Puspresnas
Pusat Prestasi Nasional

LKS SMK TINGKAT NASIONAL 30

Member Of worldskills

DESKRIPSI TEKNIS

LOMBA KOMPETENSI SISWA (LKS)-SMK TINGKAT NASIONAL XXX TAHUN 2022

BIDANG LOMBA

Teknologi Keamanan Siber
(Cyber Security)

Teknologi Informasi & Komunikasi

DESKRIPSI TEKNIS

TEKNOLOGI KEAMANAN SIBER

(CYBER SECRUITY)

KELOMPOK
TEKNOLOGI INFORMASI DAN KOMUNIKASI

LOMBA KOMPETENSI SISWA SEKOLAH MENENGAH

KEJURUANTINGKAT NASIONAL XXX

TAHUN 2022

KATA PENGANTAR

Peserta didik Sekolah Menengah Kejuruan (SMK) yang merupakan aset bangsa harus berstandar nasional maupun internasional sesuai dengan visi Indonesia tahun 2045 Pembangunan manusia dan penguasaan IPTEK (Ilmu Pengetahuan dan Teknologi) dalam rangka peningkatan taraf pendidikan masyarakat Indonesia secara merata harus sejalan dengan visi Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi. Pusat Prestasi Nasional sebagai unit pelaksana Kementerian Pendidikan, Kebudayaan, Riset dan Teknologi, salah satu tugas dan fungsinya menyelenggarakan Lomba Kompetensi Peserta didik Sekolah Menengah Kejuruan (LKS-SMK)

Sejalan dengan tugas dan fungsi diatas, Pusat Prestasi Nasional menyelenggarakan Lomba kompetensi siswa SMK (LKS-SMK) sejumlah 47 bidang lomba, dengan 6 area kategori diantaranya kelompok konstruksi, teknologi bangunan dan Agribisnis, kelompok Seni Kreatif & Fashion kelompok Teknologi Informasi & Komunikasi, kelompok Teknologi Manufaktur dan Rekayasa, kelompok Kelompok Pariwisata & Layanan Sosial dan Individual dan kelompoktransportasi yang melibatkan peserta didik terbaik dibidangnya pada tiap provinsi. Mengingat masih berlangsungnya pandemi Covid-19, LKS dilaksanakan secara daring/Online.

Dukungan dan peran serta dari kalangan dunia usaha dan dunia industri (DU/DI), Perguruan Tinggi, Balai Latihan Kerja (BLK) dan lainnya sebagai narasumber, pelatih, juri dan teknisi sangat dibutuhkan agar pelaksanaan LKS SMK dari 34 Provinsi serta kegiatan pendukung lainnya berjalan dengan baik. Sebagai panduan/acuan semua pihak yang terlibat dalam pelaksanaan LKS-SMK , maka disusun “Petunjuk Teknis LKS-SMK Tingkat Nasional ke 30 Tahun 2022 secara daring”. Rangkaian kegiatan LKS-SMK Tingkat Nasional meliputi lomba- lomba dan kegiatan pendukung, yang antara lain pameran produk hasil karya Peserta didik SMK, seminar, Job Matching, dan proses sertifikasi. Harapannya kegiatan pendukung tersebut akan memberikan motivasi Peserta didik SMK untuk lebih bisa meningkatkan kepercayaan diri

Sehubungan dengan hal tersebut, Pusat Prestasi Nasional, Kementerian Pendidikan, Kebudayaan, Riset dan Teknologi berperan dalam mendukung pengembangan kualitas SMK dalam mengikuti perkembangan IPTEK dan memenuhi Visi Indonesia 2045. LKS-SMK Tingkat Nasional Tahun 2022 merupakan salah satu kegiatan yang mendorong semangat berprestasi peserta didik SMK dalam rangka mempromosikan lulusan SMK yang berprestasi.

Kami sampaikan terima kasih kepada pihak yang telah berperan serta dalam penyusunan dokumen Petunjuk Teknis LKS-SMK Tingkat Nasional ke 30 Tahun 2022, semoga Tuhan YME membalas kebaikan semua pihak.

Jakarta, 18 February 2022
Plt. Kepala, Pusat Prestasi Nasional

Asep Sukmayadi
NIP 197206062006041001

DAFTAR ISI

DAFTAR ISI 1

PENDAHULUAN **6**

1. NAMA DAN DESKRIPSI BIDANG LOMBA 6

1.2 Isi Deskripsi Teknis 6

1.2.1 Kompetensi Keahlian Peserta Lomba 7

1.2.2 Karakter Kerja Bidang Lomba 7

1.3 Dokumen Terkait 8

2. SPESIFIKASI TERHADAP STANDAR NASIONAL (Standar Kompetensi Bidang Lomba) 8

2.1. Ketentuan umum 8

2.2. Spesifikasi Kompetensi LKS-SMK 8

3. SISTEM PENILAIAN 21

3.1. Petunjuk Umum 21

3.2. Kriteria Toleransi Pengukuran 21

3.3. Kriteria Penilaian 21

3.3.1. Penilaian Judgement 21

3.3.2. Penilaian measurement 21

3.3.3. Komposisi Penilaian Judgement dan Measurement 21

3.5. Sub Kriteria 22

3.6 Keseluruhan Penilaian 22

3.7. Prosedur Penilaian 22

3.1. Skema Penilaian 22

4. FORMAT/STRUKTUR PROYEK UJI 23

4.1. Petunjuk Umum 23

4.2. Persyaratan Uji 23

4.3. Sirkulasi Proyek Uji 24

4.4. Perubahan Proyek Uji 24

5. DAFTAR ALAT 24

5.1 Ketentuan Umum 24

5.2 Daftar Alat para Peserta 25

6. DAFTAR BAHAN 28

6.1 BAHAN PENUNJANG 28

7. LAYOUT DAN BAHAN LAYOUT 29

8. JADWAL BIDANG LOMBA 30

9. KEBUTUHAN LAIN dan SPESIFIKASINYA 31

9.1 Kebutuhan ini untuk kebutuhan juri, diantaranya: 31

9.2 Kebutuhan Juri untuk menilai, diantaranya: 31
9.3 Kapasitas listrik yang dibutuhkan: 32
10. Rekomendasi Juri **Error! Bookmark not defined.**

PENDAHULUAN

1. NAMA DAN DESKRIPSI BIDANG LOMBA

Cyber Security

1.1 Deskripsi Bidang Lomba

Lomba Cyber Security merupakan acara kompetisi keamanan siber yang secara khusus fokus pada aspek operasional pengelolaan, dan perlindungan layanan dan infrastruktur sistem informasi. Para peserta tidak hanya mendapatkan kesempatan untuk menguji pengetahuan mereka dalam bidang keamanan siber, mereka juga akan mendapatkan kesempatan untuk membangun hubungan dengan para profesional industri Teknologi Informasi. Lomba Cyber Security menyediakan kesempatan bagi para profesional dibidang keamanan siber untuk saling berinteraksi dan membahas berbagai tantangan keamanan dan operasional Teknologi Informasi dan Siber.kemampuan siswa di dalam bidang cyber security.

1.2 Isi Deskripsi Teknis

Dalam beberapa tahun terakhir, kita telah menyaksikan pertumbuhan transaksi bisnis online yang pesat, serta adopsi Internet of Things (IoT) dan komputasi awan yang cepat. Ditambah dengan ancaman terus-menerus dari para peretas, para profesional keamanan dunia maya sekarang banyak diminati secara global.

Seorang Analis Keamanan Informasi bekerja untuk melindungi jaringan sistem komputer organisasi, untuk mencegah peretas mengakses dan / atau mencuri informasi dan data sensitif. Pekerjaan seorang Analis Keamanan Informasi biasanya melibatkan pemasangan firewall dan perangkat lunak enkripsi data untuk melindungi informasi rahasia. Mereka juga memonitor jaringan organisasi mereka untuk mengawasi insiden keamanan dan menyelidiki insiden ketika terjadi. Analis Keamanan Informasi juga dapat melakukan pengujian penetrasi, yaitu ketika mereka mensimulasikan serangan untuk mencari kerentanan di jaringan mereka sebelum dapat dieksploitasi.

Analis Keamanan Informasi juga sering terlibat dalam merancang dan melaksanakan rencana disaster recovery pada organisasi mereka, yang menjelaskan langkah-langkah dan prosedur untuk memulihkan fungsi yang tepat dari sistem dan jaringan TI organisasi setelah bencana atau serangan. Rencana biasanya mencakup langkah-langkah pencegahan seperti pencadangan rutin dan transfer data ke lokasi di luar lokasi.

Analis Keamanan Informasi harus menjaga diri mereka tetap up to date agar tetap selangkah lebih maju dari penyerang cyber potensial. Mereka harus mengikuti metode terbaru yang digunakan penyerang untuk menyusup ke sistem komputer, serta teknologi keamanan baru yang dapat membantu perusahaan mereka menghadapi ancaman ini.

1.2.1 Kompetensi Keahlian Peserta Lomba

Section	Kriteria	Nilai	Aspect Marks	Variation
1	Work organization and management	5,00	3,50	1,50
2	Communication and interpersonal skills	10,00	9,00	1,00
3	Securely provision	15,00	19,70	4,75
4	Operate and maintain & oversee and govern	15,00	11,00	4,00
5	Protect and defend	15,00	14,50	0,50
6	Analyze	10,00	8,50	1,50
7	Collect and operate	15,00	18,00	3,00
8	Investigate	15,00	15,75	0,70
		Total Variation		17,00

1.2.2 Karakter Kerja Bidang Lomba

Criteria		
ID	Name	Mark
A	Infrastructure Setup and Security Hardening	20.50
B	CyberSecurity Incident Response , Digital Forensics Investigation and Application Security	25.00
C	Capture the Flag (Attack)	25.00
D	Capture the Flag (Defence)	29.50

1.3 Dokumen Terkait

Dokumen ini hanya berisi informasi tentang aspek teknis keterampilan, dokumen lain yang juga harus dipelajari adalah:

- Petunjuk Teknis Umum lomba,
- Informasi di akun Peserta, pembimbing dan Ketua Kontingen:
  a. Deskripsi Teknis Bidang Lomba LKS
  b. Kisi-kisi soal LKS
  c. Form Kebutuhan Bahan
  d. Lembar Ceklis Kebutuhan Bahan

Diskusi terkait pelaksanaan lomba dilaksanakan melalui kegiatan:
Koordinasi Kepala Dinas Pendidikan, *Technical meeting*, pembimbing dan peserta sebelum pelaksanaan lomba.

2. SPESIFIKASI TERHADAP STANDAR NASIONAL (Standar Kompetensi Bidang Lomba)

2.1. Ketentuan umum

- Cyber Security adalah sebuah lomba tim dengan jumlah peserta 2 orang untuk setiap tim.
- Umur peserta pada tahun lomba tidak melewati 25 tahun.

2.2. Spesifikasi Kompetensi LKS-SMK

Spesifikasi Kompetensi adalah rumusan target kompetensi yang akan dilombakan. Target kompetensi dirumuskan berdasarkan situasi dunia kerja atau industri dengan tetap memperhatikan kurikulum SMK. Berikut spesifikasi kompetensi LKS-SMK:

Hari		Kompetensi	WSC %	LKS Daring 2020 %	LKS Daring 2021 %	LKS Daring 2022 %
#1						
		Capture The Flag – Jeopardy (Penyisihan)	10	10	10	10
		CyberSecurity Incident Response, Digital Forensic Investigation and Application security	25	25	25	25
#2						
		Capture the Flag – Attack	25	25	25	30
#3						
		Capture the Flag – Defense & Infrastructure Setup and Security Hardening	40	25	25	25
Jumlah			100%	85%	85%	90%

Bagian		**Persentase Penilaian (%)**
1	**Organisasi dan Manajemen Kerja**	**5**
	Individu perlu mengetahui dan memahami: ● Peraturan tentang keamanan dan kesehatan, apa kewajiban, aturan dan dokumen terkait. ● Situasi ketika alat pelindung diri (APD) harus digunakan, mis. untuk ESD (electronic statis discharge) ● Pentingnya integritas dan keamanan saat berhadapan dengan peralatan dan informasi milik pengguna	

	● Pentingnya pembuangan limbah yang aman untuk daur ulang ● Teknik perencanaan, penjadwalan, dan penentuan prioritas ● Pentingnya akurasi, pengecekan, dan perhatian terhadap detail dalam setiap praktik kerja ● Pentingnya praktik kerja yang rapi dan teratur	
	Peserta mampu untuk: ● Mengikuti standar, aturan, dan peraturan kesehatan dan keselamatan ● Menjaga lingkungan kerja yang aman ● Identifikasi dan gunakan Peralatan Pelindung Pribadi yang sesuai untuk ESD ● Memilih, menggunakan, membersihkan, merawat, dan menyimpan alat dan peralatan dengan aman dan aman ● Merencanakan area kerja untuk memaksimalkan efisiensi dan menjaga disiplin dalam merapikan secara teratur ● Bekerja secara efisien dan memeriksa kemajuan dan hasil secara teratur ● Tetap mendapatkan informasi dan persyaratan terbaru dan biaya dari ‘license to practice’ ● Melakukan metode penelitian yang menyeluruh dan efisien untuk mendukung penambahan pengetahuan ● Secara proaktif mencoba metode, sistem, dan beradaptasi dengan perubahan	
2	**Kemampuan Komunikasi dan Interpersonal**	**10**
	Peserta perlu mengetahui dan memahami: ● Pentingnya mendengarkan sebagai bagian dari komunikasi yang efektif ● Peran dan persyaratan rekan kerja dan metode komunikasi ● yang paling efektif	

	● Pentingnya membangun dan mempertahankan hubungan kerja yang produktif dengan kolega dan manajer ● Teknik untuk kerja tim yang efektif ● Teknik untuk menyelesaikan kesalahpahaman dan kepentingan yang saling bertentangan ● Proses untuk mengelola konflik dan perselisihan agar dapat mencairkan sebuah suasana yang tegang.	
	Peserta mampu untuk: ● Menggunakan kemampuan mendengar dan bertanya yang baik agar dapat memahami situasi yang rumit ● Mengelola secara konsisten dan efektif komunikasi verbal dan tertulis dengan rekan kerja ● Mengenali dan beradaptasi dengan perubahan kebutuhan rekan kerja ● Secara proaktif berkontribusi pada pengembangan tim yang kuat dan efektif ● Membagi pengetahuan dan keahlian dengan rekan dan mengembangkan dukungan pada budaya belajar ● Secara efektif mengelola kesalahpahaman / konflik dan memberikan keyakinan pada individu dalam penyelesaian masalah	
3	**Securely Provision**	**15**
	Peserta perlu mengetahui dan memahami: ● Standar manajemen risiko, kebijakan, Kebutuhan dan Prosedur di bidang Teknologi Informasi. ● Perangkat Cyberdefence dan vulnerability dan kemampuan perangkat tersebut. ● Sistem operasi. ● Konsep pemrograman komputer, termasuk bahasa komputer, ● pemrograman, pengujian, debugging, dan tipe file.	

	● Prinsip dan metode cybersecurity dan privasi yang berlaku untuk pengembangan perangkat lunak.	
	Peserta mampu untuk: ● Menerapkan prinsip keamanan dunia maya dan privasi sesuai dengan kebutuhan organisasi (relevan terhadap kerahasiaan, integritas, ketersediaan, otentikasi, penerimaan) ketika merancang dan mendokumentasikan prosedur Uji & Evaluasi program secara keseluruhan. ● Melakukan penilaian komprehensif independen terhadap manajemen, operasional, dan kontrol keamanan teknis dan peningkatan kontrol yang digunakan di dalam atau diwarisi oleh sistem teknologi informasi (TI) untuk menentukan efektivitas keseluruhan control. ● Mengembangkan, membuat, dan memelihara aplikasi komputer baru, perangkat lunak, atau program utilitas khusus. ● Memodifikasi aplikasi komputer yang ada, perangkat lunak, atau program utilitas khusus. ● Menganalisis keamanan aplikasi komputer baru, yang ada, perangkat lunak, atau program utilitas khusus untuk memberikan hasil yang dapat ditindaklanjuti. ● Mengembangkan dan memelihara bisnis, sistem, dan proses informasi untuk mendukung kebutuhan misi perusahaan. ● Mengembangkan aturan dan persyaratan teknologi informasi yang menggambarkan arsitektur dasar dan target. ● Memastikan bahwa persyaratan keamanan pemangku kepentingan yang diperlukan untuk melindungi misi dan proses bisnis organisasi ditangani secara memadai dalam semua aspek arsitektur perusahaan termasuk model	

	referensi, arsitektur segmen dan solusi, dan sistem yang dihasilkan yang mendukung misi dan proses bisnis tersebut ● Melakukan rekayasa perangkat lunak dan sistem dan riset sistem perangkat lunak untuk mengembangkan kemampuan baru, memastikan keamanan siber terintegrasi penuh. ● Melakukan penelitian teknologi yang komprehensif untuk mengevaluasi potensi kerentanan dalam sistem ruang maya ● Berkonsultasi dengan pemangku kepentingan untuk mengevaluasi persyaratan fungsional dan menerjemahkan persyaratan fungsional menjadi solusi teknis ● Merencanakan, menyiapkan, dan melaksanakan tes sistem ● Menganalisis, mengevaluasi, dan melaporkan hasil berdasarkan spesifikasi dan Persyaratan ● Merancang, mengembangkan, menguji, dan mengevaluasi keamanan sistem informasi sepanjang siklus hidup pengembangan system	
4	**Menjalankan, Memelihara, Mengawasi dan Mengatur**	**15**
	Peserta perlu mengetahui dan memahami: ● Query languages seperti SQL dan system Database ● Kebijakan Pencadangan dan pemulihan data, administrasi, dan standardisasi data ● Protokol jaringan seperti TCP / IP, Konfigurasi Dynamic Host, ● Domain Name System (DNS), dan Directory Services. ● Konsep dan fungsi Firewall (mis., Satu titik dari ● otentikasi / audit / penegakan kebijakan, pemindaian pesan untuk konten berbahaya, anonimisasi data untuk PCI dan PII Compliance, pemindaian perlindungan kehilangan data, percepatan operasi kriptografi, keamanan SSL, pemrosesan REST / JSON).	

	● Konsep arsitektur keamanan jaringan termasuk topologi, protokol, komponen, dan prinsip (mis., application of defence in depth). ● Sistem Administrasi, jaringan, dan pengerasan sistem operasi ● teknik. ● Kebijakan keamanan pengguna teknologi informasi (TI) organisasi (mis., pembuatan akun, aturan kata sandi, kontrol akses). ● Prinsip dan metode keamanan teknologi informasi (mis., ● firewall, zona demiliterisasi, enkripsi). ● Otentikasi, otorisasi, dan metode kontrol akses. ● Prinsip cyber security, vulnerability dan privacy. ● Prinsip dan proses selektif untuk melakukan pelatihan dan penilaian kebutuhan pendidikan. ● Sistem Manajemen Pembelajaran dan penggunaannya dalam mengelola pembelajaran. ● Kompetisi siber sebagai cara mengembangkan keterampilan dengan memberikan pengalaman dalam simulasi dari situasi dunia nyata. ● Hukum cyber dan pertimbangan hukum serta pengaruhnya terhadap perencanaan cyber	
	Peserta mampu untuk: ● Mengembangkan dan mengelola basis data dan / atau sistem manajemen data yang memungkinkan untuk penyimpanan, permintaan, perlindungan, dan pemanfaatan data. ● Mengelola dan mengadmin proses dan alat yang memungkinkan organisasi untuk mengidentifikasi, mendokumentasikan, dan mengakses muatan intelektual dan muatan informasi.	

	● Mengatasi masalah; instal, konfigurasikan, atasi masalah, dan memberikan pemeliharaan dan pelatihan dalam merespon kebutuhan atau pertanyaan pelanggan ● Pasang, konfigurasikan, uji, operasikan, kelola, dan kelola jaringan dan firewall mereka, termasuk perangkat keras dan perangkat lunak yang memungkinkan pembagian dan transmisi semua transmisi spektrum informasi untuk mendukung keamanan informasi dan sistem informasi. ● Menginstal, melakukan konfigurasi, trouble shooting, dan merawat konfigurasi server (perangkat keras dan perangkat lunak) untuk memastikan kerahasiaan, integritas, dan ketersediaannya. ● Kelola akun, firewall, dan Patches. ● Kontrol akses, kata sandi, dan pembuatan dan administrasi akun. ● Tinjau sistem dan prosedur komputer organisasi saat ini ● untuk merancang solusi sistem informasi untuk membantu ● organisasi beroperasi dengan lebih aman, efisien, dan efektif. ● Menyatukan bisnis dan teknologi informasi (TI) bersama ● menanggapi kebutuhan dan keterbatasan keduanya. ● Melakukan pelatihan personel dalam bidang keahliannya sendiri. ● Mengembangkan, merencanakan, mengoordinasikan, memberikan dan / atau mengevaluasi kursus pelatihan, ● metode, dan teknik dalam bidang keahlian sendiri. ● Membantu dalam pengawasan program keamanan siber informasi ● sistem atau jaringan, termasuk mengelola implikasi keamanan informasi dalam organisasi, program spesifik, atau bidang tanggung jawab lainnya, untuk memasukkan	

	strategi, personel, infrastruktur, persyaratan, penegakan kebijakan, perencanaan darurat, kesadaran keamanan, dan sumber daya lainnya. ● Membantu dalam pengembangan kebijakan dan rencana dan / atau mengadvokasi perubahan dalam kebijakan yang mendukung inisiatif ruang maya organisasi atau perubahan / peningkatan yang disyaratkan. ● Mengawasi, mengelola, dan / atau memimpin pekerjaan dan pekerja yang melakukan pekerjaan siber dan terkait siber dan / atau pekerjaan siber.	
5	**Protect and Defend**	**15**
	● Peserta perlu mengetahui dan memahami ● Implementasi sistem file (mis., Sistem File Teknologi Baru [NTFS], Tabel Alokasi File [FAT], Ekstensi File [EXT]). ● File sistem (mis., File log, file registri, file konfigurasi) berisi ● informasi yang relevan dan di mana menemukan file-file sistem tersebut. ● Konsep arsitektur keamanan jaringan termasuk topologi, protokol, komponen, dan prinsip (mis., penerapan pertahanan-dalam-dalam). ● Prinsip analisis standar industri dan diterima secara organisasi, ● metode dan alat untuk mengidentifikasi kerentanan. ● Investigasi ancaman, pelaporan, alat investigasi dan ● hukum / peraturan. ● Kategori insiden, metodologi respons dan penanganan. ● Alat penilaian pertahanan dan kerentanan dunia maya dan kemampuan perangkat mereka ● Desain penanganan untuk risiko keamanan yang diidentifikasi.	

	● Otentikasi, otorisasi, dan pendekatan akses (mis. Role based kontrol akses, kontrol akses wajib dan kontrol akses diskresioner).	
	Peserta mampu untuk: ● mengelola jaringan penyedia layanan pertahanan jaringan komputer dan sumber daya. ● Monitor jaringan untuk secara aktif memulihkan system dari unauthorized activities. ● Menanggapi krisis atau situasi mendesak dalam bidang keahlian masing masing untuk mengurangi ancaman langsung dan potensial. ● Gunakan pendekatan mitigasi, kesiapsiagaan, dan respons serta pemulihan, sesuai kebutuhan, untuk memaksimalkan kelangsungan hidup, pelestarian properti, dan informasi keamanan. ● Selidiki dan analisis semua kegiatan respons yang relevan. ● Melakukan penilaian ancaman dan kerentanan ● Menentukan penyimpangan dari konfigurasi yang dapat diterima, perusahaan atau kebijakan lokal ● Menilai tingkat risiko dan mengembangkan dan / atau merekomendasikan yang sesuai penanggulangan mitigasi dalam situasi operasional dan non-operasional.	
6	**Analisa**	**10**
	Peserta perlu mengetahui dan memahami: ● Aktor cyber threat, ekuitas dan metode mereka. ● Metode dan teknik yang digunakan untuk mendeteksi berbagai kegiatan eksploitasi. ● Kemampuan dan repositori pengumpulan / informasi intelijen Cyber. ● Ancaman dan kerentanan dunia maya.	

	● Dasar-dasar keamanan jaringan (mis., Enkripsi, firewall, otentikasi, honey pot, perlindungan perimeter). ● Sumber penyebaran informasi kerentanan (mis., Lansiran, ● saran, errata, dan buletin). ● File sistem mana (mis., File log, file registri, file konfigurasi) ● berisi informasi yang relevan dan di mana menemukan file-file sistem tersebut. ● Struktur, pendekatan, dan strategi alat eksploitasi (mis., Sniffer, ● keyloggers) dan teknik (mis., mendapatkan akses pintu belakang, mengumpulkan / mengelupas data, melakukan analisis kerentanan sistem lain dalam jaringan). ● Taktik internal untuk mengantisipasi dan / atau meniru kemampuan dan tindakan ancaman. ● Kemampuan dan alat operasi cyber partner internal dan eksternal. ● Pengembangan target (mis., Konsep, peran, tanggung jawab, produk, dll.) ● Artefak Sistem dan kasus penggunaan forensik	
	Peserta mampu untuk: ● Identifikasi dan nilai kemampuan dan aktivitas cybersecurity ● penjahat atau entitas intelijen asing ● Menghasilkan temuan untuk membantu menginisialisasi atau mendukung penegakan hukum dan investigasi atau kegiatan kontra intelijen. ● Menganalisis informasi yang dikumpulkan untuk mengidentifikasi kerentanan dan potensi untuk eksploitasi. ● Menganalisis informasi ancaman dari berbagai sumber, disiplin ilmu, dan lembaga di seluruh Komunitas Intelijen.	

	● Mensintesis dan menempatkan informasi intelijen dalam konteks; menggambar wawasan tentang implikasi yang mungkin terjadi. ● Menerapkan pengetahuan terkini tentang satu atau lebih wilayah, negara, non-negara, entitas, dan / atau teknologi.	
7	**Collect and Operate**	**15**
	● Peserta perlu mengetahui dan memahami Strategi pengumpulan, teknik, dan alat. ● Kemampuan dan repositori pengumpulan / informasi intelijen Cyber. ● Kebutuhan informasi dan persyaratan pengumpulan diterjemahkan, dilacak, dan diprioritaskan di perusahaan yang diperluas. ● Diperlukan produk perencanaan intelijen yang terkait dengan perencanaan operasional cyber. Program, strategi, dan sumber daya perencanaan operasional Cyber. ● Strategi, sumber daya, dan alat operasi siber. ● Konsep operasi cyber, terminologi / leksikon (yaitu, lingkungan persiapan, serangan dunia maya, pertahanan dunia maya), prinsip, kemampuan, batasan, dan efek.	
	Peserta mampu untuk: ● Jalankan pengumpulan menggunakan strategi yang tepat dan dalam prioritas ditetapkan melalui proses manajemen pengumpulan. ● Melakukan penargetan bersama yang mendalam dan proses perencanaan keamanan siber.	

	● Kumpulkan informasi dan kembangkan Rencana Operasional terperinci dan Pesanan yang mendukung persyaratan. ● Membantu perencanaan tingkat operasional dan strategis di seluruh jajaran operasi untuk operasi informasi dan dunia maya terintegrasi. ● Mendukung kegiatan untuk mengumpulkan bukti kriminal atau asing entitas intelijen untuk mengurangi kemungkinan atau ancaman waktu nyata, melindungi terhadap spionase atau ancaman orang dalam, sabotase asing, kegiatan teroris internasional, atau untuk mendukung kegiatan intelijen lainnya.	
8	**Investigasi**	**15**
	Peserta perlu mengetahui dan memahami ● Investigasi ancaman, pelaporan, alat investigasi, dan hukum / peraturan. ● Konsep dan metodologi analisis malware. ● Proses pengumpulan, pengemasan, pengangkutan, dan penyimpanan bukti elektronik sambil mempertahankan *chain of custody*. ● Proses peradilan, termasuk penyajian fakta dan bukti. ● Jenis dan kumpulan data persisten. ● Konsep dan praktik pengolahan data forensik digital. ● Jenis data forensik digital dan cara mengenalinya. ● Implikasi forensik dari struktur dan operasi sistem operasi. ● Dampak operasional spesifik dari penyimpangan keamanan siber.	
	Peserta mampu untuk: ● Mendukung pekerjaan personel senior dengan serangkaian alat dan proses investigasi untuk memasukkan, tetapi tidak	

	terbatas pada, teknik wawancara dan interogasi, pengawasan, pengawasan balik, dan deteksi pengawasan. ● Mengumpulkan, memproses, melestarikan, menganalisis, dan menyajikan bukti terkait komputer untuk mendukung mitigasi kerentanan jaringan dan / atau kejahatan, penipuan, kontra intelijen, atau investigasi penegakan hukum.	
	Total	**100**

3. SISTEM PENILAIAN

3.1. Petunjuk Umum

Penilaian akan berdasarkan pada kriteria penilaian ***judgement*** dan ***measurement***

3.2. Kriteria Toleransi Pengukuran

Nilai yang dialokasikan untuk setiap Kriteria akan dihitung oleh CIS. Ini akan menjadi jumlah kumulatif dari nilai yang diberikan untuk setiap Aspek dalam Kriteria Penilaian.

3.3. Kriteria Penilaian

3.3.1. Penilaian Judgement

Berdasarkan pada laporan yang dikumpulkan oleh tim peserta, dan akan dinilai oleh juri, dan dari penilaian subjektif ini akan diperiksa untuk mengetahui kebenaran dari nilai yang berada di web scoring, sehingga dari penilaian judgement ini bisa membatalkan penilaian measurement yang ada di web scoring apabila ditemukan ketidaksesuaian antara laporan dan pengerjaan tim peserta di web scoring.

3.3.2. Penilaian measurement

Berdasarkan pada poin yang ada di web scoring

3.3.3. Komposisi Penilaian Judgement dan Measurement

Penialian	**Persentase**

Measurement	90%
Judgement	10%
Total	100%

3.5. Sub Kriteria

Setiap Kriteria Penilaian dibagi menjadi satu atau lebih Sub Kriteria. Setiap Sub Kriteria menjadi judul untuk formulir penandaan WorldSkills. Setiap formulir penandaan (Sub Criterion) berisi Aspek yang akan dinilai dan ditandai oleh pengukuran atau penilaian, atau pengukuran dan penilaian.

Setiap formulir penandaan (Sub Criterion) menentukan hari yang akan ditandai, dan identitas tim penandaan.

3.6 Keseluruhan Penilaian

Penilaian akhir didasarkan pada hasil kalkulasi penilaian ***judgement*** dan ***measurement***

3.7. Prosedur Penilaian

Juri akan mencatat poin yang dikumpulkan oleh peserta pada web scoring atau *scoreboard* dan melakukan pemeriksaan laporan yang dikumpulkan peserta untuk memastikan hasil dari web scoring sesuai.

3.1. Skema Penilaian

No.	Modul	Kriteria/Sub-Kriteria	Total
1	A	Infrastructure Setup and Security Hardening	20,5
2	B	CyberSecurity Incident Response , Digital Forensics Investigation and Application Security	25
3	C	Capture the Flag (Attack)	25
4	D	Capture the Flag (Defence)	29,5
Total			**100**

4. FORMAT/STRUKTUR PROYEK UJI

4.1. Petunjuk Umum

Proyek uji akan memungkinkan penilaian keterampilan di setiap bagian. Tujuan dari Proyek uji adalah untuk memberikan peluang penuh, seimbang dan autentik untuk penilaian dan penandaan di Spesifikasi Standar, dalam hubungannya dengan Format Penilaian. Hubungan antara Proyek uji, Format Penilaian, dan Spesifikasi Standar akan menjadi indikator utama kualitas, sebagaimana juga hubungannya dengan kinerja kerja aktual.

Proyek uji tidak akan mencakup area di luar Spesifikasi Standar, atau mempengaruhi keseimbangan tanda dalam Spesifikasi Standar selain dari keadaan yang ditunjukkan oleh Bagian 2. Proyek uji akan memungkinkan pengetahuan dan pemahaman untuk dinilai hanya melalui aplikasi mereka dalam pekerjaan praktis. Proyek uji tidak akan menilai pengetahuan tentang peraturan dan regulasi lomba. Uraian Teknis ini akan mencatat setiap masalah yang mempengaruhi kapasitas Proyek uji untuk mendukung berbagai penilaian relatif terhadap Spesifikasi Standar.

Proyek uji akan meminta Peserta untuk mengatur, menginstal, mengkonfigurasi, dan memperkuat komputer, server, firewall, peralatan jaringan, dan perangkat lunak terkait untuk memenuhi tugas spesifik jaringan dan teknisi atau konsultan keamanan sistem.

Proyek uji akan dibagi menjadi tiga area berbeda yang akan dilakukan selama tiga (3) hari dari lomba:

1. Infrastructure Setup and Security Hardening
2. Capture the Flag – Attack
3. Capture the Flag – Defense
4. CyberSecurity Incident Response, Digital Forensic Investigation and Application security

4.2. Persyaratan Uji

Setiap modul Proyek uji harus :

1. Pada tingkat yang dapat diselesaikan oleh seorang kontestan dengan nyaman;

2. Tingkat kesulitan tertinggi dalam modul termasuk lomba, harus kurang dari atau sama dengan pengetahuan, kumpulan keterampilan, dan kemampuan yang ditentukan dalam tujuh (7) fungsi keamanan siber yang dinyatakan dalam Spesifikasi Standar WorldSkills
3. Skema penilaian yang akan diselesaikan pada lomba sesuai dengan Deskripsi Teknis;

Setiap modul harus memiliki gambar topologi fisik yang rinci diikuti oleh logika rinci gambar topologi;

4.3. Sirkulasi Proyek Uji

Proyek uji akan di informasikan pada saat lomba.

4.4. Perubahan Proyek Uji

Tidak ada perubahan pada proyek uji.

5. DAFTAR ALAT

5.1 Ketentuan Umum

Alat dan bahan yang telah disediakan oleh peserta masing-masing dan melakukan konfirmasi alat dengan juri pada saat pelaksanaan ujicoba. Peserta diberikan waktu familiarisasi fasilitas lomba 1 hari sebelum lomba (maksimal 2 jam).

Alat yang diperlukan ada yang berbentuk perangkat lunak (software), ada yang berbentuk perangkat keras (hardware) dan peralatan penunjang seperti furniture dan peralatan kesehatan dan keselamatan.

Untuk lomba Cyber Security diperlukan perangkat penunjang sebagai berikut:

Sistem Lomba (Software):

- CTF Attack VM
- CTF Defence dan Infrastructure Setup and Security Hardening VM
- CyberSecurity Incident Response, Digital Forensic Investigation and Application security VM
- CTF Penyisihan
- VPN Server dan Client

- Web Scoring System

Hosting

- Hosting untuk Web Lomba

5.2 Daftar Alat para Peserta

Alat yang dipersiapkan oleh peserta meliputi:

IT Software

Jumlah	Nama	Keterangan	Penempatan
1 per peserta	Snort NIDS/NIPS		Area Kerja Peserta
1 per peserta	Wireshark		Area Kerja Peserta
1 per peserta	Apache TCPMon		Area Kerja Peserta
1 per peserta	Nmap		Area Kerja Peserta
1 per peserta	Metasploit Framework		Area Kerja Peserta
1 per peserta	Splunk		Area Kerja Peserta
1 per peserta	WAF mod_security		Area Kerja Peserta
1 per peserta	Microsoft Server OS 2016		Area Kerja Peserta
1 per peserta	Linux OS (use CentOS)		Area Kerja Peserta
1 per peserta	MySQL		Area Kerja Peserta
1 per peserta	Web server (on Linux)		Area Kerja Peserta
1 per peserta	Tripwire (open source version)		Area Kerja Peserta
1 per peserta	IDA Free		Area Kerja Peserta
1 per peserta	Radare		Area Kerja Peserta
1 per peserta	OllyDbg		Area Kerja Peserta
1 per peserta	Volatility		Area Kerja Peserta
1 per peserta	FTK		Area Kerja Peserta
1 per peserta	Autopsy		Area Kerja Peserta
1 per peserta	Kali		Area Kerja Peserta
1 per peserta	OSSEC		Area Kerja Peserta
1 per peserta	OSSIM SIEM		Area Kerja Peserta
1 per peserta	ELK		Area Kerja Peserta

1 per peserta	Cisco OpenSOC		Area Kerja Peserta
1 per peserta	VMWare vSphere ESXi		Area Kerja Peserta
1 per peserta	VMWare vSphere Client		Area Kerja Peserta
1 per peserta	PuTTY Utilities		Area Kerja Peserta
1 per peserta	VMWare Workstation		Area Kerja Peserta
1 per peserta	Windows 10 Enterprise (Eval)		Area Kerja Peserta
1 per peserta	PDF reader		Area Kerja Peserta

Catatan:

Semua kebutuhan di bagian Software bisa dipenuhi oleh OS Kali Linux dan OS Windows

IT Hardware

Jumlah	Nama	Keterangan	Penempatan
1 per peserta	Laptop/PC	Peserta boleh menggunakan Laptop Jenis apa saja selama laptop tersebut mampu OS Kali Linux dan/atau Windows 10	Area Kerja Peserta
1 per tim	Webcam	Perlengkapan untuk zoom	Area Kerja Peserta
2 per tim	Camera	-	Area Kerja Peserta
2 per keahlian	Digital Clock	-	Briefing Area

IT Services

Jumlah	Nama	Keterangan	Penempatan
(10x3) 30 per keahlian	VPS Final (3 per tim)	1 CPU dual Core, Ram 4Gb, Storage 125gb	VPS Provider

1 Server Soal	VPS (Penyisihan)	4 CPU dual core, RAM 32GB, Storage 1TB, VPS Panel, Unmetered Bandwidth	VPS Provider
1 Untuk Scoreboard	VPS (Penyisihan)	4 CPU dual core, RAM 32GB, Storage 1TB, VPS Panel, Unmetered Bandwidth	VPS Provider
1 untuk semua peserta	VPN Peserta Penyisihan	dedicated Static IP, 10 mbps, Location: Indonesia, Quota: unlimited, PPTP L2TP OVPN	VPS Provider
10 per keahlian	VPN Peserta Final	dedicated Static IP, 10 mbps, Location: Indonesia, Quota: unlimited, PPTP L2TP OVPN	VPS Provider
1 per keahlian	VPS Red Team	1 CPU dual Core, Ram 4Gb, Storage 250 GB,VPS Panel, Unmetered Bandwidth	VPS Provider
1 per keahlian	VPN Blue Team	dedicated Static IP, 10 mbps, Location: Indonesia, Quota: unlimited, PPTP L2TP OVPN	VPS Provider
1 per keahlian	PC/Laptop Red Team	i5, 8GB, SSD 512GB, OS Linux	Ruang Pakar

1 per keahlian	PC/Laptop Blue Team	i5, 8GB, SSD 512GB, OS Linux	Ruang Pakar

Kesehatan dan Keamanan

Jumlah	Nama	Keterangan	Penempatan
1 per keahlian	Hand sanitizer		Briefing Room

6. DAFTAR BAHAN

A. Bahan yang dipersiapkan oleh peserta meliputi:

Peserta perlu mempersiapkan 2 buah PC/Laptop yang terhubung ke Internet (minimal bandwidth 10Mbps) dan dilengkapi dengan:

- Operating System Windows/Linux (Kali Linux)/Apple
- WebCam
- Zoom.us
- Discord
- Office Application untuk pembuatan laporan

B. Bahan yang dipersiapkan oleh pelaksana meliputi:

Pelaksana lomba perlu menyiapkan:

- Sistem/Server Soal dan untuk tahap penyisihan dan final yang berupa Virtual Private Server, dengan spesifikasi minimal 2 CPU dual core, RAM 16GB, HDD 512GB.
- Sistem Scoring untuk tahap penyisihan dan final yang berupa Virtual Private Server, dengan spesifikasi minimal 2 CPU dual core, RAM 16GB, HDD 512GB.
- Sarana Kompetisi dapat disediakan oleh penyelenggara layanan Cloud.
- Soal-Soal sesuai dengan jumlah jumlah dan tingkat kompetisi.

6.1 BAHAN PENUNJANG

Bahan Penunjang Lomba sebagai Referensi para Peserta

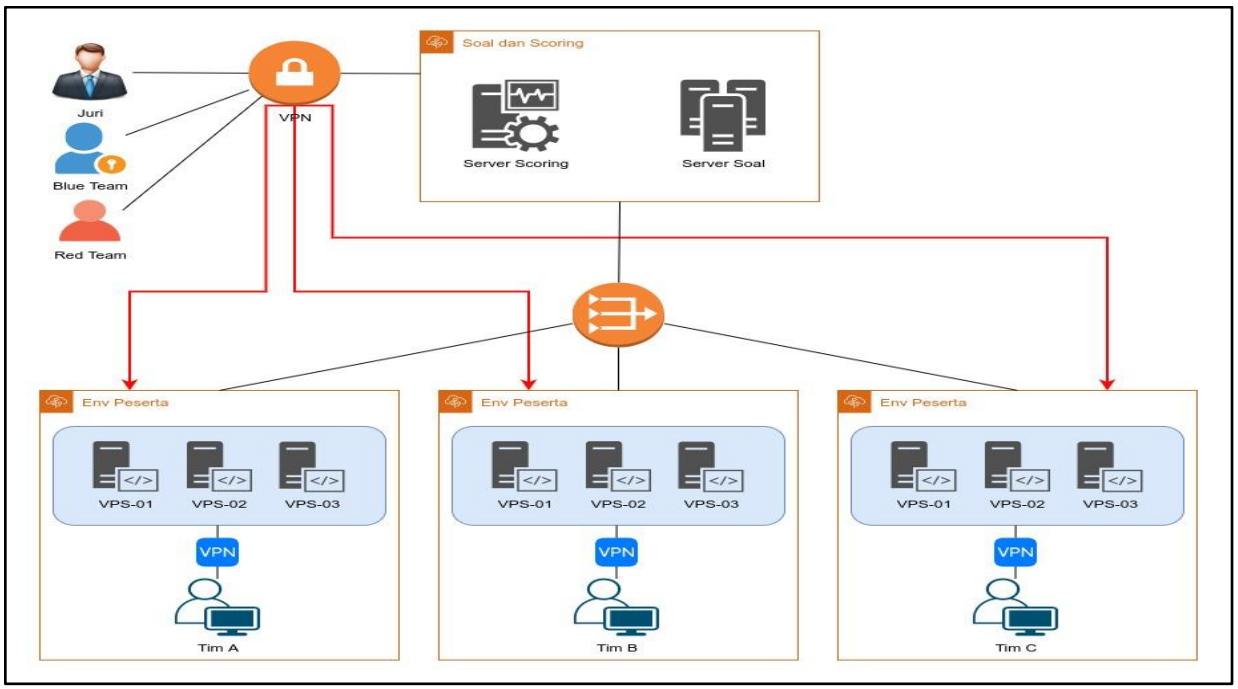
Keterangan Tambahan Jika ada.

7. LAYOUT DAN BAHAN LAYOUT

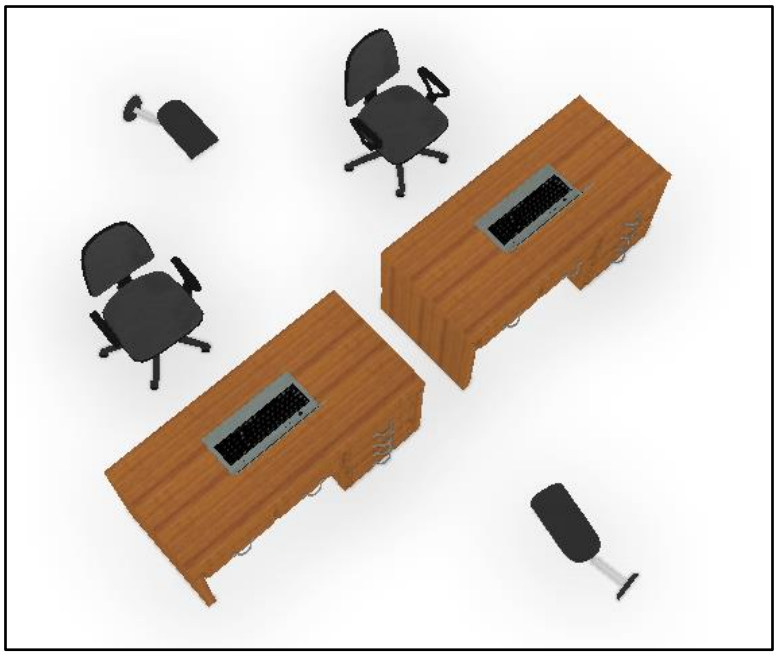
Luasan Ruang yang diperlukan:

- Ruang Kerja Peserta (Ruang Lomba) dengan kebutuhan luasan: min. 12m^2
- Ruang Juri Penilaian dengan kebutuhan luasan: 30m^2

Tata layout topologi sistem perlombaan :

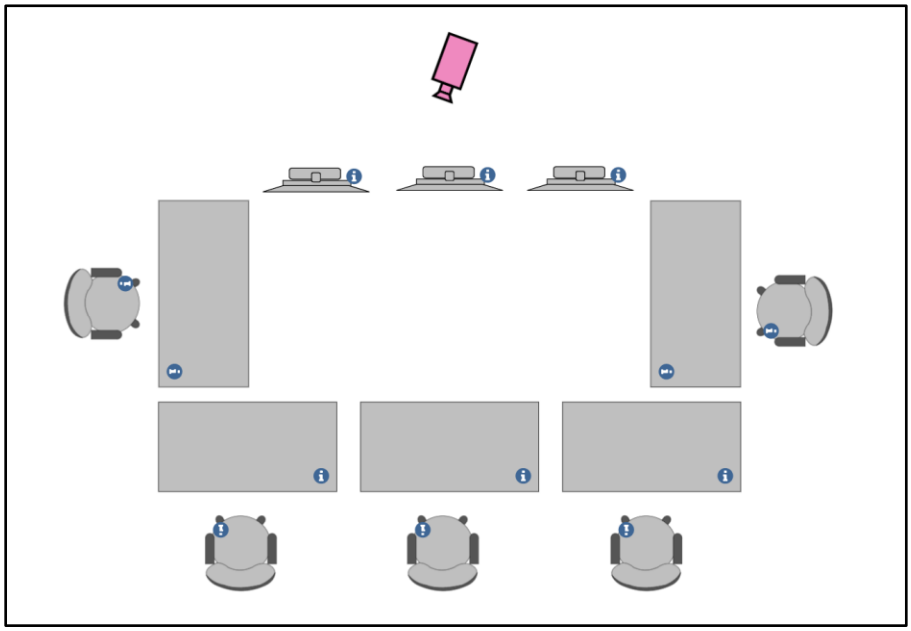


Tata layout area kerja peserta berikut deskripsinya :



Harus ada 2 camera yang mengawasi depan belakang dan harus melakukan live streaming dari camera pengawasan.

Tata layout penempatan peralatan utama berikut deskripsinya :



8. JADWAL BIDANG LOMBA

Kegiatan	Waktu Perlombaan

Hari Ke - 1	
Pembacaan Rules Of The Game	10 Menit
Capture The Flag Jeopardy Penyisihan	3.5 Jam
CyberSecurity Incident Response, Digital Forensic Investigation and Application security	3.5 Jam
Hari Ke - 2	
Pembacaan Rules Of The Game	10 Menit
Capture the Flag – Attack	5 Jam
Hari Ke - 3	
Pembacaan Rules Of The Game	10 Menit
Capture the Flag – Attack	5 Jam

9. KEBUTUHAN LAIN dan SPESIFIKASINYA

9.1 Kebutuhan ini untuk kebutuhan juri, diantaranya:

No	Peralatan	Jumlah	Satuan	Gambar
Bidang Cyber Security tidak membutuhkan tambahan karena menggunakan system Scoreboard				

9.2 Kebutuhan Juri untuk menilai, diantaranya:

No	Peralatan	Kualitas	Satuan
1	Cable HDMI (3 m)	Cable HDMI (3 m)	1
2	Laser printer A4 - Type 2	Color laser Jet	1
3	TV Monitor	50 inch, HDMI	3
4	Cable HDMI	Cable HDMI	3

5	Hand sanitizer	Hand sanitizer	1
6	Koneksi Internet dengan bandwith minimal 30Mbps	Dedicated	1
7	Stop Kontak isi 4	SNI	4
8	Webcam	Perlengkapan untuk Zoom Ruang Juri	1
9	Laptop	Core i5, 8GB Ram, 320GB HDD, HDMI Port, LAN Port, Wifi, Windows OS	1

9.3 Kapasitas listrik yang dibutuhkan:

No.	Nama Alat	Daya
1	**Projector**	250 watt
2	**TV Monitor**	250 watt
3	**Laser Printer A4 – Type 2**	250 watt
4	**5 Laptop juri dan teknisi**	250 watt
TOTAL		**1000 watt**

10. Rekomendasi Juri

Lampiran Rekomendasi juri

Lampiran 1: Format Penilaian

Sub Criterion ID	Sub Criterion Name or Description	Day of Marking	Aspect Type M = Meas = Judg	Aspect - Description	Judg Score	Extra Aspect Description (Meas or Judg) OR Judgement Score Description (Judg only)	Requirement (Measurement Only)	WSSS Section	Calculation Row (Expert only)	Max Mark
A1	Logon and password policies	4								
			M	Security banner (Linux machines)		On random linux machine go to login sreen	Look for banner	4		0.25
			M	Password minimum length (Linux machines)		Pick random preconfigured account, change password to random one with length of 8 (which meets complexity requirements)	Error messege (doesn't meet minimal length)	4		0.25
			M	Password complexity (Linux machines)		Pick random preconfigured account, change password to random one low complexity (which meets length requirements)	Error messege (doesn't meet complexity requirements)	4		0.25
			M	Account lockdown (Linux machines)		On random linux machine - try to login 3 times with incorrect password	Login screen must be locked down for 1 min	4		0.25
			M	Inactivity timeout (Linux machines)		On random linux machine login and wait for 1 min	After 1 min you should be logged off	4		0.25
A2	Public services protection	4								
			M	Web-01 website is running HTTPS, all HTTP requests are redirected to HTTPS			HTTP request must be redirected to HTTPS, web site should be opened successfully	4		0.50
			M	Web-02 accepts explicit SSL / TLS connections only			Connection must be successful, in logs look for STARTTLS	4		1.25
			J	Additional security measures listing				1		1.50
					0	no attempt				
					1	1 logical security measure				
					2	2 logical additional security measures				
					3	3 logical additional security measures				
A3	Events monitoring	4								
			M	FTP traffic alerts			Look for FTP traffic alerts	7		2.00
			M	ICMP traffic alerts			Look for ICMP traffic alerts	7		2.00
			M	Malware traffic alerts			Look for malware traffic alerts	7		2.00
			J	Additional security measures listing				1		2.00
					0	no attempt				
					1	1 logical security measure				
					2	2 logical additional security measures				
					3	3 logical additional security measures				

Sub	Sub Criterion	Day of	Aspect	Aspect - Description	Judg	Extra Aspect Description (Meas or Judg)	Requirement	WSSS	Calculation	Max
A4	Firewall policy	4								
			M	IDS		Check Iptables and firewalld	Doesn't contain "permit all or any any"	4		2.00
			M	LOG		Check Iptables and firewalld	Doesn't contain "permit all or any any"	4		2.00
			M	Web-01		Check Iptables and firewalld	Doesn't contain "permit all or any any"	4		2.00
			M	Web-02		Check Iptables and firewalld	Doesn't contain "permit all or any any"	4		2.00
B1	Incident Response:Work Task Server	1								
			M	Find and submit the relevant commands and the parameters that is used in the		Answer to be recorded in the Web Scoring		5		1.25
			M	Submit the time that the hack first executed the attack command				5		0.50
			M	Find and submit the filename of infected file in the web server used in the attack.				5		0.50
			M	Find and submit the webshell code used in the attack.				5		0.50
			M	Find and submit the name of webshell created by hacker				5		0.50
			M	Find and submit the name of the function called by the webshell created by the				5		0.50
			M	Find and submit the target IP of the http tunnel used in the attack				5		0.50
			M	Submit the username and password that the hacker logged into the server though the http tunnel		Fill in the cybersecurity incident response report		5		0.50
B2	Incident Response:Work Task Server	1								
			M	Find and submit the i) pathname and ii) filename of the malicious program that		Answer to be recorded in the Web Scoring		5		1.25
			M	ii) filename				5		0.50
			M	Submit the SHA1 checksum of the malicious program that locked your screen in the				5		0.50
			M	Find and submit the i) pathname and ii) filename of the stager program linked to the				5		0.50
			M	ii) filename				5		0.50
			M	Enumerate the steps of the stager program in the attack		Fill in the cybersecurity incident response report		5		0.50
B3	Vulnerability Detection and Repair:	1								
			M	Modify PHP to forbid dangerous functions and submit changes made.		Fill in the cybersecurity incident response report		6		1.00
			M	Modify Mysql's setting to limit the actions of importing and exporting and submit				6		0.50

B4	Vulnerability Detection and Repair: Work Task	1								
			M	Delete THREE malicious programs on the operating system and the i) pathnames and ii) filenames.		Fill in the cybersecurity incident response report		6		1.00
B5	Digital Forensic Investigation: Work Task Serv	1								
			M	Identify malicious program processes		Answer to be recorded in the Web Scoring		8		0.50
			M	Locate malicious program files				8		0.50
			M	Recover system settings modified by malware (Describe the steps, how to recover system)				8		0.50
B6	Digital Forensic Investigation: Work Task Wi	1								
			M	Identify malicious program processes		Answer to be recorded in the Web Scoring		8		1.00
			M	Find hidden locations of malicious programs				8		0.50
			M	Find the key left by malicious programs in memory				8		0.50
B7	Digital Forensic Investigation: Work Task Netv	1								
			M	Identify malicious program process		Answer to be recorded in the Web Scoring		8		1.00
			M	Find the key and answer SHA1 checksum(task dump.raw)				8		0.50
			M	Retrieve the file and submit the file content.				8		0.75
B8	Digital Forensic Investigation: Work Task Tex	1								
			M	Extract malicious file, and submit the MD5 of malicious file		Answer to be recorded in the Web Scoring		8		0.75
			M	Decrypt the encrypted file, and submit the file content				8		0.75
B9	Code Review: Work Task Code Review1	1								
			M	Identify the vulnerable line of code that poses a security threat.		Fill in the cybersecurity incident response report		3		1.00
			M	Name the possible cybersecurity attack against the vulnerable code.				3		0.25
			M	Explain how one can makes the code secure.				3		0.50
			M	Provide the secure code (or line of codes) against the vulnerability.				3		0.50
B10	Code Review: Work Task Code Review2	1								
			M	Identify the vulnerable line of code that poses a security threat.		Fill in the cybersecurity incident response report		3		1.00
			M	Name the possible cybersecurity attack against the vulnerable code.				3		0.25
			M	Explain how one can makes the code secure.				3		0.50
			M	Provide the secure code (or line of codes) against the vulnerability.				3		0.50
B11	Code Review: Work Task Code Review3	1								
			M	Identify the vulnerable line of code that poses a security threat.		Fill in the cybersecurity incident response report		3		1.00
			M	Name the possible cybersecurity attack against the vulnerable code.				3		0.25
			M	Explain how one can makes the code secure.				3		0.50
			M	Provide the secure code (or line of codes) against the vulnerability.				3		0.50

Sub Criterion ID	Sub Criterion Name or Description	Day of Marking	Aspect Type M = Meas J = Judg	Aspect - Description	Judg Score	Extra Aspect Description (Meas or Judg) OR Judgement Score Description (Judg only)	Requirement (Measurement Only)	WSSS Section	Calculation Bow (Export only)	Max Mark
C1	Enumeration	3								
			M	All flags related to protocol enumeration		Protocol Enumberation Flags (Flags 1-3) (1 flag - 0.5)		6		2.00
			M	All flags related to protocol enumeration		Protocol Enumberation Flags (Flags 4-5) (1 flag - 0.5)		2		1.00
			M	All flags related to protocol enumeration		Protocol Enumberation Flags (Flags 6-10) (1 flag - 0.2)		6		1.00
C2	Web Based Attacks	3								
			M	All flags related to web attacks		Web Attack Flags (Flags 1-3) (1 flag - 0.5)		6		2.00
			M	All flags related to web attacks		Web Attack Flags (Flags 4-5) (1 flag - 0.5)		2		1.00
			M	All flags related to web attacks		Web Attack Flags (Flags 6-10) (1 flag - 0.2)		6		1.00
C3	Database Attacks	3								
			M	All flags related to exploiting databases		Database Attack Flags (Flags 1-3) (1 flag - 0.5)		5		2.00
			M	All flags related to exploiting databases		Database Attack Flags (Flags 4-5) (1 flag - 0.5)		2		1.00
			M	All flags related to exploiting databases		Database Attack Flags (Flags 6-10) (1 flag - 0.2)		5		1.00
C4	Root Access	3								
			M	All flags after root access into vulnerable system		Root Access Flags (Flags 1-3) (1 flag - 0.5)		5		2.00
			M	All flags after root access into vulnerable system		Root Access Flags (Flags 4-5) (1 flag - 0.5)		2		1.00
			M	All flags after root access into vulnerable system		Root Access Flags (Flags 6-10) (1 flag - 0.2)		5		1.00
C5	Cryptography	3								
			M	All flags related to cryptography		Cryptography Flags (Flags 1-3) (1 flag - 0.5)		3		2.00
			M	All flags related to cryptography		Cryptography Flags (Flags 4-5) (1 flag - 0.5)		3		1.00
			M	All flags related to cryptography		Cryptography Flags (Flags 6-10)(1 flag - 0.2)		3		1.00
C6	Steganography	3								
			M	All flags related to steganography		Steganography Flags (Flags 1-3) (1 flag - 0.5)		3		2.00
			M	All flags related to steganography		Steganography Flags (Flags 4-5) (1 flag - 0.5)		3		1.00
			M	All flags related to steganography		Steganography Flags (Flags 6-10) (1 flag - 0.2)		3		1.00
			M	At least 1 flag from 5 categories				7		1.00

Sub Cr	Sub Criterion	Day of	Aspect	Aspect - Description	Judg	Extra Aspect Description (Meas or Judg)	Requirement	WSSS	Calculation	Max
D1	Reconnaisance Application	4								
			M	All flags related to understanding Reconnaisance Application Detection, And Web Server Hardening		Reconnaisance Application Detection, And Web Server Hardening (Flags 1-3) (1 flag - 0.5)		7		2.00
			M	All flags related to understanding Reconnaisance Application Detection, And Web Server Hardening		Reconnaisance Application Detection, And Web Server Hardening (Flags 4-5) (1 flag - 0.5)		2		1.00
			M	All flags related to understanding Reconnaisance Application Detection, And Web Server Hardening		Reconnaisance Application Detection, And Web Server Hardening (Flags 6-10) (1 flag - 0.2)		7		1.00
D2	Red Team/Hacker Attack Detection And Prevention, including Active Directory Hardening	4								
			M	All flags relating to detecting Red Team/Hacker Attack Detection And Prevention		Red Team/Hacker Attack Detection And Prevention Flags (Flags 1-3) (1 flag - 0.5)		3		2.00
			M	All flags relating to detecting Red Team/Hacker Attack Detection And Prevention		Red Team/Hacker Attack Detection And Prevention Flags (Flags 4-5) (1 flag - 0.5)		2		1.00
			M	All flags relating to detecting Red Team/Hacker Attack Detection And Prevention		Red Team/Hacker Attack Detection And Prevention Flags (Flags 6-10) (1 flag - 0.2)		7		1.00
D3	Application Vulnerability Patching	4								
			M	All flags related to Application Vulnerability Patching		Application Vulnerability Patching (Flags 1-3) (1 flag - 0.5)		7		2.00
			M	All flags related to Application Vulnerability Patching		Application Vulnerability Patching (Flags 4-5) (1 flag - 0.5)		2		1.00
			M	All flags related to Application Vulnerability Patching		Application Vulnerability Patching (Flags 6-10) (1 flag - 0.2)		7		1.00
D4	Hardening And Configuration	4								
			M	All flags in Hardening And Configuration Patching Database Server		Hardening And Configuration Patching Database Server Flags (Flags 1-3) (1 flag - 0.5)		7		2.00
			M	All flags in Hardening And Configuration Patching Database Server		Hardening And Configuration Patching Database Server Flags (Flags 4-5) (1 flag - 0.5)		2		1.00
			M	All flags in Hardening And Configuration Patching Database Server		Hardening And Configuration Patching Database Server/Botnet Flags (Flags 6-10) (1 flag - 0.2)		7		1.00
D5	Hardening And Configuration	4								
			M	All flags in detecting Hardening And Configuration Patching SSH Server		Hardening And Configuration Patching SSH Server (Flags 1-3) (1 flag - 0.5)		3		2.00
			M	All flags in detecting Hardening And Configuration Patching SSH Server		Hardening And Configuration Patching SSH Server (Flags 4-5) (1 flag - 0.5)		2		1.00
			M	All flags in detecting Hardening And Configuration Patching SSH Server		Hardening And Configuration Patching SSH Server (Flags 6-10) (1 flag - 0.2)		3		1.00
D6	Hardening And Configuration	4								
			M	All flags related to Hardening And Configuration Patching File Server		Hardening And Configuration Patching File Server Flags (Flags 1-3) (1 flag - 0.5)		8		2.00
			M	All flags related to Hardening And Configuration Patching File Server		Hardening And Configuration Patching File Server Flags (Flags 4-5) (1 flag - 0.5)		8		1.50
			M	All flags related to Hardening And Configuration Patching File Server		Hardening And Configuration Patching File Server (Flags 6-10) (1 flag - 0.2)		8		1.00
D7	Malware/Backdoor Detection	4								
			M	All flags related to Malware/Backdoor Detection		Malware/Backdoor Detection Flags (Flags 1-3) (1 flag - 0.5)		8		2.00
			M	All flags related to Malware/Backdoor Detection		Malware/Backdoor Detection Flags (Flags 4-5) (1 flag - 0.5)		8		1.00
			M	All flags related to Malware/Backdoor Detection		Malware/Backdoor Detection Flags (Flags 6-10) (1 flag - 0.2)		8		1.00
			M	All flags related to Malware/Backdoor Detection				7		1.00

Kisi Kisi Cyber Security LKSN 2022

1. Infrastructure Setup and Security Hardening
    1. Logon and Password Policies
    2. Network Equipment Handling
    3. Public Services Protection
    4. Events Monitoring
    5. Firewall Policies

2. Cyber Security Incident Response, Digital Forensics Investigation and Application Security
    1. Incident Response Work Task Server, Web Server
    2. Incident Response Work Task Server, File Server
    3. Vulnerability Detection and Repair, Web Server
    4. Vulnerability Detection and Repair, File Server
    5. Digital Forensic, Linux Server
    6. Digital Forensic, Win Img, Memory Dump
    7. Digital Forensic, Network analysis (network pcap)
    8. Digital Forensic, system img
    9. Code Review

3. Capture the Flag (**Attack**)
    1. Enumeration
    2. Web-based Attack
    3. Database Attack
    4. Windows Attack
    5. Root Access
    6. Cryptography
    7. Steganography

4. Capture the Flag (**Defense**)
    1. Reconnaissance and Application detection
    2. Malicious URL
    3. Exploits

4. Botnet
5. Data leak
6. Reverse Engineering