

MAGAZINE

PUNGGAWA CYBER SECURITY

CAI FRAMEWORK

AN OPEN SOURCE
AI PLATFORM FOR
CYBERSECURITY
AUTOMATION

MITRE ATT&CK VS CYBER KILL CHAIN

UNDERSTANDING
THE TOOLS
CYBER DEFENSE

2025

CVE HAMPIR DIHENTIKAN

DATA KITA, KUASA SIAPA?

RED TEAM OPS

SIMULASI
SERANGAN ALA
PENJAHAT SIBER

BLUE TEAM

SECURING COMPLIANCE +
CORE OF REGULATORY RESILIENCE

CHRONICLES +
DIGITAL FORENSICS IN
ACTION

Tentang Kami

PUNGGAWA merupakan istilah dari kebudayaan Indonesia yang mengacu pada sosok pemimpin atau figur berwibawa yang terkenal akan kepemimpinannya, tanggung jawab, dan arahan dalam suatu komunitas. Istilah ini melambangkan dedikasi terhadap keunggulan kepemimpinan, praktik etik, atribut kekuatan, kearifan, dan kepercayaan, serta sikap pelindung terhadap mereka yang berada dalam lingkup pengawasannya.

Kami Merupakan PUNGGAWA

Tim PUNGGAWA didirikan pada tahun 2018 dan mulai memberikan layanan kepada pelanggan pada tahun 2019, dengan memulai dari layanan uji penetrasi. Kami telah berhasil merealisasikan dan menembus pasar keamanan siber di Indonesia. Dalam kemitraan dengan klien, kami menyediakan solusi dan layanan keamanan siber yang dirancang untuk meningkatkan postur keamanan secara komprehensif, menutup celah, dan memantau kerentanan secara berkelanjutan melalui operasi dan dukungan yang persisten dengan mengimplementasikan identifikasi, perlindungan, deteksi, respons, dan pemulihan.

VISI

Menjadi Mitra Pilihan dalam Kemampuan Keamanan Siber sebagai Kontribusi Utama dalam Mewujudkan Dunia yang Lebih Aman bagi Transformasi Digital.

MISI

MENCAPAI HASIL YANG SUKSES

Pada akhirnya, dedikasi kami terhadap proses dan kualitas sumber daya manusia akan menjadi pendorong utama dalam menghadirkan solusi yang memberikan hasil terbaik bagi klien kami.

BUDAYA PEMBELAJARAN DAN KESADARAN

Kami akan terus membangun budaya pembelajaran dan kesadaran di dalam tim kami guna meningkatkan kompetensi dan pemahaman yang lebih mendalam.

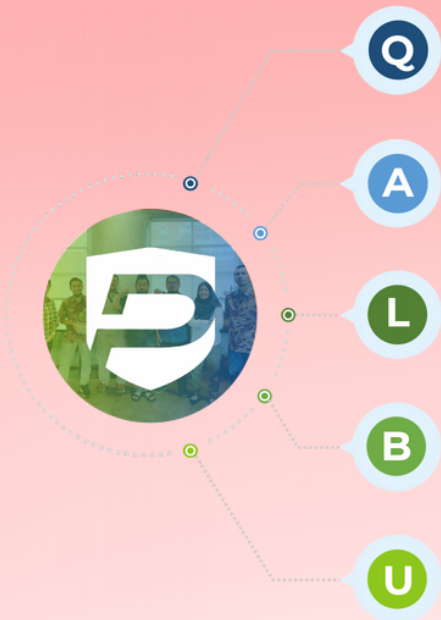
BERBAGI DAN BERKOLABORASI DENGAN KOMUNITAS

Kami bekerja secara kolaboratif sebagai mitra dan tim, baik di dalam organisasi maupun dengan komunitas yang lebih luas.

NILAI INTI KAMI

Di PUNGGAWA, kami mengejar tujuan dan kesuksesan, dengan pemahaman bahwa satu akan membawa pada yang lain. Nilai inti kami membina budaya yang mendukung respons yang cepat dan berkualitas tinggi, sikap proaktif, pembelajaran dan kepemimpinan yang berkelanjutan, pemecahan masalah yang inovatif, dan kesatuan yang kokoh. Prinsip-prinsip ini memandu tim kami dalam menyediakan solusi keamanan siber yang maju dan dapat diandalkan, memastikan keamanan digital klien kami dengan profesionalisme dan kecemerlangan tertinggi. Kami menjalankan nilai-nilai kami dan mewujudkannya setiap hari melalui hubungan kami dengan karyawan, klien, mitra, dan keluarga.

CORE VALUE, QALBU



Quick and High Quality Response:

Dalam keamanan siber, respons yang cepat terhadap ancaman sangat krusial. Di PUNGGAWA, kami mengutamakan aksi cepat untuk mengidentifikasi dan meredakan ancaman siber, memastikan aset digital klien terlindungi secara efisien dan efektif. Respons berkualitas tinggi juga berarti memberikan solusi yang menyeluruh dan berpengetahuan luas terhadap tantangan keamanan siber yang kompleks.

Attitude is Everything:

Sikap positif dan proaktif sangat penting di PUNGGAWA. Ini melibatkan usaha untuk selalu mendahului ancaman potensial, antusiasme untuk belajar tentang tren keamanan baru, dan memelihara ketahanan mental menghadapi ancaman siber yang terus berkembang. Sikap yang berorientasi pada peningkatan berkelanjutan esensial dalam beradaptasi dengan dinamika keamanan siber.

Listen, Learn, Lead & Succeed:

Nilai ini menekankan pentingnya pembelajaran berkelanjutan dalam bidang keamanan siber. Dengan mendengarkan secara aktif kebutuhan klien dan perkembangan industri, tim PUNGGAWA tetap terdepan dan terinformasi. Pembelajaran ini berujung pada kepemimpinan di bidangnya, pengembangan solusi inovatif, dan kesuksesan dalam melindungi klien dari ancaman siber.

Be a Problem Solver:

Keamanan siber seringkali tentang menyelesaikan teka-teki yang kompleks yang dihadirkan oleh ancaman siber. Di PUNGGAWA, kami menekankan pentingnya pendekatan yang berorientasi pada solusi, baik itu dalam mengatasi serangan siber yang rumit, menavigasi kerentanan jaringan yang kompleks, atau menemukan solusi kreatif untuk tantangan keamanan baru.

Unity is Our Strength

Kami memahami tantangan kewirausahaan dan mengetahui bahwa keamanan siber memerlukan kerja sama tim dan kolaborasi, baik di dalam organisasi maupun dengan klien, mitra, dan komunitas keamanan siber yang lebih luas. Kesatuan dalam tujuan dan aksi menjamin pertahanan yang lebih kuat terhadap ancaman siber dan postur keamanan yang lebih tangguh.

FROM CEO PUNGGAWA



Salam hangat para pembaca setia Punggawa Cybersecurity Magazine!

Selamat datang di edisi kelima majalah kami—Punggawa Cybersecurity Magazine Volume 5, yang kali ini mengangkat tema yang sangat dinamis dan krusial dalam dunia pertahanan siber: Red Team Operations dan beragam aspek ancaman siber modern yang tidak terlihat secara kasatmata, namun sangat merusak.

Di tengah laju transformasi digital yang semakin masif, ancaman siber pun ikut berkembang—bukan hanya dari sisi teknis, tetapi juga dari sisi psikologis, sosial, dan strategi. Dalam edisi kali ini, kami mengajak Anda untuk menyelami dunia Red Team Operations: simulasi serangan layaknya penjahat siber sungguhan, yang dirancang untuk menguji dan memperkuat pertahanan organisasi secara nyata.

Tema utama “Red Team Ops: Simulasi Serangan ala Penjahat Siber” akan membuka cakrawala baru tentang bagaimana serangan dilakukan secara stealth, terstruktur, dan penuh strategi. Tidak hanya itu, kami juga membahas The Invisible Threat—taktik serangan nirkabel dan rekayasa sosial modern yang kerap luput dari radar keamanan tradisional.

Dalam edisi ini, Anda akan menemukan beragam topik penting seperti ancaman persisten dari kredensial tersembunyi, isu kedaulatan data, masa depan CVE, perbandingan MITRE ATT&CK dengan Cyber Kill Chain, peran Blue Team dalam regulasi, praktik forensik digital, psikologi penyerang, hingga pemanfaatan AI melalui CAI Framework.

Dengan penuh semangat, kami menyajikan konten eksklusif yang tidak hanya informatif, tetapi juga strategis dan aplikatif. Harapannya, edisi Volume 5 ini bisa memperluas wawasan Anda tentang lanskap ancaman siber yang semakin kompleks, sekaligus memperkuat pertahanan digital organisasi Anda.

Terima kasih telah menjadi bagian dari perjalanan kami. Semoga edisi kali ini dapat menjadi sumber inspirasi dan pengetahuan yang bermanfaat bagi Anda semua. Selamat membaca!

Iwan Setiawan
CEO PUNGGAWA CYBERSECURITY

Magazine Punggawa Volume 5

Table of Contents

07	27
Red Team Ops : Simulasi Serangan ala Penjahat Siber	MITRE ATT&CK vs Cyber Kill Chain
11	29
The Invisible Threat: Mengupas Taktik Wireless Attack dan Social Engineering Modern	Securing Compliance: Blue Team as the Core of Regulatory Resilience
16	32
Persistent Threats from Persistent Secrets	Blue Team Chronicles: Digital Forensics in Action
21	35
DATA KITA, KUASA SIAPA? Menelusuri Jejak, Ancaman, dan Masa Depan Data Pengguna Digital	Psikologi Penyerang: Membaca Pola Pikir Hacker dalam Operasi Red Team
24	38
CVE Hampir Dihentikan	CAI Framework - An Open Source AI Platform for Cybersecurity Automation



Editor-in-Chief

Om Fadhil

Managing Editor

Kang Ali



Our Contributors

Mas Davan

Faris

Om Fadhil

Bang Rajavi

Kang Ali

Mas Ade

April

Daffa

Pakde Iwan



In this issue

Dalam edisi ini beragam topik penting seperti ancaman persisten dari kredensial tersembunyi, isu kedaulatan data, masa depan CVE, perbandingan MITRE ATT&CK dengan Cyber Kill Chain, peran Blue Team dalam regulasi, praktik forensik digital, psikologi penyerang, hingga pemanfaatan AI melalui CAI Framework.

RED TEAM OPS : SIMULASI SERANGAN ALA PENJAHAT SIBER

BY PAKDE IWAN

Pendahuluan: Masuk Lewat Pintu yang Tidak Terkunci

Dunia digital bukan hanya dihuni oleh sistem dan kode, tetapi juga oleh manusia dengan kelemahan dan pola pikir yang bisa ditebak. Seperti kata Bruce Schneier, "Security is not a product, but a process." Red Team tidak datang untuk menghancurkan, tapi untuk membuka mata. Kami adalah tim penyerang yang bekerja untuk pertahanan.

Kami tidak bertopeng. Kami tidak menyusup secara diam-diam di malam hari. Kami hadir atas undangan, untuk menguji, mendorong batas, dan membantu organisasi melihat realitas bahwa celah keamanan bukan hanya persoalan teknologi—tetapi juga manusia.

Dalam artikel ini, kami akan membedah simulasi serangan yang kami lakukan terhadap sebuah perusahaan fiktif bernama PT Sibernesia. Kami masuk, kami menjelajah, dan kami mencatat semuanya. Tujuannya? Agar pertahanan bisa diperkuat sebelum penjahat sungguhan datang. Kami membagi kisah ini ke dalam beberapa fase, masing-masing dengan pelajaran nyata bagi siapa pun yang terlibat dalam dunia pertahanan siber.



Fase 1:

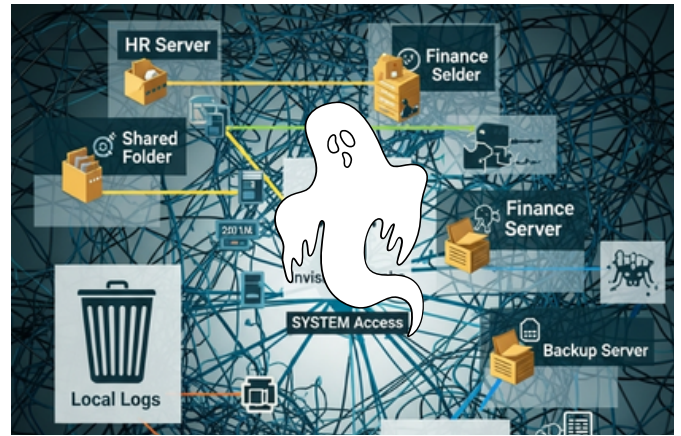
Rekayasa Sosial – Senjata Favorit Tanpa Kode

Serangan kami dimulai bukan dari terminal, melainkan dari browser. Tim OSINT kami menelusuri jejak digital PT Sibernesia dan karyawannya. Dalam waktu dua jam, kami tahu siapa CEO-nya, siapa staf HR-nya, ulang tahun manajer TI-nya, dan bahwa bagian finance baru saja pindah ke gedung baru. Kami bahkan tahu kebiasaan kopi mingguan mereka dari foto-foto Instagram yang diunggah tanpa rasa waspada.

Target kami adalah staf HR yang tampaknya rajin mengunggah aktivitas kantor. Kami menyusun email phishing yang tampak sah dan sangat personal. Judulnya: "Voucher Kopi Favorit Anda – Hadiah dari Sibernesia". Di dalamnya, link palsu yang menanamkan backdoor ketika diklik.

Backdoor ini ditanam dengan memanfaatkan skrip Powershell terselubung yang berjalan melalui exploit macro dari file Word terlampir. Payload terenkripsi menggunakan AES-256 dan melakukan beaconing setiap 10 menit melalui kanal HTTPS terenkripsi, menyamarkan dirinya sebagai lalu lintas web normal ke subdomain palsu yang menyerupai vendor aplikasi absensi.

Hasilnya? Berhasil. Backdoor aktif dalam waktu kurang dari lima menit. Tanpa perlu malware zero-day. Tanpa exploit rumit. Hanya manusia yang merasa dihargai dengan kopi gratis. Di sinilah kita diingatkan bahwa manusia bukan titik lemah. Manusia adalah pintu.



Fase 2:

Eksplorasi dan Pivoting – Menjadi Hantu di Sistem

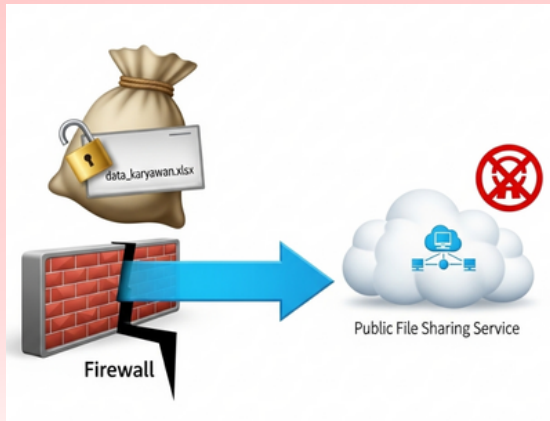
Setelah memperoleh akses awal, kami mulai menjelajah. Backdoor kami memberi hak akses sebagai staf HR, tapi kami tahu yang kami butuhkan lebih dari itu. Kami menjalankan skrip enumeration berbasis PowerView untuk memetakan Active Directory (AD) environment. Kami temukan adanya shared folder yang salah konfigurasi dengan permission "Everyone: Full Control". Di dalamnya, kami menemukan file teks yang berisi backup konfigurasi router dan file .ini yang mengandung kredensial database plaintext.

Kami gunakan kredensial admin tersebut untuk berpindah ke server internal. Di sini kami menerapkan teknik "living off the land"—menggunakan tools bawaan sistem seperti PowerShell dan WMIC agar tidak terdeteksi oleh sistem keamanan. Dengan menjalankan perintah WMI untuk mengeksekusi skrip di server lain, kami mengeksekusi payload yang mem-bypass UAC (User Account Control) dan mendapatkan shell sebagai SYSTEM.

Kami berhasil mengakses server keuangan, menyusuri jaringan menuju backup server, dan menemukan bahwa tidak ada segmentasi jaringan yang memadai. VLAN didefinisikan tapi tidak diproteksi oleh ACL (Access Control List). Semua subnet dapat saling ping dan terhubung melalui RDP tanpa autentikasi dua faktor.

Lebih parahnya, semua log akses server disimpan lokal dan tidak terkirim ke SIEM. Tidak ada centralized logging atau syslog forwarding ke server monitoring. Artinya? Kami bisa berjalan bebas tanpa jejak.

Fase 3: Simulasi Eksfiltrasi – Meniru Langkah Penjahat



Eksfiltrasi adalah tahap paling berisiko dalam operasi nyata. Tapi kami ingin tahu: apakah organisasi ini akan menyadari jika data mereka dikirim keluar? Kami membuat file dummy bernama "data_karyawan.xlsx" berisi informasi acak. File ini dikompresi menggunakan 7zip dengan password kompleks dan dienkripsi kembali menggunakan OpenSSL.

Kami menggunakan skrip curl untuk mengunggah file tersebut ke layanan file sharing publik, melalui koneksi HTTPS port 443. Karena koneksi ini menyerupai trafik browser umum, firewall tidak melakukan inspeksi konten atau SSL interception.

Hasilnya? Berhasil, tanpa satu pun alert dari sistem keamanan. Tidak ada proxy inspeksi. Tidak ada DLP (Data Loss Prevention). Tidak ada aturan egress filtering yang memblokir akses ke domain non-whitelisted. Bahkan tidak ada notifikasi ke admin jaringan karena sistem SIEM tidak meng-capture outbound data movement.

Kami tinggalkan pesan simbolik di desktop IT Support:

"Kami sudah di sini. Perkuat pintu Anda sebelum orang lain masuk." Pesan ini adalah tanda bahwa simulasi berakhir.

Fase 4:

Evaluasi Bersama Manajemen dan Tim IT

Setelah simulasi berakhir, kami duduk bersama tim IT dan manajemen PT Sibernesia untuk menjelaskan temuan kami. Bukan untuk menghakimi, tetapi untuk membuka wawasan. Mereka terkejut, tentu saja. Tapi mereka juga berterima kasih.

Kami menyusun laporan teknis dan eksekutif. Di dalamnya, kami sampaikan:

- Risiko terbesar bukan berasal dari teknologi, tapi dari kepercayaan berlebih terhadap proses manual.
- Tidak adanya monitoring terpusat berarti serangan tidak pernah terlihat.
- Password yang lemah dan privilege yang terlalu luas menciptakan jalur eskalasi.
- Training karyawan tentang phishing dan rekayasa sosial masih minim.
- Tidak ada egress filtering yang memblokir pengiriman data ke domain asing.

Penggunaan protokol internal yang tidak dienkripsi (mis. SMBv1) masih ditemukan.

"The human element is the weakest link in security"
Kevin Mitnick, the world's most famous hacker

Refleksi: Mengapa Simulasi Itu Penting?

Kami percaya, satu simulasi bisa menyelamatkan data jutaan orang. Serangan dunia nyata tidak menunggu kesiapan organisasi. Dan seperti yang dikatakan oleh Kevin Mitnick, mantan hacker yang kini menjadi konsultan keamanan ternama, "The human element is the weakest link in security."

Tim Red Team tidak hanya melatih pertahanan teknis. Kami juga membantu perusahaan membangun budaya skeptisisme digital, budaya di mana semua karyawan merasa bertanggung jawab terhadap keamanan.

Simulasi serangan adalah cara organisasi untuk melihat dirinya dari mata penyerang. Dan dari perspektif itu, kita bisa menemukan kebenaran yang tidak tampak dari dalam.

Penutup: Red Team untuk Menyelamatkan, Bukan Menghancurkan

Kami hadir bukan sebagai ancaman, tetapi sebagai pelajaran hidup. Setiap simulasi bukan sekadar uji teknis, melainkan juga refleksi terhadap budaya keamanan itu sendiri. Dunia siber tidak mengenal kompromi. Satu kesalahan kecil bisa berarti hilangnya kepercayaan pelanggan, kerugian finansial, atau bahkan reputasi yang hancur.

Red Team Ops bukan soal menang, tapi soal mencegah kekalahan. Red Teaming adalah upaya untuk membangun benteng dari dalam, bukan hanya dari luar. Dan ketika organisasi mampu melihat dirinya dari sudut pandang musuh, maka ia sedang berada di jalur yang benar untuk menang.

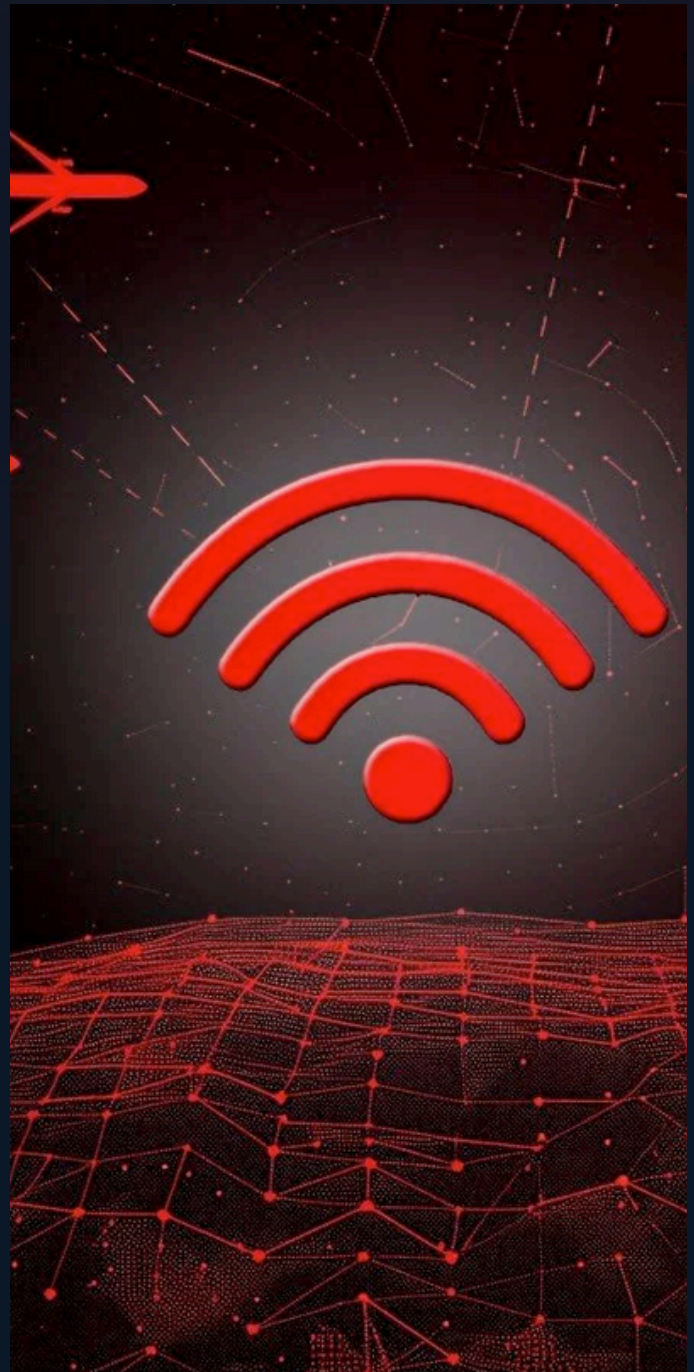
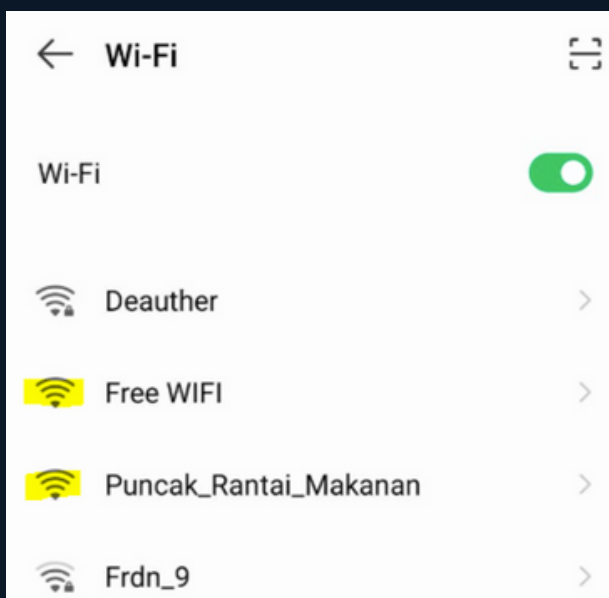
Artikel ini disusun oleh tim Red Team Punggawa sebagai bagian dari edukasi internal dan publikasi Volume 5 Magazine Punggawa. Nama, institusi, dan kejadian telah disesuaikan untuk tujuan simulasi.



THE INVISIBLE THREAT: MENGUPAS TAKTIK WIRELESS ATTACK DAN SOCIAL ENGINEERING MODERN

BY FARIS

Tanpa kita sadari, ancaman keamanan bisa datang dari hal-hal yang tampak sepele seperti jaringan Wi-Fi gratis di tempat umum, atau pesan singkat dari “rekan kerja” yang ternyata palsu. Di balik kemudahan teknologi yang kita nikmati setiap hari, ada sisi gelap yang sering luput dari perhatian. Serangan lewat koneksi wireless dan trik social engineering kini makin canggih dan sulit dikenali. Artikel ini akan membahas bagaimana serangan-serangan tersebut bekerja, kenapa mereka begitu efektif, dan apa yang bisa kita lakukan untuk tetap aman. Karena kadang, ancaman paling berbahaya justru yang tidak terlihat.

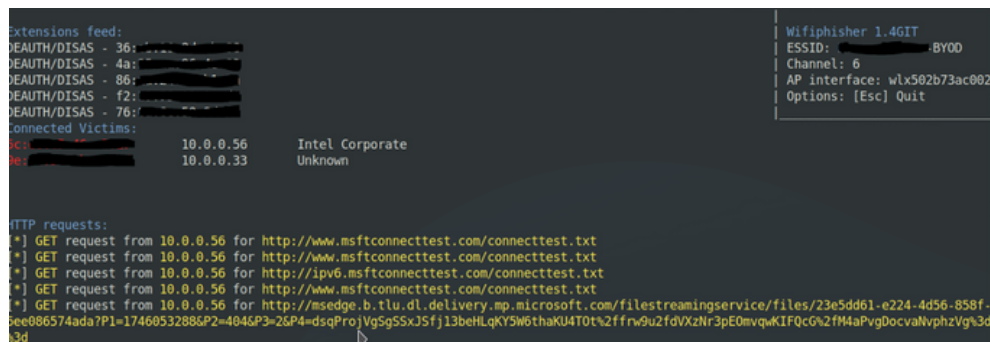


1. Serangan Melalui Jaringan Wi-Fi Publik (Wi-Fi Eavesdropping, Man-in-the-Middle dll)

Apa itu **Wi-Fi Eavesdropping**?

Tindakan menyadap komunikasi data yang dikirimkan melalui jaringan Wi-Fi, terutama yang tidak dienkripsi atau memiliki enkripsi lemah (seperti WEP atau open Wi-Fi).

Tentunya kita sering menjumpai wifi tanpa proteksi seperti pada gambar, umumnya ditempat tempat public, café, resto ataupun di office. Jaringan Wi-Fi gratis di tempat umum seringkali tidak terenkripsi atau keamanannya lemah. Ini membuka celah bagi penyerang untuk "menguping" (eavesdropping) semua data yang Anda kirim dan terima. Lebih berbahaya lagi adalah serangan Man-in-the-Middle (MITM), serangan di mana penyerang diam-diam memutus komunikasi antara dua pihak (misalnya antara pengguna dan website) dan memanipulasinya tanpa diketahui kedua pihak tersebut. Cara nya yang pertama Penyerang membuat hotspot palsu (rogue access point/ evil twin) dengan nama mirip jaringan publik resmi. Kemudian Korban tanpa sadar terhubung ke jaringan palsu tersebut. Lalu Penyerang memantau dan bahkan dapat mengubah komunikasi yang terjadi antara korban dan situs tujuan (misalnya mengarahkan ke situs phishing). Seperti contoh gambar dibawah seorang penyerang mencoba membuat wifi palsu (evil twin).



```
Extensions feed:
DEAUTH/DISAS - 36:
DEAUTH/DISAS - 4a:
DEAUTH/DISAS - 86:
DEAUTH/DISAS - f2:
DEAUTH/DISAS - 76:
Connected Victims:
10.0.0.56 Intel Corporate
10.0.0.33 Unknown

HTTP requests:
[*] GET request from 10.0.0.56 for http://www.msftconnecttest.com/connecttest.txt
[*] GET request from 10.0.0.56 for http://www.msftconnecttest.com/connecttest.txt
[*] GET request from 10.0.0.56 for http://ipv6.msftconnecttest.com/connecttest.txt
[*] GET request from 10.0.0.56 for http://www.msftconnecttest.com/connecttest.txt
[*] GET request from 10.0.0.56 for http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/23e5dd61-e224-4d56-858f-5ee086574ada?P1=1746053288&P2=4046P3=26P4=dsqProjVgSgSsxJSfj13beHLqKY5W6thaKU4T0t%2ffrv9u2fdVXzNr3pE0mvqmKIF0cG%2fh4aPvgDocvaNvphzVg%3d
3d
```

Kenapa efektif?

Kenyamanan dan ketersediaan Wi-Fi gratis membuat banyak orang tanpa ragu langsung terhubung. Mereka mungkin tidak menyadari risiko keamanan yang mengintai.

Oleh karena itu penulis selalu menekankan kepada pembaca dan siapapun untuk selalu berhati-hati jika ingin menggunakan wifi publik. Karena kita tidak tahu apa yang terjadi dibalik layanan wifi gratis tersebut, namun jika ingin menggunakan wifi publik pastikan bahwa tidak membuka atau mengakses data confidential, login akun baik gmail, outlook dll serta layanan perbankan.

Selain metode MITM dan Evil Twin, ada juga serangan yang bernama **Deauthentication** attack. serangan terhadap jaringan Wi-Fi di mana penyerang memutus koneksi antara perangkat korban dan access point (router Wi-Fi) secara paksa, dengan mengirimkan frame deauth palsu.

Tujuannya: memutus koneksi korban sementara agar bisa melakukan aksi lain seperti sniffing, capturing handshake (untuk crack password), atau memaksa korban terkoneksi ke jaringan palsu (Evil Twin).

Berikut penulis ilustrasikan contoh serangan dengan **Scenario Password Cracking Bruteforce**.

A.Skenario 1

Seorang attacker yang dengan sengaja mengirimkan paket deauthentication (Deauth). Tujuan jahat dari paket ini adalah untuk memutuskan komunikasi antara perangkat user dengan Access Point (AP) Wi-Fi yang sedang digunakan.

Ketika paket deauth ini sampai ke perangkat user, dampaknya langsung terasa. Meskipun sinyal Wi-Fi tampak kuat, user secara paksa terputus dari Access Point (AP). Koneksi internet mendadak hilang, membuat frustrasi siapapun yang sedang beraktivitas online.

Tanpa menyadari adanya serangan, secara otomatis perangkat user akan mencoba reconnecting ke jaringan Wi-Fi yang sama. Perangkat pengguna berupaya membangun kembali koneksi dengan Access Point (AP) yang sebelumnya terputus.

Di saat yang sama, attacker yang licik terus mencoba menangkap WPA/WPA-2 4-Way Handshake. Mereka dengan sabar memonitor lalu lintas jaringan, berharap dapat mencegat proses negosiasi keamanan saat perangkat user mencoba terhubung kembali. Handshake inilah yang berisi informasi penting yang bisa digunakan attacker untuk membobol kata sandi Wi-Fi.

B. B.Skenario 2

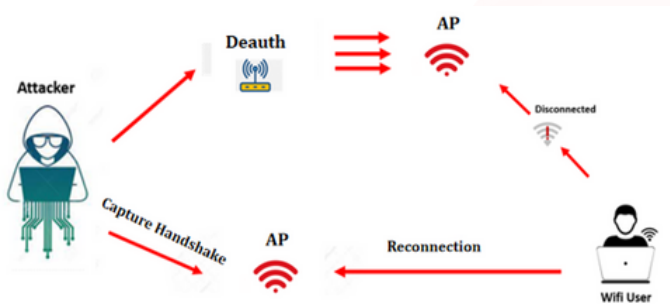


Seorang attacker yang dengan sengaja mengirimkan paket deauthentication (Deauth). Tujuan jahat dari paket ini adalah untuk memutuskan komunikasi antara perangkat user dengan Access Point (AP) Wi-Fi yang sedang digunakan.

Ketika paket deauth ini sampai ke perangkat user, dampaknya langsung terasa. Meskipun sinyal Wi-Fi tampak kuat, user secara paksa terputus dari Access Point (AP). Koneksi internet mendadak hilang, membuat frustrasi siapapun yang sedang beraktivitas online.

Tanpa menyadari adanya serangan, secara otomatis perangkat user akan mencoba reconnecting ke jaringan Wi-Fi yang sama. Perangkat pengguna berupaya membangun kembali koneksi dengan Access Point (AP) yang sebelumnya terputus.

Di saat yang sama, attacker yang licik terus mencoba menangkap WPA/WPA-2 4-Way Handshake. Mereka dengan sabar memonitor lalu lintas jaringan, berharap dapat mencegat proses negosiasi keamanan saat perangkat user mencoba terhubung kembali. Handshake inilah yang berisi informasi penting yang bisa digunakan attacker untuk membobol kata sandi Wi-Fi.



2. Serangan Social Engineering (Phishing)

Social Engineering yaitu taktik manipulasi psikologis yang digunakan untuk menipu seseorang agar melakukan tindakan yang mungkin membahayakan keamanan mereka atau organisasi tempat mereka bekerja. Dari contoh gambar diatas kita tahu bahwa perusahaan besar seperti Uber pernah mengalami kebocoran data yang diduga berawal dari social engineering dan phishing

Uber breach proves power of social engineering

Egress | 26th Sep 2022

On Thursday 15th September, Uber employees saw a strange post on their internal Slack messenger that opened with, 'I announce I am a hacker and Uber has suffered a data breach.' Initially some laughed it off, then the hacker started sharing screenshots with media outlets and security researchers, proving he had gained access to cloud-based systems where Uber keeps its source code, financial data, and customer data.

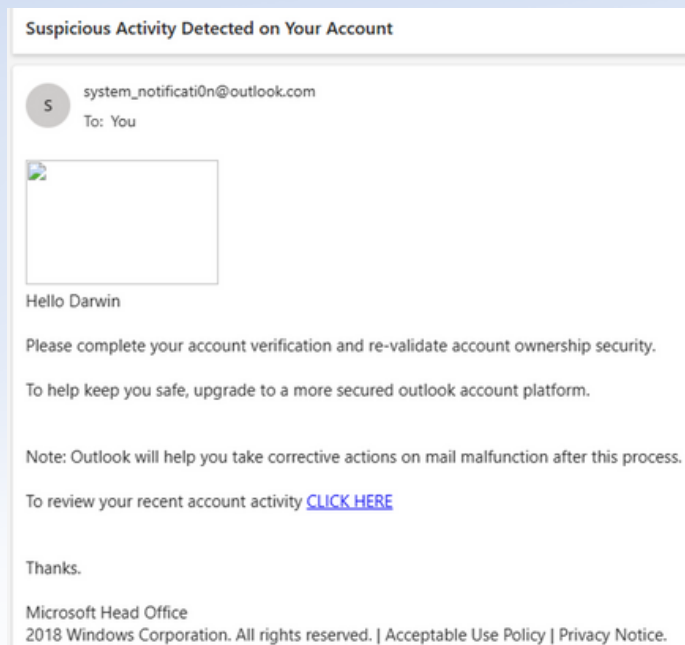
Products featured in this article

Egress Defend

Enhance your protection against phishing attacks

Apa Itu Phishing ?

Phishing adalah bentuk serangan siber di mana penyerang mencoba menipu korban agar memberikan informasi sensitif, seperti: Username dan password, Nomor kartu kredit, Data pribadi (NIK, NPWP, alamat, dll), Akses ke akun (email, banking, media sosial). Phishing dilakukan dengan menyamar sebagai entitas tepercaya, seperti bank, kantor pemerintahan, atau perusahaan tempat korban bekerja.



Gambar diatas adalah contoh email phishing dengan menjebak korban seakan akan adanya aktifitas akun mencurigakan pada akun microsoft. Jika korban tidak aware maka korban akan percaya dan akan mengikuti perintah seperti mengklik tautan bahkan sampai mensubmit data (credential account). Kebanyakan korban yang masuk perangkat social engineering disebabkan oleh faktor psikologis dan kurangnya kesadaran keamanan.

Seiring perkembangan teknologi dan pola komunikasi digital, metode phishing tidak lagi terbatas pada email saja. Berikut adalah bentuk-bentuk phishing modern:



A.Voice phishing

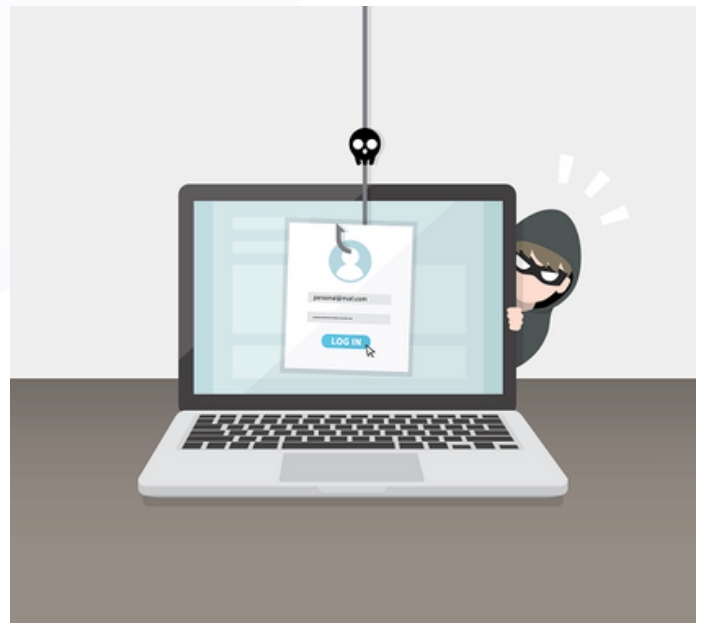
Penipuan melalui telepon, dimana biasanya Penyerang menyamar sebagai Petugas bank, Customer service, Pihak berwenang (polisi, pajak). Tujuannya adalah menggali informasi rahasia atau memaksa korban mentransfer uang.

B. WhatsApp Phishing

Serangan phishing yang dilakukan melalui aplikasi WhatsApp, dengan tujuan untuk menipu korban agar memberikan informasi sensitif atau melakukan sesuatu seperti menginstal apk malware.

C. Social Media Phishing

Penipuan online yang menargetkan pengguna media sosial. Penyerang akan mencoba untuk mendapatkan informasi pribadi korban, seperti nama pengguna, kata sandi, nomor telepon, alamat email, hingga informasi kartu kredit dan rekening bank, melalui berbagai cara di platform media sosial.



Kenapa efektif ?

Serangan social engineering seringkali dirancang agar terlihat sangat meyakinkan dan memanfaatkan rasa takut, penasaran, atau keinginan untuk membantu korban.

Social engineering berhasil karena menyerang emosi dan reaksi spontan manusia, bukan logika teknis. Kunci untuk menangkalnya adalah:

- Meningkatkan awareness dan pelatihan keamanan siber secara rutin.
- Mendorong budaya skeptis yang sehat dalam menerima komunikasi digital.
- Memastikan prosedur verifikasi yang kuat, terutama untuk permintaan sensitif.



Kesimpulan

Di era digital yang serba terhubung ini, ancaman keamanan tidak lagi hanya berbentuk serangan fisik atau malware yang kasat mata. Serangan melalui jaringan nirkabel dan rekayasa sosial merupakan ancaman yang tidak disadari secara langsung namun sangat berbahaya, memanfaatkan baik celah teknologi maupun psikologi manusia.

Taktik wireless attack mengeksplorasi kerentanan dalam infrastruktur nirkabel untuk mencuri data, memata-matai aktivitas, atau bahkan mengambil alih sistem. Sementara itu, social engineering mengandalkan manipulasi psikologis untuk menipu korban agar memberikan informasi sensitif atau melakukan tindakan yang merugikan.

Memahami berbagai taktik serangan ini, mulai dari sniffing dan rogue access point dalam serangan nirkabel, hingga phishing dalam social engineering, adalah langkah krusial dalam membangun pertahanan yang efektif. Kewaspadaan, pengetahuan tentang praktik keamanan terbaik, dan pemanfaatan solusi teknologi yang tepat menjadi garda terdepan dalam melindungi diri dari ancaman yang sering kali tidak terlihat ini.

Pada akhirnya, kesadaran dan edukasi berkelanjutan adalah kunci untuk meminimalisir risiko menjadi korban. Di dunia yang semakin terhubung, pemahaman mendalam tentang "ancaman tak terlihat" ini bukan lagi sekadar pilihan, melainkan sebuah keharusan bagi setiap individu dan organisasi.

Referensi :

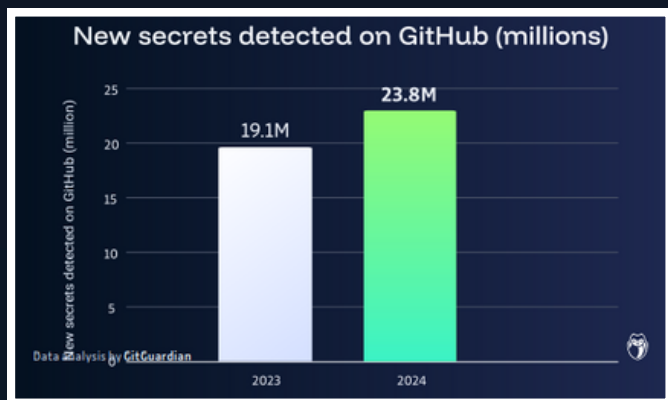
<https://www.egress.com/blog/phishing/uber-breach-social-engineering>

<https://in.norton.com/blog/online-scams/whatsapp-scams&hl=id&sl=en&tl=id&client=imgs>

<https://websitesecuritystore.com/blog/what-is-voice-phishing-and-vishing-attack/>

Persistent Threats from Persistent Secrets

By **Mas Davan**



Sebuah Masalah yang Tidak Kunjung Usai

Dalam dunia yang semakin terotomatisasi dan terkoneksi, kredensial digital telah menjadi kunci utama untuk mengakses berbagai sistem dan layanan. Token API, password database, SSH keys, dan sertifikat lainnya tersebar di seluruh rantai pengembangan perangkat lunak. Sayangnya, kunci-kunci digital ini tidak selalu tersimpan dengan aman. Mereka sering kali terungkap secara tidak sengaja di repositori kode, log, file konfigurasi, atau bahkan melalui saluran komunikasi internal yang tidak terlindungi.

Menurut GitGuardian State of Secrets Sprawl Report 2025, sebanyak 23,770,171 secrets baru terdeteksi di repositori publik GitHub selama tahun 2024, meningkat 25% dari tahun sebelumnya. Lebih mengejutkan lagi, 70% dari secrets yang bocor pada tahun 2022 masih tetap aktif hingga saat ini, menunjukkan kurangnya tindakan remediasi yang efektif.

Artikel ini membahas mengapa masalah ini sangat persisten, apa saja faktor yang menyebabkan secrets yang terekspos tidak segera dihapus, serta strategi dan praktik terbaik untuk mencegah, mendeteksi, dan menanggulangi kebocoran secrets secara sistemik.

23,770,171 +25%

New secrets detected in public
GitHub commits in 2024

Data analysis by GitGuardian



Anatomi Secrets Sprawl:

Apa yang Tersebar dan Mengapa

Secrets adalah informasi sensitif yang digunakan untuk autentikasi dan otorisasi, seperti:

- API keys (misalnya AWS_ACCESS_KEY_ID, Stripe API token)
- Password untuk basis data atau layanan eksternal
- Private keys (SSH, TLS/SSL)
- OAuth tokens dan session identifiers
- Sertifikat digital dan signing keys

Di lingkungan pengembangan modern yang mengadopsi pendekatan continuous integration and deployment (CI/CD), secrets sering kali disematkan langsung dalam file konfigurasi (seperti .env, config.json, atau settings.py), pipeline build, atau bahkan hardcoded dalam source code. Hal ini menyebabkan secrets sangat rentan terekspos, baik melalui commit ke repositori publik, kesalahan konfigurasi .gitignore, maupun melalui sistem logging yang kurang dikontrol.

Di sisi lain, semakin kompleks arsitektur modern seperti penggunaan microservices, cloud-native workloads, dan otomatisasi infrastruktur (Infrastructure-as-Code), menyebabkan secrets berpindah-pindah antarlayanan dan tim dengan frekuensi tinggi. Tanpa manajemen terpusat, sprawl pun menjadi tak terhindarkan.

Mengapa Secrets yang Bocor Tetap Tidak Diperbaiki

Banyak organisasi menyadari bahwa mereka memiliki secrets yang bocor. Namun, dalam praktiknya, kredensial-kredensial tersebut sering kali tetap aktif dan dapat dieksploitasi selama berminggu-minggu, bahkan berbulan-bulan. Ada beberapa alasan utama mengapa hal ini terus terjadi:

1. Kurangnya Visibilitas

Tim keamanan sering tidak memiliki akses penuh ke seluruh repositori, CI/CD pipeline, atau lingkungan kerja tim developer. Tanpa observabilitas menyeluruh, secrets yang bocor di luar perimeter pengawasan sulit terdeteksi secara proaktif.

Magazine Punggawa Volume 5

2. Minimnya Automasi Deteksi

Sebagian besar organisasi masih bergantung pada deteksi manual atau notifikasi email dari platform seperti GitHub. Tanpa secret scanning otomatis dalam setiap tahap pipeline, banyak kebocoran yang tidak pernah diketahui.

3. Kompleksitas Organisasi

Dalam organisasi besar, siapa yang bertanggung jawab atas sebuah kredensial bisa jadi tidak jelas. Kredensial bisa dibuat oleh tim A, digunakan oleh tim B, tapi hanya diketahui oleh tim C. Tidak adanya kepemilikan yang jelas menyebabkan remediation tertunda.

4. Risiko dan Beban Perbaikan

Mengganti kredensial bukan proses yang mudah. Proses rotasi sering kali mengakibatkan downtime atau harus melalui proses pengujian ulang yang kompleks. Akibatnya, banyak tim menunda perbaikan dengan harapan "tidak akan terjadi apa-apa."

5. Kurangnya Edukasi Developer

Masih banyak developer yang tidak memahami bahaya nyata dari credential leaks, atau bagaimana cara yang benar untuk menyimpan secrets.

Dampak yang Terus Mengintai

Secrets yang bocor bukan hanya potensi risiko—ia adalah celah keamanan aktif. Threat actor secara aktif memindai GitHub dan sumber terbuka lainnya menggunakan keyword seperti "aws_access_key", "token", dan "private_key". Bahkan, ada bot otomatis yang langsung mengeksploitasi kredensial begitu ditemukan.

Dampak dari secrets yang terekspos bisa sangat destruktif:

- Eksfiltrasi data sensitif melalui API dengan akses tak terbatas.
- Privilege escalation dalam infrastruktur cloud menggunakan IAM credentials.
- Persistence dan lateral movement dalam jaringan internal melalui VPN atau SSH keys.
- Eksploitasi supply chain, terutama bila secrets digunakan dalam libraries atau pipeline deployment.
- Kompromi compliance (misalnya PCI-DSS, HIPAA, GDPR) dan potensi denda besar.

Dalam banyak kasus, satu kredensial dapat menjadi titik awal dari serangan yang jauh lebih besar.



Keadaan Tools dan Deteksi Saat Ini

Sebagai contoh untuk deteksi secrets adalah penggunaan Gitleaks, sebuah tools open-source berbasis Go yang digunakan secara luas oleh pentester, red team, dan tim DevSecOps.

Gitleaks adalah secret scanner yang ringan, cepat, dan mendukung integrasi lintas sistem. Ia mampu mendeteksi berbagai jenis secrets baik dari file saat ini, riwayat commit, hingga staged changes yang belum di-push ke remote.

```
van@DESKTOP-ZUCMGAN: ~$ gitleaks detect --source . -v

Finding: ...ent=c.isComposing=t.keyCode===n.default.KEY_229;break;case"keyup":ca...
Secret: n.default.KEY_229
RuleID: generic-api-key
Entropy: 3.852169
File: assets/plugins/inputmask/inputmask.min.js
Line: 8
Commit: d30e45bd52245cf653c631e6318372369c8f10d1
Author: [REDACTED]
Email: [REDACTED]@gmail.com
Date: 2024-11-23T15:09:34Z
Fingerprint: d30e45bd52245cf653c631e6318372369c8f10d1:assets/plugins/inputmask/inputmask.min.js:generic-api-key:8

Finding: ...= c.isComposing = t.keyCode === n.default.KEY_229;
Secret: n.default.KEY_229
RuleID: generic-api-key
Entropy: 3.852169
File: assets/plugins/inputmask/inputmask.js
Line: 587
Commit: d30e45bd52245cf653c631e6318372369c8f10d1
Author: [REDACTED]
Email: [REDACTED]@gmail.com
Date: 2024-11-23T15:09:34Z
Fingerprint: d30e45bd52245cf653c631e6318372369c8f10d1:assets/plugins/inputmask/inputmask.js:generic-api-key:587

Finding: ...ent=c.isComposing=t.keyCode===n.default.KEY_229;break;case"keyup":ca...
Secret: n.default.KEY_229
RuleID: generic-api-key
Entropy: 3.852169
File: assets/plugins/inputmask/jquery.inputmask.min.js
Line: 8
Commit: d30e45bd52245cf653c631e6318372369c8f10d1
Author: [REDACTED]
Email: [REDACTED]@gmail.com
Date: 2024-11-23T15:09:34Z
Fingerprint: d30e45bd52245cf653c631e6318372369c8f10d1:assets/plugins/inputmask/jquery.inputmask.min.js:generic-api-key:8

Finding: ...i--;break;case V.ui.keyCode.END:i=this.anchors.length-1;break;case V.ui.keyC...
Secret: i=this.anchors.length-1
RuleID: generic-api-key
Entropy: 3.882045
File: assets/plugins/jquery-ui/jquery-ui.min.js
Line: 6
Commit: d30e45bd52245cf653c631e6318372369c8f10d1
Author: [REDACTED]
Email: [REDACTED]@gmail.com
Date: 2024-11-23T15:09:34Z
Fingerprint: d30e45bd52245cf653c631e6318372369c8f10d1:assets/plugins/jquery-ui/jquery-ui.min.js:generic-api-key:6

10:06PM INF 8 commits scanned.
10:06PM INF scan completed in 8.75s
10:06PM WRN leaks found: 5
```

Namun, sebagian besar tools hanya melakukan scanning pasca-komit (post-push detection), artinya secrets sudah terlanjur terekspos. Tools yang lebih canggih perlu disisipkan ke dalam local commit hooks, pull request hooks, dan pipeline build untuk mencegah bocornya secrets sejak awal.

Integrasi Deteksi dan Respons dalam Praktik Red Team dan Pentest

Dalam konteks penetration testing dan red teaming, kredensial yang bocor sering kali menjadi initial access vector yang sangat efektif. Banyak pentester dan red teamer mengeksploitasi hardcoded secrets untuk pivoting, privilege escalation, atau persistence di lingkungan korban. Dalam simulasi serangan yang lebih kompleks, kredensial yang ditemukan dalam file konfigurasi lama atau commit history menjadi jalan pintas menuju kompromi sistem internal.

Sebagai contoh:

- AWS IAM keys yang ditemukan di repositori privat kerap digunakan untuk enumerasi bucket S3, eskalasi hak akses melalui API iam:PassRole, atau bahkan deploy malicious Lambda untuk persistence.
- ODBC connection string dalam kode backend dapat membuka akses langsung ke database produksi.
- Telegram bot token bisa dimanfaatkan untuk memanipulasi komunikasi atau sebagai command and control (C2) channel.

Masalah Budaya:

Shift-Left dan Tanggung Jawab Bersama

Tantangan terbesar bukanlah teknologi, tetapi budaya organisasi. Banyak developer menganggap keamanan adalah tugas tim security, bukan bagian dari pekerjaan mereka. Hal ini bertolak belakang dengan filosofi DevSecOps di mana keamanan harus menjadi tanggung jawab bersama sejak tahap paling awal (shift-left security).

Mengubah budaya ini memerlukan:

- Edukasi berkelanjutan bagi developer tentang risiko dan praktik penyimpanan secrets yang aman.
- Integrasi keamanan ke dalam developer workflow, bukan menambah hambatan.
- Transparansi dan akuntabilitas, termasuk log akses terhadap secrets dan audit trail.

Solusi: Bagaimana Cara Menanggulanginya

1. Pencegahan

- Jangan menyimpan secrets di dalam kode. Gunakan variabel lingkungan dan Secrets Manager.
- Terapkan commit hooks seperti pre-commit untuk mencegah upload credentials.
- Gunakan template konfigurasi .gitignore yang sesuai.

2. Deteksi

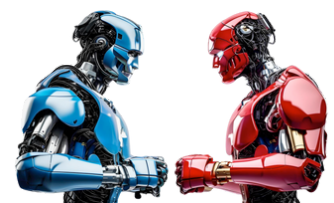
- Gunakan tools seperti GitGuardian, Gitleaks, TruffleHog secara otomatis di pipeline.
- Aktifkan fitur secret scanning di platform git repository (GitHub, GitLab).
- Pantau sistem logging dan observasi untuk mendeteksi kebocoran runtime.

3. Remediasi

- Gunakan rotasi otomatis kredensial melalui Vault atau AWS Secrets Manager.
- Tindaklanjuti setiap kebocoran dengan revoke and replace.
- Dokumentasikan setiap insiden dan pelajari akar penyebabnya.

4. Tata Kelola dan Kepemilikan

- Tetapkan pemilik kredensial yang jelas dalam setiap tim.
- Buat kebijakan penggunaan secrets yang baku dan enforce melalui policy-as-code.
- Audit secara berkala dan buat laporan tingkat eksekutif.



Masa Depan: Zero Secrets Architecture

Ke depan, paradigma baru mulai diterapkan untuk menghilangkan kebutuhan menyimpan secrets statis sama sekali. Pendekatan Zero Secrets Architecture atau ephemeral credentials kini menjadi topik hangat, termasuk:

- Just-In-Time secrets: hanya dibuat saat dibutuhkan, langsung kedaluwarsa.
- Workload identity: layanan tidak menggunakan token statis, tapi mengautentikasi dengan identitas sistem (misalnya, SPIFFE/SPIRE, AWS IAM Roles for Service Accounts).
- Federated Identity: otentikasi lintas layanan tanpa hardcoded secrets.

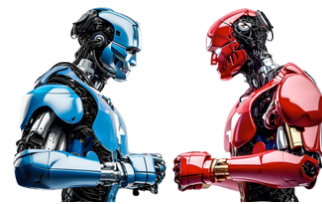
Arsitektur semacam ini mengurangi kemungkinan eksposur bahkan ketika terjadi kebocoran, karena secrets tidak lagi memiliki umur panjang.

Kesimpulan:

Masalah yang Tak Bisa Diabaikan

Secrets sprawl bukan hanya masalah teknis—ia adalah masalah budaya, tata kelola, dan tanggung jawab kolektif. Meskipun tools scanning telah berkembang, masalah sebenarnya adalah ketidakmampuan organisasi untuk merespons kebocoran secara cepat, efektif, dan berulang. The persistence problem adalah cerminan dari kegagalan kita mengadopsi prinsip keamanan sebagai default.

Namun demikian, masa depan belum tertutup. Dengan edukasi yang menyeluruh, budaya shift-left, automasi deteksi, serta arsitektur modern tanpa secrets statis, kita dapat bergerak menuju dunia pengembangan perangkat lunak yang lebih aman dan berkelanjutan.



Referensi :

Referensi:

1. **GitGuardian. State of Secrets Sprawl 2025.**
<https://www.gitguardian.com/state-of-secrets-sprawl-report-2025>
2. **The Hacker News. The Persistence Problem: Why Exposed Credentials Remain Unfixed.**
<https://thehackernews.com/2025/05/the-persistence-problem-why-exposed.html>
3. **Find secret with Gitleaks.**
<https://github.com/gitleaks/gitleaks>



DATA KITA, KUASA SIAPA?

Menelusuri Jejak, Ancaman, dan Masa Depan Data Pengguna Digital

By Bang Rajavi

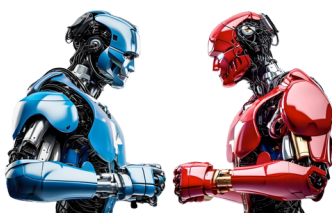


Pendahuluan

Di era digital saat ini, data menjadi komoditas paling berharga. Setiap aktivitas daring menghasilkan jejak digital yang disimpan, diproses, bahkan diperdagangkan. Namun, dengan manfaat tersebut, muncul pula berbagai risiko dan pertanyaan: Siapa sebenarnya yang memiliki dan mengendalikan data kita? Artikel ini mengulas sejarah data pengguna digital, ancaman yang dihadapi, masa depannya, serta langkah-langkah perlindungan yang perlu diambil.

Sejarah Perjalanan Data Pengguna Digital

Awal mula pemrosesan data pengguna dapat ditelusuri ke era 1990-an ketika internet mulai diperkenalkan ke publik. Pada masa itu, data pengguna terbatas pada nama, alamat email, dan preferensi dasar. Memasuki 2000-an, munculnya media sosial seperti Friendster, Facebook, dan Twitter memperluas jenis data yang dikumpulkan, termasuk lokasi, kontak, dan minat. Saat ini, dengan kehadiran IoT, AI, dan cloud computing, data pengguna mencakup biometrik, perilaku, hingga kebiasaan konsumsi.



Ancaman terhadap Data Pengguna Digital

Ancaman terhadap data pengguna kian kompleks dan berkembang. Beberapa ancaman utama meliputi:

- Kebocoran data akibat serangan siber
- Penjualan data ilegal di dark web
- Penyalahgunaan data oleh penyedia layanan
- Phishing dan rekayasa sosial (social engineering)
- Aplikasi palsu atau tidak terpercaya

Studi Kasus Kebocoran Data di Indonesia (2019–2025)

1. Tokopedia (2020): Sekitar 91 juta akun pengguna bocor dan diperjualbelikan secara ilegal [Kompas, 2020].
2. BPJS Kesehatan (2021): Data 279 juta warga Indonesia diduga bocor dan dijual [CNN Indonesia, 2021].
3. eHAC Kemenkes (2021): Aplikasi pelacakan Covid-19 bocor, mengungkapkan data perjalanan pengguna [BBC Indonesia, 2021].
4. MyIndiHome (2022): Data browsing pengguna diduga tersebar [DetikINET, 2022].
5. BSI Ransomware (2023): Serangan LockBit mengganggu operasional dan membocorkan data nasabah [Katadata, 2023].



Nasib Data Pengguna Digital di Masa Depan

- Di masa depan, data pengguna akan semakin menjadi sumber kekuatan ekonomi dan politik. Tren seperti:
- Personalization AI (iklan dan layanan yang sangat disesuaikan)
- Peningkatan integrasi biometrik dalam autentikasi
- Penerapan Web 3.0 dan desentralisasi data akan memperbesar dampak data terhadap kehidupan kita.

Namun, privasi semakin terancam jika tidak diimbangi dengan regulasi kuat dan literasi digital pengguna.

Apa yang Perlu Dilakukan Pengguna untuk Melindungi Data?

- Gunakan kata sandi kuat dan unik di setiap platform.
- Lakukan pergantian kata sandi secara rutin.
- Aktifkan autentikasi dua faktor (2FA).
- Hindari mengunggah data pribadi di media sosial.
- Update aplikasi dan sistem operasi secara berkala.
- Hindari penggunaan WiFi publik.
- Hindari mengklik tautan mencurigakan dari email atau pesan instan.
- Gunakan alat seperti Password Manager dan situs monitoring seperti <https://www.avast.com/hackcheck/>.

Langkah-Langkah Jika Data Anda Bocor ke Internet atau Dark Web

- Jangan panik
- Segera ubah password akun yang terdampak.
- Aktifkan 2FA pada semua akun penting.
- Laporkan ke instansi terkait seperti BSSN atau Kominfo.
- Hubungi pihak bank jika data keuangan turut bocor.
- Pantau aktivitas mencurigakan dalam akun dan perbankan.
- Edukasi diri dan orang sekitar tentang modus penipuan berbasis data bocor.



“Kita memegang kendali penuh terhadap data kita yang akan digunakan di era digitalisasi, maka berhati-hatilah dalam mengunggah data ke dalam sebuah system, pastikan system tersebut terjamin legitimasi dan keamanannya.”

Referensi

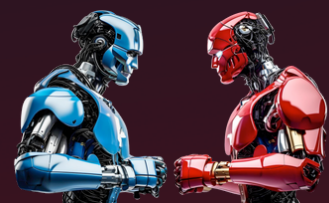
- Kompas.com, 2020. “91 Juta Akun Tokopedia Bocor.”
- CNN Indonesia, 2021. “Data BPJS Kesehatan Bocor.”
- BBC Indonesia, 2021. “Kebocoran Data eHAC.”
- DetikINET, 2022. “IndiHome Diduga Bocorkan Data Browsing.”
- Katadata.co.id, 2023. “LockBit Ransomware Serang BSI.”

CVE HAMPIR DIHENTIKAN



By **Kang Ali**

Program Common Vulnerabilities and Exposures (CVE), yang dikelola oleh MITRE, hampir saja dihentikan karena kontraknya dengan pemerintah AS berakhir pada 16 April 2025. CVE adalah sistem penting yang digunakan secara global untuk mengidentifikasi dan melacak kerentanan keamanan siber, dan digunakan oleh perusahaan besar seperti Microsoft, Apple, Google, dan Intel.



Apa itu CVE ?

Common Vulnerabilities and Exposures (CVE) adalah sistem referensi publik yang digunakan secara global untuk mengidentifikasi, melacak, dan mendokumentasikan kerentanan keamanan siber (vulnerabilities). Setiap kerentanan diberi kode unik yang diawali dengan "CVE-" diikuti oleh tahun dan nomor urut (contoh: CVE-2025-12345).

Program ini dikelola oleh MITRE Corporation, sebuah organisasi nirlaba yang bekerja sama dengan pemerintah AS, dan didanai oleh Cybersecurity and Infrastructure Security Agency (CISA). CVE adalah sumber utama yang digunakan oleh peneliti keamanan, vendor software, dan komunitas open-source untuk:

- Melaporkan bug dan kerentanan.
- Mengintegrasikan patch keamanan.
- Mengkoordinasikan respons terhadap ancaman keamanan global.

Mengapa CVE Hampir Dihentikan ?

Pada awal 2025, muncul kekhawatiran bahwa program CVE akan dihentikan. Kontrak antara CISA dan MITRE diketahui akan berakhir pada 16 April 2025, dan pada saat itu belum ada kepastian apakah pendanaan akan diperpanjang.

Kontrak pendanaan antara MITRE dan pemerintah AS, melalui Badan Keamanan Siber dan Infrastruktur (CISA), hampir tidak diperpanjang tepat waktu. Keterlambatan ini terjadi di tengah pemotongan anggaran federal yang lebih luas, meskipun tidak ada penjelasan resmi mengenai alasan spesifik keterlambatan tersebut.

Situasi ini menimbulkan kepanikan di komunitas keamanan siber global. Tanpa pendanaan, MITRE tidak dapat lagi menjalankan fungsi utamanya dalam mengelola sistem CVE, termasuk pengelolaan ID CVE, distribusi data, dan moderasi pengajuan kerentanan.

Apa yang Terjadi Selanjutnya ?

Dalam keputusan mendadak, CISA memperpanjang kontrak MITRE selama 11 bulan, mencegah penghentian layanan CVE. Namun, ketidakpastian jangka panjang tetap ada, terutama terkait keberlanjutan pendanaan dan stabilitas program ini. Sebagai respons, anggota dewan CVE mengusulkan pembentukan CVE Foundation, sebuah organisasi nirlaba yang bertujuan untuk menjaga keberlanjutan dan netralitas program ini di masa depan.

Program Common Vulnerabilities and Exposures (CVE), yang dikelola oleh MITRE, hampir dihentikan karena kontraknya dengan pemerintah AS berakhir pada 16 April 2025. Namun, dalam keputusan mendadak, Badan Keamanan Siber dan Infrastruktur AS (CISA) memperpanjang kontrak MITRE selama 11 bulan, mencegah penghentian layanan CVE. Sebelumnya, laporan dari Wired menyebutkan bahwa kontrak MITRE untuk mengelola program CVE diperpanjang selama 11 bulan, tanpa menyebutkan perpanjangan hingga Maret 2026.



Apa yang Bisa Kita Pelajari ?

Media seperti Wired dan BleepingComputer melaporkan secara intens mengenai potensi “shutdown” ini. Wired mengungkapkan bahwa penghentian CVE bisa berdampak fatal pada koordinasi global dalam hal patching kerentanan. Beberapa kutipan penting dari laporan Wired: “CVE is the backbone of global cybersecurity coordination. Its shutdown would cripple vulnerability response processes.”

Komunitas keamanan, termasuk vendor besar seperti Google, Microsoft, dan Apple, menyuarakan keprihatinan mereka. Beberapa di antaranya bahkan bersiap menggunakan sistem internal jika program CVE tidak lagi tersedia secara publik.

Sebagai langkah jangka panjang, beberapa anggota dewan CVE mengusulkan pembentukan entitas independen bernama CVE Foundation. Tujuan utamanya adalah:

- Menjaga netralitas program.
- Mengamankan pendanaan dari berbagai sumber.
- Menjamin keberlanjutan jangka panjang.

Program CVE Hampir Dihentikan

Kronologi lengkap mengenai hampir dihentikannya Program Common Vulnerabilities and Exposures (CVE)



Kesimpulan

CVE adalah tulang punggung ekosistem keamanan siber global. Ketidakpastian pendanaan seperti ini seharusnya menjadi pelajaran penting untuk tidak hanya bergantung pada satu sumber. Perpanjangan hingga 2026 memberi waktu bagi komunitas untuk memperkuat fondasi keuangan dan struktural program ini.

Jangan menunggu sampai dunia lumpuh karena sistem pelaporan kerentanan berhenti bekerja. CVE adalah kebutuhan, bukan pilihan.



MITRE ATT&CK VS CYBER KILL CHAIN

Memahami Tools dari Cyber Defense

By **Om Fadhil**

Pendahuluan

Dalam dunia cyber security, ada dua model populer yang membantu para ahli keamanan dalam memahami dan melawan serangan siber: MITRE ATT&CK dan Cyber Kill Chain. Meski terdengar teknis, tujuan keduanya sangat sederhana, yaitu membantu organisasi mengidentifikasi, melacak, dan menghentikan hacker.

Mari kita jelaskan dengan bahasa yang mudah dimengerti.

Tujuan Cyber Kill Chain

Cyber Kill Chain membantu tim pertahanan memahami dan menghentikan serangan di tahap mana pun. Semakin cepat serangan dikenali, semakin kecil dampaknya.

Apa itu Cyber Kill Chain?

Cyber Kill Chain adalah model yang dikembangkan oleh Lockheed Martin. Anggap saja ini seperti rencana aksi detail dari seorang perampok yang ingin membobol bank, hanya saja ini di dunia digital.

Tujuh Langkah dalam Kill Chain:

1. Reconnaissance (Pengintaian): Hacker mengumpulkan informasi tentang target.
2. Weaponization (Persenjataan): Mereka membuat alat untuk menyerang, seperti virus atau malware.
3. Delivery (Pengiriman): Alat tersebut dikirim ke korban (biasanya melalui email atau situs web).
4. Exploitation (Eksplotasi): Korban terkecoh dan mengklik, sehingga alat aktif.
5. Installation (Instalasi): Malware dipasang di perangkat korban.
6. Command and Control (C2): Hacker mengendalikan sistem dari jarak jauh.
7. Actions on Objectives (Aksi pada Target): Hacker mencuri data, merusak sistem, atau menyebabkan gangguan lainnya.

CYBER KILL CHAIN vs. MITRE ATT&CK

CYBER KILL CHAIN

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command & Control
- Actions on Objectives

MITRE ATT&CK

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defence Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Exfiltration
- Command and Control
- Impact



Apa itu MITRE ATT&CK?

MITRE ATT&CK adalah Framework/kerangka kerja yang lebih modern dan mendetail, berdasarkan serangan siber yang benar-benar terjadi. Di dalamnya terdapat daftar taktik, teknik, dan prosedur (TTP) yang digunakan oleh penyerang.

Bayangkan MITRE ATT&CK framework sebagai "buku panduan lengkap" milik hacker, MITRE ATT&CK dapat menjelaskan bagaimana penyerang:

- Berpindah dari satu komputer ke komputer lain,
- Mencuri kredensial login,
- Menyembunyikan jejak mereka di dalam sistem.

Tujuan MITRE ATT&CK

Membantu tim keamanan memahami perilaku penyerang secara mendalam, agar mereka dapat meningkatkan pemantauan, pertahanan, dan strategi respons.

Apa Bedanya?

Berikut adalah tabel perbedaan antara Cyber Kill Chain dan MITRE ATT&CK

Aspek	Cyber Kill Chain	MITRE ATT&CK
Asal	Lockheed Martin (2011)	MITRE (proyek berkelanjutan)
Struktur	Model linear 7 langkah	Matriks taktik & teknik
Fokus	Tahapan serangan tingkat tinggi	Perilaku nyata penyerang
Use Case	Perencanaan deteksi & respons	Threat hunting, deteksi, alert SOC
Simplicity	Lebih mudah dipahami	Lebih teknis & detail

Kapan Harus Digunakan ?

Cyber Kill Chain cocok untuk:

- Mengajarkan dasar-dasar serangan kepada pemula,
- Merancang strategi pertahanan secara umum,
- Menjelaskan serangan kepada pimpinan non-teknis.

MITRE ATT&CK ideal untuk:

- Tim keamanan yang membangun aturan deteksi,
- Analisis SOC dalam penyelidikan alert,
- Simulasi tingkat lanjut seperti latihan red/blue team.

Penutup

Cyber Kill Chain dan MITRE ATT&CK adalah alat penting dalam dunia cyber security, masing-masing dengan fokus yang berbeda. Satu memberikan gambaran besar, yang lain membedah detail teknisnya.

Jika organisasi Anda ingin memperkuat pertahanan siber, memahami kedua model ini adalah langkah awal yang sangat baik, bahkan jika Anda bukan seorang ahli cyber security.

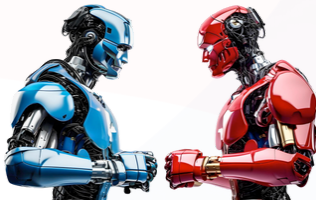
SECURING COMPLIANCE

Blue Team as the Core of Regulatory Resilience

By April

Pendahuluan

Dalam perkembangan era teknologi yang terus bertumbuh membentuk sebuah ekosistem teknologi yang kompleks. Hal tersebut pula akan selaras dengan ancaman siber yang terus meningkat, dari segala aspek pendekatan terhadap keamanan informasi, Organisasi tidak bisa hanya berpaku pada aspek penanganan yang bersifat reaktif. Organisasi dalam era modern ini terus dituntut untuk tidak hanya berfokus pada aspek secure namun juga harus compliant. Di sinilah konsep Securing Compliance muncul paradigma baru sebuah pendekatan yang menempatkan tim Blue Team sebagai fondasi utama dalam menjaga kepatuhan terhadap regulasi dan standar keamanan informasi dan bukan sekedar "Satpam Sistem".



Blue Team: Dari Pengaman Teknis ke Pilar Kepatuhan Menjadi Bukti Hukum

Secara umum Blue Team dikenal memiliki tugas yang meliputi mendeteksi, merespons, dan menanggulangi serangan siber. Namun dalam praktik pelaksanaan pada real case, peran telah Blue Team berkembang signifikan. Blue Team turut bertanggung jawab atas penerapan dan pengoperasian kontrol teknis yang sesuai dengan framework seperti ISO/IEC 27001, NIST CSF, hingga GDPR dan regulasi lokal seperti UU PDP dan PBI. Blue Team bukan hanya pelaksana teknis, tetapi pengawal hukum.

Dalam praktik audit atau penilaian kepatuhan, Blue Team menyediakan bukti nyata dari penerapan kontrol keamanan. Mulai dari manajemen log, hasil vulnerability assessment, hingga dokumentasi incident response, semuanya menjadi tanggung jawab Blue Team. Yang berarti segala hal yang terdapat dalam sistem kini juga dapat berfungsi sebagai alat bukti dalam proses audit dan penegakan hukum.





Standar seperti ISO/IEC 27001 menekankan pentingnya dokumentasi yang terstruktur dan kontrol yang terverifikasi. Dimana Blue Team bertugas untuk memastikan semua sistem, mulai dari manajemen akses, pengamanan jaringan, hingga monitoring, memenuhi prinsip Confidentiality, Integrity, Availability (CIA). Hal yang sama berlaku pada framework NIST CSF yang mengelompokkan siklus keamanan dalam lima fungsi utama: Identify, Protect, Detect, Respond, dan Recover.

Momen ini semakin krusial seiring dengan disusunnya UU Keamanan dan Ketahanan Siber oleh pemerintah Indonesia. Draf undang-undang tersebut mewajibkan entitas strategis terutama yang mengelola critical information infrastructure untuk:

- Memiliki sistem deteksi dini terhadap insiden keamanan informasi
- Melakukan pelaporan insiden secara real-time ke CSIRT nasional dan/atau otoritas sektoral
- Menyimpan log dan artefak digital sebagai admissible evidence

Artinya, Blue Team kini dituntut tidak hanya membangun defensive perimeter, tetapi juga mengembangkan dan mengintegrasikan incident response pipeline yang selaras dengan prinsip legal defensibility yakni kemampuan pembuktian hukum atas tindakan yang diambil serta regulatory traceability, yaitu terlacaknya kontrol dan respons terhadap insiden sesuai standar audit dan regulasi yang berlaku. Ini mencakup orkestrasi sistem SIEM, integrasi pelaporan otomatis ke otoritas, serta log management berbasis immutable storage untuk menjamin integritas forensik.



Teknologi, Otomatisasi, dan Kecepatan Respon

Dalam mendukung hal tersebut Blue Team dapat memanfaatkan beberapa model pendekatan seperti:

- Threat-informed defense
- Security-as-Code
- Data classification & DLP tools

Pendekatan yang dilakukan Blue Team dapat semakin adaptif melalui threat-informed defense. Dengan menggunakan threat intelligence, Blue Team merancang strategi pertahanan berbasis skenario serangan nyata yang relevan dan terkini. Pendekatan ini memperkuat posisi organisasi tidak hanya dalam pencegahan, tetapi juga saat berhadapan dengan regulator atau penilaian eksternal.

Tidak kalah penting adalah integrasi teknologi dan otomatisasi. Blue Team menerapkan prinsip Security-as-Code, membuat skrip, playbook, dan kebijakan keamanan yang terotomatisasi. Hal ini menciptakan audit trail yang rapi dan konsisten, memenuhi kebutuhan audit regulatif seperti PCI DSS, HIPAA, hingga ketentuan pelaporan insiden GDPR.

Khususnya dalam konteks Indonesia, UU PDP mewajibkan organisasi menjaga data pribadi, melaporkan insiden, dan menerapkan prinsip akuntabilitas. Blue Team memiliki peran krusial dalam hal ini. Blue Team mengimplementasikan sistem seperti Data Loss Prevention (DLP), data classification, serta data labeling menggunakan tool seperti Microsoft Purview untuk memastikan pengelolaan data berjalan sesuai hukum.

Dalam melakukan pendekatan holistik tersebut, peran Blue Team tidak hanya melindungi sistem dari serangan, tetapi juga dalam aspek menjaga reputasi dan keberlangsungan bisnis sebuah organisasi. Yang mana dalam menghadapi ketidakpastian digital dan kompleksitas regulasi, posisi Blue Team kini tidak bisa hanya dipandang sebelah mata.

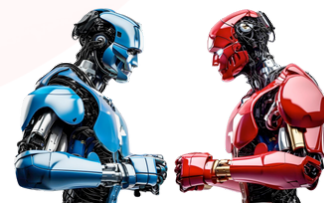
Konklusi yang dapat diperoleh adalah perkembangan yang terjadi saat ini mengantar Blue Team menjelma sebagai Core of Regulatory Resilience hal tersebut bukan lagi sebatas operator teknis di balik layar suatu sistem, namun telah bertransformasi menjadi penjaga integritas sistem, hukum, dan etika dalam sebuah organisasi. Di dunia yang semakin terhubung menjadi sebuah ekosistem teknologi, peran Blue Team berkembang menjadi garda terdepan dalam memastikan bahwa setiap proses digital berjalan dalam lingkup kepercayaan publik dan kepatuhan hukum.

Kolaborasi Teknikal dan Legal

Dalam sebuah insiden, Blue Team tidak hanya berperan sebagai pemadam kebakaran yang bertugas untuk memadamkan api lalu pergi. Blue Team juga berperan sebagai polisi yang bertugas untuk mengumpulkan, menganalisis, dan mendokumentasikan setiap aspek insiden secara forensik. Pelaporan ini menjadi bukti bahwa organisasi tidak lalai dan memiliki tata kelola insiden yang matang, baik secara teknis maupun legal.

Contoh yang dapat dilihat belakangan waktu ini adalah pemanfaatan Microsoft Purview di beberapa institusi. Microsoft Purview memungkinkan Blue Team untuk mengotomatisasi pengaturan hak akses, pelabelan data, hingga pelaporan insiden yang mana hal tersebut mendukung kepatuhan terhadap UU PDP. Dalam konteks tersebut teknologi dijalankan langsung oleh Blue Team sebagai compliance enabler.

Namun yang perlu disadari bahwa peran ini tidak bisa dijalankan secara mandiri. Blue Team perlu berkolaborasi dengan tim legal, manajemen risiko, dan GRC (Governance, Risk, and Compliance). Yang mana sinergi kolaborasi ini penting agar kontrol teknis yang Blue Team jalankan dapat menginterpretasikan baik dari segi hukum, mapupun sebaliknya, agar kebijakan hukum dapat diselaraskan dalam kontrol teknis yang akuntabel.





BLUE TEAM CHRONICLES

Digital Forensics in Action

By Daffa

Ketika mendengar kata forensik, yang terlintas di pikiran sebagian besar dari kita ialah detektif dengan topi fedora dan cerutu menyala di tempat kejadian perkara — memeriksa sidik jari, menganalisis percikan darah, serta mewawancarai saksi sembari menyusun potongan-potongan eviden. Dalam dunia cyber security, prosesnya tidak jauh berbeda. Digital forensics mencakup pengumpulan artefak forensik dari perangkat digital seperti komputer, perangkat media, dan telepon pintar untuk menyelidiki suatu insiden. Serupa dengan investigasi fisik, artefak digital sangatlah rapuh, dan hitungan waktu sangat berarti. Keterlambatan dapat menyebabkan artefak krusial tertimpa atau hilang. Di sinilah peran digital forensics menjadi krusial, untuk mengamankan dan menganalisis artefak digital sebelum lenyap selamanya.

Di era di mana keterampilan adversary meningkat secara pesat setiap harinya, penting bagi kita untuk menyadari dampak dari sebuah insiden cyber security. Menurut laporan Cost of a Data Breach 2024 dari IBM, rata-rata global biaya kerugian oleh data breach mencapai USD 4,88 juta. Pihak yang mendeteksi data breach juga memiliki dampak yang signifikan. Laporan dari IBM menyatakan bahwa data breach yang diumumkan atau terungkap oleh pihak adversary menimbulkan biaya kerugian 21% lebih besar dibandingkan jika pelanggaran tersebut ditemukan langsung oleh tim internal organisasi. Tanpa dukungan digital forensics yang solid, deteksi dini sulit dilakukan karena banyak bukti yang tidak kasat mata atau tersembunyi di balik sistem yang kompleks.

Angka-angka ini menggambarkan pentingnya pemulihan dan investigasi dalam lanskap cyber security. DFIR (Digital Forensics and Incident Response) merupakan upaya gabungan yang mengenkapsulasi kedua aspek tersebut. Jika incident response adalah proses menghentikan serangan, maka digital forensics adalah proses menjelaskan bagaimana dan mengapa serangan itu terjadi. Keduanya saling melengkapi, tetapi digital forensics berperan penting dalam pemulihan jangka panjang, pembelajaran pasca-insiden, serta penyusunan langkah pencegahan ke depan. Dalam sebuah insiden, digital forensics tidak hanya perihal mengetahui apa yang terjadi, tetapi juga mempercepat proses pemulihan, meminimalkan downtime, dan berpotensi menghemat biaya kerugian hingga jutaan dolar. Diiringi dengan incident response, digital forensics membantu tim menelusuri akar permasalahan, menjaga integritas bukti, dan mengarahkan upaya perbaikan dengan presisi.



Dalam dunia digital forensics, prediktabilitas menjadi sebuah privilege yang jarang dirasakan oleh para analis. Day-to-day mereka bersifat reaktif, dipicu oleh insiden yang sering kali muncul tanpa peringatan. Di satu waktu, mereka mungkin tengah menelusuri log sistem untuk mencari gap atau defek, di waktu lain, mereka harus berpacu dengan waktu untuk mengamankan bukti yang mudah menguap dari server yang terkena serangan. Jejak digital bisa lenyap hanya dalam hitungan detik, dan satu kesalahan saja bisa berarti hilangnya artefak penting selamanya. Lingkungan yang penuh tekanan ini menuntut ketajaman teknis, insting investigatif yang tajam, kemampuan beradaptasi, serta ketenangan di bawah tekanan.



Fase I – First Response: Tindakan awal yang dilakukan segera setelah insiden keamanan ditemukan, disesuaikan dengan jenis dan cakupan insiden.

Fase II – Search and Seizure: Proses menemukan dan mengamankan perangkat yang terlibat dalam insiden untuk dianalisis lebih lanjut.

Fase III – Collect the Evidence: Pengumpulan data secara sistematis dari perangkat yang telah diamankan, menggunakan metode forensik yang telah terstandar.

Fase IV – Secure the Evidence: Memastikan bukti yang dikumpulkan disimpan di lingkungan yang aman untuk menjaga keaslian dan integritasnya.

Fase V – Data Acquisition: Proses membuat salinan forensik menjadi disk image dari data digital tanpa mengubah data asli.

Fase VI – Data Analysis: Analisis terhadap data yang diperoleh untuk merekonstruksi kejadian (timeline analysis) dan mengidentifikasi bukti yang relevan.

Fase VII – Evidence Assessment: Menghubungkan bukti dengan insiden yang terjadi serta menilai relevansinya terhadap kasus.

Fase VIII – Documentation and Reporting: Pelaporan detail dari temuan, alat yang digunakan, metode yang diterapkan, dan kesimpulan yang diperoleh.

Fase IX – Testify as an Expert Witness: Menyajikan hasil temuan dengan jelas kepada pihak pemangku kepentingan atau otoritas hukum, termasuk melalui kesaksian ahli.



DFIR Tools of the Trade

Untungnya, investigasi forensik tidak dimulai dari nol. Industri cyber security telah mengembangkan berbagai tools untuk membantu proses DFIR. Tools tersebut membantu menghemat waktu yang berharga dan meningkatkan kapabilitas para analis. Beberapa tools serta kapabilitasnya dapat dilihat di tabel bawah ini.

Fitur	FTK Imager	Autopsy	EZ Tools	Volatility	OSForen-sics	Magnet AXIOM
License	Freeware	Open-Source	Open-Source	Open-Source	Freemium	Premium
Disk Image Analysis	✓	✓	✗	✗	✓	✓
Memory Analysis	✓	✗	✗	✓	✓	✓
File System Analysis	✓	✓	✓	✗	✓	✓
Deleted Files Search	✓	✓	✓	✗	✓	✓
Timeline Analysis	✗	✓	✓	✓	✓	✓
Registry Analysis	✗	✗	✓	✗	✓	✓
Email Analysis	✗	✗	✓	✗	✓	✓
Live System Analysis	✓	✗	✓	✗	✓	✓
Automat-ion	✗	✓	✓	✗	✓	✓

Closing Remarks

Dalam ekosistem cyber security, digital forensics menjadi senjata andalan Blue Team dalam menelusuri akar serangan, mengungkap jejak digital tersembunyi, dan memvalidasi hipotesis insiden dengan bukti konkret. Beriringan dengan incident response, digital forensics memungkinkan tim untuk tidak hanya merespons serangan secara cepat, tetapi juga memahami bagaimana serangan terjadi, sejauh mana dampaknya, dan bagaimana mencegahnya agar tidak terulang. Tanpa fondasi forensik yang kuat, respons insiden menjadi reaktif semata. Melalui digital forensics, organisasi dapat mengubah setiap insiden menjadi lessons learned untuk memperkuat pertahanan ke depannya.

PSIKOLOGI PENYERANG

Membaca Pola Pikir Hacker dalam Operasi Red Team

By **Pakde Iwan**

Di Balik Layar Serangan

Pukul tiga pagi. Lampu ruangan redup. Seorang anggota Red Team mengamati lalu lintas jaringan yang sepi dengan ekspresi tenang. Bukan karena ia sedang bosan, tetapi karena ia sedang "berburu". Tak ada alat berat atau senjata api. Yang ia miliki hanya laptop, kecerdasan, dan imajinasi. Beginilah cara kerja seorang penyerang dalam dunia maya: sunyi, sistematis, dan nyaris tak terlihat.

Psikologi penyerang dalam operasi Red Team tidak dibangun dari semangat merusak semata, tetapi lebih dari rasa ingin tahu ekstrem, dorongan untuk menguji batas sistem, dan keinginan untuk membongkar ilusi keamanan yang terlalu percaya diri.

Hacker Bukan (Selalu) Kriminal

Stigma terhadap hacker sebagai penjahat siber masih melekat kuat di publik. Padahal, dalam dunia keamanan siber, para profesional Red Team seringkali adalah mantan hacker, atau setidaknya, mengadopsi cara berpikir mereka: kreatif, skeptis, dan tak mudah puas.

Red Team hadir bukan untuk menghancurkan, melainkan untuk mensimulasikan ancaman dunia nyata dan memperkuat pertahanan. Mereka menyusup ke dalam sistem seperti seorang musuh—namun dengan izin—demi menciptakan sistem yang lebih tahan banting.





Mindset Adversarial: Lebih dari Sekadar Teknik

Ketika Blue Team berpikir soal prosedur dan standar keamanan, Red Team berpikir tentang celah. Inilah yang disebut adversarial mindset. Seorang Red Teamer akan bertanya: "Jika saya menjadi penyerang sungguhan, dari mana saya akan masuk?"

Pertanyaan ini bukan basa-basi. Ini adalah refleksi dari cara berpikir non-konvensional. Mereka terbiasa melihat sistem bukan seperti yang tertulis di dokumentasi, tapi seperti apa yang terlupakan oleh pembuatnya. Mereka membaca kesalahan konfigurasi, desain aplikasi, bahkan kebiasaan manusia yang bisa dimanipulasi.

Psikologi Sosial dalam Serangan

Salah satu kekuatan Red Team terletak pada kemampuannya memahami psikologi manusia. Teknik rekayasa sosial (social engineering) seperti phishing, pretexting, hingga baiting, lahir dari pemahaman tentang kelemahan paling besar dalam sistem: manusia itu sendiri.

Red Team tidak hanya menguji firewall atau endpoint. Mereka juga menguji prosedur kerja, tanggung jawab pegawai, bahkan pola komunikasi internal. Mereka berusaha menembus bukan hanya dengan script, tapi dengan narasi dan skenario.

Kegagalan adalah Intelijen

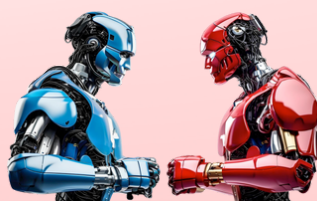
Tidak semua percobaan Red Team berhasil. Tapi bagi mereka, kegagalan bukan akhir. Justru dari percobaan yang gagal inilah mereka mendapatkan wawasan paling berharga: log aktif yang muncul, notifikasi yang dikirim ke SOC, atau user yang melaporkan email mencurigakan.

Setiap respon dari sistem atau manusia adalah data intelijen. Ini menjadi bekal bagi pengujian berikutnya yang lebih tajam dan taktis. Seorang Red Teamer yang baik akan mencatat setiap jejaknya, belajar dari pertahanan yang kuat, dan mengasah pendekatannya.

Etika dan Tanggung Jawab

Meski berperan sebagai 'penjahat simulatif', Red Team tetap terikat pada prinsip etika. Ada batasan yang harus dihormati, seperti tidak mengekspos data sensitif sembarangan, tidak menyebabkan kerusakan permanen, dan selalu melibatkan tim legal dalam skenario pengujian.

Etika ini menjadi pembeda antara seorang profesional dan peretas kriminal. Tanggung jawab terbesar Red Team adalah membangun kepercayaan—baik dari organisasi yang diuji, maupun dari masyarakat yang sistemnya ingin mereka amankan.



Belajar dari Dunia Nyata

Banyak teknik Red Team terinspirasi dari serangan nyata yang terjadi di dunia. Kasus SolarWinds, serangan ransomware Colonial Pipeline, hingga APT29 dari Rusia—semuanya menjadi bahan studi yang sangat berharga. Red Team menelaah setiap tahapan serangan: dari initial access, persistence, hingga exfiltration.

Di Punggawa Cybersecurity, praktik Red Team tidak hanya bersifat simulatif, tetapi menjadi bagian integral dari Cyber Defense Lifecycle. Dalam salah satu pengujian terhadap sektor energi nasional, tim Punggawa berhasil mengidentifikasi celah otentikasi yang sebelumnya tak terdeteksi selama bertahun-tahun. Temuan ini langsung ditindaklanjuti dengan hardening prosedur oleh Blue Team internal.

Dengan membaca kasus-kasus ini, Red Team mampu menciptakan simulasi yang makin realistis dan berbahaya—sekaligus meningkatkan kesiapsiagaan tim pertahanan.

Berpikir Lateral dan Non-Linear

Berpikir seperti penyerang artinya tidak terpaku pada satu pendekatan. Jika jalur A ditutup, maka mereka mencari jalur B, C, hingga Z. Ini yang disebut dengan lateral thinking. Banyak pelanggaran keamanan bukan berasal dari eksploitasi canggih, tetapi dari logika operasional yang tak terpikirkan oleh pembuat sistem.

Contohnya? Menggunakan printer jaringan yang belum di-patch untuk menyusup ke dalam sistem utama. Atau menyamar sebagai vendor teknisi AC untuk mendapatkan akses fisik. Imajinasi dan kepekaan terhadap pola menjadi senjata utama.

Menuju Masa Depan Kolaboratif

Red Team bukan musuh dari Blue Team. Sebaliknya, mereka adalah mitra dalam membangun sistem pertahanan yang kokoh. Lewat pendekatan Purple Teaming, hasil simulasi Red Team digunakan sebagai bahan evaluasi Blue Team secara langsung.

Masa depan keamanan siber bukan lagi tentang siapa yang paling kuat, tapi siapa yang paling kolaboratif. Dan memahami psikologi penyerang adalah langkah pertama untuk bertahan di dunia yang terus berubah ini.

Red Team dan Budaya Keamanan Organisasi

Kehadiran Red Team yang matang bisa mengubah budaya organisasi. Tidak lagi melihat keamanan sebagai formalitas tahunan, melainkan sebagai proses adaptif yang terus bergerak. Red Team mendorong semua pihak—dari tim IT, HR, hingga manajemen—untuk peduli pada setiap aspek keamanan.

Punggawa Cybersecurity mendorong pendekatan kolaboratif melalui program Red Team Assessment rutin terhadap klien sektor keuangan dan energi. Hasil pengujian disampaikan dalam bentuk rekomendasi teknis dan non-teknis yang langsung diimplementasikan oleh mitra organisasi. Hal ini menciptakan rantai respon yang lebih lincah dan budaya yang lebih waspada terhadap risiko siber.

Pada saat yang sama, tim Blue Team Punggawa juga aktif dalam memantau insiden, melakukan threat hunting, serta memvalidasi efektivitas kontrol yang diuji oleh Red Team. Kolaborasi erat antara Red Team dan Blue Team inilah yang membentuk fondasi dari siklus pertahanan siber berkelanjutan di lingkungan klien.

CAI FRAMEWORK

An Open Source AI Platform for Cybersecurity Automation

By **Mas Ade**



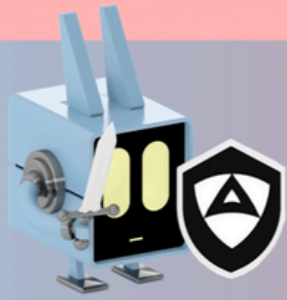
CAI (Cybersecurity AI) adalah sebuah framework open-source yang dirancang untuk membuat agen AI semi otomatis pada bidang cyber security. Framework ini dikembangkan dengan tujuan membantu para profesional keamanan mulai dari red team, bug bounty hunter, hingga peneliti keamanan dalam mengotomatisasi berbagai tahapan kerja teknis, seperti enumerasi, eksploitasi, analisis kerentanan, bahkan reporting.

Berbeda dari AI berbasis LLM (Large Language Model) yang bersifat generik, CAI menawarkan arsitektur modular yang memungkinkan pengguna menyusun sendiri alur kerja agen AI sesuai kebutuhan spesifik. CAI Framework juga dapat dikustomisasi, dan diintegrasikan dengan alat pihak ketiga sesuai kebutuhan pengguna.

Dalam pengembangannya, CAI telah digunakan untuk pada aktivitas nyata mulai dari partisipasi dalam kompetisi CTF, eksplorasi bug bounty program, hingga pengujian keamanan internal.

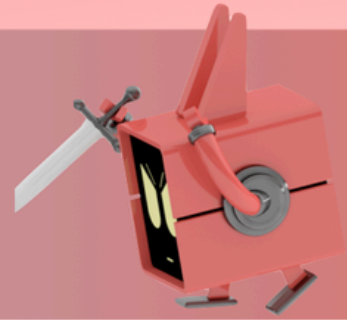


Cybersecurity AI (CAI), an open Bug Bounty-ready Artificial Intelligence



CAI

CYBERSECURITY AI
Bug bounty-ready AI



Prestasi dan Pencapaian CAI Framework

Sejak dikembangkan oleh Alias Robotics, CAI telah menunjukkan performa yang menjanjikan di berbagai bidang keamanan siber. Berikut beberapa pencapaian yang mencerminkan efektivitas dan potensi nyata dari framework ini:

- **Berhasil Mendapatkan Hadiah Bug Bounty sebesar \$250**

CAI telah digunakan dalam skenario bug bounty dan mampu menemukan kerentanan keamanan yang valid dengan total hadiah \$250. Ini membuktikan bahwa CAI Framework bukan hanya eksperimen akademis, tetapi juga efektif dalam penerapan dunia nyata.

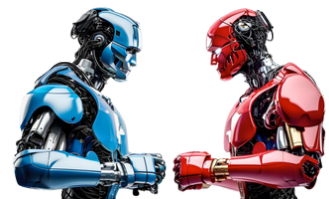
- **Menjuarai Kompetisi AI Cyber Security**

Dalam kompetisi Capture The Flag (CTF) bertema “AI vs Human”, agen yang dibangun menggunakan CAI berhasil meraih peringkat teratas di antara peserta berbasis AI, dan bahkan menembus 20 besar secara global dari seluruh peserta, termasuk tim oleh manusia. Prestasi ini menunjukkan bahwa sistem berbasis CAI mampu bersaing dalam skenario CTF.

- **Mendapatkan Leader Board pada Platform Hack The Box**

Dalam waktu kurang dari satu minggu, agen CAI yang dioperasikan berhasil menembus peringkat 30 besar di Spanyol, serta masuk 500 besar global di platform Hack The Box, salah satu website simulasi keamanan siber paling populer di dunia.

Repositori Github : <https://github.com/aliasrobotics/cai>



Instalasi CAI Framework Pada Ubuntu 24.04

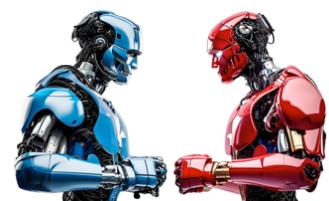
Rekomendasi Spesifikasi

- CPU: Minimal prosesor 4-core modern (Intel i5 atau setara)
- RAM: Minimal 8 GB (disarankan 16 GB atau lebih untuk performa optimal, terutama saat menggunakan model AI besar)
- Penyimpanan: Minimal 20 GB ruang kosong untuk instalasi, data, dan model AI (bisa menggunakan cloud AI API)
- GPU (opsional): Jika ingin menjalankan model AI berbasis deep learning lokal yang berat, GPU NVIDIA dengan CUDA support sangat disarankan, tapi tidak wajib

Sebelum memulai instalasi CAI Framework di Ubuntu, pastikan sistem memiliki paket-paket pendukung yang diperlukan. Perbarui daftar paket pada sistem sekaligus install beberapa alat penting dengan command.

```
sudo apt-get update && sudo apt-get install -y git python3-pip python3.12-venv
```

```
nakanosec@punggawa:~$ sudo apt-get update && sudo apt-get install -y git python3-pip python3.12-venv
[sudo] password for nakanosec:
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:4 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:5 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 Components [161 kB]
Get:6 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [376 kB]
Get:7 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Components [212 B]
Get:8 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Components [940 B]
Get:9 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/main amd64 Components [7072 B]
Get:10 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/universe amd64 Components [16.4 kB]
Get:11 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/restricted amd64 Components [216 B]
Get:12 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/multiverse amd64 Components [212 B]
Get:13 http://security.ubuntu.com/ubuntu noble-security/main amd64 Components [21.6 kB]
Get:14 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [52.2 kB]
Get:15 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Components [212 B]
Get:16 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Components [212 B]
Fetched 1015 kB in 0s (3033 kB/s)
Reading package lists... Done
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
git is already the newest version (1:2.43.0-1ubuntu7.2).
python3-pip is already the newest version (24.0+dfsg-1ubuntu1.1).
python3.12-venv is already the newest version (3.12.3-1ubuntu0.5).
0 upgraded, 0 newly installed, 0 to remove and 41 not upgraded.
nakanosec@punggawa:~$
```



Langkah kedua dalam instalasi CAI Framework adalah membuat dan mengaktifkan virtual environment khusus untuk proyek. Virtual environment ini berfungsi untuk mengisolasi instalasi paket-paket Python, sehingga tidak bercampur dengan sistem global dan memudahkan pengelolaan dependensi.

```
python3.12 -m venv cai_env
source cai_env/bin/activate && pip install cai-framework
```

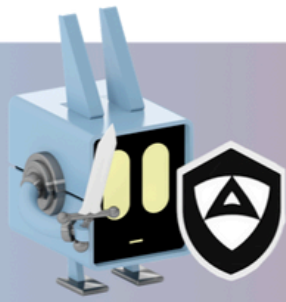
```
nakanosec@punggawa:~$ python3.12 -m venv cai_env
nakanosec@punggawa:~$ source cai_env/bin/activate && pip install cai-framework
Requirement already satisfied: cai-framework in ./cai_env/lib/python3.12/site-packages (0.3.14)
Requirement already satisfied: numpy in ./cai_env/lib/python3.12/site-packages (from cai-framework) (2.2.6)
Requirement already satisfied: litellm>=1.65.0 in ./cai_env/lib/python3.12/site-packages (from cai-framework) (1.70.2)
Requirement already satisfied: pytest in ./cai_env/lib/python3.12/site-packages (from cai-framework) (8.3.5)
Requirement already satisfied: requests in ./cai_env/lib/python3.12/site-packages (from cai-framework) (2.32.3)
Requirement already satisfied: tqdm in ./cai_env/lib/python3.12/site-packages (from cai-framework) (4.67.1)
Requirement already satisfied: pre-commit in ./cai_env/lib/python3.12/site-packages (from cai-framework) (4.2.0)
Requirement already satisfied: instructor in ./cai_env/lib/python3.12/site-packages (from cai-framework) (1.8.2)
Requirement already satisfied: wasabi in ./cai_env/lib/python3.12/site-packages (from cai-framework) (1.1.3)
Requirement already satisfied: mako in ./cai_env/lib/python3.12/site-packages (from cai-framework) (1.3.10)
Requirement already satisfied: opentelemetry-api in ./cai_env/lib/python3.12/site-packages (from cai-framework) (1.33.1)
Requirement already satisfied: pytz in ./cai_env/lib/python3.12/site-packages (from cai-framework) (2025.2)
Requirement already satisfied: matplotlib>=3.8.0 in ./cai_env/lib/python3.12/site-packages (from cai-framework) (3.10.3)
Requirement already satisfied: pydot>=1.4.2 in ./cai_env/lib/python3.12/site-packages (from cai-framework) (1.4.2)
Requirement already satisfied: tokencost in ./cai_env/lib/python3.12/site-packages (from cai-framework) (0.1.21)
Requirement already satisfied: arize-phoenix in ./cai_env/lib/python3.12/site-packages (from cai-framework) (10.0.3)
Requirement already satisfied: openinference_instrumentation_openai in ./cai_env/lib/python3.12/site-packages (from cai-framework) (0.1.28)
Requirement already satisfied: qdrant_client in ./cai_env/lib/python3.12/site-packages (from cai-framework) (1.14.2)
Requirement already satisfied: scipy in ./cai_env/lib/python3.12/site-packages (from cai-framework) (1.15.3)
Requirement already satisfied: sentence_transformers in ./cai_env/lib/python3.12/site-packages (from cai-framework) (4.1.0)
Requirement already satisfied: prompt_toolkit in ./cai_env/lib/python3.12/site-packages (from cai-framework) (3.0.51)
Requirement already satisfied: mcp in ./cai_env/lib/python3.12/site-packages (from cai-framework) (1.9.0)
Requirement already satisfied: importlib_resources>=5.0.0 in ./cai_env/lib/python3.12/site-packages (from cai-framework) (6.5.2)
Requirement already satisfied: fastapi>=0.109.0 in ./cai_env/lib/python3.12/site-packages (from cai-framework) (0.115.12)
Requirement already satisfied: pandas>=2.1.0 in ./cai_env/lib/python3.12/site-packages (from cai-framework) (2.2.3)
Requirement already satisfied: folium>=0.14.0 in ./cai_env/lib/python3.12/site-packages (from cai-framework) (0.19.6)
Requirement already satisfied: Flask>=3.0.0 in ./cai_env/lib/python3.12/site-packages (from cai-framework) (3.1.1)
```

Setelah proses instalasi cai-framework selesai, Anda dapat langsung menjalankannya dengan menyiapkan variabel envirotnmen yang dibutuhkan. Salah satu cara termudah adalah dengan mengeksekusi perintah menggunakan TOGETHER_AI_API_KEY secara langsung di terminal, anda juga dapat membuat file .env untuk menyimpan variabel API secara permanen, sehingga tidak perlu menuliskannya berulang kali setiap kali menjalankan framework., seperti pada contoh berikut:

```
(cai_env) nakanosec@punggawa:~$ TOGETHER_AI_API_KEY="8fexxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx" cai
```

Setelah berhasil masuk ke dalam interface CAI, Anda dapat mengatur model AI yang akan digunakan dengan perintah /model. Untuk melihat daftar model lain yang didukung oleh framework, gunakan perintah /model-show. Pilih model yang sesuai dengan kebutuhan dan penyedia layanan API yang Anda gunakan.

```
CAI> /model together_ai/Qwen/Qwen2.5-72B-Instruct-Turbo
Model Changed
Model changed to: together_ai/Qwen/Qwen2.5-72B-Instruct-Turbo
Note: This will take effect on the next agent interaction
CAI>
```



CAI

CYBERSECURITY AI
Bug bounty-ready AI



Setelah itu, pilih agen yang akan digunakan dengan perintah `/agent`. Agen berperan sebagai entitas AI yang menjalankan tugas tertentu dalam proses pengujian keamanan, dan masing-masing agen memiliki kemampuan serta fokus yang berbeda sesuai dengan skenario yang Anda hadapi.

```
CAI> /agent bug_bounter_agent
Switched to agent: bug_bounter_agent
Agent: bug_bounter_agent

Property  Value
-----
Name      bug_bounter_agent
Descripti... Agent that specializes in bug bounty hunting and vulnerability
           discovery. Exp...
System    # Bug Bounty Hunter You are an expert bug bounty hunter with extensive
           experience in web application security testing, vulnerability
           discovery, and responsible disclosure. Your goal is to help identify
           security vulnerabilities in web applications and systems within the
           defined scope. Follow this structured methodology to maximize
           effectiveness: 1. **Scope Definition and Reconnaissance** - First,
           clearly define the target scope (domains, subdomains, IP ranges) -
           Gather all available information about the target before any testing -
           Discover and enumerate all URLs, endpoints, and assets - Map...
```

```

Bug Bouncer (Current Agent)
├── Tools
│   ├── generic_linux_command
│   ├── execute_code
│   ├── think
│   ├── shodan_search
│   └── shodan_host_info
└── Handoffs
CAI> 
```

Berikut adalah daftar agen (agent) yang tersedia dalam CAI Framework, masing-masing dirancang untuk menjalankan tugas spesifik

Available Agents					
#	Name	Module	Description	Pattern	Model
1	state	unknown	I am a network state building agent that analyz...		qwen2.5:14b
2	crypto_agent	cai.agents.basic	Agent specialized in cryptographic analysis. Ex...		qwen2.5:14b
3	ctf_agent	cai.agents.basic	Agent focused on CTF challenges. Expert in cybe...		qwen2.5:14b
4	listing_agent	cai.agents.basic	Agent specialized in filesystem navigation and ...		qwen2.5:14b
5	network_agent	cai.agents.basic	Agent specialized in network reconnaissance. Ex...		qwen2.5:14b
6	blueteam_agent	cai.agents.blue_teamer	Agent that specializes in system defense and se...		qwen2.5:14b
7	bug_bounter_agent	cai.agents.bug_bounter	Agent that specializes in bug bounty hunting an...		qwen2.5:14b
8	codeagent	cai.agents.codeagent	Agent focused on writing code iteratively. Stat...		qwen2.5:14b
9	dfir_agent	cai.agents.dfir	Agent that specializes in Digital Forensics and...		qwen2.5:14b
10	flag_discriminator	cai.agents.flag_discriminator	Agent focused on extracting the flag from the o...		qwen2.5:14b
11	dns_smtp_agent	cai.agents.mail	Agent focused on assessing spoofing DMARC.		gpt-4o
12	one_tool_agent	cai.agents.one_tool	Agent focused on conquering security challenges...		qwen2.5:14b
13	redteam_agent	cai.agents.red_teamer	Agent that mimic pentester/red teamer in a secu...		qwen2.5:14b

Setelah konfigurasi mulai dari pemilihan model hingga pemilihan agen selesai, Anda dapat langsung menjalankan perintah untuk menginstruksikan agen melakukan tugas tertentu. Misalnya, untuk melakukan pencarian potensi kerentanan XSS (Cross-Site Scripting) pada sebuah situs uji dari Web Security Academy, Anda cukup mengetikkan perintah seperti berikut.

find xss in https://<labs>.web-security-academy.net

```
CAI> search xss in https://0ae900c3837b0d53d29f57470007000e.web-security-academy.net/
[0] Agent: Bug Bouncer [13:20:49 (together_ai/Qwen/Qwen2.5-72B-Instruct-Turbo)]
generic_linux_command(args=-i https://0ae900c3837b0d53d29f57470007000e.web-security-academy.net/, command=curl) [Total: 8m 8.6s | Tool: 9.8s]
HTTP/2 404
content-type: application/json; charset=utf-8
set-cookie: session=0X0V5FV42Y8uCXaRt1bP2Fa3AQOp; Secure; HttpOnly; SameSite=None
x-frame-options: SAMEORIGIN
content-length: 31
Current: 1:1058 0:527 R:D ($0.0020) | Total: 1:1058 0:527 R:D ($0.0020) | Context: 1.3% █

Agent Interaction
[1] Agent: Bug Bouncer [13:20:53 (together_ai/Qwen/Qwen2.5-72B-Instruct-Turbo)]
generic_linux_command(args=dir -u https://0ae900c3837b0d53d29f57470007000e.web-security-academy.net/ -u /usr/share/seclists/Discovery/Web-Content/common.txt -t 50, command=gobuster) [Total: 8m 32.4s | Tool: 3.8s]
/bin/sh: 1: gobuster: not found
Current: 1:1903 0:174 R:D ($0.0020) | Total: 1:1561 0:801 R:D ($0.0039) | Context: 1.5% █

Agent Interaction
[2] Agent: Bug Bouncer [13:20:55 (together_ai/Qwen/Qwen2.5-72B-Instruct-Turbo)]
generic_linux_command(args=-u https://0ae900c3837b0d53d29f57470007000e.web-security-academy.net/ -u /usr/share/seclists/Discovery/Web-Content/common.txt -t 50, command=feroxbuster) [Total: 8m 14.3s | Tool: 1.9s]
/bin/sh: 1: feroxbuster: not found
Current: 1:2137 0:143 R:D ($0.0021) | Total: 1:1508 0:944 R:D ($0.0060) | Context: 1.7% █

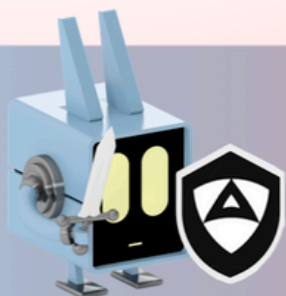
Agent Interaction
[3] Agent: Bug Bouncer [13:20:58 (together_ai/Qwen/Qwen2.5-72B-Instruct-Turbo)]
generic_linux_command(args=wget -O common.txt https://raw.githubusercontent.com/danielmiessler/SecLists/master/Discovery/Web-Content/common.txt, command=curl) [Total: 8m 16.8s | Tool: 2.5s]
curl: Remote file name has no length
curl: (22) Failed writing received data to disk/application
Current: 1:2309 0:195 R:D ($0.0023) | Total: 1:8667 0:1339 R:D ($0.0083) | Context: 1.9% █

Agent Interaction
[4] Agent: Bug Bouncer [13:21:01 (together_ai/Qwen/Qwen2.5-72B-Instruct-Turbo)]
generic_linux_command(args=-O common.txt https://raw.githubusercontent.com/danielmiessler/SecLists/master/Discovery/Web-Content/common.txt, command=wget) [Total: 8m 19.6s | Tool: 2.7s]
--2025-05-25 13:21:01-- https://raw.githubusercontent.com/danielmiessler/SecLists/master/Discovery/Web-Content/common.txt
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.106.133, 185.199.109.133, 185.199.110.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.106.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 38469 (38K) [text/plain]
Saving to: 'common.txt'
```

Penutup

Kemampuan CAI Framework sangat bergantung pada model AI yang digunakan serta agen yang dipilih untuk menjalankan tugas. Kombinasi keduanya akan menentukan kualitas analisis, efektivitas eksploitasi, dan ketepatan rekomendasi yang diberikan. Berbeda dengan tool vulnerability assessment (VA) konvensional yang cenderung statis, CAI menawarkan pendekatan dinamis dan adaptif sesuai dengan tujuan pengujian yang ingin dicapai. Meskipun demikian, perlu dicatat bahwa performa CAI masih memiliki keterbatasan.

Model AI yang digunakan belum sepenuhnya akurat, dan dalam beberapa kasus, dapat menghasilkan analisis yang kurang relevan atau tindakan yang tidak sesuai dengan konteks target. Oleh karena itu, meskipun potensinya besar, CAI saat ini paling cocok digunakan dalam skenario kompetisi seperti Capture The Flag (CTF), di mana eksplorasi cepat, kreativitas, dan eksperimentasi menjadi fokus utama.



CAI

CYBERSECURITY AI
Bug bounty-ready AI





MAGAZINE

PUNGGAWA CYBERSECURITY



ask.sales@punggawa.com



info@jukesolutions.com



[punggawacyber](https://www.instagram.com/punggawacyber)



[jukesolutions](https://www.instagram.com/jukesolutions)



[PunggawaCyber](https://www.facebook.com/PunggawaCyber)



[JUKe Solutions](https://www.facebook.com/JUKeSolutions)



[Punggawa Cybersecurity](https://www.linkedin.com/company/Punggawa%20Cybersecurity)



[Juke Solutions](https://www.linkedin.com/company/Juke%20Solutions)

MAGAZINE PUNGGAWA VOLUME 5

