SYS://SIBERLAB MODE: SIMULASI STATUS: AMAN UNTUK BELAJAR



MODUL AJAR · PEMBELAJARAN MENDALAM

SiberLab

Ruang Aman untuk Belajar Keamanan Jaringan

```
> coba → salah → ulangi → paham _
# kesalahan adalah anak tangga terbaik untuk mendapatkan ilmu
```

Fase E dan Fase F | Program Keahlian TKJ | Kurikulum Merdeka | Pembelajaran Mendalam

PENGEMBANG DAN PENYUSUN

Aliyudin

Guru Mata Pelajaran Produktif TKJ · SMK Ciledug Al Musaddadiyah

Modul Ajar

Keamanan Jaringan Berbasis Simulasi SiberLab

Ruang aman untuk belajar: boleh salah, boleh mengulang, karena kesalahan adalah anak tangga terbaik untuk mendapatkan ilmu

Penyusun: Aliyudin, Guru Mata Pelajaran Produktif TKJ, SMK Ciledug Al Musaddadiyah

Pengantar dari Penyusun

Modul ini disusun sebagai usulan rancangan pembelajaran, bukan sebagai pedoman yang harus diikuti apa adanya. Setiap kelas memiliki karakter, waktu, dan perangkat yang berbeda, sehingga Bapak dan Ibu Guru sangat dipersilakan menyesuaikan, memotong, atau menggantinya sesuai kebutuhan murid.

Penyusun menyadari bahwa modul ini masih jauh dari sempurna. Bila ada bagian yang bermanfaat, itu berkat ilmu dari banyak guru dan praktisi yang lebih dahulu berbagi. Bila ada kekeliruan, penyusun berterima kasih atas koreksi yang membangun dan berjanji memperbaikinya dengan lapang dada.

> **Pegangan utama modul ini**
> Murid boleh salah. Murid boleh mengulang. Setiap kesalahan di dalam simulasi adalah anak tangga menuju pemahaman, bukan alasan untuk merasa kecil.

A. Identitas Modul

Penyusun	Aliyudin
Satuan pendidikan	SMK Ciledug Al Musaddadiyah
Mata pelajaran	Produktif program keahlian TKJ (bidang keamanan jaringan)
Fase dan kelas	Fase E (Kelas X) pada jalur fondasi, dan Fase F (Kelas XI dan XII) pada jalur penguatan. Pembagian jalur dijelaskan pada bagian diferensiasi.
Topik	Dasar jaringan, firewall, VPN, hardening server, membaca log, kata sandi dan MFA, respons insiden, serta backup dan pemulihan
Alokasi waktu	Empat pertemuan. Contoh di modul ini memakai 4 jam pelajaran per pertemuan dan dapat disesuaikan dengan struktur jam di sekolah.
Model pembelajaran	Pembelajaran berbasis masalah dan simulasi, dengan kerja berpasangan dan kelompok
Media utama	SiberLab, aplikasi simulasi yang berjalan di peramban tanpa koneksi ke jaringan nyata
Pendekatan	Kurikulum Merdeka dengan Pembelajaran Mendalam: berkesadaran, bermakna, dan menggembirakan

B. Piagam Ruang Aman

Sebelum menyentuh simulasi, kelas menyepakati piagam sederhana. Guru mengajak murid merumuskannya dengan kata-kata sendiri, kemudian menempelkannya di tempat yang mudah terlihat.

Kesepakatan	Wujud di kelas
Boleh salah	Kekeliruan di dalam simulasi tidak merusak apa pun dan tidak dijadikan bahan ejekan. Pertanyaan yang dianggap sepele tetap disambut baik.
Boleh mengulang	Setiap lab dan simulasi dapat diatur ulang. Murid dianjurkan mengulang dengan strategi yang berbeda.
Kesalahan dicatat sebagai pelajaran	Setiap murid memiliki Jurnal Anak Tangga untuk mencatat kekeliruan, penyebabnya, dan langkah perbaikan.
Saling menghargai	Murid membantu teman dengan bertanya, bukan langsung memberi jawaban atau menertawakan.
Etika dan izin	Keterampilan ini hanya dipraktikkan di lab simulasi, mesin virtual milik sendiri, atau sistem yang memberi izin tertulis.

C. Komponen Inti Modul

C.1 Capaian dan fokus kompetensi

Rumusan capaian pembelajaran mengikuti dokumen capaian pembelajaran mata pelajaran yang berlaku di satuan pendidikan. Modul ini berfokus pada kemampuan memahami, mengonfigurasi secara sederhana, menguji, dan mendokumentasikan pengamanan jaringan serta merespons insiden dengan prosedur dan etika. Guru dipersilakan memetakan tujuan di bawah ini ke rumusan capaian dan tujuan pembelajaran yang digunakan sekolah.

C.2 Tujuan pembelajaran

Setelah mengikuti rangkaian pembelajaran, murid diharapkan mampu:

1. menjelaskan peran alamat IP, port, dan paket, serta alasan pentingnya keamanan jaringan;
2. menyusun dan menguji aturan firewall pada rantai INPUT dengan memperhatikan urutan aturan dan policy default;
3. menjelaskan cara kerja VPN dan membandingkan lalu lintas sebelum dan sesudah terowongan terbentuk;
4. menerapkan langkah hardening dasar pada server dan memverifikasi dampaknya melalui log;
5. mengenali pola ancaman umum dan membaca log untuk menemukan bukti;
6. menerapkan tahapan penanganan insiden secara berurutan serta menyusun laporan insiden;
7. menerapkan etika, izin, dan kehati-hatian dalam mempelajari keamanan jaringan;
8. merefleksikan kesalahan menjadi strategi perbaikan yang konkret.

C.3 Dimensi profil lulusan yang dikuatkan

Dimensi	Wujud dalam pembelajaran
Penalaran kritis	Menilai bukti pada log, memprediksi hasil aturan firewall, dan memilih tindakan insiden yang paling beralasan.
Kemandirian	Membaca materi dan mencoba lab sesuai kecepatan sendiri, mengulang tanpa menunggu perintah.
Kolaborasi	Bekerja berpasangan dan berkelompok pada simulasi insiden dan penyusunan laporan.
Komunikasi	Menjelaskan temuan, menulis laporan, dan mempresentasikan hasil dengan bahasa yang jelas.
Kewargaan	Mematuhi etika, hukum, dan menjaga data pribadi serta kerahasiaan kunci dan kata sandi.
Keimanan dan ketakwaan	Kejujuran, amanah, dan tanggung jawab dalam menggunakan ilmu yang berpotensi disalahgunakan.

Dimensi lain, seperti kreativitas, dapat tumbuh pada saat murid merancang strategi perbaikan, dan kesehatan pada saat guru menjaga suasana belajar yang tenang. Pemilihan dimensi dapat disesuaikan dengan kebutuhan kelas.

C.4 Pemahaman bermakna dan pertanyaan pemantik

- **Pemahaman bermakna:** keamanan bukan produk yang dipasang sekali, melainkan kebiasaan yang dipelihara. Teknisi yang baik bukan yang tidak pernah keliru, melainkan yang tenang, teliti, dan mau memperbaiki.
- Mengapa banyak pembobolan terjadi bukan karena sistem canggih ditembus, tetapi karena kata sandi lemah atau orang dibujuk?
- Apa yang membedakan teknisi yang panik dengan teknisi yang bekerja dengan prosedur?
- Bagaimana kesalahan yang dibuat di simulasi dapat mencegah kerugian di sistem yang sesungguhnya?

C.5 Kompetensi awal dan diferensiasi

Murid diasumsikan telah mengenal konsep dasar jaringan komputer. Karena SiberLab memuat materi Fase E dan Fase F, guru dapat membagi jalur belajar secara luwes. Jalur bukan label permanen, dan murid boleh berpindah jalur kapan saja.

Jalur	Sasaran	Materi dan tantangan
Fondasi (Fase E)	Murid yang masih membangun konsep dasar	Dasar jaringan, firewall, VPN, ancaman nyata, serta kata sandi dan MFA. Lab dikerjakan dengan petunjuk “Mulai dari sini” yang ada di aplikasi.
Penguatan (Fase F)	Murid yang siap konfigurasi dan analisis	Hardening, membaca log, etika dan laporan, respons insiden, serta backup dan pemulihan. Tantangan akhir Fase F dan penulisan laporan remediasi.
Pengayaan	Murid yang sudah cepat menguasai	Menjadi pendamping sebaya, membuat variasi skenario, atau menelaah rujukan resmi seperti CIS Benchmarks dan NIST SP 800-61.

C.6 Sarana dan prasarana

- Satu perangkat per murid atau per pasangan, dengan peramban modern. Berkas SiberLab dapat dijalankan secara luring.
- Proyektor atau layar untuk demonstrasi singkat.
- Kertas atau berkas Jurnal Anak Tangga dan lembar kerja pada lampiran.
- Papan atau tempelan untuk Piagam Ruang Aman.

C.7 Pembelajaran Mendalam dalam modul ini

Pengalaman belajar	Yang dilakukan murid	Wujud ruang aman
Memahami	Membaca materi singkat, berdiskusi, dan menjelaskan ulang dengan kata sendiri	Tidak ada pertanyaan yang salah untuk diajukan
Mengaplikasi	Mencoba lab, memprediksi hasil, sengaja menguji kekeliruan, lalu memperbaikinya	Reset dan ulang tanpa konsekuensi
Merefleksi	Mengisi Jurnal Anak Tangga dan membagikan pelajaran terbaik	Kekeliruan dibahas sebagai bahan belajar bersama

Kerangka pembelajaran	Penerapan
Praktik pedagogis	Prediksi, uji, dan jelaskan; kerja berpasangan dan kelompok; umpan balik langsung.
Kemitraan pembelajaran	Guru sebagai pendamping, teman sebaya, dan bila memungkinkan pengelola jaringan sekolah atau praktisi sebagai narasumber.
Lingkungan pembelajaran	Piagam Ruang Aman dan suasana yang menghargai percobaan.
Pemanfaatan digital	SiberLab sebagai laboratorium simulasi yang aman dan dapat diulang.

D. Rancangan Kegiatan Pembelajaran

Susunan empat pertemuan berikut mengikuti usulan pada FAQ aplikasi. Waktu pada tabel adalah contoh untuk 4 jam pelajaran per pertemuan dan dapat disesuaikan.

Pertemuan	Fokus	Produk belajar
1	Dasar jaringan dan firewall	Aturan firewall yang diuji dan Jurnal Anak Tangga 1
2	VPN	Tabel perbandingan lalu lintas dan Jurnal Anak Tangga 2
3	Hardening, ancaman, log, serta kata sandi dan MFA	Skor hardening, catatan bukti log, dan Jurnal Anak Tangga 3
4	Respons insiden, remediasi, dan backup	Laporan insiden kelompok, tiga temuan remediasi, dan Jurnal Anak Tangga 4

Pertemuan 1: Dasar Jaringan dan Firewall

Fokus	Memahami IP, port, dan paket, serta menyusun dan menguji aturan firewall
Materi SiberLab	Dasar jaringan: IP, port, dan paket; Firewall dan rantai filter; Etika, hukum, dan laporan (pengantar)
Laboratorium	Tab Firewall: Terapkan baseline aman, Uji paket, Skenario lalu lintas, Reset

Tujuan pertemuan

- Menjelaskan arti alamat IP, port, dan paket.
- Menjelaskan bahwa aturan firewall dicocokkan dari atas ke bawah dan aturan pertama yang cocok yang berlaku.
- Menyusun serta menguji aturan, lalu memperbaiki aturan yang keliru.

Pertanyaan pemantik

- Mengapa urutan aturan dapat menentukan nasib sebuah paket?
- Apa yang terjadi bila tidak ada satu pun aturan yang cocok?

Tahap	Kegiatan	Menit
Pendahuluan	Salam dan pembiasaan sesuai kebiasaan sekolah. Kelas menyepakati Piagam Ruang Aman. Guru mengajukan pertanyaan pemantik dan mengajak murid menebak jawabannya tanpa takut keliru.	15
Memahami	Murid membaca materi dasar jaringan dan firewall, lalu berpasangan menjelaskan ulang konsepnya dengan kata sendiri. Guru menegaskan peran policy default.	30
Mengaplikasi	1) Tekan Terapkan baseline aman dan amati daftar aturan. 2) Prediksi, uji, jelaskan: tulis dugaan nasib sebuah paket, lalu kirim paket uji dan bandingkan. 3) **Anak Tangga 1:** sengaja menyusun satu aturan yang keliru, misalnya aturan penolakan yang menutupi aturan yang seharusnya mengizinkan, amati akibatnya, lalu perbaiki. 4) Coba skenario brute-force SSH dan temukan aturan yang menangkapnya. 5) Tekan Reset dan ulangi dengan strategi yang lebih baik.	90
Merefleksi	Murid mengisi Jurnal Anak Tangga 1: satu kekeliruan, penyebabnya, dan langkah perbaikan. Beberapa murid sukarela berbagi.	25
Penutup	Guru merangkum, menegaskan etika (tidak memindai tanpa izin), dan murid dapat mencoba kuis topik Dasar dan Firewall sebagai umpan balik.	20

Asesmen pada pertemuan ini

- Observasi proses dan diskusi (formatif).
- Jurnal Anak Tangga 1 (formatif).
- Kuis mini topik Dasar dan Firewall sebagai umpan balik, boleh diulang.

> **Catatan ruang aman**
>
> Murid yang aturannya keliru justru diberi apresiasi karena menemukan perilaku firewall yang penting. Guru bertanya, “Apa yang kamu pelajari dari hasil ini?”, bukan “Mengapa salah?”.

Pertemuan 2: VPN: Terowongan Terenkripsi

Fokus	Memahami cara kerja VPN, enkripsi lalu lintas, kill switch, dan kebocoran DNS
Materi SiberLab	VPN: terowongan terenkripsi, serta bagian tentang kapan VPN dipakai
Laboratorium	Tab VPN: Hubungkan, panel tcpdump, Kill switch, opsi DNS, Buat ulang kunci

Tujuan pertemuan

- Menjelaskan fungsi VPN dan perbedaan lalu lintas sebelum dan sesudah terowongan terbentuk.
- Menjelaskan fungsi kill switch dan akibat kebocoran DNS.
- Membandingkan dua protokol, WireGuard dan OpenVPN, pada tingkat konfigurasi dasar.

Pertanyaan pemantik

- Apa yang dapat dilihat penyadap di Wi-Fi publik sebelum dan sesudah VPN aktif?
- Bagaimana VPN yang aktif tetap dapat membocorkan informasi?

Tahap	Kegiatan	Menit
Pendahuluan	Guru mengaitkan dengan pengalaman murid memakai Wi-Fi publik dan bertanya apa yang mungkin dilihat orang lain. Piagam Ruang Aman dibacakan kembali.	15
Memahami	Murid membaca materi VPN dan kapan VPN dipakai (akses jarak jauh dan antarcabang), lalu berdiskusi berpasangan.	30
Mengaplikasi	1) Tekan Hubungkan dan amati langkah handshake serta status. 2) Bandingkan panel tcpdump saat terputus dan tersambung, lalu catat perbedaannya. 3) **Anak Tangga 2:** putuskan VPN dengan dan tanpa Kill switch, amati lalu lintas. 4) Matikan opsi DNS lewat terowongan, amati kebocoran, lalu perbaiki. 5) Pilih WireGuard atau OpenVPN, bandingkan konfigurasinya, dan coba Buat ulang kunci.	90
Merefleksi	Jurnal Anak Tangga 2. Murid menuliskan satu hal yang semula dikira aman tetapi ternyata tidak.	25
Penutup	Guru menegaskan bahwa kunci dan alamat di aplikasi hanyalah contoh, dan kunci pribadi asli tidak pernah dibagikan. Kuis topik VPN sebagai umpan balik.	20

Asesmen pada pertemuan ini

- Tabel perbandingan lalu lintas (produk, formatif).
- Jurnal Anak Tangga 2 (formatif).
- Kuis topik VPN sebagai umpan balik.

> **Catatan ruang aman**
> Eksperimen memutus VPN dilakukan dengan sengaja agar murid melihat akibatnya di lingkungan yang tidak berisiko. Guru menekankan bahwa temuan seperti kebocoran DNS adalah penemuan yang berharga.

Pertemuan 3: Hardening, Ancaman, Log, serta Kata Sandi dan MFA

Fokus	Mengamankan server dengan langkah bertahap, mengenali ancaman nyata, dan membaca log
Materi SiberLab	Hardening server; Ancaman nyata yang paling sering terjadi; Membaca log seperti detektif; Kata sandi, MFA, dan faktor manusia
Laboratorium	Tab Hardening: Jalankan audit, Terapkan semua, Reset server, auth.log; Tab Simulasi insiden: Berburu di log

Tujuan pertemuan

- Menerapkan langkah hardening dan menjelaskan risiko yang ditutup oleh tiap langkah.
- Membaca baris log dan membedakan kegagalan login, login berhasil, dan pola mencurigakan.
- Menjelaskan peran kata sandi panjang dan MFA, serta bahaya rekayasa sosial.

Pertanyaan pemantik

- Mengapa satu login berhasil setelah ribuan kegagalan lebih mendesak daripada ribuan kegagalan itu sendiri?
- Mengapa kode OTP tidak boleh diberikan kepada siapa pun?

Tahap	Kegiatan	Menit
Pendahuluan	Guru menampilkan satu baris log dan mengajak murid menebak artinya. Murid menyebutkan pengalaman mendengar kata sandi atau akun yang diretas, tanpa menyebut nama orang.	15
Memahami	Pembelajaran jigsaw: tiap kelompok ahli mendalami satu materi (hardening, ancaman, log, kata sandi dan MFA), lalu mengajarkannya kepada kelompok lain. Bila memungkinkan, materi dibaca sebelum pertemuan.	30
Mengaplikasi	1) Jalankan audit dan catat skor awal. 2) Terapkan langkah satu per satu sambil mengamati auth.log, dan baca risiko yang ditutup. 3) **Anak Tangga 3:** pada percobaan pertama murid bebas memilih urutan, lalu Reset server dan mencoba urutan lain untuk melihat dampaknya. 4) Targetkan skor 90 ke atas. 5) Pada tab Simulasi insiden, kerjakan Berburu di log: tandai baris yang menjadi bukti penyerang berhasil masuk dan periksa hasilnya.	90
Merefleksi	Jurnal Anak Tangga 3: tanda log mana yang sempat terlewat dan bagaimana mengenalinya lain kali.	25
Penutup	Guru merangkum pola log yang mencurigakan dan pentingnya MFA. Kuis topik Hardening sebagai umpan balik.	20

Asesmen pada pertemuan ini

- Skor hardening dan catatan bukti log (produk, formatif).
- Jurnal Anak Tangga 3 (formatif).
- Diskusi kelompok ahli dan penjelasan antarmurid (observasi).

> **Catatan ruang aman**
> Berburu di log memuat banyak baris yang tampak mencurigakan. Salah menandai baris adalah bagian dari belajar, dan guru membahasnya sebagai latihan ketelitian, bukan kegagalan.

Pertemuan 4: Respons Insiden, Remediasi, dan Backup

Fokus	Menangani insiden dengan prosedur, menyusun laporan, dan menjaga pemulihan data
Materi SiberLab	Merespons insiden: dari panik menjadi prosedur; Backup 3-2-1 dan pemulihan; Remediasi: dari temuan menjadi perbaikan
Laboratorium	Tab Simulasi insiden (tiga skenario), tab Remediasi, dan tab Kuis

Tujuan pertemuan

- Menerapkan tahapan penanganan insiden secara berurutan dan terdokumentasi.
- Menjelaskan aturan 3-2-1 beserta alasan pentingnya menguji pemulihan.
- Menyusun laporan insiden berisi kronologi, akar masalah, dan pencegahan, serta tiga temuan remediasi.

Pertanyaan pemantik

- Mengapa server yang diretas sebaiknya diisolasi dulu, bukan langsung dimatikan paksa?
- Mengapa backup yang belum pernah dipulihkan belum bisa disebut backup?

Tahap	Kegiatan	Menit
Pendahuluan	Guru memaparkan situasi: situs nilai sekolah mendadak lambat. Murid menyebutkan apa yang akan mereka lakukan lebih dahulu.	15
Memahami	Murid membaca tahapan penanganan insiden, aturan emas (catat waktu, jangan hapus bukti, isolasi dulu, beri tahu orang yang tepat), dan aturan 3-2-1.	30
Mengaplikasi	Kelompok 3 sampai 4 murid memilih skenario (brute-force SSH, ransomware di PC TU, atau phishing akun guru) dan mengambil keputusan tahap demi tahap. 1) Diskusikan setiap pilihan sebelum mengklik. 2) **Anak Tangga 4:** bila hasil kurang tepat, baca penjelasannya dan ulangi skenario. 3) Pada tab Remediasi pilih tiga temuan dan tulis risiko, perbaikan, serta bukti verifikasi. 4) Susun laporan insiden kelompok memakai contoh laporan yang muncul di akhir simulasi sebagai pola.	90
Merefleksi	Pameran singkat: tiap kelompok mempresentasikan satu keputusan yang awalnya keliru dan pelajaran yang diambil. Jurnal Anak Tangga 4.	25
Penutup	Kuis pemahaman berbasis skenario. Hasil menunjukkan tingkat penguasaan dan topik yang perlu diulang. Guru menutup dengan apresiasi proses dan kutipan inspiratif.	20

Asesmen pada pertemuan ini

- Laporan insiden kelompok (produk, dinilai dengan rubrik).
- Tiga temuan remediasi (produk).
- Kuis pemahaman sebagai umpan balik dan bahan perencanaan pengulangan.
- Jurnal Anak Tangga 4 dan observasi kolaborasi.

> **Catatan ruang aman**
>
> Kelompok yang memilih langkah kurang tepat dan mengulangnya justru memahami akibatnya lebih dalam. Guru menghargai keberanian mengakui “kami keliru di sini” dan menjadikannya contoh bagi kelas. Bila waktu tidak cukup, penyusunan laporan dapat dilanjutkan sebagai tugas terbimbing.

E. Asesmen

Asesmen dirancang untuk menumbuhkan. Hasil percobaan pertama tidak dijadikan satu-satunya dasar penilaian, dan perbaikan yang disertai alasan dipandang sebagai bukti kompetensi.

Jenis	Bentuk	Keterangan
Diagnostik	Pertanyaan pemantik dan percobaan awal di lab	Memetakan pemahaman awal untuk menentukan jalur belajar
Formatif	Observasi, Jurnal Anak Tangga, umpan balik langsung dari simulasi, kuis mini	Tidak mengurangi nilai; kuis boleh diulang
Sumatif	Tantangan akhir Fase F: skor hardening yang ditargetkan, bukti serangan terblokir pada log, tiga temuan remediasi, dan laporan insiden	Dinilai dengan rubrik pada lampiran
Refleksi diri	Catatan tentang kesalahan yang paling bermakna	Menguatkan kemandirian dan kesadaran belajar

Bobot dan cara pengolahan nilai akhir ditetapkan oleh guru dan satuan pendidikan sesuai ketentuan penilaian yang berlaku.

F. Pengayaan dan Remedial

Kebutuhan	Tindak lanjut
Pengayaan	Menjadi pendamping sebaya; menyusun skenario insiden versi sendiri berdasarkan pola log; membandingkan konfigurasi dengan rujukan resmi seperti CIS Benchmarks; menulis laporan remediasi tambahan.
Remedial	Mengulang lab dengan petunjuk “Mulai dari sini”; belajar berpasangan dengan teman sebaya; mengerjakan ulang kuis pada topik yang ditunjukkan hasilnya; sesi tanya jawab singkat dengan guru.
Murid yang pemalu atau cemas keliru	Memulai dari pasangan kecil, memberi pilihan berbagi secara tertulis, dan menegaskan bahwa Jurnal Anak Tangga bersifat pribadi kecuali murid memilih membagikannya.

G. Etika, Hukum, dan Keselamatan

- Seluruh praktik dilakukan di lab simulasi, mesin virtual milik sendiri, atau sistem dengan izin tertulis pengelola.
- Jaringan sekolah dan milik orang lain tidak dipindai atau diuji tanpa izin, walaupun tanpa niat merusak.
- Bila menemukan celah, laporkan kepada pengelola dan jangan dieksploitasi.
- Kunci, alamat, dan data di SiberLab hanyalah contoh. Kunci pribadi asli tidak pernah dibagikan.
- Perintah di SiberLab disederhanakan. Sebelum dipakai di sistem sungguhan, cocokkan dengan dokumentasi resmi dan uji di lingkungan lab atau mesin virtual.

Aplikasi memuat rujukan terkait UU ITE dan UU Pelindungan Data Pribadi sebagai bahan diskusi. Penyusun bukan ahli hukum, sehingga guru dianjurkan merujuk pada teks peraturan yang berlaku dan berkonsultasi dengan pihak yang berwenang bila diperlukan.

H. Refleksi Guru

Setelah pembelajaran, guru dapat menjawab pertanyaan berikut secara jujur dan tanpa tergesa:

- Pada saat mana murid tampak paling berani mencoba, dan apa yang membuatnya demikian?
- Murid mana yang masih ragu keliru, dan dukungan apa yang dapat saya berikan?
- Bagian modul mana yang perlu saya sederhanakan atau perdalam?
- Apa yang saya pelajari dari kekeliruan saya sendiri selama mengajar modul ini?

Lampiran

Lampiran 1. Jurnal Anak Tangga

Satu lembar untuk setiap pertemuan. Isian bersifat pribadi dan tidak dinilai benar atau salah. Yang dihargai adalah kejujuran dan kemauan memperbaiki.

Pertemuan dan topik	
Kekeliruan yang kutemukan	
Penyebabnya, menurutku	
Bukti atau pengamatan yang membuatku sadar	
Langkah perbaikan yang akan kucoba	
Satu hal yang kupelajari dan ingin kubagikan	

Lampiran 2. Lembar Kerja Murid Ringkas

Pertemuan	Tugas inti	Bukti yang dikumpulkan
1	Susun dan uji aturan firewall; tangkap satu aturan yang keliru lalu perbaiki	Salinan daftar aturan sebelum dan sesudah perbaikan, serta prediksi dan hasil uji paket
2	Bandingkan lalu lintas saat VPN terputus dan tersambung; uji kill switch dan DNS	Tabel perbandingan dan penjelasan singkat tiap perbedaan
3	Capai skor hardening yang ditargetkan; telusuri bukti pada log	Skor awal dan akhir, daftar langkah, serta baris log yang menjadi bukti
4	Selesaikan satu skenario insiden; tulis tiga temuan remediasi	Laporan insiden dan tiga temuan dengan risiko, perbaikan, dan bukti verifikasi

Lampiran 3. Format Laporan Insiden

Sistem yang terdampak	
Deteksi (gejala dan waktu relatif)	
Ringkasan kejadian	
Kronologi tindakan	
Akar masalah	
Pembatasan, pemberantasan, dan pemulihan	
Pencegahan dan tindak lanjut	
Bukti pendukung	

Tulis waktu secara relatif atau sesuai catatan simulasi. Contoh laporan yang muncul pada akhir simulasi dapat dijadikan pola.

Lampiran 4. Rubrik

Rubrik 1. Proses belajar dan perbaikan (Jurnal Anak Tangga)

Aspek	Baru memulai	Berkembang	Cakap	Mahir
Mengakui kekeliruan	Belum mencatat kekeliruan	Mencatat tetapi masih umum	Mencatat dengan jelas	Mencatat dengan jelas dan jujur
Menemukan penyebab	Belum mengaitkan penyebab	Penyebab dugaan saja	Penyebab didukung pengamatan	Penyebab didukung bukti dan alternatif
Merencanakan perbaikan	Belum ada rencana	Rencana umum	Rencana konkret	Rencana konkret dan sudah dicoba
Berbagi pelajaran	Belum berbagi	Berbagi bila ditanya	Berbagi atas inisiatif	Membantu teman belajar dari pengalamannya

Rubrik 2. Laporan insiden

Aspek	Baru memulai	Berkembang	Cakap	Mahir
Kronologi	Urutan belum jelas	Urutan sebagian jelas	Urutan jelas dan lengkap	Urutan jelas, lengkap, dan bertanda waktu
Akar masalah	Belum teridentifikasi	Menyebut gejala	Menyebut penyebab utama	Menyebut penyebab utama dan faktor pendukung
Penanganan	Tidak mengikuti tahapan	Sebagian tahapan	Mengikuti tahapan berurutan	Berurutan dengan alasan tiap keputusan
Pencegahan	Belum ada	Umum	Spesifik dan relevan	Spesifik, relevan, dan dapat diverifikasi
Bukti dan bahasa	Tanpa bukti	Bukti terbatas	Bukti memadai, bahasa jelas	Bukti kuat, bahasa ringkas dan profesional

Rubrik 3. Kolaborasi dan etika (observasi guru)

Indikator	Belum tampak	Mulai tampak	Konsisten
Menghargai pendapat dan percobaan teman			
Berbagi tugas secara adil			
Menjaga kerahasiaan kunci dan data contoh			
Menyatakan izin sebelum menguji sistem			
Membantu teman tanpa menertawakan kekeliruan			

Lampiran 5. Glosarium Singkat

Istilah	Arti singkat
Firewall	Penyaring lalu lintas jaringan berdasarkan aturan
Policy default	Tindakan yang berlaku bila tidak ada aturan yang cocok
VPN	Terowongan terenkripsi antara perangkat dan jaringan tujuan
Kill switch	Pemblokiran lalu lintas bila VPN terputus mendadak
DNS leak	Pertanyaan DNS yang keluar dari terowongan dan terlihat pihak lain
Hardening	Pengetatan konfigurasi agar permukaan serangan berkurang
Brute-force	Penebakan kata sandi berulang oleh mesin
MFA	Verifikasi berlapis dengan faktor tambahan selain kata sandi
Remediasi	Proses menutup celah: identifikasi, prioritas, perbaikan, verifikasi, dokumentasi
Backup 3-2-1	Tiga salinan, dua jenis media, satu salinan di luar lokasi atau offline

Lampiran 6. Rujukan

- CIS Benchmarks: standar konfigurasi aman untuk server dan sistem operasi.
- NIST SP 800-61: panduan penanganan insiden keamanan komputer.
- OWASP Top 10: risiko keamanan aplikasi web yang paling umum.
- Dokumentasi netfilter/iptables dan WireGuard.
- RFC 5737: rentang alamat IP contoh yang dipakai pada simulasi.
- UU ITE dan UU Pelindungan Data Pribadi (rujuk teks resmi yang berlaku).

// KREDIT PENGEMBANG

SiberLab

Laboratorium Simulasi Keamanan Teknis

PENGEMBANG DAN PENYUSUN

Aliyudin

Guru Mata Pelajaran Produktif TKJ

SMK Ciledug Al Musaddadiyah

Modul ini disusun mendampingi SiberLab, media belajar keamanan jaringan untuk Fase E dan Fase F program keahlian TKJ. Seluruh simulasi berjalan di perangkat pengguna tanpa koneksi ke jaringan nyata.

// KUTIPAN INSPIRATIF

> **“Ing ngarsa sung tuladha, ing madya mangun karsa, tut wuri handayani.”**
>
> Ki Hajar Dewantara
>
> *Di depan memberi teladan, di tengah membangun semangat, di belakang memberi dorongan.*

> **“Kesalahan adalah anak tangga terbaik untuk mendapatkan ilmu.”**
>
> Pegangan yang melandasi lahirnya SiberLab

> **“Belajarlah dengan berani keliru, karena dari situlah pemahaman yang kokoh dibangun.”**
>
> Pesan penutup untuk setiap murid dan pendidik

Terima kasih telah berkenan menggunakan modul ini. Masukan Anda sangat berharga.