Balai Pengembangan Talenta Indonesia
Pusat Prestasi Nasional
Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi

MERDEKA BELAJAR

LKS SMK TINGKAT NASIONAL

SMK

Deskripsi Teknis

Lomba Kompetensi Siswa Nasional 2024

Teknologi Keamanan Siber

(Cyber Security)

DESKRIPSI TEKNIS

Cyber Security (Cyber Security)

KELOMPOK
TEKNOLOGI INFORMASI & KOMUNIKASI

LOMBA KOMPETENSI SISWA SEKOLAH MENENGAH KEJURUAN

TINGKAT NASIONAL XXXI

TAHUN 2024

KATA PENGANTAR

Kegiatan ajang talenta merupakan wahana aktualisasi unjuk prestasi peserta didik, yang juga menjadi momentum untuk menemukenali anak-anak berbakat atau yang mempunyai potensi talenta di atas rata-rata. Dalam mengikuti ajang talenta, mereka akan mendapatkan tantangan terutama dalam menghasilkan suatu karya dan menjadi yang terbaik. Kegiatan ajang talenta merupakan bagian dari proses pembinaan prestasi talenta secara berkelanjutan, dan turut andil dalam mengembangkan karakter peserta didik menuju profil Pelajar Pancasila.

Balai Pengembangan Talenta Indonesia (BPTI) menyelenggarakan ajang talenta setiap tahun di berbagai bidang. Dalam kerangka program Manajemen Talenta Nasional (MTN), BPTI/Puspresnas melakukan pembinaan berkelanjutan untuk menghasilkan bibit-bibit talenta unggul di bidang-bidang Riset dan Inovasi; Seni dan Budaya; serta Olahraga.

Menandai semangat Merdeka Belajar, Merdeka Berprestasi, aktualisasi prestasi melalui ajang talenta didasarkan pada minat dan bakat. Pemerintah mulai memberikan perhatian yang lebih serius terhadap anak-anak yang berprestasi di berbagai bidang ketalentaan. Mereka yang berhasil akan mendapatkan banyak manfaat untuk pengembangan karir belajar atau karir profesionalnya, seperti beasiswa atau pembinaan lanjut untuk mencapai prestasi maksimal.

Lomba Kompetensi Siswa Sekolah Menengah Kejuruan (LKS SMK) adalah sebuah ajang talenta di bidang riset dan inovasi yang diselenggarakan untuk peserta didik Sekolah Menengah Kejuruan (SMK). Ajang LKS diselenggarakan secara bertingkat mulai dari daerah hingga nasional, untuk menjaring peserta terbaik dari 38 provinsi. Mekanisme bertingkat tersebut merupakan salah satu cara untuk memberikan kesempatan yang sama dan adil bagi peserta didik di seluruh Indonesia untuk berprestasi dan menjadi bibit-bibit talenta potensial.

Pedoman ini disusun untuk memberikan informasi dan gambaran berbagai aspek penyelenggaraan ajang LKS SMK kepada para peserta, pendamping, pembina, juri, dan para pemangku kepentingan lainnya. Selamat mempersiapkan diri, belajar, berlatih, dan bekerja sebaik-baiknya agar kegiatan ajang dapat terlaksana sesuai rencana dan memberikan hasil maksimal.
Kami mengucapkan terima kasih kepada semua pihak yang berpartisipasi dan berperan aktif dalam penyusunan pedoman ini.

Jakarta, 1 Mei 2024

Dr. Maria Veronica Irene Herdjiono, S.E., M.Si
NIP 198103292012122001

DAFTAR ISI

PENDAHULUAN

A. Nama dan Deskripsi Lomba

1. Deskripsi Lomba

Lomba Kopetensi Siswa Nasional (LKSN) Bidang Lomba Cyber Security ke XXX bagi siswa Sekolah Menengah Kejuruan (SMK) Seluruh Indonesia, adalah untuk mengukur kopetensi peserta didik SMK untuk menghadapi *Era globalisasi* yang memberikan dampak signifikan terhadap perkembangan sumber daya manusia. Terbukanya kesempatan kerjasama yang luas antar daerah bahkan antar negara membuat persaingan yang semakin kompetitif.

LKSN Bidang Lomba *Cyber Security* akan dilaksanakan secara *luring.* LKSN Bidang Lomba *Cyber Security* dilakuan dengan proses pemantauaan secara *onsite* dan penilaian akan dilakukan setelah material diterima oleh juri, sedangkan proses Cyber Security dilaksanakan secara langsung dengan tetap memperhatikan prosedur Covid – 19.

Kisi-kisi soal disusun dengan mengacu pada perkembangan kemajuan IPTEK , *Asean Skill Competition (ASC), Word Skill Competition (WSC), dan standard – standard Cyber Security*

2. Isi Deskripsi Teknis

Peserta lomba adalah siswa siswi Sekolah Menengah Kejuruan (SMK) dari seluruh wilayah provinsi yang ada di Indonesia yang telah dipersiapkan melalui berbagai seleksi untuk mewakili masing-masing provinsi. Lomba Kompetensi Siswa Tingkat Nasional sudah berjalan selama 29 tahun, kegiatan ini dimaksudkan untuk mengukur kompetensi siswa SMK sesuai dengan bidang keahliannya masing masing dan menjadi tolok ukur seberapa besar siswa SMK dapat memasuki dunia industri ataupun menjadi wirausaha mandiri.

Tujuan

1. Mendorong SMK untuk meningkatkan kualitas pelaksanaan kegiatan belajar mengajar yang mengacu pada Standar Kompetensi Kerja Nasional Indonesia (SKKNI) khusus untuk Kompetensi Bidang Cyber Security.
2. Mempromosikan kompetensi siswa SMK dibidang Cyber Security kepada dunia usaha atau Industri sebagai calon pengguna tenaga kerja.
3. Memberikan kesempatan dan motivasi kepada siswa untuk berkompetisi secara positif, untuk menumbuhkan kebanggaan pada kompetensi keahlian yang ditekuninya, juga kebanggaan bagi sekolah dan daerah / provinsinya masing masing .

4. Memilih peserta untuk mengikuti ajang kompetisi yang lebih tinggi yaitu ASC, WSA dan WSC dengan meningkatkan kualitas dan kuantitas materi lomba kompetensi siswa tingkat nasional mengacu pada materi ASC, WSA dan WSC.

Kompetisi dilakukan secara tim yang terdiri dari 2 individu, mewakili daerah dari SMK yang terpilih.

3. Dokumen Terkait

Kisi-kisi ini mengacu pada :

- WorldSkills Standards Specification framework
- WSI – WorldSkills Assessment Strategy
- Open Worldwide Application Security Project (OWASP)

Dokumen lain yang juga harus dipelajari adalah:

- Petunjuk Teknis Umum lomba.
- Informasi di akun peserta, pembimbing dan ketua kontingen

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

B. STANDAR KOMPETENSI BIDANG LOMBA

1. Ketentuan Umum

Lomba Kompetensi Siswa dimaksudkan untuk melihat skill kompetensi praktek terbaik seperti pada standard internasional. Oleh karena itu spesifikasi standar merupakan panduan untuk pelatihan yang diperlukan dan persiapan lomba. Dalam lomba kompetensi siswa, penilaian pengetahuan dan pemahaman dilakukan melalui penilaian kinerja

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 :

No	Kompetensi	LKS Daring 2022 %	LKS Luring 2023 %	LKS Luring 2024 %
1.	Work organization and management	3,00	15,00	15,00
2.	Communication and interpersonal skills	3,00	5,00	5,00
3.	Secure systems design and creation	4,00	5,00	5,00
4.	Secure systems operation and maintenance	10,00	17,50	17,50
5.	Secure systems protection and defence	0,00	15,00	15,00
6.	Operations and Management	0,00	12,50	12,50
7.	Intelligence collection and analysis	7,00	15,00	15,00
8.	Investigation and Digital Forensics	3,00	15,00	15,00
Jumlah		100%	100%	100%

C. SISTEM PENILAIAN

1. Petunjuk Umum

Penilaian LKS-SMK menggunakan ketentuan yang telah ditetapkan panitia.

Pada Lomba Kompetensi Siswa tingkat Nasional menggunakan 2 (dua) metode penilaian :

a. ***Measurement* / *Pengukuran***

Measurement merupakan metode yang digunakan untuk menilai akurasi, presisi dan kinerja lain yang diukur secara objektif. Dalam penilaian *Measurement* harus di hindari hal-hal yang bersifat multitafsir.

Pertimbangan pengujian dan penilaian untuk *measurement* adalah sebagai berikut:

- **Iya** atau **tidak.**
- Skala kesesuaian yang telah ditentukan sebelumnya terhadap tolok ukur tertentu.

b. ***Judgment* / Pertimbangan**

Judgement merupakan metode yang digunakan untuk menilai kualitas kinerja yang dimungkinkan adanya perbedaan pandangan berdasarkan tolak ukur penerapan di industri. Skor merupakan penghargaan yang diberikan juri untuk aspek *judgement* pada sub kriteria. Skor harus dalam kisaran 0, 1, 2 atau 3. Nilai yang diberikan dihitung dari skor yang diberikan oleh juri dalam tim penilaian.

Masing-masing dari juri menilai setiap aspek penilaian, apakah peserta sudah mengerjakan atau tidak. Skor dari 0 hingga 3 terkait dengan standar industri sebagai berikut:

- 0: Kinerja dibawah standar industri, termasuk tidak mengerjakan
- 1: Kinerja memenuhi standar industri
- 2: Kinerja melampaui standar industri
- 3: Kinerja luar biasa terkait dengan ekspektasi industri

Baik *measurement* maupun *judgement* harus berdasarkan tolok ukur yang diambil dari praktik terbaik. Semua penilaian harus berdasarkan tolok ukur yang ditetapkan dalam Skema Penilaian. Dalam melakukan penilaian tidak diizinkan menggunakan metode pemeringkatan hasil pekerjaan peserta.

2. Kriteria Toleransi Pengukuran

Penilaian diberikan berdasarkan standar. Masing-masing pekerjaan yang di*breakdown* menjadi sub pekerjaan, dan diberikan bobot penilaian secara proporsional dengan berbagai pertimbangan (tingkat kesulitan, waktu yang dibutuhkan, proses standar yang harus dilalui), sehingga menghasilkan penilaian standar yang obyektif dengan kriteria yang jelas. Semua penilaian pada masing-masing aspek akan diakumulasi dan peserta yang berhasil mengumpulkan nilai tertinggi dalam skala CIS, adalah peserta yang menang.

3. Sub Kriteria

Modul	**Nama Modul**	**Hari**
A	Capture-The-Flag (CTF) Jeopardy	Hari 1
B	Capture-The-Flag (CTF) Attack & Defense	Hari 2

4. Keseluruhan Penilaian

Modul	**Nama Modul**	**Waku** (menit)	**Score**

A	Capture-The-Flag (CTF) Jeopardy	360	50
B	Capture-The-Flag (CTF) Attack & Defense	360	50
Total			100

5. Prosedur Penilaian

Modul	Deskripsi	Hari
A	1. Penilaian proses *security assessment* menggunakan dokumentasi PoC (*proof-of-concept*) yang dibuat peserta. 2. Basis poin didapatkan peserta saat peserta men-submit *flag* kedalam *web scoreboard*	Hari 1
B	1. Penilaian proses *security assessment* menggunakan dokumentasi PoC (*proof-of-concept*) yang dibuat peserta. Pada modul ini, juga dilakukan penilaian kemampuan peserta dalam mempertahankan sistem nya dari serangan/ 2. Basis poin didapatkan peserta saat peserta men-submit *flag* kedalam *web scoreboard*	Hari 2

6. Skema Penilaian

No.	Modul	Kriteria/Sub-Kriteria	Total Nilai

1	A	1. Web Exploitation 2. Binary Exploitation 3. Reverse Engineering 4. Forensic 5. Cryptography	50
2	B	1. Enumeration 2. CVE exploit and mitigation 3. Event and process monitoring 4. Attack detection 5. Authentication protocol (i.e., Active Directory, etc.) 6. Privilege escalation 7. Source code review 8. Code patching	50

D. FORMAT/STRUKTUR PROYEK UJI/*TEST PROJECT*

1. Definisi

Proyek Uji (*Test project*) adalah instruksi/gambar kerja yang menjelaskan pekerjaan di masing-masing bidang keahlian. Proyek uji tersebut akan dilakukan oleh Peserta untuk menunjukkan keunggulan dan keahlian dalam melaksanakan pekerjaan dalam Proyek Uji. Proyek Uji harus meliputi konteks, tujuan, proses, dan hasil kerja, serta skema penilaian yang berlaku.

2. Durasi

Durasi efektif lomba pada tiap proyek uji disesuaikan dengan skema penilaiaan.

3. PROYEK UJI

Modul A

Kompetitor melaksanakan kompetisi Capture-the-flag dengan format Jeopardy dan menyelesaikan tantangan-tantangan yang diberikan dengan batasan waktu yang ditentukan dan dalam kategori sebagai berikut:

1. Web Exploitation
2. Binary Exploitation
3. Reverse Engineering
4. Forensic
5. Cryptography

Modul B

Kompetitor melaksanakan kompetisi Capture-the-flag dengan format Attack & Defense, dimana kompetitor akan menyerang dan bertahan dari serangan kompetitor lain sesuai

dengan batasan waktu yang ditentukan. Perlu diingat bahwa penentuan pemenang tidak hanya melalui perolehan poin di *scoreboard* CTF, tetapi juga melalui keberhasilan kompetitor dalam mengeksploitasi semua/sebanyak mungkin *service* yang tersedia (tidak hanya 1 *service* yang dieksploitasi berulang kali), serta kemampuan masing-masing dalam mempertahankan server dari serangan peserta lain. Perihal ini akan masuk kedalam perhitungan berdasarkan pada skema CIS.

4. PERUBAHAN PROYEK UJI

Penentuan proyek uji akan disampaikan pada saat Teknikal Meeting.

E. ALAT

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 dan Infrastruktur Lomba:

- Server untuk Platform CTF (Web Scoring System)
- Server untuk Hosting CTF Challenges (Jeopardy dan Attack & Defense)

2. Daftar Alat 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	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. **Disarankan dalam satu tim terdapat peserta yang menggunakan OS Windows dan OS Linux.**	Area Kerja Peserta
1 per peserta	Monitor External		Area Kerja Peserta

IT Services

Jumlah	Nama	Keterangan	Penempatan
1 Server CTF Challenges	VPS	4 CPU dual core, RAM 32GB, Storage 1TB, VPS Panel, Unmetered Bandwidth	VPS Provider
1 Server Platform CTF (Web Scoring System)	VPS	4 CPU dual core, RAM 32GB, Storage 1TB, VPS Panel, Unmetered Bandwidth	VPS Provider

Catatan: Selama Alat tidak dicantumkan pada daftar alat akan diperiksa dan tidak boleh dipergunakan sebelum disetujui oleh tim teknis dan persetujuan ketua juri.

E. BAHAN

Tidak ada bahan habis pakai yang diperlukan dalam penyelenggaraan kompetisi LKS bidang lomba Cyber Security.

F. BAHAN PENUNJANG

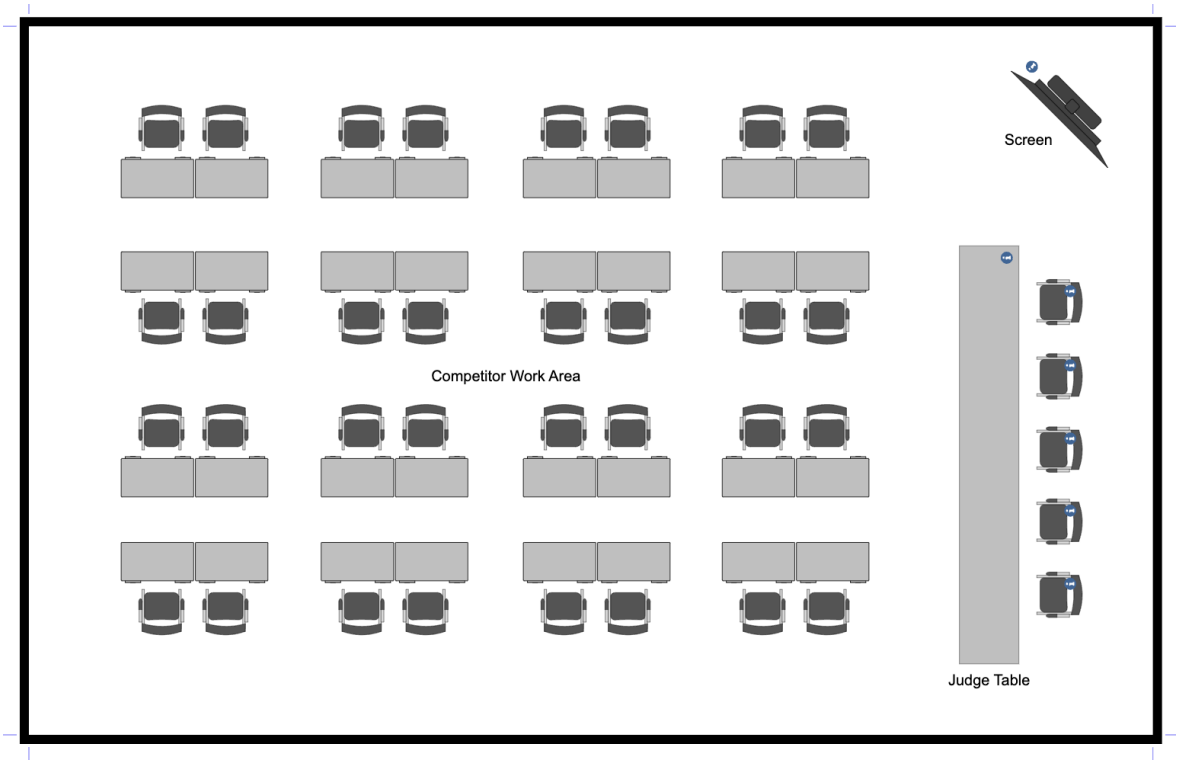
1. Bahan Penunjang Lomba sebagai Referensi para Peserta

Tidak ada bahan penunjang habis pakai yang diperlukan dalam penyelenggaraan kompetisi LKS bidang lomba Cyber Security.

G. LAYOUT DAN BAHAN LAYOUT

1. Layout

Tata layout penempatan peralatan utama berikut deskripsinya



H. JADWAL BIDANG LOMBA

Waktu		Kegiatan	Keterangan
Hari ke-1			
08.00	09.00	Persiapan dan penjelasan *Code-of-conduct* dan aturan kompetisi.	1 Jam
09.00	12.00	Pelaksanaan assessment Modul A: Capture-the-flag Jeopardy	3 Jam

12.00	13.00	Ishoma	1 Jam
13.00	16.00	Pelaksanaan assessment Modul A: Capture-the-flag Jeopardy	3 Jam
16.00	19.00	Pembuatan dokumentasi *Proof-of-concept* (POC)	3 Jam
Hari ke-2			
08.00	09.00	Persiapan dan penjelasan *Code-of-conduct* dan aturan kompetisi.	1 Jam
09.00	12.00	Pelaksanaan assessment Modul B: Capture-the-flag Attack & Defense	3 Jam
12.00	13.00	Ishoma	1 Jam
13.00	16.00	Pelaksanaan assessment Modul B: Capture-the-flag Attack & Defense	4 Jam
16.00	19.00	Pembuatan dokumentasi *Proof-of-concept* (POC)	3 Jam

I. KEBUTUHAN LAIN DAN SPESIFIKASINYA

1. Kebutuhan Juri untuk Menilai

Bidang lomba Cyber Security tidak membutuhkan sarana/prasarana tambahan karena menggunakan system CTF Scoreboard.

2. Kebutuhan Perlombaan

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

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	Laptop juri dan teknisi	5 * 250 watt
5	Laptop peserta	jumlah peserta * 250 watt
TOTAL		**2000++ watt**

J. REKOMENDASI JURI

Recomendasi juri ada pada file terpisah dengan Technical Deskripsi ini.

Lampiran 1: Format Penilaian

Skema penilaian tidak diberikan karena dapat memberikan petunjuk dari cara penyelesaian soal dan tantangan yang diberikan. Namun, kompetitor dapat menggunakan silabus berikut untuk melakukan persiapan kompetisi. Dapat dipastikan bahwa **soal dan tantangan dibuat sesuai dengan kategori/aspek/kelemahan yang tertera** pada silabus ini. Kompetitor dapat fokus mempelajari kategori/aspek/kelemahan yang tertera dibawah ini.

Web Exploitation

- Insecure Direct Object Reference (IDOR)
- Form Injection (e.g. File Upload)
- Session Injection & Broken Access Control
- Business Logic Error
- Mass Assignment
- SQLi
- Blind SQLi
- LFI
- RFI
- SSTI
- XSS
- SSRF
- Object Deserialization
- Prototype Pollution
- RCE

Binary Exploitation

- Buffer overflow
- Integer overflow / underflow
- Shellcode
- Format String
- ROP chain (ret2libc, ret2win, dll)

- Stack Pivoting
- bypass protection (PIE, CANARY, NX, Relro)
- Heap Exploitation (Heap overflow, UAF, Double Free)

Reverse Engineering

- Run Program (ELF/EXE)
- Strings, Pipe (|), Grep
- Static Analysis (Reconstruct Algorithm), z3
- Dynamic Analysis (Tracing, GDB)
- Low Level File Formats (Assembly & Bytecodes Translation)
- Anti RE: Anti Debug (PTRACE), Simple Anti disassembly, Simple Anti Decompiler
- Unoptimized Algorithm
- Compiled Programming Language Syntax Format in Executable (i.e C, C++, Golang, Rust)
- Arsitektur : x86_64, x64, ARM, MIPS
- Obfuscation (Known/Custom Encryption) & Binary Patching
- Mobile Android Reverse Engineering

Forensic

- Steganography
- Exiftool & Strings (Metadata)
- File Carving (binwalk, foremost, photorec)
- Network Forensic (PCAP/PCAPNG)
- Log Forensic (SIEM, Standalone Logs)
- OS Forensic (Browser Forensic, AppData Forensic, Third Party App Forensic, Digital Artifact Discovery <- This include in Windows/Linux/macOS)
- Memory Forensic (Volatility)
- Malware Analysis

Cryptography

- Classical ciphers (contoh: Vigenere, Caesar, Atbash, Affine, Substitution, XOR)
- Attack on RSA (contoh: Hastad, common modulus attack, twin prime, multiprimes)
- Attack on PRNG (contoh: Mersenne Twister, LCG, LFSR)
- Attack on AES (contoh: serangan pada mode-mode ECB, CBC, OFB, CFB, CTR, GCM)
- Attack on ECC (contoh: Smart's attack)
- Attack on DSA (contoh: attack on ECDSA, attack on RSA signature)
- Hashing (contoh: length extension attack)

System Security (terkait Attack & Defense)

- VPN connection
- SSH connection
- CVE exploit and mitigation
- Attack detection
- Linux-based OS administration (user, group, permissions, root access, package installation, etc.)
- Windows-based OS administration (system scheduler, password policy, banner, etc.)
- Event and process monitoring
- Enumeration (port scanning, etc.)
- Data exfiltration
- Privilege escalation
- Firewall policy
- User account policy
- Authentication protocol (contoh: Active Directory)
- Source code review (PHP, Python, Go, Java, C)
- Source code patching

BALAI PENGEMBANGAN TALENTA INDONESIA
PUSAT PRESTASI NASIONAL
KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET, DAN TEKNOLOGI

Jalan Gardu Rt. 10 Rw. 02, Srengseng Sawah, Kec. Jagakarsa, Kota Jakarta Selatan,
Daerah Khusus Ibukota Jakarta 12640