PERANCANGAN PORTABEL KOMPUTER KALI LINUX BERBASIS RASPBERRY PI 3 MODEL B MANFAAT UNTUK TEST PENETRASI

Ilham Herlangga[1], Hary Nugroho[2]
[1,2]Akademi Teknik Telekomunikasi Sandhy Putra Jakarta
[1,2]Jalan Poris Indah Blok G19, RT. 01/RW.06,Cipondoh Tangerang, Daerah Khusus Kota Tangerang 15148, Indonesia
harynug@gmail.com

Website sudah menjadi bagian penting dalam setiap aspek kehidupan kita sehari-sehari, dari belanja online hingga bersosialisasi, Setiap website adalah unik dengan caranya sendiri mulai dari coding hingga eksekusi, tetapi secara umum di setiap website terdapat celah-celah keamanan yang mudah disalahgunakan oleh para hacker, oleh karena itu perlu dilakukannya scanning celah keamanan yang ada pada sebuah website. melihat permasalahan terjadi namun dibalik itu semua terdapat inovasi yang dapat memudahkan scanning website itu sendiri yaitu dengan menggunakan raspberry sebagai komputer nya dan berbagai komponen yang seperti layar mini, dan power bank sebagai baterainya sehingga memudahkan pengguna untuk melakukan Test penetrasi dengan konsep pengontrolan jarak jauh yang dapat diaplikasikan dimana saja dan yang pada akhir nya dengan menggunakan raspberry sebagai komputer bisa mengurangi biaya dan bisa membantu meperkuat situs website.

Kata kunci: Scanning web, Owasp zap, raspberry, os kali linux

Abstract:

Websites have become an important part of every aspect of our daily lives, from online shopping to socializing. Each website is unique in its own way from coding to execution, but in general every site has security holes that are easily misused by hackers, therefore need to be based on a security scan that is on a website. looking at the problems that occur, but behind it all there are innovations that can facilitate scanning the website itself, namely by using a raspberry as a computer and various components such as a mini screen, and a power bank as the battery, making it easier for users to perform penetration tests with the concept of a remote controller can be applied anywhere and in the end using the raspberry as a computer can reduce costs and can help strengthen a website

I. PENDAHULUAN

A. Latar Belakang

Saat ini banyak sekali perusahaan-perusahaan menggunakan perangkat pc yang digunakan untuk menyimpan data-data dan mengamankan sebuah situs website sebagai pengontrolan jarak jauh yang memiliki ruang lingkup cukup luas untuk memungkinkan suatu pengontrolan jarak jauh. Akan tetapi pengontrolan jarak jauh dengan menggunakan perangkat pc terdapat ketidak efesienan dalam dimensi atau ukuran perangkat pc dan konsumsi daya dan biaya yang cukup besar. Sekarang ini telah muncul suatu perangkat untuk menggantikan perangkat pc pada umum nya yaitu portabel pc untuk digunakan memperkuat situs web site menggunakan software Owasp Zap Salah satu dengan metode paling efektif adalah melakukan pengujian pentest bisa menemukan vulnerabilities dan celah-celah bug yang ada dapat diketahui dan dengan demikian dapat diperbaiki secepatnya. Dengan itu pengontrolan jarak jauh dapat diaplikasikan dirumah yang didalamnya terdapat peralatan yang dapat kita pantau.

Berbicara tentang pengunaan daya yang cukup besar saat melakukan Test penetrasi, terdapat sebuah inovasi, yang dikenal dengan nama Raspberry Pi, sering disingkat dengan nama raspi, adalah komputer papan tunggal (single-board circuit; SBC) yang seukuran dengan kartu kredit yang dapat digunakan untuk menjalankan program perkantoran, permainan komputer, dan sebagai pemutar media hingga video beresolusi tinggi dengan komputer berukuran portabel yang disebut dengan raspberry pi 3 model B. Pada portabel raspberry pi 3 model B ini sudah dilengkapi dengan semua fungsi layaknya sebuah komputer lengkap menggunakan soc (system-on-a-chip) arm, dengan dimensi 5.5cmx8.5cm dan ketinggian 2cm. sifat nya yang lengkap, multi guna, mudah dioperasikan. Raspberry PI itu sendiri bahkan dapat memiliki Operating System sehingga dapat berfungsi layaknya kompter biasa mulai dari membuat pengolah kata, menyimpan file, memutar music, memutar video, browsing internet, bahkan memainkan game layaknya di komputer.

B. Tujuan Penelitian

Tujuan dari perancangan portabel komputer kali linux bebrbasis Raspberry pi 3 model B manfaat untuk pentest ini adalah sebagai berikut:

1. Untuk melakukan instalasi perancangan portabel komputer kali linux berbasis Raspberry pi 3 model B melakukan pentest terhadap situs website.
2. Mengetahui suatu jenis serangan yang berpotensi yang bermasalah pada situs web
3. Mengetahui cara kerja menggunakan Portabel Komputer kali linux berbasis Raspberry Pi 3 model B untuk Pentest terhadap situs website

C. Rumusan Masalah

Berdasarkan tujuan dan maksud penelitian di atas, maka permasalahan yang akan dipecahkan dalam penelitian ini adalah:

1. Bagaimana cara installasi perancangan portabel komputer kali linux bebrbasis Raspberry pi 3 model B untuk melakukan test penetrasi terhadap situs website?
2. Bagaimana Hasil Pengujian test penetrasi menggunakan Owasp zap dengan perangkat portabel komputer terhadap situs websiate?
3. Bagaimana kerja fungsi alat menggunakan Portabel komputer kali linux berbasis Raspberry pi 3 model B pada saat melakukan test penetrasi?

D. Batasan Masalah

1. Perangkat ini hanya dapat digunakan sebagai Komputer Portabel untuk melakukan pentest.
2. Perangkat ini hanya memiliki OS Kali Linux tidak dapat menggunakan dual OS karena keterbatasan penyimpanan perangkat.
3. Perangkat ini tidak dapat digunakan untuk melakukan berbagai hal yang berkaitan dengan software yang memerlukan spesifikasi yang tinggi

II. DASAR TEORI

A. Penjelasan Mengenai Raspberry Pi 3 Model B

Raspberry Pi 3 adalah model terbaru Raspberry Pi. Raspberry pi 3 menggunakan prosesor baru yaitu Broadcom BCM2837, 64bit. BCM2837 lebih cepat dari pada BCM2836. Raspberry Pi 3 juga merupakan model pertama yang memiliki built-in wireless (mampu terhubung ke jaringan Wifi dan juga perangkat Bluetooth). Padaboard terdapat sedikit perbedaaan tata letak dengan raspberry Pi 2. Raspberry Pi 3 memiliki 40 pin GPIO, 4 port USB, sebuah port jaringan LAN 10/100 dan semua port lain seperti model-model sebelumnya.

Pada Raspberry pi 3 terdapat perubahan kecil untuk masalah kompatibilitasnya dengan add-on tertentu. Keuntungan utama dari Raspberry pi 3 adalah 64bit prosesor serta performa yang lebih baik dari pada model-model sebelumnya lalu memiliki built in wireless.

Jenis–jenis Rasberry Pi sebgai berikut:

1. Raspberry Pi model A
2. Raspberry Pi 3 Model B
3. Raspberry Pi 2 Model B

Raspberry pi 3 model B memiliki spesifikasi sebagai berikut:

1) SoC: Broadcom BCM2837, 64 Bit.
2) CPU: 4x ARM Cortex-A53, 1.2GHz.
3) GPU: Broadcom Video Core IV.
4) RAM: 1GB LPDDR2 (900 MHz)
5) Networking: 10/100 Ethernet, 2.4GHz 802.11n wireless.
6) Bluetooth: Bluetooth 4.1 Classic, Bluetooth Low Energy.
7) Storage: microSD.
8) GPIO: 40-pin header, populated.
9) Ports: HDMI, 3.5mm analogue audio-video jack, 4x USB 2.0, Ethernet, Camera Serial Interface (CSI), Display Serial Interface (DSI)

B. Penjelasan mengenai Kali Linux

Linux adalah proyek open source yang awalnya didirikan untuk menghasilkan kernel gratis yang di gunakan semua orang. Kernel adalah jantung dari system dari operasi yang menangani komunikasi antara pengguna dengan hardware.

Versi asli dari Linux di kombinasikan dengan sekumpulan tools yang di buat oleh sebuah group yang disebut GNU. System yang dihasilkan adalah system dasar tetapi powerful yang di kenal dengan nama GNU/Linux. Tidak seperti kebanyakan system operasi di zamannya, linux menawarkan fasilitas seperti multiple user account dimana beberapa pengguna berbagi dalam satu komputer. Selanjutnya rival dari Linux juga menerapkannya pada system operasinya. Dalam linux, kita akan menghabiskan sebagian besar waktu untuk menjalankan sebuah user account terbatas. Namun hal tersebut tidak berarti bahwa kita sangat di batasi atas apa yang kita lakukan, tetapi hal tersebut mencegah ketidak sengajaan untuk melakukan hal-hal yang merusak perangkat lunak kita dan juga mencegah virus malware lainnya untuk menginfeksi system.

Berikut ini adalah perintah Dasar untuk Kali Linux:

1. *Is*, perintah ini digunakan untuk melihat daftar isi dari sebuah direktori. Misalnya kita mengetik *Is/home* pada terminal maka akan menghasilkan daftar terkait isi dari direktori home.
2. cd, perintah ini di gunakan untuk berpindah direktori. Kita ketika mengetik cd saja pada terminal, maka secara otomatis akan ke direktori home kita. jikakita mengetik cd Bersama dengan nama direktori, maka kita akan berpindah ke direktori yang kita ketik. Sebagai catatan jika kita mengetik cd boot, maka kita akan pindah ke direktori boot di bawah direktori sekarang berada (direktori boot disini sebagai child dari direktori actual).

3. mv, adalah perintah move. Perintah ini memiliki dua tujuan, yaitu mengijinkan sebuah file di pindahkan dari satu direktori ke direktori lain dan mengijinkan mengganti nama file
4. rm, adalah perintah remove. perintah ini digunakan untuk menghapus satu file, semua file atau list file.
5. rmdir, perintah ini digunakan untuk menghapus direktori
6. mkdir, perintah ini digunakan untuk membuat direktori baru. Misalnya, mengetik mkdir MyFolder di terminal, perintah tersebut akan menciptakan sebauh direktori baru bernama MyFolder bawah direktori saat ini.

C. Penjelasan Mengenai Owasp Zap

Pengujian keamanan perangkat lunak adalah proses menilai dan menguji perangkat lunak untuk menemukan risiko keamanan dan kerentanan. Pengujian semacam itu bisa berupa pemindaian pasif untuk mencari kerentanan. Atau bisa juga berupa tes penetrasi aktif (alias tes pena) yang mensimulasikan pengguna jahat yang mencoba menyerang sistem.

Zap (Zed Attack Proxy) adalah alat open source untuk secara otomatis menemukan kerentanan dan meperbaiki bug dalam aplikasi web. Itu bagian dari Proyek Keamanan Aplikasi Web Terbuka (OWASP).

ZAP dapat digunakan sebagai man-in-the-middle antara browser dan server aplikasi. Itu juga dapat digunakan sebagai aplikasi mandiri, atau sebagai proses daemon tanpa UI. ZAP cocok untuk profesional keamanan berpengalaman serta pengembang web dan penguji fungsional.

Fitur – fitur yang terdapat pada Owasp zap:

1. Konteks: Biasanya, konteks akan sesuai dengan aplikasi web. Ini adalah cara pengelompokan satu set URL.
2. Lingkup: Didefinisikan oleh konteks, ini adalah set URL untuk diuji.
3. Mode: Setiap mode memungkinkan untuk jenis serangan tertentu. Ini memberikan fleksibilitas saat pengujian. Memilih mode mempengaruhi ruang lingkup.
4. Peringatan: Peringatan adalah potensi kerentanan. Itu terkait dengan permintaan. Permintaan dapat memiliki beberapa peringatan. Lansiran ditandai dengan tingkat risiko: Tinggi, Sedang, Rendah, Informasional, False Positive.
5. Tag: Teks pendek yang terkait dengan permintaan. Permintaan dapat memiliki beberapa tag. Pemindaian pasif dapat melakukan penandaan otomatis berdasarkan aturan yang telah ditetapkan
6. Catatan: dapat mengaitkan teks dengan permintaan. Ini untuk referensi atau tindakan selanjutnya.
7. Add-on: Tambahkan fungsionalitas tambahan ke inti ZAP. Mereka dapat diinstal dari Add-on Marketplace online. Contohnya termasuk Ajax Spider, Diff, Forced Browse, Fuzzer, dll.
8. Replacer: Ini adalah add-on untuk mengganti string dalam permintaan dan respons.

D. Empat Mode yang digunakan dalam Owasp Zap

1. Mode aman: Mode ini tidak memungkinkan bisa melakukan apa pun yang berpotensi berbahaya.
2. Mode terlindung: Mode ini memungkinkan bisa melakukan mensimulasikan kerentanan yang berpotensi berbahaya. Pengguna hanya dapat melakukan tindakan berbahaya pada URL yang disebutkan dalam ruang lingkup.
3. Mode standar**:** Dalam mode ini pengguna dapat melakukan apa saja yang relevan.
4. Mode ATTACK: Node baru dalam lingkup dipindai secara aktif segera setelah ditemukan.

E. Mengenali fitur spider dalam Owasp Zap

Laba-laba dan perayap web biasanya digunakan oleh mesin pencari untuk menemukan konten Internet. Dalam konteks ZAP, Spider adalah tambahan. Ini digunakan untuk secara otomatis menemukan sumber daya baru (URL) disitus tertentu. Itu dimulai dengan daftar URL untuk dikunjungi, disebut seed, yang tergantung pada bagaimana Spider dimulai. Spider kemudian mengunjungi URL-URL ini, mengidentifikasi semua hyperlink di halaman, dan menambahkannya ke daftar URL untuk dikunjungi. Proses ini berlanjut secara rekursif sampai sumber daya baru tidak ditemukan.

Selain menggunakan Spider, ada dua cara berbeda di mana ZAP mencari kerentanan terdiri dari:

1. Pemindaian Pasif: ZAP secara default memindai semua pesan HTTP (permintaan dan respons) yang dikirim ke aplikasi web secara pasif. Pemindaian pasif tidak mengubah permintaan dan respons dengan cara apa pun, dan karenanya aman untuk digunakan.
2. Pemindaian Aktif: Berusaha untuk menemukan kerentanan potensial dengan menggunakan serangan yang diketahui terhadap target yang dipilih. harus melakukan pemindaian aktif hanya jika memiliki izin untuk menguji aplikasi. Fuzzing adalah teknik yang dapat digunakan sebagai bagian dari pemindaian aktif. Dengan fuzzing, data yang tidak valid atau tidak terduga dikirimkan untuk menemukan kerentanan.

Kerentanan logis, seperti kontrol akses yang rusak, tidak akan ditemukan oleh pemindaian kerentanan aktif atau otomatis. Pengujian penetrasi manual harus selalu dilakukan selain pemindaian aktif untuk menemukan semua jenis kerentanan.

F. Cara Menggunakan Owasp Zap sebagai Proxy

ZAP dapat digunakan sebagai intersepsi proxy itu berdiri di antara browser penguji dan aplikasi web sehingga dapat mencegah dan memeriksa pesan yang dikirim, dan kemudian meneruskannya ke tujuan. Dalam pemindaian pasif, isi pesan tidak

dimodifikasi. Dalam pemindaian aktif, mereka dimodifikasi untuk mensimulasikan serangan.

Untuk menggunakan ZAP sebagai proksi, harus memperbarui konfigurasi dalam zap serta peramban yang ingin digunakan untuk pengujian. Mengkonfigurasi halaman Proxy di zap memberikan detailnya. Setelah mengonfigurasi zap sebagai proxy browser, sambungkan ke aplikasi web yang sedang diuji. Zap sekarang harus mulai menampilkan satu atau lebih entri di tab Situs dan Riwayat. Ini adalah permintaan dan tanggapan yang disadap ZAP untuk dianalisis.

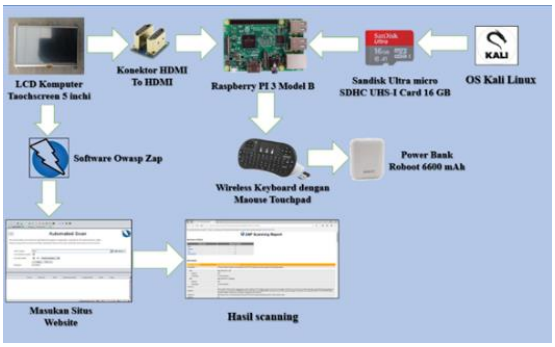
G. Cara Penggunaan Sertikat SSL Owasp zap di situs HTTPS.

Karena ZAP diatur untuk bertindak sebagai proksi antara browser dan aplikasi web, menggunakan SSL (HTTPS) akan menyebabkan validasi sertifikat gagal dan koneksi terputus. Ini karena zap mengenkripsi dan mendekripsi lalu lintas yang dikirim ke aplikasi web menggunakan sertifikat aplikasi web asli. Ini dilakukan agar zap dapat mengakses teks biasa dalam permintaan dan tanggapan.

Untuk mencegah kegagalan ini terjadi, zap secara otomatis membuat sertifikat SSL untuk setiap host yang diakses, ditandatangani oleh sertifikat Otoritas Sertifikat (CA) milik zap. Agar browser bisa mempercayai sertifikat SSL ini, harus terlebih dahulu mengimpor dan mempercayai sertifikat zap Root CA. Setelah dipercaya, sertifikat SSL zap lainnya yang ditandatangani olehnya akan dipercaya juga.

III. PERANCANGAN

A. Skema Rancangan Sebuah Sistem

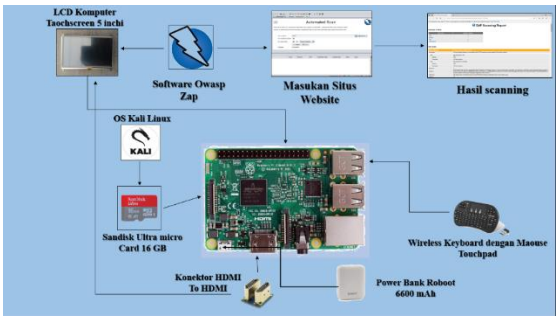


Gambar 1.2 Tampilan Rancangan Sebuah Sistem

Berikut ini beberapa komponen perancangan Hardware, softwre dan os secara keseluruhan yang di gunakan ditampilkan kedalam bentuk tabel sebagai berikut:

1. LCD Komputer Taouchscreen 5 Inchi, Fungsi nya digunakan untuk menampilkan sebuah informasi atau tampilan dari OS kali linux.
2. Konektor HDMI to HDMI, Fungsi nya digunakan untuk menyambungkan LCD ke port HDMI Raspberry pi 3 model B.
3. Raspberry PI 3 Model B, Fungsi nya digunakan untuk menjalankan sebuah program.
4. Sandisk Ultra Micro SDHC USH-I Card 16 GB, Fungsi nya digunakan untuk dimasukan ke OS kali linuk, dikarenakan untuk tempat penyimpanan OS kali linux harus memiliki spesifikasi tinggi minimal di 8GB.
5. OS Kali Linux, Fungsi nya digunakan untuk menampilkan sebuah operasi sistem dan penetrasi situs web.
6. Wireless Keyboard dengan Maouse Touchpad, Fungsi nya digunakan untuk kepentingan mengetik Program atau sebuah perintah kepada Raspberry yang memerlukan koneksi USB.
7. Power Bank Roboot 6600 mAh, Fungsi nya untuk menyalakan sebuah Portabel Komputer atau menjalankan sebuah sistem.
8. Software Owasp Zap, Fungsi nya untuk Menjalankan sebuah Test Penetrasi atau disebut paintes

B. Perancangan Sistem



Gambar 1.3 Perancangan Sistem

Berdasarkan gambar skema yang diatas bahwa pastikan sudah melakukan download os kali linux menggunakan USB card reader kemudian masukkan sd Card yang sudah terinstall os kali linux ke raspberry Pi, setelah itu pastikan lcd sudah di setting atau di program melalui monitor komputer menggunakan raspberry pi kemudian sambungkan atau satukan lcd touchscreen ke port GPIO menggunakan Konektor HMDI to HDMI ke raspberry pi selanjutnya sambungkan wireless keyboard dengan maouse Touchpad ke port usb dan yang terakhir sambungkan power bank ke port power in raspberry pi untuk menyalakan sebuah portabel komputer, kemudian pastikan sudah terinstall dan terpasang sebuah software owasp zap untuk menjalankan sebuah pentest.

C. Parameter Pengukuran dan Metode Pengujian Sistem

Parameter pengukuran dan pengujian sistem ini dilakukan untuk mengetahui tingkat keberhasilan dari alat yang telah dibuat dan apakah sesuai dengan yang diinginkan atau belum. Parameter ini diukur dengan

melakukan ringkasan peringatan atau disebut (Summary of Alerts) dan pengujian sistem ini menggunakan metode owasp zap dan os kali linux diperangkat portabel pc, ini dilakukan terhadap perangkat keras dan perangkat lunak yang digunakan, dimana proses pengujiannya adalah sebagai berikut:

1. Pengujian perangkat keras

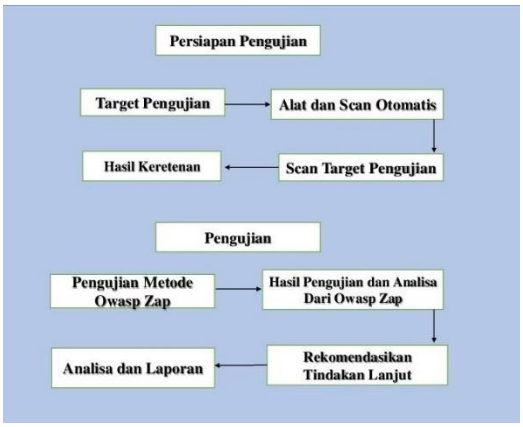
Pengujian dilakukan dengan memastikan perangkat yang digunakan antara lain seperti raspberry pi 3 model B, memory card Kartu sd 16 GB, lcd komputer taouchscreen 5 Inchi, konektor HDMI to HDMI, Wireless Keyboard dengan maouse touchpad dan power bank 6600 mAh. pengujian perangkat keras ini dilakukan untuk menjalankan instalasi os kali linuxm dan software owasp zap apakah berhasil atu tidak dan apakah sesuai dengan prosedur yang telah di rancang atau tidak.

2. Pengujian perangkat lunak

Pada tahapan uji coba perangkat lunak yang digunakan pada alat portabel pc ini adalah meggunakan software owasp zap dan os kali linux yang dilakukan dengan menjalankan pemrograman dan mealakukan scanning yang bertujuan untuk mengetahui keretanan pada sistem dan situs website, pada perangkat lunak ini modul-modul pada sistem bekerja dan melihat apakah hasil program tersebut dapat menjalankan perintah sesuai dengan prosedur sistem atau tidak.

D. Pengujian Fungsi Kerja Alat dan Cara Kerja Perangkat

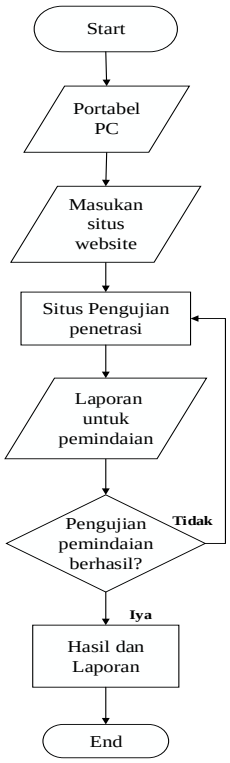
1. Pengujian fungsi kerja alat



Gambar 1.4 Topologi Pengujian Fungsi Kerja Alat

Berdasarkan Topologi di atas bahwa terlihat mulai dengan tahap persiapan pengujian lalu kemudian siapkan situs website yang ingin ditargetkan menggunakan alat dan scan otomatis kemudian mulai lah dengan melakukan scan target situs website lalu muncul hasil keretanan, kemudian Tahap pengujian ini menggunakan metode owasp Zap dan hasil dari pengujian nya dari owasp zap kemudian direkomendasikan untuk tindakan lanjut lalu dibuat laporan dan analisa.

2. Pengujian Cara Kerja Perangkat



Gambar 1.5 Flowchart Cara Kerja Perankat

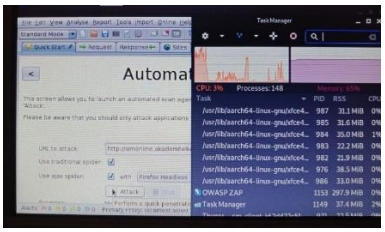
Pada flowchart yang diatas dapat dijelaskan bahwa portabel pc sebagai input dengan kondisi sudah terinstall dan terpasang dengan os kali linux dan software awasp zap setalah itu pastikan masukan sebuah situs website sebagai input untuk melakukan prosess situs pengujian penetrasi atau disebut pentest setalah itu hasil pemindaian dilaporan untuk pemindaian sebagai output kemudian jika pengujian hasil pemindaian tidak berhasil maka pastikan mengecek kembali ke situs pengujian penetrasi agar sistem dapat dipergunakan sebagai tingkat keamanan sebuah website, jika pengujian pemindaian nya berhasil langsung membuat sebuah laporan.

IV. Hasil Pembahasan

A. Pengujian Fungsi alat Menggunakan Portabel saat melakukan Test Pentrasi

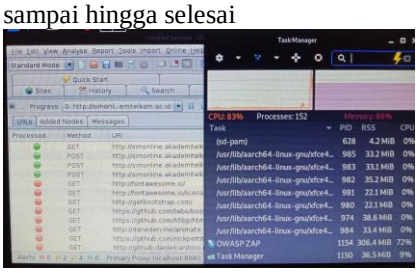
a. Target situs website http://simonline.akademitelkom.ac.id

1. Buka software Owasp Zap, Masukan Situs Website nya pilih “attack”



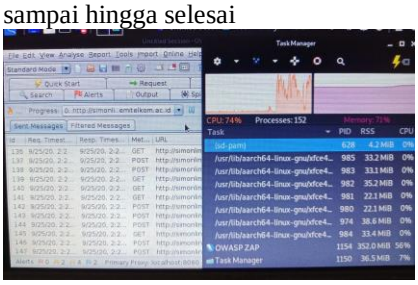
Disini bahwa portabel komputer saat melakukan masukan situs website dengan prosesor CPU 2% dan pemakaian RAM sebesar 65%

2. Tunggu Prosess pertama scanning sampai hingga selesai



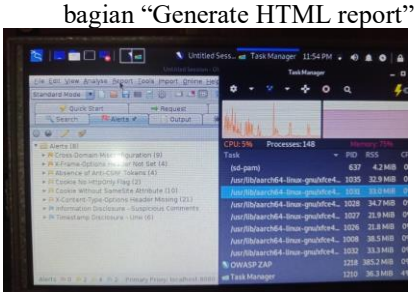
Disini bahwa portabel komputer sedang melakukan proses scanning pertama dengan prosesor CPU 83% dan pemakaian RAM sebesar 66%.

3. Tunggu Proses Kedua scanning sampai hingga selesai



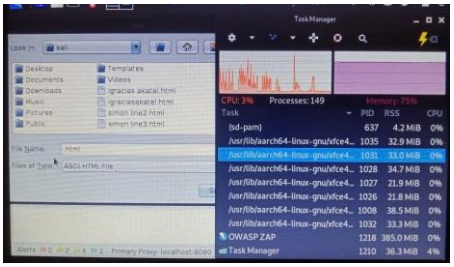
Disini bahwa portabel komputer sedang melakukan proses scanning kedua dengan prosesor CPU 74% dan pemakaian RAM sebesar 71%

4. Porses scanning telah selesaikemudian pilih “report” klik bagian “Generate HTML report”



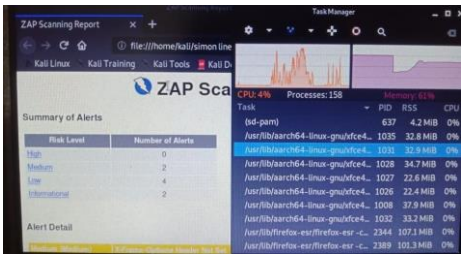
Disini diperlihatkan bahwa portabel komputer sudah menyelesaikan proses Test penetrasi dengan prosesor CPU 83% dan pemakaian RAM sebesar 65%

5. Simpan hasil file report di folder dengan format “contoh.html”



Disini diperlihatkan bahwa portabel komputer sedang melakukan report hasil Test penetrasi dengan prosesor CPU 3% dan pemakaian RAM sebesar 75%

6. buka hasil report nya di folder



Disini diperlihatkan bahwa portabel komputer sudah menyelesaikan hasil report Test penetrasi dengan prosesor CPU 83% dan pemakaian RAM sebesar 65%

7. peneliti akan membuat sebuah laporan hasil dari scanning Tets penetrasi sebagai berikut

Target: http://simonline.akademitelkom.ac.id
Peringkat: Medium
Temuan: X-Frame-Options-Header No Set

Dampak: X-Frame-Options-Header bahwa Tidak disertakan dalam respon HTTP untuk bisa melindungi terhadap serangan Clickjacking

Analisa: Berdasarkan Analisa pada X-frame options merlihatkan bahwa untuk menghindari serangan clickjacking harus menggunakan X-frame-options dengan memastikan tidak disematkan ke situs X-frame-options. Bahwa untuk menggunakan DENY (Deny adalah halaman tidak dapat menampilkan dalam bingkai) maka memuat halaman dalam bingkai akan gagal saat dimuat dari situs lain, upaya untuk melakukannya akan gagal saat dimuatkan situs yang sama, sedangkan memakai SAMEORIGIN dapat menggunakan halaman website dengan bingkai selama situs itu memasukannya kedalam bingkai sama dengan situs yang menjajikan.

Peringkat: Medium

Temuan: Cross-Domain Misconfiguration

Dampak: Serangan Cross-Domain Misconfiguration Bahwa pemuatan data mungkin karena kesalahan konfigurasi (CORS) atau disebut dengan Cross Orgin Resource Sharing dibagian web server.

Analisa: Berdasarkan Analisa bahwa menggunakan alamat IP white – listing, misal nya menkonfigurasi sebuah header HTTP karena bahwa data sensitif tidak tersedia atau disebut dengan terauthenticated. CORS atau disebut dengan Cross Orgin Resource Sharing pastikan menerapkan kebijakan asal yang sama yaitu SOP dengan cara yang lebih ketat.

Peringkat: Low

Temuan: X-Content-Type-Options Header Missing

Dampak: serangan X-Content-Type-Options Header Missing Hal ini memungkinkan versi internet Exsplorer dan chrome menggunakan versi lebih lama untuk melakukan MIME-sniffing pada isi tanggapan yang berpotensi meyebabkan tanggapan diinterpretasikan

Analisa: Berdasarkan Analisa bahwa menggunakan web Browser itu harus dengan sesuai dengan standar modern yang tidak melakukan sniffing MIME karena akan menolak tanggapan dengan jenis MIME akan salah jika server akan mengirimkan header X-content-type-options. dan pastikan bahwa server atau web menetapkan header dengan banar contoh X-content-type-options: nosniff, X-frame-options: sameorogin dan X-XSS-protection untuk semua halaman situs website.

Peringkat: Low

Temuan: Cookie No HTTP Only Flag

Dampak: Serangan Cookie No HTTP

Only Flag bahwa Cookie dapat diakses oleh javaskript, jika javaskript berbahaya dapat dijalankan oleh orang lain karena Cookie bisa diakses dan bisa ditransmisikan kesituslain mungkin bisa terjadi pembajakan.

Analisa: Berdasarkan Analisa bahwa cookie sebagai httponly ini tidak terpasang atau dinonaktifkan kedalam server web karena bisa terjadi pembajakan melaui javascrip maka dari itu pastikan mengatur flaghttp only ke semua cookie.

Peringkat: Low

Temuan: Cookie without same site attribute

Dampak: Cookie without same site attribute ditetapkan bahwa dengan nilai atribut samesite berarti bahwa cookie dapat dikirim sebagai akibat dari permintaan lintas situs, atribut same site adalah langkah penghitung yang efektif untuk pemalsuan permintaan lintas situs.

Analisa: berdasarkan Analisa bahwa atribut same site diatur ke LAX karena cookie akan dikirim bersama dengan permintaan GET yang diperiksa oleh situs website.

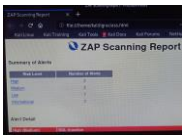
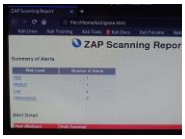
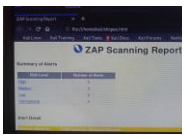
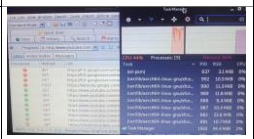
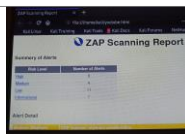
Peringkat: Low

Temuan: Absence of Anti-CSRF Tokens

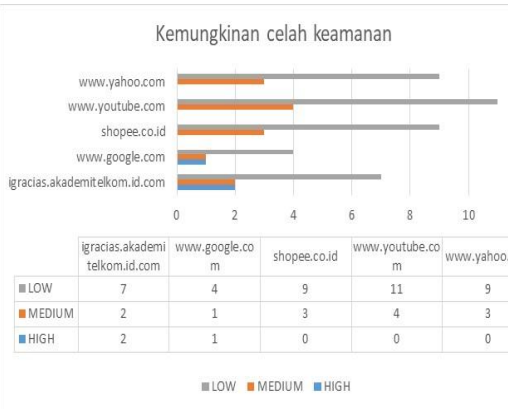
Dampak: Absence of Anti-CSRF Tokens bahwa serangan yang melibatkan memaksa korban untuk mengirim permintaan HTTP ke tujuan target tanpa sepengetahuan atau niat mereka untuk melakukan tindakan sebagai korban. Penyebab utamanya adalah fungsionalitas aplikasi menggunakan tindakan URL / formulir yang dapat diprediksi dengan cara yang dapat diulang. Sifat serangannya adalah CSRF mengeksploitasi kepercayaan yang dimiliki situs web kepada pengguna

Analisa: Berdasarkan Analisa bahwa menggunakan CSRF atau disebut dengan Cross site request forgery bahwa sebuah serangan yang dipaksakan oleh pengguna agar bisa mengeksekusi perintah yang tidak seharus nya di izinkan dan pastikan bahwa aplikasi nya bebas dari masalah skrip karena sebagian besar pertahanan CSRF itu dapat dilewati menggunakan scrip yang dikendalikan penyerang

B. Pengujian Test penetrasi menggunakan owasp zap dengan pernagkat portabel komputer terhadap 5 situs website

Domain situs	Proses Test penetrasi	Hasil Scanning
Akatel		
google		
shopee		
youtube		

Dari proses Scanning yang telah dilakukan didapat hasil kemungkinan terdapat celah keamanan pada 5 situs website yang berdomain Google, Youtube, Yahoo, Shopee dan Akatel.



	igracias.akademitelkom.id.com	www.google.com	shopee.co.id	www.youtube.com	www.yahoo
LOW	7	4	9	11	9
MEDIUM	2	1	3	4	3
HIGH	2	1	0	0	0

C. Tabel performa portabel komputer saat melakukan test pentrasi pada situs sebagai berikut:

Domain situs	Pengujian	Performa perangkat	Kondisi Perangkat
Igracias.akademitelkom	Performa CPU	79%	Tidak ada kendala
	Perforam RAM	69%	Tidak ada Kendala
www.google.com	Performa CPU	67%	Tidak ada Kendala
	Performa RAM	72%	Tidak ada kendala
Shoppe.co.id	Performa CPU	63%	Tidak ada Kendala
	Performa RAM	72%	Tidak Ada Kendala
www.youtube.com	Performa CPU	44%	Tidak ada kendala
	Performa RAM	86%	Sedikit lag
www.yahoo.com	Performa CPU	28%	Tidak ada kendala
	Performa RAM	87%	Sedikit lag

Jika dilihat data tabel di atas sudah menunjukkan bahwa saat melakukan Tets penetrasi pada perangkat mengalami kondisi berbeda beda tergantung domain apa yang sedang di scanning. Yang dimana saat melakukan pada Test pentrasi situs web akatel dengan kondisi performa CPU 79% dan RAM 69%, yang dimana pada kondisi ini peneliti tidak merasakan adanya kendala pada perangkat berupa lag, atau hang sama dengan seperti situs web google dengan kondisi performa CPU 67% dan RAM 72% tidak merasakan adanya kendala pada perangkat sama seperti situs website shopee dengan kondisi 63 % dan 72% beda dengan situs website youtube kondisi performa CPU 44% RAM 86% mengalami penurunan performa sama seperti situs website yahoo dengan kondisi performa CPU 28% dan RAM 87 % yang dimana mengalami penurunan peforma pada perangkat.

V PENUTUP

A. Kesimpulan

Setelah peneliti meyelesaikan pembuatan perangkat dan telah berhasil melakukan serangkaian pengujian terhadap perangkat maka dapat diambil kesimpulan.

1. Pada saat penginstallan portabel komputer melakukan dengan baik berjalan dengan sesuai harapan
2. Dari Test Pentrasi yang dilakukan peneliti kebeberapa situs website peneliti menyimpulkan bahwa dari 5 situs website yang di scanning bahwa situs akatel dan google memiliki banyak masalah di keamanan nya jika dilihat dari data tabel pengujian akatel memiliki keretanan pada level High 2 medium 2 low 7 di ikuti oleh google dengan level High 1 medium 1 low 4 kemudian di ikuti oleh youtube medium 4 low 11 kemudian di ikuti oleh shoope medium 3 low 9 kemudian di ikuti oleh yahoo medium 2 low 12.
3. Setelah melakukan test penetrasi terhadap beberapa situs website peneliti saat melakukan test penetrasi pada masing-masing situs dengan keadaan yang berbeda-beda, jika dilihat dari table pengujian sejak pertama perangkat di hidupkan peneliti melakukan test penetrasi terhadap situs website yahoo yang dimana menghabiskan 28% dilanjuti dengan youtube, shopee, google dan akatel dengan hasil nya semakin lama alat bekerja penggunaan cpu semakin banyak juga cpu yang terkuras

Saran

Setelah peneliti meyelesaikan pembuat perangkat portabel komputer dan telah berhasil melakukan fungsi pengujian pada perangkat portabel saat melakukan test penetrasi pada situs website, peneliti juga memberikan saran yang bertujuan untuk mdapat dijadikan bahan pengembangan dari perangkat portabel komputer yaitu:

1. Menambahkan RAM lebih dari 1GB dan menambahakan memory sd card melebihi 16 GB agar para pekeraja bisa melakukan Tespenetrasi pada situs website.
2. Menggunakan ukuran LCD touchreen lebih dari 5 inci touchreen agar bisa melihat lebih jelas para pekerja.
3. Menggunakan power bank dengan kapasitas 10.000 ribu Mah agar bisa melakuan Test penetrasi menjadi lebih lama.

DAFTAR PUSTAKA

Wicaksonomudah, M.F. (2018). Mudah Belajar Raspberry pi Bandung BI obsess: Informatika

Kadir, A. (2017). Panduan Praktis untuk Mempelajari Pemrograman perangkat keras menggunakan Raspberry Pi Model B. Yogyakarta:

Rakman, E. (2015). Raspberry Pi-Mikrokontroler Mungil Yang serba bisa Yogyakarta:

Samuel, P. (2015). Jaringan komputer linux: konsep Dasar aplikasi Keamanan Yogyakarta:

Syahputra, A. (2015). Jaringan Berbasis Linux. Yogyakarta:

Suharyanto, C.E. (2019). Pemanfaatan minicomputer raspberry sebagai network monitoring tool portabel. Jurnal: ilmu pengetahuan dan teknologi, 5, 2527-4864.

Abrar, A. (2017). Server portabel berbasis Raspberry pi sebagai media pembelajaran di politeknik negri balik papan. Jurnal: sains terapan, 2, 2406-8810.

Rudito, A.R. (2015). Pembuatan server portabel berbasis raspberry pi untuk mendukung pelaksaan assessment. Jurnal: e-proceeding off applied science, 1, 2442-5826. (hlm. 21-96)

Basuki, A. (2018). Analisis performansi raspberry-pi box sebagai portabel server Moocs. Jurnal: EECCIS, 12, 2

Dewanto, A.P. (2018).Penetration Testing pada Domain UII.AC.ID menggunakan Owasp 10. (Laporan Tugas Akhir) jurusan Teknik Informatika, Falkustas Teknologi inudstri, Universitas Islam indonesia, Yogyakarta.

.