LOMBA KOMPETENSI SISWA (LKS)
SEKOLAH MENENGAH KEJURUAN
TINGKAT PROVINSI JAWA BARAT
TAHUN 2024

INFORMASI DAN KISI-KISI

Bidang Lomba

TEKNOLOGI KEAMANAN SIBER
(CYBER SECURITY)

PEMERINTAH DAERAH PROVINSI JAWA BARAT
DINAS PENDIDIKAN
Jalan Dr. Radjiman No. 6 Telp. (022) 4264813 Fax. (022) 4264881
Website : disdik.jabarprov.go.id
e-mail: disdik@jabarprov.go.id/sekretariatdisdikjabar@gmail.com
BANDUNG - 40171

LOMBA KOMPETENSI SISWA (LKS)
SEKOLAH MENENGAH KEJURUAN
TINGKAT PROVINSI JAWA BARAT
TAHUN 2024

NASKAH SOAL
*(~~Terbuka~~ / Tertutup)

Bidang Lomba
TEKNOLOGI KEAMANAN SIBER
(CYBER SECURITY)

PEMERINTAH DAERAH PROVINSI JAWA BARAT

DINAS PENDIDIKAN

Jalan Dr. Radjiman No. 6 Telp. (022) 4264813 Fax. (022) 4264881
Website : disdik.jabarprov.go.id
e-mail: disdik@jabarprov.go.id/sekretariatdisdikjabar@gmail.com
BANDUNG - 40171

INFORMASI DAN KISI-KISI SOAL LOMBA CYBER SECURITY

1. Peserta Lomba

Peserta Lomba adalah perwakilan dari masing-masing SMK Provinsi Jawa Barat yang sudah mendaftar dan telah terverifikasi Panitia.

Alat dan bahan di SMKN 1 Cimahi sebagai tempat penyelenggara LKS mata lomba Cyber Security yaitu 2 buah server dengan spesifikasi berikut ini :

Dell PowerEdge T40 / Intel Xeon E-2224G 3.5GHz, 8M cache, 4C/4T, turbo (71W) / 4x16GB Ram / 1TB 7.2K Entry SATA 3.5 /SSD 512gb /Dvdrw /Keyboard and Mouse / Single Power Supply 300W / NO OS / 3 Yrs Next Business Day Onsite Service panitia penyelenggara: Dell PowerEdge T40 / Intel Xeon E-2224G 3.5GHz, 8M cache, 4C/4T, turbo (71W) / 4x16GB Ram / 1TB 7.2K Entry SATA 3.5 /SSD 512gb /Dvdrw /Keyboard and Mouse / Single Power Supply 300W / NO OS / 3 Yrs Next Business Day Onsite Service.

Perangkat yang wajib dibawa oleh setiap peserta lomba untuk pelaksanaan LKS Mata Lomba Cyber Security adalah **Laptop** dengan minimal **RAM 8 GB**

2. Tata Tertib Lomba

✓ **Pembimbing diharapkan**:

a. Memberikan kisi-kisi materi yang akan diujikan sebelum hari H pelaksanaan lomba
b. Menjelaskan secara detail kisi-kisi dan soal
c.Jujur dan adil baik dalam memberikan arahan, penjelasan, maupun penilaian kepada peserta lomba.

✓ **Peserta diharapkan :**

a. Memahami dasar-dasar kompetensi keamanan siber secara mendalam
b. Mempersiapkan diri pada soal teori dan pratikum sebelum mengikuti acara lomba

c. Menyelesaikan seluruh soal dengan sebaik-baiknya dan dengan motivasi yang tinggi
d. Jujur dan sportif
e. Mematuhi tata tertib yang telah ditentukan oleh panitia atau juri, apabila melanggar maka akan dikenakan sanksi.

3. Jenis Soal

- **Soal Praktek**: *Hardening, VPN, Email security* dan *CTF (Capture The Flag)* -- (1,5 hari)
- **Wawancara** -- (1/2 hari)

4. Skema Penilaian

- Disampaikan **menjelang Hari Pelaksanaan** atau pada saat ***technical meeting***

5. Dokumentasi Peserta

- Semua Poin Penilaian akan dihitung apabila setiap peserta mampu menuangkannya dalam Dokumen yang dapat mewakili *Proof of Concept* terjadinya *Threat*, *Vulnerability*, *Attack*

6. Hal hal yang dilarang

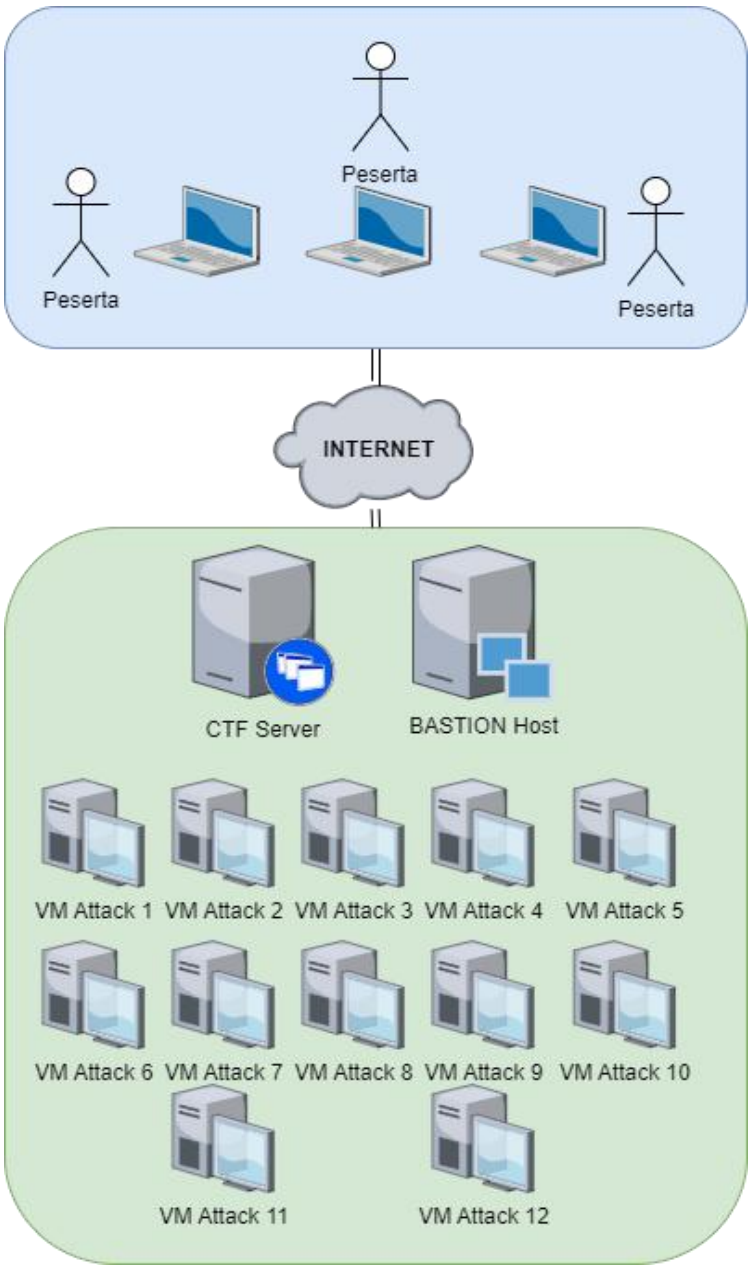
- Bekerjasama dengan Peserta lain.
- Dilarang meninggalkan hasil perubahan atau penambahan file atau penyisipan *Backdoor* setelah Penetrasi selesai
- Menggunakan *tools* Pemindaian otomatis

7. Gambaran Umum Soal Uji Praktek

Peserta menggunakan perangkat komputer yang dibawa sendiri dalam menjalankan lomba Cyber Security Tingkat Provinsi Jawa Barat. Nantinya peserta akan diminta untuk bekerja di *virtual machine* menggunakan *image* yang baru diinstal. Peserta kemudian akan terhubung ke jaringan Private CTF *server*.

Jenis soal terbagi menjadi 3 bagian yaitu CTF, *Hardening* dan *Interview*. Dokumentasi Sistem Menjadi Penilaian tersendiri dan memiliki bobot skor, dokumentasi harus dapat mendokumentasikan *Proof of Concept*, Metodologi dan *Table Vulnerability*, *Attack*, *Mitigation*.

Setiap jawaban benar dari soal CTF maupun *hardening* akan diberi nilai apabila sudah tertulis dalam bentuk dokumentasi



Gambar 1. Gambaran Umum Soal Uji Praktek

.

8. ***Hardening*** **Linux**
   - Dijalankan di VM Masing Masing Komputer / Laptop Peserta. Dimulai dari tahapan Instalasi Sistem Operasi Linux Centos 7 (VMware / VirtualBox masing-masing)
   - Pada Kondisi Awal Peserta Harus dapat Membuktikan secara terbalik (Reverse) tentang Vulnerabilitynya
   - Konfigurasi dan Pengujian Hardening Document Host Information (Linux machines)
   - Konfigurasi dan Pengujian Hardening Hardisk Encription (Linux machines)
   - Konfigurasi dan Pengujian Hardening Closed Unusual Open Port (Linux machines)
   - Konfigurasi dan Pengujian Hardening Whitelisting Selinux (Linux machines)
   - Konfigurasi dan Pengujian Hardening CHROOT Shell (Linux machines)
   - Konfigurasi dan Pengujian Hardening Certificate Shell Login (Linux machines)
   - Konfigurasi dan Pengujian Hardening Directory Listing (Linux machines)
   - Konfigurasi dan Pengujian Hardening Remote Command Exec (Linux machines)

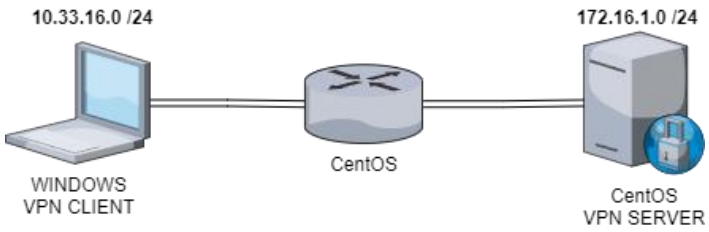
9. **Pengiriman Email PGP**

   Menggunakan VM Windows / OS / Laptop / Komputer masing-masing Peserta (VMware / Virtualbox Masing masing)

   - Digital Signature

- Encryption + Signing
- Decrypt
- Verification

10. Konfigurasi OpenVPN



- Instalasi dan Konfigurasi OpenVPN pada VM Linux dengan Protokol Standar
- Membuat Sertifikat File Client
- Konektifitas VPN Client dapat Berjalan di Background
- Uji Konektifitas OpenVPN
- VM Linux Centos 7 (VMware / Virtualbox Masing masing)

11. IDS (SNORT / Suricata)

- Diletakan di mesin Linux Centos 7 Peserta. (VMware / Virtualbox Masing masing)
- Instalasi dan Konfigurasi Instruction Detection System (IDS) pada web server
- Penambahan / Aktifasi Rule SQL Injection / Blind SQL Injection, Brute Force Attack dan Cross Site Scripting
- Ujicoba Terbalik Attack dan Defence

12. ModEvasive

- Peserta harus bisa buktikan log percobaan DOS yang dibuat sendiri
- Instalasi Konfigurasi Module ModEvasive
- Customisasi Parameter ModEvasive
- Instalasi Konfigurasi Module ModSecurity
- Customisasi Parameter / Rule ModEvasive
- Diletakan di mesin Linux Centos 7 Peserta. (VMware / Virtualbox Masing masing)

13. **Analisis dan Patching Security Header Web**

- Menyiapkan Sebuah file php berisi phpinfo(); pada sebuah web server di virtualbox / vmware masing masing peserta.
- Menemukan dan Menggunakan Tools untuk melakukan Pengecekan Security Header Web Server
- Peserta membuat sendiri aplikasi Web yang berisi info.php yang vulnerable disisi Header. Peserta harus mampu Mengaktifkan semua Mitigasi Security Header tanpa mengganggu Fungsionalitas Aplikasi
- Patching Strict-Transport-Security pada Apache
- Patching X-Frame-Options pada Apache
- Patching X-Content-Type-Options pada Apache
- Patching Referrer-Policy pada Apache
- Patching Permissions-Policy pada Apache
- Patching Content-Security-Policy (CSP) pada Apache
- Peserta akan mendeploy aplikasi yang disediakan panitia untuk di hardening di sisi WebHeader.

14. Capture the Flag

No.	Deskripsi Kerentanan	Jumlah Flag
1	Kerentanan ini terjadi tidak adanya validasi terhadap paramater ke query database yang dapat menyebabkan penyerang untuk melihat atau mengunduh database di server target dan penyerang dapat melakukkan mengambilan alih server target.	2
2	Kerentanan ini terjadi dikarenakan path dari .git dapat dilihat oleh publik dan dapat di unduh oleh orang yang tidak berwenang	1
3	Kerentanan ini terjadi dikarenakan n dalam perubahan yang dilakukan pada normalisasi jalur di Apache HTTP Server 2.x.x.x (versi Http diinformasikan pada saat hari H). Penyerang dapat menggunakan serangan path traversal untuk memetakan URL ke file di luar root dokumen yang diharapkan. Jika file di luar direktori ini tidak dilindungi oleh konfigurasi default biasa "require all denied", permintaan ini dapat berhasil. Jika skrip CGI juga diaktifkan untuk jalur alias ini, ini dapat memungkinkan Dilakukannya serangan	1
4	Kerentanan ini terjadi dikarenakan penyerang dapat mengirim pesan *MSG_USERAUTH_SUCCESS* sebelum otentikasi berhasil. Itu dapat melewati otentikasi dan mengakses server SSH target	1
5	celah kerentanan di mana terdapat suatu endpoint Rest API yang menerima request data tidak terdapat validasi dengan baik, sehingga kita dapat memodifikasi request dengan menambahkan parameter lain yang terdapat pada resource database tersebut	1
6	Kerentanan ini memungkinkan penyerang/attacker untuk menyertakan file lokal yang tersimpan di server agar dapat menjadi bagian dari proses eksekusi aplikasi. Bahkan bisa melakukan Remote Code Execution.	1
7	Menebak username dan password yang digunakan, pada target beriktu adalah pada service SSH, dan melakukan	2

	Local Privilege Escalation dari user biasa ke root	
8	Fungsi "COPY TO/FROM PROGRAM" memungkinkan pengguna super dan pengguna dalam grup 'pg_execute_server_program' untuk mengeksekusi kode arbitrer dalam konteks pengguna sistem operasi database. Fungsionalitas ini diaktifkan secara default dan dapat disalahgunakan untuk menjalankan perintah sistem operasi yang sewenang-wenang di Windows, Linux, dan macOS.	1

15. **Waktu Pelaksanaan Lomba**
    - *Technical Meeting* akan dilaksanakan pada **paling lambat seminggu sebelum pelaksanaan lomba** secara daring.
    - Lomba akan dilaksanakan pada **14 s.d 16 Mei 2024** (Jika ada perubahan jadwal akan disampaikan di grup WhatsApp)
    - Link *Zoom* akan disampaikan pada grup WhatsApp.

16. Penutup.
- Hal-hal yang belum tercantum dalam lembar informasi ini akan di informasikan pada waktu rapat teknis atau *(technical meeting*).