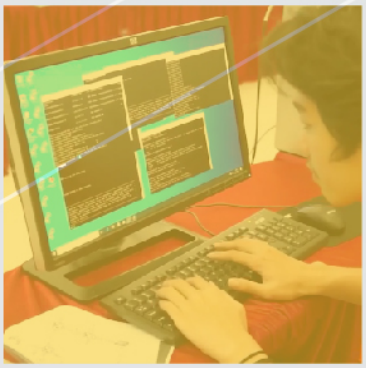
PUSAT PRESTASI NASIONAL
KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN

LKS SMK TINGKAT NASIONAL 28

PANDUAN TEKNIS PELAKSANAAN LKS SMK TINGKAT NASIONAL XXVIII TAHUN 2020

Teknologi Keamanan Siber *Cyber Security*



KATA PENGANTAR

Salah satu dari 4 pilar utama visi Indonesia tahun 2045 adalah pembangunan manusia dan penguasaan IPTEK (lmu Pengetahuan dan Teknologi), dengan peningkatan taraf Pendidikan rakyat Indonesia secara merata, peran kebudayaan dalam pembangunan, sumbangan IPTEK (lmu Pengetahuan dan Teknologi) dalam pembangunan, derajat kesehatan dan kualitas hidup rakyat, serta reformasi ketenagakerjaan. Sejalan dengan visi tersebut, dalam peningkatan pendidikan IPTEK (ilmu Pengetahuan dan Teknologi) merata pada era digitalisasi ini, siswa Sekolah Menengah Kejuruan (SMK) dituntut tidak saja harus menguasai penggunaan peralatan digital tetapi juga wajib menguasai softskill yang mumpuni.

Karena IPTEK dan komunikasi saling terkait dan tidak bisa dipisahkan, maka pada era digitalisasi disruptif, akan ada pekerjaan baru yang tercipta dan pekerjaan konvensional yang akan hilang. Untuk itu, siswa SMK harus senantiasa meningkatkan kualitas diri dan penguasaan keterampilan agar dapat memenuhi tuntutan pasar kerja, baik di masa kini maupun di masa yang belum kita prediksikan. Pekerjaan – pekerjaan yang selama ini dikerjakan yang sudah ada akan digantikan oleh sistim Artificial Intelligence (AI), otomatisasi atau robot yang dapat mengambil alih beberapa peran kerja manusia. Namun secanggih-canggihnya kemajuan IPTEK, hal yang pasti muskil digantikan oleh AI adalah *softskills* seperti Komunikasi & Empati, Berpikir Kritis, Kreatifitas, Strategi, Pengelolaan Teknologi, instalasi dan maintenance, keterampilan fisik, dan visi & imajinasi. Era digitalisasi maupun otomasi, dapat mengubah struktur ekonomi maupun tenaga kerja di Indonesia, kecuali beberapa pekerjaan yang sulit diotomasi misalnya kemampuan *softskills* (berinteraksi dengan orang lain dan keahlian khusus).

Lomba Kompetensi Siswa (LKS) SMK Tingkat Nasional XXVIII Tahun 2020 ini akan berbeda dengan LKS pada umumnya, dengan munculnya pandemi Covid-19 mendorong Indonesia untuk berubah dan tidak lagi menjalankan pola-pola yang lama. Seluruh lomba-lomba yang diselenggarakan oleh Pusat Prestasi Nasional dilakukan secara daring dengan memperhatikan protokol kesehatan Covid-19. Sisi baik dari tantangan ini adalah siswa SMK diajak untuk bersahabat dan berkolaborasi dengan teknologi daring. Pusat Prestasi Nasional melakukan pembaharuan dengan melaksanakan LKS 2020 secara daring. LKS Tingkat Nasional Tahun 2020 melombakan sebanyak 42 bidang lomba. Diharapkan pada masa pandemi Covid-19 tidak mengurangi semangat siswa untuk berprestasi.

Sehubungan dengan hal tersebut, Pusat Prestasi Nasional, Sekretariat Jenderal, Kementerian Pendidikan dan Kebudayaan ikut mendukung pengembangan kualitas SMK dalam mengikuti perkembangan IPTEK dan memenuhi Visi Indonesia 2045. LKS Tingkat Nasional Tahun 2020 adalah salah satu kegiatan untuk mendorong semangat berprestasi peserta didik SMK yang diadakan setiap

tahun dan sebagai upaya mempromosikan lulusan SMK kepada dunia usaha/dunia industri serta pemangku kepentingan lainnya.

Panduan Teknis LKS SMK Tingkat Nasional XXVIII Tahun 2020 Daring merupakan dokumen pendukung pelaksanaan LKS demi tercapainya kegiatan agar berjalan dengan baik dan dapat memberikan informasi kepada semua pihak yang ikut berpartisipasi dalam pelaksanaan LKS.

Dalam kesempatan ini disampaikan ucapan terimakasih kepada semua pihak yang telah mendukung dalam penyusunan Panduan Teknis pelaksanaan LKS SMK Tingkat Nasional XXVIII Tahun 2020.

Plt. Kepala Pusat Prestasi Nasional

Asep Sukmayadi, S.IP., M.Si

NIP. 197206062006041001

DAFTAR ISI

Halaman

A. PENDAHULUAN

A.1. Nama dan Deskripsi Bidang Lomba

A.1.1. Nama Bidang Lomba

Cyber Security

A.1.2. 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 kemanan 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.

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.

A.2. Faktor Resiko dan Keselamatan Kerja

Semua personel yang terlibat harus mematuhi undang-undang Kesehatan, Keselamatan, dan Lingkungan yang ditentukan oleh Penyelenggara lomba serta Kebijakan dan Regulasi Kesehatan, Keselamatan, dan Lingkungan WorldSkills untuk kompetisi keterampilan.

A.3. Kompetensi Keahlian Peserta Lomba

Section	Kriteria	Nilai	Aspect Marks	Variation
1	Work organization and management	5,00	0,00	5,00
2	Communication and interpersonal skills	10,00	0,00	10,00
3	Securely provision	15,00	0,00	15,00
4	Operate and maintain & oversee and govern	15,00	0,00	15,00
5	Protect and defend	15,00	0,00	15,00
6	Analyze	10,00	0,00	10,00
7	Collect and operate	15,00	0,00	15,00
8	Investigate	15,00	0,00	15,00
		Total Variation		100,00

A.4. Karakter Kerja Bidang Lomba

Criteria		
ID	Name	Mark
A	Infrastructure Setup and Security Hardening	25,00
B	CyberSecurity Incident Response , Digital Forensics Investigation and Application Security	25,00
C	Capture the Flag (Attack)	25,00
D	Capture the Flag (Defence)	25,00
E		
F		
G		
H		
I		

B. STANDAR KOMPETENSI BIDANG LOMBA

B.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

B.2. Spesifikasi Kompetensi LKS-SMK

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**

C. SISTEM PENILAIAN

C.1. Petunjuk Umum

Bagian ini menjelaskan peran dan tempat Skema Penilaian, bagaimana Juri akan menilai pekerjaan peserta seperti yang ditunjukkan melalui *Test Project*, dan juga prosedur dan persyaratan untuk penilaian.

Skema Penilaian adalah instrumen penting dari lomba, di mana akan menghubungkan penilaian dengan standar nilai yang mewakili keterampilan. Hal Ini dirancang untuk mengalokasikan nilai untuk setiap aspek kinerja yang dilombakan sesuai dengan bobot dalam Spesifikasi Standar.

Dengan memberikan bobot dalam Spesifikasi Standar, Format Penilaian menetapkan parameter untuk desain *Test Project*. Bergantung pada sifat keterampilan dan kebutuhan penilaiannya. Pada awalnya mungkin tepat untuk mengembangkan Format Penilaian secara lebih rinci sebagai panduan untuk desain Test Project. Atau, desain *Test Project* awal dapat didasarkan

pada garis besar Skema Penilaian. Dari titik ini dan seterusnya, Skema Penilaian dan Test Project harus dikembangkan bersama.

Format Penilaian dan *Test Project* dapat dikembangkan oleh satu orang, atau beberapa, atau oleh semua Ahli. Format Penilaian dan *Test Project* yang terperinci dan final harus disetujui oleh seluruh Juri Ahli sebelum diajukan untuk jaminan kualitas independen. Pengecualian untuk proses ini adalah untuk kompetisi keterampilan yang menggunakan perancang independen untuk pengembangan Format Penilaian dan *Test Project*. Silakan lihat Peraturan untuk perincian lebih lanjut.

Para ahli dan perancang independen diwajibkan untuk menyerahkan Format Penilaian dan Test Project untuk komentar dan persetujuan sementara sebelum penyelesaian, untuk menghindari kekecewaan atau kemunduran pada tahap akhir. Mereka juga disarankan untuk bekerja dengan Tim *Competition Information System* (CIS) pada tahap menengah ini, untuk memanfaatkan sepenuhnya kemungkinan CIS.

Dalam semua kasus konsep Format Penilaian harus dimasukkan ke dalam CIS setidaknya delapan minggu sebelum Kompetisi menggunakan *spreadsheet* standar CIS atau metode lain yang disepakati.

D. TEST PROJECT

D.1. Petunjuk Umum

Apakah itu merupakan entitas tunggal, atau serangkaian modul yang berdiri sendiri atau terhubung, Test Project akan memungkinkan penilaian keterampilan di setiap bagian. Tujuan dari Test Project adalah untuk memberikan peluang penuh, seimbang dan otentik untuk penilaian dan penandaan di Spesifikasi Standar, dalam hubungannya dengan Format Penilaian. Hubungan antara Test Project, Format Penilaian, dan Spesifikasi Standar akan menjadi indikator utama kualitas, sebagaimana juga hubungannya dengan kinerja kerja aktual.

Test Project tidak akan mencakup area di luar Spesifikasi Standar, atau mempengaruhi keseimbangan tanda dalam Spesifikasi Standar selain dari keadaan yang ditunjukkan oleh Bagian 2.

Test Project akan memungkinkan pengetahuan dan pemahaman untuk dinilai hanya melalui aplikasi mereka dalam pekerjaan praktis. *Test Project* tidak akan menilai pengetahuan tentang peraturan dan regulasi lomba. Uraian Teknis ini akan mencatat setiap masalah yang memengaruhi kapasitas *Test Project* untuk mendukung berbagai penilaian relatif terhadap Spesifikasi Standar.

D.2. Kriteria Penilaian

Judul utama Skema Penandaan adalah Kriteria Penilaian. Judul-judul ini diturunkan bersamaan dengan *Test Project*. Dalam beberapa kompetisi keterampilan, Kriteria Penilaian mungkin serupa dengan judul bagian dalam Spesifikasi Standar; pada orang lain mereka mungkin sama sekali berbeda. Biasanya akan ada antara lima dan sembilan Kriteria Penilaian. Apakah judul cocok atau tidak, Skema Penandaan secara keseluruhan harus mencerminkan bobot dalam Spesifikasi Standar.

Kriteria Penilaian dibuat oleh orang yang mengembangkan Skema Penandaan, yang bebas untuk menentukan kriteria yang mereka anggap paling cocok untuk penilaian dan penandaan Proyek Uji. Setiap Kriteria Penilaian didefinisikan oleh huruf (A-I). Dianjurkan untuk tidak menentukan Kriteria Penilaian, atau alokasi tanda, atau metode penilaian, dalam Deskripsi Teknis ini.

Formulir Ringkasan Merek yang dihasilkan oleh CIS akan terdiri dari daftar Kriteria Penilaian.

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.

D.3. 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.

D.4. Aspek

Setiap Aspek mendefinisikan, secara rinci, satu item yang akan dinilai dan ditandai bersama dengan tanda, atau instruksi untuk bagaimana tanda tersebut diberikan. Aspek dinilai baik dengan pengukuran atau penilaian.

Formulir penandaan mencantumkan, secara rinci, setiap Aspek yang akan ditandai bersama dengan tanda yang dialokasikan untuknya.

Jumlah tanda yang dialokasikan untuk setiap Aspek harus berada dalam kisaran tanda yang ditentukan untuk bagian keterampilan dalam Spesifikasi Standar tersebut. Ini akan ditampilkan dalam Tabel Alokasi Mark CIS, dalam format berikut, ketika Skema Penandaan ditinjau dari C-8 minggu. (Bagian 4.1)

		CRITERIA								TOTAL MARKS PER SECTION	WSSS MARKS PER SECTION	VARIANCE
		A	B	C	D	E	F	G	H			
STANDARDS SPECIFICATION SECTION	1	5.00								5.00	5.00	0.00
	2		2.00					7.50		9.50	10.00	0.50
	3								11.00	11.00	10.00	1.00
	4			5.00						5.00	5.00	0.00
	5				10.00	10.00	10.00			30.00	30.00	0.00
	6		8.00	5.00				2.50	9.00	24.50	25.00	0.50
	7			10.00				5.00		15.00	15.00	0.00
TOTAL MARKS		5.00	10.00	20.00	10.00	10.00	10.00	15.00	20.00	100.00	100.00	2.00

D.5. Penilaian Measurement

Harus ada satu tim penilaian untuk setiap Sub Kriteria, apakah dinilai dan ditandai oleh penilaian, pengukuran, atau keduanya. Tim penandaan yang sama harus menilai dan menandai semua pesaing, dalam segala keadaan. Tim penanda harus diorganisir untuk memastikan bahwa tidak ada tanda rekan senegaranya dalam keadaan apa pun. (Lihat 4.6.)

D.6. Komposisi Penilaian *Judgement* dan Measurement

Penilaian menggunakan skala 0-3. Untuk menerapkan skala dengan ketelitian dan konsistensi, penilaian harus dilakukan menggunakan:

• tolok ukur (kriteria) untuk panduan terperinci untuk setiap Aspek (dalam kata-kata, gambar, artefak atau catatan pedoman terpisah)

• skala 0-3 untuk menunjukkan:

• 0: kinerja di bawah standar industri

• 1: kinerja memenuhi standar industri

• 2: kinerja memenuhi dan, dalam hal tertentu, melebihi standar industri

• 3: kinerja sepenuhnya melebihi standar industri dan dinilai sangat baik

Tiga Pakar akan menilai setiap Aspek, dengan yang keempat untuk mengkoordinasikan penilaian dan bertindak sebagai juri.

D.7. Keseluruhan Penilaian Keterampilan

Karena ini adalah keterampilan baru, spesifikasi penilaian keterampilan akan ditentukan oleh Para Pakar.

D.8. Prosedur Asesmen Keterampilan

Semua Ahli harus ditugaskan ke tim modul. Hasil kerja Peserta tidak dapat diubah dengan cara apa pun untuk memfasilitasi penilaian kecuali termasuk dalam skema penilaian.

Para Ahli yang menghadiri Kompetisi akan dibagi menjadi kelompok penilaian yang lebih kecil dalam tim modul mereka untuk menandai setiap bagian spesifik dari kriteria penilaian. Penandaan progresif untuk semua bagian Kompetisi Setiap modul / tugas / bagian akan diselesaikan pada hari yang ditentukan sehingga penandaan progresif dapat terjadi.

Skema penandaan:

• Setiap Pesaing diberikan Formulir Ringkasan Nilai

• "Skema cara-penilaian" lengkap hanya akan dilihat oleh Para Ahli. (Alasan: Skema Penandaan lengkap akan memberikan jawaban kepada peserta.)

E. ALAT

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

Skenario peralatan adalah dengan jumlah finalis sebanyak 11 Tim (22 peserta), 3 juri dan 10 Pakar.

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	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	Webserver (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.

IT Hardware

Jumlah	Nama	Keterangan	Penempatan
1 per peserta	Laptop	Peserta boleh menggunakan Laptop Jenis apa saja selama laptop tersebut mampu OS Kali Linux dan/atau Windows 10	Area Kerja Peserta
2 per keahlian	Digital Clock		Briefing Area
2 per keahlian	Laptop	Spesifikasi Minimal CPU i5 / RAM 8 GB DDR4 / HDD 1Tb OS Win/Linux	Ruang Pakar
1 per keahlian	Projector	20000:1, 1280x800, HDMI	Ruang Pakar
1 per keahlian	Screen Projector	Lumien, 244x244 cm	Ruang Pakar
1 per keahlian	Cable HDMI (3 m)		Ruang Pakar
1 per keahlian	Laser printer A4 - Type 2	Color laser Jet	Ruang Pakar
1 per juri	Laptop	Spesifikasi Minimal CPU i5 / RAM 8 GB DDR4 / HDD 1Tb OS Win/Linux	Ruang Juri
1 per keahlian	TV Monitor	50 inch, HDMI	Ruang Juri
1 per keahlian	Cable HDMI	Cable HDMI	Ruang Juri

IT Services

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

		GB,VPS Panel, Unmetered Bandwidth	
1 per keahlian	VPS (Live Monitoring)	2 CPU Dual Core, RAM 16GB, Storage 512 GB, VPS Panel, Unmetered Bandwidth	VPS Provider
1 per keahlian	VPS (Penyisihan)	4 CPU dual core, RAM 32GB, Storage 1TB, VPS Panel, Unmetered Bandwidth	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 Red 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
1 per keahlian	Earplugs		Briefing Room

F. BAHAN

Peserta perlu mempersiapkan:

- 1 buah PC/Laptop yang terhubung ke Internet dan dilengkapi dengan:
    - *Operating System* Linux, *Distro* Kali Linux
    - *WebCam*
    - Zoom.us
    - Telegram *Desktop*
- 1 buah PC/Laptop yang terhubung ke internet dan dilengkapi dengan:
    - OS Windows/Linux/Apple
    - *Webcam*
    - Zoom.us
    - *Office Application* untuk pembuatan laporan
- Pelaksana lomba perlu menyiapkan:
    - Sistem Uji dan Penilaian Daring untuk tahap penyisihan dan final yang berupa *Virtual Private Server*, dengan spesifikasi minimal 2 CPU dual core, RAM 16GB, HDD 512GB.
    - *Virtual Private Server* sebagai sarana final kompetisi daring dengan spesifikasi minimal 1 CPU dual core, RAM 4, HDD 128GB
    - *Virtual Private Network* sebagai sarana koneksi dari peserta final kompetisi daring ke VPS
    - Saran Kompetisi dapat disediakan oleh penyelenggara layanan *Cloud*.
    - Soal -Soal sesuai dengan jumlah jumlah dan tingkat kompetisi.
    - Blue Team, sebagai tim untuk melakukan pemantauan scoring/nilai dan progress kompetisi.
    - Red Team, sebagai tim penyerang

G. BAHAN PENUNJANG

~~Peserta tidak diperbolehkan membawa bahan penunjang selama mengikuti lomba~~

H. LAYOUT DAN LUASAN

Luasan Ruang yang diperlukan:

- Ruang Kerja Peserta (Ruang Lomba) dengan kebutuhan luasan: min. 12m^2
- Ruang Juri Penilaian dengan kebutuhan luasan: 30m^2
- Ruang Briefing dengan luasan: min. 60m^2
- Ruang Pakar dengan luasan: min. 20m^2

I. JADWAL BIDANG LOMBA

Usulan jadwal untuk bidang lomba Cyber Security adalah sebagai berikut:

- Tahap Penyisihan
    - Durasi: 1 hari, setiap sesi berlangsung selama 135 menit
    - Materi *Capture the Flag* dan Forensik
- Tahap Final,
    - Durasi: 1 hari, setiap sesi berlangsung selama 135 menit
    - Materi: *Cyber Security Incident Response, Digital Forensic Investigation, and Application Security*

J. KEBUTUHAN LAIN DAN SPESIFIKASINYA

Ukuran 12 x 20m Kebutuhan Ruang untuk pengunjung

K. REKOMENDASI JURI

Juri yang direkomendasikan:

- Irwin Day (Federasi Teknologi Informasi Indonesia)
- Muhammad Salahuddien (CISRT.ID)
- Bisyron Wahyudi (CISRT.ID)

Lampiran 1: Test Project LKS

Test Project 1: Infrastructure Setup and Security Hardening

Test Project 2: Cyber Security Incident Response, Digital Forensic Investigation, and Application Security

Test Project 3: Capture the Flag (CTF) Attack

Test Project 4: Capture the Flag (CTF) Defence

Lampiran 2: Format Penilaian

Cyber Security Marking Scheme

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 Row (Export only)	Max Mark
A1	Logon and password policies	2								
			M	Security banner (Windows machines)		On random windows machine go to login sreen	Look for banner	4		0,25
			M	Password minimum length (Windows machines)		Pick random preconfigured account, change password to rand	Error messege (doe	4		0,25
			M	Password complexity (Windows machines)		Pick random preconfigured account, change password to rand	Error messege (doe	4		0,25
			M	Cached logins (Windows machines)		On random windows client machine - login with random accou	Should not be let yo	4		0,25
			M	Account lockdown (Windows machines)		On random windows machine - try to login 3 times with incorre	Login screen must b	4		0,25
			M	Inactivity timeout (Windows machines)		On random windows machine login and wait for 1 min	After 1 min you shou	4		0,25
			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 rand	Error messege (doe	4		0,25
			M	Password complexity (Linux machines)		Pick random preconfigured account, change password to rand	Error messege (doe	4		0,25
			M	Account lockdown (Linux machines)		On random linux machine - try to login 3 times with incorrect pa	Login screen must b	4		0,25
			M	Inactivity timeout (Linux machines)		On random linux machine login and wait for 1 min	After 1 min you shou	4		0,25
			M	Password minimum length (Network equipment)		Pick random preconfigured account, change password to rand	Error messege (doe	4		0,25
			M	Password complexity (Network equipment)		Pick random preconfigured account, change password to rand	Error messege (doe	4		0,25
			M	Reversible cipher text for non-hashed passwords (Network equipment		On random IOS device - sh run | i password	Look for service pas	4		0,25
			M	Scrypt hash for username passwords (Network equipment)		On random IOS device - sh run | i username	Look for secret 9 $9	4		0,25
			M	Security banner (Network equipment)		On random cisco device go to login sreen	Look for banner	4		0,25
			M	Account lockdown (Network equipment)		On random cisco device - try to login 3 times with incorrect pas	Login screen must b	4		0,25
			M	Remote console authentication (Network equipment)		From any machine — SSH to a random cisco device	Look for username/p	4		0,25
			M	Inactivity timeout (Network equipment)		On random cisco device login and wait for 1 min	After 1 min you shou	4		0,25
			M	Restrict Guest to be logon locally for Guests group		Check on both DC and Ivan	Policy applied to the	4		0,25
			M	Disable FIPS compliant alogrithms for encryption, hashing and signing		Check on both DC and Ivan	Policy applied to the	4		0,25
			M	Enforce Digital encryption or signing the secure channel data for Dom		Check on both DC and Ivan	Policy applied to the	4		0,25
			M	Always Digitally sign the communication for the Server		Check on both DC and Ivan	Policy applied to the	4		0,25
A2	Network equipment hardening	2								
			M	Site-to-site VPN is operational		From random machine on IAR site ping dc.nlsz.ru	Ping must be succes	4		0,50
			M	Remote access VPN is operational		From Nikolai - if nothing indicated in Remote access VPN impl	Ping must be succes	4		0,50
			J	IPsec implementation				4		0,75
					0	Not operational or AH is used				
					1	IKEv1+PSK				
					2	IKEv1+RSA or IKEv2+PSK				
					3	IKEv2+RSA				
			J	Remote access VPN implementation				4		0,75
					0	Not operational				
					1	PPTP				
					2	L2TP / IPsec				
					3	AnyConnect (or FlexVPN, DirectAccess, etc.)				
			J	Additional security measures listing				1		0,75
					0	no attempt				
					1	1 logical security measure				
					2	2 logical additional security measures				
					3	3 logical additional security measures				
			J	Implementation of additional security measures				1		1,00
					0	no attempt				
					1	1 logical security measure				
					2	2 logical additional security measures				
					3	3 logical additional security measures				
A3	Public services protection	2								
			M	Web-01 website is running HTTPS, all HTTP requests are redirected t		From Nikolai — open http://www.nlsz.ru	HTTP request must	4		0,50
			M	Web-02 accepts explicit SSL / TLS connections only		From Nikolai — open ftp.nlsz.ru, check logs on Web-02	Connection must be	4		0,50
			J	Additional security measures listing				1		0,75
					0	no attempt				
					1	1 logical security measure				
					2	2 logical additional security measures				
					3	3 logical additional security measures				
			J	Implementation of additional security measures				1		1,00
					0	no attempt				
					1	1 logical security measure				
					2	2 logical additional security measures				
					3	3 logical additional security measures				
A4	Events monitoring	2								
			M	Installation and configuration of splunk universal forwarder			Splunk universal for	7		0,50
			M	Configuring splunk for receiving the logs on port 8090			Splunk configured to	7		0,50
			M	Configuring the data input on splunk to integrate domain controller			DC integrated with S	7		0,50
			M	Validating the integration of the logs by navigating to settings --> data			Logs validated.	7		0,50
			M	FTP traffic alerts		From Ivan — open IDS dashboard at log.nlsz.ru	Look for FTP traffic .	7		1,00
			M	ICMP traffic alerts		From Ivan — open IDS dashboard at log.nlsz.ru	Look for ICMP traffic	7		1,00
			M	Malware traffic alerts		From Ivan — open IDS dashboard at log.nlsz.ru	Look for malware tra	7		1,00
			J	Additional security measures listing				1		0,75
					0	no attempt				
					1	1 logical security measure				
					2	2 logical additional security measures				
					3	3 logical additional security measures				
			J	Implementation of additional security measures				1		1,00
					0	no attempt				
					1	1 logical security measure				
					2	2 logical additional security measures				
					3	3 logical additional security measures				
A5	Firewall policy	2								
			M	DC		Check firewall for Domain network, Private Network, Public Ne	Should be green, do	4		0,50
			M	Ivan		Check firewall for Domain network, Private Network, Public Ne	Should be green, do	4		0,50
			M	Boris		Check firewall for Domain network, Private Network, Public Ne	Should be green, do	4		0,50
			M	Anton		Check firewall for Domain network, Private Network, Public Ne	Should be green, do	4		0,50
			M	Firewall on Domain Controller to be configured to allow the communica			Check Windows firel	4		0,50
			M	IDS		Check Iptables and firewalld	Doesn't contain "per	4		0,50
			M	LOG		Check Iptables and firewalld	Doesn't contain "per	4		0,50
			M	Web-01		Check Iptables and firewalld	Doesn't contain "per	4		0,50
			M	Web-02		Check Iptables and firewalld	Doesn't contain "per	4		0,50
			M	LED		Check access groups on outbound interface	ACL doesn't contain	4		0,50
			M	IAR		Check access groups on outbound interface and global policy	ACL doesn't contain	4		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 Row (Export only)	Max Mark
B1	Incident Response:Work Task Server Web_Server	1								
			M	Find and submit the relevant commands and the parameters that is us		Answer to be recorded in the Data sheet given		5		0,50
			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				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 create				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 se		Fill in the cybersecurity incident response report		5		0,50
			J	Analyze the intrusion behavior and influence of hacker.				5		0,50
					0	does not have enough report incident factor				
					1	enough report incident factor				
					2	enough report incident factor and exceeds it in some respects				
					3	is excellent relative to the report				
			J	What are safety corrective measures for this incident?				5		0,50
					0	does not have enough report incident factor				
					1	enough report incident factor				
					2	enough report incident factor and exceeds it in some respects				
					3	is excellent relative to the report				
B2	Incident Response:Work Task Server File_Server	1								
			M	Find and submit the i) pathname and ii) filename of the malicious prog		Answer to be recorded in the Data sheet given		5		0,50
			M	ii) filename				5		0,50
			M	Submit the SHA1 checksum of the malicious program that locked your				5		0,50
			M	Find and submit the i) pathname and ii) filename of the stager program				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
			J	What is the harmful impact of this incident?				6		0,50
					0	does not have enough report incident factor				
					1	enough report incident factor				
					2	enough report incident factor and exceeds it in some respects				
					3	is excellent relative to the report				
			J	What are safety corrective measures for this incident?				6		0,50
					0	does not have enough report incident factor				
					1	enough report incident factor				
					2	enough report incident factor and exceeds it in some respects				
					3	is excellent relative to the report				
B3	Vulnerability Detection and Repair: Work Task Serve	1								
			M	Modify PHP to forbid dangerous functions and submit changes made.		Answer to be recorded in the Data sheet given		6		0,25
			M	Modify Mysql's setting to limit the actions of importing and exporting ar				6		0,25
			M	Delete and submit the directory of the management tool on the web er		Fix the weak password issues		6		0,25
			M	Submit the plain text of the weak password				6		0,25
			M	Submit the URL of the pages with weak password				6		0,25
			M	Submit the signature string "Passw0rd_*******" on the feedback page a				6		0,25
B4	Vulnerability Detection and Repair: Work Task Serve	1								
			M	Delete THREE malicious programs on the operating system and the i)		Answer to be recorded in the Data sheet given		6		0,25
			M	Delete THREE malicious programs on the operating system and the i)				6		0,25
			M	Delete THREE malicious programs on the operating system and the i)				6		0,25
			M	Change the administrator password to the string in parentheses (App[				6		0,25
			M	Deny access the 3389 port on the file server through the windows firev				6		0,50
B5	Digital Forensic Investigation: Work Task Server Lin	1								
			M	Identify malicious program processes		Answer to be recorded in the Data sheet given		8		0,50
			M	Locate malicious program files				8		0,50
			M	Recover system settings modified by malware (Describe the steps, ho				8		0,50
			J	Analyse ELF files to describe their behaviour				8		0,50
					0	does not have enough report incident factor				
					1	enough report incident factor				
					2	enough report incident factor and exceeds it in some respects				
					3	is excellent relative to the report				
B6	Digital Forensic Investigation: Work Task Win.img, n	1								
			M	Identify malicious program processes		Answer to be recorded in the Data sheet given		8		0,25
			M	Find hidden locations of malicious programs				8		0,50
			M	Find the key left by malicious programs in memory				8		0,50
			M	Recover the corrupted file by malware and then submit the file conten				8		0,25
			J	Analyse PE files to describe their behaviour				8		0,50
					0	does not have enough report incident factor				
					1	enough report incident factor				
					2	enough report incident factor and exceeds it in some respects				
					3	is excellent relative to the report				
B7	Digital Forensic Investigation: Work Task Network A	1								
			M	Identify and submit the key(dump_rev.pcap)		Answer to be recorded in the Data sheet given		8		0,50
			M	Identify malicious program process.				8		0,25
			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
			J	Analyse PE files to describe their behaviour.				8		0,50
					0	does not have enough report incident factor				
					1	enough report incident factor				
					2	enough report incident factor and exceeds it in some respects				
					3	is excellent relative to the report				
B8	Digital Forensic Investigation: Work Task Test.pdf, s	1								
			M	Extract malicious file, and submit the MD5 of malicious file		Answer to be recorded in the Data sheet given		8		0,75
			M	Decrypt the encrypted file, and submit the file content				8		0,75
			J	Analyse the malicious file(payload).				8		0,50
					0	does not have enough report incident factor				
					1	enough report incident factor				
					2	enough report incident factor and exceeds it in some respects				
					3	is excellent relative to the report				
B9	Code Review: Work Task Code Review1	1								
			M	Identify the vulnerable line of code that poses a security threat.		Answer to be recorded in the Data sheet given		3		0,25
			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.		Answer to be recorded in the Data sheet given		3		0,25
			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.		Answer to be recorded in the Data sheet given		3		0,25
			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 Row (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		1,50
			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		1,50
			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		1,50
			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	Windows Attacks	3								
			M	All flags to the vulnerable windows server		Windows Attack Flags (Flags 1-3) (1 flag - 0.5)		5		1,50
			M	All flags to the vulnerable windows server		Windows Attack Flags (Flags 4-5) (1 flag - 0.5)		2		1,00
			M	All flags to the vulnerable windows server		Windows Attack Flags (Flags 6-10) (1 flag - 0.2)		5		1,00
C5	Root Access	3								
			M	All flags after root access into vulnerable system		Root Access Flags (Flags 1-3) (1 flag - 0.5)		5		1,50
			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
C6	Cryptography	3								
			M	All flags related to cryptography		Cryptography Flags (Flags 1-3) (1 flag - 0.5)		3		1,50
			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
C7	Steganography	3								
			M	All flags related to steganography		Steganography Flags (Flags 1-3) (1 flag - 0.5)		3		1,50
			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		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 Row (Export only)	Max Mark
D1	Reconnaisance and Application Detection	4								
			M	All flags related to understanding application and recon methods		Recconaisance and Application Detection (Flags 1-3) (1 flag -		7		1,50
			M	All flags related to understanding application and recon methods		Recconaisance and Application Detection (Flags 4-5) (1 flag -		2		1,00
			M	All flags related to understanding application and recon methods		Recconaisance and Application Detection (Flags 6-10) (1 flag		7		1,00
D2	Malicious URL	4								
			M	All flags relating to detecting spam email and malicious url detection		Malicious URL Flags (Flags 1-3) (1 flag - 0.5)		3		1,50
			M	All flags relating to detecting spam email and malicious url detection		Malicious URL Flags (Flags 4-5) (1 flag - 0.5)		2		1,00
			M	All flags relating to detecting spam email and malicious url detection		Malicious URL Flags (Flags 6-10) (1 flag - 0.2)		7		1,00
D3	Exploits, Drive by download malware	4								
			M	All flags related to exploits and malware		Exploit & Malware Flags (Flags 1-3) (1 flag - 0.5)		7		1,50
			M	All flags related to exploits and malware		Exploit & Malware Flags (Flags 4-5) (1 flag - 0.5)		2		1,00
			M	All flags related to exploits and malware		Exploit & Malware Flags (Flags 6-10) (1 flag - 0.2)		7		1,00
D4	Botnet	4								
			M	All flags in detecting bots and botnet traffic & lateral propagation		Botnet Flags (Flags 1-3) (1 flag - 0.5)		7		1,50
			M	All flags in detecting bots and botnet traffic & lateral propagation		Botnet Flags (Flags 4-5) (1 flag - 0.5)		2		1,00
			M	All flags in detecting bots and botnet traffic & lateral propagation		Botnet Flags (Flags 6-10) (1 flag - 0.2)		7		1,00
D5	Data Leakage	4								
			M	All flags in detecting data being leaked out of the network		Data Leakage Flags (Flags 1-3) (1 flag - 0.5)		3		1,50
			M	All flags in detecting data being leaked out of the network		Data Leakage Flags (Flags 4-5) (1 flag - 0.5)		2		1,00
			M	All flags in detecting data being leaked out of the network		Data Leakage Flags (Flags 6-10) (1 flag - 0.2)		3		1,00
D6	Reverse Engineering	4								
			M	All flags related to reverse engineering		Reverse Engineering Flags (Flags 1-3) (1 flag - 0.5)		8		1,50
			M	All flags related to reverse engineering		Reverse Engineering Flags (Flags 4-5) (1 flag - 0.5)		8		1,00
			M	All flags related to reverse engineering		Reverse Engineering Flags (Flags 6-10) (1 flag - 0.2)		8		1,00
D7	Forensic	4								
			M	All flags related to forensics		Forensics Flags (Flags 1-3) (1 flag - 0.5)		8		1,50
			M	All flags related to forensics		Forensics Flags (Flags 4-5) (1 flag - 0.5)		8		1,00
			M	All flags related to forensics		Forensics Flags (Flags 6-10) (1 flag - 0.2)		8		1,00
			M	At least 1 flag from 5 categories				7		0,50

Kisi Kisi Cyber Security LKS 2020

1. Infrastrucure Setup and Security Hardening
    a. Logon and Password Policies
    b. Network Equipment Handling
    c. Public Services Protection
    d. Events Monitoring
    e. Firewall Policies

2. CyberSecurity Incident Response, Digital Forensics Investigation and Application Security
    a. Incident Response Work Task Server, Web Server
    b. Incident Response Work Task Server, File Server
    c. Vulnerability Detection and Repair, Web Server
    d. Vulnerability Detection and Repair, File Server
    e. Digital Forensic, Linux Server
    f. Digital Forensic, Win Img, Memory Dump
    g. Digital Forensic, Network analysis (network pcap)
    h. Digital Forensic, system img
    i. Code Review

3. Capture the Flag/Attack
    a. Enumeration
    b. Web Based Attack
    c. Database Attack
    d. Windows Attack
    e. Root Access
    f. Cryptography
    g. Steganography

4. Capture the Flag/Defence
    a. Reconnaisance and Application detection
    b. Malicious URL
    c. Exploits
    d. Botnet
    e. Data leak
    f. Reverse Engineering