Berlatih Jadi Hacker

Menggunakan VirtualBox, Kali Linux dan Tool Lainnya untuk Hacking

Happy Chandraleka, S.T.

Berlatih Jadi Hacker:
Menggunakan VirtualBox, Kali Linux dan Tool Lainnya untuk Hacking

Penulis	: Happy Chandraleka, S.T.
Penyunting	: Happy Chandraleka, S.T.
Perancang Sampul	: Happy Chandraleka, S.T.
Penata Letak	: Happy Chandraleka, S.T.

حَدَّثَنَا آدَمُ بْنُ أَبِي إِيَاسٍ، حَدَّثَنَا ابْنُ أَبِي ذِئْبٍ، حَدَّثَنَا سَعِيدٌ الْمَقْبُرِيُّ، عَنْ أَبِي هُرَيْرَةَ . رضى الله عنه . قَالَ قَالَ رَسُولُ اللَّهِ صلى الله عليه وسلم **" مَنْ كَانَتْ لَهُ مَظْلَمَةٌ لأَحَدٍ مِنْ عِرْضِهِ أَوْ شَىْءٍ فَلْيَتَحَلَّلْهُ مِنْهُ الْيَوْمَ، قَبْلَ أَنْ لاَ يَكُونَ دِينَارٌ وَلاَ دِرْهَمٌ، إِنْ كَانَ لَهُ عَمَلٌ صَالِحٌ أُخِذَ مِنْهُ بِقَدْرِ مَظْلَمَتِهِ، وَإِنْ لَمْ تَكُنْ لَهُ حَسَنَاتٌ أُخِذَ مِنْ سَيِّئَاتِ صَاحِبِهِ فَحُمِلَ عَلَيْهِ** ". قَالَ أَبُو عَبْدِ اللَّهِ قَالَ إِسْمَاعِيلُ بْنُ أَبِي أُوَيْسٍ إِنَّمَا سُمِّيَ الْمَقْبُرِيَّ لأَنَّهُ كَانَ نَزَلَ نَاحِيَةَ الْمَقَابِرِ. قَالَ أَبُو عَبْدِ اللَّهِ وَسَعِيدٌ الْمَقْبُرِيُّ هُوَ مَوْلَى بَنِي لَيْثٍ، وَهُوَ سَعِيدُ بْنُ أَبِي سَعِيدٍ، وَاسْمُ أَبِي سَعِيدٍ كَيْسَانُ.

Telah menceritakan kepada kami [Adam bin Abi Iyas], telah menceritakan kepada kami [Ibnu Abi Dza'bi], telah menceritakan kepada kami [Sa'id Al Maqburiy], dari [Abu Hurairah radhiallahu 'anhu] berkata; “Rasûlullah shallallaahu ’alaihi wa sallam bersabda, “Barang siapa berbuat zhalim kepada saudaranya, yang berkaitan dengan kehormatan atau sesuatu apapun, hendaklah dia meminta halal darinya pada hari ini, sebelum (datang hari kiamat) yang tidak ada dinar dan dirham. Jika dia memiliki amal shalih diambil darinya seukuran kezhalimannya. Jika dia tidak memiliki keabaikan-kebaikan, diambil kesalahan-kesalahan orang yang dizhalimi lalu ditimpakan padanya.”

[HR. Al-Bukhâri, no. 2449, 6534; Ahmad 2/435, 506; Ibnu Hibban no. 7361]

Berlatih Jadi Hacker:

Menggunakan VirtualBox, Kali Linux dan Tool Lainnya untuk Hacking

Oleh Happy Chandraleka, S.T.

Prakata

Di era digital ini, pengetahuan dan skill tentang hacking menjadi suatu yang sangat penting dan berharga untuk dimiliki. Bukan untuk semata-mata untuk menyerang, tetapi lebih pada upaya mengamankan diri dan mengamankan sistem informasi yang kita kelola.

Buku ini memberikan dasar-dasar tentang penetration testing yang merupakan tahapan penting dalam proses hacking. Kemudian penyediaan perangkat virtualisasi. Hal ini dikarenakan sebagian pengguna komputer saat ini menggunakan sistem operasi Windows. Sehingga diharapkan dengan virtualisasi dapat dipasang sistem operasi Kali Linux tanpa perlu mengganggu sistem operasi Windows yang telah eksis sebelumnya.

Bagian berikutnya buku ini akan membimbing pembaca untuk melakukan instalasi sistem operasi Kali Linux yang merupakan sistem operasi khusus untuk kepentingan hacking. Dalam buku ini dipraktekkan sebagian perangkat hacking yang ada di Kali Linux yaitu cara menggunakan Wireshark untuk mendapatkan usesname dan password login; cara menggunakan Nmap untuk mengetahui port yang terbuka; cara menggunakan John the Ripper untuk membongkar password; dll.

Perangkat hacking tidak hanya ada di Kali Linux. Banyak juga bertebaran di Internet. Oleh karena itu pada bagian berikutnya buku ini melatih pembaca untuk menggunakan tool dari luar Kali Linux. Di antaranya adalah menggunakan Security Header; Web Check; OWASPZAP untuk mendeteksi kerentanan dan celah pada suatu aplikasi berbasis web. Penulis berharap buku ini dapat memberikan dasar-dasar yang kuat bagi siapa yang akan memasuki dunia hacking.

Akhirnya buku ini selesai disusun dengan pertolongan Allah semata pada Selasa, 10 Jumadal Ula 1446 H atau 12 November 2024. Wal hamdulillah, segala puji bagi Allah, Rabb Yang Bersemayam Di Atas Arsy.

Daftar Isi

Dasar-Dasar Penetration Testing

Lima Prinsip Keamanan Informasi

Dalam dunia keamanan informasi, ada lima prinsip keamanan informasi yang harus menjadi pedoman. Kelima prinsip ini pula tertuang dalam dalam Sistem Pemerintahan Berbasis Elektronik (SPBE) di negara kita. Lima prinsip tersebut adalah:

1. Kerahasiaan
2. Keutuhan
3. Ketersediaan
4. Keaslian
5. Kenirsangkalan

Lima prinsip ini termaktub dalam pasal 40 Peraturan Presiden Republik Indonesia nomor 95 tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik yang ditetapkan pada 2 Oktober 2018.

Lima prinsip ini pula yang menjadi standar teknis keamanan data dan informasi sebagaimana tertuang dalam Peraturan Badan Siber dan Sandi Negara nomor 4 tahun 2021 pada pasal 19. Peraturan ini diketok pada 19 Mei 2021.

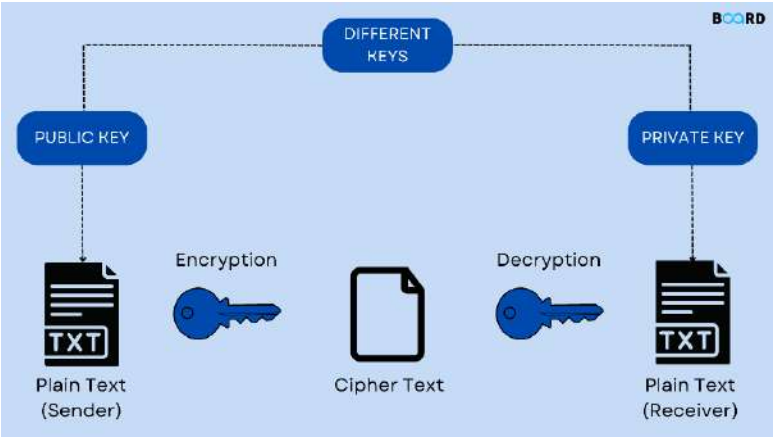
Lima prinsip tersebut harus tercakup dalam semua sumber daya terkait dengan data dan informasi, infrastruktur SPBE, dan aplikasi SPBE.

Kerahasiaan (Confidentiality)

Aspek kerahasiaan maksudnya data dan informasi tersebut hanya tersedia atau bisa diakses hanya untuk orang-orang yang diberi hak saja. Aspek kerahasiaan dilakukan dengan cara membuat klasifikasi informasi maksudnya membuat filter bahwa informasi tersebut ada yang bersifat umum, terbatas, atau rahasia. Ini cara yang pertama.

Cara yang kedua, aspek kerahasiaan dapat dicapai dengan cara penerapan pembatasan akses terhadap data dan informasi sesuai dengan kewenangan dan kebijakan yang telah digariskan.

Cara yang ketiga, dilakukan dengan penerapan sistem kriptografi. Kriptografi adalah suatu teknik untuk mengacak informasi (enkripsi) sehingga informasi tersebut tidak tersedia dalam bentuk *plain text*. Sehingga siapa pun yang berhasil mendapatkan informasi teracak itu harus mengembalikan (dekripsi) pesan yang teracak ke bentuk semula.



(https://www.boardinfinity.com/blog/cryptography-explanation-and-types/)

Keutuhan (Integrity)

Aspek keutuhan maksudnya data atau informasi tersebut utuh dan tidak berubah. Kalau pun bisa diubah hanya oleh orang-orang yang diberi kewenangan. Aspek keutuhan dilakukan dengan menerapkan pendeteksian modifikasi.

Selain itu aspek keutuhan dapat dilakukan dengan menerapkan tanda tangan elektronik tersertifikasi. Saat ini Balai Sertifikasi Elektronik (BsrE) merupakan penyelenggara tanda tangan elektronik di Indonesia.

Ketersediaan (Availability)

Aspek ketersediaan ini maksudnya adalah bahwa data atau informasi tersebut harus dapat diakses kapan saja dan di mana saja. Bila tidak dapat diakses berarti telah terjadi gangguan pada sistem penyedia data dan informasi tersebut.

Aspek ketersediaan dapat dicapai dengan menerapkan sistem pencadangan (backup) secara berkala. Membuat perencanaan untuk menjamin data dan informasi dapat selalu diakses.

Selain itu perlu dilakukan pula sistem pemulihan (recovery) yang handal sebagai antisipasi bila terjadi insiden.

Keaslian (Authentication)

Aspek keaslian maksudnya sistem mengenali bahwa sistem sedang berhadapan dengan orang yang memiliki kewenangan untuk mengakses. Aspek ini dapat dicapai dengan melakukan verifikasi dan validasi.

Verifikasi maksudnya adalah sistem berhadapan dengan pemilik akun yang sah. Misalnya dengan mengirimkan kode verifikasi ke nomor handphone atau alamat email yang dimasukkan pengguna.

Validasi maksudnya data dan informasi yang diberikan sah dan akurat. Misalnya seorang pengguna memasukkan kata sandi atau PIN saat melakukan transaksi elektronik.

Teknologi untuk mengimplementasikan aspek ini adalah dengan tanda tangan elektronik, enkripsi, Two-Factor Authentication (2FA) atau Multi-Factor Authentication (MFA), sertifikat digital, dan otoritas berbasis peran.

(https://www.zoho.com/blog/directory/why-is-mfa-important-for-your-business.html)

Kenirsangkalan (Nonrepudiation)

Aspek kenirsangkalan maksudnya adalah menjamin informasi tersebut tidak dapat disangkal oleh pihak pengirim atau penerima. Aspek ini dapat diterapkan dengan implementasi tanda tangan elektronik tersertifikasi atau sertifikat elektronik.

Vulnerability atau Kerentanan

Secara bahasa vulnerability adalah suatu keadaan dimana keadaan tersebut terbuka kemungkinan untuk mendapat serangan dari luar. Dalam bahasa Indonesia dikenal dengan istilah kerentanan atau kelemahan. Suatu sistem dengan vulnerability yang tinggi artinya sistem tersebut memiliki banyak kerentanan atau kelemahan. Selain itu suatu sistem dikatakan baik bila memiliki vulnerability yang rendah.

Vulnerability pada Sistem Informasi

Setiap sistem berpeluang memiliki vulnerability. Vulnerability pada brainware (pengguna komputer) bisa terjadi semisal pengguna tersebut salah mengoperasikan sistem komputer yang tidak sesuai prosedur kerja. Vulnerability bisa terjadi pada aplikasi web, misalnya sebuah web menggunakan plugin yang tidak ter-update atau menggunakan versi yang sudah kadaluarsa. Bisa jadi pula vulnerability terjadi pada sistem operasi yang sedang digunakan, karena tidak menggunakan update yang terkini yang disediakan oleh penyedia sistem operasi. Vulnerability bisa terjadi

pula pada aplikasi software, misalnya software tersebut memuat bug yang dapat dimanfaatkan oleh penyerang untuk masuk ke salam sistem. Dengan demikian vulnerability bisa terjadi pada banyak sisi di sistem informasi.

(Sumber: Getty Images)

Vulnerability merupakan kelemahan dan sangat potensial untuk dimanfaatkan oleh penyerang atau pihak-pihak yang tidak bertanggung jawab.

Penganganan Vulnerability

Vulnerability pada suatu sistem informasi bisa berjumlah ratusan atau bahkan ribuan. Kelemahan ini perlu mendapatkan penganganan dengan melakukan tata kelola atau manajemen vulnerability. Misalnya dengan melakukan grading atau pemeringkatan dari resiko yang bisa ditimbulkan. Ada suatu lembaga yang melakukan pemeringkatan menjadi level critical, high, medium, dan low. Cara ini bisa saja ditempuh agar pengelola sistem dapat memprioritaskan kerentanan yang mana yang akan dibereskan terlebih dahulu.

Contoh pemeringkatan atau scoring yang dilakukan oleh Imperva, sebuah perusahaan cyber security yang berbasis di Austin, Texas. Imperva melakukan grading seperti di bawah ini.

Severity	Base Score
None	0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

Pemeringkatan dari Imperva (sumber: imperva.com)

Lain halnya dengan Owasp, sebuah yayasan nirlaba yang berfokus pada keamanan aplikasi, memberikan pemeringkatan pada hasil scanning kerentanan seperti contoh di bawah ini.

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	4
Low	4
Informational	3

Pemeringkatan resiko vulnerability dari Owasp Zap

Penjelasan lebih detail terkait pemeringkatan resiko dari Owasp Zap ini akan dijelaskan pada bagian lain di buku ini.

Pemeringkatan tersebut memudahkan pengelola sistem informasi untuk bisa berfokus pada level kerentanan tertentu, misalnya level high terlebih dahulu untuk diselesaikan baru kemudian level di bawahnya.

Top 10 Vulnerabilities

Berikut 10 vulnerabilities atau kerentanan yang paling banyak terjadi pada akhir-akhir ini menurut penilaian dari OWASP. Yang perlu diingat pemeringkatan ini bisa berubah sepanjang tahun.

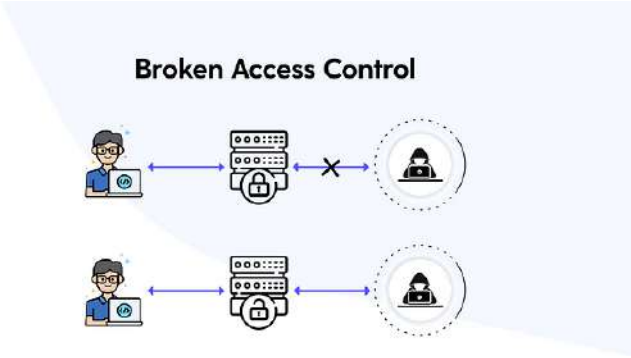
1. Broken-Access Control
2. Cryptographic Failures
3. Injection
4. Insecure Design
5. Security Misconfiguration
6. Vulnerable and Outdated Components
7. Identification and Authentication Failures
8. Software and Data Integrity Failures
9. Security Logging and Monitoring Failures
10. Server-Side Request Forgery (SSRF)

Detail penjelasan dari kerentanan tersebut dapat dilihat di bawah ini.

Broken-Access Control

Access control atau pengendalian akses merupakan suatu cara agar siapa dan dalam kondisi apa dapat mengakses suatu sistem informasi. Pengendalian ini penting untuk memfilter siapa yang berhak untuk mendapatkan akses dan dalam syarat dan kondisi yang telah ditentukan. Selain itu untuk menentukan orang tersebut dapat mengakses apa saja. Inti dari access control adalah pembatasan dan pemfilteran akses.

Dalam suatu aplikasi berbasis web, implementasi dari access control ini bisa menggunakan authentication atau session management. Bila terjadi broken-access control akibatnya orang atau pihak yang tidak berwenang dapat mengakses sistem informasi. Seperti diperlihatkan pada gambar di bawah ini. Ilustrasi yang paling bawah menggambarkan telah terjadi broken-access control (ditandai dengan gembok yang tidak terkunci) sehingga pihak yang tidak berwenang dapat mengakses sistem informasi.



Broken-access control (sumber: medium.com)

Penyebab broken-access control dapat terjadi karena beragam faktor. Sebagian di antaranya adalah cross-site scripting; injection flaws; broken authentication; broken session management; brute force attacks; session hijacking; man-in-the-middle attacks; privilege escalation attacks; dll.

Sebagai solusi untuk mengatasi kerentanan broken-access control di antaranya dengan menggunakan multi-factor authentication; menjalankan validasi akses; melakukan audit access controls; dll.

Multi-factor authentication (sumber: teamascend.com)

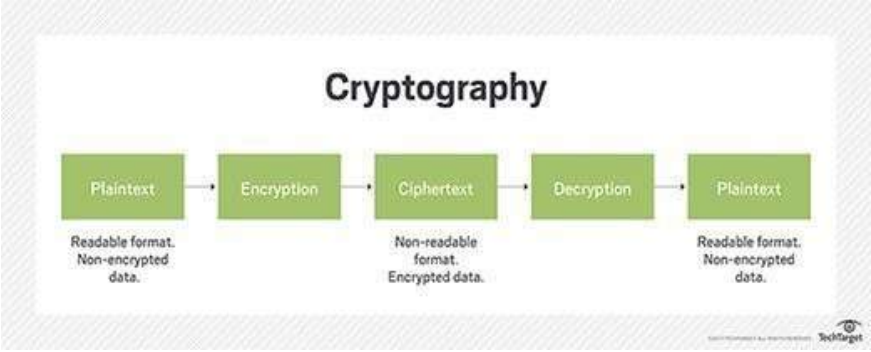
Cryptographic Failures

Cryptographic failures atau kegagalan proses kriptografi. Hal ini terjadi pada data sensitif (misalnya pasword; data kartu kredit; data pribadi; dll) yang tidak diamankan secara benar. Cryptographic failures berujung pada kebocoran data atau pencurian data.

Biasanya pengamanan data dilakukan dengan menggunakan proses kriptografi yaitu dengan mengenkripsi data tersebut dengan metode enkripsi tertentu. Tujuan mengenkripsi data ini agar bila data tersebut dicuri atau bocor ke pihak yang tidak berwenang, data tersebut tidak mudah untuk dibongkar ke bentuk aslinya karena masih dalam bentuk teracak (terenkripsi). Sehingga pencuri data harus membongkar enkripsi data agar bisa membaca data yang telah dia curi. Cryptographic failures atau kegagalan kriptografi pada suatu sistem informasi menyebabkan pencuri data dengan mudah membaca data apa adanya alias tanpa effort yang sulit.

Cryptographic failures ini bisa diakibatkan karena metode enkripsi menggunakan algoritma yang lemah atau abal-abal atau algoritma yang sudah jadul. Cryptographic failures ini dapat terjadi juga karena data

ditransmisikan menggunakan protokol biasa tanpa enkripsi misalnya HTTP, FTP, atau SMTP.



Cryptography (sumber: techtarget.com)

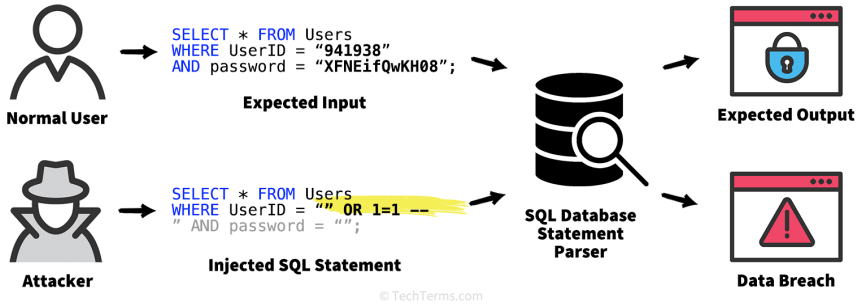
Sebagai solusi untuk mengatasi cryptographic failures ini adalah dengan menggunakan algoritma enkripsi yang handal. Pastikan menggunakan algoritma yang baik misalnya Advanced Encryption Standard untuk melindungi data sensitif. Selain itu gunakan protokol yang terenkripsi misalnya HTTPS untuk mentransmisikan data melalui internet. Penting juga untuk dipertimbangkan agar tidak menyimpan data yang tergolong sensitif tanpa ada kepentingan yang urgent.

Injection

Injection diartikan dengan menyuntikkan, atau semakna dengan 'insertion' yang berarti menyisipkan. Dalam dunia komputer dimaksudkan dengan menyuntikkan atau menyisipkan sepenggal kode ke dalam suatu aplikasi.

Dalam dunia cyber security, kegiatan injection yang biasa dilakukan adalah dengan menginjeksi penggalan kode SQL atau dikenal dengan SQL injection. Yaitu dengan menyisipkan query SQL ke dalam suatu aplikasi, biasanya melalui form inputan. Kode yang diinputkan tersebut dikenal dengan istilah SQL injection exploit. Dengan exploit tersebut seorang

hacker dapat membaca data yang sensitif bahkan dapat melakukan modifikasi data yaitu melakukan insert data, update data atau bahkan hapus data.



SQL injection (sumber: techterms.com)

Untuk mengatasi SQL injection ini dapat dilakukan validasi dan sanitasi input. Sehingga inputan yang dimasukkan oleh user harus bersih dari kode-kode yang berbahaya. Teks yang diinputkan harus dibatasi dan harus bebas dari karakter yang bersifat exploit. Selain itu perlu juga mematikan pesan database error saat inputan yang dimasukkan salah, karena pesan error tersebut biasanya memberikan informasi tentang database yang digunakan oleh aplikasi.

Insecure Design

Arsitektur perangkat lunak yang salah dapat menyebabkan kerentanan dalam hal insecure design. Vulnerability jenis ini berkaitan dengan seorang developer aplikasi dalam membangun sebuah sistem yang menerapkan prinsip-prinsip keamanan informasi dan menutup celah potensi ancaman.

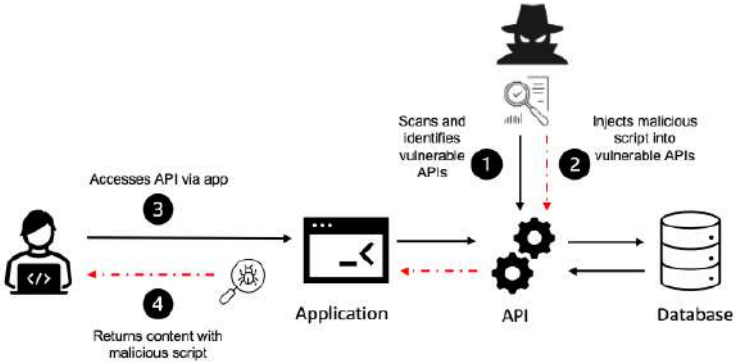
Menarik untuk dipahami bahwa pembangunan perangkat lunak dilakukan oleh programmer sebagai seorang manusia yang bisa saja berbuat kesalahan dalam merancang programnya. Kuncinya di sini adalah berupaya agar sang programmer seminimal mungkin melakukan kesalahan *development*.

Vulnerability ini bisa diakibatkan karena beberapa hal. Di antaranya minimnya validasi input; session management yang tidak benar; pengelolaan storage yang tidak aman; dan bisa juga karena penggunaan protokol komunikasi yang tidak tepat.

Solusi untuk mengatasi insecure design adalah dengan melakukan audit pada sistem keamanan aplikasi; atau bisa juga dengan melakukan harddening pada server; dll.

Hal lain yang perlu dilakukan dalam secure design adalah dengan membangun aplikasi pada teknologi yang terbukti handal. Gunakan library atau patch atau plugin yang terbukti baik.

Penting juga untuk melakukan automatic check dengan penetration testing pada aplikasi untuk mengetahui kerentanan apa saja. Cara ini termasuk cukup efektif untuk mengetahui security vulnerability. Meski harus juga dilakukan manual checking.



Insecure design pada vulnerable API (sumber: lembergsolutions.com)

Security Misconfiguration

Security misconfiguration merupakan jenis vulnerability yang diakibatkan karena pengaturan setting yang salah dan tidak tepat. Misalnya saja pemilik server tetap mengaktifkan fitur-fitur yang tidak dibutuhkan, seperti tetap mengaktifkan fitur remote access padahal fitur tersebut tidak diperlukan. Hal ini bisa menjadi celah kerentanan dan membuka potensi serangan hacker.

Security misconfiguration bisa menjadi pintu masuk untuk serangan berupa:

- Brute force attack
- SQL injection
- Cross-site scripting (XSS)
- Dll

Sebagai solusi untuk mengantisipasi kerentanan security misconfiguration ini adalah dengan melakukan hardening pada server yang ada. Selain itu meminimalkan fitur-fitur yang ada dan hanya mengaktifkan fitur-fitur

yang hanya dibutuhkan. Hapus dan uninstall fitur yang tidak digunakan. Lakukan juga review atas settingan konfigurasi keamanan dalam sistem.

Vulnerable and Outdated Components

Kerentanan ini terjadi bila kita menggunakan komponen, plugin, modul atau library yang sudah tidak didukung lagi oleh developernya, atau sudah umum diketahui bahwa komponen, plugin, modul, atau library tersebut diketahui memiliki celah keamanan.

Seorang hacker akan masuk ke dalam jaringan yang menjadi target kemudian melakukan scanning untuk mengetahui komponen-komponen yang sudah lawas atau komponen yang memiliki celah keamanan. Bila ditemukan, maka hacker tersebut akan mengeksploitasi celah keamanan tersebut dengan memasang kode-kode yang berbahaya yang diinginkannya. Bisa jadi juga memasang back door atau meningkatkan previlege aksesnya.

Kerentanan jenis ini akan membuka pintu untuk serangan berupa:

- SQL injection
- Atau injection lainnya
- Cross-site scripting (XSS)

Sebagai pencegahan atau solusi dari kerentanan jenis ini adalah dengan tetap menggunakan komponen, plugin, atau modul dengan versi yang paling terkini dan hanya menggunakan dari sumber-sumber yang terpercaya.

Identification and Authentication Failures

Kerentanan ini terjadi bila sistem gagal melakukan identifikasi dan autentikasi dengan benar. Misalnya saja gagal mengecek yang masuk ke

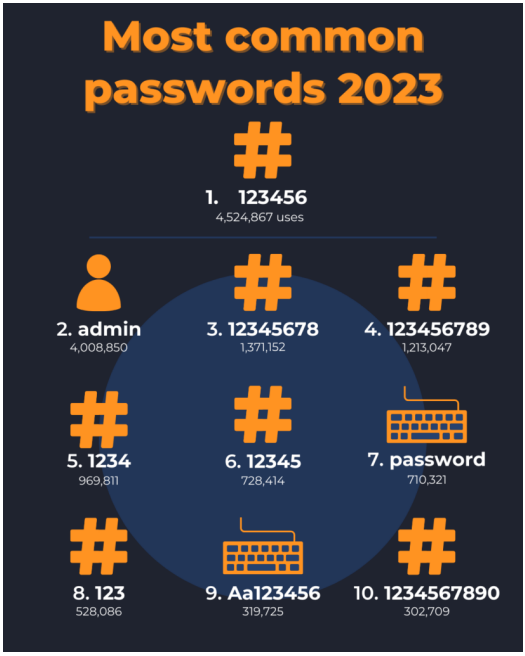
sistem itu seorang user biasa atau seorang admin sistem. Kerentanan ini bisa berakibat akses data dan sistem oleh yang tidak berwenang.

Beberapa penyebab vulnerability jenis ini adalah:

- Penggunaan kata sandi yang lemah. Misalnya menggunakan ’1234567890’, atau kata sandi lain yang mudah ditebak.
- Tidak menerapkan two-factor authentication atau multi-factor authentication.
- Sistem dimungkinkan pula terkena serangan brute-force attacks, yaitu dengan mencoba kombinasi karakter yang mungkin dan berharap salah satunya adalah password yang tepat.

Sebagai solusi untuk mencegah kerentanan ini adalah:

- Menerapkan two-factor authentication atau multi-factor authentication.
- Menerapkan kebijakan kata sandi yang baik. Yaitu sistem hanya menerima kata sandi dengan minimal 8 karakter misalnya, dan harus terdiri dari huruf besar dan huruf kecil, angka, dan karakter khusus.
- Menerapkan algoritma hashing untuk menyimpan password sehingga tidak mudah dibongkar.
- Membatasi percobaan login yang gagal. Hal ini untuk mencegah pembobolan password dengan menggunakan metode brute-force attacks.



Password yang umum digunakan (sumber: omnicybersecurity.com)

Software and Data Integrity Failures

Kerentanan ini diakibatkan karena kegagalan keutuhan data dan perangkat lunak sehingga data tersebut tidak terlindungi dengan baik. Akibatnya penyerang dapat melakukan modifikasi data.

Kerentanan ini bisa membuka jalan untuk terjadinya injection seperti SQL injection atau bahkan Denial of Service.

Solusi dari kerentanan ini adalah dengan menggunakan tanda tangan digital atau mekanisme yang semisal untuk melakukan verifikasi pemutakhiran perangkat lunak. Selain itu gunakan komponen dari sumber-sumber yang terpercaya.

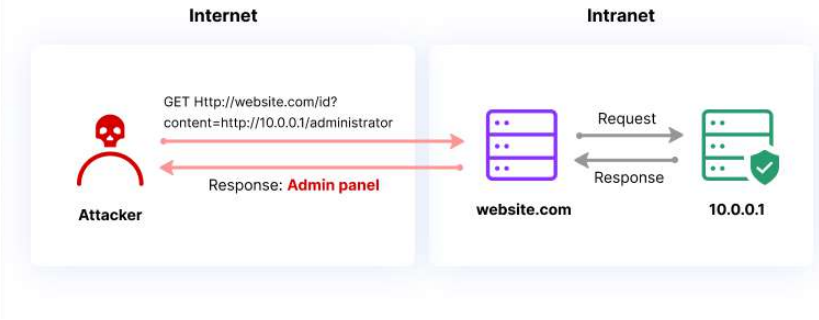
Security Logging and Monitoring Failures

Istilah ini dikenal dengan kegagalan pencatatan dan pemantauan keamanan. Hal ini bukan perkara sepele, mengingat kegagalan dalam hal ini berarti kegagalan dalam mengantisipasi adanya serangan yang akan terjadi di kemudian hari. Karena seharusnya interaksi dari luar dengan sistem yang kita miliki harus tercatat terutama yang berkaitan dengan keamanan.

Sedemikian pentingnya pencatatan keamanan ini menyebabkan sistem harus mencatat semua percobaan login yang terjadi ke sistem. Untuk kemudian dilakukan verifikasi siapa yang telah login, kapan dan di mana. Pencatatan tersebut baiknya tidak disimpan di satu server yang sama dengan aplikasi, tetapi disimpan terpisah untuk mengantisipasi bila terjadi hardware failure atau bencana.

Server-Side Request Forgery (SSRF)

Kerentanan ini terjadi bila seorang penyerang menyalahgunakan fungsi dari server untuk mengakses atau memodifikasi sumber daya. Penyerang menargetkan aplikasi pada server yang mendukung impor data melalui URL. Dengan URL yang telah disisipkan kode tertentu maka aplikasi pada sisi server akan mengeksekusi kode tersebut sesuai keinginan penyerang.



Server-side request forgery (sumber: imperva.com)

Akibat dari kerentanan ini bisa mengakibatkan pencurian data; eksekusi kode secara remote; atau bahkan denial of service.

Sebagai pencegahan dari kerentanan ini perlu dilakukan hardening pada aplikasi. Penerapan validasi dan sanitasi kode juga perlu diperhatikan. Selain itu perlu implementasi firewall.

Penetration Testing

Penetration testing atau disingkat dengan pentest adalah suatu simulasi serangan cyber yang menargetkan pada suatu sistem komputer tertentu dengan tujuan untuk menganalisa keamanan sistem tersebut. Penyerang yang melakukan simulasi serangan ini haruslah seorang yang telah diberi ijin atau kewenangan, sehingga tidak bisa sembarang orang bertindak dengan dalih melakukan penetration testing atas suatu website.

Penetration testing ini dilakukan dengan tujuan untuk mengidentifikasi kelemahan atau vulnerability pada suatu sistem. Dari kegiatan penetration testing ini bisa menjadi pengukuran tingkat keamanan suatu website. Daftar vulnerability yang dihasilkan untuk kemudian dilakukan analisa dan menutup celah-celah keamanan pada sistem itu. Kegiatan ini diharapkan dapat mengantisipasi resiko yang diakibatkan dari celah keamanan yang ada.

Untuk memperjelas posisi penetration hacking dalam tahapan hacking, kegiatan penetration testing ini berada pada tahap kedua yaitu scanning (perhatikan gambar di bawah ini). Tahap yang pertama adalah

reconnaissance atau footprinting. Tahapan ini merupakan tahapan pertama berupa pengumpulan informasi target sebanyak-banyaknya. Hal ini bisa dilakukan dengan active footprinting yaitu berinteraksi secara langsung dengan target sistem atau dengan passive footprinting yaitu mendapatkan informasi target tanpa berinteraksi dengan sistem target tetapi melalui media sosial, dokumen, laporan, dan sumber informasi publik yang lain.

Tahapan hacking (sumber: www.linkedin.com)

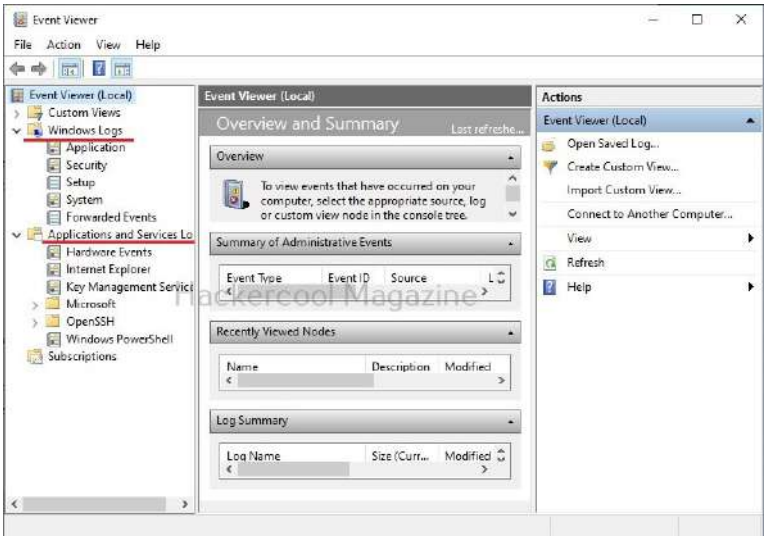
Tahapan yang kedua adalah scanning. Pada tahapan ini seorang hacker bisa menggunakan perangkat scanning untuk melakukan penetration testing sehingga diperoleh informasi tambahan yang lebih detail tentang target sistem.

Tahapan yang ketiga adalah gaining access. Yaitu berusaha untuk masuk ke dalam sistem target berdasarkan informasi yang telah diperoleh pada dua tahap sebelumnya.

Tahapan yang keempat dalah maintaining access. Sebagai mana namanya, tahap ini seorang hacker berusaha untuk tetap bisa masuk ke dalam

sistem, caranya di antaranya adalah dengan memasang trojan, backdoor, dll. Sehingga akses ke sistem target dapat dikuasai secara penuh.

Tahapan yang kelima adalah clearing tracks atau covering tracks. Tahapan ini bertujuan untuk menghapus jejak hacker di dalam sistem, karena proses masuk dan interaksi ke sistem tentu akan dicatat oleh sistem. Maka dari itu perlu bagi seorang hacker untuk menghapus jejak-jejak ini sehingga sistem target terlihat seolah tidak ada perubahan apa-apa seperti sedia kala. Tahapan ini mencakup menghapus cache, log file, cookies, menutup port yang dibuka, dll.



Event Viewer memperlihatkan semua log yang tercatat oleh sistem (hackercoolmagazine.com)

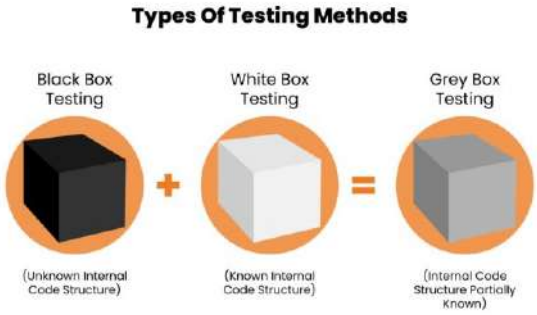
White-box, Black-box, atau Grey-box Testing

Dalam kaitannya dengan penetration testing, ada tiga istilah yang perlu dipahami terkait dengan kondisi sasaran yang akan diserang. Yang pertama adalah white-box testing, yaitu suatu metode atau cara penyerangan di mana informasi penyerang diketahui oleh penyerang.

Informasi tentang kondisi system yang akan diserang diberitahukan kepada penyerang, misalnya IP address, port yang dibuka, aplikasi dan plugin yang dipasang, bahasa pemrograman yang digunakan, dll. Sehingga penyerang telah terpapar dengan informasi sasaran sebanyak-banyaknya.

Metode penyerangan yang kedua adalah black-box testing. Dalam metode ini penyerang tidak mempunyai informasi yang banyak dengan objek yang akan diserang. Informasi yang ada bersifat minimal dan penyerang harus mencari informasi tentang objek yang akan diserang secara mandiri dan mencari celah informasi secara mandiri.

Metode yang ketiga adalah grey-box testing. Ini merupakan metode gabungan antara white-box dengan black-box. Dalam metode ini penyerang mendapatkan informasi awal atas objek yang akan diserang secara terbatas.



Black-box, white-box dan grey box (sumber: securityboulevard.com)

Perangkat yang Digunakan

Ada banyak perangkat atau tool yang bisa digunakan untuk melakukan penetration testing. Terbagi atas dua kelompok besar, yaitu:

Yang pertama adalah perangkat berbasis sistem operasi. Perangkat jenis ini merupakan paket banyak perangkat pada suatu sistem operasi. Sistem operasi tersebut memang dikhususkan untuk melakukan vulnerability assessment seperti penetration testing. Di antaranya adalah sistem operasi:

- BlackArch yang berdasarkan Arch Linux
- BackBox yang mendasarkan apda sistem operasi Ubuntu
- Kali Linux. Sebelumnya bernama BackTrack yang berdasarkan pada distribusi Debian
- WHAX, berdasarkan Slackware
- Parrot Security OS yang berdasarkan Debian
- Pentoo, yang berdasarkan Gentoo

Kali Linux (sumber: kali.org)

Yang kedua adalah perangkat berbasis perangkat lunak mandiri, yaitu:

- BackBox
- Hping
- Metasploit Project
- Nessus
- Nmap

- OWASP ZAP
- SAINT
- w3af
- Burp Suite
- Wireshark
- John the Ripper
- Hashcat

Penyediaan Perangkat VirtualBox

Virtualisasi dan VirtualBox

Oracle VM VirtualBox atau biasa disebut dengan VirtualBox merupakan perangkat lunak virtualisasi, artinya perangkat lunak tersebut digunakan untuk menjalankan suatu sistem operasi di dalam sistem operasi utama.

Virtualisasi sendiri diartikan sebagai suatu teknologi yang memungkinkan suatu komputer untuk berbagi sumber daya perangkat kerasnya dengan banyak lingkungan yang terpisah secara digital. Satu lingkungan virtual dapat dijalankan dengan menggunakan sumber daya yang telah dialokasikan, baik memori, processing dan storage. Dengan menggunakan teknologi virtualisasi seseorang dapat berpindah dari satu sistem operasi ke sistem operasi lain tanpa perlu melakukan booting ulang.

Umumnya istilah virtualisasi mengacu pada virtualisasi perangkat keras. Yaitu membuat suatu mesin virtual yang bekerja seperti layaknya sistem komputer lengkap dengan sistem operasinya.

Virtualisasi (sumber: openclipart.org)

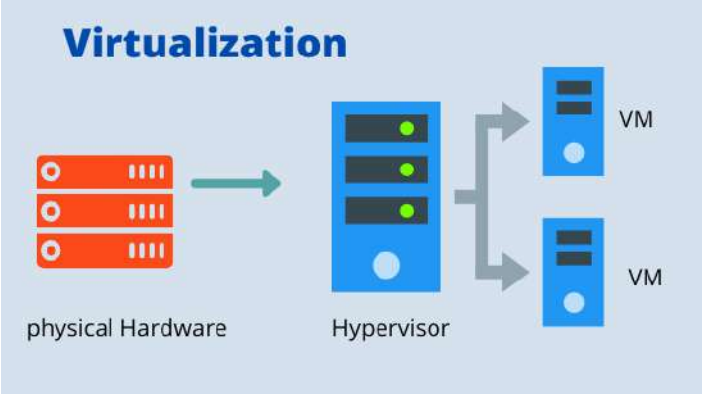
Manfaat Virtualisasi

Ada banyak manfaat virtualisasi yaitu:

1. Menghemat hardware dan daya listrik
   Dengan virtualisasi hanya dibutuhkan satu perangkat hardware yang sama dengan satu sumber daya listrik. Tidak perlu memperbanyak jumlah hardware dan sumber listrik sejumlah sistem yang akan dibuat.
2. Mempermudah proses backup dan recovery
   Dengan virtualisasi, akan mempermudah proses backup dan recovery. Karena operasi keduanya dilakukan pada satu sistem yang sama.
3. Mempermudah kegiatan monitoring
   Kegiatan monitoring dapat dilakukan secara terpusat untuk memantau banyak sistem-sistem yang sedang berjalan.
4. Mempermudah kegiatan kloning sistem

Kegiatan kloning sistem menjadi mudah karena dilakukan pada satu sistem induk yang tidak perlu berganti-ganti sistem.

5. Untuk kepentingan simulasi
   Kegiatan simulasi dapat dilakukan pada sistem virtualisasi yang telah disediakan, sehingga tidak perlu membuat sistem lingkungan yang baru. Misalnya ketika seseorang telah menggunakan sistem operasi dan ingin mencoba sistem operasi lain tanpa perlu kehilangan sistem operasi yang telah ada, maka dia bisa melakukan virtualisasi sebagai simulasi.

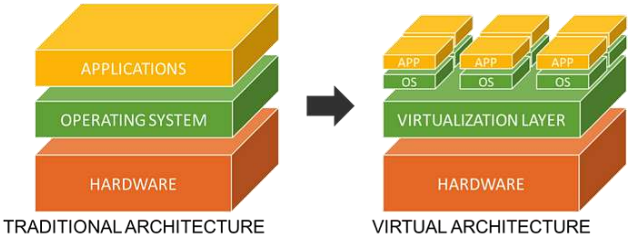


Konsep virtualisasi (sumber: gt-emea.com)

Jenis Virtualisasi

Sebenarnya ada beberapa jenis virtualisasi dilihat dari obyek yang di-virtual-kan. Ini jenis-jenisnya:

1. Virtualisasi aplikasi
2. Virtualisasi jaringan
3. Virtualisasi server
4. Virtualisasi data
5. Virtualisasi desktop



Operating System berada di atas virtualisasi (sumber: aliya-fatima.medium.com)

Beberapa Perangkat Virtualisasi

Beberapa perangkat virtualisasi yang dapat dicoba dijelaskan berikut ini:

1. VirtualBox

   VirtualBox merupakan perangkat virtualisasi yang dikeluarkan oleh Oracle dengan berbasis pada prosessor x86 dan AMD64. Perangkat ini bersifat open souce dan didistribusikan di bawah lisensi GNU General Public License (GPL).

   Dengan VirtualBox memungkinkan Anda untuk menjalankan virtual machine pada sistem operasi induk. VirtualBox tersedia untuk versi Windows, Linux, Mac OS, juga Oracle Solaris.

Logo VirtualBox (sumber: siliconangle.com)

2. VMware Workstation

Perangkat ini merupakan besutan dari perusahaan VMware Inc. Tersedia untuk sistem operasi Windows dan Linux dengan basis prosessor x64. Selain itu tersedia dalam lisensi freeware dan commercial. Rilis pertama kali pada bulan Mei 1999.

Logo VMWare (sumber: medium.com)

3. QEMU

QEMU merupakan singkatan dari Quick Emulator. Sebenarnya perangkat ini merupakan emulator yang memungkinkan untuk menjalankan sistem operasi yang ada di dalamnya. QEMU dapat berjalan pada basis x64, ARM, PowerPC, dll.

QEMU yang dibangun dengan bahasa C ini sendiri berlisensi GPL versi 2 dan dapat berjalan pada sistem operasi Linux, Microsoft Windows, Mac OS, dll.

Logo QEMU (sumber: icon-icons.com)

4. KVM

   KVM merupakan singkatan dari Kernel-based Virtual Machine yang merupakan perangkat virtualisasi yang bersifat open-source. Dikembangkan oleh komunitas Linux Kernel dan berlisensi GNU GPL.

   KVM berjalan pada sistem operasi Unix-like dan berjalan di atas plaform x86. Untuk melakukan konfigurasi diperlukan skill ekstra, maka dari itu KVM tidak disarankan untuk pengguna yang masih pemula.

   KVM tersedia di distribusi Linux sejak tahun 2007. KVM ini menjadi acuan bagi yang mengandalkan performa tinggi, keamanan dan stabilitas.

Logo KVM (sumber: qwords.com)

5. Hyper-V

   Hyper-V merupakan perangkat Windows Server Virtualization yang dikembangkan oleh Microsoft. Digunakan untuk membuat mesin virtual pada platform x86-64 yang menjalankan sistem operasi Windows.

   Hyper-V dirilis pertama kali pada Juni 2008 dalam paket Windows Server 2008.

Logo Hper-V (sumber: www.wjengland.com)

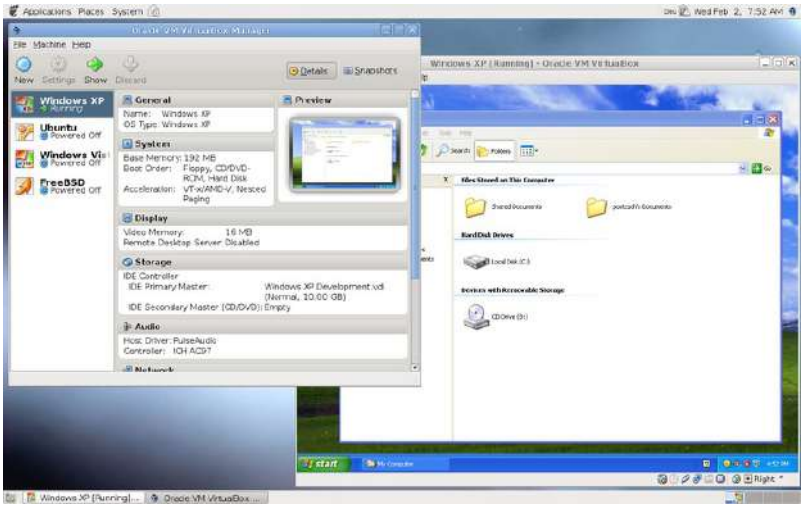
Lebih Lanjut tentang VirtualBox

Saat ini VirtualBox dapat berjalan pada sistem operasi Windows, Linux, Mac OS, Solaris. Semua sistem operasi tersebut bisa disebut sistem operasi host. Sedangkan untuk sistem operasi tamu (guest operating systems) yang dapat dijalankan di VirtualBox adalah:

- Windows (termasuk di dalamnya adalah NT 4.0, 2000, XP, Server 2003, Vista, 7, 8, Windows 10 and Windows 11),

- DOS/Windows 3.x,
- Linux (2.4, 2.6, 3.x, 4.x, 5.x and 6.x),
- Solaris and OpenSolaris,
- OS/2,
- OpenBSD,
- NetBSD,
- FreeBSD.

Untuk mengunduh VirtualBox dapat diperoleh pada alamat ini https://www.virtualbox.org/wiki/Downloads. Saat ini yang tersedia adalah VirtualBox versi 7.0.18.



VirtualBox dengan beberapa sistem operasi (sumber: virtualbox.org)

Gambar di atas memperlihatkan sistem operasi Linux sedang menjalankan VirtualBox dan dengan VirtualBox tersebut menjalankan sistem operasi Windows XP. Menarik *bukan*? Dengan VirtualBox, kita dapat menjalankan suatu sistem operasi lain di dalam sistem operasi induk.

Pada bagian lain di buku ini dijelaskan cara menjalankan Kali Linux pada sistem operasi Windows. Dengan pertimbangan bahwa umumnya pengguna komputer di Indonesia menggunakan sistem operasi Windows.

Sedangkan Kali Linux merupakan sistem operasi yang memuat banyak perangkat hacking yang tergolong handal.

Untuk dapat menjalankan VirtualBox, sebuah komputer harus memenuhi persyaratan sebagai berikut:

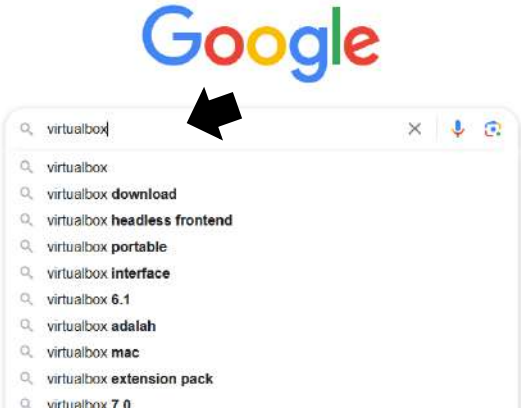
- Menggunakan perangkat keras x86. Komputer dengan prosessor Intel atau AMD sudah memenuhi syarat ini.
- Minimalnya membutuhkan RAM 512 MB, tergantun dari sistem operasi yang akan dipasang di VirtualBox, bisa melebihi kebutuhan memori 512 MB.
- Aplikasi VirtualBox sendiri hanya membutuhkan ruang harddisk sekitar 107 MB untuk versi 7.0.18.

Untuk proses instalasi perangkat VirtualBox akan dijelaskan di bagian lain dari buku ini.

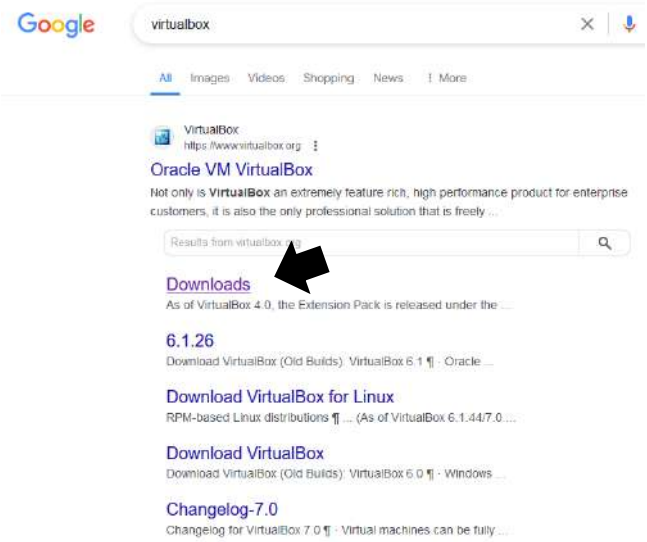
Mengunduh dan Melakukan Instalasi VirtualBox

Ikuti langkah-langkah di bawah ini untuk mengunduh dan melakukan instalasi Oracle VM VirtualBox:

1. Jalankan browser dan buka situs Google.
2. Ketik '**virtualbox**' pada kotak pencarian.

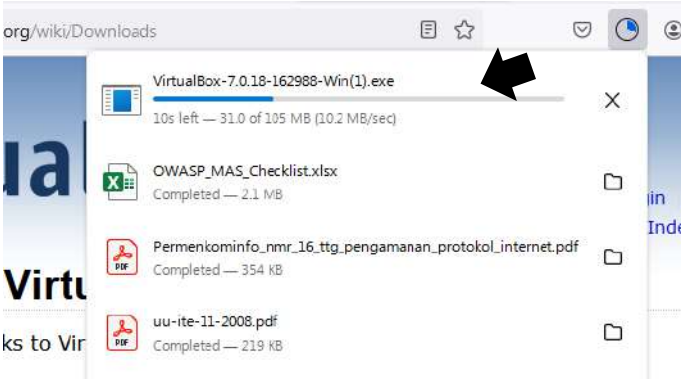


3. Akan tampil hasil pencarian.
4. Pada halaman hasil pencarian, yaitu di bagian VirtualBox, klik tautan **Downloads**.

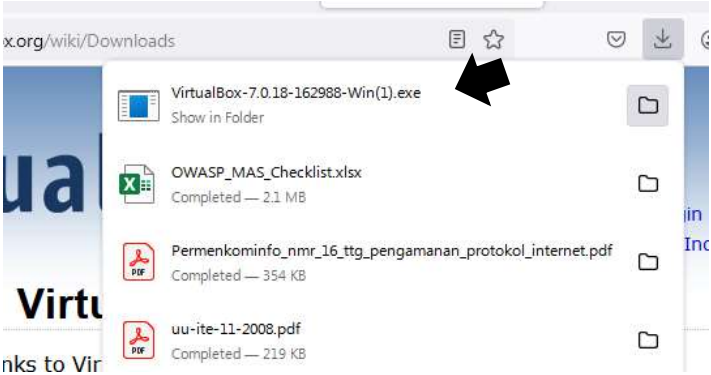


5. Akan tampil halaman Download VirtualBox.

6. Klik tautan **Windows hosts**. Dengan demikian kita akan mengunduh VirtualBox yang akan dipasang pada sistem operasi Windows. Proses unduh akan berlangsung beberapa saat. Tunggulah sampai selesai.

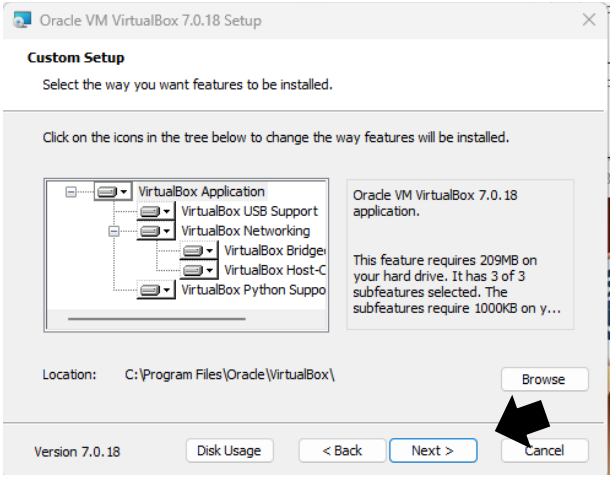


7. Setelah proses unduh selesai, klik pada file unduhan VirtualBox.



8. Akan tampil kotak dialog Wizard untuk proses instalasi VirtualBox. Klik tombol **Next** untuk memulai proses instalasi.

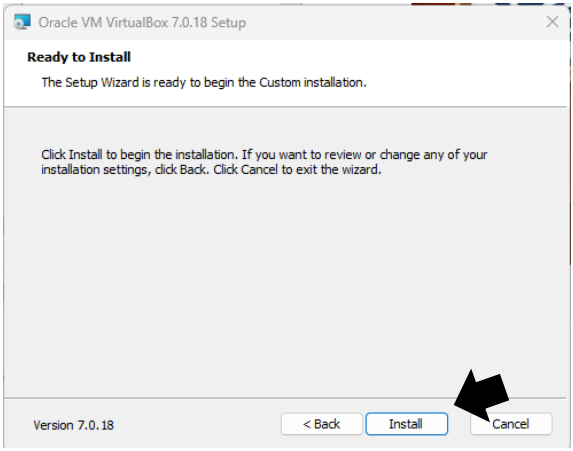
9. Akan tampil kotak dialog Custom Setup. Pada bagian ini kita dapat melakukan kustomisasi atau perubahan fitur-fitur yang akan diinstal. Bila kita tidak ingin pusing, cukup biarkan sesuai custom bawaan, dan klik saja tombol **Next**.



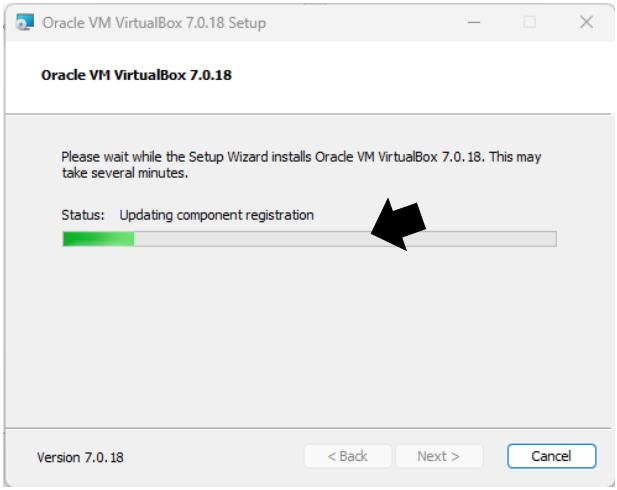
10. Bila tampil kotak dialog Warning tetang network interface, abaikan saja dan klik tombol **Yes**.

11. Bila tampil kotak dialog Missing Dependencies seperti di bawah ini, abaikan saja dan klik tombol **Yes**.

12. VirtualBox siap melakukan instalasi. Klik tombol **Install**.

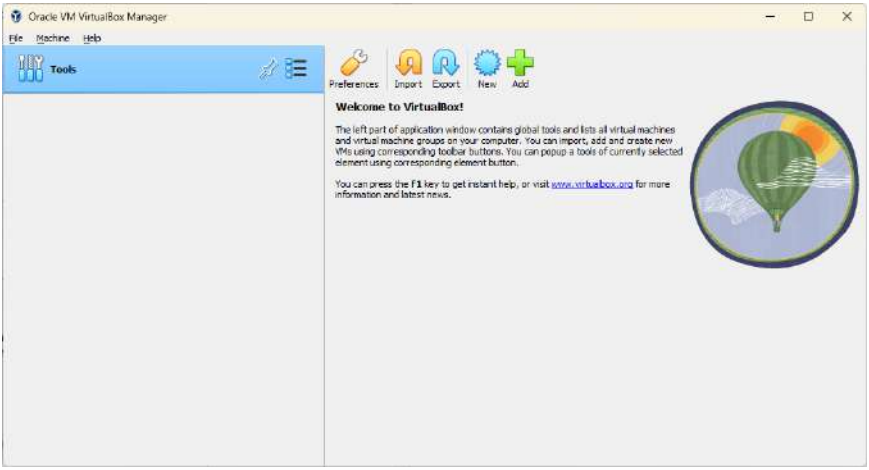


13. Proses instalasi akan berlangsung beberapa saat. Tunggu sampai proses tersebut selesai.



14. Proses instalasi selesai dengan tampilnya kotak dialog instalation is complete. Klik tombol **Finish**.

15. Akan tampil jendela aplikasi VirtualBox di layar monitor, dengan demikian proses instalasi telah selesai dan berhasil.

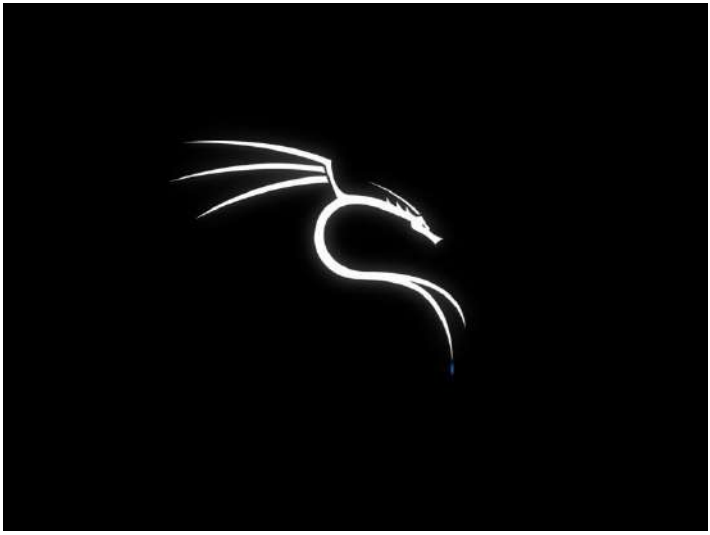


Penyediaan Perangkat Kali Linux

Kali Linux: Sistem Operasi Khusus Hacking

Kali Linux merupakan sistem operasi yang bersifat *open source* yang merupakan distribusi Linux yang khusus digunakan untuk melakukan kegiatan keamanan informasi. Kegiatan keamanan informasi tersebut di antaranya penetration testing, *digital forensics*, riset keamanan dan *reverse engineering*. Dikembangkan oleh suatu lembaga yang bernama Offensive Security. Offensive Security merupakan sebuah perusahaan internasional berbasis di New York, Amerika Serikat yang bergerak di bidang keamanan informasi*, penetration testing*, dan *digital forensics*.

Kali by Offensive Security (sumber: www.ifixit.com)

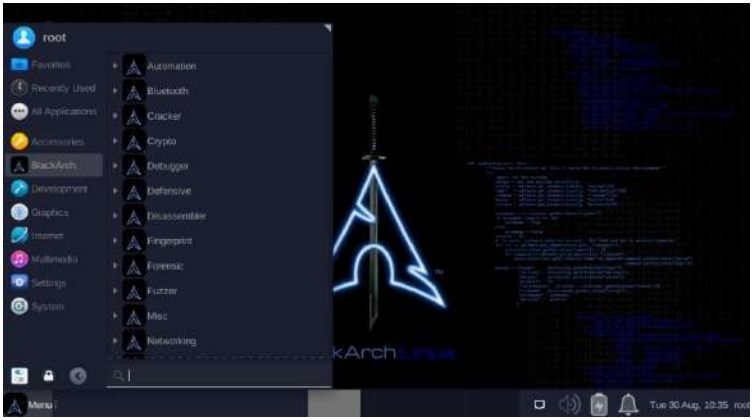


Logo naga pada Kali Linux (sumber: unix.stackexchange.com)

Kali Linux resmi dirilis pada 13 Maret 2013 yang merupakan turunan dari distribusi Debian. Maka tidak aneh pula bila banyak repositori di Kali Linux merupakan bawaan dari repositori Debian. Kali Linux versi *full* setidaknya memuat 600an perangkat keamanan informasi yang terbagi dalam beberapa *genre* atau jenis penggunaan.

Dengan pengkhususan sebagai sistem operasi untuk keamanan informasi, maka tepatlah bila seseorang yang ingin menekuni dunia hacking atau keamanan informasi untuk mempunyai dan memasang Kali Linux pada komputernya. Kali Linux dapat digunakan sebagai laboratorium untuk pengujian-pengujian keamanan informasi.

Kali Linux dikembangkan khusus untuk kegiatan keamanan informasi, meski ada pula distribusi Linux yang lain yang dapat digunakan untuk penetration testing seperti Parrot OS yang mengkhususkan pada bidang security dan privacy. Selain itu ada pula distribusi BlackArch dan Wifislax.



Sistem operasi BlackArch Linux (sumber: www.makeuseof.com)

Distribusi Wifislax dapat digunakan untuk menganalisa kerentanan pada jaringan wifi.

Sistem operasi Wifislax (sumber: www.wifi-antennas.com)

Untuk menjalankan Kali Linux diperlukan kebutuhan hardware sebagai berikut:

- Prosessor Intel atau AMD.
- Kebutuhan ruang harddisk minimal sekitar 20 GB, meskipun ini tergantung dari versi Kali Linux yang akan diinstal.
- Minimal 2 GB RAM.

(Sumber: www.kali.org)

Beberapa Tool untuk Hacking di Kali Linux

Ada lebih dari 600 perangkat di Kali Linux yang dapat digunakan untuk kegiatan keamanan informasi. Berikut ini daftar perangkat keamanan informasi pada Kali Linux yang dikelompokkan berdasarkan jenis kegunaannya.

01 Information Gathering

- DNS Analysis
    - Dnsenum

    - Dnsmap
    - Dnsrecon
    - fierce
- IDS/IPS Identification
    - Lbd
    - Wafw00f
- Live Host Identification
    - Arping
    - Fping
    - Hping3
    - Masscan
    - Netcat
    - Thcping6
    - unicornscan
- Network & Port Scanners
    - Masscan
    - Nmap
    - unicorn
- OSINT Analysis
    - Maltego
    - Spiderfoot
    - Spiderfoot-cli
    - theharvester
- Route Analysis
    - Netdiscover
    - netmask
- SMB Analysis
    - Enum4linux
    - Nbtscan
    - smbmap
- SMTP Analysis
    - Smtp-user-enum
    - Swaks

- SNMP Analysis
    - Onesixtyone
    - Snmp-check
- SSL Analysis
    - Ssldump
    - Sslh
    - sslyze
- Amass
- Dmitry
- Ike-scan
- Legion
- Maltego
- Netdiscover
- Nmap
- Recon-ng
- spiderfoot

02 Vulnerability Analysis

- Fuzzing Tools
    - Spike-generic_chunked
    - Spike-generic_listen_tcp
    - Spike-generic_send_tcp
    - Spike-generic_send_udp
- VoIP Tools
    - voiphopper
- Legion
- Nikto
- Nmap
- Unix-privesc-check

03 Web Application Analysis

- CMS & Framework Identification
  - wpscan
- Web Application Proxies
  - burpsuite
- Web Crawlers & Directory Brut
  - Cutycapt
  - Dirb
  - Dirbuster
  - Ffuf
  - wfuzz
- Web Vulnerability Scanners
  - Cadaver
  - Davtest
  - Nikto
  - Skipfish
  - Wapiti
  - Whatweb
  - Wpscan
- Burpsuite
- Commix
- Skipsifh
- Sqlmap
- Webshells
- Wpscan

04 Database Assessment

- SQLite database browser
- Sqlmap

- Offline Attacks
    - Chntpw
    - Hashcat
    - Hashid
    - Hash-identifier
    - John
    - Ophcrack-cli
    - Samdump2
- Online Attacks
    - Hydra
    - Hydra-graphical
    - Medusa
    - Ncrack
    - Onesixtyone
    - Patator
    - Thc-pptp-bruter
- Passing the Hash Tools
    - Crackmapexec
    - Evil-winrm
    - Impacket
    - Mimikatz
    - Pth-curl
    - Pth-net
    - Pth-rpcclient
    - Pth-smbclient
    - Pth-smbget
    - Pth-sqsh
    - Pth-winexe
    - Pth-wmic
    - Pth-wmis
    - Pthxfreerdp
    - smbmap

- Password Profiling & Wordlists
    - Cewl
    - Cruch
    - Rsmangler
    - Wordlists
- Cewl
- Crunch
- Hashcat
- Hydra
- John
- Medusa
- Ncrack
- Ophcrack
- Wordlists

06 Wireless Attacks

- 802.11 Wireless Tools
    - Bully
    - Fern wifi cracker (root)
- Bluetooth Tools
    - spooftooph
- Aircrack-ng
- Fern wifi cracker (root)
- Kismet
- Pixiewps
- Reaver
- wifite

07 Reverse Engineering

- clang

- clang++
- NASM shell
- Radare2

08 Exploitation Tools

- Crackmapexec
- Metasploit framework
- Msf payload creator
- Searchsploit
- Social engineering toolkit (root)
- sqlmap

09 Sniffing & Spoofing

- Network Sniffers
    - Dnschef
    - Dsniff
    - Netsniff-ng
- Spoofing & MITM
    - Dnschef
    - Rebind
    - Sslsplit
    - tcpreplay
- Ettercap-graphical
- Macchanger
- Minicom
- Mitmproxy
- Netsniff-ng
- Responder
- Scapy
- Tcpdump

- Wireshark

10 Post Exploitation

- OS Backdoors
  - Dbd
  - Powersploit
  - sbd
- Tunneling & Exfiltration
  - Dbd
  - Dns2tcpc
  - Dns2tcpd
  - Exe2hex
  - Iodine
  - Miredo
  - Proxychains4
  - Proxytunnel
  - Ptunnel
  - Pwnat
  - Sslh
  - Stunnel4
  - udptunnel
- Web Backdoors
  - Laudanum
  - weevely
- Evil-winrm
- Exe2hex
- Impacket
- Mimikatz
- Netcat
- Powershell empire
- Powersploit
- Proxychains4

- Starkiller
- Weevely

11 Forensics

- Forensic Carving Tools
    - Magicrescue
    - Scalpel
    - Scrounge-ntfs
- Forensic Imaging Tools
    - Guymager (root)
- PDF Forensics Tools
    - Pdfid
    - Pdf-parser
- Sleuth Kit Suite
    - Autopsy (root)
    - Blkcalc
    - Blkcat
    - Blkls
    - Blkstat
    - Ffind
    - Fls
    - Fsstat
    - Hfind
    - Icat-sleuthkit
    - Ifind
    - Ils-sleuthkit
    - Img_cat
    - Img_stat
    - Istat
    - Jcat
    - Jls
    - Mactime-sleuthkit

    - Mmcat
    - Mmls
    - Mmstat
    - Sigfind
    - Sorter
    - Srch_strings
    - Tsk_comparedir
    - Tsk_gettimes
    - Tsk_loaddb
    - Tsk_recover
- Autopsy (root)
- Binwalk
- Bulk_extractor
- Hashdeep

12 Reporting Tools

- CherryTree
- Cutycapt
- Faraday start
- Maltego
- Pipal
- Recordmydesktop

13 Social Engineering Tools

- Maltego
- Msf payload creator
- Social engineering toolkit (root)

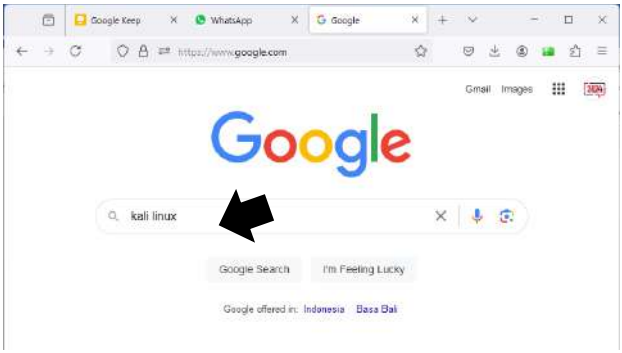
42 Kali & Offset Links

- Exploit Database
- Kali Bugs
- Kali Docs
- Kali Forums
- Kali Linux
- Kali Tools
- NetHunter
- Offset Training
- VulnHub

Mengunduh Kali Linux

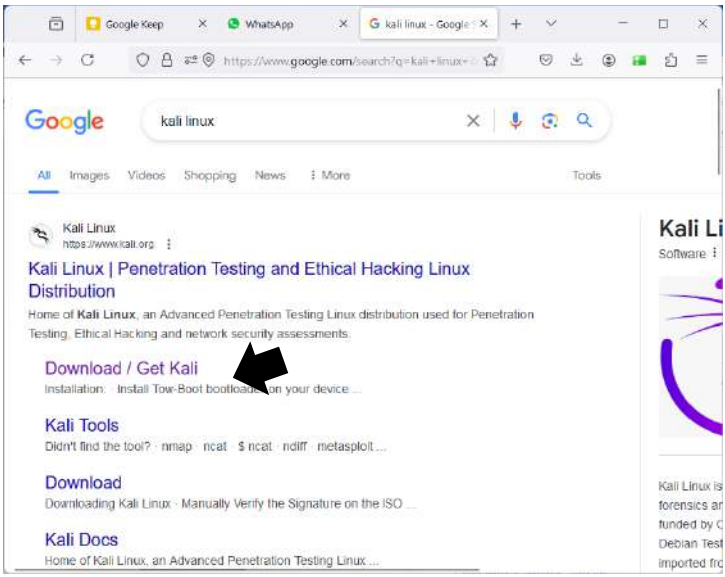
Kali Linux yang akan diunduh di sini adalah yang akan dijalankan pada VirtualBox. Untuk mengunduh Kali Linux ini ikuti langkah-langkah di bawah ini:

1. Jalankan browser dan arahkan ke Google.
2. Ketik Kali Linux pada kotak pencarian Google.

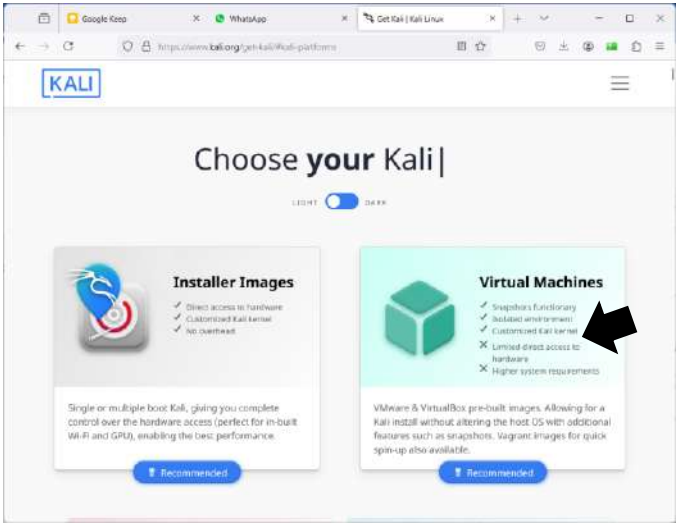


Mencari alamat situs Kali Linux

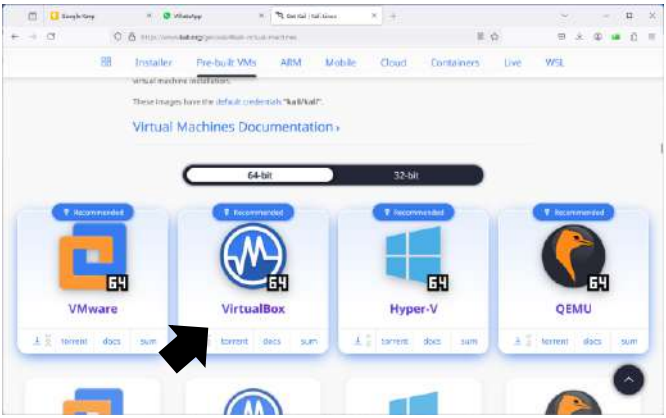
3. Pada halaman pencarian yang tampil, klik Download/ Get Kali.



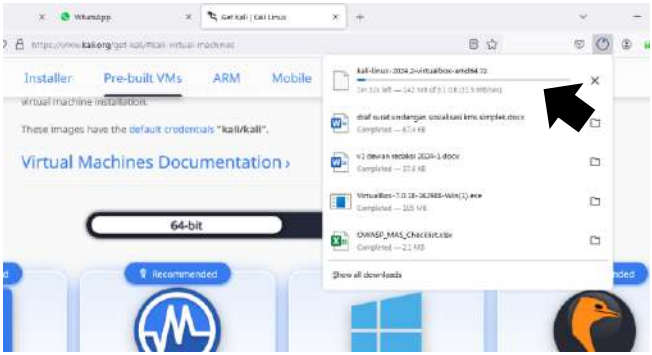
4. Akan tampil halaman situs Kali Linux. Klik pada bagian Virtual Machines, karena kita akan mengunduh Kali Linux untuk dipasang pada VirtualBox.



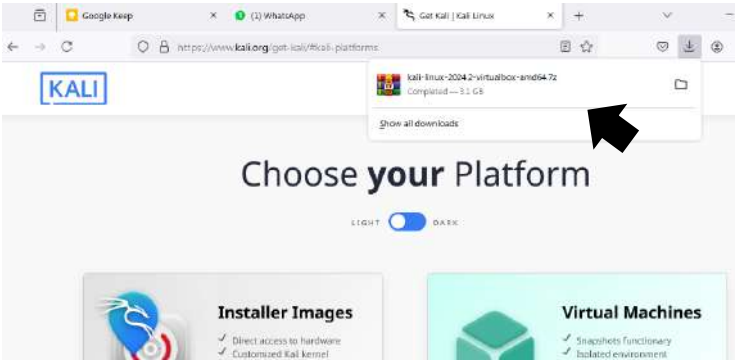
5. Pada halaman berikutnya klik pada logo VirtualBox, karena yang akan diunduh adalah Kali Linux untuk VirtualBox.



6. Proses unduh akan berlangsung beberapa saat, tunggu sampai proses unduh selesai.



7. Bila proses unduh selesai dapat dilihat pada bagian unduh di browser yang digunakan.

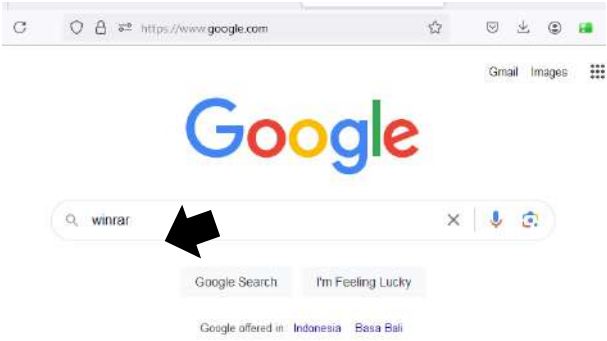

Google Keep
(1) WhatsApp
Get Kali | Kali Linux
https://www.kali.org/get-kali/#kali-platforms
KALI
kali-linux-2024.2-virtualbox-amd64.7z
Completed — 3.1 GB
Show all downloads
Choose your Platform
LIGHT
DARK
Installer Images
Direct access to hardware
Customized Kali kernel
Virtual Machines
Snapshots functionary
Isolated environment

Mengunduh dan Melakukan Instalasi WinRAR

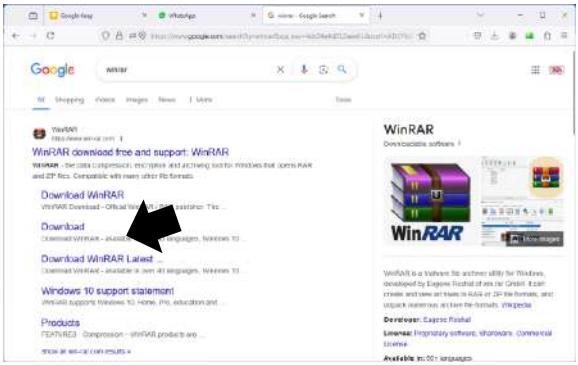
File Kali Linux yang telah kita unduh pada bagian sebelumnya adalah dalam bentuk archive. Sebelum dapat digunakan harus dilakukan ekstraksi terlebih dahulu. Ada banyak aplikasi untuk melakukan ektraksi file archive ini, di antarnya adalah WinRAR, 7-Zip, WinZip, PeaZip, Bandizip, The Unarchiver, IZArc, Universal Extractor, FreeARC, HaoZip, dll.

Pada buku ini dijelaskan cara mendapatkan dan melakukan instalasi aplikasi WinRAR. Meski demikian Anda bisa menggunakan aplikasi yang lain. Inilah langkah-langkahnya:

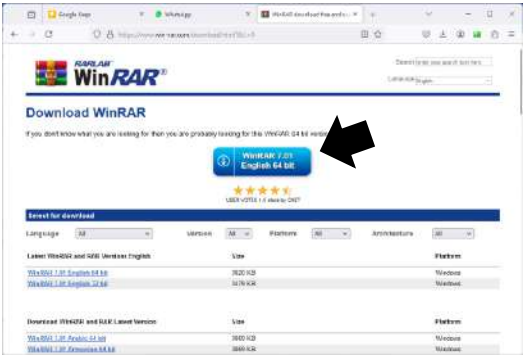
1. Jalankan browser dan arahkan ke Google.
2. Pada halaman Google yang tampil, ketik 'Winrar'.



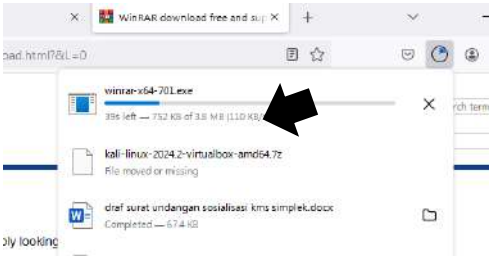
3. Pada halaman yang tampil, klik tautan Download WinRAR.



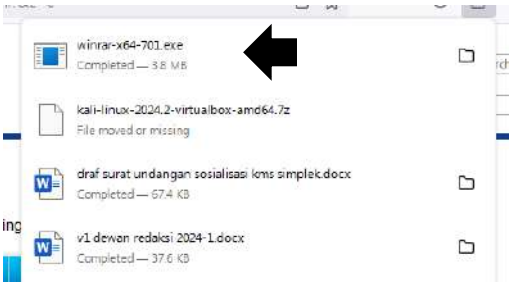
4. Akan tampil halaman situs WinRAR. Untuk mengunduhnya klik pada tombol berwarna biru bertuliskan WinRAR 7.01 English 64 bit.



5. Proses unduh akan berlangsung beberapa saat. Tunggu sampai selesai.

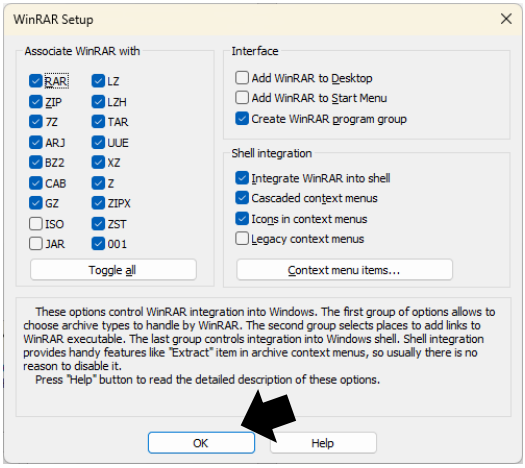


6. Bila proses unduh selesai, klik file unduhan tersebut.

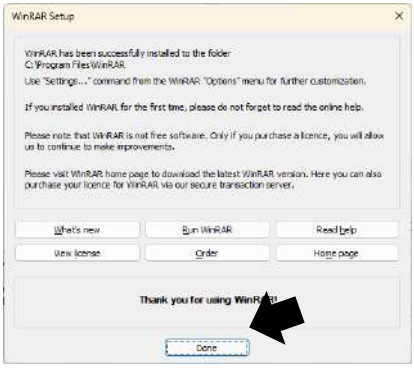


7. Akan tampil jendela aplikasi instalasi WinRAR. Klik saja tombol Install.

8. Pada kotak dialog yang tampil, tentukan jenis file-file archive yang akan dibuka secara otomatis dengan WinRAR. Bisa juga kita biarkan opsi yang ada sesuai bawaan WinRAR. Klik tombol OK.



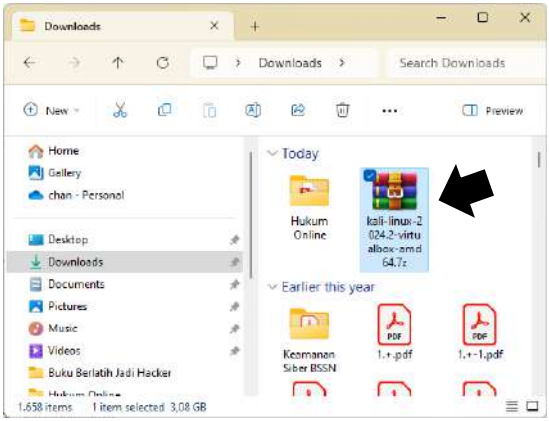
9. Proses instalasi akan berlangsung beberapa saat. Bila proses instalasi selesai akan tampil kotak dialog seperti di bawah ini. Klik saja tombol Done.



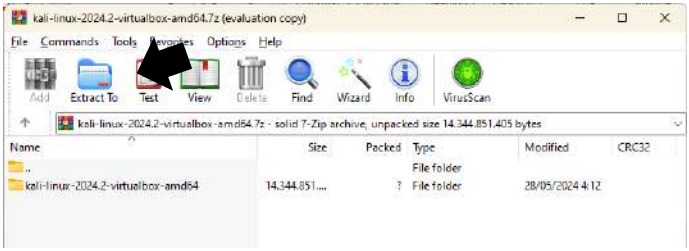
Mengekstrak File Kali Linux

Setelah proses instalasi WinRAR pada bagian terdahulu selesai, kita dapat melakukan ekstraksi file Kali Linux yang masih dalam bentuk file archive. Ikuti langkah-langkah di bawah ini:

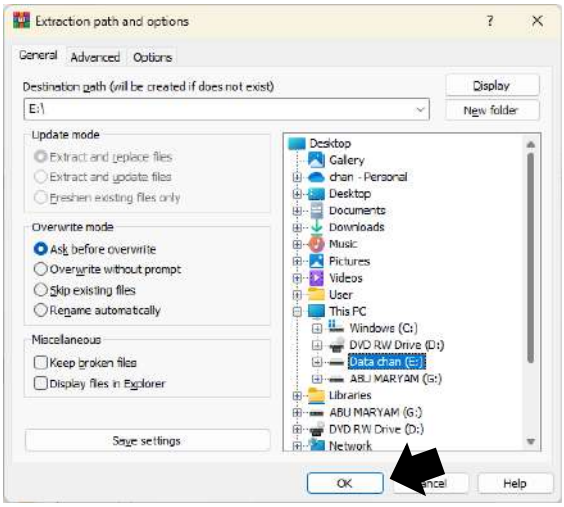
1. Carilah file Kali Linux yang telah kita unduh. Klik ganda pada file tersebut.



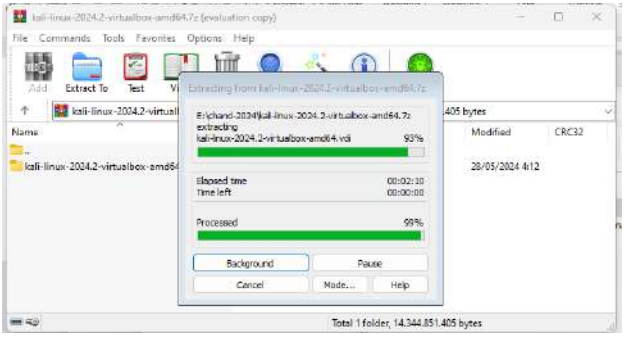
2. File tersebut akan dibuka secara otomatis dengan WinRAR. Klik tombol Extract To yang ada di bagian atas untuk mengekstraknya.



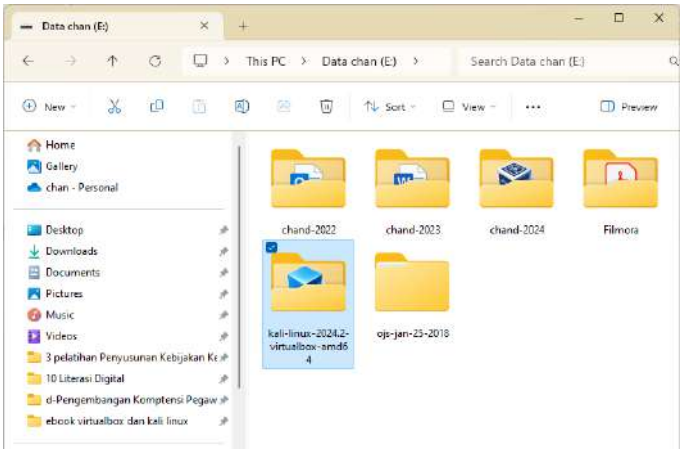
3. Akan tampil kotak dialog untuk menentukan path dan folder yang akan menjadi tempat mengekstrak file Kali Linux.



4. Kita bisa menentukan path dan folder yang akan menjadi tempat file ekstraksi tersebut. Klik tombol OK untuk memulai ekstraksi. Proses ekstraksi akan berlangsung beberapa saat, tunggulah sampai proses selesai.



5. Bila proses telah selesai, perhatikan bahwa akan ada folder baru dengan nama kali-linux-2024.2-virtualbox-amd64. Inilah folder tempat file ekstraksi Kali Linux berada.

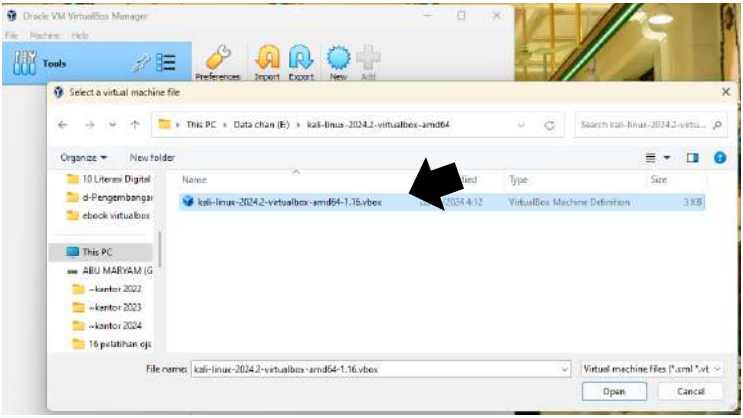


Menjalankan Kali Linux di VirtualBox

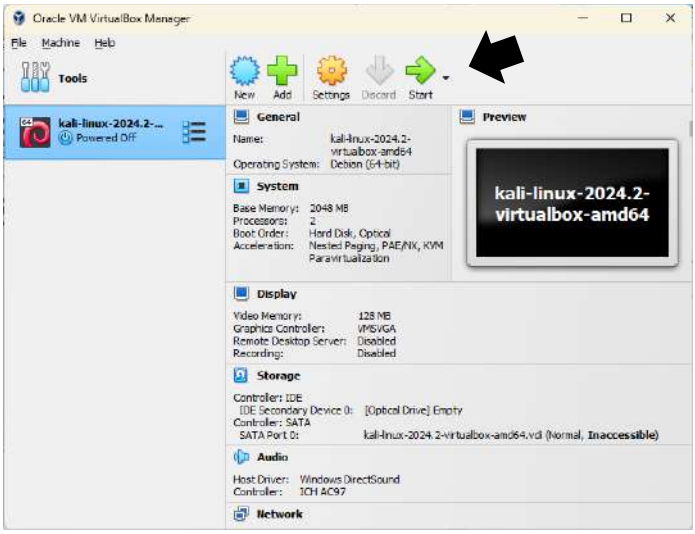
Untuk menjalankan Kali Linux di VirtualBox, inilah langkah-langkahnya:

1. Jalankan aplikasi VirtualBox.
2. Pada aplikasi VirtualBox yang tampil, klik tombol + yang berwarna hijau di bagian atas.

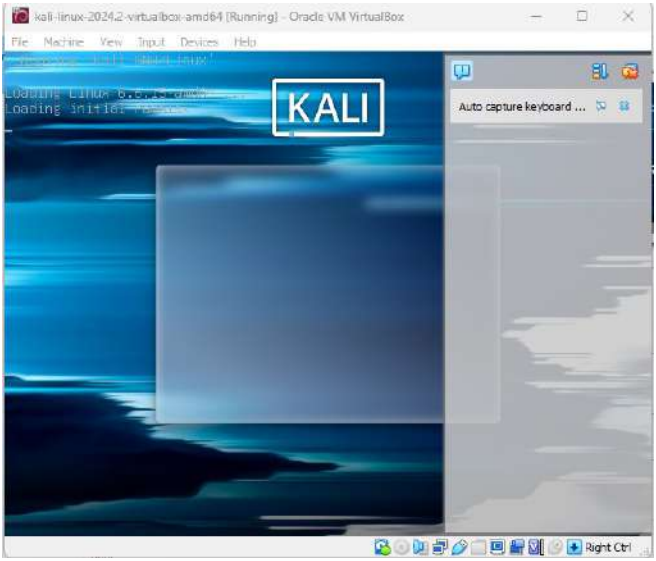
3. Akan tampil kotak dialog untuk memilih file virtual machine. Carilah file dengan jenis VirtualBox Machine Definition pada folder yang telah diekstrak pada bagian sebelum ini. Kemudian klik tombol Open.



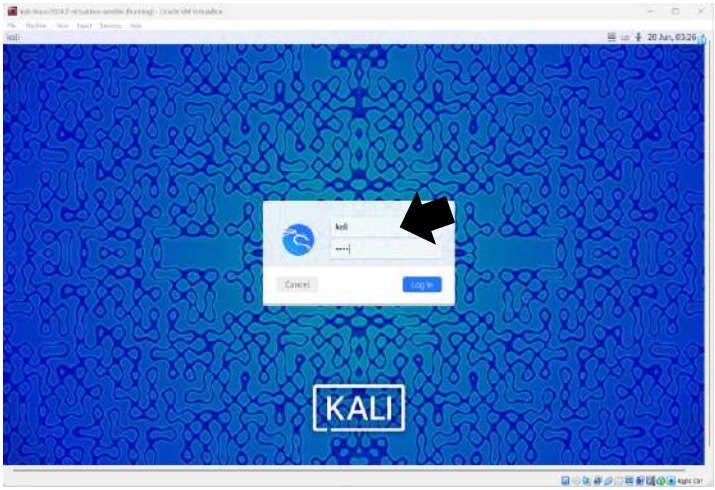
4. Dengan demikian file Kali Linux tersebut akan terintegrasi dengan aplikasi VirtualBox, seperti diperlihatkan pada gambar di bawah ini. Untuk mulai menjalankan sistem operasi Kali Linux, klik tombol Start berupa panah hijau yang ada di bagian atas.



5. Proses loading dan booting Kali Linux akan berlangsung. Tunggu beberapa saat sampai proses selesai dengan sempurna.

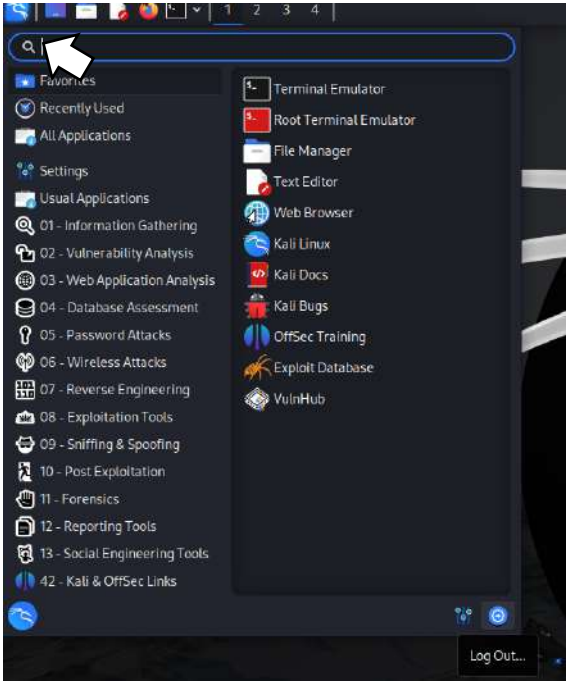


6. Akhirnya sistem operasi Kali Linux berhasil dijalankan. Tampilannya akan terlihat seperti gambar di bawah ini.

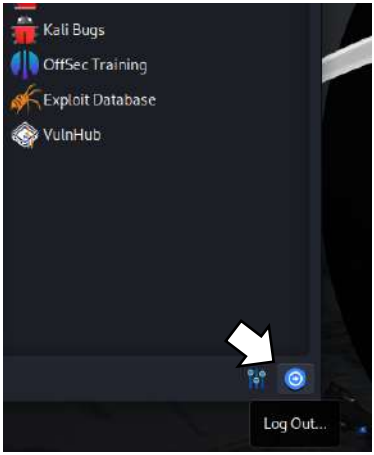


7. Untuk masuk ke dalam Kali Linux ketik 'kali' pada bagian username dan ketik 'kali' pada bagian kotak password. Ini adalah username dan password bawaan dari Kali Linux.
8. Akhirnya Anda dapat masuk ke desktop sistem operasi Kali Linux seperti terlihat pada gambar berikut ini.

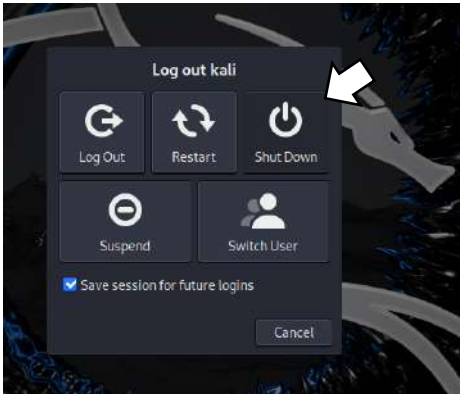
9. Klik pada tombol naga yang ada di pojok kiri atas berwarna biru. Akan tampil banyak aplikasi-aplikasi yang bisa kita gunakan untuk hacking, penetration testing, reserve engineering, dll. Penjelasan tentang cara pakai aplikasi-aplikasi ini akan dijelaskan pada bagian lain di buku ini.



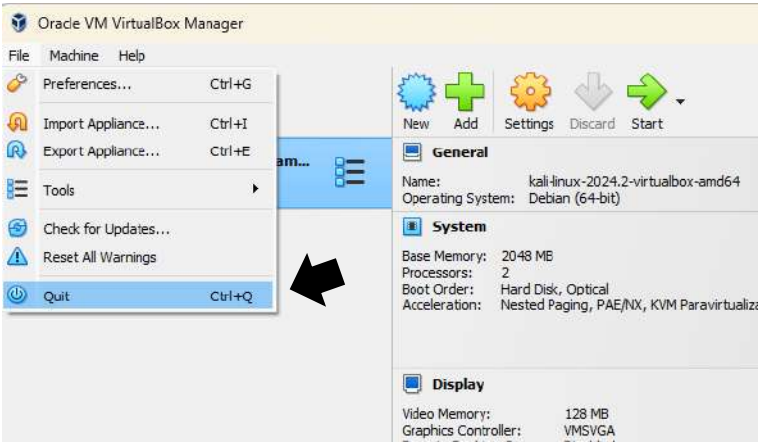
10. Untuk melakukan shutdown klik pada tombol naga berwarna biru di pojok kiri atas. Lanjutkan dengan mengklik tombol Log Out yang ada di pojok kanan bawah.



11. Akan tampil kotak dialog seperti gambar di bawah ini. Klik tombol Shut Down untuk mematikan Kali Linux.



12. Akan tampil bidang aplikasi VirtualBox. Untuk keluar dari VirtualBox klik menu File > Quit. Anda akan keluar dari VirtualBox.



Perangkat Hacking di Kali Linux

Menggunakan Nmap untuk Mengetahui Port yang Terbuka

Nmap merupakan singkatan dari *network mapper*, yang merupakan perangkat yang dapat digunakan untuk mengetahui kerentanan jaringan. Perangkat Nmap bersifat *open source*. Meski digunakan untuk mengetahui kerentanan jaringan, Nmap dapat digunakan untuk aktivitas harian seorang pengelola jaringan sebuah perusahaan.

Logo Nmap (sumber: nmap.org)

Dengan Nmap dapat diketahui port yang dalam kondisi open atau closed. Maksudnya dapat diketahui port mana saja yang terbuka (*listening*) atau

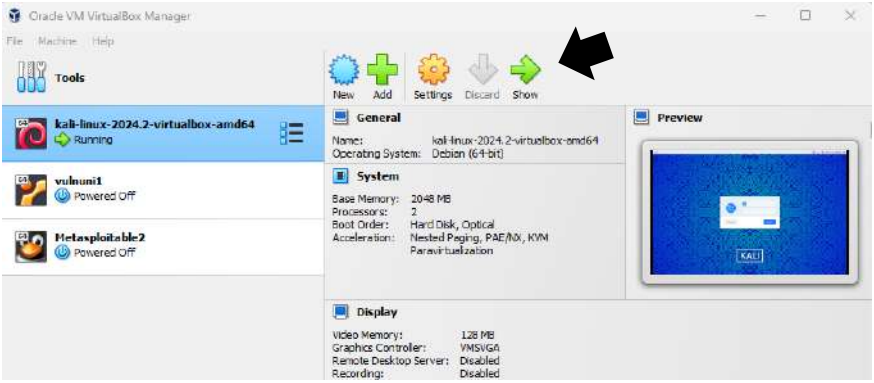
tertutup. Selain itu dengan Nmap dapat diketahui port mana saja yang dalam kondisi filtered. Maksudnya berada dibalik firewall, filter atau penghalang port yang lain.

Perintah yang paling sederhana untuk menggunakan Nmap adalah

```
Nmap <IP address/host target>
```

Berikut cara menggunakan Nmap di Kali Linux.

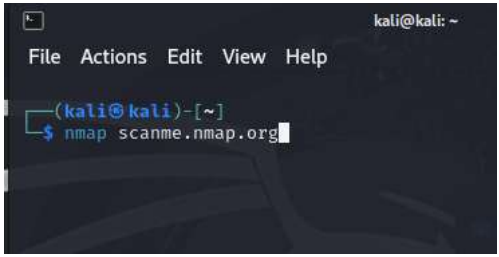
1. Jalankan Oracle VM VirtualBox Manager yang telah terpasang di komputer Anda.
2. Kemudian jalankan Kali Linux yang telah terpasang di VirtualBox. Klik panah hijau untuk menjalankannya.



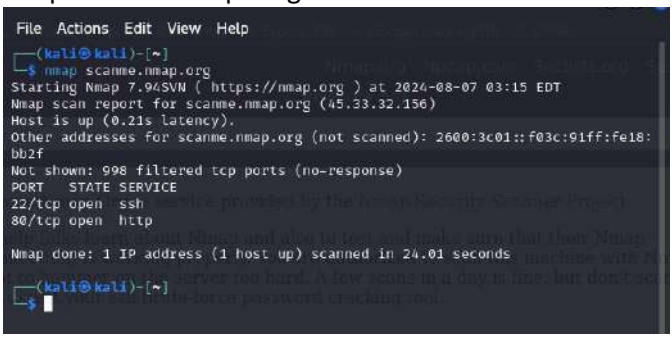
3. Setelah Kali Linux berjalan di VirtualBox. Lakukan login. Ketik ’kali’ di kotak Username dan ’kali’ di kotak Password.

4. Setelah login, jalankan Terminal Emulator.
5. Anda dapat melakukan testing penggunaan Nmap dengan melakukan scaning atas situs scanme.nmap.org. Ketikkan perintah berikut

```
nmap scanme.nmap.org
```



6. Akan didapatkan hasil seperti gambar di bawah ini.



Dari hasil tersebut terlihat bahwa url scanme.nmap.org sedang up.

Tanggal scanning adalah 07 Agustus 2024 pukul 03:15 waktu EDT.
IP address scanme.nmap.org adalah 45.33.32.156.
Ada sejumlah 988 port dalam kondisi filtered (no response).
Port 22 dan 80 dalam keadaan open.

7. Sekarang kita coba untuk melakukan scanning atas target yang sesungguhnya. Tentukan target Anda. Penulis telah menentukan target tersendiri yang tidak ditulis dalam buku ini. Akan tampil hasil seperti di bawah ini. Perhatikan.

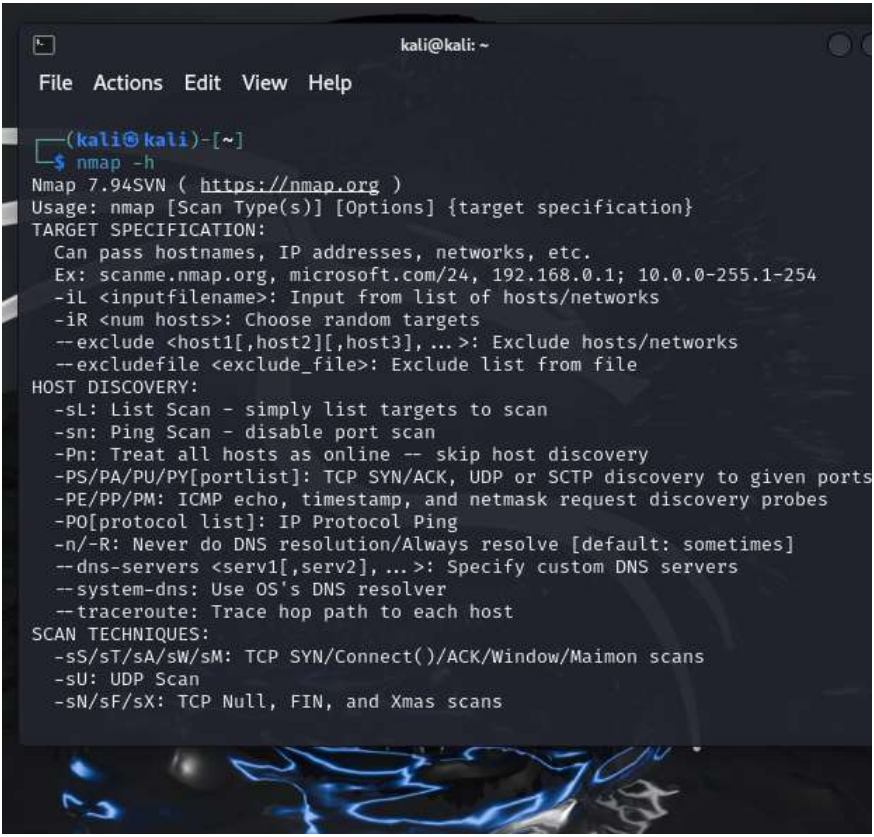
Cara membaca hasil tersebut adalah:
Baris a menunjukkan perintah yang Anda ketikkan.
Baris b menunjukkan tanggal dan waktu proses scanning berdasarkan waktu Eastern Daylight Time (EDT) yang bisa dikonversi ke waktu WIB.
Baris c akan menampilkan IP addres dari url yang Anda scan.
Baris D menunjukkan ada 998 port yang di-filtered karena bisa jadi berada di balik penghalang seperti firewall atau perangkat lainnya.
Baris e menunjukkan port 80 dan 443 dalam kondisi terbuka dan bisa dieksploitasi.
Baris f menunjukkan lama proses scanning.

Informasi-informasi inilah yang bisa didapatkan dari Nmap.

Untuk mengetahui opsi-opsi yang dalam dalam perintah nmap bisa menggunakan perintah ini

```
nmap -h
```

Akan dihasilkan daftar lengkap opsi-opsi untuk perintah nmap.



Selamat mencoba.

Menggunakan Wireshark untuk Mendapatkan Username dan Password Login

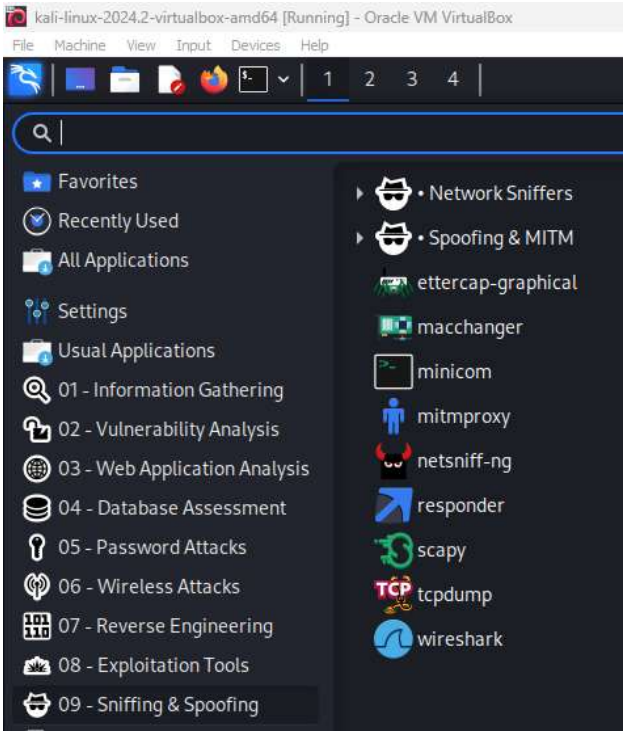
Wireshark merupakan perangkat lunak yang dapat digunakan untuk menganalisa lalu lintas jaringan, lebih khusus lagi dapat digunakan untuk menganalisa paket data yang melewati suatu jaringan. Penggunaannya pun harus dengan bijak. Pada awalnya aplikasi ini bernama Ethereal, kemudian berubah menjadi Wireshark pada bulan Mei 2006. Wireshark mudah digunakan karena aplikasi ini berbasis Graphical User Interface (GUI).

Logo Wireshark (sumber: logowik.com)

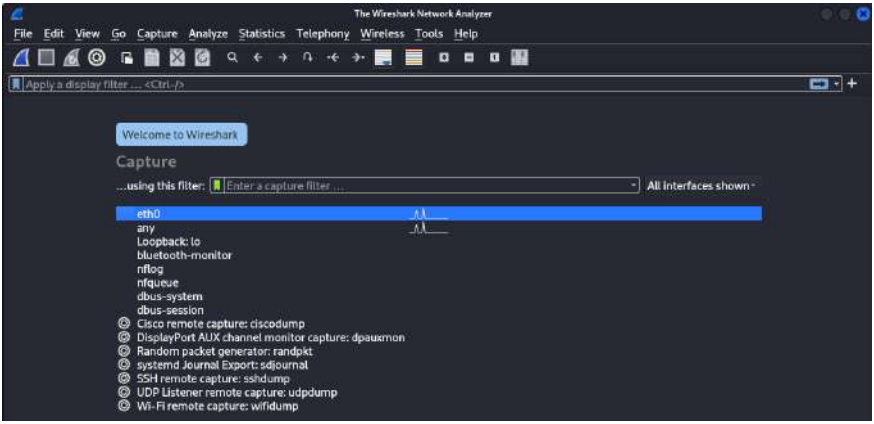
Berikut ini dijelaskan cara menggunakan Wireshark untuk mendapatkan username dan password dari aktifitas login yang dilakukan oleh seseorang. Apa yang dijelaskan di sini hanyalah untuk kepentingan belajar semata.

Inilah langkah-langkahnya:

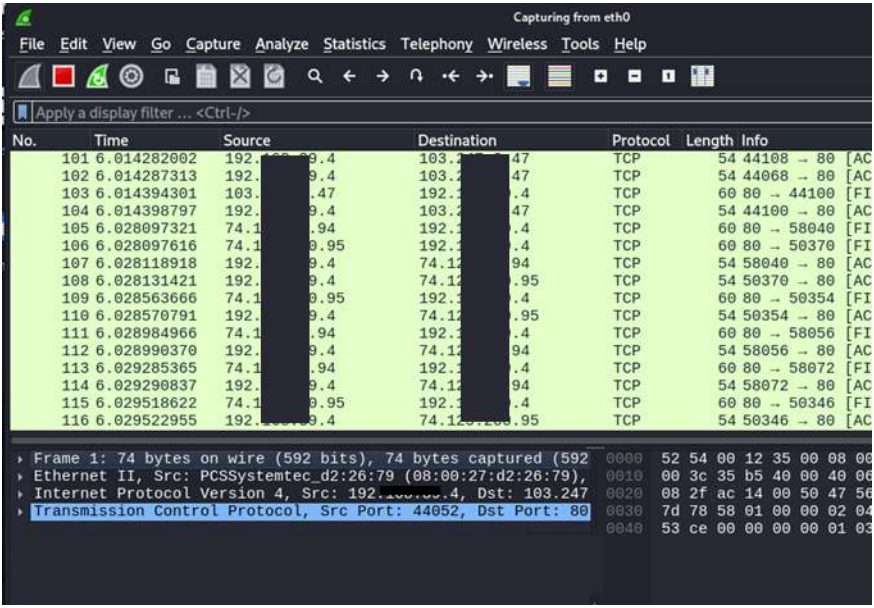
1. Setelah Kali Linux berhasil dijalankan, klik pada logo Kali Linux yang ada di pojok kiri atas, kemudian sorot pada menu Sniffing & Spoofing. Lanjutkan dengan memilih menu wireshark.



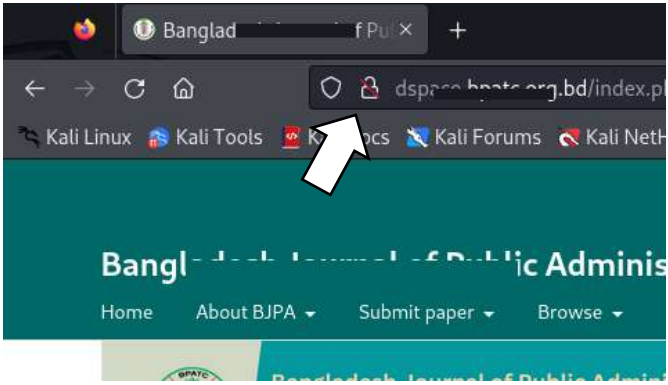
2. Akan tampil aplikasi Wireshark seperti gambar di bawah ini. Untuk memulai bisa dengan mengklik tombol Start capturing packets yang berbentuk sirip ikan hiu berwarna biru. Tombol ini ada di pojok kiri atas.



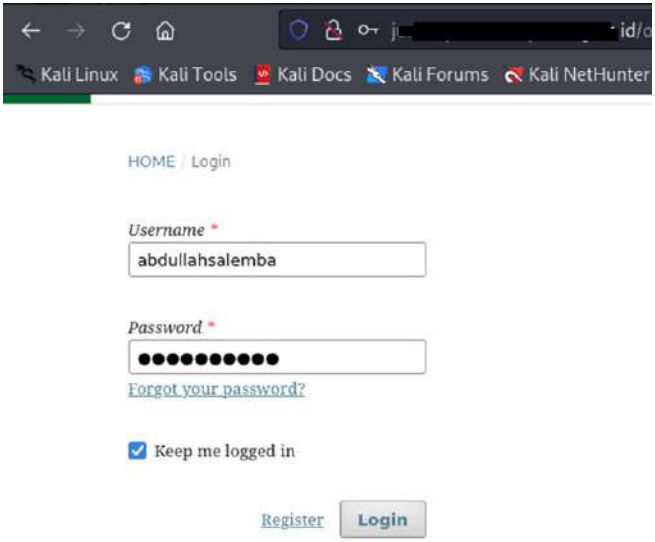
3. Dengan demikian aplikasi ini telah berjalan.
   Wireshark akan mencegat dan merekam paket-paket data yang keluar dan masuk ke dalam jaringan atau komputer Anda. Proses perekaman ini akan berlangsung terus sampai Anda menekan tombol stop yang berwarna merah.
   Inilah tampilan Wireshark saat melakukan capturing paket data.



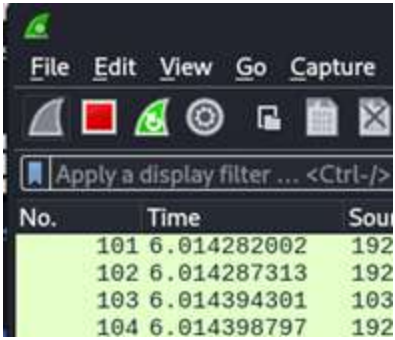
4. Biarkah Wireshark bekerja merekam aliran paket data. Sekarang Anda buka browser dan carilah situs di Internet yang memuat login dan Anda telah terdaftar di situs tersebut. Syaratnya situs web tersebut belum menggunakan SSL, ditandai dengan domain yang masih murni http saja, bukan https. Atau terdapat logo gembok yang dicoret di sampil url.



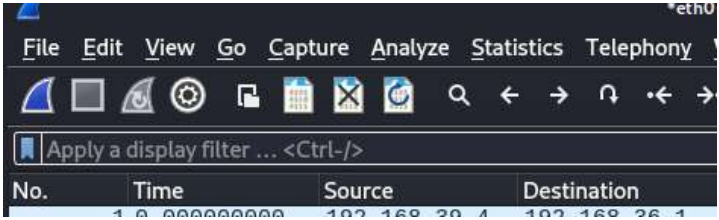
5. Berikutnya lakukan login pada situs tersebut. Ketik username dan password, kemudian klik tombol Login.



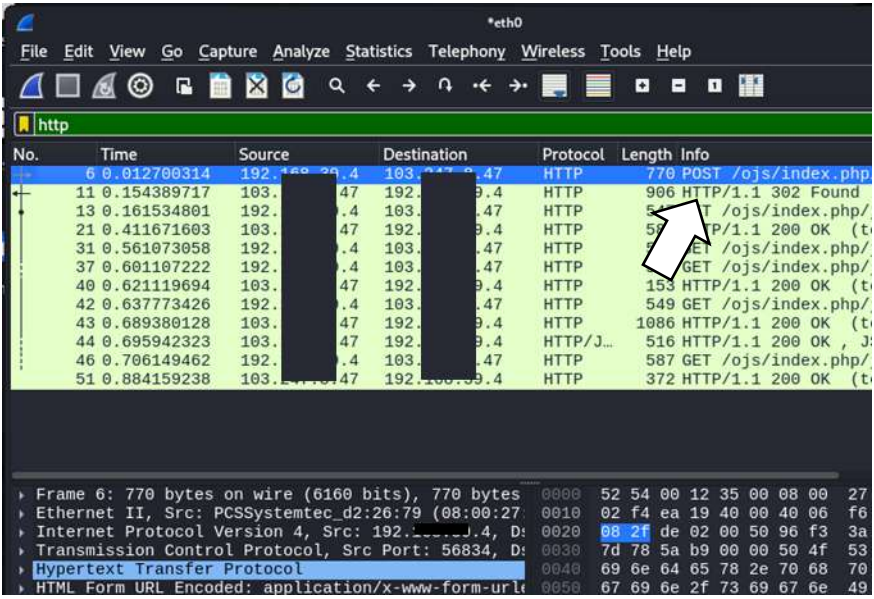
6. Setelah login berhasil, beralihlah ke aplikasi Wireshark. Klik tombol Stop capturing packets yang berwarna merah.



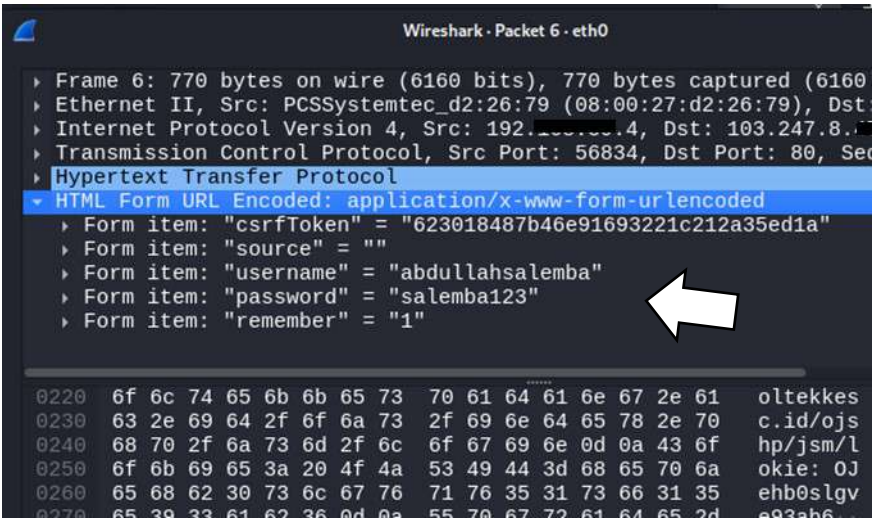
7. Sekarang saatnya menganalisa paket datanya.
8. Karena akan banyak paket data yang telah direkam oleh Wireshark, maka kita lakukan filter. Ketik 'http' pada kotak Apply a display filter. Kemudian Enter.



9. Kemudian Anda perlu mencari paket data yang memuat method POST. Kenapa demikian? Karena method POST digunakan untuk mengirimkan data dari HTTP Client untuk diproses di HTTP Server, kemudian HTTP server memberikan hasil dari proses tersebut ke HTTP Client. *Nah*, Wireshark merekam semua aliran data tersebut.
   Dan didapatkan paket data yang memuat method POST. Perhatikan pada gambar di bawah ini.



10. Klik ganda pada paket data tersebut. Akan tampak tampilan seperti gambar di bawah ini. Kemudian klik panah pada bagian HTML Form URL Encoded, dan terungkaplah username dan password loginnya.



Demikian cara menggunakan Wireshark untuk mendapatkan username dan password login seseorang. Dari hal ini kita pun memahami betapa berbahayanya aktifitas login pada situs yang tidak menggunakan SSL.

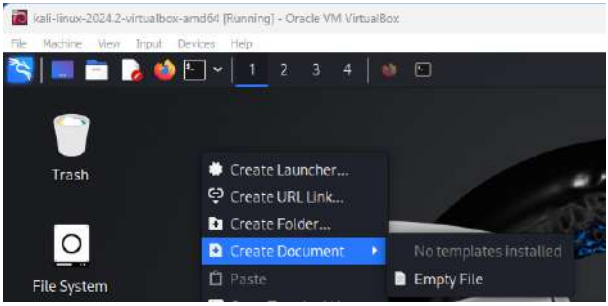
Menggunakan John The Ripper untuk Membongkar Password Suatu File

John the Ripper merupakan password recovery tool alias perangkat yang dapat digunakan untuk memulihkan password. John the Ripper masuk dalam paket aplikasi hacking yang ada di Kali Linux dan bekerja dengan interface command line di Terminal. John the Ripper dikembangkan oleh OpenWall dan pertama kali dirilis pada tahun 1996. Perangkat ini bersifat Open Source dan pada asalnya berjalan di sistem operasi Linux.

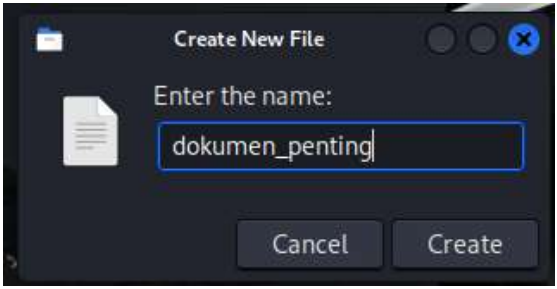
Logo John The Ripper (sumber: www.kali.org)

Dengan fungsinya sebagai perangkat untuk mengetahui password yang 'lupa', John the Ripper bisa juga digunakan untuk password auditing tool, yaitu mengetahui seberapa handal password yang dibuat. Pada tutorial di bawah ini dijelaskan cara membongkar password sebuah file archive dengan menggunakan John the Ripper. Inilah simulasi langkah-langkahnya di Kali Linux:

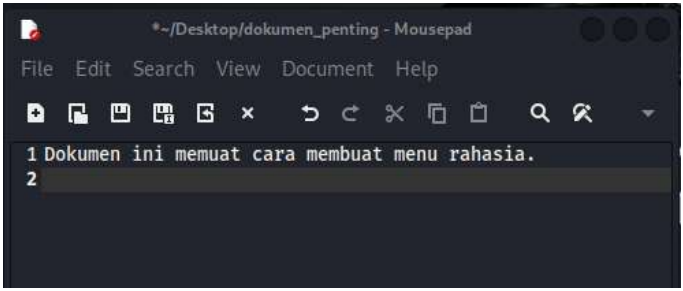
1. Pertama kali Anda akan membuat sebuah file text sederhana. Klik kanan pada Desktop di Kali Linux > Create Document > Empty File.



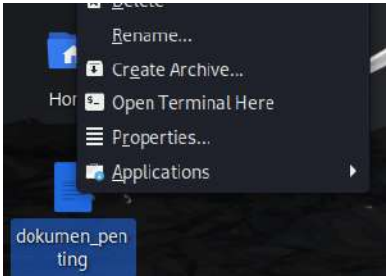
2. Beri nama dengan 'dokumen_penting' misalnya, atau sesuai keinginan Anda.



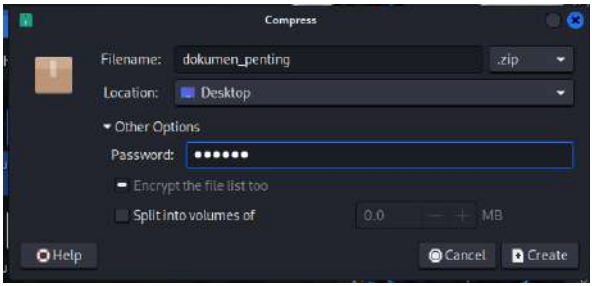
3. Pada Desktop akan terdapat file kosong. Klik file dokumen_penting tersebut. Sekarang buat tulisan sebagai isi dokumen text tersebut. Jangan lupa simpan.



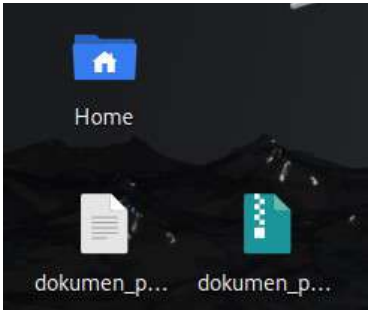
4. Berikutnya Anda akan membuat file archive dari file tersebut. Klik kanan pada file 'dokumen_penting' tersebut dan pilih menu Create Archive.



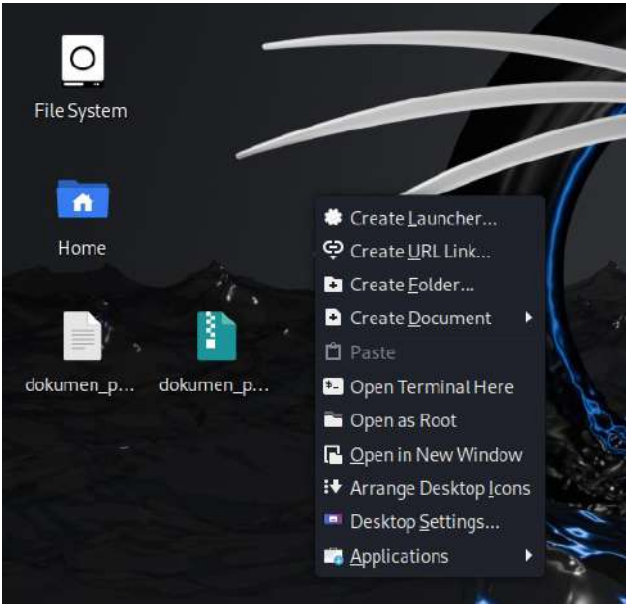
5. Akan tampil jendela Compress. Beri nama sesuai keinginan Anda dan pada bagian opsi pilih .zip. Kemudian isikan kata sandi pada bagian Password. Klik Create.



6. Akhirnya pada Desktop akan ada file archive dengan nama dokumen_penting.zip yang telah diberi password. Password inilah yang akan kita bongkar menggunakan John the Ripper.



7. Sekarang klik kanan pada Desktop kemudian pilih menu Open Terminal Here. Pastikan file archive yang akan dibongkar ada di Dekstop juga.

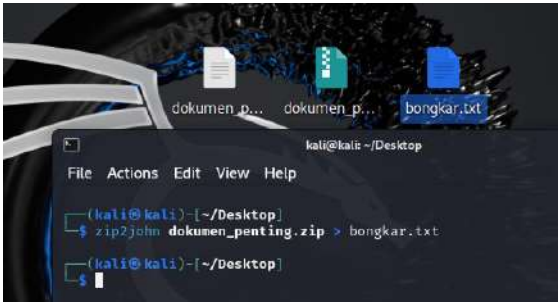


8. Pada bidang Terminal yang tampil klik perintah

```
Zip2john dokumen_penting.zip > bongkar.txt
```

Perintah ini artinya memerintahkan aplikasi John the Ripper untuk mengubah file archive dengan nama dokumen_penting.zip menjadi file bongkar.txt. File archive tersebut harus dibongkar ke bentuk file yang dikenal oleh aplikasi John the Ripper.

9. Akhirnya akan dibuat file baru di Desktop dengan nama bongkar.txt.

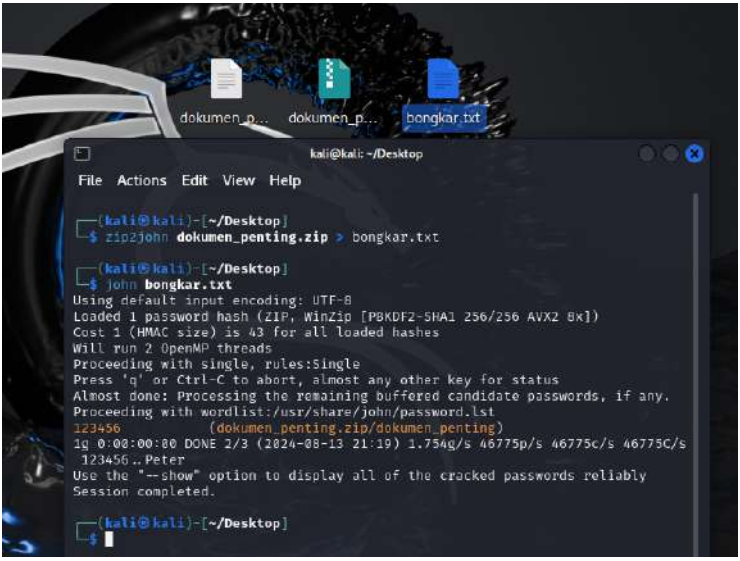


10. Nah, sekarang waktunya membongkar password-nya. Jalankan perintah di Terminal

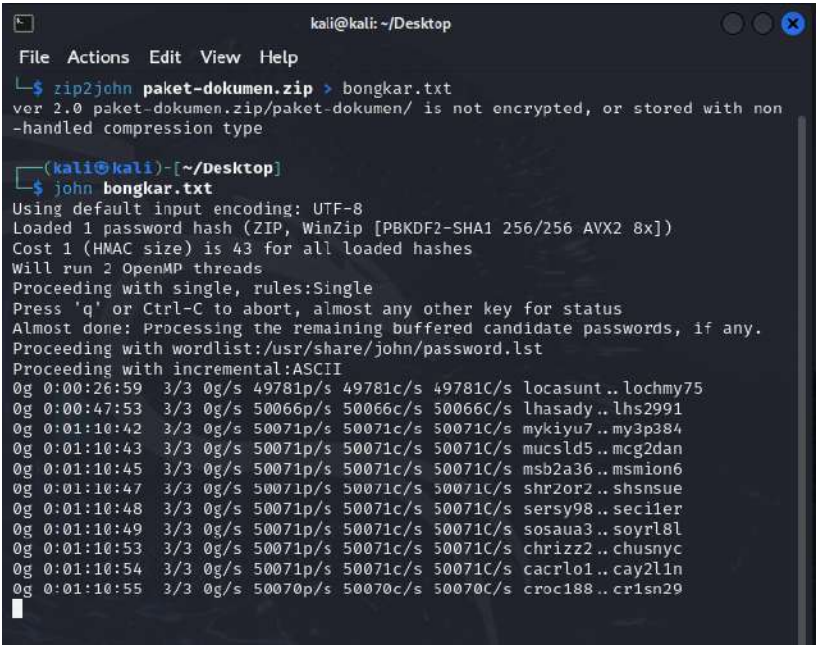
```
John bongkar.txt
```

Perintah ini artinya aplikasi John the Ripper akan membongkar password pada file bongkar.txt yang sudah dikenali bentuknya oleh John the Ripper.

Proses pembongkaran bisa berlangsung cepat atau lama, tergantung kompleksitas dari karakter penyusun password. Hasil kata sandi yang terungkap akan tampil pada warna coklat seperti gambar di bawah ini yaitu ’123456’.



11. Pada pembongkaran password yang rumit akan membutuhkan waktu yang lama, seperti terlihat pada gambar di bawah ini.



Demikian pembongkaran password archive dengan menggunakan John the Ripper.

Perangkat Hacking di Luar Kali Linux

Mengidentifikasi Kerentanan dengan Security Headers

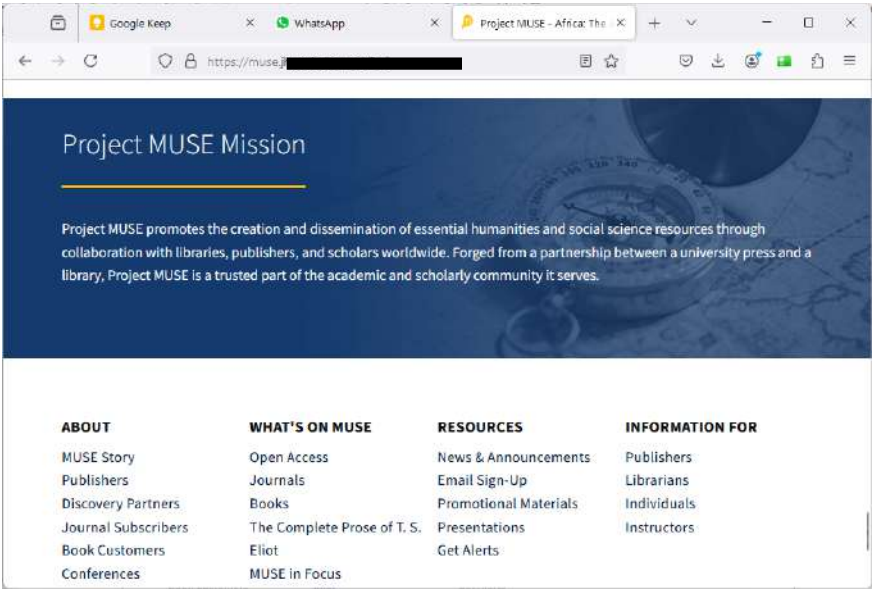
Isu keamanan aplikasi berbasis web nampaknya belum digarap secara serius. Misalnya saja ketika pembangunan suatu aplikasi berbasis web, sisi keamanan sering kali tidak mendapatkan porsi yang memadai. Padahal keberlangsungan aplikasi tersebut di Internet ditentukan oleh ketahanannya dari sisi keamanan.

Suatu aplikasi berbasis web yang sudah tayang di Internet, harus memenuhi prosedur keamanan. Tujuannya agar aplikasi berbasis web tersebut tidak mudah dibobol atau di-*hack* oleh pihak yang tidak berwenang.

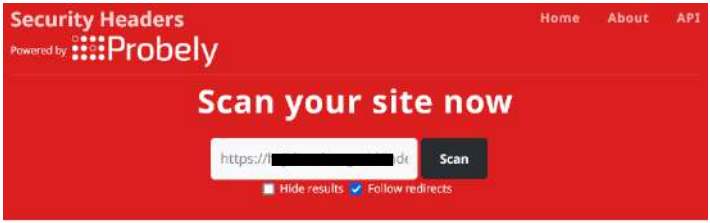
Dari banyak dan beragam upaya untuk meningkatkan keamanan suatu aplikasi web, **salah satunya** adalah meningkatkan dan membentengi aplikasi web dari sisi *security headers*. Langkah-langkah yang perlu dilakukan dijelaskan di bawah ini.

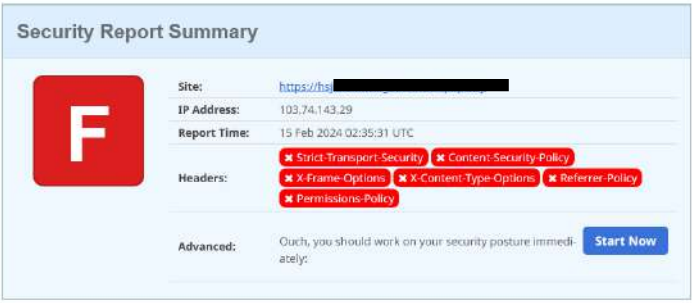
1. Tahap pertama, Anda perlu melakukan *scanning* aplikasi *website* tersebut. Apakah sudah aman atau masih rentan dan pada level berapa tingkat keamanannya.

2. Tentukan aplikasi berbasis web yang akan Anda amankan dari sisi *security headers*-nya. Tentukan alamat URL-nya dan coba kunjungi alamat tersebut.



3. Arahkan browser ke alamat https://securityheaders.com/ dan masukkan url dari aplikasi yang akan diperiksa terlebih dahulu. Kemudian klik tombol Scan untuk memulai pemeriksaan. Hasil pemeriksaan akan ditampilkan dengan rentang dari A+ sampai F. Level A+ menyatakan *security headers* aplikasi berada pada tataran yang sangat aman, sedangkan F berada pada tataran yang sangat tidak aman.

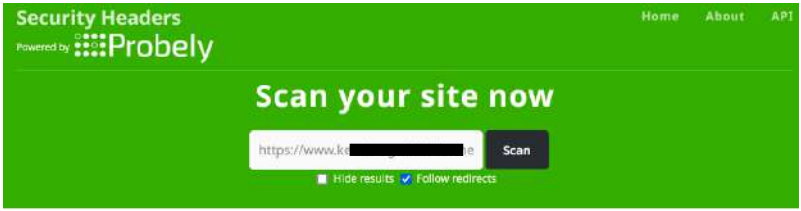




4. Secara gamblang, untuk meningkatkan sisi *security headers* pada aplikasi web, Anda harus menambahkan *script* kode keamanan. Tambahkan saja *script* di bawah ini pada file config.inc.php.

```
Header always set X-XSS-Protection: "1; mode=block"

Header always set X-Content-Type-Options: "nosniff"

Header always set X-Frame-Options: "SAMEORIGIN"

Header always set Referrer-Policy: "strict-origin"

Header always set Permissions-Policy:
"geolocation=(),midi=(),syncxhr=(),microphone=(),came
ra=(),magnetometer=(),gyroscope=(),fullscreen=(self),
payment=()"

Header always set Strict-Transport-Security: "max-
age=31536000; includeSubDomains; preload"

Header always set Content-Security-Policy: "default-
src 'self' ; font-src *;img-src * data:; "
```

5. Setelah kode tersebut diinputkan, lakukan *scanning* ulang menggunakan https://securityheaders.com/. Hasilnya, aplikasi webiste sekarang berada pada nilai A+ yang artinya telah aman.



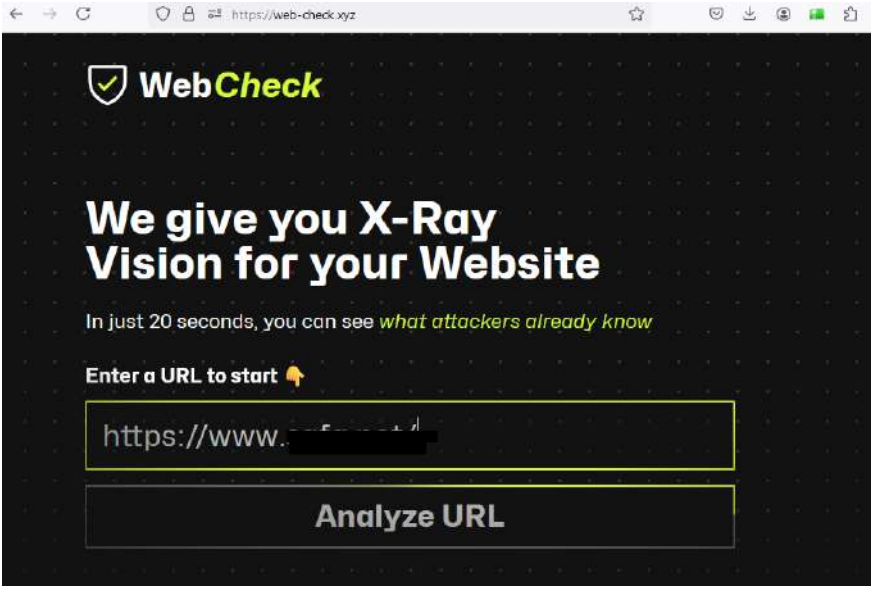
Proses peningkatan keamanan suatu aplikasi berbasis web merupakan upaya yang terpadu. Banyak sisi yang harus diamankan dengan upaya pemutakhiran yang terus berlangsung.

Mengidentifikasi Kerentanan dengan Web Check

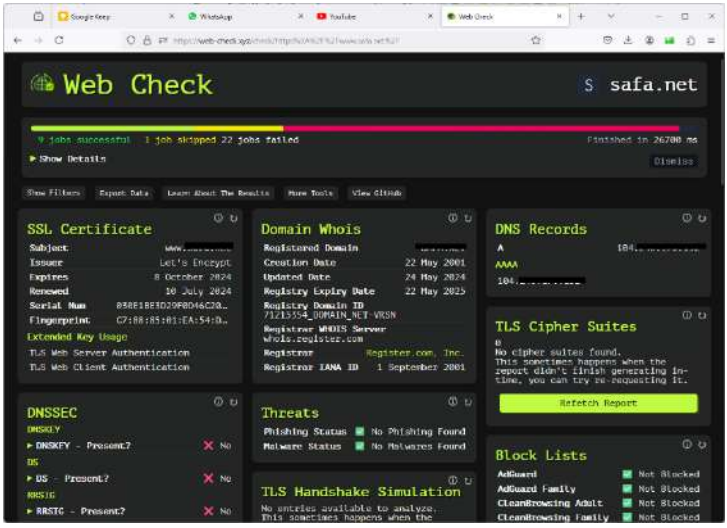
Kerentanan suatu website dapat dianalisa dengan menggunakan aplikasi berbasis web, di antaranya adalah Web Check. Dari hasil scannng menggunakan aplikasi ini dihasilkan beragam informasi seperti tentang SSL Certificate, Domain Whois, DNS records, dll.

Berikut dijelaskan langkah-langkah untuk melakukan identifikasi kerentanan dengan Web Check:

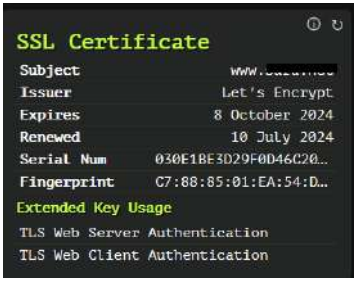
1. Jalankan browser dan arahkan ke alamat https://web-check.xyz.
2. Pada kotak Enter a URL tuliskan alamat situs yang menjadi target scanning.
3. Klik tombol Analyze URL untuk memulai.



4. Proses scanning akan berlangsung. Tunggu beberapa saat.
5. Setelah selesai akan tampil laporan hasil scanning seperti pada gambar di bawah ini.



6. Pada bagian Show Details akan tampil daftar pengecekan yang berhasil (success), gagal (error) atau yang kehabisan waktu (time out).
7. Selanjutnya pada bagian di bawahnya terdapat detail informasi pengecekan yang telah di kelompokkan. Misalnya pada bagian SSL Certificate akan terungkap bahwa web target menggunakan SSL yang dikeluarkan oleh Let's Encrypt dan akan kadaluarsa pada tanggal 8 Oktober 2024. Dst.



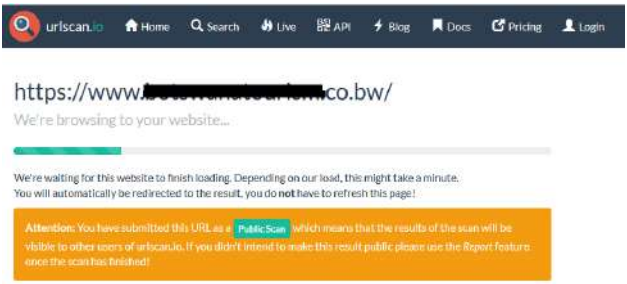
8. Informasi-informasi tersebut sangat bermanfaat untuk menambah pengetahuan tentang kondisi target. Misalnya saja dari proses ini terungkap pula DNS records dari target, kapan kadaluarsa fitur SSL-nya, dll.
   Bila informasi yang kita cari tidak dihasilkan dari scanning tool ini, kita bisa menggunakan perangkat lainnya.
9. Untuk mengunduh hasil bisa dengan mengklik tombol Download Results yang ada di bagian bawah.

Mengidentifikasi Kerentanan dengan URL Scan

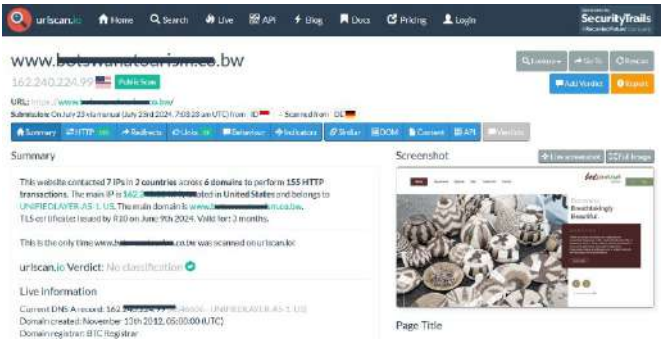
Perangkat lain yang berbasis web yang dapat digunakan untuk mendapatkan informasi pada suatu sistem berbasis web adalah Urlscan.io. Caranya dijelaskan berikut ini:

1. Jalankan browser dan arahkan ke alamat https://urlscan.io/.
2. Pada kotak url to scan, ketik url yang akan kita scanning.

3. Selanjutnya klik tombol panah hijau Public Scan di sisi kanannya dengan demikian proses scanning akan dimulai.



4. Urlscan.io akan melakukan proses scanning. Tunggu beberapa saat sampai proses scanning selesai.
5. Hasil scanning akan tampil seperti gambar di bawah ini. Dari hasil scanning ini terungkap banyak informasi. Kita dapat menelusuri pada tab Summary, HTTP, Redirects, dst.

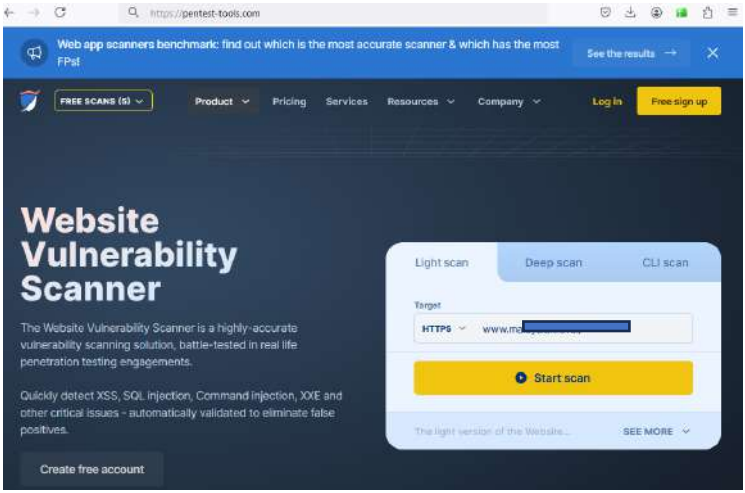


Mengidentifikasi Kerentanan dengan Pentest Tools

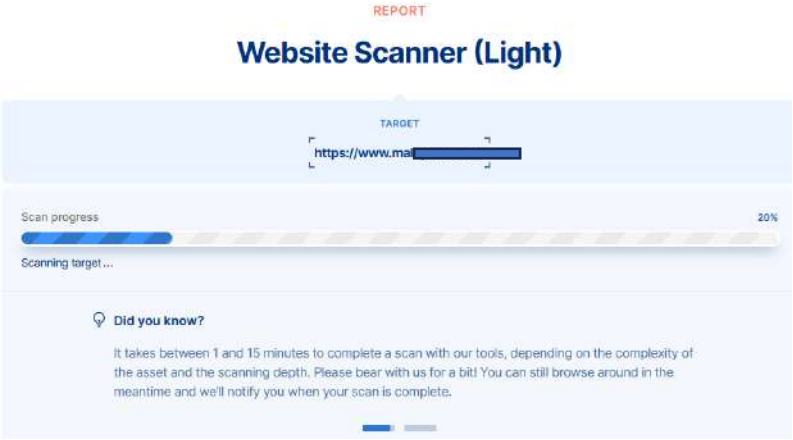
Vulnerability atau kerentanan pada aplikasi berbasis web dapat pula diidentifikasi menggunakan aplikasi dari Pentest-Tools. Pentest-Tools merupakan suatu paket aplikasi berbasis web yang merupakan bagian dari The Open Web Application Security Project (OWASP).

Berikut ini langkah-langkah melakukan scanning aplikasi berbasis web menggunakan Pentest-Tools.

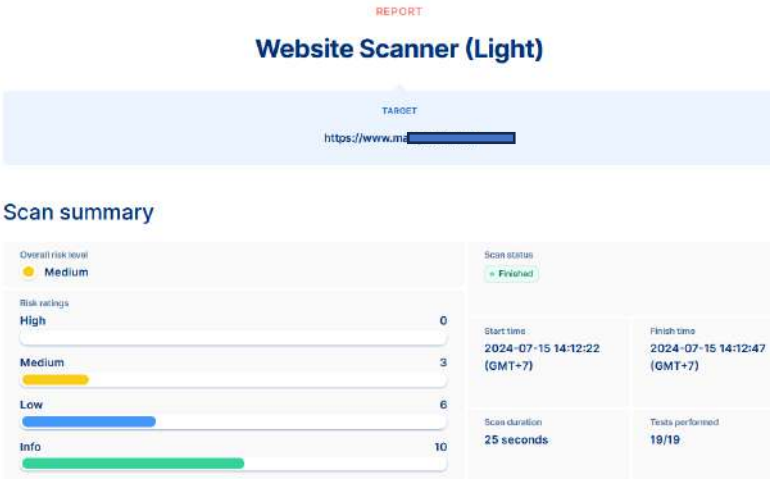
1. Jalankan browser dan arahkan ke alamat https://pentest-tools.com.
2. Pada bagian Light scan, ketik url target web yang akan dianalisa. Pastikan untuk menyesuaikan memilih protokol https atau http untuk urlnya. Kemudian klik tombol kuning Stat scan.



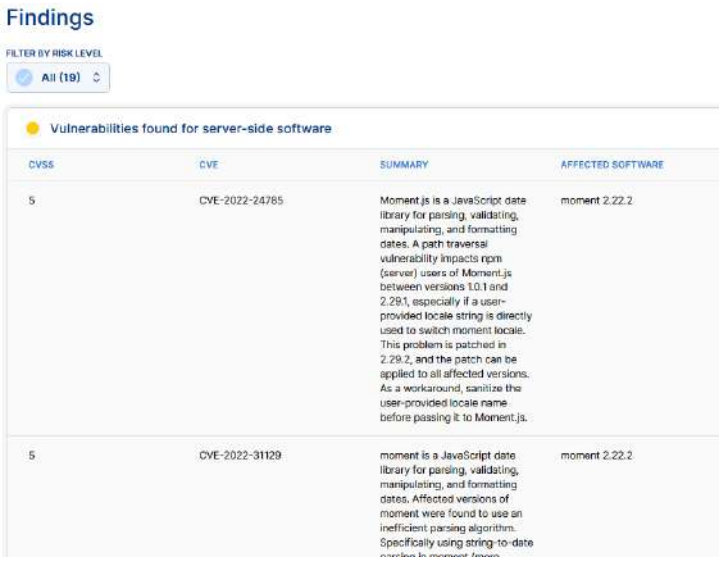
3. Proses scanning akan berlangsung beberapa saat. Tunggu sampai proses selesai.



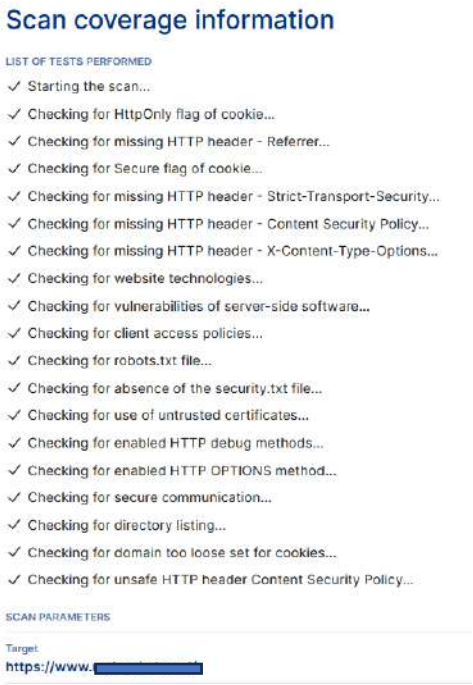
4. Setelah proses scanning selesai, akan tampil laporan yang bisa kita analisa lebih lanjut. Perhatikan pada bagian Scan summary.



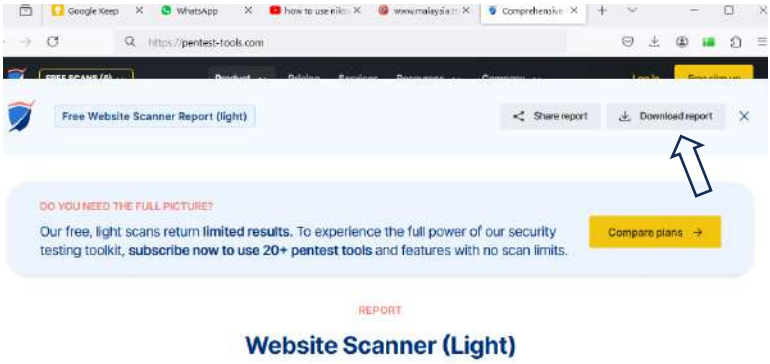
5. Gulung halaman agak ke bawah. Perhatikan juga bagian Findings.



6. Untuk detail cakupan scanning yang dilakukan dapat dilihat pada bagian akhir laporan.



7. Untuk mengunduh laporan hasil scanning bisa mengklik tombol Download report yang ada di pojok kanan atas.



Mengidentifikasi Kerentanan dengan OWASP ZAP

Sebagai antisipasi keamanan pada aplikasi berbasis web, perlu dilakukan *penetration testing*. Kegiatan *penetration testing* ini dilakukan dengan melakukan banyak aktifitas pengujian sistem dalam bentuk simulasi untuk mendapatkan informasi kelemahan-kelemahan suatu sistem. Setelah mendapatkan beragam informasi kelemahan sistem, langkah selanjutnya adalah memperbaiki dan menutup celah keamanan tersebut. Semua ini dilakukan agar sistem aplikasi yang kita bangun dalam kondisi aman dan kuat terhadap serangan dari luar yang memanfaatkan celah keamanan.

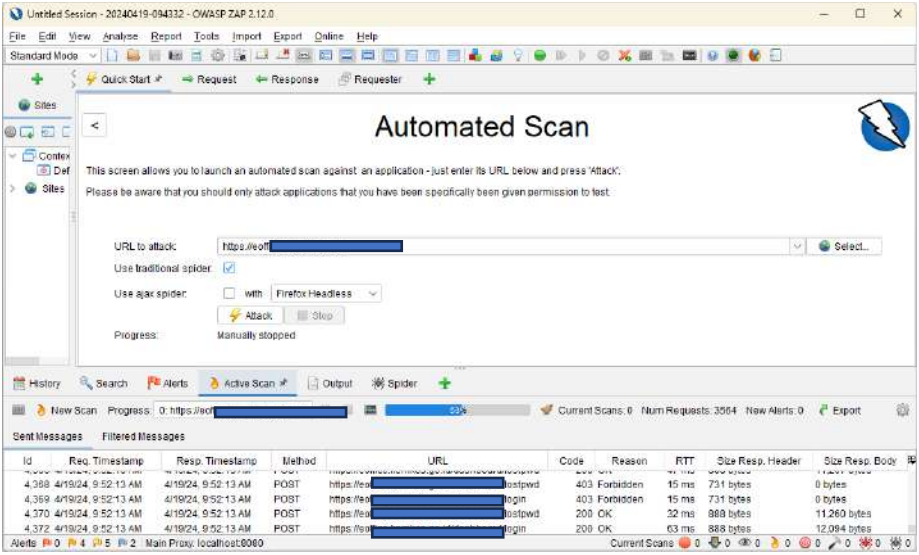
Apa yang kami sampaikan di sini adalah untuk diterapkan pada sistem aplikasi yang dibangun oleh masing-masing pihak, bukan untuk diterapkan atau membaca kelemahan sistem milik orang lain yang kemudian mengeksploitasi kelemahan tersebut. Perlu diingat, untuk melakuan *scanning* terhadap sebuah sistem, seseorang harus mendapatkan kewenangan dari pihak yang bersangkutan.

Berikut ini adalah langkah-langkah untuk mendapatkan dan mengumpulkan informasi kelemahan suatu aplikasi berbasis web dan

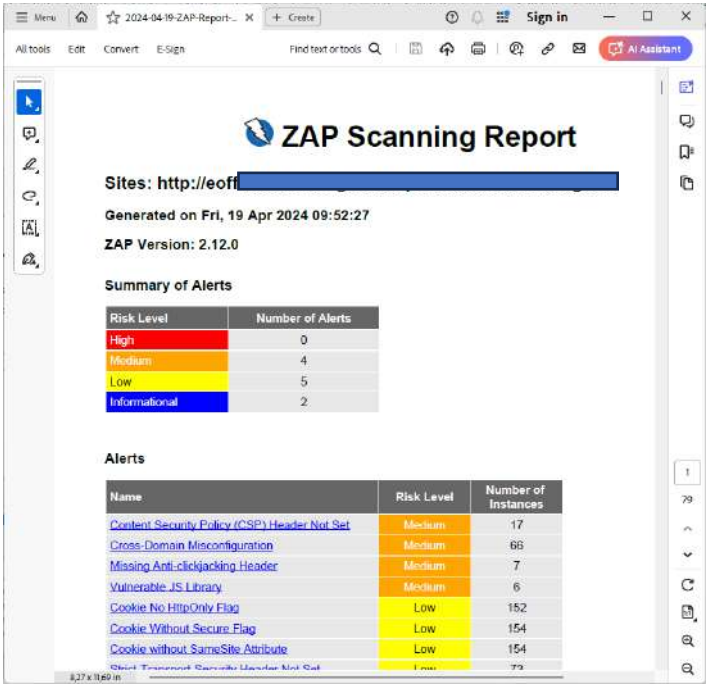
solusi untuk menutup kelemahan-kelemahan tersebut. Kegiatan ini menggunakan perangkat aplikasi OWASP ZAP yang harus kita unduh dan install sebelumnya. Inilah langkah-langkahnya:

1. Lakukan pengunduhan aplikasi OWASP ZAP yang ada di alamat https://www.zaproxy.org/download/.

2. Lanjutkan dengan proses instalasi OWASP ZAP.
3. Jalankan aplikasi OWASP ZAP.
4. Pilih fitur **Automated Scan**.



5. Ketik alamat pada bagian **URL to attack**.
6. Biarkan opsi yang lain seperti pada gambar.
7. Klik tombol **Attack**.
8. Proses *scanning* akan berjalan beberapa waktu. Bisa memakan waktu beberapa jam tergantung kerumitan aplikasi web yang di-*scan*.
9. Bila proses sudah selesai, laporan hasil *scanning* dapat dibuat secara otomatis. Klik pada menu **Report** > **Generate Report**.
10. Berikut tampilan laporan hasil *scanning* dalam format dokumen PDF.



ZAP Scanning Report

Sites: http://eoff

Generated on Fri, 19 Apr 2024 09:52:27

ZAP Version: 2.12.0

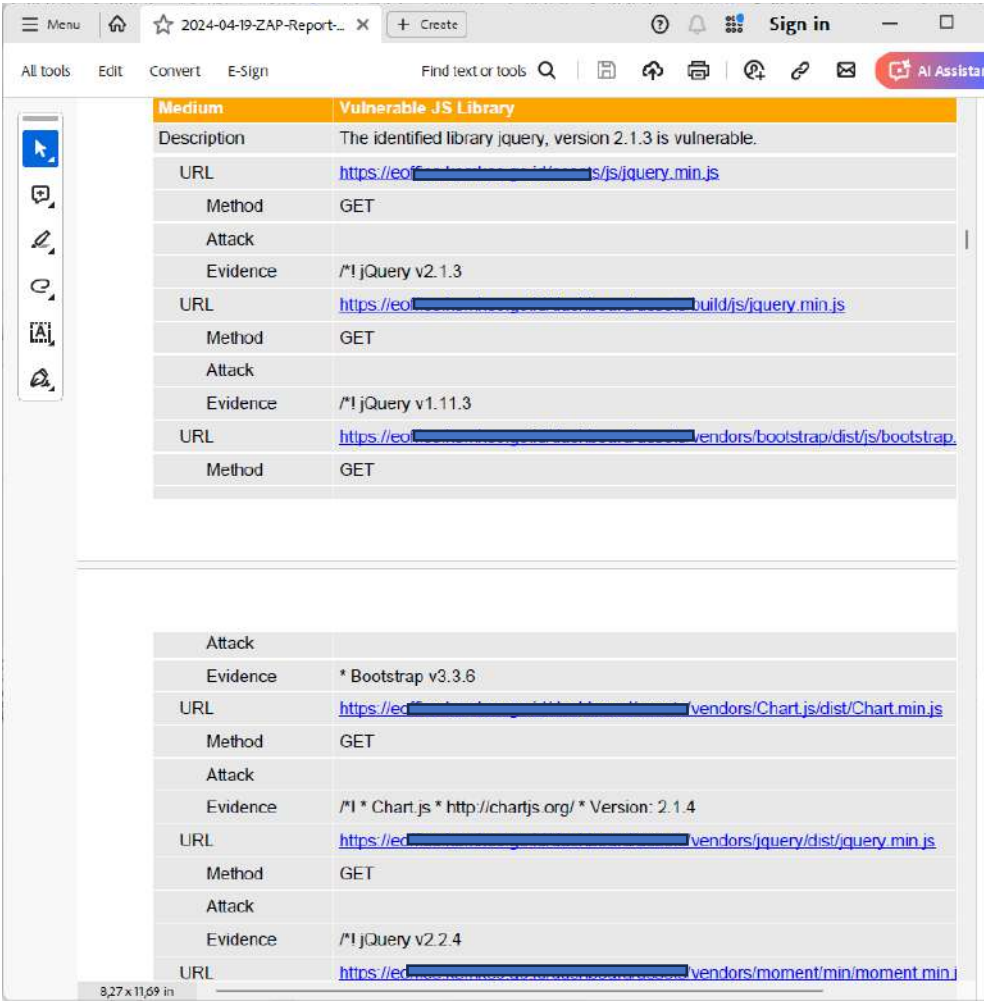
Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	4
Low	5
Informational	2

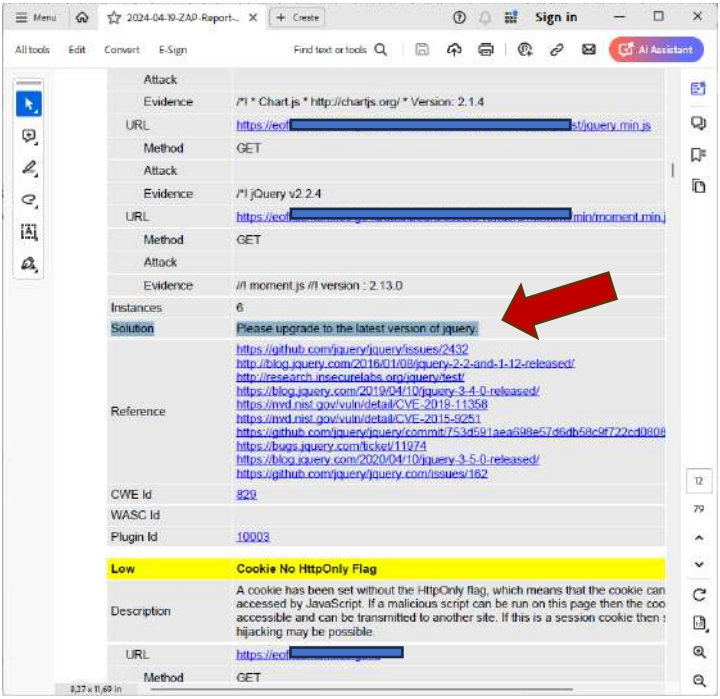
Alerts

Name	Risk Level	Number of Instances
Content Security Policy (CSP) Header Not Set	Medium	17
Cross-Domain Misconfiguration	Medium	66
Missing Anti-clickjacking Header	Medium	7
Vulnerable JS Library	Medium	6
Cookie No HttpOnly Flag	Low	152
Cookie Without Secure Flag	Low	154
Cookie without SameSite Attribute	Low	154

11. Untuk memahami laporan hasil *scanning* dari ZAP, yang paling utama perhatikan pada bagian **Summary of Alerts**. Ada beberapa kategori yaitu *high*, *medium*, *low*, dan *informational*. Masing-masingnya disertakan jumlah *alerts* yang berhasil di-*scan*. Misalnya pada kategori medium ada 4 kelompok *alerts*.
12. Kelompok *alerts* tersebut dirinci pada bagian berikutnya, perhatikan pada bagian **Alerts** di bawahnya. Dari kelompok *alerts* yang berjenis medium, ada 4 kelompok *alerts*, salah satunya adalah **Vulnerable JS Library**, ada 6 kasus yang terbaca.
13. Misalnya diklik pada *alerts* **Vulnerable JS Library**. Akan tampil pada bagian **Vulnerable JS Library** dengan 6 kasus yang terbaca.



14. Untuk mengatasi kasus ini, dijelaskan pada bagian akhir solusi yang harus dilakukan. Perhatikan pada bagian **Solution**.



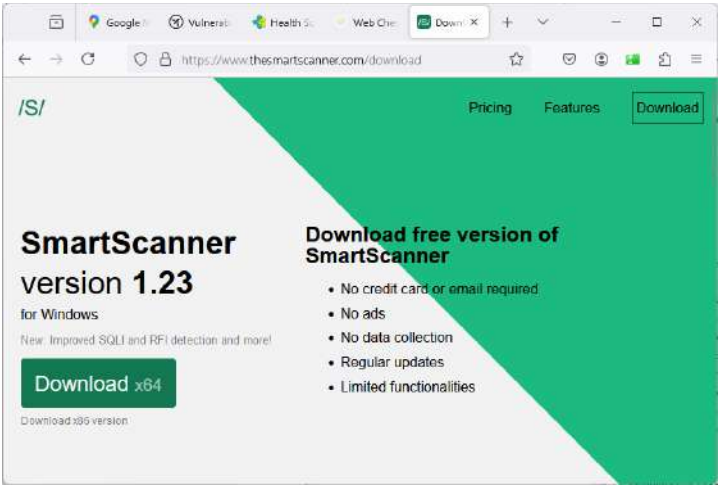
15. Solusi dari kasus **Vulnerable JS Library** adalah dengan melakukan *update* pada versi jquery yang terakhir.
16. Demikian pula pada *alerts* yang lain hasil dari *scanning* OWASP ZAP, memiliki rekomendasi solusi yang berbeda beda. Perhatikan pula pada referensi yang disertakan.

Mengidentifikasi Kerentanan dengan SmartScanner

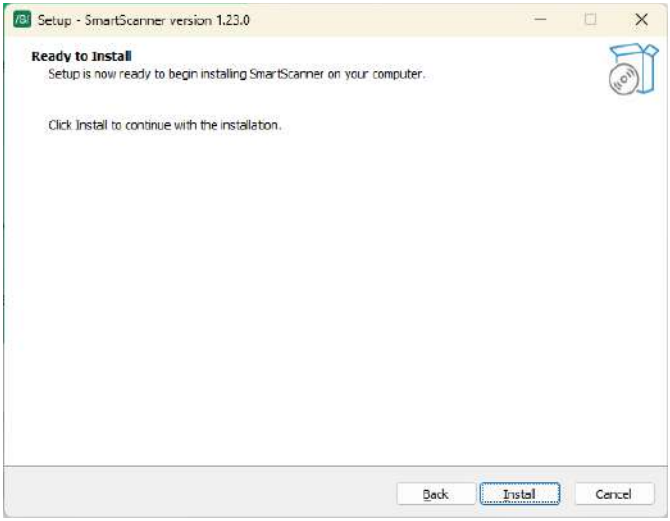
Tool yang lain yang dapat juga digunakan untuk mengidentifikasi kerentanan aplikasi berbasis web adalah SmartScanner. Tool ini bukan berbasis web, tetapi berupa aplikasi yang harus diunduh terlebih dahulu kemudian dilakukan instalasi pada PC.

Untuk mengidentifikasi kerentanan dengan SmartScanner langkah-langkahnya adalah:

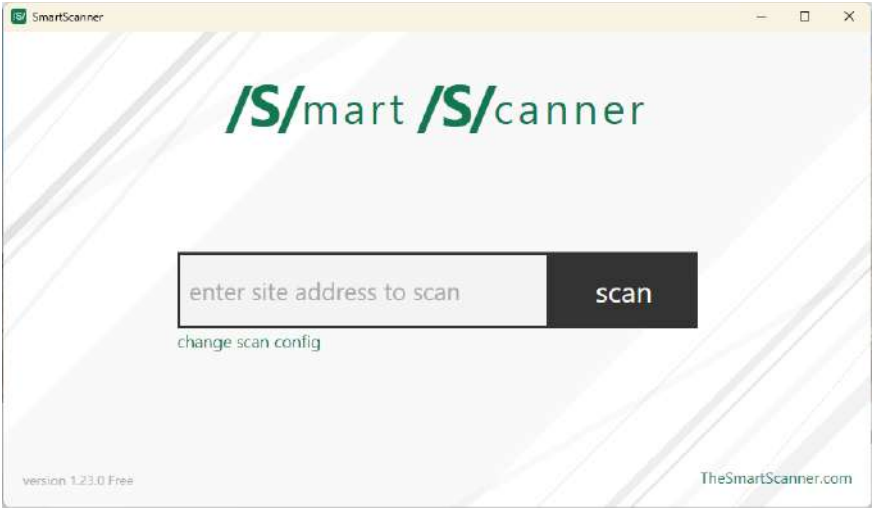
1. Jalankan browser dan arahkan pada alamat https://www.thesmartscanner.com/download untuk mengunduh aplikasi SmartScanner.
2. Pada halaman SmartScanner yang tampil, klik tombol Download untuk mengunduhnya.



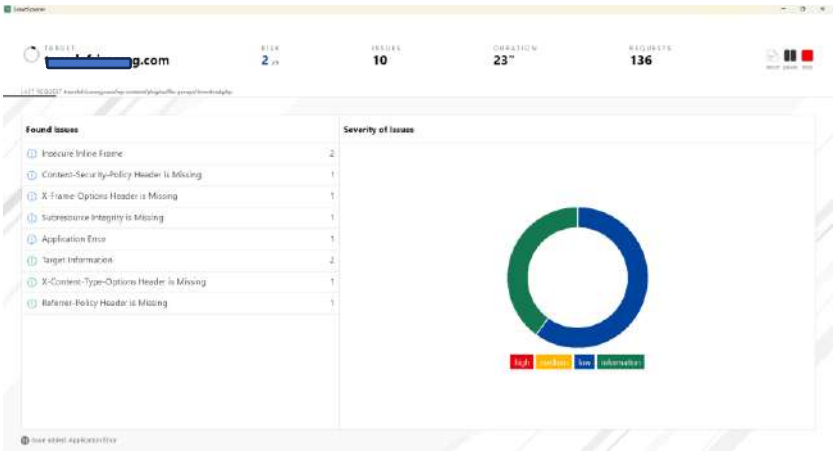
3. Lanjutkan dengan proses instalasi sampai selesai.



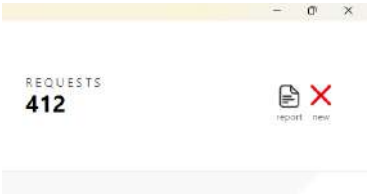
4. Sekarang jalankan SmartScanner untuk melakukan scan terhadap situs yang akan kita analisa.
5. Ketik alamat web yang akan kita scan pada kotak enter site address to scan.
6. Lanjutkan dengan mengklik tombol scan yang berwarna hitam.



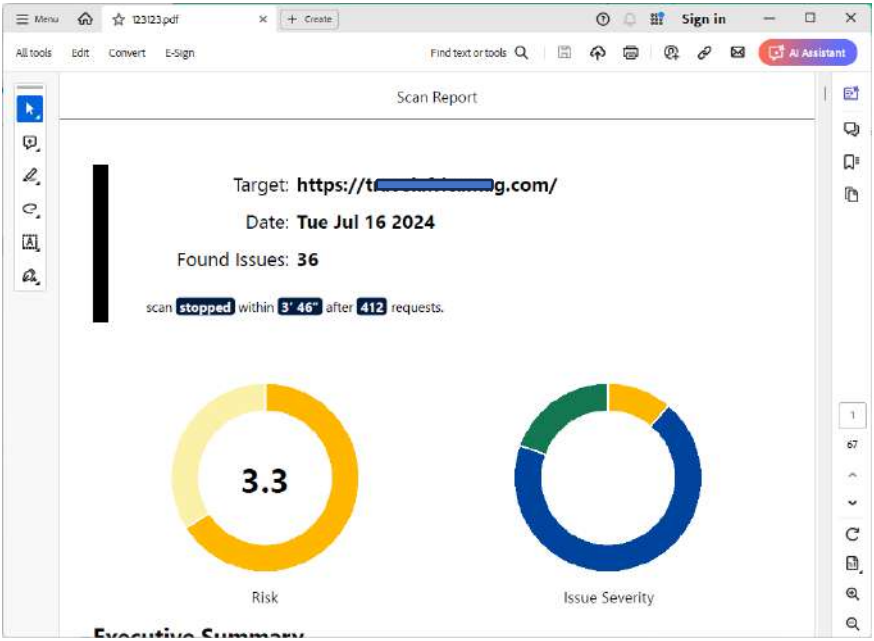
7. Proses scanning akan berlangsung. Tunggu sampai proses selesai.



8. Daftar kerentanan yang ditemukan ditampilkan pada bagian Found Issues.
9. Bila dirasa cukup, proses scanning bisa dihentikan dengan mengklik tombol Stop yang ada di pojok kanan atas.



10. Laporan hasil scanning dapat pula diperoleh dengan mengklik tombol Report yang ada di pojok kanan atas. Terdapat pilihan bentuk dokumen berupa PDF, HTML, atau JSON.



Profil Penulis

Profil Penulis

Happy Chandraleka atau dikenal dengan nama Cakrabirawa adalah seorang penulis TI independen yang telah lama berkecimpung di dunia TI. Tulisannya banyak tersebar di Internet dan diterbitkan oleh berbagai penerbit nasional. Awal mula terjerembab dalam dunia tulis-menulis adalah ketika tulisan pertamanya diterbitkan oleh majalah Mikrodata yang membahas tentang pengaksesan registry Windows menggunakan bahasa pemrograman Delphi. Kala itu terjadi sekitar tahun 2000. Sampai sekarang kecanduan menulis masih belum bisa dihilangkan.

Jebolan Teknik Elektro Universitas Diponegoro ini telah menerbitkan banyak buku pada berbagai penerbit nasional. Beberapa buku di antaranya yang bergenre keamanan komputer di antaranya adalah Keylogger dan Pemrogramannya (Penerbit Andi); Virus, Worm dan Trojan Horse (Penerbit Andi); Kiat Praktis Mengamankan Data pada Office (Penerbit Andi); Siapa Bilang Nge-Hack Itu Susah (Penerbit Elex Media Komputindo); Mengamankan Data Pribadi Ala Agen Rahasia (Penerbit Elex Media Komputindo); Trik Mengantisipasi Hacking Email (Penerbit Media

Kita); Password Undercover (Penerbit Elex Media Komputindo), dll. Buku yang Anda pegang ini merupakan karya penulis yang ke-35.

Penulis yang gemar literatur klasik Islam dan merupakan ASN di salah satu kementerian di Indonesia dapat dihubungi di hchandraleka@gmail.com. Kunjungi juga blog penulis di https://thecakrabirawa.wordpress.com/.

Berlatih Jadi Hacker

Buku ini memberikan dasar-dasar tentang penetration testing yang merupakan tahapan penting dalam proses hacking. Kemudian penyediaan perangkat virtualisasi. Hal ini dikarenakan sebagian pengguna komputer saat ini menggunakan sistem operasi Windows. Sehingga diharapkan dengan virtualisasi dapat dipasang sistem operasi Kali Linux tanpa perlu mengganggu sistem operasi Windows yang telah eksis sebelumnya.

Bagian berikutnya buku ini akan membimbing pembaca untuk melakukan instalasi sistem operasi Kali Linux yang merupakan sistem operasi khusus untuk kepentingan hacking. Dalam buku ini dipraktekkan sebagian perangkat hacking yang ada di Kali Linux yaitu cara menggunakan Wireshark untuk mendapatkan usesname dan password login; cara menggunakan Nmap untuk mengetahui port yang terbuka; cara menggunakan John the Ripper untuk membongkar password; dll.

Perangkat hacking tidak hanya ada di Kali Linux. Banyak juga bertebaran di Internet. Oleh karena itu pada bagian berikutnya buku ini melatih pembaca untuk menggunakan tool dari luar Kali Linux. Di antaranya adalah menggunakan Security Header; Web Check; OWASPZAP untuk mendeteksi kerentanan dan celah pada suatu aplikasi berbasis web.

Diharapkan buku ini dapat memberikan dasar-dasar yang kuat bagi siapa yang akan memasuki dunia hacking. Selamat berlatih!

Jakarta, 10 Jumadal Ula 1446 H/
12 November 2024 M