



**LOMBA KOMPETENSI SISWA (LKS)
SEKOLAH MENENGAH KEJURUAN
TINGKAT KABUPATEN TASIKMALAYA
TAHUN 2026**

**NASKAH SOAL
*(Terbuka / ~~Tertutup~~)**

**Bidang Lomba
CYBER SECURITY**





LOMBA KOMPETENSI SISWA SEKOLAH MENENGAH KEJURUAN

TINGKAT KABUPATEN TASIKMALAYA TAHUN 2026



I. Pendahuluan

Penyelenggaraan Lomba Kompetensi Cybersecurity Jawa Barat bagi siswa/i Sekolah Menengah Kejuruan (SMK) seluruh Jawa Barat adalah sebagai wujud nyata salah satu upaya dalam pengembangan sumber daya manusia yang dilakukan oleh Pemerintah melalui Dinas Pendidikan Provinsi Jawa Barat untuk mengasah dan menguji kemampuan siswa khususnya di bidang Cybersecurity dalam memahami teknologi serta perkembangannya.

II. Tujuan

1. Mendorong SMK dalam peningkatan kualitas pelaksanaan Kegiatan Belajar Mengajar (KBM) yang mengacu kepada Standar Kompetensi Kerja Nasional Indonesia (SKKNI) kompetensi keahlian analisis keamanan siber dan sistem operasi.
2. Mengasah kemampuan siswa/i dalam menganalisa permasalahan sistem dan keamanan siber yang ada.
3. Meningkatkan kemampuan siswa/i dalam mencari solusi dari permasalahan sistem dan keamanan siber yang diberikan

III. Peserta

Peserta adalah siswa SMK dengan kriteria sebagai berikut:

1. Tercatat Siswa Aktif SMK Negeri atau Swasta Tahun Pelajaran 2025/2026.
2. Siswa yang pernah mengikuti LKS SMK tingkat nasional pada tahun sebelumnya tidak diperkenankan untuk menjadi peserta

IV. Materi Lomba

Jenis kegiatan yang dilombakan adalah Tes Praktek dan Tes Wawancara, yaitu:

- a. Tes Praktek (450 Menit)
Meliputi tes kemampuan mengenai:
 1. Hardening Operating System (240 Menit)
 2. Capture the Flag (210 Menit)



**LOMBA KOMPETENSI SISWA
SEKOLAH MENENGAH KEJURUAN
TINGKAT KABUPATEN TASIKMALAYA TAHUN 2026**



b. Tes Wawancara (30 Menit)

Meliputi tes pengetahuan
tentang:

1. Teori Operating System
2. Teori Keamanan Siber
3. Penjelasan mengenai Kemampuan Teknis pada Tes Praktek

V. Nilai dan Bobot Penilaian

Nilai maksimum dan bobot:

1. Tes Praktek, nilai maksimum 100, bobot 60%
2. Tes Wawancara, nilai maksimum 100, bobot 40%

$$\text{Nilai Akhir (NA)} = (\text{Tes Praktek} \times 60\%) + (\text{Tes Wawancara} \times 40\%)$$

VI. Aspek Penilaian

- a. Aspek yang dinilai untuk tes praktek yaitu kemampuan, keterampilan dan sikap meliputi:

No	Aspek Yang Dinilai	Kriteria	Penilaian			
			Ya			Tidak
			100 - 90	80,9 - 80	70,9 - 70	<70
1	Kemampuan Hardening Sistem Operasi	OS, E-mail, Port, IDS, MySQL, Account, VPN, Forensic				
2	Kemampuan Capture the Flag	Steganography, Cryptography, Network Packet, Web Exploit, Binary Exploit				
Jumlah nilai						
Nilai Akhir						

Nilai akhir maksimum untuk tes praktek yaitu 100.



LOMBA KOMPETENSI SISWA SEKOLAH MENENGAH KEJURUAN

TINGKAT KABUPATEN TASIKMALAYA TAHUN 2026



- b. Aspek yang dinilai untuk tes wawancara yaitu penguasaan pengetahuan yang meliputi:

No	Aspek Yang Dinilai	Kriteria	Penilaian			
			Ya			Tidak
			100-90	80,9 - 80	70,9 - 70	<70
1	Kemampuan Hardening Sistem Operasi	Kemampuan menjelaskan teori teknologi hardening				
		Kemampuan menjelaskan tahapan yang telah dilakukan ketika tes praktek dilaksanakan				
		Kemampuan menjelaskan analisa dari persoalan yang diberikan				
2	Kemampuan Capture the Flag	Kemampuan menjelaskan teori teknologi				
		Kemampuan menjelaskan tahapan dan solusi yang ditemukan ketika tes praktek dilaksanakan				
	Jumlah nilai					
	Nilai Akhir					

Nilai akhir maksimum untuk tes wawancara yaitu 100.

VII. Tim Penguji

Tim Juri terdiri dari Praktisi/Akademis/Profesional dalam bidang Cybersecurity dan Dosen Matakuliah Sistem Informasi yang ditetapkan dengan Surat Kepala Dinas Pendidikan Provinsi Jawa Barat.

VIII. Kriteria Pemenang Lomba

Juara Lomba adalah peserta yang memiliki nilai akhir tertinggi dari seluruh nilai para peserta lomba. Tes Praktek dan Tes Wawancara telah mencakup ketepatan, kelengkapan dan kecekatan dalam menjawab setiap soal yang diberikan. Para Juara ditentukan langsung oleh Juri meliputi: Juara I, II dan III

IX. Tata Tertib Lomba

Peserta diharapkan:

1. Ruangan yang digunakan ketika pelaksanaan hanya ada peserta saja, pembimbing hanya boleh menemani ketika lomba belum dimulai.
2. Menjawab soal yang memiliki poin masing-masing dalam penyelesaiannya.
3. Mematuhi seluruh tata tertib yang telah ditentukan oleh panitia dan juri, apabila melanggar akan dikenakan sanksi.



**LOMBA KOMPETENSI SISWA
SEKOLAH MENENGAH KEJURUAN
TINGKAT KABUPATEN TASIKMALAYA TAHUN 2026**



X. Penutup

Hal-hal yang belum tercantum dalam lembar informasi ini akan diinformasikan pada waktu rapat teknis (technical meeting).

XI. Kisi-kisi Lomba

1. Hardening

Terdiri dari 8 soal yang berfokus pada peningkatan keamanan Sistem Operasi, Jaringan Komputer, dan Aplikasi, yaitu:

a. Hardening Sistem Operasi

1. Nonaktifkan login root via SSH
2. Ganti port default SSH ke 2202
3. Aktifkan firewall dan hanya izinkan port:
 - 2202 (SSH baru)
 - 80 (HTTP)
 - 443 (HTTPS)
4. Nonaktifkan dan matikan layanan cups dan avahi-daemon (jika ada)
5. Buat user baru bernama adminlks dengan hak sudo tanpa password
6. Pasang dan aktifkan fail2ban untuk SSH
7. Aktifkan auditd dan pastikan log audit berjalan

b. Keamanan Komunikasi E-mail

1. Install GnuPG (GPG):
2. Pastikan sistem memiliki gpg versi terbaru.



LOMBA KOMPETENSI SISWA SEKOLAH MENENGAH KEJURUAN

TINGKAT KABUPATEN TASIKMALAYA TAHUN 2026



3. Buat sepasang key PGP:

Nama: LKS SMK

Email: lks@smkprovinsi.id

Key type: RSA & RSA

Ukuran kunci: 4096 bit

Expiry: 0 (never expire)

4. Ekspor public key Anda ke file public-lks.asc

5. Buat file pesan pesan.txt berisi teks:

Ini adalah pesan rahasia untuk panitia LKS.

6. Enkripsi file tersebut menggunakan public key Anda sendiri.
Simpan hasilnya sebagai pesan.txt.gpg

7. Buat digital signature terhadap file pesan.txt dan hasilkan file
pesan.txt.sig

8. Verifikasi kembali signature yang telah Anda buat

c. Keamanan Port dan Jaringan Server

1. Pasang firewall dan konfigurasi rule hanya untuk:

SSH (port 2202)

HTTP (port 80)

HTTPS (port 443)

2. Semua port selain itu harus ditutup.

3. Nonaktifkan ICMP/ping agar tidak bisa diping dari luar.

4. Pasang dan aktifkan TCP Wrappers (hosts.deny dan hosts.allow)

5. Tolak semua default dari ALL

6. Hanya izinkan akses SSH dari 192.168.0.0/24

7. Pasang dan jalankan psad atau portsentry



LOMBA KOMPETENSI SISWA SEKOLAH MENENGAH KEJURUAN

TINGKAT KABUPATEN TASIKMALAYA TAHUN 2026



-
8. Untuk mendeteksi port scan
 9. Simulasikan satu port scan menggunakan nmap (ke localhost)
- d. Analisa Intrusion Detection System (IDS) Snort
1. Pasang Snort pada Ubuntu (versi terbaru).
 2. Buat aturan Snort sederhana untuk mendeteksi port scan pada port 80 dan 22.
 3. Jalankan Snort dalam mode IDS pada interface jaringan utama (eth0 atau ens33).
 4. Lakukan simulasi serangan port scan menggunakan nmap ke localhost.
 5. Periksa log Snort dan identifikasi hasil deteksi port scan.
 6. Laporkan hasil serangan yang terdeteksi dan buat ringkasan singkat (2-3 kalimat) pada file laporan-snort.txt.
- e. Keamanan MySQL pada XAMPP
1. Pastikan XAMPP sudah terpasang dan MySQL berjalan.
 2. Nonaktifkan akses root MySQL dari host selain localhost.
 3. Buat user baru bernama lksuser dengan password yang kuat, dan beri hak akses terbatas hanya pada database lksdb.
 4. Ubah password root MySQL ke password yang kompleks.
 5. Matikan user anonymous di MySQL.
 6. Nonaktifkan fitur remote login root MySQL (jika belum).
 7. Lakukan audit konfigurasi MySQL menggunakan perintah `mysql_secure_installation`.
 8. Cek apakah port MySQL (3306) hanya terbuka untuk localhost menggunakan firewall.



LOMBA KOMPETENSI SISWA SEKOLAH MENENGAH KEJURUAN

TINGKAT KABUPATEN TASIKMALAYA TAHUN 2026



-
9. Buat laporan singkat tentang langkah-langkah hardening yang sudah dilakukan.
- f. Keamanan Akun Ubuntu
1. Tampilkan daftar user aktif di sistem (bukan user sistem).
 2. Periksa apakah ada user yang tidak memiliki password atau menggunakan password kosong.
 3. Cek policy password minimum (umur password, panjang, kompleksitas) menggunakan chage dan pam config.
 4. Aktifkan 2 User yang sudah disediakan untuk diamankan, 2 user dinonaktifkan
 5. Pasang dan konfigurasi faillock untuk memblokir login setelah 5 kali gagal percobaan selama 10 menit.
 6. Aktifkan autentikasi dua faktor (2FA) untuk user tertentu (misal adminlks).
 7. Buat laporan singkat (maksimal 1 paragraf) tentang hasil analisis dan langkah perbaikan yang sudah dilakukan.
- g. Keamanan Koneksi OpenVPN Server
1. Install OpenVPN dan Easy-RSA pada Ubuntu server.
 2. Buat Public Key Infrastructure (PKI) untuk OpenVPN menggunakan Easy-RSA:
 3. Generate CA (Certificate Authority)
 4. Generate server certificate & key
 5. Generate client certificate & key
 6. Generate Diffie-Hellman parameters
 7. Konfigurasi OpenVPN server:
 8. Gunakan protokol UDP port 1194
 9. Konfigurasi routing agar client bisa akses jaringan lokal 10.8.0.0/24

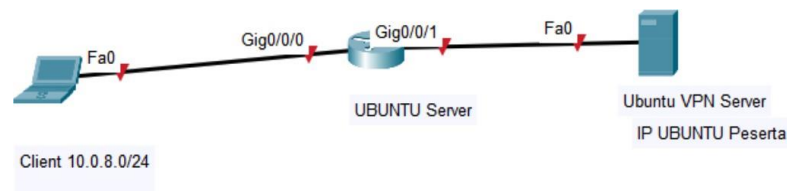


LOMBA KOMPETENSI SISWA SEKOLAH MENENGAH KEJURUAN

TINGKAT KABUPATEN TASIKMALAYA TAHUN 2026



10. Aktifkan IP forwarding di kernel
11. Buat file konfigurasi client .ovpn yang dapat dipakai untuk koneksi.
12. Jalankan OpenVPN server dan tes koneksi client dengan konfigurasi yang sudah dibuat.
13. Pastikan koneksi client terhubung dan IP client dapat akses jaringan lokal secara aman.



Gambar Topologi VPN Server

h. Analisis Forensik Ubuntu OS

1. Cari dan tampilkan log login terakhir menggunakan last dan lastb.
2. Analisa file log auth.log di /var/log untuk aktivitas login yang mencurigakan (misal: percobaan login gagal berulang).
3. Cari file-file yang diubah atau dibuat dalam 24 jam terakhir di file anda.
4. Periksa proses berjalan yang tidak biasa atau mencurigakan (ps aux + grep).
5. Cari file yang memiliki permission tidak biasa (misal: file skrip yang bisa dijalankan oleh semua orang).
6. Buat laporan singkat (maks 1 paragraf) berisi ringkasan hasil analisis dan rekomendasi tindakan keamanan.



LOMBA KOMPETENSI SISWA SEKOLAH MENENGAH KEJURUAN

TINGKAT KABUPATEN TASIKMALAYA TAHUN 2026



2. Capture the Flag

Terdiri dari 7 soal yang berfokus pada pencarian pesan rahasia dari teknologi keamanan siber, yaitu:

a. Steganografi

Peserta akan mencari FLAG di dalam sebuah file untuk dapat ditemukan/dipecahkan. File bisa berupa apa saja (Gambar, Text, Audio, dst.)

b. Cryptography

Peserta akan mencari FLAG di dalam sebuah text berupa Ciphertext yang perlu ditemukan pesan rahasianya

c. Network Packet

Peserta akan mencari FLAG dari sebuah file capture untuk ditemukan pesan rahasianya

d. Web Exploitation

Peserta akan mencari FLAG dalam suatu website yang berisikan kode Base64

e. Binary Exploitation

Peserta akan mencari FLAG dalam sebuah Binary yang telah disediakan