka memahami manfaat dan tujuan penggunaan SSL dalam melindungi data pengguna saat berkomunikasi dengan situs web yang menggunakan SSL.		v		
4	Mengidentifikasi Kelebihan SSL: Peserta didik mampu mengidentifikasi kelebihan SSL dalam melindungi data, termasuk aspek keamanan yang ditawarkan oleh SSL seperti integritas data, keaslian identitas, dan kerahasiaan informasi.		v		
5	Mengidentifikasi Potensi Ancaman: Peserta didik mampu mengidentifikasi potensi ancaman terhadap keamanan data, seperti serangan Man-in-the-Middle, peretasan data, dan pengintaian. Mereka juga memahami bagaimana SSL dapat membantu melindungi data dari ancaman tersebut.	v			

6	Menerapkan SSL dalam Konteks Praktis: Peserta didik mampu menerapkan pemahaman mereka tentang SSL dalam konteks praktis. Misalnya, mereka mampu menjelaskan langkah-langkah yang dilakukan saat mengakses situs web yang menggunakan SSL, atau menjelaskan proses enkripsi dan dekripsi data dalam komunikasi yang dilindungi SSL.		v	
	Menyampaikan Tanggapan: Peserta didik mampu memberikan tanggapan yang relevan dan terinformasi terhadap materi yang telah dipelajari, baik dalam bentuk pertanyaan, masukan, atau pemikiran kritis terkait konsep keamanan data dan enkripsi menggunakan SSL.		v	
	Portofolio dan Presentasi: Peserta didik menyimpan hasil karya dan laporan sebagai bagian dari portofolio mereka. Mereka juga mampu menyampaikan presentasi tentang konsep keamanan data dan enkripsi menggunakan SSL dengan jelas dan terstruktur.		v	

KKTP:

0 – 40 %	<i>Belum tuntas, remidi pada seluruh materi</i>
41 – 60 %	<i>Belum tuntas, remidi pada materi yang belum dikuasai</i>
61 – 80 %	<i>Sudah tuntas, tetapi tanpa pengayaan</i>
81 – 100%	<i>Sudah tuntas, perlu pengayaan atau tantangan lebih</i>

Profil Pelajar Pancasila

No	Dimensi Kreatif-Sub Elemen	Terlihat maks	Terlihat sedikit	Belum terlihat
1	Mengeksplorasi dan mengekspresikan pikiran dan/atau perasaannya dalam bentuk karya dan/atau tindakan, serta mengevaluasinya dan mempertimbangkan dampak dan risikonya bagi diri dan lingkungannya			
2	Menghasilkan gagasan yang beragam untuk mengekspresikan pikiran dan/atau perasaannya, menilai gagasannya, serta memikirkan segala risikonya dengan mempertimbangkan banyak perspektif seperti etika dan nilai kemanusiaan ketika gagasannya direalisasikan			

3. ASESMEN PEMBELAJARAN, REMEDIAL DAN PENGAYAAN

1. Teknik penilaian

- | | |
|---------------------------|---|
| a. Sikap Prilaku Karakter | : Observasi (Format Penilaian Sikap) |
| b. Sikap Sosial | : Observasi (Format Penilaian Sikap) |
| c. Produk | : LKPD Peserta Didik |
| d. Proses | : Tes Lisan (Format Assessmen Kinerja Proses) |
| e. Keterampilan | : Praktikum (Format Assessmen Kinerja Keterampilan) |

2. Instrumen penilaian

- | | |
|-----------------------|-----------------------------------|
| a. Lembar Penilaian | : Sikap Perilaku Karakter |
| b. Lembar Penilaian 2 | : Sikap Sosial |
| c. Lembar Penilaian 3 | : Produk dilengkapi kunci jawaban |
| d. Lembar Penilaian 4 | : Proses |
| e. Lembar Penilaian 5 | : Keterampilan |

3. Pembelajaran remedial dan pengayaan

a) Remedial

Remedial dilaksanakan setelah diadakan penilaian pengetahuan bagi peserta didik yang mendapat nilai di bawah KKM dengan memberi tugas berupa:

- Mengulang Pendalaman Materi terkait rincian materi yang sulit
- Memanfaatkan peserta didik yang nilainya paling baik dan mempunyai kemampuan lebih untuk melakukan tutor sebaya
- Mengulang Melakukan Evaluasi dengan materi yang sama

b) Pengayaan

Peserta didik yang mendapat nilai di atas KKM diberikan pengayaan berupa:

- Memberikan tugas baru yang sepadan

- Mengembangkan materi yang sudah dikuasai dan membandingkan dari berbagai sumber belajar.

Lampiran

1. Bahan Ajar (materi ajar, e-book)
2. Jobsheet (LKPD)
3. Media
4. Rubrik Penilaian (P,K,S) dan Kisi – kisi

Mengetahui
Kepala SMK Negeri 1 Punggelan

Banjarnegara, 19 Juni 2023
Guru Mata Pelajaran,

Drs. Supriyadi
NIP. 19660128 199302 1 002

Idiarso, S.Kom
NIP.19830804 202221 1 006

BAHAN BACAAN

1. "SSL/TLS: A Beginner's Guide" by J. Clark and A. Tatham - Buku ini memberikan pengantar mendalam tentang SSL/TLS, menjelaskan konsep, protokol, dan penerapannya dalam keamanan web. (Tersedia di toko buku atau perpustakaan terdekat)
2. "Understanding SSL/TLS: Securing Web Applications with Cryptography" by P. Zakas - Buku ini menjelaskan secara rinci tentang SSL/TLS, termasuk enkripsi, sertifikat digital, dan praktik keamanan terkait. (Tersedia di toko buku atau perpustakaan terdekat)
3. "SSL and TLS: Theory and Practice" by Rolf Oppliger - Buku ini memberikan pemahaman yang komprehensif tentang SSL/TLS, termasuk teori dasar, protokol, dan implementasi praktisnya. (Tersedia di toko buku atau perpustakaan terdekat)

referensi web tentang SSL:

1. "SSL/TLS Strong Encryption: An Introduction" - Artikel ini memberikan pemahaman dasar tentang SSL/TLS dan mengapa enkripsi yang kuat penting dalam komunikasi web. Tersedia di: [<https://www.ssl.com/article/ssl-tls-strong-encryption-an-introduction/>](https://www.ssl.com/article/ssl-tls-strong-encryption-an-introduction/)
2. "How SSL/TLS Works" - Artikel ini menjelaskan langkah-langkah yang terlibat dalam proses SSL/TLS dan bagaimana koneksi aman terbentuk antara klien dan server. Tersedia di: [<https://howhttps.works/>](https://howhttps.works/)
3. "SSL Certificate Guide: What Are SSL Certificates & How Do They Work?" - Panduan ini menjelaskan tentang sertifikat SSL, otoritas sertifikat, dan proses verifikasi yang terlibat dalam memvalidasi keaslian situs web. Tersedia di: [<https://www.digicert.com/ssl-certificates.htm>](https://www.digicert.com/ssl-certificates.htm)
4. "SSL/TLS Best Practices" - Artikel ini memberikan panduan praktis tentang penggunaan SSL/TLS, termasuk konfigurasi server, pemilihan algoritma enkripsi, dan

manajemen sertifikat. Tersedia di: https://developer.mozilla.org/en-US/docs/Web/Security/Secure_Contexts

5. "SSL/TLS Deployment Best Practices" - Dokumen ini memberikan pedoman praktis tentang penerapan SSL/TLS yang aman, termasuk konfigurasi server, manajemen kunci, dan pemilihan sertifikat yang tepat. Tersedia di: https://ssl-config.mozilla.org/

Glosarium

1. SSL (Secure Sockets Layer): Protokol keamanan yang digunakan untuk mengamankan komunikasi data antara klien dan server di internet.
2. TLS (Transport Layer Security): Pengganti SSL, TLS adalah protokol keamanan yang digunakan untuk enkripsi dan otentikasi data yang dikirim melalui jaringan.
3. Enkripsi: Proses mengubah data menjadi bentuk yang tidak dapat dibaca atau dimengerti kecuali oleh penerima yang dituju. Dalam konteks SSL/TLS, enkripsi digunakan untuk melindungi kerahasiaan data yang dikirim antara klien dan server.
4. Sertifikat Digital: Sebuah file elektronik yang berisi informasi tentang identitas dan kunci publik dari entitas yang diverifikasi oleh Autoritas Sertifikat (CA). Sertifikat digital digunakan dalam SSL/TLS untuk memverifikasi keaslian situs web.
5. Protokol: Aturan dan prosedur yang digunakan untuk mengatur komunikasi antara komputer dan perangkat jaringan. Dalam konteks SSL/TLS, protokol mengacu pada serangkaian langkah-langkah yang digunakan untuk membentuk koneksi aman.
6. Kriptografi: Ilmu yang berkaitan dengan teknik pengamanan informasi melalui

penggunaan algoritma dan kunci enkripsi. SSL/TLS menggunakan kriptografi untuk melindungi data yang dikirim melalui jaringan.

7. Verifikasi: Proses memvalidasi keaslian dan integritas data atau identitas pihak yang terlibat dalam komunikasi. Dalam SSL/TLS, verifikasi dilakukan melalui sertifikat digital yang dikeluarkan oleh CA.
8. Klien: Komputer atau perangkat yang menginisiasi permintaan untuk mengakses suatu layanan atau sumber daya di jaringan. Dalam SSL/TLS, klien biasanya berfungsi sebagai pengguna yang mengakses situs web.
9. Server: Komputer atau perangkat yang menyediakan layanan atau sumber daya kepada klien melalui jaringan. Dalam SSL/TLS, server berperan sebagai entitas yang menyediakan situs web yang diamankan.
10. Algoritma Enkripsi: Metode matematika yang digunakan untuk melakukan enkripsi dan dekripsi data. SSL/TLS menggunakan berbagai algoritma enkripsi seperti RSA, AES, dan Elliptic Curve untuk melindungi data yang dikirim melalui jaringan.
11. Keamanan Web: Praktik dan teknologi yang digunakan untuk melindungi data dan privasi pengguna saat berinteraksi dengan situs web melalui internet. SSL/TLS adalah salah satu aspek keamanan web yang penting.
12. Autoritas Sertifikat (CA): Organisasi terpercaya yang mengeluarkan sertifikat digital untuk mengotentikasi keaslian situs web. CA melakukan verifikasi dan validasi identitas pemilik situs sebelum menerbitkan sertifikat.
13. Kunci Publik: Bagian dari pasangan kunci kriptografi yang digunakan dalam enkripsi asimetris. Kunci publik digunakan untuk melakukan enkripsi data dan memverifikasi tanda tangan digital.
14. Kunci Privat: Bagian

dari pasangan kunci kriptografi yang digunakan dalam enkripsi asimetris. Kunci privat digunakan untuk mendekripsi data yang telah dienkripsi dengan kunci publik yang sesuai.

15. Tanda Tangan Digital: Metode yang digunakan untuk memverifikasi keaslian dan integritas data. Tanda tangan digital dibuat menggunakan kunci privat dan dapat diverifikasi menggunakan kunci publik yang sesuai.

Harap dicatat bahwa ini adalah beberapa istilah yang umum digunakan dalam konteks SSL.

Ada banyak istilah dan konsep lain yang terkait dengan SSL/TLS yang dapat dieksplorasi lebih lanjut untuk pemahaman yang lebih mendalam.