LAPORAN KEAMANAN JARINGAN

“PEMAHAMAN MATA KULIAH MINGGU LALU”



**NAMA : TANTRI LANGGENG WIDODO**

**MK : KEAMANAN JARINGAN**

**NIM : 09040581721005**

**KELAS : TEKNIK KOMPUTER JARINGAN**

**Penetration Test**

**Penetration Testing** (disingkat pentest) adalah suatu kegiatan dimana seseorang mencoba mensimulasikan serangan yang bisa dilakukan terhadap jaringan organisasi / perusahaan tertentu untuk menemukan kelemahan yang ada pada sistem jaringan tersebut.

**Tahapan *Penetration Testing***

*Penetration Testing* memiliki standar (PTES) yang digunakan sebagai acuan dalam pelaksanaanya yang dibagi ke dalam beberapa tahap :

* ***Pre-engagement Interactions***

Tahap dimana seorang *pentester* menjelaskan kegiatan *pentest* yang akan dilakukan kepada *client* (perusahaan). Disini seorang *pentester* harus bisa menjelaskan kegiatan-kegiatan yang akan dilakukan dan tujuan akhir yang akan dicapai.

* ***Intelligence Gathering***

Tahap dimana seorang *pentester* berusaha mengumpulkan sebanyak mungkin informasi mengenai perusahaan target yang bisa didapatkan dengan berbagai metode dan berbagai media. Hal yang perlu dijadikan dasar dalam pengumpulan informasi adalah : karakteristik sistem jaringan, cara kerja sistem jaringan, dan metode serangan yang bisa digunakan.

* ***Threat Modeling***

Tahap dimana seorang *pentester* mencari celah keamanan (*vulnerabilities*) berdasarkan informasi yang berhasil dikumpulkan pada tahap sebelumnya

**WHOIS**

**Who Is merupakan fasilitas yang berguna untuk mengecek registrasi dari domain tertentu yang sudah mendaftarkan diri di layanan hosting. Jika Anda ingin melihat data secara detail maka berikut adalah beberapa data yang akan bisa Anda dapatkan dalam Who Is:**

**Contact Administrative**

**Informasi yang satu ini berisikan hal-hal yang berkaitan dengan data administrative domain tersebut, misalnya kapan expired date domain tersebut. Apakah pemilik memperpanjang masa hosting domain mereka atau tidak. Selain itu ada juga data mengenai kapan website tersebut didaftarkan dan juga berapa usia aktifnya.**

**Billing Contact**

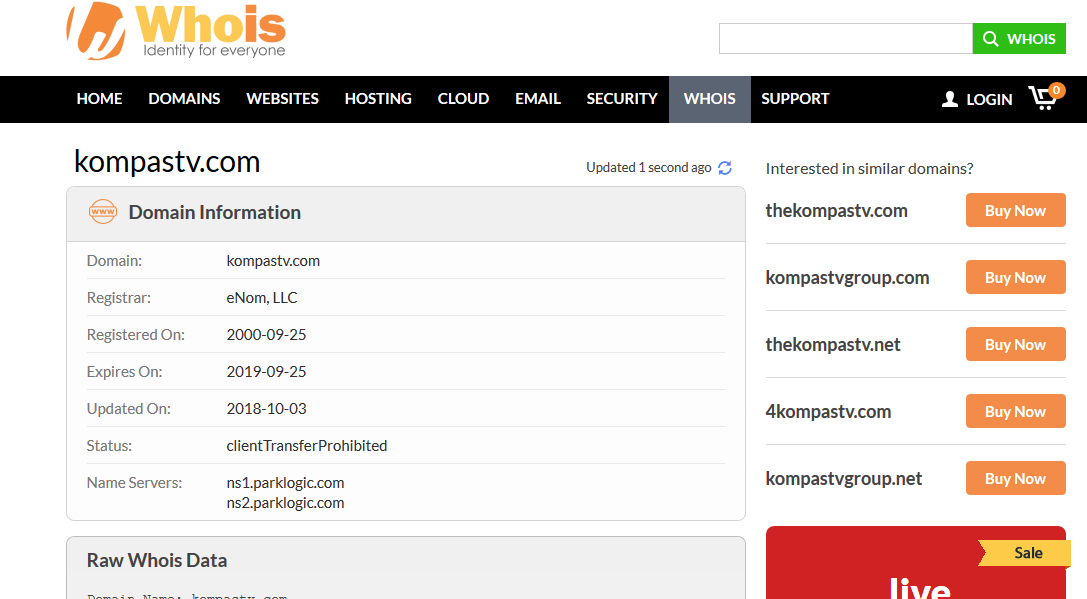
**Informasi lainnya yang bisa didapatkan adalah tentang pembayaran atau penerimaan tagihan terhadap domain tersebut.**

**Server Name**

**Informasi lainnya adalah terkait nama server yang digunakan domain tersebut. Disinilah anda juga akan mendapatkan informasi tentang status dari domain ini. Apakah masih aktif, sedang registar lock, hold, atau pending-restore.**

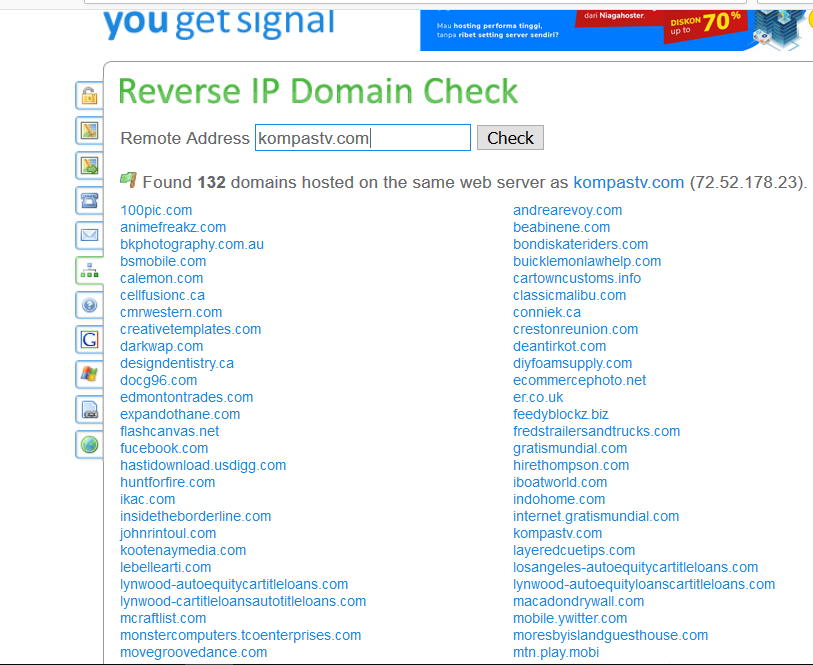
**Technical Contact**

**Informasi lainnya adalah yang berkaitan dengan data teknis, seperti email yang digunakan dan juga detail-detail lainnya yang ada di dalamnya.**



**Reverse IP Domain Checker**

**Reverse IP Domain Checker adalah layanan langka yang ditawarkan oleh situs web hosting. Alat ini menunjukkan situs web yang dibagikan di server web dengan situs web yang Anda masukkan.**



**OS FINGERPRINTING**

**Sidik jari aktif**

Sidik jari aktif adalah proses pengiriman paket ke host jarak jauh dan menganalisis balasan yang sesuai.

**Sidik jari pasif**

Sidik jari pasif adalah proses menganalisis paket dari suatu host pada suatu jaringan. Dalam hal ini, fingerprinter bertindak sebagai [sniffer](https://translate.googleusercontent.com/translate_c?depth=1&hl=id&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=http://www.forensicswiki.org/wiki/Sniffer&xid=25657,15700022,15700186,15700191,15700248,15700253&usg=ALkJrhhovUUde1asT_O7kYF8TtZl_A9FAA) dan tidak menempatkan lalu lintas di jaringan.

**Teknik sidik jari**

Hampir semua teknik sidik jari didasarkan pada pendeteksian perbedaan dalam paket yang dihasilkan oleh sistem operasi yang berbeda.

Teknik umum didasarkan pada analisis:

* Nilai IP TTL;
* Nilai ID IP;
* Ukuran Jendela TCP;
* Opsi TCP (umumnya, dalam paket TCP SYN dan SYN + ACK);
* Permintaan DHCP;
* Permintaan ICMP;
* Paket HTTP (umumnya, bidang User-Agent).

Teknik lain didasarkan pada analisis:

* Menjalankan layanan;
* Buka pola port.

**Keterbatasan**

Banyak sidik jari pasif semakin bingung ketika menganalisis paket dari perangkat NAT.

**Alat**

Sidik jari aktif:

* [Nmap](https://translate.googleusercontent.com/translate_c?depth=1&hl=id&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=http://www.forensicswiki.org/wiki/Nmap&xid=25657,15700022,15700186,15700191,15700248,15700253&usg=ALkJrhhGJ4-pP5KSONR-F-gZAcTY11QYeQ)

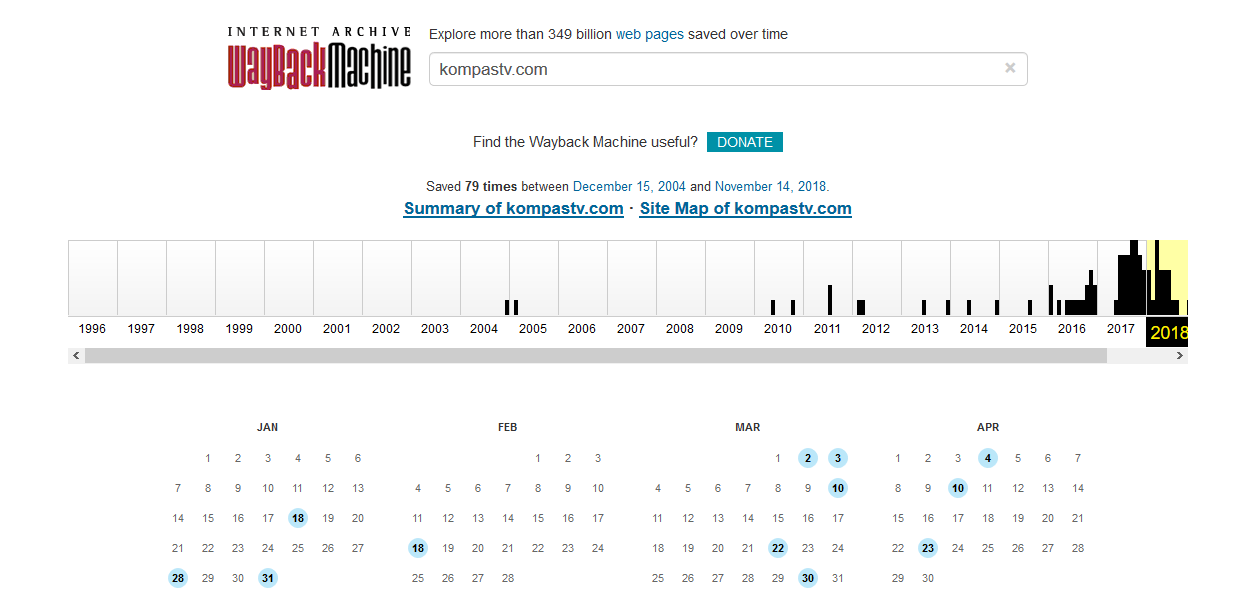
Sidik jari pasif:

* [NetworkMiner](https://translate.googleusercontent.com/translate_c?depth=1&hl=id&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=http://www.forensicswiki.org/wiki/NetworkMiner&xid=25657,15700022,15700186,15700191,15700248,15700253&usg=ALkJrhi2d-ZQSQS6Z4-HbrmRChPIQn-w_Q)
* [p0f](https://translate.googleusercontent.com/translate_c?depth=1&hl=id&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=http://www.forensicswiki.org/index.php%3Ftitle%3DP0f%26action%3Dedit%26redlink%3D1&xid=25657,15700022,15700186,15700191,15700248,15700253&usg=ALkJrhi624TiIopo5dzHhI4kjpNUqxY06w)
* [Satori](https://translate.googleusercontent.com/translate_c?depth=1&hl=id&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=http://www.forensicswiki.org/wiki/Satori&xid=25657,15700022,15700186,15700191,15700248,15700253&usg=ALkJrhiMrwwAbkSxkNcZvqu1_pE5P2-ILg)

**ARCHIVE WEB**

**web** adalah proses mengumpulkan bagian dari [World Wide Web](https://translate.googleusercontent.com/translate_c?depth=1&hl=id&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/World_Wide_Web&xid=25657,15700022,15700186,15700191,15700248,15700253&usg=ALkJrhg80VgXaaOCmio7ByrI3RIiZadnPQ) untuk memastikan informasi tersebut [disimpan](https://translate.googleusercontent.com/translate_c?depth=1&hl=id&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/Digital_preservation&xid=25657,15700022,15700186,15700191,15700248,15700253&usg=ALkJrhgcR6mU_pNWnK7U9w-Vifuy-FpmLQ) dalam [arsip](https://translate.googleusercontent.com/translate_c?depth=1&hl=id&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/Archive&xid=25657,15700022,15700186,15700191,15700248,15700253&usg=ALkJrhjl-jzcUC2H6MyTIBG89sNMGYayOA) untuk peneliti, sejarawan, dan publik di masa depan. [[1]](https://translate.googleusercontent.com/translate_c?depth=1&hl=id&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/Web_archiving&xid=25657,15700022,15700186,15700191,15700248,15700253&usg=ALkJrhjoHgnDWd0SIhxo6Ik83YJkKleUIQ#cite_note-1) Pengarsip Web biasanya menggunakan [perayap web](https://translate.googleusercontent.com/translate_c?depth=1&hl=id&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/Web_crawler&xid=25657,15700022,15700186,15700191,15700248,15700253&usg=ALkJrhibu0Hs24UNXyQGkjUjg8R17Xyb-g) untuk penangkapan otomatis karena ukuran besar dan jumlah informasi di Web. Organisasi pengarsipan web terbesar berdasarkan pendekatan perayapan massal adalah [Internet Archive](https://translate.googleusercontent.com/translate_c?depth=1&hl=id&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/Internet_Archive&xid=25657,15700022,15700186,15700191,15700248,15700253&usg=ALkJrhh9Pn_PzeGaszRo2bhNRTAa_PovMw) yang berusaha untuk menjaga arsip seluruh Web.

International Web Archiving Workshop (IWAW), yang dimulai pada tahun 2001, telah menyediakan platform untuk berbagi pengalaman dan bertukar gagasan. Pendirian [Konsorsium Pelestarian Internet Internasional (IIPC)](https://translate.googleusercontent.com/translate_c?depth=1&hl=id&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/International_Internet_Preservation_Consortium&xid=25657,15700022,15700186,15700191,15700248,15700253&usg=ALkJrhjIdB5aH3s9-UKYmo65gdmgdxVjEg) , pada tahun 2003, telah sangat memfasilitasi kolaborasi internasional dalam mengembangkan standar dan alat sumber terbuka untuk pembuatan arsip web. Perkembangan ini, dan semakin berkembangnya budaya manusia yang diciptakan dan dicatat di web, bergabung untuk menjadikannya tak terhindarkan bahwa semakin banyak perpustakaan dan arsip harus menghadapi tantangan pengarsipan web. [[2]](https://translate.googleusercontent.com/translate_c?depth=1&hl=id&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/Web_archiving&xid=25657,15700022,15700186,15700191,15700248,15700253&usg=ALkJrhjoHgnDWd0SIhxo6Ik83YJkKleUIQ#cite_note-2) [Perpustakaan](https://translate.googleusercontent.com/translate_c?depth=1&hl=id&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/National_library&xid=25657,15700022,15700186,15700191,15700248,15700253&usg=ALkJrhjOYXyLGFIdlEj1mzjsG0bPiHySJA) [nasional](https://translate.googleusercontent.com/translate_c?depth=1&hl=id&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/National_archive&xid=25657,15700022,15700186,15700191,15700248,15700253&usg=ALkJrhijyrDXTJ89PaGlDLcnipIp95K7Ng) , [arsip nasional](https://translate.googleusercontent.com/translate_c?depth=1&hl=id&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/National_archive&xid=25657,15700022,15700186,15700191,15700248,15700253&usg=ALkJrhijyrDXTJ89PaGlDLcnipIp95K7Ng) , dan berbagai konsorsium organisasi juga terlibat dalam pengarsipan konten Web yang penting secara budaya.

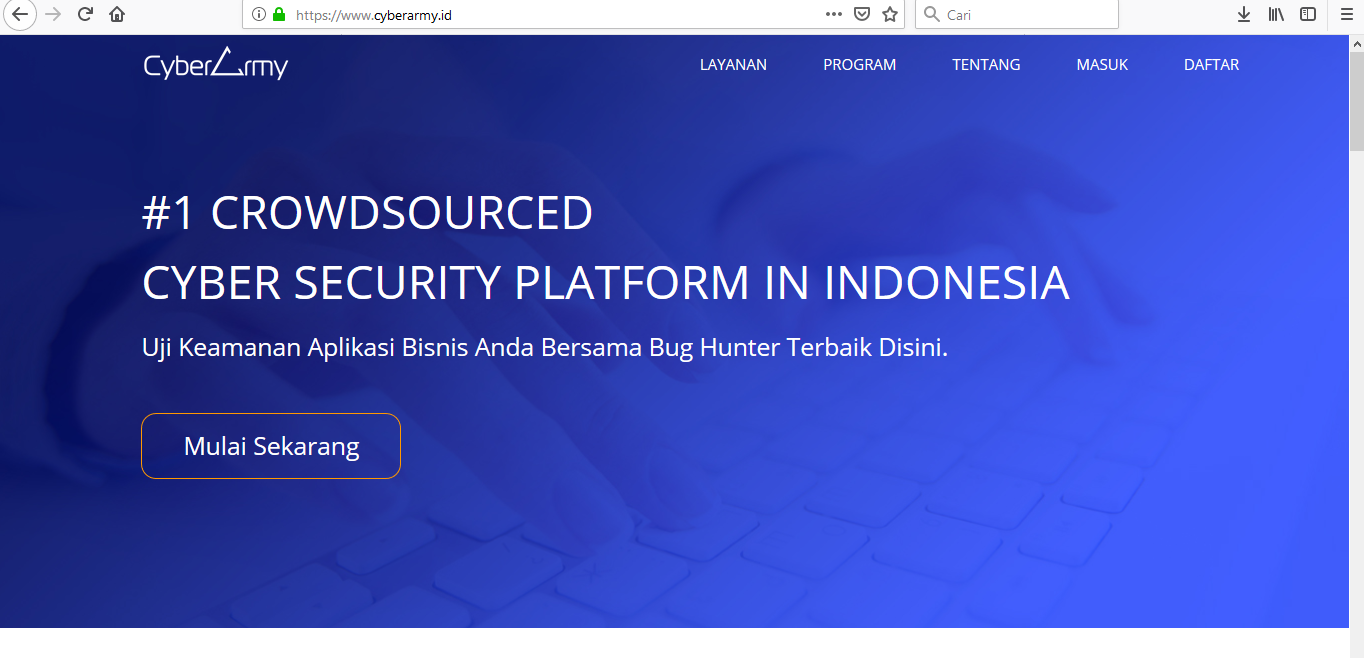


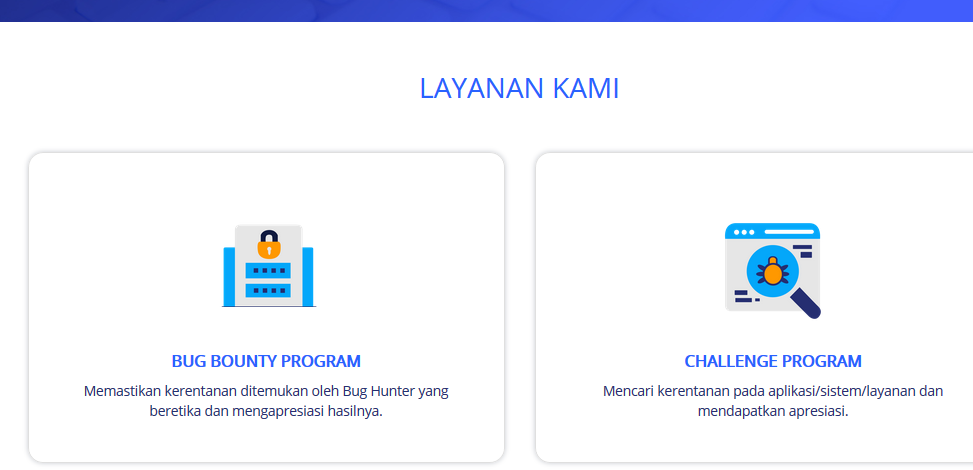
**CYBER ARMY INDONESIA**

1.Cyber Army Indonesia (CyberArmyID) merupakan platform pertama di Indonesia yang mengumpulkan dan memvalidasi laporan dari rekan-rekan Peretas (disebut sebagai Bug Hunter) mengenai kerentanan yang ada pada suatu Organisasi. Selanjutnya, pihak Organisasi akan menerima laporan tersebut untuk ditindaklanjuti, dan kemudian memberikan apresiasi kepada Bug Hunter yang melaporkannya.

CyberArmyID juga berperan sebagai salah satu Pusat Koordinasi Kerentanan dari sektor publik yang hasilnya nanti akan dapat menjadi acuan Keamanan Siber dan Informasi yang terintegrasi di Indonesia.

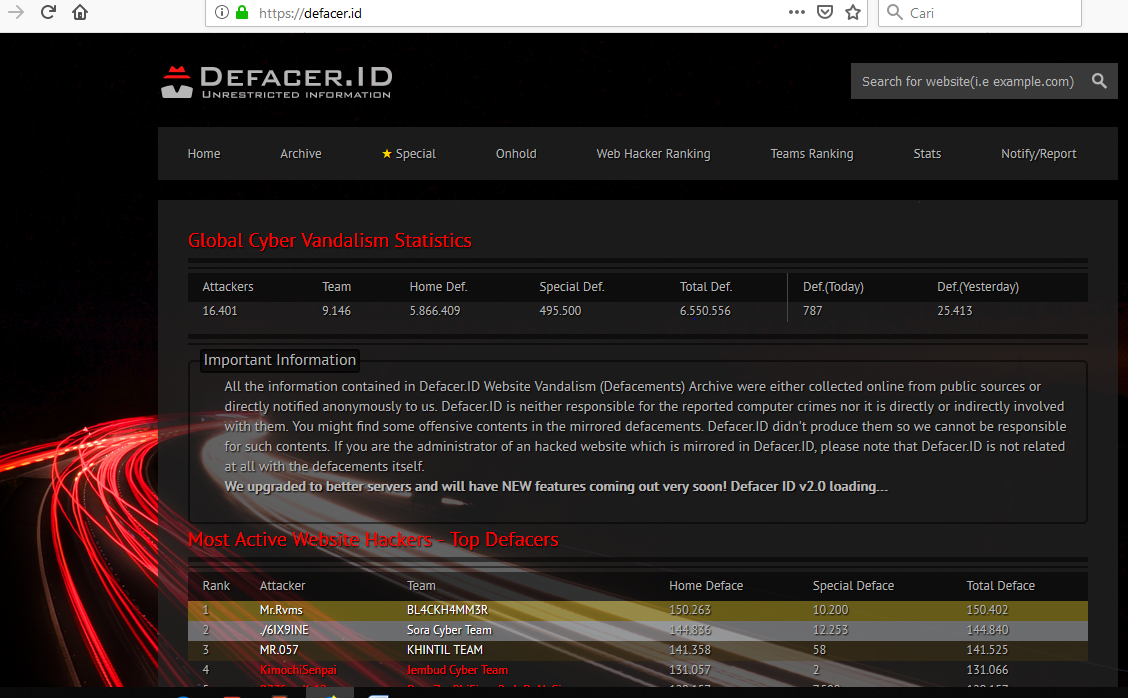
Cyber armyID juga sebagai wadah untuk perusahaan-perusaahaan untuk menguji keamanan server website dan networking pada perusahaan tersebut atau juga dikenla juga dengan pentest

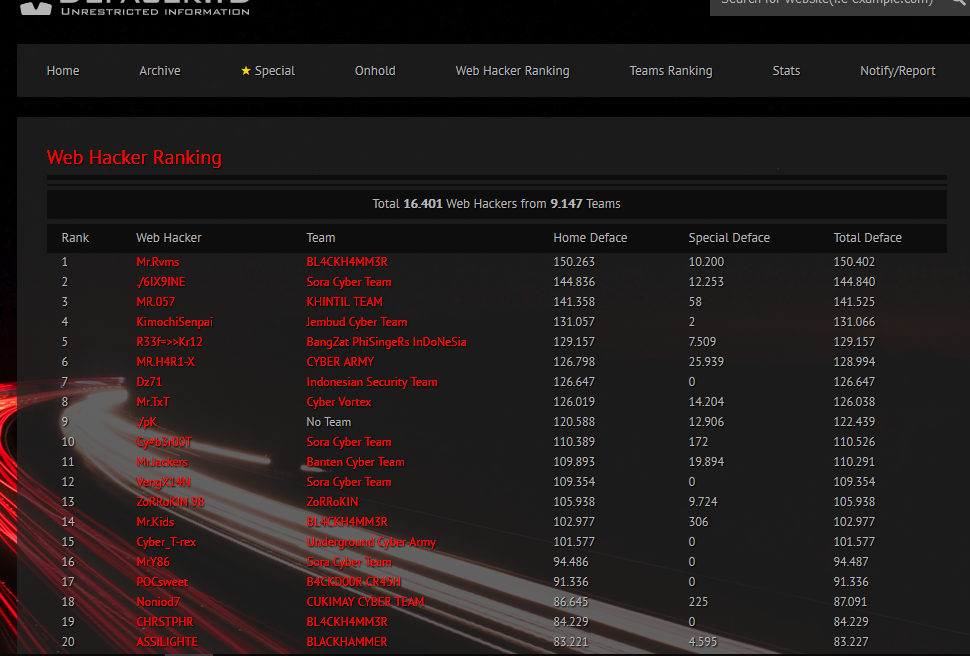




**DEFACER ID**

Defacer pada umumnya adalah orang iseng yang ssedang mecoba mencari tahu baik dari segi ilmu kemampuan, dan jati diri. Kebiasaan yang mudah diketahui dari mereka adalah mereka gemar merubah tampilan utama website, menggunakan kelemahan atau kecacatan dalam sebuah program. Defacer umumnya tidak begitu memahami tentang level pemrograman, mereka lebih sering memahami tenatng kinerja sebuah webserver beserta script yang ada didalamnya. Defacer.id dikenal didunia karena kemampuan nya merubah tampilan website secara ilegal dan juga banyaknya website yang telah diretas hingga ribuan website.





**CVE MITRE**

Dokumentasi MITER Corporation mendefinisikan Pengidentifikasi CVE (juga disebut "nama CVE", "nomor CVE", "CVE-IDs", dan "CVEs") sebagai pengidentifikasi umum yang unik untuk kerentanan keamanan informasi yang diketahui publik dalam paket perangkat lunak yang dipublikasikan untuk umum. Secara historis, pengidentifikasi CVE memiliki status "kandidat" ("CAN-") dan kemudian dapat dipromosikan menjadi entri ("CVE-"), namun praktik ini berakhir beberapa waktu yang lalu dan semua pengidentifikasi sekarang ditetapkan sebagai CVE. Penugasan nomor CVE bukan jaminan bahwa itu akan menjadi entri CVE resmi (misalnya CVE mungkin ditugaskan secara tidak tepat untuk masalah yang bukan kerentanan keamanan, atau yang menduplikasi entri yang ada).

CVE ditugaskan oleh CVE Numbering Authority (CNA); [[3]](https://translate.googleusercontent.com/translate_c?depth=1&hl=id&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures&xid=25657,15700022,15700186,15700191,15700248,15700253&usg=ALkJrhjpNRKKfWk0bW59hokDLhu3Jw9xJg#cite_note-3) ada tiga jenis utama penugasan nomor CVE:

1. Fungsi [Mitre Corporation](https://translate.googleusercontent.com/translate_c?depth=1&hl=id&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/Mitre_Corporation&xid=25657,15700022,15700186,15700191,15700248,15700253&usg=ALkJrhglBTLV8Sq-Mfx8jNYtai21B66ieg) sebagai Editor dan CNA Utama
2. Berbagai CNA menetapkan nomor CVE untuk produk mereka sendiri (mis. Microsoft, Oracle, HP, Red Hat, dll.)
3. Koordinator pihak ketiga seperti [Pusat Koordinasi CERT](https://translate.googleusercontent.com/translate_c?depth=1&hl=id&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/CERT_Coordination_Center&xid=25657,15700022,15700186,15700191,15700248,15700253&usg=ALkJrhiF10D6KH3qqOhJ2orkKtI29IqYlw) dapat menetapkan nomor CVE untuk produk yang tidak tercakup oleh CNA lainnya

Ketika menyelidiki kerentanan atau potensi kerentanan, membantu untuk memperoleh nomor CVE sejak dini. Nomor CVE mungkin tidak muncul di database MITER atau NVD CVE untuk beberapa waktu (hari, minggu, bulan, atau tahun potensial) karena masalah yang diembargo (nomor CVE telah ditetapkan tetapi masalahnya belum dipublikasikan), atau dalam kasus di mana entri tersebut tidak diteliti dan ditulis oleh MITER karena masalah sumber daya. Manfaat pencalonan CVE awal adalah bahwa semua korespondensi di masa mendatang dapat merujuk ke nomor CVE. Informasi tentang mendapatkan pengidentifikasi CVE untuk masalah dengan proyek sumber terbuka tersedia dari [Red Hat](https://translate.googleusercontent.com/translate_c?depth=1&hl=id&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/Red_Hat&xid=25657,15700022,15700186,15700191,15700248,15700253&usg=ALkJrhhHd290l0jppnX_ZvdT2Tg_OOEW4A) . [[4]](https://translate.googleusercontent.com/translate_c?depth=1&hl=id&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures&xid=25657,15700022,15700186,15700191,15700248,15700253&usg=ALkJrhjpNRKKfWk0bW59hokDLhu3Jw9xJg#cite_note-4)

CVE adalah untuk perangkat lunak yang telah dirilis untuk umum; ini dapat mencakup beta dan versi pra-rilis lainnya jika mereka banyak digunakan. Perangkat lunak komersial termasuk dalam kategori "dirilis secara publik", namun perangkat lunak yang dibuat khusus yang tidak didistribusikan umumnya tidak akan diberi CVE. Selain itu layanan (mis. Penyedia email berbasis web) tidak ditugaskan CVE untuk kerentanan yang ditemukan dalam layanan (misalnya kerentanan XSS) kecuali ada masalah dalam produk perangkat lunak yang mendasarinya yang didistribusikan secara publik.



**DIRTY COW**

Dirty COW ( Dirty copy-on-write ) adalah kerentanan keamanan komputer untuk kernel Linux yang mempengaruhi semua sistem operasi berbasis Linux termasuk Android yang menggunakan versi lama dari kernel Linux. Ini adalah bug eskalasi hak istimewa lokal yang mengeksploitasi kondisi ras dalam implementasi mekanisme copy-on-write dalam subsistem manajemen memori kernel. Kerentanan itu ditemukan oleh Phil Oester . [1] [2] Karena kondisi balapan, dengan waktu yang tepat, penyerang lokal dapat mengeksploitasi mekanisme copy-on-write untuk mengubah pemetaan read-only dari file menjadi pemetaan yang dapat ditulis. Meskipun ini merupakan eskalasi hak istimewa lokal, penyerang jarak jauh dapat menggunakannya bersamaan dengan eksploit lain yang memungkinkan eksekusi kode non-privilege secara remote untuk mencapai akses root jarak jauh di komputer. [1] Serangan itu sendiri tidak meninggalkan jejak di log sistem. [2]

Kerentanan memiliki sebutan CVE Common Vulnerabilities and Exposures - 2016-5195 . [3] Dirty Cow adalah salah satu masalah keamanan pertama yang diperbaiki secara transparan di Ubuntu oleh layanan Canonical Live Patch. [4]

Kerentanan COW Kotor memiliki banyak kasus penggunaan yang dirasakan termasuk contoh terbukti, seperti mendapatkan izin root di perangkat Android, serta beberapa implementasi berspekulasi. Ada banyak biner yang digunakan di Linux yang hanya-baca, dan hanya dapat dimodifikasi atau ditulis oleh pengguna dengan izin yang lebih tinggi, seperti root. Ketika hak istimewa ditingkatkan, apakah dengan cara asli atau jahat - seperti dengan menggunakan exploit COW Kotor - pengguna dapat memodifikasi biner dan file yang biasanya tidak dapat dimodifikasi. Jika individu jahat dapat menggunakan kerentanan COW Kotor untuk meningkatkan izin mereka, mereka dapat mengubah file, seperti / bin / bash, sehingga melakukan fungsi tambahan yang tidak terduga, seperti keylogger. Ketika pengguna memulai program yang telah terinfeksi, mereka secara tidak sengaja akan membiarkan kode jahat dijalankan. Jika exploit menargetkan suatu program yang dijalankan dengan privilege root, eksploit akan menikmati privilege yang sama.



**BUG COUNTY PROGRAM**

Program karunia bug adalah kesepakatan yang ditawarkan oleh banyak situs web dan pengembang perangkat lunak di mana individu dapat menerima pengakuan dan kompensasi [1] untuk melaporkan bug , terutama yang berkaitan dengan eksploitasi dan kerentanan . Program-program ini memungkinkan para pengembang untuk menemukan dan menyelesaikan bug sebelum masyarakat umum menyadarinya, mencegah insiden penyalahgunaan yang meluas. Program karunia bug telah diterapkan oleh sejumlah besar organisasi, termasuk Mozilla , [2] [3] Facebook , [4] Yahoo! , [5] Google , [6] Reddit , [7] Square , [8] dan Microsoft . [9] [10] Perusahaan di luar industri teknologi, termasuk organisasi tradisional konservatif seperti Departemen Pertahanan Amerika Serikat , telah mulai menggunakan program karunia bug. [11] Penggunaan Pentagon terhadap program karunia bug adalah bagian dari perubahan postur yang telah membuat beberapa Instansi Pemerintah AS berbalik arah dari mengancam peretas topi putih dengan bantuan hukum untuk mengundang mereka untuk berpartisipasi sebagai bagian dari kerangka kerja atau kebijakan pengungkapan kerentanan komprehensif. [12] Dalam arti yang lebih umum, istilah ini telah diterapkan untuk membuka masalah dalam penelitian matematika dan ilmu komputer , yang juga menawarkan jumlah yang signifikan untuk solusi mereka.

