(2024), 2 (7): 73–77 Scientica 3021-8209
Jurnal Ilmiah Sains dan Teknologi

Analisis dan Evaluasi Terkait Keamanan pada Web Server

Syaafi'atul Faatihah[1], Atika Dewi Zulaikha[2], Galih Satrio Wicaksono[3]

[1,2,3]Informatika, Universitas Teknologi Yogyakarta
Jl. Siliwangi, Jombor Lor, Sendangadi, Kec. Mlati, Kabupaten Sleman, Daerah Istimewa Yogyakarta 55285
fiablnk07@gmail.com, zulaikhaatikadewi@gmail.com, galihsww@gmail.com

Abstract (English)
With the rapid growth in the use of web-based applications, network security has become increasingly important in maintaining the integrity and confidentiality of organizational information. Threats to data and information security are increasing along with the increase in hacker attacks on information systems. Attacks on web servers are one of the most common attacks, showing the urgency to strengthen computer network security. This article discusses the importance of network security in the context of protecting information systems from cyber attacks, with an emphasis on the need for attack detection systems in networks to identify and respond to attacks quickly. Thus, this article underscores the importance of network security in maintaining the integrity, confidentiality, and availability of information in an internet organization.

Article History
Submitted: 25 May 2024
Accepted: 4 June 2024
Published: 5 June 2024

Key Words
web server, network security, information, internet

Abstrak (Indonesia)
Dengan pertumbuhan penggunaan aplikasi berbasis web yang pesat, keamanan jaringan menjadi semakin penting dalam menjaga integritas dan kerahasiaan informasi organisasi. Ancaman terhadap keamanan data dan informasi semakin meningkat seiring dengan meningkatnya serangan hacker terhadap sistem informasi. Serangan pada web server menjadi salah satu serangan yang umum terjadi, memperlihatkan urgensi untuk memperkuat keamanan jaringan komputer. Artikel ini membahas pentingnya keamanan jaringan dalam konteks melindungi sistem informasi dari serangan cyber, dengan penekanan pada perlunya sistem pendeteksi serangan dalam jaringan untuk mengidentifikasi dan merespons serangan dengan cepat. Dengan demikian, artikel ini menggarisbawahi pentingnya keamanan jaringan dalam menjaga integritas, kerahasiaan, dan ketersediaan informasi dalam sebuah organisasi internet.

Sejarah Artikel
Submitted: 25 May 2024
Accepted: 4 June 2024
Published: 5 June 2024

Kata Kunci
web server, keamanan jaringan, informasi, internet.

1. PENDAHULUAN

Perkembangan jaringan internet dan semakin banyaknya pengguna aplikasi berbasis web telah meningkatkan ancaman terhadap keamanan data dan informasi. Salah satu aspek penting dalam sistem informasi organisasi dan perusahaan adalah keamanan jaringan. Lemahnya keamanan jaringan dapat meningkatkan serangan hacker pada sistem.

Serangan hacker pada sistem dapat menyebabkan kerusakan dan perubahan fungsi sistem. Dengan banyaknya pengguna memanfaatkan aplikasi web, termasuk untuk layanan penting, aplikasi web menjadi target serangan yang populer. Salah satu serangan yang sering terjadi adalah serangan pada web server, karena web server terhubung dengan internet yang dapat diakses luas.

Keamanan jaringan tidak hanya bergantung pada infrastruktur teknis, tetapi juga pada kecepatan dan kecerdasan dalam menanggapi gangguan. Untuk memperkuat keamanan, organisasi dapat menerapkan sistem pendeteksi serangan (Intrusion Detection System) yang dapat mengidentifikasi dan merespons serangan dengan cepat.

Dengan demikian, keamanan jaringan menjadi aspek yang sangat penting dalam menjaga integritas, kerahasiaan, dan ketersediaan informasi dalam organisasi. Penerapan strategi keamanan yang komprehensif sangat diperlukan untuk menghadapi ancaman siber yang semakin berkembang.

2. LANDASAN TEORI

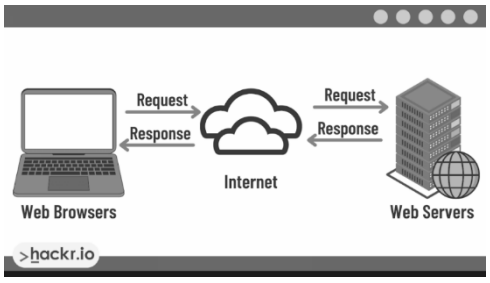
WEB SERVER

Secara umum, web server dapat diartikan sebagai perangkat yang memberikan pengguna ke situs web. Web server memiliki komponen Utama yang terdiri dari perangkat keras dan perangkat lunak yang bekerja bersama-sama untuk mengelola dan menyediakan berbagai konten web.

Dari sisi perangkat keras, web server merupakan sebuah penyimpanan yang digunakan untuk menyimpan berbagai file dan komponen situs web. Biasanya, komputer server ini terhubung ke internet dan dapat bertukar data dengan perangkat lain yang juga terhubung ke jaringan web.

Sementara itu, dari aspek perangkat lunak web server meliputi sejumlah komponen yang bertanggung jawab atas pengaturan cara pengguna yang dapat mengakses file-file yang telah disediakan. Salah satu komponen utamanya adalah server HTTP yang memahami URL (alamat web) dan protokol HTTP yang digunakan oleh browser untuk menampilkan halaman web. Server HTTP dapat diakses melalui nama domain situs web yang disimpan, dan akan menyajikan konten situs web tersebut kepada perangkat pengguna.

Web server beroperasi dengan menyimpan file-file situs web dalam sistemnya. Ketika seorang pengguna meminta halaman web tertentu, server akan mencari file yang dimaksud di dalam sistem filenya. Jika file ditemukan, server akan menyediakan konten tersebut kepada pengguna. Namun, jika file tidak ditemukan, server akan mengembalikan respons kesalahan 404. Begitu pula jika file ditemukan tetapi tidak dapat ditampilkan dengan benar, server akan mengembalikan jenis kesalahan yang lain.



Gambar 1.1 Cara Kerja Web Server

Selain menyediakan dukungan protokol HTTP dalam memproses permintaan dan respons, hampir semua web server juga menawarkan fitur-fitur standar yang serupa, antara lain:

1. Pencatatan log file (file logging)
   Web server akan mencatat berbagai peristiwa atau aktivitas yang terjadi di dalamnya, seperti permintaan yang masuk, catatan keamanan, dan log kesalahan. Setiap kali web server menerima permintaan baru, maka akan ditambahkan baris teks ke dalam log tersebut.
   Autentikasi
   Banyak web server yang menyediakan fitur autentikasi, baik untuk mengizinkan akses penuh maupun akses terbatas ke sumber daya situs web. Fitur autentikasi biasanya mencakup permintaan otorisasi, yang memerlukan nama pengguna dan kata sandi.
2. Pembatasan Bandwidth
   Web server memiliki bandwidth tertentu, yaitu jumlah data yang dapat ditransfer atau diproses dalam waktu tertentu. Fitur pembatasan bandwidth digunakan untuk mengontrol kecepatan respons, guna memastikan jaringan tidak terlalu padat sehingga file dapat dikirimkan dengan lancar.
3. Ruang penyimpanan
   Aspek ini mengacu pada jumlah ruang disk yang tersedia untuk menyimpan file-file, yang akan menentukan apakah web server dapat menghosting situs web dengan baik.

Selain itu, web server juga memiliki beberapa fungsi penting lainnya, seperti:

1. Membersihkan cache dan dokumen yang tidak terpakai lagi dari penyimpanan.
2. Melakukan pemeriksaan terkait keamanan HTTP yang diminta dari permintaan klien atau web browser.
3. Menyediakan data sesuai permintaan yang masuk, sehingga dapat menjamin sistem berjalan dengan aman dan lancar.

KEAMANAN WEB SERVER

Keamanan web server merupakan aspek penting dalam menjaga keamanan server yang digunakan di seluruh domain web atau Internet. Keamanan ini biasanya diimplementasikan melalui beberapa metode dan lapisan, seperti:

1. Keamanan sistem operasi (OS)
   Memastikan hanya pengguna atau entitas yang berwenang yang dapat mengakses dan mengoperasikan komponen serta layanan penting dari server web.
2. Keamanan aplikasi
   Memastikan kontrol yang ketat atas konten dan layanan yang dihosting di server web.
3. Keamanan jaringan
   Memberikan perlindungan terhadap berbagai eksploitasi, virus, dan serangan keamanan berbasis Internet.

Server merupakan bagian integral dari back-end aplikasi yang mengelola data, merespons permintaan pengguna, dan menentukan perilaku aplikasi. Baik organisasi yang menyebarkan aplikasi mereka menggunakan server fisik atau virtual, mengamankan server menjadi prioritas utama selama pengembangan aplikasi web.

Web server dapat rentan terhadap berbagai ancaman, seperti serangan peretasan, ancaman dari dalam, kesalahan konfigurasi keamanan, dan risiko lainnya. Saat ini, banyak bisnis yang memanfaatkan website untuk mengembangkan produk mereka, serta bidang pendidikan yang membutuhkan web server untuk mendukung pembelajaran dan menyimpan data yang sangat rahasia. Jika web server tidak dilindungi dengan baik, dapat menimbulkan risiko-risiko, seperti:

1. Kehilangan data sensitif: Web server menyimpan banyak data pengguna yang sensitif dalam database, yang dapat bocor atau dicuri karena insiden keamanan.
2. Respons aplikasi yang lambat: Serangan seperti distributed denial of service (DDoS) dapat menyebabkan sumber daya web server cepat berkurang, memperlambat pemuatan halaman, dan mengganggu respons terhadap permintaan pengguna.

Oleh karena itu, keamanan web server menjadi sangat penting untuk menjaga kelangsungan dan kepercayaan pengguna terhadap aplikasi atau layanan yang dihosting di server web.

3. ANALISIS PENYELESAIAN MASALAH KEAMANAN WEB SERVER

Keamanan sistem sangat penting dalam sistem informasi. Jika keamanannya lemah, bisa meningkatkan risiko serangan yang dapat merusak sistem. Salah satu serangan sering terjadi di web server. Ini karena web server terhubung ke internet dan diakses banyak pengguna, jadi risikonya tinggi.

Untuk mengamankan web server, kita dapat melakukkan pencegahan sebagai berikut :

1. Secure Socket Layer (SSL)
   SSL adalah cara untuk mengenkripsi data yang dikirim melalui internet, agar aman dari penyadapan atau perubahan.
   Dengan mengatur SSL di web server, bisa berpengaruh dengan meningkatnya keamanan dan dapat mencegah potensi serangan.
   Caranya dengan memasang sistem operasi, perangkat lunak web server, dan konfigurasi sertifikat SSL.Selanjutnya, Hasil tes menunjukkan web server lebih aman setelah diatur SSL.

2. Wireless Application Framework (WAF)
   WAF khususnya ModSecurity, bisa melindungi pengguna aplikasi web dari serangan. WAF fokus melindungi dari kelemahan aplikasi web, seperti XSS dan SQL Injection.
   Kelemahan aplikasi web sering dimanfaatkan untuk serang situs resmi dan bajak kode.
   WAF memeriksa situs dan kode berbahaya, lalu melakukkan penolakan kode-kode itu. WAF bekerja berdasarkan aturan, jadi hanya bisa melakukkan pencegahan serangan berbahaya sesuai aturan.

   Dengan menerapkan ini, diharapkan bisa meningkatkan keamanan web server dan melindungi sistem informasi dari serangan, sehingga aman untuk data dan transaksi online.

DAFTAR PUSTAKA

[1]. Developer.mozilla.org (Jul 3, 2023). What is a web server? - Learn web development. Diakses 30 Mei 2024, dari https://developer.mozilla.org/en-US/docs/Learn/Common_questions/Web_mechanics/What_is_a_web_server

[2]. Apriorit.com (Feb 22, 2024). 11 Best Practices for Web Server Security. Diakses 5 Mei 2024, dari https://www.apriorit.com/dev-blog/web-server-security

[3]. Hostinger.co.id (Apr 14, 2023). Apa Itu Web Server? Pengertian, Fungsi, dan Cara Kerjanya. Diakses 5 Mei 2024, dari https://www.hostinger.co.id/tutorial/apa-itu-web-server#Bagaimana_Cara_Kerja_Web_Server

[4]. Hackr.io (Jan 26, 2024). What is a Web Server and How Do They Work? Ultimate Guide [2024]. Diakses 6 Mei 2024, dari https://hackr.io/blog/what-is-a-web-server

[5]. Dicoding.com (Jan 27, 2021). Apa itu Web Server dan Fungsinya?. Diakses 7 Mei 2024, dari https://www.dicoding.com/blog/apa-itu-web-server-dan-fungsinya/

[6]. Cahyo Utomo, Ihsan. & Rokhmah, Siti. (2022). Jurti. *Konfigurasi SSL Untuk Meningkatkan Keamanan Web server*, 6, 143 - 149.

[7]. Made Suartana, I., Endah Wahanani, Henni., Noor Sandy, Aditya. (2015). Scan. *Sistem Pengamanan Web Server dengan Web Application Firewall*, Vol X No 1, 39 - 44.

[8]. Subandi, Kotim., Ilyas Sugara, Victor. (2021). Jurnal UMJ. *Analisa Serangan Vulnerabilities Terhadap Server Selama Periode WFH di Masa Pandemi Covid-19 Sebagai Prosedur Mitigasi.* 1-9.