Penerapan Sectigo Positive Ssl Pada Pengamanan Web Site

Khairullah, Evita Rahmadona, Rozali Toyib, Muhammad Imanullah

[1,2, 3,4] Program Studi Teknik Informatika Fakultas Teknik Universitas Muhammadiyah Bengkulu.
Email: khairullah@umb.ac.id, evitarahmadona48@gmail.com, rozalitoyib@umb.ac.id, muhammad.iman@umb.ac.id
Jl. Bali, Po Box 118 Telp. (0736) 22756 Fax. (0736) 26161 Fakultas Teknik Universitas Muhammadiyah Bengkulu

(Received: Nopember 2024, Revised : Februari 2024, Accepied : April 2024)

Abstract-System security is the most important aspect in an information system, weak system security increases the risk of attacks that can cause system damage. One of the attacks that often occurs is an attack on a web server, this is because the web server is connected to the internet network and is accessed by many users widely, so the risk of attack increases. For example, the New Student Admission web site of Universitas Muhammadiyah Bengkulu, which manages data on prospective new students who have registered themselves. So that a web server security system is needed to avoid potential attacks and to increase data security. One method of securing a web server is by using the Secure Socket Layer (SSL). SSL is often used to secure communication between client and server. The stages carried out in this study are scanning web servers that have not used SSL and those that have used SSL. This research aims to determine the security of web servers and anticipate various potential attacks on web servers.
Keywords: Web server, Secure Socket Layer, data and network security.

Intisari-Keamanan sistem merupakan aspek terpenting dalam sebuah sistem informasi, lemahnya keamanan sistem meningkatkan resiko serangan yang dapat menimbulkan kerusakan sistem. Salah satu serangan yang sering terjadi adalah serangan pada web server, hal tersebut dikarenakan web server terkoneksi dengan jaringan internet dan di akses oleh banyak user secara luas, sehingga resiko serangan menjadi meningkat. Sebagai contoh web site Penerimaan Mahasiswa Baru Universitas Muhammadiyah Bengkulu, yang mengelola data calon mahasiswa baru yang sudah mendaftarkan diri. Sehingga diperlukan sistem pengamanan web server untuk menghindari potensi serangan dan untuk mengingkatkan keamanan data. Salah satu metode dalam mengamankan web server dengan menggunakan Secure Socket Layer (SSL). SSL sering digunakan untuk mengamankan komunikasi antara client dan server. Tahapan yang dilakukan dalam penelitian ini adalah melakukan scaning pada web server yang belum menggunakan SSL dan yang sudah menggunakan SSL. Penelitian ini bertujuan untuk mengetahui keamanan web server dan mengantisipasi berbagai potensi serangan pada web server.
Kata kunci : Web server, Secure Socket Layer, Keamanan data dan jaringan.

I. PENDAHULUAN

.[1] Banyak hal yang bisa dilakukan terhadap data-data penting. Setelah seseorang berhasil mendapatkan data yang diinginkan, data itu bisa diperjualbelikan. Ada oknum yang menjual data pengguna, adapula oknum yang rela membelinya. *Phishing* adalah akrivitas *cyber crime* yang secara illegal mengambil data-data penting, seperti informasi terkait *banking* hingga *password* perangkat. Biasanya serangan *phishing* ini dilancarkan melalui SMS, *email*, dan telepon yang masuk HP. *Phishing* merupakan bentuk *cyber crime* yang saat ini tengah marah terjadi dengan pelaku akan membuat korbannya memberikan informasi pribadi secara sukarela. Pelaku biasanya menggunakan *website* dan email yang menyerupai versi resminya untuk kemudian menuntuk korban agar mengikuti arahan yang diinstruksikan. Setelah itu, informasi pribadi korban yang berhasil dicuri akan dimanfaatkan untuk melakukan kejahatan lainnya seperti menipu. Prinsip operasi kejahatan phising sebagai salah satu jenis kejahatan dunia maya di dasarkan pada digital pada data digital calon korban, pada tahap awal biasanya penjahat mengidentifikasi calon korban. Biasanya pemegang target adalah pembayaran elektronik atau rekening bank online. Penjahat membuat situs web dan email palsu, yang kemudian di distribusikan ke target. Maka dari itu, keamanan data itu sangat penting bagi individu maupun perusahaan karena setiap informasi itu berharga. Informasi seperti nama, alamat, nomor HP, KTP, dan sebagaiana mungkin terkesan biasa saja dan tidak membahayakan. Namun, jika informasi sensitive seperti ini jatuh di tangan orang yang tidak bertanggung jawab, maka dipastikan akan rugi jika hal itu terjadi. Ketika diterapkan dengan benar, strategi *data security* yang baik dan akan dapat melindungi aset data dan informasi dari aktivitas kejahatan *cyebr*, ancaman orang dalam dan kesalahan manusia. Oleh karena itu, *data security* adalah hal yang sangat wajib diterapkan oleh setiap pengguna website dan data lainnya untuk menganmankan nya. Ada berbagai macam jenia keamanan data yang bisa diterapkan, seperti Enkripsi (*Encryptyion*), Kontrol Akses (*Access Control*), Autentukasi (*Authentucation*), Pencadangan dan Pemulihan (*Backup and Recovery*), Penghapusan Data (*Data Erasure*), Penyamaran Data (*Data Masking*), dan Ketahanan Data (*Data Resiliency*). Saat ini banyak website yang telah menggunakan Secure Socket Layer (SSL), bukan tanpa alasan, melainkan SSL ini memiliki banyak sekali manfaat tersembunyi dari berbagai aspek, seperti keamanan, SEO, dan lain- lain. SSL itu sendiri adalah teknologi keamanan standar untuk mendirikan sebuah link yang terenkripsi antara klien dan server, sehingga tidak ada yang dapat mencuri informasi yang dikirimkan. SSL berjalan di antara layer aplikasi dan layer network, tepatnya berada pada layer transportasi yang bertugas membawa data dan informasi yang sudah terenkripsi.Keamanan informasi merupakan suatu praktik, atau tahapan yang dirancang dan diimplementasikan untuk melindungi suatu informasi atau data pribadi melalui akses, penggunaan, penyalahgunaan, gangguan, atau modifikasi yang tidak valid. Website merupakan halaman informasi

P-ISSN 1858-2680
e-ISSN 2723-4673

yang didapatkan via internet sehingga bisa diakses oleh seluruh dunia selama masih terkoneksi dengan internet. Keamanan dalam suatu sistem tentunya sangat dibutuhkan untuk menjaga integritas data yang terkandung dalam sistem tersebut [2]. Hypertext Transfer Protocol Source (HTTPS) adalah versi aman protocol HTTP yang menggunakan SSL/TLS Protokol untuk enkripsi dam otentikasi. Protokol HTTPS memungkinkan pengguna situa web untuk mngirimkan data sensitive seperti nomor kartu kredit, informasi perbankan dan kredensial login denngan aman melalui internet, untuk allasan ini HTTPS sangat penting unutk mengamankan aktivitas online seperti belanja, perbankan dan pekerjaan jarak jauh. Namun, HTTPS dengan cepat menjadi protocol standar untuk semua situs web, baik mereka bertukar data sensitive dengan pengguna atau tidak. HTTPS juga menambahkan **enkripsi, pembuktian keaslian,** dan **integritas** ke protocol HTTP. Karena HTTP pada awalnya dirancang sebagai protocol teks yang jelas, ia rentan terhadap penyadapan. Dengan menyertakan SSL/TLS enkripsi, HTTPS mencegah data yang dikirim memalui internet disadap dan dibaca oleh pihak ketiga. Melalui kriptografi kunci public dan SSL/TLS, sesi komunikasi terenkripsi dapat diatur dengan aman antara dua pihak yang belum pernah bertemu secara langsung melalui pembuatan kunci rahasia bersama. Keamanan perangkat lunak memainkan peran penting dalam banyak aspek keamanan siber. Untuk melindungi web server dari serangan pihak yang tidak bertanggung jawab, sebaiknya pengujian web server harus dilakukan dengan melakukan selftest pada sistem web server itu sendiri menggunakan metode penetration testing [3].

II.TINJAUAN PUSTAKA

A. Website

Menurut Bekti (2015:35) Website merupakan kumpulan halaman-halaman yang digunakan untuk menampilkan informasi teks, gambar diam atau gerak, animasi, suara dan atau gabungan dari semuanya, baik yang bersifat statis maupun dinamis yang berbentuk satu rangkaian yang saling terkait, yang masing-masing dihubungkan dengan jarigan-jaringan halaman. Situs web (*website*) adalah sekumpulan halaman web yang saling berhubungan yang umumnya berada pada peladen yang sama berisikan kumpulan informasi yang disediakan secara perorangan, kelompok, atau organisasi.[2] Sebuah situs web biasanya ditempatkan setidaknya pada sebuah server web yang dapat diakses melalui jaringan seperti Internet, ataupun jaringan area lokal (LAN) melalui alamat Internet yang dikenali sebagai URL. Gabungan atas semua situs yang dapat diakses publik di Internet disebut pula sebagai World Wide Web atau lebih dikenal dengan singkatan WWW. Meskipun setidaknya halaman beranda situs Internet umumnya dapat diakses publik secara bebas, pada praktiknya tidak semua situs memberikan kebebasan bagi publik untuk mengaksesnya, beberapa situs web mewajibkan pengunjung untuk melakukan pendaftaran sebagai anggota, atau bahkan meminta pembayaran untuk dapat menjadi anggota untuk dapat mengakses isi yang terdapat dalam situs web tersebut, misalnya situs-situs yang menampilkan pornografi, situs-situs berita, layanan surel (*e-mail*), dan lain-lain. Pembatasan-pembatasan ini umumnya dilakukan karena alasan keamanan, menghormati privasi, atau karena tujuan komersial tertentu.

B. Internet

Menurut Simarmata (2010:47) Internet adalah sekelompok atau kumpulan dari jutaan computer. Penggunaan internet memungkinkan kita untuk mendapatkan informasi dari computer yang ada didalam kelompok tersebut dengan asumsi bahwa pemilik computer memberikan izin akses. Untuk mendapatkan sebuah informasi, sekumpulan protokol harus digunakan, yaitu sekumpulan aturan yang menetapkan bagaimana satu informasi dapat dikirim dan diterima. Internet adalah jaringan global yang terdiri dari jaringan komputer yang saling terhubung menggunakan protokol komunikasi standar. Secara sederhana, internet adalah infrastruktur global yang memungkinkan komunikasi dan pertukaran informasi antara jutaan pengguna di seluruh dunia.

Web server sendiri merupakan wadah untuk menopang sebuah *website* yang berisikan informasi, konten, maupun akun surel atau *email* pengguna, sekaligus sebagai penghubung antara *server* dan *client* dalam pengiriman perolehan informasi dan data serta mempercepat dan mengorganisasikannys secara terpusat. *Web server* sendiri menggunakan port 80 dan terdiri dari 2 komponen, yaitu perangkat computer dan *software web server* yang dipakai, yang dimana *web server* inilah yang akan menopang *website* yang ditujukan kepada *client* atau pengguna untuk memberikan dan bertukar informasi. *Web server* juga terdapat beberapa jenis antara lain : *Nginx, Apache Tomcat, Apache Web Server, Microsoft Windows Server, Ligh HTTP, Internet Information Server (IIS), Sun Java System Web Server, dan Zerus Web Server*. Dan terkhusus untuk *Hosting Server*, hanya akan berfokus pada implementasi *web server* yang membahas bagaimana kinerja *web server* yang akan diimplementasikan (Aziz & Tampati, 2015)

Web Browser

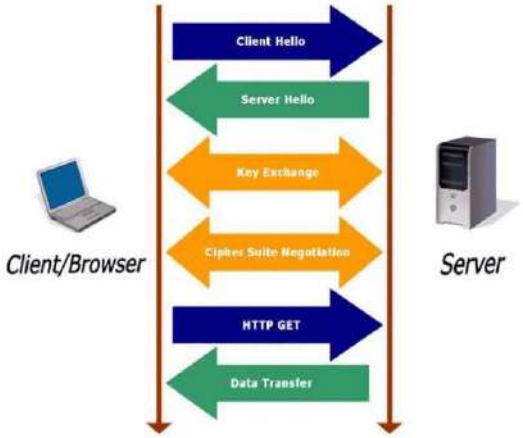
Web Browser atau diringkas browser adalah program atau software yang dirancang untuk mencari dan menampilkan dokumen web dalam bentuk formal HTML. Dengan browser, para pengguna computer dapat mencari dan menelusuri (browser) serta melihat isi dari dokumen wes dan berpindah dari sebuah tempat (halaman) ke tempat lain di web. Contoh program browser yang popular misalnya internet expoler, netscape, opera, mozila, dan lainnya.

Menurut Rosa dan Shalahuddin (2013:48) system basis data adalah system terkomputerisasi yang tujuan nya adalah memelihara data yang sudah diolah

P-ISSN 1858-2680
e-ISSN 2723-4673

atau informasi dan membuat informasi tersedia saat dibutuhkan. Pada intinya basis data adalah media untuk penyimpanan data agar diakses dengan mudah dan Vulnerability dapat didefinisikan sebagai kerentanan jaringan komputer atau lubang keamanan, dan kerentanan keamanan dipahami sebagai kelemahan program/infrastruktur yang memungkinkan sistem untuk dieksploitasi. Kerentanan ini disebabkan oleh kesalahan desain, pembuatan, atau implementasi sistem. Kerentanan ini digunakan sebagai sarana bagi peretas untuk mendapatkan akses tidak sah ke sistem. Peretas sering mengeksploitasi kerentanan yang ditemukan [8].

Secara umum, cara kerja protokol SSL adalah sebagai berikut :



Gambar 1 Prinsip Kerja SSL

Celah keamanan yang paling umum untuk SSL dating dari empat area : *certificate distribution, authentication, failure handling, dan dari lower-layer protocols*. Vulnerability (kerentanan) adalah kondisi atau kelemahan dalam suatu sistem yang dapat dimanfaatkan oleh penyerang untuk melakukan serangan atau akses yang tidak sah. Keberadaan vulnerability dapat mengancam keamanan dan integritas sistem, serta menyebabkan kerugian yang signifikan, seperti kebocoran data, kerusakan infrastruktur, atau pencurian informasi sensitif.

Nmap atau Network Mapper adalah aplikasi terbuka yang dipakai khusus untuk eksplorasi jaringan dan audit keamanan jaringan. Fyodor Vaskovich adalah orang yang pertama kali mengembangkan Nmap pada tanggal 1 September 1997. Fyodor Vaskovich adalah salah satu pendiri Honeynet project yaitu sebuah organisasi yang melakukan riset untuk keamanan jaringan computer (Abdullah, 2016). Nmap dirancang untuk memeriksa jaringan besar secara cepat, meskipun ia dapat pula bekerja terhadap host mana saja yang tersedia pada jaringan, layanan apa yang diberikan, system operasi dan versinya apa yang digunakan, dan sejumlah karateristik lainnya.

a. Nmap –sF
   Teknik ini mengirim suatu paket FIN ke port sasaran. Berdasarkan RFC 793,, system sasaran akan mengirimkan balik suatu RST untuk setiap port yang tertutup.
b. Nmap –A
   Nmap –A adalah perintah yang memberi tahu Nmap untuk menentukan dan menampilkan informasi Operation Sistem tentang host/ip target. Nmap –A bisa juga disebut sebagai agrsif scanning karena hasil dari scanning menggunakan perintah tersebut sangat lengkap.
c. Nmap –O
   Nmap –O memungkinkan deteksi OS untuk host atau rentang host.
d. Nmap –sV
   Untuk mendeteksi informasi layanan dan versi. Pengguna jahat biasanya menggunakan ini untuk memeriksa apakah host menjalankan layanan yang rentan atau tidak.
e. Nmap –sX
   Teknik ini mengirimkan paket FIN, URG dan PUSH ke port sasaran. Berdasarkan RCF 739, system sasaran akan mengembalikan suatu RST untuk semua port yang tertutup.

1) Kali Linux

Kalilinux merupakan sistem operasi berbasis linux debian yang di kembangkan oleh Offensive Security. Kalilinux memiliki tampilan sederhana dan tidak terlalu mencolok dan penggunaanya pun tergolong cukup mudah, sehingga kalilinux sangat baik untuk para pemula yang sedang belajar dalam melakukan penetrasi pada sistem, jaringan dan aplikasi. Selain terdapat di PC, Kalilinux juga memiliki versi yang terdapat di Android yang disebut KaliNethunter yang memiliki fungsi yang sama. Kalilinux merupakan reinkarnasi dari sistem operasi legenda BackTrack, salah satu distri Linux yang diciptakan secara khusus supaya bisa memenuhi keperluan dalam penetration juga testing di sebuah system serta keamanan pada komputer. Dengan pengembangan Kalilinux diharapkan akan lebih stabil serta powerful dari generasi sebelumnya “BackTrack” [10].

III. METODE PENELITIAN

A. Metode

Metodelogi pengujian perangkat lunak merupakan suatu proses pengorganisasian dengan kumpulan metode dan kovensi notasi yang telah didefinisikan untuk mengembangkan perangkat lunak. Secara prinsip ini bertujuan untuk membantu menghasilkan perangkat lunak yang berkualitas.

B. Metode Pengumpulan Data

1. **Analisa**

Tahapan pertama dalam penelitian adalah analisa kebutuhan, sehingga peneliti bisa mempersiapkan apa saja yang dibutuhkan agar penelitian ini berjalan dengan lancar. Kebutuhan yang disiapkan adalah yang behubungan dengan rancangan bangun

P-ISSN 1858-2680
e-ISSN 2723-4673

pengujian, protocol ssl, web yang akan diuji, dan aplikasi pengujian yang akan digunakan. Salah satu proses penting dalam penelitian adalah mengumpulkan data-data yang dibutuhkan yang berhubungan dengan topic penelitian. Untuk mengumpulkan data-data tersebut penulis akan menggunakan metode sebagai berikut :

Suatu cara mengumpulkan data yang digunakan untuk memperoleh informasi langsung dari sumbernya. Wawancara ini.

Observasi

Dalam hal ini observasi dilakukan secara formal maupun informal untuk mengamati secara kualitatif berbagai kegiatan dan peristiwa yang terjadi. Dalam penelitian ini perlu dilakukan observasi untuk memperoleh data atau informasi yang lebih spesifik tentang pengujian system web site yang terlah tersedia.

Studi Pustaka

Studi pustaka yaitu pengumpulan data yang bersumber sari arsip/dokumen yang terdapat data yang bersumber dari buku kepustakaan, hasil penelitian dan dokumen yang berhubungan dengan penlitian ini.

Analisis system

Pada tahapan ini dilakukan analisis kebutuhan dari software yang akan diuji, merupakan persiapan aplikasi, fungsi/proses yang dibutuhkan dan analisis kebutuhan.

Pengujian

Pada tahap ini dilakukan pengujian software yang tersedia dan suda terinstal. Pengujian in dilakukan untuk mengetahui apakah software yang telah sesuai dengan desain dan apakah berjalan sesuai instruksi yang telah dimasukkan.

IV.HASIL DAN PEMBAHASAN

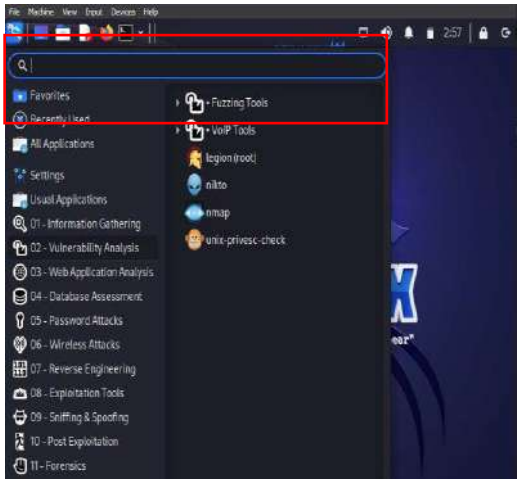
A. Hasil

Hasil dari penerapan sectigo positive SSL pada pengamanan web site sebagai berikut :

1) Mengetahui bahwa website yang diuji belum sepenuhnya aman dari vulnerability dan rentan Sniffing.
2) Implementasi SSL untuk pengamanan Website sangat dianjurkan.

Adapaun tampilan dari hasil sistem yang telah diuji adalah sebagai berikut :

Pengujian pada website menggunakan Nikto dan Nmap



Gambar 2. Aplikasi pengujian yang digunakan

Scan website bklvision.com

Gambar 3. Mengetahu IP Address

Gambar 3 merupakan gambar hasil dari scan Nmap untuk mengetahui IP Address dan Domain dari website yang diuji keamanan nya menggunakan nikto. Didapatkan bahwa IP Address dari bklvision.com adalah 202.52.146.162.

Scan domain

Gambar 4. Domain yang digunakan

Pada scan Nmap diatas dapat diketahui bahwa domain yang digunakan dalam website bklvision.com secara lengkap dan rinci, yaitu BKLVISION.COM, domain id, domain server, update, membuat, dan lain nya.

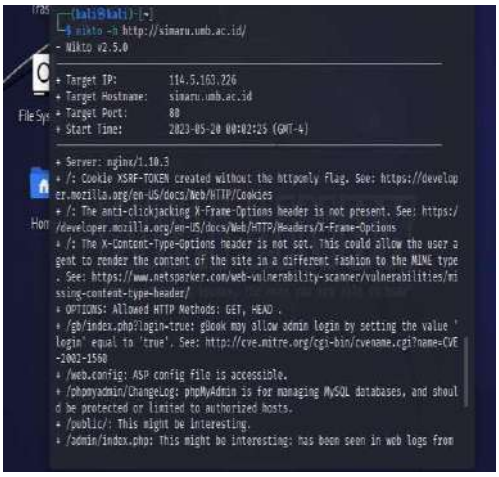
Scan Nikto website dengan –ssl dan -Tuning 9

P-ISSN 1858-2680
e-ISSN 2723-4673

Gambar 5. Port, Hostname dan Chiphers

Gambar 5 diatas berisi informasi tentang Port, Hostname dan Chiphers yang digunakan didalam website. –Tuning 9 merupakan perintah scan nikto untuk mengetahui kerentanan SQL Injection.

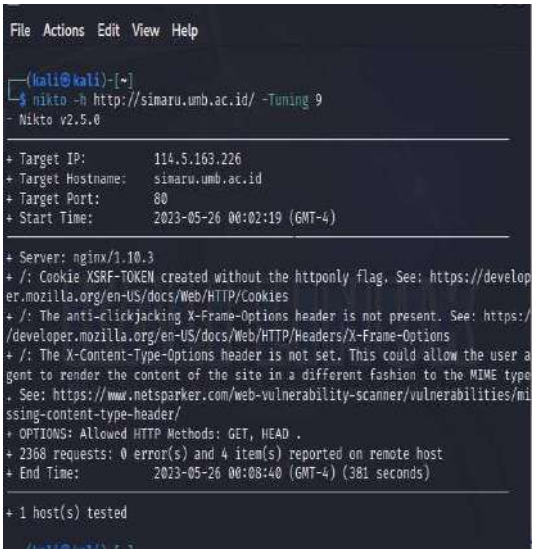
Scan nikto pada website simaru.umb.ac.id



Gambar 6. Scan Website simaru.umb.ac.id

Pada gambar diatas memberikan informasi mengenai Ip Address, Port dan hostname pada website simaru umb.ac.id. didapatkan dadat yaitu IP Address dari simaru umb.ac.id adalah 114.5.163.226, juga port 80 dengan hostname simaru.umb.ac.id. Terdapat beberapa informasi juga mengenai vulnerability pada website tersebut.

Scan website simaru.umb.ac.id dengan –Tuning 9



Gambar 7 Scan dengan –Tuning 9

Pada gambar 7 diatas terdapat beberapa informasi mengenai scan yang telah dilakukan nikto, perintan –Tuning 9 untuk mengetahui kerentanan SQL Injection pada website simaru.umb.ac.id.

Scan website bklvision.com dengan Nmap

Gambar 8. Scaning Open Port Menggunakan Nmap

Pada gambar diatas adalah sebuah scanning Open Port dengan menggunakan NMAP pada Operating Sistem Linux Ubuntu. Terdapat 5 open port yang ada pada system bklvision.com yang terdiri dari port 465, 587, 993, 995 dan 3306. Tugas dari port-port tersebut adalah :

465 merupakan yang digunakan jika ingin mengirimkan pesan menggunakan SMPT dengan jalur yang aman (SSL/TLS). Port 587 merupakan yang digunakan untuk mengirimkan email (message submission port).Port 993 merupakan port default IMAP pada layanan webmail dengan menggunakan enkripsi keamanan SSL. Port 995 merupakan port default POP3 yang terenkripsi SSL/TLS. Port 3306 merupakan port protokol MySQL default, yang digunakan oleh klient MySQL, konektor MySql, dan utilitas seperti mysqldump dan mysqlpump.

Nmap website simaru.umb.ac.id

P-ISSN 1858-2680
e-ISSN 2723-4673

Gambar 9 Scanning Open Port menggunakan Nmap

Pada gambar diatas adalah sebuah scanning Open Port dengan menggunakan NMAP pada Operating Sistem Linux Ubuntu. Terdapat 5 open port yang ada pada system simaru.umb.ac.id yang terdiri dari port 53, 80, 443, 2000 dan 8011. Tugas dari port-port tersebut adalah :

Port 53 digunakan untuk komunikasi antara perangkat AppStream 2.0 pengguna dan server DNS. Port 80 adalah port WWW atau HTTP yang umum digunakan oleh suatu server website untuk dapat diakses oleh client. Port 443 adalah port penjelajahan web yang digunakan untuk mengamankan komunikasi browser web atau layanan HTTPS. Port 2000 adalah bandwidth test Port 8011 adalah port http

Scan vulnerability iframe pada website

Gambar 10. Perintah Iframe

Gambar diatas merupakan perintan untuk scan vulnerability iframe pada website simaru.umb.ac.id dan bklvision.com

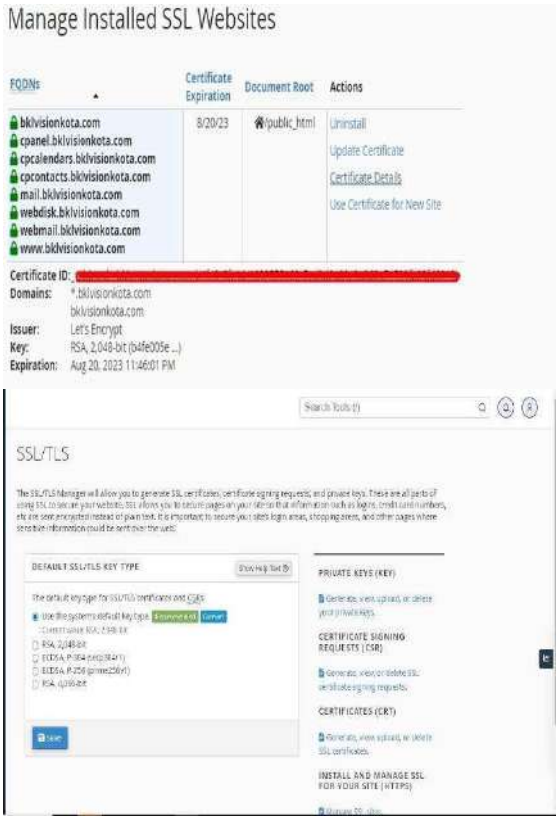
Hasil scan dengan Iframe

Gambar 11. Hasil scan perintah Iframe

Gambar diatas merupakan hasil scan vulnerability iframe di situs simaru.umb.ac.id dan hasilnya belum ada iframe di situs tersebut. Iframe adalah komponen HTML yang membantu dan menyematkan banyak file di situs web tanpa harus menyimpan dan mempostingnya terlebih dahulu. Selain untuk menghemat penyimpanan data (storage) dan mencegah pelanggaran hak cipta, iframe juga menjadi salah satu elemen yang cukup besar pengaruhnya terhadap website engagement.

Informasi SSL bklvision.com

P-ISSN 1858-2680
e-ISSN 2723-4673



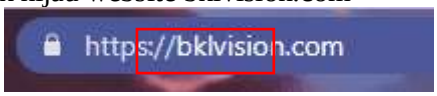
Gambar 12 Informasi SSL bklvision.com

Kegunaan sertifikat SSL utamanya adalah untuk menjaga keamanan dan kerahasiaan data ketika melakukan transaksi. SSL memberikan jaminan keamanan pada pemilik dan pengunjung situs atas data yang dikrimkan lewat web. SSL memungkinkan pengirim data yang aman dengan mengenkripsi informasi yang dikirimkan melalui jaringan internet.SSL yang sering digunakan dapat dilihat pada situs perbankan untuk melakukan transaksi e-banking.

a. Enkripsi Data: Sertifikat SSL menggunakan teknologi enkripsi untuk melindungi data yang dikirimkan antara pengguna dan server web. Enkripsi mengubah data menjadi format yang tidak dapat dibaca (terenkripsi) selama transmisi, sehingga informasi tidak dapat diakses oleh pihak yang tidak berwenang. Enkripsi ini membantu mencegah pencurian data dan penyadapan oleh pihak ketiga.
b. Keotentikan: Sertifikat SSL juga berperan dalam memastikan keotentikan situs web yang dikunjungi oleh pengguna. Sertifikat SSL yang valid membuktikan bahwa situs web tersebut telah diverifikasi oleh pihak otoritas sertifikat yang terpercaya. Hal ini memberikan keyakinan kepada pengguna bahwa mereka berkomunikasi dengan situs web yang asli dan bukan dengan situs palsu atau jahat yang berusaha melakukan serangan phishing atau mencuri data pribadi.
c. Otoritas Sertifikat: Sertifikat SSL dikeluarkan oleh Otoritas Sertifikat (Certificate Authority/CA), entitas tepercaya yang bertanggung jawab untuk memverifikasi keotentikan situs web dan menerbitkan sertifikat SSL. Otoritas Sertifikat melakukan verifikasi terhadap identitas dan keaslian situs web sebelum menerbitkan sertifikat SSL. Beberapa contoh Otoritas Sertifikat terkenal adalah DigiCert, Comodo, Symantec, dan Let's Encrypt.
d. Proses Handshake SSL: Ketika pengguna mengunjungi situs web yang dilindungi dengan SSL, proses yang disebut "handshake SSL" terjadi antara browser pengguna dan server web. Selama proses ini, informasi keamanan dan kunci enkripsi pertukaran antara kedua pihak untuk memulai sesi aman. Proses handshake ini memastikan bahwa komunikasi antara pengguna dan server terlindungi dan aman.
e. Indikator Keamanan: Sertifikat SSL memungkinkan pengguna untuk mengidentifikasi situs web yang menggunakan koneksi aman. Biasanya, situs web yang dilindungi dengan SSL ditandai dengan simbol gembok hijau atau ikon kunci pada browser, serta URL yang dimulai dengan "https://" (Hypertext Transfer Protocol Secure).

Sertifikat SSL adalah komponen penting dalam menjaga keamanan dan privasi dalam komunikasi online. Dengan menggunakan sertifikat SSL, situs web dapat menjaga integritas data, melindungi informasi sensitif pengguna, dan membangun kepercayaan dengan pengunjung situs.

Icon gembok hijau website bklvision.com



Gambar 13. Icon gembok bklvision.com

Gembok SSL, juga dikenal sebagai ikon gembok hijau, adalah simbol keamanan yang ditampilkan pada browser saat mengunjungi situs web yang menggunakan koneksi aman melalui protokol SSL/TLS. Simbol gembok SSL ini menunjukkan bahwa komunikasi antara browser pengguna dan server web terlindungi dengan enkripsi yang kuat. Gembok SSL menggambarkan bahwa website telah mengimplementasikan sertifikat SSL/TLS dan menggunakan protokol keamanan yang memastikan bahwa data yang dikirim antara pengguna dan server terenkripsi dan tidak dapat diakses oleh pihak ketiga yang tidak berwenang.

Ketika pengguna mengunjungi sebuah situs web yang menggunakan SSL, mereka akan melihat ikon gembok hijau di bilah alamat browser atau di bagian bawah halaman. Klik pada ikon gembok akan menampilkan informasi tentang sertifikat SSL, termasuk detail tentang otoritas sertifikat yang menerbitkan sertifikat tersebut dan informasi mengenai validitas sertifikat.

P-ISSN 1858-2680
e-ISSN 2723-4673

Gembok SSL memberikan keyakinan kepada pengguna bahwa interaksi mereka dengan situs web tersebut dilindungi dan data yang mereka kirimkan aman dari serangan peretas atau penyadapan oleh pihak yang tidak berwenang.

Penting untuk diingat bahwa gembok SSL menunjukkan bahwa koneksi antara pengguna dan server web dilindungi dengan enkripsi, tetapi itu tidak menjamin bahwa situs web itu sendiri bebas dari kerentanan atau serangan lainnya. Oleh karena itu, selain menggunakan situs web dengan gembok SSL, pengguna juga harus memperhatikan praktik keamanan umum, seperti menggunakan kata sandi yang kuat, menghindari mengklik tautan yang mencurigakan, dan memperbarui perangkat lunak secara teratur untuk menjaga keamanan online mereka.

Not Secure website simaru.umb.ac.id

Gambar 14. Not Secure simaru.ac.id

Ketika sebuah website ditandai dengan ‘Not Secure’ berarti bahwa koneksi antara browser pengguna dan website tersebut tidak dienkripsi. Peringatan ini biasanya ditampilkan di bilah alamat broser, seringkali disertai denga ikon gembok terbuka atau tanda seru di dalam segitigaa.

Peringatan 'Not Secure' dimaksudkan untuk memberi tahu pengguna bahwa informasi yang mereka kirimkan pada website tersebut, seperti kata sandi, rincian kartu kredit, atau informasi pribadi, dapat terlihat oleh penyerang atau pihak yang menyadap. Hal ini menunjukkan bahwa website tersebut tidak menggunakan HTTPS (Hypertext Transfer Protocol Secure), yang merupakan versi yang aman dari HTTP, protokol yang digunakan untuk mengirimkan data melalui internet.

HTTPS menggunakan protokol SSL/TLS (Secure Sockets Layer/Transport Layer Security) untuk mengenkripsi data yang ditransmisikan antara browser pengguna dan server website. Enkripsi ini memastikan bahwa informasi yang ditukar aman dan terlindungi dari akses yang tidak sah.

Website yang ditandai sebagai 'Not Secure' umumnya menggunakan HTTP biasa, yang berarti data ditransmisikan dalam teks biasa tanpa enkripsi, sehingga rentan terhadap intersepsi dan manipulasi oleh penyerang. Peringatan ini penting terutama pada website yang mengelola data sensitif atau melibatkan transaksi, karena menyoroti risiko potensial terhadap privasi dan keamanan pengguna.

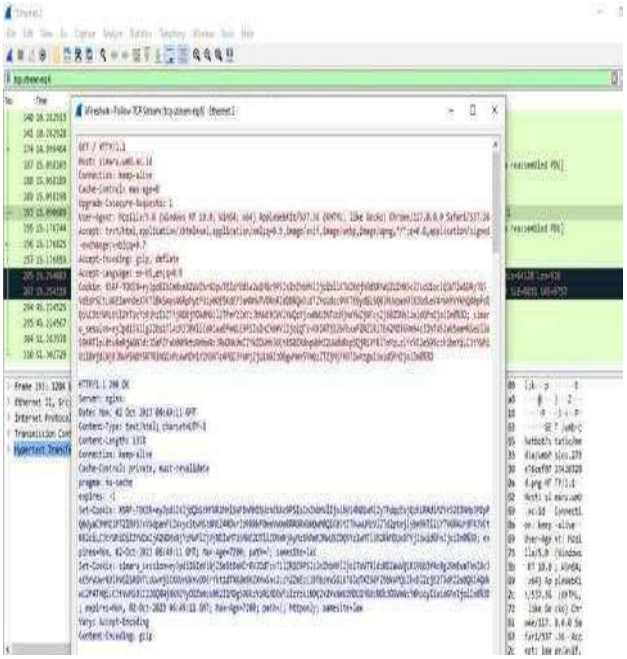
Untuk memastikan pengalaman browsing yang aman, disarankan untuk berhati-hati saat memasukkan informasi pribadi atau sensitif pada website yang ditandai sebagai 'Not Secure'. Pengguna harus mempertimbangkan untuk menghindari website tersebut atau menahan diri untuk tidak membagikan data sensitif kecuali mereka dapat memverifikasi keaslian dan langkah-langkah keamanan yang diterapkan oleh website tersebut.

Penting untuk dicatat bahwa meskipun peringatan 'Not Secure' menunjukkan kurangnya enkripsi, itu tidak selalu berarti bahwa website tersebut berbahaya atau terinfeksi. Namun, pengguna harus berhati-hati dan berpikir dua kali sebelum membagikan informasi sensitif pada website tersebut untuk melindungi privasi dan keamanan mereka.

Scan Vulnerability dengan Wireshark

a) Website simaru.umb.ac.id

Pada scan website simaru.umb.ac.id menggunakan software wireshark yang tersedia di aplikasi Virtualbox Kali Linuk.

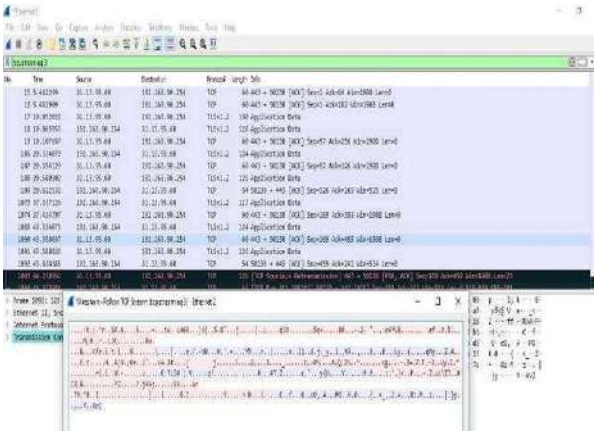


Gambar 15. bagian a) Hasil scanwebsite simaru.umb.ac.id menggunakan software Wireshark

Setelah melakukan uji penetrasi menggunakan software Wireshark didapatkan hasil yang menunjukkan bahwa website simaru.umb.ac id telah menggunakan enkripsi, sehingga tidak terdeteksi username dan passwordnya. Meskipun masih Not Secure, namun telah menggunakan enkripsi sha yang membantu mengamankan websbite.

Website bklvision.com

P-ISSN 1858-2680
e-ISSN 2723-4673



Gambar 17. bagian b) Hasil scan website bklvisionkota.com menggunakan software Wireshark

Website bklvisionkota.com telah menggunakan SSL (Secure Socket Layer) yang mengamankan data didalamnya dari serangan *Sniffing*, sehingga ketika melakukan scan vulnerability menggunakan Wireshark akan menampilkan hasil berupa symbol.

Pembahasan

Dalam pembahasan ini, dibahas beberapa vulnerability yang terbuka di dalam website bklvison.con dan simaru.umb.ac.id yang telah diuji. Dibawah ini beberapa kerentanan yang ada sebagai berikut :Vulnerability Clickjacking Frame

Clickjacking adalah aktivitas jahat yang dilakukan oleh peretas atau grup peretas dengan menipu pengguna agar mengklik tombol atau tautan. Ini menjadi berbahaya karena peretas menyematkan skrip atau kode yang melaluinya skrip tersebut dapat mencuri data atau mengontrol computer pengguna yang mengklik tautan atau tombol dan mengalihkannya ke serve lain. Di dua situs yang diperiksa oleh Nmap dan Nikto. Memberikan informasi bahwa situs-situs tersebut belum memiliki alat anti-clikcjacking, sehingga memudahkan peretas untuk mengelabuhi calon korban agar mengklik tautan yang diberikan kepada pengguna.Vulnerability X-Content-Type-Options. X-Content-Type-Options adalah respon header respons HTTP header yang digunakan oleh server untuk menunjukkan bahwa tipe MIME yang dikirim harus diikuti dan tidak diubah. Hal memungkinkan untuk menghindari sniffing tipe MIME (Multipurpose Internet Mail Extensions or Mime). Kedua situs diatas belum memasang pengaturan konten untuk pengamanan website, guna mencegah adanya pencurian atau pembobolan data. Hasil scan juga menunjukkan informasi bahwan content encoding header is set to ‘deflate’ which may mean that the server is vulnerable to the brech attact yang berarti header pengkodean konten diatur ke ‘deflate’ yang mungkin berarti server rentang terhadap serangan pembobolan data. Pengujian virtual box berfokus pada software Nikto dan Nmap, untuk mendapatkan serangkaian informasi yang sesuai dengan tujuan pada penelitian. Berikut ini beberapa informasi yang didapatkan setelah pengujian website dengan menggunakan software Nikto dan Nmap pada website bklvison.com dan simaru.umb.ac.id :

Table 1. Hasil Scan

No	Hasil scan	bklvision.com		simaru.umb.ac.id	
		Ada	Tidak	Ada	Tidak
1	Anti Clickjacking		✓		✓
2	X-Content type-Options		✓		✓
3	Content-Encodinig		✓		✓

Dari hasil Scanning aplikasi virtualbox menggunakan software Nikto dan Nmap mengdapatkan hasil seperti pada table diatas. Ada beberapa celah keamanan dan port yang terbuka, dan rentan terhadap pembobolan data secara illegal.

V. PENUTUP

A. Kesimpulan

Setelah menyelesaikan pengujian pada kedua website tersebut, maka penulis dapat menarik kesimpulan sebagai berikut :

1. Scanning website menggunakan software Nikto dan Nmap mampu memberikan berbagai informasi yang memungkinkan kebocoran celah keamanan.
2. Dengan Scanning ini, telah dicoba juga menggunakan perintah Iframe dan terbukti masih rentan terhadap kebobolan data.
3. Diperlukan penerapan lebih dalam pada saat penerapan SSL untuk sebuah website, guna mencegah pencurian data oleh pihak yang tidak bertanggung jawab.

B. Saran

Pengujian terhadap website bklvision.com dan simaru.umb.ac.id yang telah di uji coba melalui aplikasi virtualbox, menggunakan software Nikto dan Nmap mampu memberikan beberapa informasi mengenai port atau celah kerentanan yang ada di website simaru.umb.ac.id dan bklvision.com. Sehingga aplikasi yang diuji kalilinux terdeteksi kelemahannya dan data bisa diselamatkan. oleh karena itu, perlu diperhatikan kembali ketika tedeteksi kelemahan nya ketika mengamankan

P-ISSN 1858-2680
e-ISSN 2723-4673

website. Ada baiknya, pemilik dan administrator website dianjurkan untuk menerapkan sertifikat SSL/TLS dan mengaktifkan HTTPS untuk memberikan pengalaman browsing yang aman bagi pengguna mereka. Dengan melakukannya, mereka dapat melindungi data pengunjung mereka dan membangun kepercayaan dalam lingkungan online. Juga menerapkan keamanan lainnya yang telah disediakan oleh SSL untuk administrator/pemilik website. Penulis berharap jika nantinya ada yang ingin membahas hal yang sama, maka bisa melengkapi dengan berbagai fitur scanning lainnya.

DAFTAR PUSTAKA

[1] A. T. P. Tambunan, A. P. Lubis, and S. Anggraini, "Perancangan Sistem Keamanan File Transfer Protocol Dengan Secure Socket Layer Pada Server Centos 7," *J-Com (Journal Comput.*, vol. 1, no. 2, pp. 95–102, 2021, doi: 10.33330/j-com.v2i1.1206.

[2] R. N. Dasmen, T. L. Widodo, and M. Tio, "PENGUJIAN PENETRASI PADA WEBSITE ELEARNING2 . BINADARMA . AC . ID DENGAN METODE PTES (PENETRATION TESTING EXECUTION STANDARD)," vol. 11, no. 1, pp. 91–95, 2023, doi: 10.35508/jicon.v11i1.9809.

[3] M. Rafi Ramdani, N. Heryana, and A. Susilo Yuda Irawan, "Penetration Testing pada Website Universitas Singaperbangsa Karawang Menggunakan Open Web Application Security Project (OWASP)," *J. Pendidik. dan Konseling*, vol. 4, no. 4, pp. 5522–5529, 2022.

[4] J. T. Elektro, F. Teknik, and U. Andalas, "SECURE SOCKET LAYER UNTUK KEAMANAN DATA REKAM MEDIS TUMOR OTAK PADA HEALTH INFORMATION SYSTEM," no. 3, 2017.

[5] I. cahyo Utomo and S. Rokhmah, "Konfigurasi SSL Untuk Meningkatkan Keamanan Web server Pada Program Studi Teknik Informatika Universitas Muhammadiyah Surakarta," *Jurti*, vol. 6, no. 2, pp. 143–150, 2022, [Online]. Available: https://ocs.unmul.ac.id/index.php/INF/article/view/8333/pdf

[6] W. Agustiara *et al.*, "Analisis Keamanan Protokol Secure Socket Layer Terhadap Serangan Packet Sniffing Pada Website Portal Berita Harian Umum Koran Padang," *J. Tek. Inform. Kaputama*, vol. 6, no. 1, 2022.

[7] H. Pranata, L. A. Abdillah, and U. Ependi, "Analisis Keamanan Protokol Secure Socket Layer (SSL) Terhadap Proses Sniffing di Jaringan," pp. 21–22, 2015, [Online]. Available: http://arxiv.org/abs/1508.05457

[8] Y. Thurfah, A. Rosaliah, and B. Hananto, "Pengujian Celah Keamanan Website Menggunakan Teknik Penetration Testing dan Metode OWASP TOP 10 pada Website SIM xxx," no. September, pp. 752–761, 2021.

[9] D. Utomo, M. Sholeh, and A. Avorizano, "Membangun Sistem Mobile Monitoring Keamanan Web Aplikasi Menggunakan Suricata dan Bot Telegram Channel," *Semin. Nas. Teknoka*, vol. 2, no. 2502, pp. 1–7, 2017.

[10] R. Hermawan, P. Studi, and T. Informatika, "TEKNIK UJI PENETRASI WEB SERVER MENGGUNAKAN SQL," vol. 6, no. 2, 2021.

P-ISSN 1858-2680
e-ISSN 2723-4673