



BRIEFING LKS SMK TINGKAT NASIONAL

CYBERSECURITY

15 AGUSTUS 2024



Stanley Halim
Chrisando Ryan
Felix Alexander
Prajna Prasetya
Muhammad Faishol A M



JADWAL LOMBA



20 AGUSTUS 2024*
WARMUP TES PLATFORM

21 AGUSTUS 2024

JEOPARDY CAPTURE THE FLAG
Waktu pengerjaan: 7 jam
(10.00 - 18.00) [1 jam istirahat]

22 AGUSTUS 2024

ATTACK-DEFENSE
Waktu pengerjaan: 7 jam
(09.00 - 17.00) [1 jam istirahat]

JEOPARDY CAPTURE THE FLAG

LKSN Cybersecurity 2024



CAPTURE THE FLAG

FINAL

- Peserta diminta untuk mencari data khusus (flag) dengan cara mengeksploitasi celah sistem, menganalisis data atau menyelesaikan permasalahan
 - Format Flag = **LKSN{flag}**
 - Kategori Soal
 - Web Exploitation
 - Reverse engineering
 - Binary Exploitation/Pwn
 - Digital Forensic & Incident Response / DFIR
 - Cryptography
 - Kisi-kisi sesuai yang sudah di-share 😊
 - Soal untuk *Jeopardy* di-host pada platform CTFd yang nanti akan disebarakan dengan *credentials* yang sudah dikirimkan via *e-mail* (harap di cek per tim akan mendapatkan 1 credential)
-

PRE-LKSN NOTES

- Terdapat 1 soal yang akan memerlukan peserta untuk mengunduh file nya terlebih dahulu.
 - Size File (ZIPPED | UNZIPPED) = +/- 350 MB | +/- 2 GB
 - Soal ini khusus untuk forensik digital (**APT-41 Devil's Curriculum**)

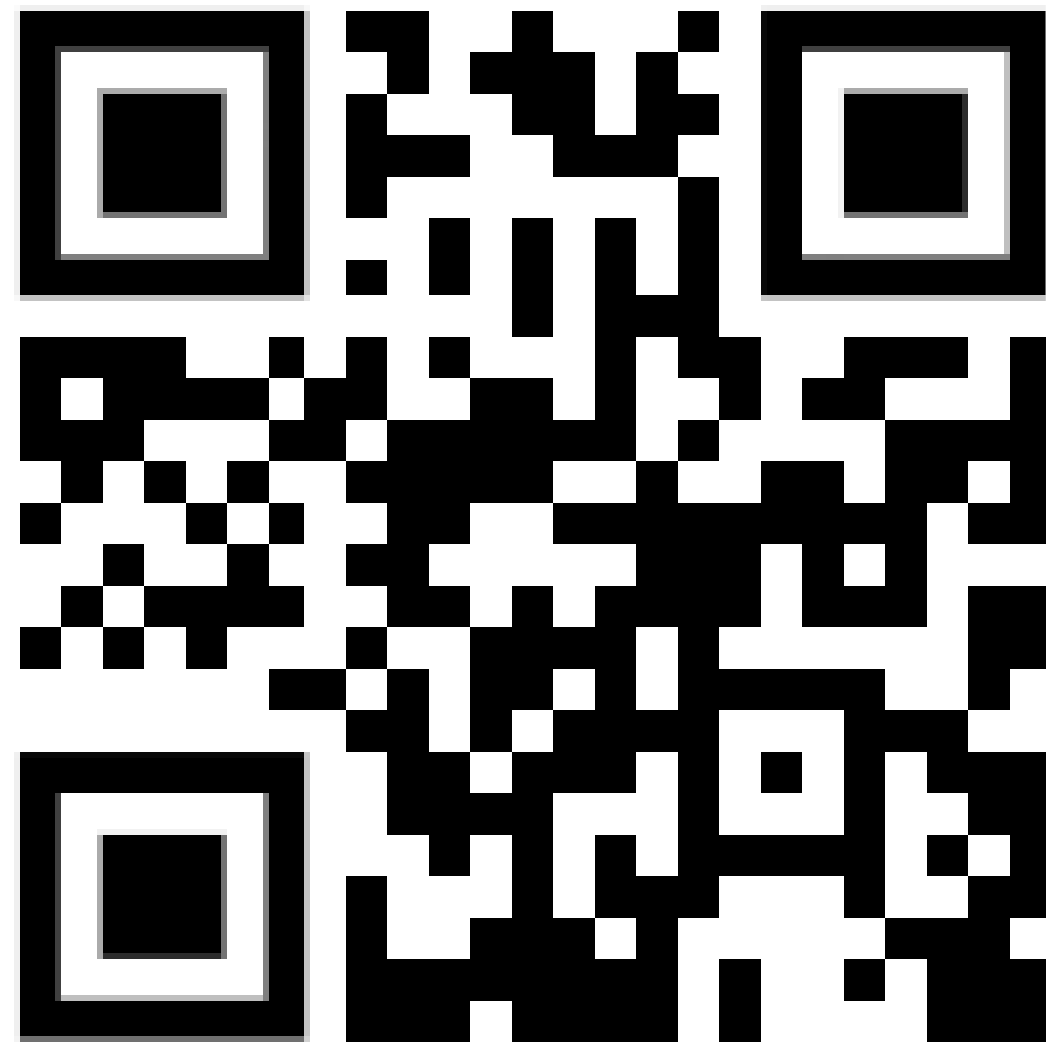


<https://shorturl.at/vJ5sQ>

PRE-LKSN NOTES

- Harap semua pembimbing dan peserta juga sudah **bergabung ke dalam grup Discord LKSN Cyber Security 2024** agar informasi yang akan diedarkan menyebar secara merata sehingga tidak ada lagi alasan bahwa file yang dibutuhkan belum sempat diunduh demi efisiensi perlombaan berlangsung
 - QR code untuk join ke grup Discord dapat dilihat setelah *slides* ini.
-

DISCORD SERVER




<https://discord.gg/ywvqC3rsP4>





PENILAIAN CTF JEOPARDY



- 
- **Jumlah soal 15 nomor dengan skor bervariasi untuk setiap nomornya**
 - **Scoring sifatnya statis**
 - **Peserta diminta untuk meraih poin sebanyak-banyaknya**
 - **Tidak ada ketentuan mengenai urutan pengerjaan soal maupun jumlah minimal soal yang harus dikerjakan**

SCORING STATIS JEOPARDY

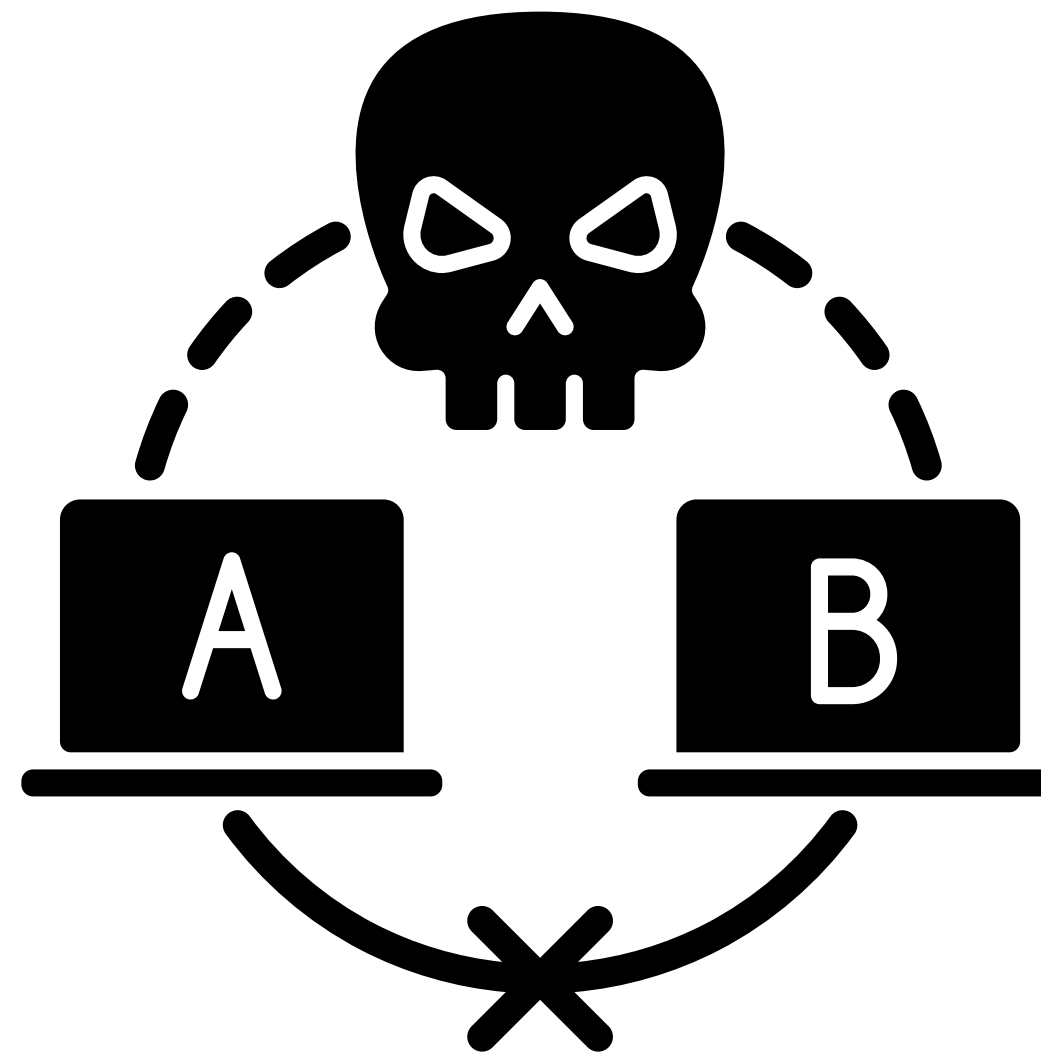
- Scoring statis artinya jumlah solve/tim yang berhasil menyelesaikan soal tersebut tidak mempengaruhi score yang ada, sehingga score sifatnya permanen.
 - Contoh:
 - Soal Web Exploitation: PPP akan bernilai 500 poin dari awal hingga akhir lomba, meskipun sudah banyak diselesaikan oleh beberapa peserta/tim
-

PROSEDUR PELAKSANAAN

- Pengerjaan Jeopardy CTF dimulai dari jam **10.00 - 18.00 (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: MAX 4 jam (19.00 - 22.00), akan lebih baik jika sambil mengerjakan juga dicicil dan di-screenshot POC/gambar pendukung bukti**
-

ATTACK AND DEFENSE

LKSN Cybersecurity 2024



SKEMA KONTES

- 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 based attack
 - Database based attack
 - Privilege escalation
 - Cryptography
 - Exploitation
 - CVE-Based Vulnerability (public exploit)
-

SKEMA KONTES

- Attack and defense akan diadakan selama 7 jam.
 - 09.00 WIB - 12.00 WIB: Periode 1
 - 12.00 WIB - 13.00 WIB: Istirahat (Contest Paused)
 - 13.00 WIB - 17.00 WIB: Periode 2
 - Peserta dapat melakukan defense maupun attack secara langsung.
 - **Peserta diharuskan menyusun laporan yang dikumpulkan sebelum jam 22.00 WIB (5 jam setelah lomba selesai).** Laporan setidaknya berisikan hal berikut.
 - *Attack vector*
 - *Exploit*
 - *Patch* yang dilakukan
 - **Setelah kompetisi berlangsung, peserta tidak dapat mengakses platform dan server** kembali. Oleh karena itu, disarankan kerangka laporan disusun selama kompetisi.
-

The diagram illustrates a network topology. On the left, two user icons labeled 'Team 1' and 'Team 2' are connected to a 'VPN' router. The 'VPN' router is connected to a 'Competition Platform' (represented by a globe icon). The 'VPN' router is also connected to a 'Router'. The 'Router' is connected to a 'Checker' (represented by a server rack icon) and two other servers labeled 'Server Team 1' and 'Server Team 2'.

- Peserta **harus terhubung ke VPN** untuk mengakses platform kompetisi dan server team.
- Checker merupakan sistem untuk mengecek setiap service di server peserta berjalan dengan sesuai.
- Peserta **hanya dapat dan boleh** mengakses server team dan platform kompetisi.
- IP seluruh request ke server peserta akan di-masking oleh router.

VPN & PLATFORM

VPN Wireguard

- Instalasi wireguard client: <https://www.wireguard.com/install/>
- Tutorial penggunaan wireguard client:
<https://gist.github.com/faishol01/6cf562acd107d019b631a30c19526bbf>

Platform

- Akan ada warmup setelah upacara pembukaan LKSN untuk pengenalan platform.
 - Dokumentasi terkait API platform:
<https://gist.github.com/faishol01/fe9c95ae8febc923564573201c5bb590>
-

CHECKER

- Checker akan mengecek secara periodik seluruh service yang ada.
 - Terdapat juga checker agent yang ditanam di setiap server team. Lebih lanjut akan dibahas pada bagian “Server Security”.
 - Berikut status yang dikeluarkan oleh checker:
 - **valid**: semuanya berjalan dengan baik.
 - **agent lost**: platform tidak menerima data dari checker agent.
 - **flag missing**: service tampaknya berjalan namun checker gagal mengakses flag.
 - **service faulty**: service dapat diakses, namun tidak sesuai.
 - **not reachable**: service tidak dapat diakses.
 - **internal error**: terdapat kesalahan pada checker.
-

SERVER

- Spesifikasi:
 - CPU: 2 core*
 - RAM: 4 GB*
 - OS: Ubuntu versi 24.04 LTS
- Setiap tim mendapat akses ke user **ubuntu** dengan privilege sudo.
- Autentikasi SSH menggunakan private key yang dapat dilihat di platform kompetisi.
- Reset server dapat dilakukan melalui platform kompetisi. Kegagalan server memberikan respon ke checker selama proses reset berjalan tetap diperhitungkan.

*apabila terdapat perubahan, akan diinformasikan sebelum kompetisi berlangsung.

SERVER SECURITY

- Juri akan menambahkan user **ctf** ke setiap server team. User tidak boleh diotak-atik. Juri akan mengumumkan public key dari SSH key yang digunakan oleh user.
 - Setiap server team dibekali dengan SELinux untuk tujuan berikut.
 - Menghilangkan kapabilitas sudo pada root, serta su pada semua user.
 - Membatasi akses ke flag.
 - Agent checker akan dipasang di seluruh team server. Agent checker akan mengecek kondisi internal dari server team, seperti namun tidak terbatas pada:
 - Status SELinux.
 - Akses flag.
 - Service yang berjalan.
-

SERVICE & FLAG

- Banyaknya service dapat dilihat di hari kompetisi melalui platform.
 - Akan terdapat sebanyak (banyak service) + 1 flag, terdiri dari flag service dan tambahan flag root.
 - Sebuah service bisa saja memiliki lebih dari satu kerentanan.
 - Flag root akan berada di /root/flag, sedangkan flag service akan berada di dalam folder utama dari service tersebut.
 - Flag akan dirotasi setiap 5 menit (1 tick), sehingga setiap tim dapat melakukan serangan kembali.
 - Format flag: **LKSN{<random-string>}**
 - Setiap team **harus memastikan** bahwa owner process dari service dan folder flag adalah user yang sama, terkecuali root flag.
-

Attack and Defense

PENILAIAN

- Penilaian akan didasarkan pada komponen CIS.

Criteria	Aspect	Aspect - Description	Judg	Extra Aspect Description (Meas or Judg)	Max
Enumeration	M	Participant should be able to perform necessary network enumeration and			1,50
	M	Participant should be able to perform necessary application enumeration and			1,00
Service N-th	J	Participant should be able to exploit the-Nth vulnerable service Attack percentage = flag captured / total flag * 100%	0 1 2 3	No attack Gain >0% attack percentage Gain >30% attack percentage Gain >60% attack percentage	1,00
	J	POC contains participants discovery result about service attack vector	0 1 2 3	No POC Discover >=25% attack vector Contain >=50% attack vector Contain >=75% attack vector	2,00
	J	Service N in the server should be available and functioning properly	0 1 2 3	The service is down continuously throughout the The service is up 1% - 33% of the competition The service is up 34% - 66% of the competition The service is up 67% - 100% of the competition	1,00
	J	Participant should be able to defend from attack for service Nth Defend percentage = (1 - flag stolen / (number team * number tick)) * 100%	0 1 2 3	No defend Gain >0% defend percentage Gain >30% defend percentage Gain >60% defend percentage	1,00
	J	Participant should be able to patch vulnerable service Nth	0 1 2 3	No patch Patch >= 25% of the attack vector Patch >= 50% of the attack vector Patch >= 75% of the attack vector	2,00

Attack and Defense

PENILAIAN

Criteria	Aspect	Aspect - Description	Judg	Extra Aspect Description (Meas or Judg)	Max
Root flag	J	Participant should be able to get root flag	0 1 2 3	No attack Gain >0% attack percentage Gain >30% attack percentage Gain >60% attack percentage	1,50
Privilege Escalation N-th	M	Participant should be able to exploit the artefact and perform privilege escalation POC contains these three mandatory remarks: 1. A clear and conscise step-by-step exploitation report 2. A clear evidence of how the exploitation is performed 3. A clear evidence of how the flag is obtained/produced	0 1 2 3	No POC Contain 1 mandatory remarks Contain 2 mandatory remarks Contain 3 mandatory remarks	1,50
	J				1,50
	M	Participant should be able to patch privilege escalation vulnerability			1,00
Unfair Attack - Disruption	J	Participant should never perform actions that are intentionally disturb their	0 1 2 3	Caught performing illegal strategy multiple times Caught performing illegal strategy two times Caught performing illegal strategy once Participant's strategy is according to the rules	2,00
Unfair Attack - Integrity	J	Participant should never perform actions that are intentionally destroys the	0 1 2 3	Caught performing illegal strategy multiple times Caught performing illegal strategy two times Caught performing illegal strategy once Participant's strategy is according to the rules	2,00
Abuse of Platform	J	Participant is caught to perform intentonal attack against the competition's A&D	0 1 2 3	Caught performing attack against platform multiple Caught performing attack against platform two Caught performing attack against platform once Participant's attack is directed properly and	2,00

LARANGAN

Segala bentuk pelanggaran akan berdampak pada pengurangan poin hingga diskualifikasi.

- Mematikan dan mengubah konfigurasi SELinux di server team.
 - Melakukan perubahan pada user atau proses di bawah user ctf (e.g. mematikan agent checker, mengubah SSH authorized_keys).
 - Mematikan ataupun merestart server team.
 - Merusak ataupun memberi beban berlebihan server team lain.
 - Melakukan attack pada infrastruktur perlombaan (e.g. platform, checker, VPN server).
 - Mengirimkan credentials VPN ataupun platform ke pihak lain, selain anggota tim.
-