Kemendikdasmen
Pusat Prestasi Nasional

#PENDIDIKAN BERMUTU UNTUK SEMUA
KEMENDIKDASMEN RAMAH

LKS DIKMEN
TINGKAT NASIONAL

Kisi-kisi
Lomba Kompetensi Siswa Nasional 2026

SMA/MA/SMK/MAK/Sederajat

Cabang Ajang

Teknologi Keamanan Siber
(*Cyber Security*)

Soal dan tantangan yang diujikan pada kompetisi LKS bidang lomba Cyber Security bersifat rahasia, namun sesuai dengan kategori/aspek/kelemahan yang tertera pada silabus ini. Kompetitor dapat fokus mempelajari kategori/aspek/kelemahan yang tertera dibawah ini.

Infrastructure Hardening

Linux

- Privileged Access Management (PAM)
- Dangerous/Exposed Services
- Common Linux Misconfigurations
- Network Service Security
- Logging

Windows

- Privileged Access Management (PAM)
- Basic Security Configurations on Active Directory
- GPO Local/AD Policy
- Network Service Security
- AV
- Logging

Offensive / Red Team Based CTF

Jeopardy Style Challenge Skills-Based

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)

Web Exploitation

- Account Takeover
- OAuth Misconfiguration
- Business Logic Errors
- CVE Exploits
- CSRF
- Command Injection
- Dependency Confusion
- Directory Traversal & File Inclusion
- GraphQL Injection
- HTTP Parameter Pollution
- Insecure Deserialization
- Insecure Direct Object References
- Insecure Management Interface
- Insecure Randomness
- JSON Web Token
- Java RMI
- LDAP Injection
- LaTeX Injection
- NoSQL Injection

- Prototype Pollution
- Race Condition
- Request Smuggling
- SAML Injection
- SQL Injection
- Server Side Include Injection
- Server Side Request Forgery
- Server Side Template Injection
- Type Juggling
- Upload Insecure Files
- Web Cache Deception
- Web Sockets
- XPATH Injection
- XSLT Injection
- XSS Injection
- XXE Injection
- Prompt Injection
- OWASP API Security Top 10

Binary Exploitation

- Buffer overflow
- Integer overflow / underflow
- Shellcode
- Format String
- ROP chain (ret2libc, ret2win, dll)
- Type Confusion
- Uninitialized Memory Use
- bypass protection (PIE, CANARY, NX, Relro)
- Heap Exploitation (Heap overflow, UAF, Double Free)

Boot2Root Style Challenge Skills-Based

- Service Level Enumerations
- Service Level Exploitation
- Vertical & Horizontal Privilege Escalation Techniques (Abuse or Living-Off-The-Land)

Defensive / Blue Team Based CTF

Jeopardy Style Challenge Skills-Based

Reverse Engineering

- 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
- Compiled Programming Language Syntax Format in Executable (i.e C, C++, Golang, Rust, etc.)
- Arsitektur : x86_64, x64, ARM, MIPS
- Special Framework : Flutter, Kotlin, Desktop Apps (Qt), et cetera
- Obfuscation (Known/Custom Encryption) & Binary Patching
- Mobile Reverse Engineering

Digital Forensic

- 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)
- Memory Forensic (Volatility)
- Malware Analysis