

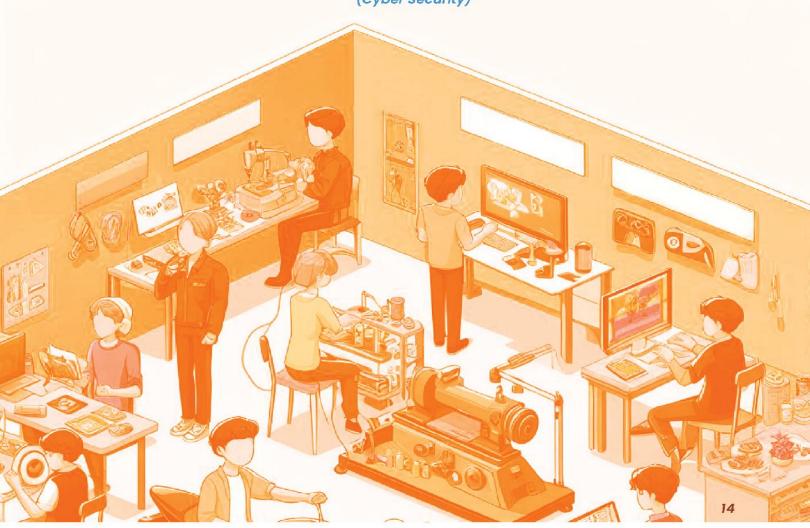


# Kisi-Kisi

Lomba Kompetensi Siswa Nasional 2024

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.

# **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)</li>

- 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 Infrastructure Hardening dan Attack & Defense)

- VPN connection
- SSH connection
- CVE exploit and mitigation
- 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

