

# RULEBOOK LOMBA ICS2C

Lomba CTF ( capture the flag ) adalah lomba dalam bidang keamanan informasi dimana peserta akan mencari flag yang disembunyikan dalam soal lomba.nantinya flag ini akan disubmit ke scoring system.Jika flag yg dimasukan benar,maka peserta akan mendapatkan nilai.besar nilai yang didapat bergantung dari tingkat kesulitan soal.semakij sulit soal semakin besar pula nilainya.

Salah satu jenis style CTF yang sering dilombakan adalah jeopardy.pada lomba jenis ini,soal disediakan dalam berbagai macam kategori dengan nilai dan tingkat kesulitan yang berbeda beda.semakin sulit soal semakin besar nilainya.

Berikut adalah contoh kategori dalam ajang CTF :

## 1. Network analysis

Pada kategori ini,peserta akan diberikan berbagaimacam soal yg ada kaitannya dengan keamanan jaringan misalnya diberikan file pcap untuk dianalisa .nantinya akan ada flag pada file yg dianalisa tersebut.tujuanx untuk melatih kemampuan peserta dalam melakukan analisa terhadap kemanan jaringan

## 2. Reverse engineering

Kategori ini peserta diberikan file binary maupun source code baik yang berjalan pada os linux,unix maupun windows untuk dianalisis.masing masing file memiliki flag tersendiri.tujuannya adalah untuk melatih peserta dalam melakukan analisa terhadap binary untuk mengetahui alur cara kerja binary tersebut

## 3. Binary exploitation (pwn)

Peserta diberikan alamat dari aplikasi yang berjalan pada jaringan dan binary dari aplikasi tersebut.selanjutnya peserta akan melakulan analisa dan eksploitasi terhadap aplikasi tersebut untuk mendapatkan flag.tujuannya adalah untuk melatih peserta dalam menemukan celah keamanan pada aplikasi jaringan.

#### 4. Crypto

Peserta diberikan berbagai macam file yg telah dienkripsi dan mencari cara untuk mengembalikan file aslinya.jenis ini baik berupa file offline maupun online yang berjalan pada aplikasi.tujuannya untuk melatih kemampuan cryptography dari peserta

#### 5. Web application

Peserta diberikan berbagaimacam web application untuk dieksploitasi dengan teknik tertentu.misalnya web dengan kelemahan sql injection,file inclusion,remote code execution.

#### 6. Forensic /misc

Peserta diberikan soal misalnya berupa image memory atau log file dan harus mencari indikantor adanya aksi hacking pada kedua file tersebut

Konsep dari Capture The Flag (CTF) yang diselenggarakan, berupa Jeopardy CTF pada 1 babak penyisihan, serta hybrid Jeopardy dan Attack-Defense pada babak final, yang menguji kemampuan dan pengetahuan peserta dalam berbagai kategori, seperti: web hacking, cryptography, digital forensic, reverse engineering, dan binary exploitation. Salah satu rangkaian dari kompetisi CTF adalah Warming up , yang akan diadakan secara online sebelum perlombaan dimulai untuk melatih peserta mengenai bidang-bidang yang akan dilombakan.

### **Penghargaan**

1. Juara
2. 1<sup>st</sup> runner-up
3. 2<sup>nd</sup> runner-up
4. Honorable Mention (2 Tim)

## Syarat dan ketentuan

1. Peserta adalah pihak yang telah mengikuti mekanisme pendaftaran pada website resmi.
2. Peserta harus melengkapi berkas pendaftaran dengan data yang benar dan legal secara hukum.
3. Peserta yang tidak memenuhi persyaratan pendaftaran sampai waktu yang ditentukan akan dinyatakan gugur.
4. Peserta menyetujui apabila sewaktu-waktu dihubungi oleh panitia maupun partner dari
5. Setiap peserta hanya boleh terdaftar pada tepat satu tim pada kompetisi yang sama.
6. Setiap peserta hanya dapat menjadi ketua tim pada maksimal 1 (satu) kompetisi.
7. Jawaban yang dilombakan pada kompetisi harus merupakan karya orisinal peserta.
8. Hak kekayaan intelektual dari karya peserta pada kompetisi akan tetap menjadi hak dari peserta.
9. Karya peserta yang diikutsertakan pada kompetisi berhak untuk dipublikasikan oleh pihak
10. Peserta yang lolos dari babak penyisihan wajib mengikuti rangkaian acara Final.
11. Peserta yang tidak mengonfirmasi kehadiran acara Final akan didiskualifikasi.
12. Tim yang merupakan finalis kompetisi wajib menghadiri acara Awarding Night.
13. Pemenang yang tidak menghadiri akan kehilangan hak atas hadiah yang dimenangkan kecuali telah memberikan alasan yang mendesak dengan menghubungi panitia terlebih dahulu.
14. Panitia berhak untuk mencabut gelar juara dari pemenang jika ditemukan kecurangan serius atau pelanggaran hukum dalam karya yang dilombakan atau pun dalam proses pelaksanaan perlombaan.
15. Panitia berhak mendiskualifikasi tim yang melakukan tindak kecurangan maupun pelanggaran terhadap aturan kompetisi
16. Keputusan juri dan panitia tidak dapat diganggu gugat.

17. Panitia dapat mengubah seluruh aturan dalam rulebook sewaktu-waktu. Segala perubahan yang terjadi akan diberitahukan melalui email dan/atau website.

### **Tahap warming Up**

- Warming Up merupakan sesi pelatihan untuk melatih kemampuan peserta dan memperkenalkan sistem yang akan digunakan selama kompetisi. Situs dan informasi akun yang akan digunakan selama kelas berlangsung akan diberikan hanya kepada peserta yang telah diverifikasi dan telah memenuhi prosedur pendaftaran.
- Warming Up menggunakan format perlombaan jeopardy, dengan banyak soal tiap minggunya berkisar 5-7 soal.
- Hasil Warming Up tidak mempengaruhi hasil babak penyisihan dan babak final.
- Warming Up akan diadakan selama satu minggu.
- Tingkat kesulitan soal pada Warming Up belum tentu mencerminkan tingkat kesulitan soal yang akan diujikan pada babak penyisihan maupun babak final

### **Tahap Penyisihan**

- Babak penyisihan akan dilaksanakan secara online pada URL yang akan diumumkan.
- Babak penyisihan akan dilaksanakan selama 6 jam. Format perlombaan di babak penyisihan adalah jeopardy dengan banyak soal 12-15 soal.
- Scoreboard akan dibekukan pada 1 (satu) jam sebelum kontes berakhir.
- Tiap tim mengumpulkan write-up yang berisi deskripsi singkat soal, flag, dan langkah penyelesaian singkat selambat-lambatnya 3 jam setelah kontes selesai (platform dan soal penyisihan tetap dibuka hingga penutupan penerimaan write-up).
- Sepuluh tim terbaik yang menyelesaikan sekurang-kurangnya 1 (satu) soal dan mengumpulkan write-up yang valid berhak mengikuti babak final.
- Selama kompetisi berlangsung, setiap tim dilarang:
  - o Bekerjasama dalam bentuk apapun dengan yang bukan termasuk peserta dalam tim yang

bersangkutan (seperti dengan tim lain). o Mengganggu atau merugikan peserta lain maupun panitia.

- Tim yang diindikasikan melakukan pelanggaran atau kecurangan akan didiskualifikasi.

## Grand Final

- Babak final dilaksanakan secara onsite
- Babak final akan dilaksanakan selama 6 jam. Format perlombaan di babak final adalah tipe Hybrid Jeopardy dan Attack & Defense. Jeopardy 3 jam dan attack defence 3 jam.
- Setiap tim akan diberikan akses menuju Virtual Private Server (VPS) yang identik satu sama lain. Di dalam VPS akan terdapat beberapa container terisolasi yang masing-masing berisi service-service yang dapat dipertahankan oleh peserta ataupun diserang peserta tim lain. Setiap service mengandung flag dengan poin tertentu sesuai dengan tingkat kesulitan eksploitasinya. Peserta kemudian dapat mencari celah keamanan pada service miliknya sendiri, melakukan patching, dan menyerang celah keamanan service peserta lain (lihat bagian Sistem Penilaian). Detail jam nya seperti apa. Defence nya berapa jam, attack nya berapa jam .
- Setiap tim mempersiapkan maksimal 3 (tiga) laptop yang memiliki port LAN (atau membawa ekstensinya) untuk digunakan pada babak final. Jika tidak dapat menyediakan minimal 1 (satu) laptop, ketua tim dapat mengontak panitia untuk disiapkan laptop dari pihak panitia.
- Setiap tim diperbolehkan mengakses internet selama babak final berlangsung
- Setiap tim baru diperbolehkan menyerang service tim lainnya setelah 1 (satu) jam kompetisi berjalan.
- Scoreboard akan dibekukan pada 1 (satu) jam sebelum kompetisi berakhir.
- Selama kompetisi berlangsung, setiap tim dilarang:
  - a. Berkomunikasi dengan peserta tim lain.
  - b. Mengganggu atau merugikan peserta lain maupun panitia, seperti melakukan DoS, merusak service peserta lain, merusak properti penyelenggara, dan sebagainya.

- c. Mengganggu jalannya kompetisi dalam bentuk apapun.
- Tim yang diindikasikan melakukan pelanggaran atau kecurangan akan didiskualifikasi.

### **Awarding Night**

Awarding Night merupakan acara yang diadakan sebagai bentuk apresiasi kepada seluruh peserta kompetisi. Rangkaian acara Awarding Night akan berisi sambutan dari para tamu undangan, pengumuman pemenang setiap kompetisi, serta hiburan kepada seluruh tamu dan peserta yang hadir.