
2025
31 Maret – 6 April 2025
Kamsib Indonesia on Paper
Edisi 9
Tetap Aman Bersama Kamsib
Kamsib Indonesia on Paper adalah majalah yang membahas berbagai aspek keamanan siber, mulai dari ancaman terbaru, teknik perlindungan, hingga tren teknologi yang memengaruhi lanskap keamanan digital.

Kamsib Indonesia on Paper

Edisi 9
31 Maret – 6 April 2025

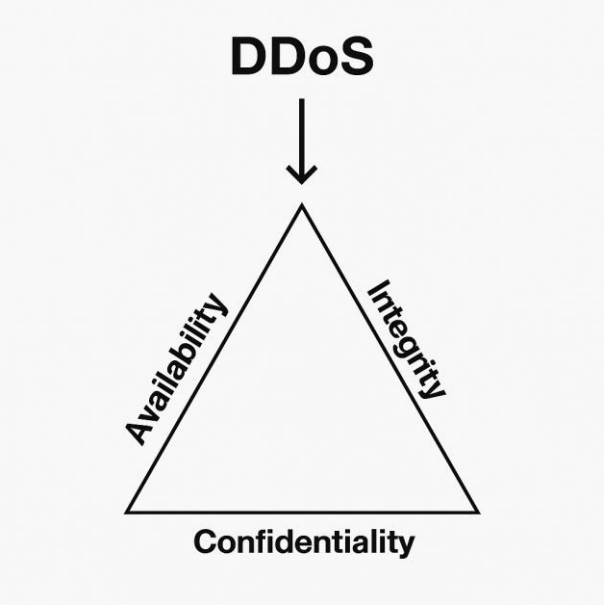
DDoS bisa saja menjadi pintu masuk untuk pencurian data dalam serangan gabungan.

Distributed Denial of Service dan Hubungan dengan CIA Triad

Penulis: **Anton Lepari**

Hubungan antara *Distributed Denial of Service* (DDoS) dengan CIA Triad sangat penting untuk dipahami dalam konteks keamanan siber. *Confidentiality* (kerahasiaan), *integrity* (integritas), dan *availability* (ketersediaan) adalah tiga pilar utama dalam keamanan informasi.

Pilar *availability* memastikan bahwa sistem dan data tersedia bagi pengguna yang berwenang saat dibutuhkan. Serangan DDoS secara langsung menyerang aspek *availability*. Tujuan utama DDoS adalah membuat layanan (seperti website, API, DNS, atau sistem jaringan) tidak bisa diakses oleh pengguna sah, dengan cara membanjiri sistem dengan trafik palsu atau tidak perlu. Contohnya ketika sebuah bank *online* diserang DDoS, nasabah tidak bisa mengakses layanan perbankan mereka—ini adalah pelanggaran terhadap aspek *availability*.



Gambar 1: DDoS Menyerang CIA Triad.

Hubungan Tidak Langsung dengan *Integrity* dan *Confidentiality*

Meskipun DDoS tidak secara langsung mengubah data, serangan ini bisa dijadikan gangguan sementara yang menyembunyikan serangan lain (misalnya, peretasan atau manipulasi data yang dilakukan secara bersamaan).

Dalam konteks ini, integritas bisa terganggu jika DDoS digunakan sebagai pengalih perhatian. Misalnya saat sistem IT sibuk menangani DDoS, peretas bisa menyusup ke sistem untuk mencuri atau mengubah data.

DDoS bukanlah serangan yang mencuri data. Tapi seperti pada integritas, DDoS bisa digunakan sebagai bagian dari serangan gabungan (*multi-vector attack*). Saat semua perhatian tertuju ke serangan DDoS, peretas bisa mencoba mencuri data secara diam-diam. Contohnya saat layanan VPN diserang DDoS, pelaku bisa mencoba menembus *server backend* dan mencuri informasi pelanggan saat lalu lintas kacau.

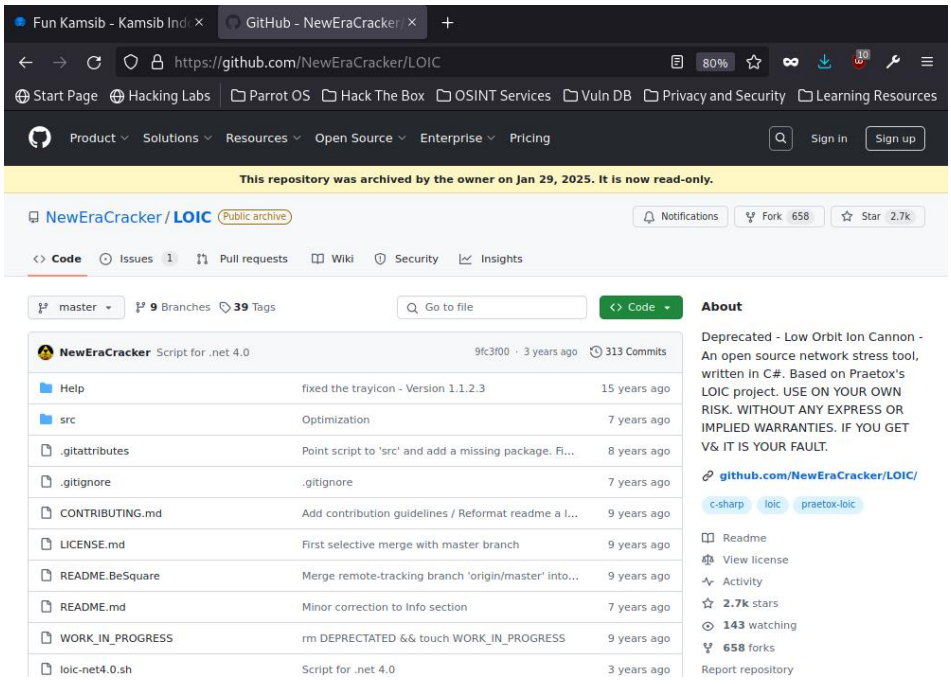
Apakah melakukan serangan DDoS merupakan tindak pidana?.

LOIC (Low Orbit Ion Cannon) dan DDoS

Penulis: **Anton Lepari**

LOIC (Low Orbit Ion Cannon) adalah alat open-source yang awalnya dibuat untuk melakukan stress testing pada jaringan, namun lebih dikenal karena sering digunakan dalam serangan DDoS (Distributed Denial of Service), terutama oleh kelompok aktivis dunia maya seperti Anonymous.

- **Nama**: Low Orbit Ion Cannon
- **Dibuat oleh**: Praetox Technologies
- **Bahasa**: .NET (versi aslinya), tapi ada juga versi web dan JavaScript (JS LOIC)
- **Fungsi utama**: Mengirim permintaan HTTP, UDP, atau TCP ke target secara terus-menerus untuk membanjiri server atau layanan tersebut.
- **Platform**: Windows, Linux (melalui Mono), Mac



Gambar 2: LOIC di GitHub.

LOIC bekerja dengan cara membanjiri server target dengan trafik yang sangat tinggi dari banyak klien (komputer) untuk membuat server menjadi tidak dapat

merespons permintaan pengguna yang sah. Bila dilakukan dari banyak komputer sekaligus, ini menjadi serangan DDoS.

Disclaimer

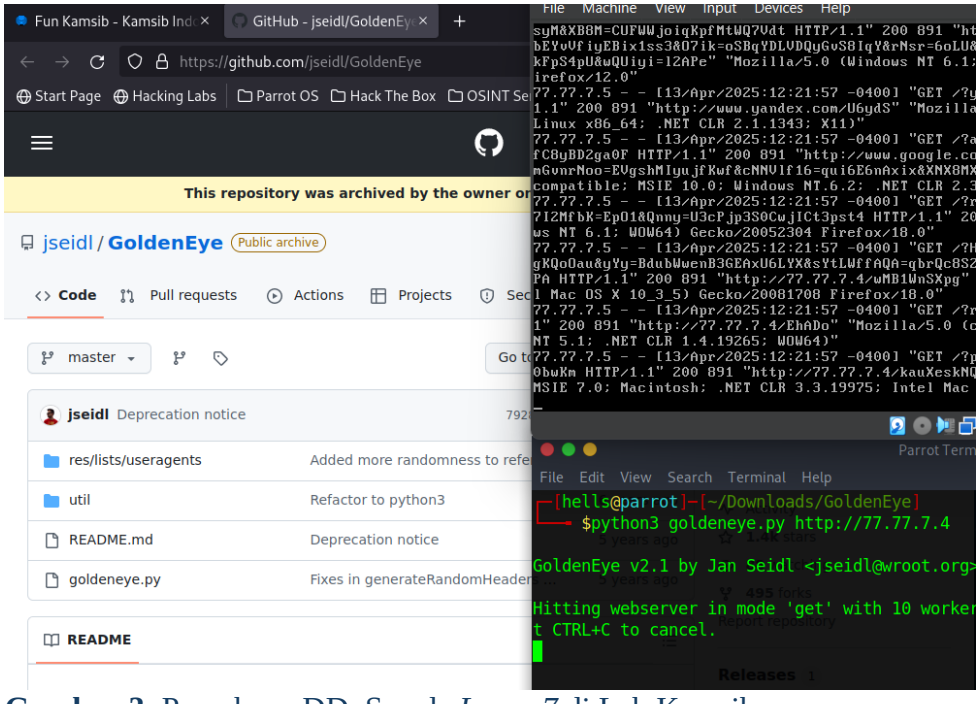
Pengetahuan ini disampaikan untuk tujuan edukasi dan pembelajaran saja. Melakukan DDoS tanpa izin adalah tindakan illegal. Jangan gunakan pengetahuan ini untuk menyerang sistem yang bukan milikmu atau tanpa izin eksplisit dari pemilik.

"Kelelahan sumber daya"

Mengapa DDoS Menyebabkan Down pada Server?

Penulis: **Anton Lepari**

Serangan DDoS menyebabkan server menjadi *down* karena server atau sistem target dibanjiri dengan lalu lintas (*traffic*) yang sangat besar dan tidak wajar dari banyak sumber sekaligus, sehingga sumber daya server tidak mampu menangani permintaan tersebut. Bayangkan ada toko kecil yang hanya bisa melayani 5 pelanggan sekaligus. Lalu 500 orang pura-pura datang ingin dilayani padahal hanya ingin mengganggu. Pelanggan asli tidak bisa masuk, karyawan toko jadi kewalahan. Akhirnya toko itu tutup sementara — itu mirip seperti server yang *down* karena DDoS.



Gambar 3: Percobaan DDoS pada *Layer 7* di Lab Kamsib.

Overload pada *Bandwidth*

Lalu lintas yang sangat besar menghabiskan kapasitas jaringan (*bandwidth*) yang tersedia. Akibatnya, koneksi sah dari pengguna asli jadi tertunda atau bahkan gagal.

Kelelahan Sumber Daya Server

Permintaan palsu yang terus-menerus menyebabkan CPU tinggi, memori habis, *thread* atau proses penuh, serta server tidak bisa lagi memproses permintaan normal.

Crash atau *Freeze*

Jika sistem tidak didesain untuk menghadapi beban besar, bisa menjadi tidak responsif atau langsung *crash* (mati total).

Gangguan pada *Firewall* atau *Load Balancer*

Perangkat keamanan seperti *firewall* bisa *overload* juga, yang menyebabkan kegagalan sistem proteksi dan jalur akses sah ikut terganggu.

Penting banget untuk paham perbedaan DDoS Layer 4 vs Layer 7, terutama kalau kamu mau belajar deteksi dan mitigasinya.

DDoS di Layer 4 dan Layer 7

Penulis: **Anton Lepari**

Serangan *Distributed Denial of Service* dapat terjadi di berbagai lapisan dalam model OSI, namun dua jenis yang paling umum adalah serangan pada *Layer 4* (*Transport Layer*) dan *Layer 7* (*Application Layer*). Serangan *Layer 4* umumnya mengeksploitasi protokol TCP atau UDP untuk membanjiri server dengan trafik mentah dalam jumlah besar, seperti dalam kasus *SYN flood* atau *UDP flood*. Tujuannya adalah untuk menghabiskan sumber daya jaringan dan memutus konektivitas sebelum permintaan bahkan mencapai aplikasi itu sendiri.

Aspek	Layer 4 (Transport Layer)	Layer 7 (Application Layer)
📶 Protokol	TCP, UDP	HTTP, HTTPS, DNS, SMTP, dll
🎯 Target	Port tertentu (misal TCP 80, UDP 53)	Aplikasi spesifik (misal website, API, login page)
⚒️ Cara kerja	Banjiri koneksi TCP/UDP agar server/network overload	Kirim request HTTP/HTTPS berlebihan ke aplikasi
📈 Volume trafik	Biasanya **besar & cepat** (raw packet flood)	Bisa **rendah tapi pintar** (bypass detection)
🛡️ Mitigasi	Firewall, rate-limit TCP/UDP, IDS/IPS	Web Application Firewall (WAF), CAPTCHA, Bot detection
📁 Contoh tools	`hping3`, `UDP flood`, `SYN flood`, `LOIC (TCP/UDP)`	`slowloris`, `GoldenEye`, `HULK`, `LOIC (HTTP)`, `Xerxes`
📝 Terdeteksi di	`iptables`, `netstat`, log kernel/network	`access.log` web server, WAF log, application log

Gambar 4: Tabel Perbedaan Ketika Melakukan DDoS di *Layer 4* (*Transport*) dan *Layer 7* (*Application*).

Sementara itu, serangan *Layer 7* beroperasi pada lapisan aplikasi, menyerang layanan seperti HTTP atau HTTPS. Serangan ini lebih canggih karena meniru permintaan pengguna yang sah, misalnya dengan mengirim ribuan permintaan HTTP GET ke halaman website. Meski jumlah permintaan tidak sebesar *Layer 4*, jenis serangan ini dapat sangat efektif karena langsung membebani aplikasi, database, dan logika bisnis yang berjalan di belakangnya. Akibatnya, server menjadi lambat merespons atau bahkan tidak dapat digunakan.

Perbedaan utama antara kedua jenis serangan ini terletak pada tingkat serangan dan metode deteksinya. Serangan *Layer 4* cenderung lebih mudah dikenali melalui monitoring *bandwidth* atau *log firewall*, sementara serangan *Layer 7*

sering kali memerlukan deteksi berbasis perilaku, seperti penggunaan *Web Application Firewall* (WAF) atau sistem deteksi anomali. Oleh karena itu, memahami perbedaan keduanya sangat penting dalam merancang strategi pertahanan yang komprehensif terhadap DDoS.

Kamsib Indonesia
Jakarta, Indonesia
hubungi@kamsib.id

Kamsib ID *adalah sebuah platform edukasi yang berfokus pada keamanan informasi dan siber dalam bahasa Indonesia. Kehadiran Kamsib dipicu oleh lonjakan pesat penggunaan internet yang tidak diimbangi dengan kesadaran akan pentingnya keamanan di dunia maya. Fenomena ini juga menjadi salah satu pemicu dari banyaknya kasus penipuan, kebocoran data, dan insiden dalam sistem elektronik, baik yang dimiliki oleh pemerintah maupun swasta.*

Kamsib Indonesia on Paper *adalah majalah yang membahas berbagai aspek keamanan siber, mulai dari ancaman terbaru, teknik perlindungan, hingga tren teknologi yang memengaruhi lanskap keamanan digital. Diterbitkan secara berkala, majalah ini menyajikan artikel mendalam, studi kasus, serta wawancara dengan para ahli untuk memberikan wawasan bagi profesional keamanan siber, peneliti, dan penggemar dunia siber. Dengan pendekatan yang informatif dan analitis, Kamsib Indonesia on Paper bertujuan menjadi referensi utama bagi siapa saja yang ingin memahami dan menghadapi tantangan di dunia siber yang terus berkembang.* [at]kamsib_id