Kisi Kisi Soal LKS Cybersecurity Kota Bekasi 2024

I. Materi Lomba

Terdapat 2 kategori materi lomba yaitu tes teori dan praktik.

a. Tes Teori

Meliputi tes pengetahuan secara terpadu tentang:

1. Menjelaskan Prinsip Security Triad (Confidentiality, Integrity dan Availability)
2. Memahami Prinsip Security Least Access.
3. Memahami dan dapat membedakan antara Vulnerability, Threat dan Attack.
4. Memahami dan mampu membedakan Prinsip dan cara kerja antara “Ethical Hacker” dan “Cracker”.
5. Memahami dan mampu membedakan Encryption dan Hashing.

Catatan: Tes teori berbentuk essay, dikerjakan maksimal 20 menit, sebelum dimulai tes praktik (diluar dari waktu lomba).

b. Tes Praktik Defensive

Meliputi tes keterampilan terpadu tentang:

1. Konfigurasi Hardening Windows 7
2. Konfigurasi Hardening Linux Debian 9

c. Tes Praktik Offensive

Meliputi tes keterampilan terpadu tentang:

1. Capture The Flags (CTF)
2. Dokumentasi CTF (Write-up)

Catatan: Pembuatan Write-up CTF diluar dari waktu lomba, maksimal waktu pengumpulan 40 menit, setelah mata lomba CTF selesai.

II. NILAI, BOBOT PENIALAIAN, DAN WAKTU LOMBA

I.1. NILAI MAKSIMUM DAN BOBOT PENILAIAN

Nilai Maksimum dan Bobot Penilaian

1. Tes Teori (nilai maksimum 100, bobot 10%).....N_1
2. Tes Praktik Defensive (nilai maksimum 100, bobot 40%).....N_2
3. Tes Praktik Offensive (nilai maksimum 100, bobot 50%).....N_3

Nilai Akhir (NA) = Σ (Nilai tes N_1 + N_2 + N_3)

I.2. WAKTU LOMBA

Diberikan waktu lomba selama 4 Jam (Tes Praktik), tidak termasuk tes teori dan penulisan write-up.

III. Aspek Penilaian

Aspek yang dinilai untuk tes teori adalah:

No.	Aspek Yang Dinilai	Kriteria	Nilai
1.	Menjelaskan Prinsip Security Triad (Confidentiality, Integrity dan Availability)	● Mampu Menjelaskan dan menguraikan secara Konsep dan contoh implementasi pada Aspek Confidentiality	5
		● Mampu Menjelaskan dan menguraikan secara Konsep dan contoh implementasi pada Aspek Integrity	10
		● Mampu Menjelaskan dan menguraikan secara Konsep dan contoh implementasi pada Aspek Availability	5
2.	Memahami Prinsip Security Least Access	● Mampu Menjelaskan dan menguraikan secara Konsep dan contoh Kasus Prinsip Least Access	10
		● Mampu Menjelaskan dan menguraikan secara Konsep keterkaitan antara Security, Functionality dan Easy of Access	10
3.	Memahami dan dapat membedakan antara Vulnerability, Threat dan Attack.	● Mampu Menjelaskan dan menguraikan secara Konsep dan Contoh implementasi pada Aspek Vulnerability	10
		● Mampu Menjelaskan dan menguraikan secara Konsep dan contoh implementasi pada Aspek Threat	10
		● Mampu Menjelaskan dan	10

		menguraikan secara Konsep dan contoh implementasi pada Aspek Attack	
4.	Memahami dan mampu membedakan Prinsip dan cara kerja antara “Ethical Hacker” dan “Cracker”.	● Mampu Menjelaskan dan menguraikan cara kerja dari Cracker, Hacker, Ethical hacker, Black hat, Grayhat, Script Kiddy.	10
5.	Memahami dan mampu membedakan Encryption dan Hashing.	● Mampu Menjelaskan dan menguraikan secara Konsep teknik Encryption	10
		● Mampu Menjelaskan dan menguraikan secara Konsep teknik Hashing	10
Jumlah Nilai			

Aspek yang dinilai untuk tes praktik defensive adalah:

No.	**Aspek Yang Dinilai**	**Kriteria**	**Nilai**
1.	Windows Hardening	● Konfigurasi dan Pengujian Hardening Account lockdown (Windows machines)	15
		● Konfigurasi dan Pengujian Hardening Password minimum length (Windows machines)	15
		● Konfigurasi dan Pengujian Hardening Password complexity (Windows machines)	15
		● Konfigurasi dan Pengujian Hardening Remote Access (Windows machines)	20
2.	Linux Hardening	● Konfigurasi dan Pengujian Hardening Document Host Information	15

		● Konfigurasi dan Pengujian Hardening Hardisk Encription	40
		● Konfigurasi dan Pengujian Hardening Closed Unusual Open Port	15
		● Konfigurasi dan Pengujian Hardening Certificate Shell Login	25
		● Konfigurasi dan Pengujian Hardening Directory Listing (Apache Web Server)	15
		● Patching Content-Security-Policy (CSP) pada Apache	15
		● Patching X-Frame-Options pada Apache	15
		● Patching X-Content-Type-Options pada Apache	15
		● Patching Referrer-Policy pada Apache	15
		● Patchin Permissions-Policy pada Apache	15
Jumlah Nilai			

Aspek yang dinilai untuk tes praktik offensive adalah:

No.	**Aspek Yang Dinilai**	**Kriteria**	**Nilai**
1.	Capture The Flags	● Web Exploitation	30
		● Digital Forensics	20
		● Reverse Engineering	10
		● Cryptography	20
		● Steganography	20

2.	Write-Up CTF	● Mendokumentasikan Langkah-Langkah Penemuan Flag pada Soal CTF.	**WAJIB**
Jumlah Nilai			

Catatan: Peserta wajib mengumpulkan Write-up, sebagai bukti bahwa nilai yang ada pada scoreboard benar. Nilai mata lomba CTF akan dikurangi jika tidak mengumpulkan write-up.

IV. ALAT DAN BAHAN

I.1. ALAT DAN BAHAN YANG DISIAPKAN/DIBAWA PESERTA

No.			**Peruntukan**
1.	VM Windows	2 VCore VPU Minimal 4 GB RAM	Semua konfigurasi Client dan hardening Windows.
2.	VM Linux	2 VCore VPU Minimum 4 GB RAM	Semua konfigurasi Client dan hardening Linux.
3.	VM Kali-Linux	2 VCore VPU Minimum 4 GB RAM	Capture The Flags.