Format penyisihan adalah Capture the Flag (CTF) dengan tipe Jeopardy secara online. Pada CTF Jeopardy, peserta akan dihadapkan dengan sejumlah skenario keamanan dan mencari data khusus (Flag) yang bisa didapat dengan mengeksploitasi celah dari sistem atau mencari informasi penting yang terkait dengan keamanan dari data yang disiapkan.

BABAK KUALIFIKASI

JADWAL :

- **Pembagian akun :** 6 September 2019
- **Persiapan & pre-test :** 7 September 2019 (10.00 WIB - 12.00 WIB)
- **Kualifikasi :** 7 September 2019 (12.00 WIB - 23.59 WIB)
- **Batas pengiriman PoC :** 8 September 2019 (10.00 WIB)

KATEGORI DAN JUMLAH SOAL

1. Web Vulnerabitliy Assessment & Penetration Testing (5 soal)
2. Executable Binary Vulnerability Assessment & Penetration Testing (4 soal)
3. Network Packet & Log Analysis (3 soal)
4. Digital Forensic Analysis (3 soal)
5. Cryptography (3 soal)
6. Reverse Engineering (4 soal)

MEKANISME

1. Setiap soal berisi narasi kasus beserta berkas pendukung ataupun alamat layanan jaringan/web yang harus dianalisis keamanannya.
2. Setiap soal mempunyai bobot/poin yang berbeda-beda yang akan dihitung secara dinamis berdasarkan jumlah tim yang menyelesaikan soal tersebut.
3. Untuk mendapatkan nilai pada suatu soal, peserta harus melakukan submit Flag pada sistem penyisihan melalui submission form soal yang bersangkutan.
4. Scoreboard akan ditampilkan selama penyisihan berlangsung dan dibekukan pada saat 1 jam terakhir kompetisi.
5. Peserta yang berada di peringkat atas wajib mengumpulkan Proof of Concept (PoC) atau langkah penyelesaian tiap soal dalam bentuk PDF (tanpa template khusus) selambat-lambatnya 10 jam setelah kualifikasi berakhir melalui email cyberjawar4@gmail.com . **Soal yang tidak disertai dengan PoC yang jelas akan diberikan nilai 0** .

PERATURAN KHUSUS

Peserta dapat diberikan penalti hingga didiskualifikasi apabila terbukti melakukan hal berikut:

1. Melakukan DoS (Denial of Service) dalam bentuk apapun.
2. Melakukan kecurangan seperti berbagi Flag, melihat pekerjaan tim lain, memberikan akun kepada orang di luar tim, atau melakukan kerja sama antar tim.
3. Merusak sistem atau mengeksploitasi target berlebihan sehingga tidak bisa diselesaikan tim lain. Apabila peserta melakukan hal itu dengan tidak sengaja, harap laporkan ke panitia sesegera mungkin.
4. Melakukan akses berlebihan terhadap server. Tidak ada kasus yang membutuhkan online brute force . Akses berlebihan akan mengakibatkan IP di-ban secara otomatis dalam rentang waktu tertentu.

REFERENSI KOMPETISI

Model pelaksanaan kompetisi ini menggunakan standard Capture the Flag (https://ctftime.org/).