(2024), 2 (8): 1–5 Scientica 3021-8209
Jurnal Ilmiah Sains dan Teknologi

ANALISIS METODE-METODE PENINGKATAN KEAMANAN WEB SERVER

Azra Hita Dahayu Putri[1], Aisyatul Muhdiyyah[2], Raya Rambu Anarki[3]
[1,2,3]Informatika, Universitas Teknologi Yogyakarta
Jakarta Selatan, DKI Jakarta, Indonesia 12640
azra.5220411226@uty.student.ac.id, aisyatulnew85@gmail.com, ryaanarki@gmail.com

Abstract (English)
Web server security is one of the most important aspects of web application development. Over time, Web Server technology has increased, as has security attacks that threaten systems. Organizations and web developers need to implement methods that can improve the reliability of their web server systems. The purpose of creating this journal is to analyze several methods that can be used to improve web server security by paying attention to effectiveness and suitability in different contexts.

Article History
Submitted: 11 June 2024
Accepted: 20 June 2024
Published: 21 June 2024

Key Words
Web Server, Safety, Method

Abstrak (Indonesia)
Keamanan Web Server adalah salah satu aspek penting dalam dunia pengembangan aplikasi web. Seiring berjalannya waktu, teknologi Web Server semakin meningkat, begitu pula dengan serangan keamanan yang mengancam sistem. Penting bagi organisasi dan pengembang web untuk mengimplementasikan metode-metode yang dapat meningkatkan keamanan sistem web server mereka. Tujuan dari dibuatnya jurnal ini adalah untuk menganalisis beberapa metode yang dapat digunakan untuk meningkatkan keamanan web server dengan memperhatikan keefektifan dan kecocokan dalam konteks yang berbeda.

Sejarah Artikel
Submitted: 11 June 2024
Accepted: 20 June 2024
Published: 21 June 2024

Kata Kunci
Web Server, Keamanan, Metode

1. PENDAHULUAN

Web server merupakan *software* (perangkat lunak) yang memberikan layanan berupa data. Web Server memiliki fungsi untuk menerima permintaan HTTP atau HTTPS dari klien atau yang kita kenal dengan web browser (Chrome, Firefox). Setelah itu, ia akan mengirimkan respon atas permintaan tersebut kepada *client* dalam bentuk halaman web. Web server menjadi salah satu kebutuhan *user* sebab web server memiliki kapasitas penyimpanan yang besar dan akses yang cepat. Sehingga dapat mencegah terjadinya kesalahan pada suatu website maupun aplikasi [1].

Contoh kasus :

a. Pada penelitian [1] diangkat masalah pada keamanan dari sistem dalam melindungi data pengguna, meminimalkan kesalahan eksekusi dari sistem serta mengurangi risiko *error*, sehingga sistem *login* bisa digunakan secara aman. Peneliti akan menggunakan *Burp Suite* untuk menguji keamanan sistem yang

dibangun, dan akan menggunakan Teknologi *Blockchain* untuk meningkatkan keamanan pada sistem *login*.

b. Pada penelitian [2] mengimplementasikan sistem keamanan web server menggunakan Pfsense. Dengan meluncurkan serangan DDoS pada sistem (layar aplikasi) lalu melakukan pendekatan dengan PPDIOO *Network Life Cycle* yang membantu mempermudah tahap penelitian, dan akhirnya melakukan pengujian keamanan pada sistem.

c. Pada penelitian [3] diangkat masalah pengembangan keamanan jaringan komputer, pengujian dilakukan dengan metode *port scanning* menggunakan aplikasi NMAP dan *bruteforce* menggunakan Brutus. Penguji akan menggunakan Suricata sebagai solusi dari metode.

2. TINJAUAN PUSTAKA

Pada artikel ini akan dibahas lebih dalam tentang penelitian terdahulu yang mengangkat masalah keamanan pada web server dengan berbagai sebab.

Penelitian [1] menjelaskan bahwa *Blockchain* adalah teknologi yang dapat menyimpan riwayat pengguna yang hanya dapat diakses oleh yang berwenang. Teknologi *blockchain* akan membuat peretas sulit mengubah identifikasi data pengguna. Sistem login biasanya memerlukan *username* dan *password* sebagai metode autentikasi, Autentikasi adalah dimana identitas pemilik sistem diperlukan untuk mengakses sistem, dapat berupa *username* dan *password*, sidik jari, bentuk wajah, bentuk tangan, dll. Permasalahan timbul jika saat sistem autentikasi diretas, pengguna akan sulit mengetahuinya. *Burp Suite* berperan sebagai *software* yang akan melakukan percobaan serangan *broken autentication* atau menyebabkan kesalahan konfigurasi manajemen *session*/kerentanan web. Autentikasi yang akan dilakukan yaitu memasukan *username* dan *password* yang sudah terdaftar. Aplikasi *Burp Suite* akan menampilkan *username* dan *password* ketika masuk kedalam sistem, *tool Burp Suite* akan mencari kombinasi *username* dan *password* yang benar untuk masuk ke dalam sistem. Setelah berhasil *login*, pengujian *broken autentication* dilakukan, dengan menggunakan *blockchain* data yang didapatkan berupa blok yang sudah terenkripsi, *username* dan *password* yang dimasukan sebelumnya berhasil diubah. Serangan *Burp Suite* tidak dapat mendeteksi data pengguna setelah penerapan *blockchain*.

Penelitian [2] menjelaskan pengujian sistem keamanan sistem dengan menggunakan serangan DDos dan menggunakan Pfsense sebagai penghubung koneksi dan pengamanan serta perlindungan terhadap web server. Pfsense adalah distribusi *firewall network* yang bebas, berdasarkan pada sistem operasi FreeBSD dengan kernel khusus dan termasuk paket perangkat lunak bebas pihak ketiga untuk fungsionalitas tambahan. Dengan bantuan sistem paket, PfSense mampu menyediakan fungsionalitas yang sama dengan *firewall* komersial. Serangan DDos adalah serangan yang diluncurkan pada lapisan aplikasi dan dapat menimbulkan konsekuensi seperti menghabiskan sumber daya (*bandwith* jaringan, pemrosesan CPU, dan memori). Penelitian menggunakan pendekatan PPDIOO *Network Life Cycle* sebagai metodologi pengembangan. Pendekatan ini berupa *Prepare, Plan, Design, Implement, Operate* dan *Optimaze*. Ketika pengujian serangan, komputer korban tidak akan mengetahui adanya serangan karna tidak dipasangkan Pfsense, komputer pengguna juga mengalami kehabisan sumber daya sehingga komputer terbebani dan tidak bisa di akses lagi. Pemasangan sistem Pfsense pada komputer akan membantu komputer untuk mendeteksi serangan *SlowLoris* yang menguji router Pfsense dan *snort* PC, Serangan ini mengidentifikasi log penyerang pada protokol HTTP dan mengidentifikasi *ip address* penyerang yang melakukan *snort*. Dengan menggunakan log ini, Pfsense akan memblokir router selama waktu yang ditetapkan dalam konfigurasi. Konfigurasi yang diperlukan pada menu *setting interface snort* pada Pfsense adalah *check list* pada *Block Offenders*. Ini harus diaktifkan pada setting umum pada bagian *Remove Blocked Hosts Interval* untuk menentukan waktu pemblokiran pada *ip address* yang melakukan penyerangan. *Snort* Pfsense memiliki banyak aturan yang harus diaktifkan. Untuk melakukan konfigurasi, pergi ke menu *interface snort*, pilih bagian tindakan, dan edit. Ini akan menunjukkan beberapa kategori yang ingin diaktifkan untuk mendeteksi serangan web server. Dengan Pfsense, *snort* mampu mengenali jenis serangan dan dapat melindungi web server dengan mengaktifkan *port* 80 dan 443.

Penelitian [3] dijelaskan bahwa Suricata merupakan *software* pendeteksi dan pencegah gangguan atau *Intuision Detection and Prevention System* (IDPS). Suricata akan melakukan deteksi ancaman dan melakukan pencegahan berupa *blocking* terhadap tindakan *scanning* dari penyerang. Peneliti menggunakan Suricata pada Linux Debian 6, dan serangan dengan metode *port scanning* menggunakan aplikasi NMAP dan *bruteforce*. Serangan dimulai dengan *intruder* yang melakukan penyusupan dengan NMAP, NMAP akan memantau *port- port* yang terbuka pada server, namun dengan menggunakan IDS Suricata, NMAP tidak mampu memantau lebih

lanjut karna Suricata telah melakukan pencegahan dengan cara melakukan *blocking* terhadap tindakan *scanning* dari penyerang. Begitu juga dengan serangan *bruteforce* yang mencoba menyerang *password* pengguna, dan mengambil alih sistem. Setelah Suricata di aktifkan, *bruteforce* tidak dapat lagi menyerang, hal ini di sebabkan karna Suricata telah memutuskan koneksi sehingga *bruteforce* tidak dapat menemukan target karna koneksi telah terputus.

3. HASIL DAN PEMBAHASAN

Untuk meningkatkan keamanan pada web server atau sistem dapat di gunakan Teknologi Blockchain, Pfsense, dan Suricata untuk kasus-kasus tertentu seperti pada penelitian [2], [3], dan [4]. Teknologi Blockchain dapat digunakan apabila komputer/ sistem terserang pada bagian autentikasi atau kasus pencurian data pribadi menyangkut sistem *login*. Pfsense akan siap melakukan pemblokiran apabila terdeteksi penyerangan, sehingga akan mempermudah penanggulangan, dan Suricata akan mendeteksi dan mencegah gangguan pada *port scanning* atau aktivitas untuk mendapatkan informasi yang menyeluruh mengenai status *port* dan melakukan tindakan preventif terhadap serangan *Nmap*.

Selain metode diatas juga terdapat banyak metode lainnya seperti Ransomware, Vulnerability Assessment, Penetration Testing, dll. Juga kita dapat meningkatkan kerumitan *password*, berhati-hati saat *login/sign-in* memastikan tidak pada komputer orang lain, tidak memberitahukan data *login* pada orang lain, dan masih banyak cara peningkatan keamanan yang berasal dari kita.

4. KESIMPULAN

Secara operasionalnya, web server terdiri atas perangkat keras dan perangkat lunak. Perangkat keras adalah alat dasar untuk pelaksanaan dan perangkat lunak bertugas membantu pada operasionalnya. Serangan terhadap perangkat lunak sistem dapat di cegah dengan menerapkan metode peningkatan keamanan, seperti Teknologi Blockchain, Pfsense, Suricata, Ransomware, Vulnerability Assessment, Penetration Testing, dll. Selain peningkatan keamanan secara metode, peningkatan keamanan dari diri sendiri dapat dimulai dari meningkatkan kerumitan *password*, berhati-hati saat *login/sign-in* memastikan tidak pada komputer orang lain, dan tidak memberitahukan data *login* pada orang lain.

Ucapan Terima Kasih

Penulis A.H.D.P, A.M, dan R.R.A mengucapkan terima kasih kepada Dosen mata kuliah Jaringan Komputer & Komunikasi atas tugas yang diberikan.

DAFTAR PUSTAKA

[1] I. Riadi, A. Zakilah Ifani, S. Informasi, F. Sains dan Teknologi Terapan, dan U. Ahmad Dahlan, “Optimasi Keamanan Web Server terhadap Serangan Broken Authentication Menggunakan Teknologi Blockchain,” 2021.

[2] M. Arman dan N. Rachmat, “Jusikom : Jurnal Sistem Komputer Musirawas IMPLEMENTASI SISTEM KEAMANAN WEB SERVER MENGGUNAKAN PFSENSE.”

[3] S. Ramadhani, U. Sultan Syarif Kasim Alamat, J. Koto Kociak Kecamatan Latina Payakumbuh Sumatera Barat, J. H. Soebrantas Kelurahan Simpang Baru No, dan K. Tampan, “Analisis Sistem Keamanan Web Server Dan Database Server Menggunakan Suricata.”