

NASKAH INOVASI PEMBELAJARAN

SecOps Lab

Simulator Interaktif Keamanan Siber

Berbasis Peramban untuk Pembelajaran Linux Hardening dan WireGuard VPN dalam Kerangka Pembelajaran Mendalam

LINUX HARDENING | WIREGUARD VPN | PEMBELAJARAN MENDALAM

DISUSUN OLEH

Aliyudin

Guru Mata Pelajaran Produktif TKJ
SMKS Ciledug Al Musaddadiyah
Garut, 2026

KATEGORI
Inovasi Pembelajaran Digital

STATUS
Pendidikan Vokasi dan Informatika

EDISI
2026 // v1.2

SIMULASI EDUKASI // AMAN // ETIS // LEGAL

KATA PENGANTAR

Kata Pengantar

Puji syukur penyusun panjatkan ke hadirat Tuhan Yang Maha Esa atas terselesaikannya naskah inovasi pembelajaran berjudul **SecOps Lab: Simulator Interaktif Keamanan Siber Berbasis Peramban untuk Pembelajaran Linux Hardening dan WireGuard VPN dalam Kerangka Pembelajaran Mendalam**.

Naskah ini berangkat dari pengalaman mengampu mata pelajaran produktif Teknik Komputer dan Jaringan (TKJ), tempat peserta didik sering kesulitan mempraktikkan keamanan sistem secara aman, mandiri, dan bermakna karena keterbatasan perangkat serta risiko kesalahan pada sistem nyata. SecOps Lab dirancang sebagai ruang berlatih yang aman untuk gagal, sekaligus sebagai media yang selaras dengan pendekatan Pembelajaran Mendalam dan Kurikulum Merdeka.

Penyusun menyadari bahwa naskah ini masih berupa rancangan yang perlu diuji, divalidasi, dan disempurnakan. Seluruh target capaian dalam naskah ini merupakan usulan yang akan dikalibrasi melalui uji coba. Karena itu, kritik dan saran dari rekan guru, praktisi keamanan siber, dan para pemangku kepentingan pendidikan sangat penyusun harapkan.

Semoga naskah ini bermanfaat bagi peningkatan mutu pembelajaran keamanan siber di satuan pendidikan, khususnya pendidikan vokasi.

Garut, 2026
Penyusun,

Aliyudin

RINGKASAN

Ringkasan Eksekutif

Keamanan siber telah bergeser dari kompetensi segelintir spesialis menjadi bagian dari literasi digital dasar. Badan Siber dan Sandi Negara (BSSN) mencatat sekitar 5,2 miliar anomali trafik internet di Indonesia sepanjang 2025, setara kurang lebih 182 potensi serangan setiap detik. Pada saat yang sama, pembelajaran praktik keamanan sistem di satuan pendidikan menghadapi sebuah paradoks: peserta didik baru benar-benar memahami ketika mengubah konfigurasi sistem yang sesungguhnya, padahal di situlah risiko kesalahan, kebutuhan perangkat, dan kesenjangan infrastruktur paling besar.

SecOps Lab adalah inovasi pembelajaran yang menjawab paradoks tersebut. Inovasi ini berupa simulator interaktif berbasis peramban (*browser*) yang berjalan dari satu berkas, tanpa instalasi, tanpa *server*, dan tanpa terhubung ke sistem nyata. Peserta didik bertugas mengamankan sebuah *server* Linux virtual yang sengaja dibuat rentan melalui sebelas kontrol *hardening* dan satu terowongan VPN WireGuard, sambil menghadapi serangan simulasi secara waktu-nyata. Alur belajarnya berjenjang: Pahami, Pelajari, Praktikkan, Uji, Perbaiki. Alur ini didukung sembilan misi terpandu, terminal simulasi, dasbor monitor keamanan, bank soal kompetensi, remediasi berbasis risiko, laporan audit, hingga sertifikat penyelesaian.

Secara pedagogis, SecOps Lab selaras dengan pendekatan Pembelajaran Mendalam (*mindful, meaningful, joyful*) dan prinsip Kurikulum Merdeka: belajar berpusat pada peserta didik, kontekstual, berdiferensiasi, dan menilai kinerja, bukan sekadar hafalan. Naskah ini menguraikan latar belakang, landasan teori dan kebijakan, rancangan produk, model implementasi, rencana evaluasi, mitigasi risiko, serta peta jalan pengembangan. Seluruh target yang dicantumkan merupakan rancangan yang perlu dikalibrasi melalui uji coba; naskah ini tidak mengklaim hasil empiris yang belum diperoleh.

> **GAGASAN INTI**
> Biarkan peserta didik gagal dengan aman, melihat dampak setiap keputusan seketika, dan memahami *mengapa* sebuah kontrol keamanan ada, bukan hanya perintah apa yang diketik.

Kata kunci: keamanan siber, *hardening* Linux, WireGuard, simulator, pembelajaran mendalam, pendidikan vokasi, Kurikulum Merdeka.

ABSTRACT

Abstract

Cybersecurity has become part of basic digital literacy, yet hands-on teaching of system security in schools is constrained by the risk of misconfiguration, limited hardware, and the difficulty of giving individual feedback. This manuscript presents **SecOps Lab**, a single-file, *browser*-based interactive simulator for learning Linux hardening and WireGuard VPN. Learners act as administrators of a deliberately vulnerable virtual *server* under simulated attack, apply eleven hardening controls and one VPN tunnel, and observe the effect of every decision through a security score, event logs, and an open-*port* table. The learning flow follows five stages (understand, study, practise, test, improve) supported by nine guided missions, a simulated terminal, a question bank, risk-based remediation, an audit report, and a completion certificate. The design is aligned with the Indonesian *Deep Learning* pedagogical approach (mindful, meaningful, joyful) and the Merdeka Curriculum. All targets stated are design proposals to be calibrated through trials; no empirical results are claimed.

Keywords: cybersecurity, Linux hardening, WireGuard, simulator, deep learning approach, vocational education.

DAFTAR ISI

Daftar Isi

Kata Pengantar i

Ringkasan Eksekutif ii

Abstract iii

Daftar Tabel vi

Daftar Gambar vi

BAB I Pendahuluan 1

A. Latar Belakang 1

B. Identifikasi Masalah 1

C. Rumusan Masalah 2

D. Tujuan 2

E. Manfaat 2

F. Kebaruan dan Keunggulan 3

G. Sistematika Penulisan 3

BAB II Kajian Teoretis dan Landasan Kebijakan 4

A. Pembelajaran Mendalam dan Kurikulum Merdeka 4

B. Landasan Teori Belajar 4

C. Landasan Keamanan Informasi 5

D. Keterkaitan dengan Profil Lulusan dan Capaian Pembelajaran 6

BAB III Deskripsi Inovasi SecOps Lab 7

A. Gambaran Umum Produk 7

B. Arsitektur Pembelajaran: Tiga Tahap, Sembilan Modul 7

C. Skenario Simulasi: Server yang Sengaja Dibuat Rentan 8

D. Kontrol Hardening dan Sistem Skor 9

E. Sembilan Misi Pembelajaran 10

F. Fitur Pendukung Pembelajaran 11

G. Prinsip Desain dan Kejujuran terhadap Batas Simulasi 11

BAB IV Model Implementasi Pembelajaran 13

A. Sintaks Pembelajaran: Pahami, Pelajari, Praktikkan, Uji, Perbaiki 13

B. Contoh Rancangan Pembelajaran Tiga Pertemuan 13

C. Peran Guru sebagai Fasilitator 13

D. Diferensiasi dan Kolaborasi 14

E. Asesmen yang Selaras 14

F. Adaptasi pada Beragam Konteks Pendidikan Indonesia 14

BAB V Rancangan Evaluasi, Etika, dan Mitigasi Risiko 16

A. Rancangan Evaluasi Efektivitas 16

B. Etika dan Kerangka Hukum 16

C. Analisis Risiko dan Mitigasi 17

D. Keterbatasan 17

BAB VI Keberlanjutan dan Peta Jalan Pengembangan 18

A. Faktor Keberlanjutan 18

B. Peta Jalan 18

C. Kebutuhan Dukungan 18

BAB VII Penutup 19

A. Kesimpulan 19

B. Rekomendasi 19

Daftar Pustaka 21

Lampiran A Rubrik Penilaian Unjuk Kerja 22

Lampiran B Kisi-kisi Bank Soal Kuis 22

DAFTAR TABEL

Daftar Tabel

Tabel 1. Identifikasi masalah pembelajaran praktik keamanan sistem . . . 1
Tabel 2. Manfaat inovasi bagi para pemangku kepentingan . . . 2
Tabel 3. Perbandingan pendekatan konvensional dan SecOps Lab . . . 3
Tabel 4. Keselarasan prinsip Pembelajaran Mendalam dengan fitur SecOps Lab . . . 4
Tabel 5. Pemetaan jenjang kognitif terhadap aktivitas pada SecOps Lab . . . 5
Tabel 6. Spesifikasi ringkas SecOps Lab . . . 7
Tabel 7. Struktur modul SecOps Lab . . . 7
Tabel 8. Dampak kontrol terhadap perilaku simulasi . . . 8
Tabel 9. Sebelas kontrol hardening dan terowongan VPN . . . 9
Tabel 10. Sembilan misi dan fokus kompetensinya . . . 10
Tabel 11. Contoh rancangan tiga pertemuan (usulan, dapat disesuaikan) . . . 13
Tabel 12. Rancangan asesmen . . . 14
Tabel 13. Indikator, instrumen, dan target rancangan . . . 16
Tabel 14. Risiko penerapan dan strategi mitigasi . . . 17
Tabel 15. Rencana pengembangan dan diseminasi (rencana, bukan capaian) . . . 18
Tabel 16. Rekomendasi bagi para pemangku kepentingan . . . 19
Tabel 17. Rubrik unjuk kerja hardening dan VPN . . . 22
Tabel 18. Kisi-kisi bank soal . . . 22

DAFTAR GAMBAR

Daftar Gambar

Gambar 1. Alur belajar lima tahap pada SecOps Lab . . . 8
Gambar 2. Kontribusi tiap kontrol terhadap skor keamanan (total 100 poin), diberi warna menurut tingkat risiko . . . 10
Gambar 3. Pemetaan kontrol ke dalam lapisan pertahanan (defense in depth) . . . 11

BAB I

Pendahuluan

A. Latar Belakang

Transformasi digital Indonesia berlangsung cepat, dan ancaman di ruang siber tumbuh seirama dengannya. BSSN melaporkan sekitar 5,2 miliar anomali trafik internet sepanjang 2025, dengan sekitar 93,78 persen di antaranya berkaitan dengan aktivitas berbasis *malware*, serta menyebut sektor keuangan, energi, telekomunikasi, dan pemerintahan sebagai sasaran utama (Antara, 2026; Warta Ekonomi, 2026). BSSN sendiri menegaskan bahwa anomali trafik belum tentu merupakan serangan, melainkan berpotensi berkembang menjadi serangan, dan bahwa kapasitas pemantauan nasional saat ini belum menjangkau sepuluh persen dari seluruh trafik internet (InfoBank News, 2026). Angka tersebut perlu dibaca dengan hati-hati, tetapi arahnya jelas: pertahanan siber tidak bisa hanya bertumpu pada lembaga negara, tetapi membutuhkan manusia-manusia yang paham cara mengamankan sistem di setiap lapisan masyarakat dan industri.

Bagi dunia pendidikan, situasi ini menghadirkan dua tuntutan sekaligus. Pertama, kebutuhan akan lulusan, terutama dari pendidikan vokasi bidang jaringan dan informatika, yang tidak hanya mampu membangun layanan tetapi juga mengamankannya. Kedua, kebutuhan akan warga digital yang memahami prinsip dasar perlindungan akun dan data. *Server* Linux menopang sebagian besar layanan internet; kemampuan mengeraskan (*hardening*) konfigurasi SSH, *firewall*, dan jalur komunikasi terenkripsi seperti VPN merupakan kompetensi dasar bagi siapa pun yang kelak mengelola infrastruktur.

Namun, di ruang kelas dan laboratorium, pembelajaran praktik keamanan sistem sering terbentur kenyataan. Mengubah konfigurasi sungguhan berisiko: satu urutan perintah yang keliru dapat mengunci peserta didik dari *server* mereka sendiri. Laboratorium dengan spesifikasi terbatas sulit menjalankan banyak mesin virtual sekaligus. Guru yang mengampu puluhan peserta didik tidak mungkin memeriksa setiap konfigurasi secara seketika. Akibatnya, kegiatan praktik kerap menyusut menjadi demonstrasi atau penyalinan perintah dari modul, tanpa pemahaman tentang mengapa sebuah kontrol dibutuhkan dan apa dampaknya bila diabaikan.

Di sinilah inovasi ini lahir. SecOps Lab mencoba mengembalikan makna pada praktik: peserta didik diberi sebuah *server* virtual yang rentan, diserang secara terus-menerus oleh penyerang simulasi, dan ditantang menutup celah satu demi satu sambil melihat skor keamanan, *log* kejadian, dan daftar *port* terbuka berubah di hadapan mereka.

B. Identifikasi Masalah

Berdasarkan pengamatan penyusun terhadap praktik pembelajaran keamanan jaringan di satuan pendidikan, enam persoalan berikut menjadi dasar perancangan inovasi.

Tabel 1. Identifikasi masalah pembelajaran praktik keamanan sistem

Masalah	Gejala di kelas	Akar penyebab
Risiko kesalahan praktik	Peserta terkunci dari *server* setelah salah urutan konfigurasi, misalnya *firewall* dinyalakan sebelum *port* SSH diizinkan.	Praktik pada sistem nyata tidak menyediakan ruang gagal yang aman.

Masalah	Gejala di kelas	Akar penyebab
Keterbatasan infrastruktur	Laboratorium tidak sanggup menjalankan satu mesin virtual per peserta; koneksi internet tidak stabil.	Solusi laboratorium konvensional menuntut spesifikasi dan konektivitas tinggi.
Jarak antara konsep dan praktik	Perintah disalin tanpa dipahami; istilah seperti *port*, *handshake*, dan kunci privat tetap abstrak.	Perintah diajarkan sebagai daftar hafalan, bukan sebagai jawaban atas ancaman tertentu.
Umpan balik lambat dan tidak individual	Peserta baru mengetahui kesalahannya di akhir sesi; guru tidak dapat memeriksa semua konfigurasi.	Rasio guru terhadap peserta dan waktu tatap muka yang terbatas.
Asesmen berorientasi hafalan	Penilaian berupa soal teori; kemampuan unjuk kerja jarang terukur.	Belum ada instrumen yang mengaitkan tindakan peserta dengan dampak yang terukur.
Dimensi etika	Pengetahuan bertahan dan menyerang dapat disalahgunakan bila dipraktikkan di jaringan sungguhan tanpa izin.	Lingkungan praktik tidak terisolasi dan kerangka etika tidak dibuat eksplisit.

Sumber: Olahan penyusun (2026).

C. Rumusan Masalah

1. Bagaimana merancang media pembelajaran yang memungkinkan peserta didik mempraktikkan *hardening* Linux dan VPN WireGuard secara aman, mandiri, dan berulang tanpa infrastruktur khusus?
2. Bagaimana media tersebut diintegrasikan ke dalam alur pembelajaran yang selaras dengan Pembelajaran Mendalam dan Kurikulum Merdeka?
3. Bagaimana kompetensi peserta didik diukur secara otentik melalui unjuk kerja, kuis, dan remediasi?
4. Bagaimana menjaga aspek etika, keselamatan, dan keberlanjutan penerapan inovasi ini?

D. Tujuan

Tujuan umum inovasi ini adalah menghadirkan pengalaman belajar keamanan sistem yang aman, bermakna, dan terjangkau bagi satuan pendidikan dengan beragam kondisi infrastruktur. Secara khusus, inovasi ini bertujuan untuk:

- menyediakan lingkungan praktik tersimulasi tempat peserta didik dapat menerapkan sebelas kontrol *hardening* dan membangun terowongan WireGuard tanpa risiko terhadap sistem nyata;
- menumbuhkan pemahaman konseptual melalui analogi sehari-hari, penjelasan arti setiap perintah, dan penghubungan setiap kontrol dengan risiko yang dicegahnya;
- memberikan umpan balik seketika dan terukur melalui skor keamanan, *log* kejadian, serta hasil kuis dan remediasi;
- membekali guru dengan skema pembelajaran, rubrik penilaian, dan instrumen evaluasi yang siap diadaptasi;
- menanamkan etika keamanan siber sejak awal: bertahan lebih dulu, menguji hanya dengan izin, dan melindungi data pribadi.

E. Manfaat

Tabel 2. Manfaat inovasi bagi para pemangku kepentingan

Pemangku kepentingan	Manfaat utama
Peserta didik	Berlatih tanpa takut merusak sistem, melihat dampak keputusan secara langsung, belajar mandiri sesuai kecepatan sendiri, dan memperoleh bukti kompetensi berupa skor, laporan audit, dan sertifikat penyelesaian.
Guru	Memiliki media praktik yang siap pakai, panduan berjenjang, bank soal, dan rubrik; beban demonstrasi berulang berkurang sehingga waktu dapat dipakai untuk membimbing dan berdiskusi.
Satuan pendidikan	Solusi berbiaya sangat rendah (satu berkas, tanpa lisensi dan *server*) yang dapat dijalankan di komputer laboratorium sederhana maupun ponsel, sehingga memperluas akses praktik keamanan.
Ekosistem dan industri	Pasokan lulusan yang terbiasa berpikir berlapis (*defense in depth*), memverifikasi hasil kerja, dan mendokumentasikan temuan.

Sumber: Olahan penyusun (2026).

F. Kebaruan dan Keunggulan

Kebaruan SecOps Lab terletak pada perpaduan tiga hal yang jarang hadir bersamaan dalam satu media: simulasi yang hidup (serangan dan *log* berubah mengikuti keputusan peserta), pedagogi berlapis (analogi, penjelasan, verifikasi, refleksi), dan asesmen yang tertanam (skor, kuis, remediasi, laporan audit). Semuanya dikemas dalam satu berkas yang dapat dijalankan secara luring.

Tabel 3. Perbandingan pendekatan konvensional dan SecOps Lab

Aspek	Pendekatan konvensional	SecOps Lab
Lingkungan praktik	*Server* atau mesin virtual nyata, atau tangkapan layar statis.	*Server* virtual tersimulasi di peramban; aman untuk gagal dan dapat diulang sebanyak-banyaknya.
Kebutuhan perangkat	Mesin virtual, ruang penyimpanan, jaringan laboratorium.	Satu berkas HTML (sekitar 130 KB) pada peramban modern di laptop, komputer laboratorium, tablet, atau ponsel.
Dampak tindakan	Tidak terlihat langsung; harus diperiksa manual.	Skor 0 sampai 100, *log* kejadian, ancaman waktu-nyata, dan tabel *port* berubah seketika.
Panduan belajar	Modul cetak atau PDF terpisah dari lingkungan praktik.	Sembilan misi terpandu dengan tombol perintah, penjelasan, dan pemandu istilah di dalam terminal.
Asesmen	Tes tulis di akhir bab.	Kuis 10 soal diacak dari bank 30 butir, skor keamanan host, remediasi, laporan audit, dan sertifikat bersyarat.
Etika	Sering implisit.	Eksplisit dan defensif: tidak memuat eksploit, menegaskan batas simulasi dan penggunaan yang legal.

Sumber: Olahan penyusun (2026).

G. Sistematika Penulisan

Naskah ini disusun dalam tujuh bab. Bab I memuat latar belakang, identifikasi dan rumusan masalah, tujuan, manfaat, serta kebaruan inovasi. Bab II membahas landasan teori belajar, keamanan informasi, dan kebijakan pembelajaran. Bab III mendeskripsikan produk SecOps Lab. Bab IV menguraikan model implementasi dan asesmen. Bab V memaparkan rancangan evaluasi, etika, dan mitigasi risiko. Bab VI menyajikan keberlanjutan dan peta jalan pengembangan. Bab VII memuat kesimpulan dan rekomendasi.

BAB II

Kajian Teoretis dan Landasan Kebijakan

A. Pembelajaran Mendalam dan Kurikulum Merdeka

Pada 2025 Kementerian Pendidikan Dasar dan Menengah memperkenalkan Pembelajaran Mendalam sebagai pendekatan, bukan kurikulum baru, yang menempatkan pengalaman belajar peserta didik sebagai pusat melalui tiga prinsip: berkesadaran (*mindful*), bermakna (*meaningful*), dan menggembirakan (*joyful*) (Kemendikdasmen, 2025). Pendekatan ini bernaung di bawah Kurikulum Merdeka yang menekankan fleksibilitas, kontekstualitas, dan pembelajaran berpusat pada peserta didik. Pergeserannya jelas: dari menghafal prosedur menuju memahami keterkaitan antarkonsep dan mampu menerapkannya pada situasi nyata.

> **CATATAN ISTILAH**
> Istilah *deep learning* dalam konteks kebijakan ini adalah pendekatan pedagogis, bukan teknik kecerdasan artifisial. Keduanya kerap tertukar dalam percakapan sehari-hari, sehingga perlu ditegaskan sejak awal.

Ketiga prinsip tersebut dapat diterjemahkan secara konkret pada rancangan SecOps Lab, sebagaimana dirangkum pada tabel berikut.

Tabel 4. Keselarasan prinsip Pembelajaran Mendalam dengan fitur SecOps Lab

Prinsip	Makna pedagogis	Wujud pada SecOps Lab
Mindful (berkesadaran)	Peserta hadir penuh, memahami tujuan, dan merefleksikan proses belajarnya.	Kolom “Ibaratnya” dan “Artinya” sebelum perintah dijalankan; peringatan “Perhatikan” pada setiap misi; kebiasaan memverifikasi (`sshd -T`, `sshd -t`, menjaga satu sesi cadangan); refleksi pada tahap Perbaiki.
Meaningful (bermakna)	Belajar terhubung dengan konteks nyata dan pengetahuan sebelumnya.	Skenario *server* produksi yang terus diserang; setiap kontrol dikaitkan dengan risiko, acuan CIS dan NIST, serta teknik MITRE ATT&CK; misi Investigasi Insiden; mode tantangan “*server* rusak acak”.
Joyful (menggembirakan)	Suasana belajar positif, menantang, dan memotivasi.	Skor dan tingkat perlindungan (Kritis sampai Sangat Terlindungi), pangkat RECRUIT, ANALYST, OPERATOR, ELITE berbasis XP, tampilan terminal bergaya, ruang gagal yang aman, dan sertifikat penyelesaian.

Sumber: Olahan penyusun berdasarkan Kemendikdasmen (2025).

B. Landasan Teori Belajar

Pembelajaran berbasis pengalaman. Kolb (1984) memandang belajar sebagai siklus pengalaman konkret, observasi reflektif, konseptualisasi abstrak, dan eksperimen aktif. Siklus itu tertanam dalam SecOps Lab: peserta menerapkan sebuah kontrol (pengalaman), mengamati perubahan skor dan *log* (observasi), membaca penjelasan arti dan risiko (konseptualisasi), lalu menguji pemahamannya lewat kuis dan mode tantangan (eksperimen).

Perancah belajar (*scaffolding*). Gagasan zona perkembangan proksimal Vygotsky (1978) menuntut bantuan yang tepat dan bertahap. Bantuan di SecOps Lab bersifat berlapis dan dapat ditarik: analogi, penjelasan arti perintah, perkiraan keluaran, pemandu istilah di terminal, hingga akhirnya peserta

mengetik sendiri tanpa tombol bantu.

Beban kognitif. Menurut Sweller (1988), materi yang kompleks perlu dipecah agar memori kerja tidak kewalahan. Karena itu pembelajaran dipecah menjadi sembilan misi dengan satu fokus konsep per misi, dan istilah teknis selalu didampingi analogi sehari-hari.

Umpan balik dan asesmen formatif. Umpan balik yang spesifik dan segera merupakan salah satu faktor paling berpengaruh terhadap pembelajaran (Black & Wiliam, 1998; Hattie & Timperley, 2007). Skor keamanan, *log*, keluaran terminal, dan pembahasan kuis menjalankan fungsi itu pada setiap langkah.

Gamifikasi. Deterding dkk. (2011) mendefinisikan gamifikasi sebagai penggunaan elemen desain permainan pada konteks non-permainan. SecOps Lab memakai skor, peringkat, tantangan, dan sertifikat secara terukur, selalu terikat pada capaian belajar nyata, bukan sekadar hiburan.

Taksonomi Bloom revisi. Anderson dan Krathwohl (2001) membedakan enam proses kognitif. Tabel berikut menunjukkan bahwa aktivitas pada SecOps Lab mencakup seluruh jenjang, termasuk jenjang berpikir tingkat tinggi.

Tabel 5. Pemetaan jenjang kognitif terhadap aktivitas pada SecOps Lab

Jenjang	Aktivitas pada SecOps Lab
C1 Mengingat	Menelusuri kamus 16 istilah, mengingat fungsi setiap kontrol, menjawab soal kuis.
C2 Memahami	Menjelaskan arti perintah dan hasil audit Lynis dengan bahasa sendiri.
C3 Menerapkan	Menjalankan perintah *hardening*, mengaktifkan UFW, fail2ban, dan WireGuard di terminal simulasi.
C4 Menganalisis	Membaca `auth.log`, membedakan serangan yang diblokir dan yang lolos, menelusuri insiden dengan `grep`, `lastb`, `journalctl`.
C5 Mengevaluasi	Memprioritaskan temuan berdasarkan tingkat risiko; menimbang untung-rugi *full tunnel* terhadap sesi SSH.
C6 Mencipta	Menyusun laporan audit dan rencana remediasi; merancang urutan aman penguatan SSH untuk *server* nyata.

Sumber: Olahan penyusun berdasarkan Anderson dan Krathwohl (2001).

C. Landasan Keamanan Informasi

Pertahanan berlapis (*defense in depth*). Tidak ada satu kontrol yang cukup. *Firewall* menutup pintu, kunci publik menghalangi tebak sandi, fail2ban memutus penebak yang gigih, audit memberi jejak, dan pembaruan menutup celah yang sudah diketahui. Gagasan ini menjadi tulang punggung rancangan skor.

Hak akses minimum (*least privilege*) mengajarkan bahwa akun dan proses hanya diberi hak yang diperlukan, sehingga *login* root dilarang dan administrasi dilakukan melalui `sudo` yang tercatat per pengguna.

Acuan konfigurasi. Sebelas kontrol dalam simulator disusun dari praktik umum yang selaras dengan CIS Benchmark (Center for Internet Security [CIS], t.t.) dan dipetakan ke kontrol NIST SP 800-53 (National Institute of Standards and Technology [NIST], 2020) sebagai acuan belajar. Pemetaan ini dinyatakan secara jujur sebagai versi yang disederhanakan, bukan klaim kepatuhan terhadap standar.

Taksonomi ancaman. Serangan simulasi memakai dua teknik yang dikenal dalam MITRE ATT&CK (MITRE, t.t.), yakni T1110 (*Brute Force*) dan T1046 (*Network Service Discovery*), sehingga peserta belajar

menamai ancaman dengan kosakata yang dipakai praktisi.

WireGuard. Donenfeld (2017) merancang WireGuard sebagai terowongan jaringan generasi baru yang ringkas, memakai kriptografi modern yang tetap (antara lain Curve25519 dan ChaCha20-Poly1305), dan berjalan di atas UDP, lazimnya pada *port* 51820. Kesederhanaannya menjadikannya cocok untuk pembelajaran: sedikit konsep, dampak yang terlihat jelas.

D. Keterkaitan dengan Profil Lulusan dan Capaian Pembelajaran

Inovasi ini menyumbang pada penguatan dimensi penalaran kritis (menganalisis *log* dan memprioritaskan risiko), kemandirian (belajar dengan kecepatan sendiri), kolaborasi (kerja berpasangan), dan kreativitas (menaklukkan mode tantangan). Pada tataran capaian pembelajaran, SecOps Lab dapat ditempatkan pada mata pelajaran kejuruan bidang jaringan dan keamanan informasi, serta pada pembelajaran informatika yang membahas keamanan sistem. Satuan pendidikan dianjurkan memetakan secara spesifik ke capaian pembelajaran dan tujuan pembelajaran pada mata pelajaran yang diampu.

BAB III

Deskripsi Inovasi SecOps Lab

A. Gambaran Umum Produk

SecOps Lab (*Advanced Security Simulator: Linux Hardening × WireGuard VPN*) adalah media pembelajaran interaktif berbentuk aplikasi web satu berkas. Seluruh logika, tampilan, dan data pembelajaran tertanam di dalam berkas tersebut sehingga dapat dibuka langsung pada peramban modern.

Tabel 6. Spesifikasi ringkas SecOps Lab

Komponen	Keterangan
Jenis inovasi	Simulator interaktif untuk pembelajaran keamanan sistem dan jaringan (media pembelajaran digital).
Platform	Peramban modern pada laptop, komputer laboratorium, tablet, dan ponsel; tata letak responsif; tema terang dan gelap mengikuti perangkat.
Kebutuhan teknis	Tanpa instalasi, tanpa *server*, tanpa akun. Berkas berukuran sekitar 130 KB sehingga mudah dibagikan lewat flash disk, jaringan lokal, atau aplikasi pesan.
Konektivitas dan data	Berjalan luring. Berdasarkan pemeriksaan kode sumber oleh penyusun, aplikasi tidak mengirim permintaan jaringan; progres belajar hanya disimpan lokal di peramban dan dapat direset.
Bahasa	Bahasa Indonesia dengan istilah teknis dipertahankan dalam bahasa Inggris dan dijelaskan.
Sasaran pengguna	Peserta didik SMK bidang jaringan dan informatika, SMA peminatan informatika, mahasiswa pemula, serta guru dan pelatih.
Aksesibilitas	Navigasi papan ketik, atribut ARIA pada komponen utama, tautan lewati konten, dan fokus yang terlihat.
Kondisi simulasi	Seluruh *server*, serangan, kunci, dan *log* bersifat simulasi. Tidak ada sistem nyata yang tersentuh.

Sumber: Olahan penyusun (2026).

B. Arsitektur Pembelajaran: Tiga Tahap, Sembilan Modul

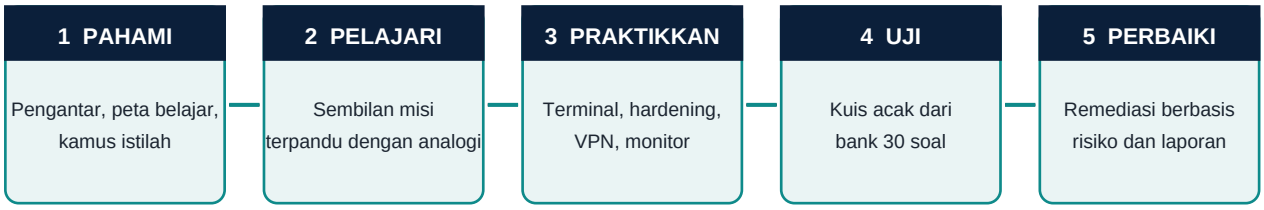
Isi aplikasi diorganisasi menjadi tiga tahap yang mencerminkan alur belajar tuntas: Belajar, Praktik, dan Evaluasi. Setiap tahap memiliki modul dengan fungsi pedagogis yang berbeda, ditambah dua modul bantuan.

Tabel 7. Struktur modul SecOps Lab

Tahap	Modul	Fungsi dan isi utama
1. Belajar	1. Pengantar	Peta belajar lima langkah dan kamus 16 istilah beserta analogi sehari-hari (mis. *firewall* sebagai satpam gerbang, VPN sebagai terowongan tertutup).
	2. Panduan Langkah	Sembilan misi berurutan. Tiap misi memuat analogi, langkah dengan tombol perintah, penjelasan “Artinya”, perkiraan “Yang akan terlihat”, dan catatan “Perhatikan”, lengkap dengan pelacak progres.

Tahap	Modul	Fungsi dan isi utama
2. Praktik	3. Terminal Lab	*Shell* simulasi `srv-prod-01`: perintah `sudo` dengan kata sandi, riwayat perintah, *pipe* (`grep`, `head`, `tail`, `wc`, `sort`, `uniq`), pesan galat realistis bila tanpa `sudo`, dan pemandu istilah yang menjelaskan setiap perintah.
	4. Kontrol Hardening	Sebelas kontrol dengan bobot, tombol terapkan, dan acuan CIS serta NIST; bagian edukasi penguatan SSH lanjutan, *backup*, dan *least privilege*; mode tantangan "*server* rusak acak".
	5. WireGuard VPN	Status terowongan `wg0`, pembangkit kunci simulasi, konfigurasi klien dan *server*, grafik *throughput*, serta catatan jebakan nyata (NAT, IP forwarding, *full tunnel*).
	6. Monitor Keamanan	Skor host, hitungan serangan dan yang diblokir, *log* kejadian (`auth.log`, ufw, fail2ban), rekomendasi prioritas, dan tabel *port* terbuka beserta statusnya.
3. Evaluasi	7. Kuis	10 soal acak dari bank 30 butir pada 13 topik, dengan pembahasan dan identifikasi topik lemah.
	8. Remediasi	Temuan diurutkan menurut risiko, disertai perintah perbaikan, verifikasi, dan *rollback*; remediasi otomatis; pembuat laporan audit.
	9. Sertifikat	Terbuka setelah tiga syarat terpenuhi; dapat dicetak atau disimpan sebagai PDF.
Bantuan	Referensi Perintah, FAQ	36 perintah yang dapat dicari dan dijalankan dengan sekali klik; sembilan pertanyaan umum dan tautan sumber belajar lanjutan.

Sumber: Olahan penyusun (2026).



Gambar 1. Alur belajar lima tahap pada SecOps Lab
Sumber: Olahan penyusun (2026).

C. Skenario Simulasi: *Server* yang Sengaja Dibuat Rentan

Peserta didik berperan sebagai administrator sistem `srv-prod-01`, sebuah *server* Linux (Ubuntu, kernel 5.15) yang awalnya berskor 0 dan berstatus Kritis. Tiga *port* terbuka sejak awal: `22/tcp` (`sshd`), `23/tcp` (`telnetd`), dan `631/tcp` (`cupsd`). Di latar belakang, penyerang simulasi terus mencoba menebak kata sandi SSH dengan nama pengguna lazim seperti root, admin, ubuntu, oracle, postgres, test, pi, dan deploy, serta memindai *port*. Setiap kontrol yang diaktifkan mengubah perilaku simulasi, sehingga peserta belajar bahwa keamanan bukanlah satu sakelar, melainkan jalur-jalur serangan yang ditutup satu per satu.

Tabel 8. Dampak kontrol terhadap perilaku simulasi

Kontrol yang diaktifkan	Perubahan yang terlihat pada simulasi
***Firewall* UFW**	Pemindaian *port* tercatat sebagai [BLOCK] dan dihitung sebagai serangan yang diblokir.
fail2ban	IP penyerang diblokir setelah tiga kali gagal *login*, tercatat sebagai "Ban" pada *log*.
Larang *login* root	Percobaan sebagai root ditolak dengan pesan "ROOT *LOGIN* REFUSED".

Kontrol yang diaktifkan	Perubahan yang terlihat pada simulasi
Autentikasi kunci publik	Koneksi ditutup pada tahap *preauth* karena autentikasi sandi dinonaktifkan.
Matikan layanan tak perlu	*Port* 23 dan 631 hilang dari keluaran `ss -tulpn` dan dari tabel *port*.
WireGuard	Terowongan aktif, *handshake* dan lalu lintas terlihat, IP publik berubah; *handshake* gagal bila UDP 51820 diblokir UFW dan belum diizinkan.

Sumber: Olahan penyusun (2026).

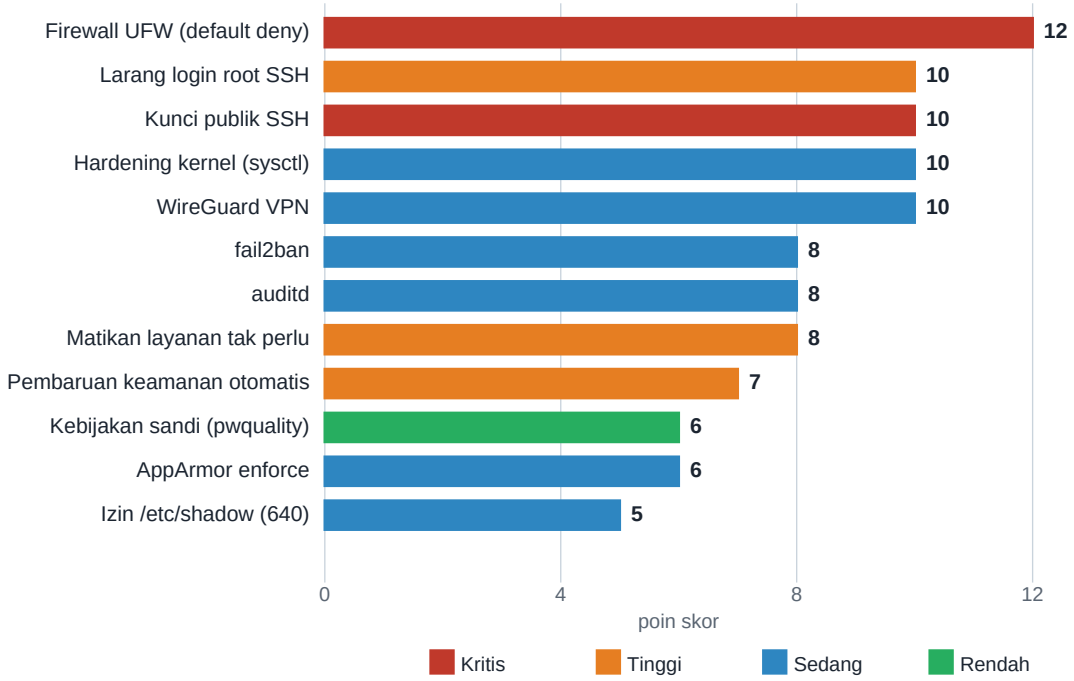
D. Kontrol Hardening dan Sistem Skor

Skor keamanan host berkisar 0 sampai 100 dan merupakan jumlah bobot sebelas kontrol *hardening* (total 90 poin) ditambah terowongan WireGuard (10 poin). Tingkat perlindungan dibaca dari skor: 0 sampai 34 Kritis, 35 sampai 59 Rentan, 60 sampai 84 Cukup Baik, dan 85 ke atas Sangat Terlindungi. Tabel berikut merinci setiap kontrol beserta tingkat risiko bila diabaikan, yang sekaligus menjadi dasar pengurutan pada modul Remediasi.

Tabel 9. Sebelas kontrol hardening dan terowongan VPN

Kontrol	Fungsi	Bobot	Risiko bila diabaikan
***Firewall* UFW (*default deny incoming*)**	Menutup seluruh *port* masuk kecuali yang diizinkan eksplisit.	12	Kritis
Larang *login* root via SSH	Mencegah *brute-force* langsung pada akun superuser.	10	Tinggi
Autentikasi kunci publik SSH	Menonaktifkan *login* sandi sehingga tebak sandi tidak berguna.	10	Kritis
Hardening kernel (sysctl)	`rp_filter`, `tcp_syncookies`; menonaktifkan *redirect* dan *source routing*.	10	Sedang
Terowongan VPN WireGuard	Jalur terenkripsi bagi lalu lintas administrasi.	10	Sedang
fail2ban	Memblokir IP setelah beberapa kali gagal *login*.	8	Sedang
Audit daemon (auditd)	Mencatat akses berkas sensitif dan perubahan konfigurasi.	8	Sedang
Matikan layanan tak perlu	Menutup telnet (sandi tanpa enkripsi) dan cups; mengurangi *attack surface*.	8	Tinggi
Pembaruan keamanan otomatis	`unattended-upgrades`; menambal CVE tanpa menunggu intervensi manual.	7	Tinggi
Kebijakan sandi kuat (pwquality)	Mensyaratkan panjang sandi minimal 12 karakter.	6	Rendah
AppArmor mode enforce	Membatasi proses pada profil yang diizinkan (*mandatory access control*).	6	Sedang
Izin `/etc/shadow` 640	*Hash* sandi hanya terbaca root dan grup shadow.	5	Sedang

Sumber: Olahan penyusun berdasarkan CIS (t.t.) dan NIST (2020).



Gambar 2. Kontribusi tiap kontrol terhadap skor keamanan (total 100 poin), diberi warna menurut tingkat risiko
Sumber: Olahan penyusun berdasarkan CIS (t.t.) dan NIST (2020).

E. Sembilan Misi Pembelajaran

Panduan Langkah menuntun peserta melalui sembilan misi yang disusun dari yang paling fundamental menuju yang paling analitis. Di dalam tiap misi, peserta mengeklik tombol perintah, melihat hasilnya langsung di Terminal Lab, lalu membaca “Artinya” agar paham, bukan sekadar mengikuti.

Tabel 10. Sembilan misi dan fokus kompetensinya

No	Misi	Fokus kompetensi
1	Mengenal Kondisi *Server*	Mengaudit dengan Lynis dan membaca *port* terbuka dengan `ss -tulpn`; menerima kondisi awal yang rentan sebagai titik berangkat.
2	Kunci Pintu Masuk (SSH)	Melarang *login* root, mewajibkan kunci publik, memverifikasi dengan `sshd -T`; urutan aman pada *server* nyata agar tidak terkunci.
3	Pasang Satpam Gerbang	*Firewall* UFW: kebijakan *deny*, mengizinkan `22/tcp` sebelum *enable*, memeriksa status.
4	Jebakan untuk Penyerang	fail2ban dan hardening kernel; memantau IP yang diblokir.
5	Tutup Pintu yang Tidak Dipakai	Mematikan telnet dan cups, memperketat izin `/etc/shadow`, memeriksa ulang *port*.
6	Lapisan Pertahanan Tambahan	Pembaruan otomatis, auditd, kebijakan sandi, dan AppArmor sebagai wujud *defense in depth*.
7	Bangun Terowongan Rahasia	WireGuard: membuka `51820/udp`, `wg-quick`, `wg show`, menguji dengan `ping` dan perubahan IP publik; peringatan *full tunnel*.
8	Verifikasi Akhir	Mengaudit ulang dan membandingkan hasil dengan kondisi awal.
9	Investigasi Insiden	Membaca `auth.log`, `lastb`, dan `journalctl`; mengaitkan temuan dengan MITRE T1110 dan T1046; mengambil keputusan tindakan tanpa menghapus bukti.

Sumber: Olahan penyusun (2026).

F. Fitur Pendukung Pembelajaran

Terminal Lab dengan pemandu istilah. Terminal meniru perilaku nyata: perintah yang memerlukan hak root ditolak bila tanpa `sudo`, riwayat perintah dapat dipanggil, dan perintah dapat dirangkai dengan *pipe*. Setiap kali peserta menjalankan perintah, pemandu istilah menjelaskan arti perintah dan *flag*-nya, sehingga terminal berfungsi sebagai kelas kecil, bukan kotak hitam.

Monitor Keamanan. Dasbor memperlihatkan skor, tingkat ancaman, jumlah percobaan serangan dan yang diblokir, kontrol aktif, serta tabel *port* beserta status dan catatannya. Peserta belajar membaca sistem sebagaimana seorang operator pusat keamanan membaca papan pantaunya.

WireGuard VPN. Modul ini menampilkan konfigurasi klien, status terowongan, dan grafik lalu lintas. Simulator secara jujur menandai bahwa kunci yang dibangkitkan adalah 32 bita acak berformat base64, bukan pasangan Curve25519 asli, serta tidak boleh dipakai pada *server* sungguhan. Catatan teknis tentang sisi *server*, IP forwarding, NAT, dan risiko *full tunnel* pada *server* yang dikelola lewat SSH melatih kewaspadaan terhadap jebakan dunia nyata.

Kuis, Remediasi, dan Laporan Audit. Kuis mengambil satu soal dari tiap topik yang dipilih acak, sehingga tiap percobaan berbeda. Topik yang lemah otomatis muncul di modul Remediasi. Peserta dapat memperbaiki temuan satu per satu atau memakai remediasi otomatis, lalu membuat laporan audit berisi skor, kontrol aktif, serta temuan tersisa yang diurutkan menurut risiko beserta acuan CIS atau NIST, risiko, perbaikan, verifikasi, dan *rollback*. Laporan ini dapat dipakai sebagai produk unjuk kerja untuk dinilai guru.

Gamifikasi dan Sertifikat. Poin pengalaman (XP) dihitung dari skor keamanan, jumlah misi selesai, dan nilai kuis, serta menentukan pangkat dari RECRUIT hingga ELITE. Sertifikat penyelesaian terbuka bila ketiga syarat terpenuhi: seluruh sembilan misi selesai, nilai kuis minimal 80, dan skor keamanan host minimal 90. Sertifikat ini ditegaskan sebagai bukti penyelesaian pelatihan simulasi, bukan sertifikasi industri.

G. Prinsip Desain dan Kejujuran terhadap Batas Simulasi



Gambar 3. Pemetaan kontrol ke dalam lapisan pertahanan (defense in depth)
Sumber: Olahan penyusun (2026).

Tiga prinsip memandu seluruh rancangan. **Aman untuk gagal:** kesalahan konfigurasi hanya berakibat pesan dan skor, bukan *server* yang terkunci. **Umpan balik seketika:** setiap tindakan berdampak terlihat pada skor, *log*, dan *port*. **Jujur tentang batas:** aplikasi berulang kali menegaskan bahwa hasilnya adalah

simulasi, bahwa pemetaan CIS dan NIST adalah acuan belajar, dan bahwa langkah pada *server* nyata menuntut kehati-hatian tambahan seperti pencadangan konfigurasi dan validasi `sshd -t` sebelum *restart*.

BAB IV

Model Implementasi Pembelajaran

A. Sintaks Pembelajaran: Pahami, Pelajari, Praktikkan, Uji, Perbaiki

Lima tahap pada peta belajar SecOps Lab dapat dijadikan sintaks pembelajaran. Tahap **Pahami** membangun kesadaran dan skema awal (*mindful*); tahap **Pelajari** dan **Praktikkan** menghubungkan konsep dengan tindakan pada konteks yang relevan (*meaningful*); tahap **Uji** dan **Perbaiki** menutup siklus dengan asesmen dan refleksi, sambil menjaga suasana tantangan yang positif (*joyful*).

B. Contoh Rancangan Pembelajaran Tiga Pertemuan

Rancangan berikut mengasumsikan satu jam pelajaran (JP) berdurasi 45 menit sebagaimana lazim pada pendidikan menengah kejuruan; satuan pendidikan dapat menyesuaikannya. Total alokasi usulan adalah 12 JP.

Tabel 11. Contoh rancangan tiga pertemuan (usulan, dapat disesuaikan)

Pertemuan	Kegiatan inti	Keluaran	Prinsip
1 (4 JP)	Pemantik dan pengantar ancaman siber; menelusuri peta belajar dan kamus istilah; Misi 1 sampai 3 (audit awal, SSH, *firewall*) secara berpasangan.	Skor awal dan skor setelah SSH dan *firewall*; catatan “Artinya” dalam kata-kata sendiri.	Mindful
2 (4 JP)	Misi 4 sampai 7: fail2ban dan kernel, menutup layanan, lapisan tambahan, terowongan WireGuard; diskusi untung-rugi *full tunnel*.	Skor host minimal 90; tangkapan layar monitor; jawaban pertanyaan pemantik.	Meaningful
3 (4 JP)	Misi 8 dan 9: verifikasi, investigasi insiden; kuis; remediasi; mode tantangan; presentasi laporan audit dan refleksi.	Laporan audit, nilai kuis, sertifikat (bila memenuhi syarat), refleksi tertulis.	Joyful

Sumber: Olahan penyusun (2026).

C. Peran Guru sebagai Fasilitator

Dalam model ini guru tidak lagi menjadi satu-satunya sumber instruksi, melainkan perancang pengalaman, pengajuk pertanyaan, dan pengarah refleksi. Pertanyaan pemantik yang disarankan antara lain:

- “Jika *server* ini adalah sebuah rumah, pintu dan jendela mana yang masih terbuka lebar sekarang?”
- “Mengapa menyalakan *firewall* sebelum mengizinkan *port* 22 justru berbahaya bagi administrator?”
- “Serangan mana yang berhasil diblokir, dan kontrol mana yang menghentikannya?”
- “Apa yang kita korbankan, yaitu kemudahan, kecepatan, atau fleksibilitas, ketika memilih *full tunnel*?”

D. Diferensiasi dan Kolaborasi

Pembelajaran berdiferensiasi mudah diwujudkan karena peserta bergerak dengan kecepatan masing-masing. Berdasarkan kesiapan, peserta yang masih pemula bertumpu pada tombol perintah dan kamus istilah, sedangkan yang mahir mengetik langsung di terminal dan menantang diri dengan mode tantangan. Berdasarkan minat, peserta yang tertarik pada analisis dapat mendalami misi Investigasi Insiden, sementara yang tertarik pada jaringan mendalami WireGuard. Berdasarkan profil belajar, peserta dapat memilih belajar lewat analogi, lewat percobaan langsung, atau lewat pembahasan kuis.

Untuk kolaborasi, disarankan skema **Pilot dan Navigator**: satu peserta mengetik, satu membaca panduan dan memverifikasi hasil, lalu bergantian per misi. Kelompok dapat pula membentuk “Tim Biru” yang menyusun laporan audit bersama dan mempresentasikan prioritas remediasinya.

E. Asesmen yang Selaras

Asesmen dirancang selaras dengan tujuan (*constructive alignment*): yang diajarkan adalah kinerja, maka yang dinilai pun kinerja.

Tabel 12. Rancangan asesmen

Jenis	Instrumen	Waktu	Bukti
Diagnostik	Pemantik, audit awal Lynis, dan kuis awal	Awal pembelajaran	Skor awal dan topik lemah
Formatif	Skor dan *log* selama praktik, pembahasan kuis, pengamatan guru	Sepanjang pembelajaran	Catatan perkembangan, tangkapan layar
Sumatif kinerja	Rubrik unjuk kerja (Lampiran A) atas laporan audit dan penjelasan lisan	Akhir pertemuan 3	Laporan audit, skor host minimal 90
Sumatif pengetahuan	Kuis 10 soal acak (kriteria 80)	Akhir pertemuan 3	Nilai kuis dan pembahasan
Refleksi	Jurnal singkat: apa yang berubah dari cara saya memandang keamanan?	Penutup	Tulisan refleksi

Sumber: Olahan penyusun (2026).

F. Adaptasi pada Beragam Konteks Pendidikan Indonesia

Keragaman kondisi satuan pendidikan di Indonesia menuntut media yang lentur. Karena SecOps Lab berupa satu berkas yang berjalan luring, ia dapat dibagikan lewat flash disk atau jaringan lokal di daerah dengan konektivitas terbatas. Satu proyektor sudah memadai untuk demonstrasi klasikal, dan ponsel dapat menjadi alternatif bagi peserta yang tidak kebagian komputer. Pada jenjang berbeda, kedalaman dapat diatur: SMA cukup menuntaskan Misi 1 sampai 4 sebagai pengantar literasi keamanan, SMK menuntaskan sembilan misi, sedangkan pendidikan tinggi dan pelatihan guru dapat memanfaatkan mode tantangan, laporan audit, serta pemetaan CIS dan NIST.

JEMBATAN MENUJU LAB NYATA

Simulator adalah pijakan, bukan tujuan akhir. Setelah peserta kompeten, lanjutkan ke mesin virtual lokal berisi Ubuntu *Server* yang terisolasi dari jaringan sekolah, ulangi langkah yang sama dengan mencadangkan konfigurasi terlebih dulu, memvalidasi dengan `sshd -t`, dan menjaga satu sesi lama tetap terbuka saat menguji. Dengan begitu rasa percaya diri yang tumbuh di simulator berpindah ke praktik nyata secara terkendali.

BAB V

Rancangan Evaluasi, Etika, dan Mitigasi Risiko

A. Rancangan Evaluasi Efektivitas

Evaluasi diarahkan menjawab satu pertanyaan utama: apakah penggunaan SecOps Lab meningkatkan kompetensi dan keterlibatan peserta didik dibandingkan pembelajaran tanpa media ini? Disarankan desain kuasi-eksperimen *pretest-posttest* dengan kelompok pembanding bila memungkinkan, atau Penelitian Tindakan Kelas (PTK) dua siklus bila guru bekerja sendiri. Data kuantitatif (nilai kuis, skor host, hasil rubrik) dilengkapi data kualitatif (wawancara, jurnal refleksi, catatan observasi).

Tabel 13. Indikator, instrumen, dan target rancangan

Aspek	Indikator	Instrumen	Target (usulan)
Penguasaan konsep	Nilai kuis minimal 80	Kuis awal dan akhir dari bank soal	Sekurang-kurangnya 75% peserta mencapai kriteria dalam dua kali percobaan
Kinerja praktik	Skor keamanan host minimal 90	Skor simulator dan laporan audit	Sekurang-kurangnya 80% peserta
Ketuntasan belajar	Sembilan misi selesai	Pelacak progres	Sekurang-kurangnya 80% peserta
Transfer ke konteks nyata	Menerapkan penguatan SSH pada mesin virtual	Rubrik unjuk kerja (Lampiran A)	Sekurang-kurangnya 70% peserta pada level Cakap
Motivasi dan keterlibatan	Persepsi keterlibatan dan kenyamanan belajar	Angket skala Likert 1 sampai 5	Rerata minimal 4,0
Kepraktisan bagi guru	Kemudahan persiapan dan penggunaan	Angket dan wawancara guru	Rerata minimal 3,5

Sumber: Rancangan penyusun (2026).

> **CATATAN METODOLOGIS**
> Seluruh target di atas adalah usulan rancangan yang perlu dikalibrasi oleh satuan pendidikan setelah uji coba awal. Naskah ini sengaja tidak memuat klaim hasil empiris, karena hasil semacam itu baru sah setelah evaluasi nyata dilaksanakan.

B. Etika dan Kerangka Hukum

Pembelajaran keamanan siber harus berpijak pada etika. SecOps Lab bersifat defensif: tidak memuat eksploit, tidak mengajarkan cara menembus sistem, dan seluruh serangan terjadi di dalam simulasi. Namun pengetahuan bertahan yang baik tetap dapat bersinggungan dengan hukum bila dipraktikkan keliru. Undang-Undang Informasi dan Transaksi Elektronik (UU Nomor 11 Tahun 2008 sebagaimana diubah, terakhir dengan UU Nomor 1 Tahun 2024) mengatur antara lain akses tanpa hak terhadap sistem elektronik milik orang lain, sedangkan UU Nomor 27 Tahun 2022 mengatur pelindungan data pribadi. Karena itu, tiap pelaksanaan perlu menegaskan kode etik berikut.

1. Hanya menguji sistem milik sendiri atau yang telah diberi izin tertulis; jaringan sekolah dan milik orang lain tidak boleh dijadikan sasaran uji.
2. Praktik pada mesin virtual harus terisolasi dari jaringan produksi.
3. Kerentanan yang ditemukan dilaporkan secara bertanggung jawab kepada pemilik sistem.
4. Data pribadi dilindungi; tidak ada kata sandi atau kunci sungguhan yang dimasukkan ke simulator.
5. Pengetahuan dipakai untuk melindungi, bukan merugikan.

C. Analisis Risiko dan Mitigasi

Tabel 14. Risiko penerapan dan strategi mitigasi

Risiko	Dampak potensial	Mitigasi
Rasa percaya diri semu karena simulasi dianggap setara produksi	Peserta lalai pada kehati-hatian di sistem nyata	Peringatan “Perhatikan” pada tiap misi, jembatan menuju mesin virtual nyata, dan penekanan pada pencadangan serta validasi konfigurasi.
Peserta menghafal urutan perintah tanpa memahami	Kompetensi dangkal dan sulit ditransfer	Kolom “Artinya”, pemandu istilah, pertanyaan pemantik, laporan audit yang menuntut penjelasan, dan rubrik yang menilai pemahaman.
Kunci dan konfigurasi simulasi disangka asli	Penggunaan kunci simulasi pada *server* sungguhan	Peringatan eksplisit di modul WireGuard dan FAQ bahwa kunci hanya acak dan bukan pasangan Curve25519 asli.
Kesenjangan literasi digital guru	Guru ragu mengelola kegiatan	Pelatihan singkat, panduan guru, dan penggunaan komunitas belajar sebagai wadah berbagi.
Penyalahgunaan pengetahuan	Pelanggaran hukum atau etika	Kode etik, isi yang murni defensif, dan penegasan batas legal sejak pertemuan pertama.
Perbedaan distribusi dan versi Linux di dunia kerja	Perintah berbeda pada sistem lain	Pencantuman acuan benchmark dan catatan bahwa nomor kontrol berbeda antarversi; rujukan sumber belajar lanjutan.

Sumber: Olahan penyusun (2026).

D. Keterbatasan

Pengembang dan pengguna perlu jujur terhadap batas inovasi ini. **Pertama**, simulator mencakup sebagian kecil dari spektrum kontrol keamanan dan tidak menggantikan laboratorium nyata. **Kedua**, progres tersimpan pada peramban masing-masing perangkat dan belum ada dasbor yang merekap capaian satu kelas bagi guru. **Ketiga**, sertifikat merupakan bukti penyelesaian pelatihan, bukan sertifikasi profesi. **Keempat**, efektivitasnya terhadap peningkatan kompetensi masih perlu dibuktikan melalui evaluasi di lapangan sebagaimana dirancang pada bagian A.

BAB VI

Keberlanjutan dan Peta Jalan Pengembangan

A. Faktor Keberlanjutan

Keberlanjutan sebuah inovasi pendidikan ditentukan oleh kemudahan replikasi, biaya, dan kepemilikan guru. SecOps Lab memiliki tiga keunggulan struktural. **Replikasi mudah:** cukup membagikan satu berkas. **Biaya hampir nol:** tanpa lisensi, *server*, atau perangkat khusus. **Mudah diadaptasi:** konten berupa data teks sehingga guru atau komunitas dapat menambah misi, soal, atau kontrol baru tanpa membangun ulang aplikasi. Wadah alami untuk berbagi praktik baik adalah musyawarah guru mata pelajaran, komunitas belajar, dan forum pelatihan guru.

B. Peta Jalan

Tabel 15. Rencana pengembangan dan diseminasi (rencana, bukan capaian)

Fase	Waktu	Kegiatan utama	Luaran
1. Validasi	Bulan 1 sampai 2	Uji coba terbatas pada satu atau dua kelas; validasi oleh ahli materi (praktisi keamanan), ahli media, dan ahli pembelajaran; uji keterbacaan.	Instrumen tervalidasi dan catatan perbaikan.
2. Penguatan	Bulan 3 sampai 5	Perbaikan berdasarkan temuan; modul lanjutan (analisis *log* mendalam, phishing dan rekayasa sosial, keamanan web dasar, *backup* dan pemulihan); dasbor rekap kelas bagi guru dengan data pribadi minimal.	Versi 2.0 dan panduan guru.
3. Perluasan	Bulan 6 sampai 9	Pelatihan guru melalui komunitas; integrasi dengan sistem manajemen pembelajaran; penjajakan kolaborasi dengan CSIRT, komunitas keamanan, dan industri untuk validasi konten.	Modul pelatihan, video panduan, dan jejaring mitra.
4. Diseminasi	Bulan 10 sampai 12	Publikasi praktik baik dan artikel ilmiah; pelisensian terbuka; penyelenggaraan kompetisi bertahan (*blue team*) tingkat pelajar.	Artikel, repositori terbuka, dan acara kompetisi.

Sumber: Olahan penyusun (2026).

C. Kebutuhan Dukungan

Keberhasilan peta jalan membutuhkan dukungan pada empat hal: waktu bagi guru untuk menjadi fasilitator, kesempatan pelatihan, akses ke praktisi sebagai pereviu konten, dan kebijakan satuan pendidikan yang mengakui laporan audit serta unjuk kerja sebagai bukti belajar yang sah.

BAB VII

Penutup

A. Kesimpulan

Keamanan siber menuntut manusia yang tidak hanya tahu, tetapi juga terbiasa bertindak, memverifikasi, dan berpikir berlapis. Pembelajaran konvensional sering gagal menumbuhkan kebiasaan itu karena praktik yang aman, terjangkau, dan berumpan balik cepat sulit diwujudkan. SecOps Lab menawarkan jalan keluarnya: simulator interaktif yang menempatkan peserta didik sebagai administrator sebuah *server* yang diserang, dengan panduan berjenjang, asesmen tertanam, dan kejujuran terhadap batas simulasi.

Inovasi ini selaras dengan Pembelajaran Mendalam dan Kurikulum Merdeka, bertumpu pada teori belajar yang mapan, dan dirancang agar dapat dijalankan di tengah keragaman kondisi infrastruktur pendidikan Indonesia. Nilai tambah terbesarnya bukan pada perintah yang dihafal peserta, melainkan pada cara berpikir yang mereka bawa: tutup yang tidak perlu, lapisi pertahanan, verifikasi, dan dokumentasikan.

Jika dikaitkan dengan rumusan masalah pada Bab I, kesimpulan naskah ini dapat dirangkum sebagai berikut.

1. Praktik *hardening* Linux dan VPN WireGuard dapat dilakukan secara aman, mandiri, dan berulang melalui simulator satu berkas tanpa infrastruktur khusus (Bab III).
2. Media ini terintegrasi dalam sintaks Pahami, Pelajari, Praktikkan, Uji, Perbaiki yang selaras dengan prinsip *mindful, meaningful, joyful* (Bab II dan Bab IV).
3. Kompetensi diukur secara otentik melalui skor host, laporan audit, kuis, remediasi, dan rubrik unjuk kerja (Bab IV dan Lampiran A).
4. Etika, keselamatan, dan keberlanjutan dijaga melalui kode etik, isi yang murni defensif, jembatan menuju lab nyata, serta peta jalan pengembangan (Bab V dan Bab VI).

B. Rekomendasi

Tabel 16. Rekomendasi bagi para pemangku kepentingan

Pihak	Rekomendasi
Guru	Mulailah dengan Misi 1 sampai 3 pada satu kelas, gunakan pertanyaan pemantik, dan kumpulkan laporan audit peserta sebagai bukti unjuk kerja. Tetapkan kode etik sejak pertemuan pertama.
Kepala satuan pendidikan	Fasilitasi waktu dan pelatihan bagi guru, serta akui unjuk kerja dan laporan audit sebagai bagian asesmen. Pastikan praktik lanjutan berlangsung pada lingkungan terisolasi.
Dinas pendidikan dan pembina vokasi	Jadikan SecOps Lab bahan praktik baik pada komunitas guru; dorong uji coba lintas sekolah dan pengumpulan data evaluasi yang seragam.
Pengembang dan mitra industri	Lakukan validasi konten bersama praktisi, kembangkan modul lanjutan dan dasbor guru, serta pertahankan prinsip simulasi defensif, ringan, dan terbuka.

Sumber: Olahan penyusun (2026).

PENUTUP

Keamanan yang baik tidak lahir dari satu gembok, melainkan dari kebiasaan berpikir berlapis. Tugas pendidikan adalah memberi ruang yang aman bagi generasi muda untuk membangun kebiasaan itu sebelum mereka dipercaya menjaga sistem yang sesungguhnya.

REFERENSI

Daftar Pustaka

Anderson, L. W., & Krathwohl, D. R. (Eds.). (2001). *A taxonomy for learning, teaching, and assessing: A revision of Bloom's taxonomy of educational objectives*. Longman.

Antara. (2026). *BSSN catat 182 potensi serangan siber tiap detik lewat internet*. https://www.antaranews.com/berita/5682957/bssn-catat-182-potensi-serangan-siber-tiap-detik-lewat-internet

Black, P., & Wiliam, D. (1998). Assessment and classroom learning. *Assessment in Education: Principles, Policy & Practice, 5*(1), 7–74.

Center for Internet Security. (t.t.). *CIS Benchmarks: Ubuntu Linux*. https://www.cisecurity.org/benchmark/ubuntu_linux/

Deterding, S., Dixon, D., Khaled, R., & Nacke, L. (2011). From game design elements to gamefulness: Defining "gamification". *Proceedings of the 15th International Academic MindTrek Conference*, 9–15.

Donenfeld, J. A. (2017). WireGuard: Next generation kernel network tunnel. *Network and Distributed System Security Symposium (NDSS)*. https://www.wireguard.com/papers/wireguard.pdf

Hattie, J., & Timperley, H. (2007). The power of feedback. *Review of Educational Research, 77*(1), 81–112.

InfoBank News. (2026). *BSSN ungkap 5,2 miliar anomali trafik internet, mayoritas berpotensi jadi ransomware*. https://infobanknews.com/bssn-ungkap-52-miliar-anomali-trafik-internet-mayoritas-berpotensi-jadi-ransomware

Kemendikdasmen. (2025). *Naskah akademik pembelajaran mendalam: Menuju pendidikan bermutu untuk semua*. Badan Standar, Kurikulum, dan Asesmen Pendidikan, Kementerian Pendidikan Dasar dan Menengah.

Kolb, D. A. (1984). *Experiential learning: Experience as the source of learning and development*. Prentice-Hall.

MITRE. (t.t.). *MITRE ATT&CK: T1110 Brute Force; T1046 Network Service Discovery*. https://attack.mitre.org/

National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations* (NIST SP 800-53 Rev. 5). https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

Sweller, J. (1988). Cognitive load during problem solving: Effects on learning. *Cognitive Science, 12*(2), 257–285.

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Vygotsky, L. S. (1978). *Mind in society: The development of higher psychological processes*. Harvard University Press.

Warta Ekonomi. (2026). *Gejolak global picu risiko siber, Indonesia hadapi 182 serangan per detik*. https://wartaekonomi.co.id/read614978/gejolak-global-picu-risiko-siber-indonesia-hadapi-182-serangan-per-detik

Catatan: data BSSN pada Bab I dirangkum dari pemaparan pejabat BSSN yang diberitakan media nasional. Angka berbeda tipis antarsumber (5,16 sampai 5,5 miliar) bergantung pada periode penghitungan, sehingga naskah ini memakai pembulatan sekitar 5,2 miliar dan menyarankan rujukan langsung ke laporan resmi BSSN untuk kutipan formal.

LAMPIRAN A

Rubrik Penilaian Unjuk Kerja

Rubrik berikut dipakai untuk menilai laporan audit dan penjelasan lisan peserta. Setiap kriteria dinilai pada empat level; skor akhir dapat dikonversi sesuai kebijakan satuan pendidikan.

Tabel 17. Rubrik unjuk kerja hardening dan VPN

Kriteria	1 Perlu Bimbingan	2 Berkembang	3 Cakap	4 Mahir
Ketepatan konfigurasi	Kurang dari 5 kontrol aktif atau banyak kesalahan urutan.	5 sampai 8 kontrol aktif dengan beberapa kesalahan.	Seluruh kontrol utama aktif dan skor host minimal 90.	Skor host minimal 90 dengan perintah efisien dan tanpa kesalahan urutan.
Pemahaman konsep	Menyebut perintah tanpa penjelasan.	Menjelaskan fungsi sebagian kontrol.	Menjelaskan fungsi dan risiko tiap kontrol dengan benar.	Menjelaskan keterkaitan antarkontrol dan menyampaikan contoh nyata.
Analisis *log* dan insiden	Belum dapat membaca *log*.	Membaca *log* tetapi belum menarik kesimpulan.	Mengidentifikasi IP, waktu, pengguna, dan jenis serangan.	Mengaitkan temuan dengan teknik ATT&CK dan merekomendasikan tindakan.
Verifikasi dan keselamatan kerja	Tidak memverifikasi hasil.	Memverifikasi sebagian langkah.	Memverifikasi setiap langkah dan menyebut cara *rollback*.	Menyusun urutan aman termasuk *backup*, `sshd -t`, dan sesi cadangan.
Etika dan kolaborasi	Pasif dalam kelompok; belum memahami batas etika.	Berkontribusi terbatas; memahami sebagian kode etik.	Berkolaborasi baik dan menaati kode etik.	Memimpin diskusi dan mengingatkan rekan akan batas etika dan legal.

Sumber: Olahan penyusun (2026).

LAMPIRAN B

Kisi-kisi Bank Soal Kuis

Bank soal terdiri atas 30 butir pilihan ganda pada 13 topik. Setiap percobaan kuis mengambil 10 topik secara acak dan satu soal dari tiap topik, dengan urutan pilihan jawaban yang juga diacak.

Tabel 18. Kisi-kisi bank soal

Topik	Butir	Indikator utama
SSH	6	Tujuan larangan *login* root; prasyarat mematikan *login* sandi; validasi `sshd -t`; kunci Ed25519; `MaxAuthTries`; `X11Forwarding`.
WireGuard	6	*Port* `51820/udp`; arti `AllowedIPs 0.0.0.0/0`; `PersistentKeepalive`; IP forwarding dan NAT; risiko *full tunnel*; izin `wg0.conf` 600.
***Firewall* UFW**	2	Kebijakan default; urutan mengizinkan *port* 22 sebelum *enable*.

Topik	Butir	Indikator utama
Pembaruan otomatis	2	Manfaat `unattended-upgrades`; kehati-hatian pada produksi.
auditd	2	Fungsi auditd; makna aturan `-w /etc/passwd -p wa`.
Layanan tak perlu	2	Bahaya telnet; prinsip mengurangi *attack surface*.
Kebijakan sandi	2	Parameter `minlen`; keterbatasan sandi dibanding kunci publik.
AppArmor	2	Jenis kontrol MAC; beda mode enforce dan complain.
***Backup* dan pemulihan**	2	Pencadangan sebelum mengubah `sshd_config`; urutan aman memulihkan.
fail2ban	1	Fungsi pemantauan *log* dan pemblokiran IP.
Kernel (sysctl)	1	Fungsi `rp_filter` terhadap IP *spoofing*.
Izin berkas	1	Izin dan pemilik ideal `/etc/shadow`.
Least privilege	1	Alasan memakai `sudo` dibanding *login* root.
Total	**30**	**13 topik**

Sumber: Olahan penyusun (2026).