KEMNAKER

Indonesia Skills

worldskills ASEAN Philippines2025

TAHUN

2024

KISI - KISI/ PANDUAN TEST PROJECT SELEKDA CALON KOMPETITOR THE 14th WORLDSKILLS ASEAN

CYBER SECURITY

KEMENTERIAN KETENAGAKERJAAN R.I.
DIREKTORAT JENDERAL PEMBINAAN PELATIHAN VOKASI DAN PRODUKTIVITAS
DIREKTORAT BINA STANDARDISASI KOMPETENSI DAN PROGRAM PELATIHAN

Gedung Vokasi, Jl. Jend Gatot Subroto Kav. 44
Jakarta Selatan 12710

https://inaskills.kemnaker.go.id

KISI-KISI SELEKDA 2024
THE 14TH WORLDSKILLS ASEAN
BIDANG LOMBA CYBERSECURITY

GAMBARAN UMUM

1. Kompetisi dilakukan secara *online* sesuai dengan jadwal yang ditentukan.
2. Kompetisi dilakukan dalam bentuk tim dengan anggota berjumlah 2 kompetitor. Kompetitor diberikan waktu selama 17 jam dalam rentang 3 hari untuk menyelesaikan Test Project yang diberikan.

RUANG LINGKUP KOMPETISI

1. Kompetisi dilakukan untuk menguji kemampuan peserta dalam melaksanakan peran-peran di bidang teknologi maupun *cybersecurity* sebagaimana tercantum pada WorldSkills Occupational Standards (WSOS).
2. Kompetitor diharapkan memiliki keterampilan teknis yang relevan yang memungkinkan mereka untuk mengkonfigurasi, mengoperasikan, mengelola, dan melindungi server, jaringan, dan firewall yang diberikan (misalnya, server Windows, server Linux. switch, router, firewall) untuk mendukung keamanan perangkat dan layanan tersebut.
3. Kompetitor diharapkan memiliki keterampilan teknis yang relevan yang memungkinkan mereka mengidentifikasi dan melakukan eksploitasi terhadap berbagai jenis server dan layanan, termasuk *web application, binary services, cryptographic services,* maupun Linux dan Windows server.
4. Kompetitor diharapkan memiliki keterampilan teknis yang relevan yang memungkinkan mereka melakukan berbagai jenis analisis untuk mendeteksi menemukan indikasi serangan lewat *service logs*, *memory dump*, *traffic dump*, maupun sumber-sumber lainnya; serta memiliki pemahaman untuk mencegah serangan terjadi terhadap server dan layanan yang diberikan.
5. Kompetitor diharapkan mampu bekerja dan berkolaborasi dalam tim yang terdiri dari 2 orang, dan dapat bekerja dengan sinergis pada kondisi yang kompleks.

SKENARIO PERLOMBAAN

Test Project yang akan diujikan pada kompetisi adalah sebagai berikut:

1. **Cyber Security Incident Response, Digital Forensic Investigation & Application Security**
    a. Kompetitor diminta untuk melakukan analisis dan investigasi untuk menemukan indikasi insiden keamanan yang terjadi pada sebuah layanan maupun server, termasuk namun tidak terbatas pada: melakukan

rekonstruksi file berbahaya, menyusun timeline terjadinya sebuah insiden, menemukan informasi indikasi serangan serta sumber serangannya, dsb.

b. Kompetitor diminta untuk melakukan *code review* dari berbagai aplikasi dengan teknologi berbeda serta memperbaiki code yang memiliki *security vulnerability*.
c. Kompetitor juga diminta untuk membuat laporan detail (PoC) dari hasil analisis yang telah dilakukan, sebagai proses verifikasi bahwa analisis yang didapatkan adalah tepat, akurat, dan sesuai standar industri.

2. Capture the Flag - Jeopardy

a. Kompetitor akan menyelesaikan soal-soal berbasis Capture-the-flag Jeopardy dengan kategori-kategori sebagai berikut:
   i. Web Exploitation
   ii. Binary Exploitation
   iii. Reverse Engineering
   iv. Cryptography
b. Kompetitor diminta untuk melakukan eksploitasi maupun analisis dari layanan, aplikasi, maupun file yang diberikan dengan tujuan untuk menemukan sebuah *string* yang disebut flag.
c. Soal-soal akan dirilis dalam bentuk *wave* berdasarkan kategori. Jika *wave* untuk suatu kategori sudah berakhir, maka soal-soal kategori tersebut tidak dapat dikerjakan lagi, dan soal-soal kategori selanjutnya akan diberikan.
d. Kompetitor juga diminta untuk membuat laporan detail (PoC) dari langkah-langkah eksploitasi yang telah dilakukan, sebagai proses verifikasi bahwa proses eksploitasi telah benar-benar berhasil dilakukan.

JADWAL PERLOMBAAN

HARI 1

NO	WAKTU	KETERANGAN	TOTAL WAKTU
1.	08.00 – 09.00	Pembukaan	1 jam
2.	09.00 – 12.00	**TP1: Cyber Security Incident Response, Digital Forensic Investigation & Application Security**	3 jam
3.	12.00 – 13.00	Istirahat /Makan Siang	1 jam
4.	13.00 – 15.00	**TP1: Cyber Security Incident Response, Digital Forensic Investigation & Application Security**	2 jam
5.	15.00 - 17.00	Penulisan laporan Proof-of-concept (POC)	2 jam

HARI 2

NO	WAKTU	KETERANGAN	TOTAL WAKTU

1.	08.00 – 09.00	Pembukaan	1 jam
2.	09.00 – 11.00	**TP2: CTF - Jeopardy Wave Web**	3 jam
3.	12.00 – 13.00	Istirahat /Makan Siang	1 jam
4.	13.00 – 15.00	**TP2: CTF - Jeopardy Wave Binary Exploitation**	3 jam
5.	15.00 - 18.00	Penulisan laporan Proof-of-concept (POC)	3 jam

HARI 3

NO	WAKTU	KETERANGAN	TOTAL WAKTU
5.	08.00 – 09.00	Pembukaan	1 jam
6.	09.00 – 12.00	**TP2: CTF - Jeopardy Wave Reverse Engineering**	3 jam
7.	12.00 – 13.00	Istirahat /Makan Siang	1 jam
8.	13.00 – 16.00	**TP2: CTF - Jeopardy Wave Cryptography**	3 jam
5.	16.00 - 19.00	Penulisan laporan Proof-of-concept (POC)	3 jam

HARI 4

NO	WAKTU	KETERANGAN	TOTAL WAKTU
1.	08.00 – 12.00	Penilaian	3 jam
2.	12.00 – 14.00	Istirahat & Makan Siang	2 jam
3.	14.00 – 16.00	Pengumunan Pemenang dan Penutupan	2 Jam

Total jam kompetisi ± 17 jam

KRITERIA PENILAIAN

Aspek yang dilakukan penilaian adalah sebagai berikut:

Test Project (TP)	Nama	Deskripsi	Poin
TP1	Cyber Security Incident Response, Digital Forensic Investigation &	Log, Memory, Malware, Network Traffic, Application Source Code	40

	Application Security		
TP2	Capture-The-Flag (CTF) Jeopardy	Web Application	15
		Binary Exploitation	15
		Reverse Engineering	15
		Cryptography	15
Total			100

ALAT, BAHAN, DAN LINGKUNGAN KOMPETISI

1. Kompetitor mengerjakan Test Project menggunakan device (Laptop / Komputer) milik masing-masing.
2. Agar dapat mengerjakan soal dan tantangan yang diberikan dengan baik, kompetitor dalam satu tim diharapkan memiliki device dengan OS berbasis Linux dan Windows.
3. Kompetitor dapat menggunakan *dual-boot* OS maupun VMWare / VirtualBox untuk menjalankan OS yang dibutuhkan.

KISI - KISI

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

1. **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

2. 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)

3. 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

4. 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

5. 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)

6. System Security and Risk Mitigation

- 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