

MODUL AJAR

SecOps Lab

Linux Hardening & WireGuard VPN

Mengamankan server virtual melalui simulator interaktif berbasis peramban
dalam kerangka Pembelajaran Mendalam: berkesadaran, bermakna, menggembirakan

FASE F | SMK TKJ / TJKT | 12 JP // 3 PERTEMUAN

DISUSUN OLEH

Aliyudin

Guru Mata Pelajaran Produktif TKJ
SMKS Ciledug Al Musaddadiyah
Garut, Jawa Barat

TAHUN AJARAN
2026 / 2027

ALOKASI WAKTU
12 JP (3 x 4 JP x 45 menit)

MEDIA UTAMA
SecOps Lab, simulator satu berkas

SIMULASI EDUKASI // AMAN // ETIS // LEGAL

BAGIAN AWAL

Lembar Pengesahan

Judul Modul Ajar	SecOps Lab: Linux Hardening dan WireGuard VPN melalui Simulator Interaktif Berbasis Peramban
Mata Pelajaran	Produktif Teknik Komputer dan Jaringan (TKJ/TJKT): Administrasi Sistem Jaringan dan Keamanan Jaringan (disesuaikan dengan struktur kurikulum satuan pendidikan)
Fase / Kelas	Fase F / Kelas XI atau XII SMK
Alokasi Waktu	12 JP (3 pertemuan x 4 JP x 45 menit)
Tahun Ajaran	2026/2027
Satuan Pendidikan	SMKS Ciledug Al Musaddadiyah, Garut, Jawa Barat

Mengetahui,
Kepala SMKS Ciledug Al Musaddadiyah

.....
NIP/NUPTK. .....

Garut, ... 2026
Guru Mata Pelajaran Produktif TKJ

Aliyudin
NIP/NUPTK. .....

Catatan penting bagi pengguna modul

Modul ini adalah rancangan yang bersifat fleksibel. Alokasi waktu, urutan misi, dan instrumen asesmen dapat disesuaikan dengan capaian pembelajaran, tujuan pembelajaran, karakteristik peserta didik, dan sarana satuan pendidikan. Seluruh target capaian pada modul ini adalah **usulan rancangan** yang perlu dikalibrasi melalui uji coba; modul ini tidak mengklaim hasil empiris yang belum diperoleh.

BAGIAN AWAL

Kata Pengantar

Puji syukur penyusun panjatkan ke hadirat Tuhan Yang Maha Esa atas terselesaikannya modul ajar *SecOps Lab: Linux Hardening dan WireGuard VPN*. Modul ini disusun sebagai pegangan praktis bagi guru dalam memanfaatkan simulator interaktif SecOps Lab untuk membelajarkan keamanan sistem dan jaringan secara aman, bermakna, dan terjangkau.

Pembelajaran praktik keamanan sistem di sekolah kerap terbentur keterbatasan perangkat, risiko kesalahan pada sistem nyata, serta waktu tatap muka yang terbatas untuk memberi umpan balik kepada puluhan peserta didik. Modul ini menawarkan jalan keluar melalui alur belajar lima tahap, yaitu **Pahami, Pelajari, Praktikkan, Uji, dan Perbaiki**, yang diselaraskan dengan pendekatan Pembelajaran Mendalam (*mindful*, *meaningful*, *joyful*) dan prinsip Kurikulum Merdeka.

Isi modul mencakup informasi umum, komponen inti (tujuan, pemahaman bermakna, pertanyaan pemantik, kegiatan tiga pertemuan, asesmen, pengayaan dan remediasi, serta refleksi), dilengkapi lampiran siap pakai berupa bahan bacaan, lembar kerja peserta didik, rubrik, instrumen kuis beserta kunci, angket, kode etik, glosarium, dan templat laporan audit.

Penyusun menyadari modul ini masih perlu diuji, divalidasi, dan disempurnakan. Kritik dan saran dari rekan guru, praktisi keamanan siber, serta pemangku kepentingan pendidikan sangat penyusun harapkan. Semoga modul ini bermanfaat bagi peningkatan mutu pembelajaran keamanan siber di pendidikan vokasi.

Garut, ... 2026
Penyusun,

Aliyudin

NAVIGASI

Daftar Isi

Lembar Pengesahan 2

Kata Pengantar 3

Daftar Isi 4

Informasi Umum 6

1. Identitas Modul . . . 6
2. Kompetensi Awal . . . 6
3. Dimensi Profil Lulusan yang Dikembangkan . . . 6
4. Selaras dengan Kerangka Pembelajaran Mendalam . . . 7
5. Sarana dan Prasarana . . . 7
6. Target dan Karakteristik Peserta Didik . . . 8
7. Persiapan Guru dan Skenario Alternatif . . . 8

Komponen Inti 9

1. Tujuan Pembelajaran dan Kriteria Ketercapaian . . . 9
2. Pemahaman Bermakna . . . 9
3. Pertanyaan Pemantik . . . 9
4. Alur Pembelajaran dan Peta Pertemuan . . . 10
5. Kegiatan Pembelajaran . . . 11
6. Asesmen . . . 15
7. Pengayaan dan Remediasi . . . 15
8. Refleksi . . . 16

Bahan Bacaan Peserta Didik 17

Bacaan 1. Mengapa Keamanan Harus Berlapis? . . . 17
Bacaan 2. Peta Lapisan Pertahanan . . . 17
Bacaan 3. SSH: Kunci Pintu Masuk . . . 18
Bacaan 4. Firewall UFW: Satpam Gerbang . . . 18
Bacaan 5. fail2ban, Layanan Tak Perlu, dan Kernel . . . 18
Bacaan 6. WireGuard: Terowongan Tertutup . . . 18
Bacaan 7. Membaca Log dan Menamai Ancaman . . . 19

Lembar Kerja Peserta Didik (LKPD) 20

LKPD-1: Mengenal Ancaman dan Mengunci Pintu Masuk (Pertemuan 1) . . . 20
LKPD-2: Pertahanan Berlapis dan WireGuard (Pertemuan 2) . . . 21

LKPD-3: Investigasi Insiden dan Remediasi (Pertemuan 3) 22

Rubrik Penilaian Unjuk Kerja **23**

Instrumen Kuis dan Kunci Jawaban **24**

Instrumen Refleksi, Angket, dan Observasi **26**

1. Jurnal Refleksi Peserta Didik 26
2. Penilaian Diri 26
3. Angket Keterlibatan dan Kenyamanan Belajar (skala Likert 1 sampai 5) 26
4. Lembar Observasi Guru (Formatif) 27

Kontrak Belajar: Kode Etik Keamanan Siber **28**

Kamus Istilah dan Analogi **28**

Templat Laporan Audit Tim Biru **30**

Daftar Pustaka **30**

BAGIAN A

Informasi Umum

1. Identitas Modul

Penyusun	Aliyudin, Guru Mata Pelajaran Produktif TKJ
Satuan pendidikan	SMKS Ciledug Al Musaddadiyah, Garut
Mata pelajaran	Produktif TKJ/TJKT: Administrasi Sistem Jaringan dan Keamanan Jaringan
Fase / kelas	Fase F / Kelas XI atau XII (SMA peminatan informatika dapat memakai Misi 1 sampai 4 sebagai pengantar)
Elemen / topik	Keamanan sistem dan jaringan: *hardening* server Linux, firewall, SSH, deteksi dan analisis insiden, serta VPN WireGuard
Alokasi waktu	12 JP, terbagi dalam 3 pertemuan @ 4 JP (180 menit per pertemuan)
Moda dan media	Tatap muka dengan simulator SecOps Lab (satu berkas HTML, sekitar 130 KB, berjalan luring di peramban)
Model pembelajaran	Pembelajaran Mendalam dengan *Problem-Based Learning* berbantuan simulator; sintaks Pahami, Pelajari, Praktikkan, Uji, Perbaiki
Kata kunci	keamanan siber, hardening Linux, WireGuard, defense in depth, least privilege, simulator, pembelajaran mendalam

Catatan: guru dianjurkan memetakan modul ini secara spesifik ke capaian pembelajaran (CP) dan tujuan pembelajaran (TP) pada mata pelajaran yang diampu di satuan pendidikan masing-masing.

2. Kompetensi Awal

Peserta didik diharapkan telah memiliki bekal berikut. Bila belum, guru memberi penguatan singkat pada tahap **Pahami** dan memanfaatkan kamus istilah di simulator.

- Konsep dasar jaringan: alamat IP, port, protokol TCP dan UDP, serta model klien-server.
- Penggunaan dasar antarmuka baris perintah Linux: `ls`, `cd`, `cat`, `grep`, dan konsep `sudo`.
- Pemahaman awal tentang layanan (*daemon*) dan berkas konfigurasi.
- Kebiasaan menggunakan perangkat digital secara bertanggung jawab.

3. Dimensi Profil Lulusan yang Dikembangkan

Dimensi	Wujud dalam pembelajaran
Keimanan dan ketakwaan kepada Tuhan YME	Amanah dan jujur: pengetahuan keamanan dipakai untuk melindungi, bukan merugikan; menjaga kepercayaan pemilik sistem dan data.
Kewargaan	Menaati kode etik dan ketentuan hukum (UU ITE dan UU Pelindungan Data Pribadi); sadar peran sebagai warga digital yang bertanggung jawab.
Penalaran kritis	Menganalisis log, membedakan serangan yang diblokir dan yang lolos, memprioritaskan risiko, menimbang untung-rugi *full tunnel*.
Kreativitas	Menaklukkan mode tantangan “server rusak acak”, merancang urutan aman dan rencana remediasi.
Kolaborasi	Skema Pilot dan Navigator; Tim Biru menyusun dan mempresentasikan laporan audit bersama.
Kemandirian	Bergerak sesuai kecepatan sendiri, mengulang tanpa takut gagal, menarik bantuan secara bertahap (tombol perintah menuju mengetik mandiri).

Dimensi	Wujud dalam pembelajaran
Kesehatan	Kebiasaan kerja sehat di depan layar (jeda, postur) dan pengelolaan frustrasi saat menghadapi kegagalan konfigurasi.
Komunikasi	Menjelaskan istilah teknis dengan bahasa sendiri; presentasi laporan audit; menulis refleksi.

4. Selaras dengan Kerangka Pembelajaran Mendalam

Pembelajaran Mendalam adalah **pendekatan pedagogis** (bukan kurikulum baru dan bukan teknik kecerdasan artifisial) yang menempatkan pengalaman belajar sebagai pusat melalui tiga prinsip dan tiga pengalaman belajar berikut.

Prinsip / pengalaman	Makna	Wujud pada modul
Mindful (berkesadaran)	Hadir penuh, paham tujuan, merefleksikan proses.	Kolom “Ibaratnya” dan “Artinya”; peringatan “Perhatikan”; kebiasaan verifikasi (`sshd -T`, `sshd -t`, sesi cadangan); refleksi tahap Perbaiki.
Meaningful (bermakna)	Terhubung dengan konteks nyata dan pengetahuan awal.	Skenario server produksi yang terus diserang; kontrol dikaitkan risiko, CIS/NIST, dan MITRE ATT&CK; Investigasi Insiden.
Joyful (menggembirakan)	Suasana positif, menantang, memotivasi.	Skor dan tingkat perlindungan, pangkat RECRUIT sampai ELITE, tampilan terminal, ruang gagal yang aman, sertifikat penyelesaian.
Memahami	Membangun konsep.	Tahap Pahami dan Pelajari (peta belajar, kamus, misi terpandu).
Mengaplikasi	Menerapkan pada konteks.	Tahap Praktikkan dan Uji (terminal, hardening, VPN, kuis).
Merefleksi	Menilai dan memperbaiki proses.	Tahap Perbaiki (remediasi, laporan audit, jurnal refleksi).

Kerangka pembelajaran	Penerapan dalam modul
Praktik pedagogis	PBL berbantuan simulator, *scaffolding* berlapis (analogi, arti perintah, perkiraan keluaran, pemandu istilah), diferensiasi, asesmen formatif berkelanjutan.
Lingkungan pembelajaran	Ruang gagal yang aman, kontrak belajar etika, kerja berpasangan, suasana kelas yang menantang namun suportif.
Kemitraan pembelajaran	Pelibatan praktisi keamanan dan CSIRT sebagai pereviu atau narasumber; komunitas guru (MGMP) sebagai wadah berbagi.
Pemanfaatan digital	Simulator luring satu berkas; tidak membutuhkan akun, server, ataupun koneksi internet; progres tersimpan lokal.

5. Sarana dan Prasarana

Kebutuhan	Keterangan
Perangkat peserta didik	Laptop, komputer laboratorium, tablet, atau ponsel dengan peramban modern. Disarankan 1 perangkat per 2 peserta (Pilot dan Navigator).
Perangkat guru	Laptop dan proyektor untuk demonstrasi klasikal.
Media digital	Berkas SecOps Lab (HTML), dibagikan lewat flash disk, jaringan lokal, atau aplikasi pesan. Siapkan salinan cadangan.
Media cetak	LKPD (Lampiran B), kartu 11 kontrol (opsional), rubrik, lembar refleksi, kontrak belajar.
Opsional (tindak lanjut)	Mesin virtual Ubuntu Server yang terisolasi dari jaringan sekolah untuk jembatan menuju lab nyata.
Internet	Tidak wajib untuk menjalankan simulator.

6. Target dan Karakteristik Peserta Didik

- **Peserta didik reguler:** memiliki bekal dasar jaringan dan Linux, mampu mengikuti alur misi dengan tombol perintah.
- **Peserta didik yang memerlukan pendampingan:** perlu penguatan istilah dan konsep dasar; diberi tombol perintah, kamus, dan pasangan mentor.
- **Peserta didik berkemampuan tinggi:** mengetik langsung tanpa tombol bantu, mencoba mode tantangan, dan merancang urutan aman untuk server nyata.
- Perhatikan juga keragaman akses perangkat, kecepatan membaca teks teknis, dan kenyamanan menggunakan bahasa Inggris teknis.

7. Persiapan Guru dan Skenario Alternatif

Waktu	Yang disiapkan
H-7	Unduh dan uji berkas SecOps Lab di peramban sekolah; tentukan pasangan dan kelompok; cetak LKPD, rubrik, dan kontrak belajar; siapkan pertanyaan pemantik.
H-1	Salin berkas ke flash disk dan beberapa perangkat cadangan; periksa proyektor; pastikan peserta tahu cara membuka berkas dan mereset progres.
Hari H	Tayangkan skenario pemantik; tegaskan kode etik; pastikan setiap pasangan dapat membuka simulator sebelum kegiatan inti dimulai.

Kendala sarana	Skenario alternatif
Perangkat terbatas	Satu perangkat per kelompok 4 sampai 5 peserta dengan peran bergilir (Pilot, Navigator, Pencatat, Penguji); atau demonstrasi klasikal dengan satu proyektor, kelas menjadi “tim operator” yang memberi komando.
Hanya ponsel	Tata letak simulator responsif; gunakan mode lanskap. Terminal dapat dioperasikan lewat tombol perintah agar tidak banyak mengetik.
Listrik atau jaringan terganggu	Permainan kartu “11 Kontrol”: peserta mengurutkan kartu kontrol menurut tingkat risiko dan menjelaskan alasannya, lalu menyimulasikan urutan aman SSH dan firewall di kertas.
Peserta tertinggal	Pasangkan dengan mentor sebaya; fokuskan pada Misi 1 sampai 3 lebih dulu; lengkapi sisanya sebagai tugas terstruktur atau pengayaan.
Progres tidak tersimpan	Progres disimpan lokal di peramban; hindari mode penyamaran (*private*) dan penghapusan data situs. Minta tangkapan layar pada akhir tiap misi sebagai bukti cadangan.

BAGIAN B

Komponen Inti

1. Tujuan Pembelajaran dan Kriteria Ketercapaian

Setelah mengikuti rangkaian pembelajaran (12 JP), peserta didik mampu:

Kode	Tujuan pembelajaran	Level	Kriteria ketercapaian (KKTP)
TP-1	Menjelaskan ancaman *brute force* dan pemindaian port serta prinsip *defense in depth* dan *least privilege* dengan bahasa sendiri.	C2	Menjelaskan sekurang-kurangnya 3 ancaman atau kontrol dengan benar pada LKPD-1 dan lisan.
TP-2	Menerapkan sebelas kontrol *hardening* pada server simulasi dengan urutan aman hingga skor host minimal 90.	C3	Skor host minimal 90; urutan SSH dan firewall benar; setiap langkah diverifikasi.
TP-3	Mengonfigurasi terowongan WireGuard simulasi, memverifikasinya, dan menimbang untung-rugi *full tunnel*.	C3, C5	Terowongan aktif (wg0), port 51820/udp diizinkan, hasil `wg show` dan ping terdokumentasi; risiko *full tunnel* dijelaskan.
TP-4	Menganalisis log (`auth.log, lastb, journalctl`) untuk mengidentifikasi IP, pengguna, waktu, dan jenis serangan, serta mengaitkannya dengan MITRE T1110 dan T1046.	C4	Rubrik “Analisis log dan insiden” level Cakap (3) atau lebih.
TP-5	Menyusun dan mempresentasikan laporan audit serta rencana remediasi berprioritas risiko, lengkap dengan verifikasi dan *rollback*.	C5, C6	Laporan memuat skor awal-akhir, kontrol aktif, temuan tersisa terurut risiko, dan rencana perbaikan.
TP-6	Menunjukkan sikap etis: hanya menguji sistem milik sendiri atau yang diizinkan, melindungi data pribadi, dan memakai pengetahuan untuk melindungi.	Afektif	Menaati kontrak belajar; rubrik “Etika dan kolaborasi” level Cakap (3) atau lebih.

*Peserta didik dinyatakan **mencapai tujuan pembelajaran** bila berada pada level Cakap atau lebih pada rubrik unjuk kerja dan memperoleh nilai kuis minimal 80. Kriteria ini merupakan usulan dan dapat disesuaikan satuan pendidikan.*

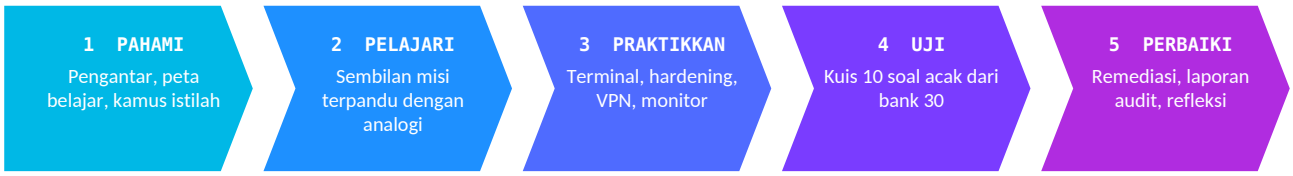
2. Pemahaman Bermakna

- Keamanan bukan satu sakelar, melainkan jalur-jalur serangan yang ditutup satu per satu dan saling melapisi.
- Setiap kontrol ada karena ancaman tertentu; memahami *mengapa* lebih penting daripada menghafal *perintah apa*.
- Verifikasi, pencadangan, dan dokumentasi adalah bagian dari pekerjaan administrator, bukan tambahan.
- Simulator adalah pijakan yang aman untuk gagal; kehati-hatian tetap wajib saat berpindah ke sistem nyata.
- Kemampuan bertahan harus disertai etika dan kepatuhan hukum.

3. Pertanyaan Pemantik

- “Jika server ini 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 (kemudahan, kecepatan, atau fleksibilitas) ketika memilih *full tunnel*?”
- “Jika hanya boleh memilih tiga kontrol, mana yang kamu pasang lebih dulu, dan apa alasannya?”
- “Bagaimana kamu memastikan perubahan konfigurasi tidak mengunci dirimu sendiri?”

4. Alur Pembelajaran dan Peta Pertemuan



Pertemuan	Fokus	Misi	Keluaran utama
1 (4 JP)	Mengenal ancaman dan mengunci pintu masuk	1, 2, 3	Skor awal dan skor setelah SSH dan firewall; LKPD-1.
2 (4 JP)	Pertahanan berlapis dan terowongan WireGuard	4, 5, 6, 7	Skor host minimal 90; tangkapan layar monitor; LKPD-2.
3 (4 JP)	Verifikasi, investigasi, evaluasi, refleksi	8, 9 + kuis + remediasi	Laporan audit, nilai kuis, refleksi; sertifikat bila memenuhi syarat; LKPD-3.

Syarat sertifikat penyelesaian di simulator: sembilan misi selesai, nilai kuis minimal 80, dan skor keamanan host minimal 90. Sertifikat adalah bukti penyelesaian pelatihan simulasi, bukan sertifikasi industri.

5. Kegiatan Pembelajaran

Setiap pertemuan berdurasi 4 JP (180 menit). Pembagian waktu berikut adalah usulan dan dapat disesuaikan.

Pertemuan 1 (4 JP): Mengenal Ancaman dan Mengunci Pintu Masuk

Tujuan pertemuan	TP-1, TP-2 (sebagian), TP-6. Peserta memahami kondisi server rentan, menutup jalur SSH, dan memasang firewall dengan urutan aman.
Media dan bahan	SecOps Lab, proyektor, LKPD-1, kontrak belajar etika, kamus istilah (Lampiran G).

Waktu	Kegiatan guru dan peserta didik	Pengalaman / prinsip
0-20 menit	**PENDAHULUAN** • Salam, doa, presensi, cek perangkat dan berkas simulator. • **Pemantik cerita:** "Server sekolah tiba-tiba lambat; ribuan percobaan login gagal tercatat tengah malam." Peserta menebak penyebabnya. • Menyampaikan tujuan, alur lima tahap, dan **kontrak belajar etika** (Lampiran F). • **Asesmen diagnostik:** tanya-jawab atau kuis awal singkat tentang port, SSH, dan firewall.	Mindful: sadar tujuan dan batas etika.
20-45 menit	**PAHAMI (25 menit)** • Guru memandu peta belajar dan kamus 16 istilah; peserta memadankan istilah dengan analogi (satpam gerbang, terowongan tertutup). • Demonstrasi Monitor Keamanan: skor 0, status Kritis, tiga port terbuka (22, 23, 631), serangan simulasi mulai masuk. • Peserta menulis satu pertanyaan: "Apa yang paling dulu ingin kuamankan, dan mengapa?"	Memahami. Mindful.
45-70 menit	**PELAJARI + PRAKTIKKAN: Misi 1 (25 menit)** • Berpasangan (Pilot dan Navigator) menjalankan audit Lynis dan `ss -tulpn`. • Membaca "Artinya" dan pemandu istilah; mengisi LKPD-1 bagian A (skor awal, port, risiko). • Guru berkeliling dengan pertanyaan penggali: "Layanan mana yang menurutmu tidak perlu?"	Mengaplikasi. Meaningful.
70-110 menit	**Misi 2: Kunci Pintu Masuk SSH (40 menit)** • Melarang login root, mewajibkan kunci publik, memverifikasi dengan `sshd -T`. • Diskusi **urutan aman pada server nyata**: cadangkan `sshd_config`, validasi `sshd -t`, pertahankan satu sesi lama terbuka, uji kunci pada sesi baru sebelum menonaktifkan sandi. • Peserta mengisi LKPD-1 bagian C dengan kata-kata sendiri.	Mengaplikasi. Mindful (verifikasi sebagai kebiasaan).
110-145 menit	**Misi 3: Pasang Satpam Gerbang (35 menit)** • Kebijakan *deny*, izinkan 22/tcp **sebelum** `enable`, periksa status. • Diskusi pemantik: "Apa yang terjadi di server nyata bila urutannya terbalik?" • Amati perubahan skor, log `[BLOCK]`, dan hitungan serangan diblokir.	Mengaplikasi. Meaningful.
145-160 menit	**PERBAIKI: refleksi singkat (15 menit)** • Pasangan membandingkan skor, saling menjelaskan satu kontrol memakai analogi. • Menjawab pertanyaan LKPD-1 bagian D.	Merefleksi. Joyful (berbagi capaian).
160-180 menit	**PENUTUP** • Rangkuman bersama; refleksi 3-2-1 (3 hal dipelajari, 2 hal menarik, 1 pertanyaan). • Tangkapan layar skor sebagai bukti; tugas: membaca Bahan Bacaan 3 sampai 5 (Lampiran A). • Doa dan salam penutup.	Mindful. Asesmen formatif.

Catatan guru

Hindari memberi daftar perintah untuk dihafal. Minta peserta lebih dulu menebak "mengapa" sebelum menekan tombol perintah. Pastikan peserta tidak memasukkan kata sandi atau kunci sungguhan ke simulator.

Pertemuan 2 (4 JP): Pertahanan Berlapis dan Terowongan WireGuard

Tujuan pertemuan	TP-2 (lanjutan), TP-3, TP-6. Peserta melengkapi lapisan pertahanan hingga skor minimal 90 dan membangun terowongan WireGuard simulasi.
Media dan bahan	SecOps Lab, proyektor, LKPD-2, bahan bacaan WireGuard (Lampiran A), kartu 11 kontrol (opsional).

Waktu	Kegiatan guru dan peserta didik	Pengalaman / prinsip
0-20 menit	**PENDAHULUAN** • Peninjauan skor akhir pertemuan 1; peserta menyebut serangan yang sudah terhenti dan yang masih lolos di Monitor Keamanan. • Pemantik: “Jika firewall sudah menyala, mengapa kita masih butuh fail2ban?” • Penegasan ulang kontrak etika dan tujuan pertemuan.	Mindful.
20-50 menit	**Misi 4: Jebakan untuk Penyerang (30 menit)** • Mengaktifkan fail2ban dan *hardening* kernel (sysctl); memantau IP yang diblokir (“Ban” pada log setelah tiga kali gagal login). • Peserta menulis di LKPD-2: ancaman yang ditutup dan bukti di log.	Mengaplikasi. Meaningful.
50-75 menit	**Misi 5: Tutup Pintu yang Tidak Dipakai (25 menit)** • Mematikan telnet dan cups, memperketat izin `/etc/shadow`, memeriksa ulang port (22 saja yang tersisa). • Diskusi: mengapa telnet berbahaya? apa itu *attack surface*?	Mengaplikasi. Meaningful.
75-105 menit	**Misi 6: Lapisan Pertahanan Tambahan (30 menit)** • Pembaruan keamanan otomatis, auditd, kebijakan sandi (pwquality), AppArmor mode *enforce*. • Kelompok memetakan sebelas kontrol ke empat lapisan (jaringan, akses, sistem, deteksi dan pemeliharaan).	Memahami, mengaplikasi. Penalaran kritis.
105-145 menit	**Misi 7: Bangun Terowongan Rahasia (40 menit)** • Izinkan 51820/udp, jalankan `wg-quick`, periksa `wg show`, uji ping dan perubahan IP publik. • Amati bagaimana *handshake* gagal bila UDP 51820 diblokir UFW dan belum diizinkan. • Tegaskan: kunci di simulator hanya acak 32 bita, **bukan** pasangan Curve25519 asli dan tidak boleh dipakai di server sungguhan.	Mengaplikasi. Meaningful.
145-160 menit	**PERBAIKI: diskusi untung-rugi *full tunnel* (15 menit)** • Kelompok mengisi tabel untung, rugi, dan keputusan pada LKPD-2; satu kelompok mempresentasikan. • Kaitan dengan sesi SSH pada server yang dikelola jarak jauh.	Merefleksi. Penalaran kritis, komunikasi.
160-180 menit	**PENUTUP** • Verifikasi skor host minimal 90 dan tangkapan layar Monitor. • Rangkuman, refleksi singkat, penugasan membaca Bahan Bacaan 6. • Doa dan salam penutup.	Mindful. Asesmen formatif.

Catatan guru

Peserta yang mencapai skor 90 lebih cepat dapat diarahkan mencoba mengetik perintah tanpa tombol bantu atau menjadi mentor sebaya. Ingatkan bahwa catatan teknis sisi server (IP forwarding, NAT) di modul WireGuard adalah “jebakan dunia nyata” untuk dibahas, bukan hafalan.

Pertemuan 3 (4 JP): Verifikasi, Investigasi, Evaluasi, dan Refleksi

Tujuan pertemuan	TP-4, TP-5, TP-6 dan asesmen sumatif. Peserta memverifikasi hasil, menginvestigasi insiden, mengikuti kuis, memperbaiki temuan, dan mempresentasikan laporan audit.
Media dan bahan	SecOps Lab (Misi 8, 9, Kuis, Remediasi, Sertifikat), LKPD-3, templat laporan audit (Lampiran H), rubrik (Lampiran C), lembar refleksi.

Waktu	Kegiatan guru dan peserta didik	Pengalaman / prinsip
0-15 menit	**PENDAHULUAN** • Pemantik: “Bagaimana kita tahu server benar-benar lebih aman daripada kemarin?” • Menjelaskan alur hari ini dan kriteria penilaian (rubrik dibagikan lebih dulu).	Mindful.
15-30 menit	**Misi 8: Verifikasi Akhir (15 menit)** • Audit ulang dengan Lynis, bandingkan dengan kondisi awal; catat selisih skor dan port.	Mengaplikasi. Merefleksi.
30-60 menit	**Misi 9: Investigasi Insiden (30 menit)** • Membaca `auth.log`, `lastb`, `journalctl` dengan `grep, head, sort, uniq`. • Mengaitkan temuan dengan MITRE T1110 (*Brute Force*) dan T1046 (*Network Service Discovery*); memutuskan tindakan **tanpa menghapus bukti**. • Mengisi LKPD-3 bagian A.	Mengaplikasi. Penalaran kritis.
60-80 menit	**UJI: Kuis (20 menit)** • Kuis 10 soal acak dari bank 30 butir di simulator (kriteria 80); pembahasan segera dan identifikasi topik lemah.	Asesmen sumatif pengetahuan.
80-105 menit	**PERBAIKI: Remediasi dan mode tantangan (25 menit)** • Memperbaiki temuan menurut risiko (perintah, verifikasi, rollback) atau memakai remediasi otomatis lalu menelaah hasilnya. • Peserta yang siap mencoba mode “server rusak acak”.	Mengaplikasi. Kreativitas.
105-130 menit	**Menyusun laporan audit (25 menit)** • Per kelompok (Tim Biru) membuat laporan audit dari simulator dan melengkapi LKPD-3 bagian B. • Guru menilai dengan rubrik sambil berkeliling.	Mencipta (C6). Kolaborasi.
130-160 menit	**Presentasi Tim Biru (30 menit)** • Setiap kelompok (sekitar 5 menit) memaparkan skor, prioritas remediasi, dan satu pelajaran terpenting; kelompok lain memberi umpan balik dengan format “bintang dan saran”.	Komunikasi. Joyful.
160-180 menit	**PENUTUP** • Jurnal refleksi: “Apa yang berubah dari cara saya memandang keamanan?” (Lampiran E). • Penegasan jembatan menuju lab nyata; pembagian sertifikat bagi yang memenuhi syarat. • Doa dan salam penutup.	Merefleksi. Mindful.

Catatan guru

Bila waktu tidak cukup, presentasi dapat dilakukan oleh perwakilan kelompok dan laporan lain dikumpulkan sebagai produk. Pada Misi 9 tekankan bahwa dalam insiden nyata, log adalah barang bukti: jangan dihapus atau diubah.

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 lebih 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.

Miskonsepsi yang Perlu Diantisipasi

Miskonsepsi	Cara meluruskan
“Firewall saja sudah cukup.”	Tunjukkan di Monitor bahwa serangan tebak sandi tetap perlu dihentikan fail2ban dan kunci publik; bahas *defense in depth*.
“Karena sudah pakai VPN, server pasti aman.”	VPN mengenkripsi jalur, tidak menggantikan *hardening*; bahas risiko *full tunnel* pada sesi SSH.
“Skor 100 di simulator berarti siap di server produksi.”	Tekankan keterbatasan simulasi, pentingnya cadangan, `sshd -t`, dan sesi cadangan di server nyata.
“Login sandi bisa langsung dimatikan.”	Pastikan kunci publik terpasang dan teruji pada sesi terpisah sebelum login sandi dinonaktifkan.
“Kunci WireGuard dari simulator boleh dipakai.”	Kunci simulasi hanya 32 bita acak berformat base64; **jangan** dipakai di server sungguhan.

6. Asesmen

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

Jenis	Teknik dan instrumen	Waktu	Bukti
Diagnostik	Pemantik cerita, audit awal Lynis (Misi 1), kuis awal singkat	Awal pertemuan 1	Skor awal dan topik lemah
Formatif	Skor dan log selama praktik, LKPD, pembahasan kuis, pengamatan guru (Lampiran E), umpan balik rekan	Sepanjang pembelajaran	LKPD, catatan perkembangan, tangkapan layar
Sumatif kinerja	Rubrik unjuk kerja (Lampiran C) atas laporan audit dan penjelasan lisan	Pertemuan 3	Laporan audit, skor host minimal 90
Sumatif pengetahuan	Kuis 10 soal acak (kriteria 80); soal uraian (Lampiran D)	Pertemuan 3	Nilai kuis dan pembahasan
Refleksi dan sikap	Jurnal refleksi, angket Likert, rubrik etika dan kolaborasi	Penutup pertemuan 3	Tulisan refleksi, angket

Pengolahan Nilai (usulan)

Komponen	Cara menghitung	Bobot
Praktik di simulator	0,7 x skor host akhir + 0,3 x (jumlah misi selesai / 9 x 100)	30%
Laporan audit dan presentasi	Rubrik unjuk kerja (jumlah skor 5 kriteria / 20 x 100)	30%
Pengetahuan	Nilai kuis simulator atau instrumen Lampiran D (skala 0-100)	25%
Refleksi, kolaborasi, etika	Jurnal refleksi dan rubrik “Etika dan kolaborasi” (skor / 4 x 100)	15%

Jumlah skor rubrik (maks 20)	Level	Keterangan
18 sampai 20	Mahir	Melampaui kriteria; dapat menjadi mentor sebaya.
14 sampai 17	Cakap	Mencapai kriteria ketercapaian tujuan pembelajaran.
10 sampai 13	Berkembang	Mendekati kriteria; perlu penguatan terarah.
5 sampai 9	Perlu bimbingan	Perlu remediasi dan pendampingan.

Rubrik rinci terdapat pada Lampiran C. Bobot dan batas level dapat disesuaikan dengan kebijakan penilaian satuan pendidikan.

7. Pengayaan dan Remediasi

Kelompok	Ciri	Tindak lanjut
Perlu bimbingan	Nilai kuis di bawah 80 atau rubrik level 1 sampai 2.	• Ulang misi dengan tombol perintah dan kamus istilah. • Modul Remediasi di simulator untuk topik lemah. • Pendampingan mentor sebaya; kuis ulang (percobaan baru selalu berbeda). • Konsultasi singkat dengan guru.
Cakap	Memenuhi kriteria ketercapaian.	• Mengerjakan mode tantangan “server rusak acak”. • Memperdalam topik pilihan (Investigasi Insiden atau WireGuard).
Mahir	Skor host 90 atau lebih dengan perintah efisien dan analisis tajam.	• Mengetik tanpa tombol bantu. • Menyusun urutan aman *hardening* untuk mesin virtual terisolasi. • Menjadi mentor, membuat soal atau misi tambahan (konten berupa data teks).

8. Refleksi

Refleksi peserta didik

- Hal apa yang paling berkesan dan paling sulit saat mengamankan server?
- Kontrol mana yang menurutmu paling penting, dan apa alasannya?
- Kesalahan apa yang kamu buat, dan apa yang kamu pelajari darinya?
- Apa yang berubah dari cara saya memandang keamanan?
- Langkah apa yang akan kamu lakukan agar kebiasaan aman ini terbawa ke praktik nyata?

Refleksi guru

- Apakah tujuan pembelajaran tercapai? Bukti apa yang mendukung?
- Bagian mana yang membuat peserta paling terlibat dan bagian mana yang membuat mereka tertahan?
- Apakah diferensiasi berjalan: siapa yang butuh bantuan lebih, siapa yang butuh tantangan lebih?
- Apa yang akan saya ubah pada alokasi waktu, pertanyaan pemantik, atau pengelompokan?
- Apakah kode etik dan batas simulasi tersampaikan dengan jelas?

LAMPIRAN A

Bahan Bacaan Peserta Didik

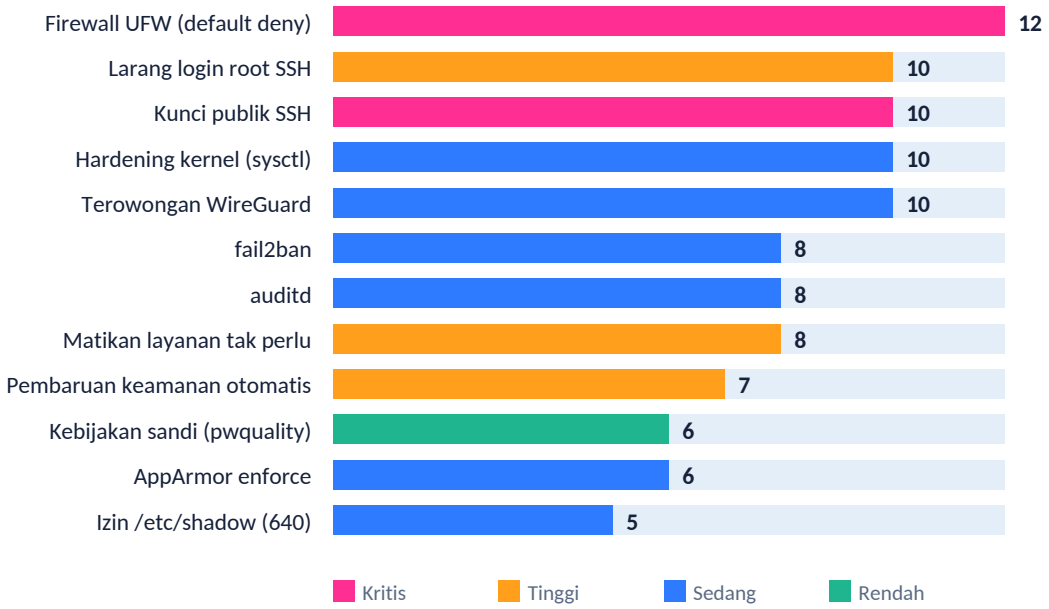
Baca dulu sebelum mencoba

Semua perintah di bawah dijalankan di **simulator**. Pada server nyata, praktikkan hanya di mesin virtual milikmu sendiri yang terisolasi dari jaringan sekolah, dan selalu cadangkan konfigurasi lebih dulu.

Bacaan 1. Mengapa Keamanan Harus Berlapis?

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 disebut **pertahanan berlapis** (*defense in depth*). Ditambah prinsip **hak akses minimum** (*least privilege*): akun dan proses hanya diberi hak yang diperlukan, sehingga login root dilarang dan administrasi dilakukan lewat `sudo` yang tercatat per pengguna.

Skor keamanan host di simulator berkisar 0 sampai 100: sebelas kontrol *hardening* bernilai total 90 poin ditambah terowongan WireGuard 10 poin. Tingkat perlindungan: 0 sampai 34 **Kritis**, 35 sampai 59 **Rentan**, 60 sampai 84 **Cukup Baik**, 85 ke atas **Sangat Terlindungi**.



Gambar A1. Kontribusi tiap kontrol terhadap skor keamanan (total 100 poin), diberi warna menurut tingkat risiko bila diabaikan.

Bacaan 2. Peta Lapisan Pertahanan

Lapisan	Kontrol	Tugasnya
Jaringan	Firewall UFW, WireGuard, tutup layanan tak perlu	Menutup pintu masuk dan mengurangi *attack surface*.
Akses	Kunci publik SSH, larang root, fail2ban, kebijakan sandi	Memastikan hanya orang yang berhak yang masuk.
Sistem	Hardening kernel, AppArmor, izin berkas sensitif	Membatasi dampak bila ada yang lolos.
Deteksi dan pemeliharaan	auditd, pembaruan keamanan otomatis	Meninggalkan jejak dan menambal celah yang sudah diketahui.

Bacaan 3. SSH: Kunci Pintu Masuk

SSH adalah pintu administrasi jarak jauh. Dua kebiasaan penting: **larang login root** (mengurangi risiko *brute force* pada akun superuser) dan **wajibkan kunci publik** (tebak sandi menjadi tidak berguna). Karena kesalahan di sini dapat mengunci administrator dari servernya sendiri, gunakan **urutan aman** berikut.

```
# 1. Cadangkan konfigurasi
sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.bak
# 2. Ubah pengaturan (PermitRootLogin no, PubkeyAuthentication yes)
# 3. Validasi sintaks SEBELUM restart
sudo sshd -t
# 4. Periksa nilai efektif
sudo sshd -T | grep -E "permitrootlogin|pubkeyauthentication|passwordauthentication"
# 5. Restart, lalu uji login kunci pada sesi BARU. Sesi lama tetap terbuka.
sudo systemctl restart ssh
```

Nonaktifkan login sandi (`PasswordAuthentication no`) hanya setelah login dengan kunci terbukti berhasil.

Bacaan 4. Firewall UFW: Satpam Gerbang

Kebijakan dasarnya *default deny incoming*: semua yang masuk ditolak kecuali yang diizinkan secara eksplisit. Urutan menentukan: **izinkan port 22 lebih dulu, baru aktifkan firewall**.

```
sudo ufw default deny incoming
sudo ufw default allow outgoing
sudo ufw allow 22/tcp      # izinkan SSH SEBELUM enable
sudo ufw enable
sudo ufw status verbose
```

Bacaan 5. fail2ban, Layanan Tak Perlu, dan Kernel

- **fail2ban** membaca log dan memblokir IP setelah beberapa kali gagal login (di simulator: tiga kali, tercatat “Ban”).
- **Matikan layanan tak perlu**: telnet mengirim sandi tanpa enkripsi; cups membuka port 631 yang tidak dibutuhkan server. Contoh: `sudo systemctl disable --now cups`. Setelah itu periksa ulang dengan `ss -tulpn`.
- **Izin** `/etc/shadow` 640 agar hash sandi hanya terbaca root dan grup shadow.
- **Hardening kernel (sysctl)**: `rp_filter` melawan IP *spoofing*, `tcp_syncookies` membantu menghadapi SYN flood, serta menonaktifkan *redirect* dan *source routing*.

Bacaan 6. WireGuard: Terowongan Tertutup

WireGuard adalah terowongan jaringan yang ringkas, memakai kriptografi modern yang tetap (antara lain Curve25519 dan ChaCha20-Poly1305), dan berjalan di atas UDP, lazimnya pada **port 51820** (Donenfeld, 2017). Sedikit konsep, dampak terlihat jelas.

Parameter	Fungsi
`PrivateKey / PublicKey`	Pasangan kunci tiap sisi. Kunci privat tidak pernah dibagikan. **Kunci di simulator hanya acak, bukan Curve25519 asli.**
`Address`	Alamat IP virtual antarmuka terowongan (wg0).
`ListenPort`	Port UDP tempat WireGuard mendengarkan (lazimnya 51820).
`AllowedIPs`	Rentang IP yang boleh lewat terowongan. `0.0.0.0/0` berarti *full tunnel*: seluruh lalu lintas IPv4 klien lewat terowongan.
`PersistentKeepalive`	Mengirim paket berkala agar koneksi tetap hidup di balik NAT.

```
sudo ufw allow 51820/udp     # tanpa ini handshake gagal bila UFW aktif
sudo wg-quick up wg0
sudo wg show
```

Jebakan dunia nyata

Pada server yang dikelola lewat SSH, *full tunnel* dapat membelokkan rute sehingga sesi SSH terputus. Pada sisi server juga perlu IP forwarding dan NAT bila server meneruskan lalu lintas klien. Izin berkas `wg0.conf` sebaiknya 600.

Bacaan 7. Membaca Log dan Menamai Ancaman

Serangan simulasi memakai dua teknik dalam MITRE ATT&CK: **T1110 (Brute Force)**, yaitu menebak kata sandi berulang, dan **T1046 (Network Service Discovery)**, yaitu memindai port. Dalam insiden, kumpulkan fakta (IP, waktu, pengguna, jenis serangan), ambil tindakan, dan **jangan menghapus bukti**.

```
sudo grep "Failed password" /var/log/auth.log | head
sudo lastb | head
sudo journalctl -u ssh --since today | tail -n 20
sudo grep "UFW BLOCK" /var/log/ufw.log | wc -l
```

LAMPIRAN B

Lembar Kerja Peserta Didik (LKPD)

Nama / Kelas	..... / .....
Pasangan (Pilot / Navigator)	..... / .....
Tanggal	.....

LKPD-1: Mengenal Ancaman dan Mengunci Pintu Masuk (Pertemuan 1)

A. Pengamatan kondisi awal (Misi 1). Skor host awal: ..... Tingkat perlindungan: .....

Port / proto	Layanan	Mengapa berisiko bila terbuka?	Kontrol yang menutup
22/tcp			
23/tcp			
631/tcp			

B. Padankan dengan analogi. Tulis analogi sehari-hari dengan kata-katamu sendiri.

Istilah	Analogi buatanmu	Fungsi teknis sebenarnya
Firewall		
VPN		
Kunci publik SSH		
fail2ban		

C. Catatan Misi 2 dan 3.

Langkah	Perintah / aksi	Artinya (kata-kata sendiri)	Skor sebelum	Skor sesudah

D. Pertanyaan refleksi.

1. Mengapa port 22/tcp harus diizinkan sebelum firewall diaktifkan? Apa akibatnya di server nyata bila terbalik?
2. Mengapa login sandi tidak boleh dimatikan sebelum kunci publik teruji?
3. Kontrol mana yang paling menaikkan skor pada pertemuan ini, dan mengapa menurutmu demikian?

LKPD-2: Pertahanan Berlapis dan WireGuard (Pertemuan 2)

A. Tabel kontrol (Misi 4 sampai 6).

Kontrol	Perintah / aksi	Ancaman yang ditutup	Skor +	Bukti (log / layar)
fail2ban				
Hardening kernel				
Matikan layanan				
Pembaruan otomatis / auditd				
Kebijakan sandi				
AppArmor				

B. Terowongan WireGuard (Misi 7). Skor host setelah semua kontrol: ..... Status wg0: .....

Parameter	Nilai yang kamu amati / atur	Fungsinya
Address		
ListenPort		
AllowedIPs		
PersistentKeepalive		

C. Diskusi untung-rugi *full tunnel*.

Keuntungan	Kerugian / risiko	Keputusan kelompok dan alasan

D. Peta lapisan. Tuliskan kontrol pada lapisan yang sesuai: Jaringan .....; Akses .....; Sistem .....; Deteksi dan pemeliharaan .....

LKPD-3: Investigasi Insiden dan Remediasi (Pertemuan 3)

A. Analisis cuplikan log. Alamat IP memakai rentang dokumentasi (TEST-NET), bukan alamat nyata.

```
Nov 29 02:14:07 srv-prod-01 sshd[1421]: Failed password for root from 203.0.113.45 port 51234
Nov 29 02:14:09 srv-prod-01 sshd[1423]: Failed password for admin from 203.0.113.45 port 51236
Nov 29 02:14:12 srv-prod-01 sshd[1425]: Failed password for ubuntu from 203.0.113.45 port 51240
Nov 29 02:14:15 srv-prod-01 sshd[1427]: Failed password for oracle from 203.0.113.45 port 51244
Nov 29 02:14:18 srv-prod-01 fail2ban.actions: NOTICE [sshd] Ban 203.0.113.45
Nov 29 02:21:40 srv-prod-01 kernel: [UFW BLOCK] SRC=198.51.100.7 PROTO=TCP DPT=3306
Nov 29 02:21:41 srv-prod-01 kernel: [UFW BLOCK] SRC=198.51.100.7 PROTO=TCP DPT=5432
```

Pertanyaan	Jawabanmu
Alamat IP penyerang dan pengguna yang dicoba?	
Berapa percobaan dan dalam berapa lama?	
Teknik ATT&CK yang cocok (T1110 / T1046)?	
Kontrol mana yang menghentikan serangan?	
Tindakan lanjutan yang kamu sarankan (tanpa menghapus bukti)?	

B. Rencana remediasi berprioritas risiko. Urutkan temuan dari risiko Kritis ke Rendah.

Temuan	Risiko	Perbaikan	Verifikasi	Rollback

C. Refleksi tim. Pelajaran terpenting kelompok kami: .....

LAMPIRAN C

Rubrik Penilaian Unjuk Kerja

Rubrik dipakai untuk menilai laporan audit dan penjelasan lisan. Setiap kriteria dinilai pada empat level; jumlah skor maksimal 20.

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 memberi 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: Aliyudin (2026), Naskah Inovasi SecOps Lab, Lampiran A.

Lembar Rekap Penilaian Kelas

No	Nama peserta didik	Praktik 30%	Laporan 30%	Kuis 25%	Refleksi 15%	Nilai akhir	Level
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							

LAMPIRAN D

Instrumen Kuis dan Kunci Jawaban

Instrumen ini melengkapi kuis acak di simulator (10 soal dari bank 30 butir pada 13 topik) dan dapat dipakai sebagai kuis awal, ulangan, atau remediasi. Kisi-kisi singkat: SSH (3), firewall (1), layanan tak perlu (1), fail2ban (1), WireGuard (2), kerangka ancaman (1), izin berkas (1); ditambah tiga uraian.

A. Pilihan Ganda (10 soal x 10 poin)

1. Urutan paling aman saat mengaktifkan UFW pada server yang dikelola lewat SSH adalah ...

A. Aktifkan UFW, lalu izinkan 22/tcp
B. Izinkan 22/tcp, lalu aktifkan UFW
C. Matikan SSH, lalu aktifkan UFW
D. Restart server, lalu aktifkan UFW

2. Tujuan utama melarang login root via SSH adalah ...

A. Mempercepat koneksi
B. Menghemat penyimpanan log
C. Mencegah brute force langsung pada akun superuser dan menerapkan least privilege
D. Mengganti port SSH

3. Sebelum menonaktifkan login sandi SSH, hal yang harus dipastikan lebih dulu adalah ...

A. Kunci publik terpasang dan login dengan kunci teruji pada sesi terpisah
B. Firewall dimatikan
C. Server direstart dua kali
D. Semua pengguna memakai sandi yang sama

4. Perintah sshd -t berfungsi untuk ...

A. Menghapus sesi SSH lama
B. Membuat pasangan kunci baru
C. Menutup port 22
D. Memeriksa sintaks konfigurasi sshd sebelum layanan dimulai ulang

5. Fungsi utama fail2ban adalah ...

A. Mengenkripsi lalu lintas jaringan
B. Memantau log dan memblokir IP setelah beberapa kali gagal login
C. Memperbarui paket keamanan
D. Membatasi proses dengan profil MAC

6. Port dan protokol lazim WireGuard adalah ...

A. 22/tcp
B. 443/tcp
C. 51820/udp
D. 23/tcp

7. AllowedIPs = 0.0.0.0/0 pada klien WireGuard berarti ...

A. Seluruh lalu lintas IPv4 klien dialirkan melalui terowongan (full tunnel)
B. Hanya jaringan lokal yang diizinkan
C. Terowongan dinonaktifkan
D. Semua port otomatis terbuka di server

8. Telnet sebaiknya dimatikan karena ...

A. Terlalu hemat memori
B. Hanya berjalan pada UDP
C. Tidak dapat dipakai pada Linux
D. Mengirim data, termasuk sandi, tanpa enkripsi

9. Teknik MITRE ATT&CK T1110 pada simulator mewakili ...

A. Network Service Discovery
B. Brute Force
C. Phishing
D. Data Exfiltration

10. Izin ideal berkas /etc/shadow pada simulator adalah ...

A. 777
B. 644
C. 640
D. 600 untuk semua pengguna

B. Uraian (3 soal, total 20 poin)

1. Jelaskan mengapa firewall saja tidak cukup untuk mengamankan server. Sebutkan sekurang-kurangnya tiga kontrol lain beserta fungsinya (4 poin).
2. Perhatikan cuplikan log pada LKPD-3. Identifikasi pelaku, teknik ATT&CK yang sesuai, kontrol yang menghentikan serangan, dan tindakan lanjutan yang tepat (10 poin).
3. Seorang administrator ingin memakai WireGuard dengan AllowedIPs 0.0.0.0/0 pada server yang ia kelola lewat SSH. Jelaskan risikonya dan langkah pencegahannya (6 poin).

C. Kunci Jawaban dan Pedoman Penskoran

No	Kunci	No	Kunci	No	Kunci
1	B	5	B	9	B
2	C	6	C	10	C
3	A	7	A		
4	D	8	D		

Uraian	Poin kunci	Skor maks
1	Konsep defense in depth (1). Tiga kontrol lain dengan fungsi tepat, misalnya kunci publik menghalangi tebak sandi, fail2ban memblokir penebak yang gigih, auditd memberi jejak, pembaruan menutup celah (3).	4
2	Penyerang 203.0.113.45 mencoba pengguna root, admin, ubuntu, oracle (2). Sekitar empat percobaan dalam sekitar 11 detik (1). Teknik T1110 Brute Force (2). Dihentikan fail2ban (Ban) (1). IP 198.51.100.7 memindai port 3306 dan 5432, teknik T1046, diblokir UFW (2). Tindakan: simpan log sebagai bukti, jangan dihapus; pastikan login root dilarang dan kunci publik diwajibkan; pantau dan laporkan (2).	10
3	Seluruh lalu lintas (termasuk sesi SSH) dapat dibelokkan ke terowongan sehingga sesi terputus dan administrator terkunci (2). Pencegahan: pertahankan sesi cadangan atau akses konsol, uji pada mesin virtual, batasi AllowedIPs ke jaringan yang diperlukan, cadangkan konfigurasi dan siapkan rollback (4).	6

Nilai akhir kuis = (jumlah poin PG + jumlah poin uraian) / 120 x 100, atau gunakan hanya PG (jumlah poin dari 100) bila waktu terbatas.

LAMPIRAN E

Instrumen Refleksi, Angket, dan Observasi

1. Jurnal Refleksi Peserta Didik

Pertanyaan refleksi	Jawabanku
Hal paling berkesan dan paling sulit hari ini?	
Kesalahan yang kubuat dan pelajarannya?	
Apa yang berubah dari cara saya memandang keamanan?	
Langkah tindak lanjutku?	

2. Penilaian Diri

Saya dapat ...	Belum	Mulai	Mampu	Mahir
menjelaskan mengapa firewall, SSH aman, dan fail2ban saling melengkapi	[ ]	[ ]	[ ]	[ ]
menerapkan urutan aman SSH dan firewall	[ ]	[ ]	[ ]	[ ]
mengonfigurasi dan memverifikasi terowongan WireGuard simulasi	[ ]	[ ]	[ ]	[ ]
membaca log dan mengaitkannya dengan T1110 dan T1046	[ ]	[ ]	[ ]	[ ]
menyusun laporan audit dan memprioritaskan remediasi	[ ]	[ ]	[ ]	[ ]
menaati batas etika dan hukum dalam praktik keamanan	[ ]	[ ]	[ ]	[ ]

3. Angket Keterlibatan dan Kenyamanan Belajar (skala Likert 1 sampai 5)

1 = sangat tidak setuju, 5 = sangat setuju. Target rerata usulan: minimal 4,0 (perlu dikalibrasi).

Pernyataan	1	2	3	4	5
Saya berani mencoba karena kesalahan di simulator tidak merusak sistem nyata.					
Saya langsung melihat dampak setiap tindakan pada skor, log, dan port.					
Penjelasan “Ibaratnya” dan “Artinya” membantu saya memahami istilah.					
Saya memahami mengapa setiap kontrol dibutuhkan, bukan hanya perintahnya.					
Belajar berpasangan membuat saya lebih paham.					
Pembelajaran ini terasa menantang namun menyenangkan.					
Saya lebih percaya diri untuk mempraktikkannya pada mesin virtual terisolasi.					
Saya memahami batas etika dan hukum dalam keamanan siber.					

4. Lembar Observasi Guru (Formatif)

Indikator pengamatan	Ya	Sebagian	Belum	Catatan
Peserta membaca “Artinya” sebelum menjalankan perintah	[ ]	[ ]	[ ]	
Peserta memverifikasi hasil (sshd -T, ss, ufw status)	[ ]	[ ]	[ ]	
Pilot dan Navigator bergantian dan berdiskusi	[ ]	[ ]	[ ]	
Peserta menjelaskan alasan, bukan hanya langkah	[ ]	[ ]	[ ]	
Peserta menaati kontrak belajar etika	[ ]	[ ]	[ ]	

LAMPIRAN F

Kontrak Belajar: Kode Etik Keamanan Siber

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. Meski demikian, 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.

Saya yang bertanda tangan di bawah ini berjanji:

1. Hanya menguji sistem milik sendiri atau yang telah diberi izin tertulis; jaringan sekolah dan milik orang lain tidak akan saya jadikan sasaran uji.
2. Melakukan praktik pada mesin virtual yang terisolasi dari jaringan produksi.
3. Melaporkan kerentanan yang saya temukan secara bertanggung jawab kepada pemilik sistem.
4. Melindungi data pribadi; tidak memasukkan kata sandi atau kunci sungguhan ke simulator.
5. Memakai pengetahuan untuk melindungi, bukan merugikan.

Garut, ... 2026

Peserta didik,	Guru Mata Pelajaran,
(.....)	**Aliyudin**

LAMPIRAN G

Kamus Istilah dan Analogi

Istilah	Arti singkat	Ibaratnya
Hardening	Memperkuat konfigurasi sistem agar lebih sulit ditembus.	Memasang gembok, teralis, dan alarm pada rumah.
Firewall (UFW)	Penyaring lalu lintas masuk dan keluar berdasarkan aturan.	Satpam gerbang yang memeriksa siapa boleh masuk.
VPN	Jalur komunikasi terenkripsi antara dua titik.	Terowongan tertutup di bawah jalan umum.
SSH	Protokol administrasi jarak jauh yang terenkripsi.	Pintu khusus untuk petugas pemeliharaan gedung.
Kunci publik	Autentikasi dengan pasangan kunci, bukan sandi.	Gembok yang hanya terbuka oleh satu anak kunci pribadimu.
Brute force	Menebak sandi secara berulang dan otomatis.	Mencoba semua kombinasi gembok angka satu per satu.
Port	Nomor “pintu” layanan pada sebuah alamat IP.	Nomor loket di sebuah kantor.
fail2ban	Memblokir IP yang berulang kali gagal login.	Satpam yang mengusir tamu setelah tiga kali salah masuk.

Istilah	Arti singkat	Ibaratnya
auditd	Daemon pencatat akses berkas dan perubahan penting.	Kamera CCTV dan buku tamu.
AppArmor	Kontrol akses wajib yang membatasi proses pada profil tertentu.	Aturan bahwa tukang hanya boleh masuk ke ruangan kerjanya.
sysctl	Pengaturan parameter kernel Linux.	Panel pengaturan mesin di ruang kontrol.
Least privilege	Memberi hak akses seperlunya saja.	Kunci kamar hanya untuk penghuni kamar itu.
Defense in depth	Banyak lapisan pertahanan yang saling melengkapi.	Pagar, gerbang, pintu, dan brankas.
Attack surface	Seluruh titik yang dapat diserang.	Jumlah pintu dan jendela yang terbuka.
Handshake	Proses awal dua pihak membuktikan identitas dan menyepakati kunci.	Jabat tangan dan saling menunjukkan tanda pengenal.
CVE	Penomoran publik untuk kerentanan yang sudah diketahui.	Nomor laporan resmi untuk sebuah lubang di pagar.

LAMPIRAN H

Templat Laporan Audit Tim Biru

Laporan audit dihasilkan dari simulator dan dilengkapi analisis kelompok. Laporan menjadi produk unjuk kerja yang dinilai dengan rubrik (Lampiran C).

Bagian	Isi yang diharapkan	Kriteria rubrik terkait
1. Identitas dan ringkasan	Nama tim, tanggal, skor awal dan akhir, tingkat perlindungan, jumlah misi selesai.	Ketepatan konfigurasi
2. Kontrol aktif	Daftar kontrol yang sudah diterapkan, fungsi, dan risiko yang ditutup.	Pemahaman konsep
3. Analisis insiden	IP, pengguna, waktu, jenis serangan, teknik ATT&CK, kontrol yang menghentikan, tindakan lanjutan.	Analisis log dan insiden
4. Temuan tersisa	Diurutkan menurut risiko beserta acuan CIS atau NIST (versi disederhanakan).	Pemahaman konsep
5. Rencana remediasi	Untuk tiap temuan: perintah perbaikan, verifikasi, dan rollback; urutan aman termasuk backup dan sshd -t.	Verifikasi dan keselamatan kerja
6. Refleksi tim	Pelajaran terpenting, kesulitan, dan rekomendasi; pernyataan kepatuhan pada kode etik.	Etika dan kolaborasi

Catatan jujur tentang batas simulasi

Pemetaan CIS dan NIST pada simulator adalah acuan belajar yang disederhanakan, bukan klaim kepatuhan terhadap standar. Nomor kontrol dapat berbeda antarversi, dan distribusi Linux di dunia kerja bisa memakai perintah yang berbeda. Rujuk sumber resmi untuk praktik nyata.

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*. 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.

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

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).

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.

Aliyudin. (2026). *Naskah inovasi pembelajaran SecOps Lab: Simulator interaktif keamanan siber berbasis peramban untuk pembelajaran Linux hardening dan WireGuard VPN dalam kerangka pembelajaran mendalam*. SMKS Ciledug Al Musaddadiyah.

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.