

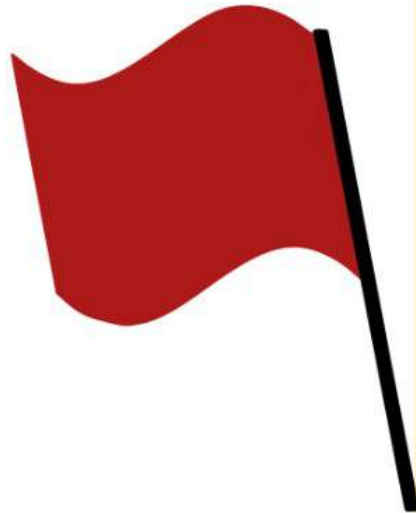
BRIEFING LKS SMK TINGKAT NASIONAL
CYBERSECURITY

9 OKTOBER 2023

Stanley Halim
Chrisando Ryan
Felix Alexander
Prajna Prasetya
Muhammad Faishol



JADWAL LOMBA



25 OKTOBER 2023



JEOPARDY CAPTURE THE FLAG

Waktu pengerjaan: **7 jam**

26 OKTOBER 2023



ATTACK-DEFENSE

Waktu pengerjaan: **7 jam**

JEOPARDY CAPTURE THE FLAG

Briefing LKSN
Cybersecurity
2023



CAPTURE THE FLAG

- Peserta diminta untuk mencari data khusus (flag) dengan cara mengeksploitasi celah sistem, menganalisis data atau menyelesaikan permasalahan
- Format Flag = **LKS{flag}**
- Kategori Soal
 - Web Exploitation (Client-side & Server-side)
 - Reverse engineering (App/Binary, ELF/EXE, Mobile APK)
 - Binary Exploitation/Pwn (Stack/Heap)
 - Digital Forensic & Incident Response / DFIR (log, memory, network analysis)
 - Cryptography (Encryption, Signature, Encoding)

PRE-LKSN NOTES

- Peserta diharapkan sudah memahami cara melakukan Image VM Imports seperti OVA/OVF pada *instance* VM yang digunakan (VMWare/VirtualBox)
 - **Terdapat 2 soal** yang akan memerlukan peserta untuk mengunduh file nya terlebih dahulu 2 hari sebelum lomba dimulai (Tanggal 23 Oktober akan diinfokan laman/*link* untuk mengunduh file tersebut via WhatsApp Group LKS Cyber Security) dengan estimasi disk size +/- **10GB**, sehingga mohon dipastikan agar peserta memiliki alokasi *storage* lebih dari ukuran tersebut.
 - **Harap semua pembimbing dan peserta** juga sudah **bergabung ke dalam grup LKS Cyber Security 2023** agar informasi yang akan diedarkan menyebar secara merata sehingga tidak ada lagi alasan bahwa file yang dibutuhkan belum sempat diunduh demi efisiensi perlombaan berlangsung
 - Wajib join Discord Server LKSN Cyber Security 2023 (QR dapat dilihat setelah slides ini)
-

DISCORD SERVER




<https://discord.gg/wpmSDq9sk>





PENILAIAN CTF



- 
- Jumlah soal 16 nomor dengan skor bervariasi untuk setiap nomornya
 - Scoring dinamis
 - Peserta diminta untuk meraih poin sebanyak-banyaknya
 - Tidak ada ketentuan mengenai urutan pengerjaan soal maupun jumlah minimal soal yang harus dikerjakan

SCORING DINAMIS

- Skor akan turun untuk soal yang mudah -> banyak yang menyelesaikan
- Parameter nilai
 - Maximum : 1000
 - Minimum : 500
 - Decay Function : **Logarithmic**

$$\left(\left(\frac{(\text{minimum} - \text{initial})}{(\text{Decay}^2)} \right) \cdot (\text{Solvecount}^2) \right)$$

- Referensi : <https://github.com/CTFd/DynamicValueChallenge>

PROSEDUR PELAKSANAAN

- Pengerjaan Jeopardy CTF dimulai dari jam **09.00 - 17.00 (7 jam)** [ISOMA 1 jam pada **12.00 - 13.00**]
- Peserta login ke portal CTF
- Peserta dapat memilih soal CTF yang akan dikerjakan
- Peserta mengirimkan **flag** yang ditemukan lewat portal CTF
- Penilaian dilakukan secara otomatis oleh sistem berdasarkan jawaban flag yang dikirimkan peserta
- Pada tahap akhir peserta diminta menuliskan laporan (write-up) dan dikirimkan via *Form/Email* (diinformasikan pada hari lomba)
- Write-Up: 3-4 jam (17.00 - 19.00/20.00), **akan lebih baik jika sambil mengerjakan juga dicicil dan di-screenshot POC/gambar pendukung bukti**



ATTACK - DEFENSE

Briefing LKSN
Cybersecurity
2023

ATTACK-DEFENSE

- Peserta diminta untuk mempertahankan server yang dikelola dari serangan tim lain sekaligus diberikan kesempatan untuk menyerang server tim lain.
 - Kategori serangan yang mungkin bisa dilakukan:
 - Reconnaissance
 - Reverse engineering
 - Web server-based attack
 - Web client-based attack
 - Database based attack
 - Privilege escalation
 - Cryptography
 - Malicious software (malware)
 - Exploitation
 - CVE-Based Vulnerability (public exploit)
-

MEKANISME

- Peserta mendapatkan daftar tim beserta alamat IP VM server masing-masing peserta ketika kompetisi akan dimulai.
 - Peserta mencoba mendapatkan akses shell (user/root) dari VM server tim lain dengan cara mengeksploitasi setiap celah keamanan yang ada.
 - Di saat yang sama, peserta melakukan pengamanan pada VM server masing-masing agar tidak dapat dieksploitasi.
 - Setelah mendapatkan akses shell, peserta menjalankan perintah curl ke server flag dari shell VM server korban. Spesifikasi URL adalah sebagai berikut :
 - **curl http://ip-server-flag**
 - Parameter ip-server-flag diberitahukan saat kompetisi.
 - Peserta harus menggunakan user root saat mengeksekusi perintah curl untuk mendapatkan flag root.
 - Output dari curl adalah flag unik dari tiap peserta.
 - Setelah mendapatkan flag dari target, peserta dapat mengirimkan ke platform AnD.
-

PENILAIAN

- Penilaian dilakukan berdasarkan kemampuan mempertahankan server sendiri sekaligus menyerang server lain
- **Tips.** Identifikasi kelemahan pada server sendiri secepat mungkin, sehingga:
 - **kelemahan** pada server **dapat diperbaiki** dan tidak bisa dimanfaatkan peserta lain
 - **skenario** untuk **menyerang server peserta lain** dapat disusun dengan cepat dan dapat dimanfaatkan untuk mendapat poin >:)

PENILAIAN: ATTACK

- Tiap **attack** dianggap sukses apabila berhasil meng-*submit* **flag**:
 - **User Flag**: 50 Poin
 - **Root Flag**: 100 Poin
 - Setiap 5 menit (**1 tick**), semua **flag** pada seluruh tim akan **diganti** dengan **flag yang baru**.
 - Setiap **tick**, peserta dapat **melakukan penyerangan ulang** untuk mendapatkan **flag terbaru** dan **mendapatkan poin**
-

PENILAIAN: DEFENSE

- Poin defense dihitung seperti berikut (per **tick**):
 - $(number_up * 90) - (number_down * 50)$
 - Apabila service up setidaknya satu menit dan **flag** peserta tidak tercuri oleh tim lain, maka akan mendapatkan tambahan 100 poin
 - **number_up**: jumlah menit *server* peserta berjalan dengan baik
 - **number_down**: jumlah menit *server* peserta *faulty*/tidak berjalan dengan semestinya
-

PENILAIAN: CONTOH

Tim 1

- 12 user flag berhasil didapatkan
- 7 root flag berhasil didapatkan
- server up 4 menit dan down 1 menit
- flag tidak tercuri

Poin attack: $(12 * 50) + (7 * 100) = 1300$

Poin defense: $(4 * 90) - (1 * 50) + 100 = 410$

Total poin pada tick tersebut = 1710

PENILAIAN: CONTOH

Tim 2

- 10 user flag berhasil didapatkan
- 10 root flag berhasil didapatkan
- server down 5 menit
- flag tidak tercuri

Poin attack: $(10 * 50) + (10 * 100) = 1500$

Poin defense: $(0 * 90) - (5 * 50) + 0 = -250$

Total poin pada tick tersebut = 1250

KETENTUAN LAIN

- Beberapa hal yang **tidak diperbolehkan** selama sesi
 - Mematikan server yang dikelola
 - Membuat service-service yang berjalan pada server yang dikelola tidak dapat diakses.
 - Melakukan upgrade/instalasi ulang OS server yang dikelola
 - Menghapus authorized_keys user **ubuntu** dan merubah port SSH
 - Menghapus file/melakukan format disk pada server korban
 - Beberapa hal yang **diperbolehkan** selama sesi
 - Melakukan patching/update/perubahan konfigurasi terhadap service/aplikasi yang berjalan pada server yang dikelola
 - Melakukan instalasi paket tambahan pengamanan server yang dikelola
 - Melakukan scanning terhadap calon korban
 - Melakukan eksploitasi terhadap celah keamanan server korban
-

ROLLBACK / RESET

- Peserta dapat mengembalikan server ke *state awal* dengan mengajukan *rollback* pada dashboard CTFd
 - **Saat rollback, server akan terhitung down pada perhitungan poin defense**
-

TERIMA KASIH