Jurnal Esensi Infokom Vol 8 No. 1 Mei 2024
e-ISSN: 2828-6707
https://esensijournal.com/index.php/infokom
DOI: 10.55886/infokom.v8i1.816

Pencegahan Web Defacement

Ariawan Aryapranata[1], Sigit Hermanto[2], Yogi Priya Agsena[3], Yuliansyah Al Rasyid[4], Fachrul Husain Habibie[5]

Program Studi Bisnis Digital, Institut Pariwisata Trisakti

Jl. IKPN Bintaro No.1, Bintaro, Pesanggrahan, Jakarta, Indonesia

ariawan.aryapranata@iptrisakti.ac.id[1], sigit.hermanto@iptrisakti.ac.id[2], yogi.agsena@iptrisakti.ac.id,[3] yuliansyah@iptrisakti.ac.id[4], fachrul@iptrisakti.ac.id[5]

Intisari— **Meningkatnya penggunaan internet memiliki risiko semakin masifnya ancaman peretasan. Badan Siber dan Sandi Negara (BSSN) mencatat hingga April 2022, serangan siber di Indonesia mencapai angka 100 juta kasus. Web defacement selalu masuk ke dalam tiga teratas insiden yang masuk dalam layanan BSSN, Web Defacement adalah tindakan merusak dan mengubah tampilan website, dan dapat merusak reputasi bisnis serta mengancam kepercayaan pengunjung. Metode penelitian tindakan (action Research) digunakan untuk langkah-langkah penerapan pencegahan web defacement yang menjadi bagian integral dari strategi keamanan website.**

Kata kunci—Serangan Siber, Web Defacement, Keamanan Web, Keamanan Siber.

*Abstract— **The increasing use of the internet has the risk of increasingly massive hacking threats. The National Cyber and Chryptography Agency (BSSN) noted that until April 2022, cyberattacks in Indonesia reached 100 million cases. Web defacement is always included in the top three incidents included in BSSN services, Web Defacement is an act of damaging and changing the appearance of the website, and can damage business reputation and threaten visitor trust. Action research methods are used to implement preventive web defacement measures that are an integral part of a website's security strategy..***

Keywords— Cyber Attack, Web Defacement, Web Security, Cyber Security.

I. PENDAHULUAN

Meningkatnya penggunaan internet memiliki risiko semakin masifnya ancaman peretasan. Badan Siber dan Sandi Negara (BSSN) mencatat hingga April 2022, serangan siber di Indonesia mencapai angka 100 juta kasus. Jenis serangan siber yang banyak ditemukan BSSN didominasi oleh serangan ransomware dan malware.[1]

Total trafik anomali di Indonesia selama tahun 2022 adalah 976.429.996 anomali dengan jenis trafik anomali tertinggi yaitu MyloBot Botnet yang memungkinkan penyerang untuk mengambil kendali penuh atas sistem pengguna. Terdapat 4.421.992 aktivitas APT serta 2.348 kasus Web Defacement yang terjadi di Indonesia pada tahun 2022. Web defacement selalu masuk ke dalam tiga teratas insiden yang masuk dalam layanan BSSN, seperti pengiriman notifikasi insiden, Asistensi penanganan insiden siber, layanan cyber threat intelligence, dan layanan digital forensic.[1]

Data di e-MP Robinopsnal Bareskrim Polri menunjukkan kepolisian menindak 8.831 kasus kejahatan siber sejak 1 Januari hingga 22 Desember 2022. Seluruh satuan kerja di Bareskrim Polri dan polda di Indonesia melakukan penindakan terhadap kasus tersebut. Polda Metro Jaya menjadi satuan kerja dengan jumlah penindakan paling banyak terhadap kasus kejahatan siber yaitu 3.709 perkara.[2]

II. LITERATUR REVIEW

Teknologi Web

Teknologi web merupakan sekelompok alat, bahasa, protokol, dan standar yang digunakan untuk mengembangkan dan menjalankan aplikasi dan situs web di World Wide Web (WWW). Teknologi web terus berkembang seiring berjalannya waktu, dan berikut ini beberapa teknologi web yang umum digunakan :

A. **HTML (Hypertext Markup Language):** HTML adalah bahasa markah yang digunakan untuk membuat struktur dasar halaman web. Ini digunakan untuk menentukan elemen-elemen seperti teks, gambar, tautan, dan lebih banyak lagi.[4]
B. **CSS (Cascading Style Sheets):** CSS digunakan untuk mengatur tampilan dan desain halaman web. Ini memungkinkan pengembang untuk mengontrol warna, ukuran, layout, dan elemen visual lainnya pada halaman web.[5]
C. **JavaScript:** JavaScript adalah bahasa pemrograman yang berjalan di sisi klien (browser) dan digunakan untuk menambahkan interaktivitas ke halaman web. Dengan JavaScript, dan dapat membuat efek animasi, validasi formulir, dan berbagai fitur lainnya.[6]
D. **HTTP (Hypertext Transfer Protocol):** HTTP adalah protokol komunikasi yang digunakan untuk mengirim dan menerima data antara server web dan browser. Ini adalah dasar dari semua interaksi web.[7]
E. **Web Servers:** Web server seperti Apache, Nginx, dan Microsoft IIS digunakan untuk menyajikan halaman web kepada pengguna melalui HTTP.

e-ISSN: 2828-6707
https://esensijournal.com/index.php/infokom
DOI: 10.55886/infokom.v8i1.816

F. **Database:** Untuk aplikasi web yang memerlukan penyimpanan dan pengambilan data, database seperti MySQL, PostgreSQL, MongoDB, dan lainnya sering digunakan.
G. **Web Frameworks:** Framework web seperti Ruby on Rails, Django, Express.js, dan Angular.js menyediakan alat dan struktur untuk membangun aplikasi web dengan lebih cepat dan efisien.
H. **Content Management Systems (CMS):** CMS seperti WordPress, Drupal, dan Joomla memungkinkan pengguna untuk membuat dan mengelola situs web tanpa harus menulis kode dari awal.
I. **API (Application Programming Interface):** API memungkinkan berbagai aplikasi untuk berkomunikasi dan berbagi data. RESTful API dan GraphQL adalah contoh API yang digunakan secara luas di web.
J. **Responsive Web Design:** Teknik desain yang memungkinkan halaman web untuk menyesuaikan diri dengan berbagai perangkat dan ukuran layar, memastikan pengalaman yang baik bagi pengguna di semua perangkat.
K. **Web Security:** Keamanan web adalah aspek penting dari teknologi web. Ini mencakup penggunaan SSL/TLS untuk enkripsi data, manajemen akses pengguna, dan perlindungan terhadap serangan seperti SQL injection dan Cross-Site Scripting (XSS).
L. **Cloud Computing:** Layanan cloud seperti AWS, Azure, dan Google Cloud memungkinkan pengembang untuk menyimpan, mengelola, dan menjalankan aplikasi web secara skalabel di infrastruktur yang dikelola secara profesional.
M. **Progressive Web Apps (PWA):** PWA adalah aplikasi web yang menyediakan pengalaman mirip aplikasi native, termasuk dukungan offline, notifikasi, dan responsif terhadap perangkat.
N. **Single Page Applications (SPA):** SPA adalah jenis aplikasi web yang memuat hanya satu halaman HTML utama dan mengganti konten secara dinamis menggunakan JavaScript.
O. **WebAssembly (Wasm):** WebAssembly adalah format biner yang dapat dijalankan oleh browser dan memungkinkan kinerja yang lebih tinggi untuk aplikasi web dengan menggunakan bahasa pemrograman selain JavaScript.

Web Server

Web server merupakan perangkat keras atau perangkat lunak yang bertugas menerima permintaan (requests) dari klien (biasanya browser web) dan mengirimkan respon (responses) yang sesuai dalam bentuk halaman web atau data lainnya. Web server adalah salah satu komponen kunci dalam infrastruktur internet yang memungkinkan pengguna untuk mengakses situs web dan aplikasi web. Berikut beberapa informasi lebih lanjut tentang web server:

A. **Perangkat Keras vs. Perangkat Lunak:** Web server dapat berupa perangkat keras fisik atau perangkat lunak yang dijalankan pada server komputer. Contoh perangkat lunak web server yang populer termasuk Apache HTTP Server, Nginx, Microsoft Internet Information Services (IIS), dan LiteSpeed.
B. **Protokol HTTP:** Web server berfungsi menggunakan protokol HTTP (Hypertext Transfer Protocol) untuk berkomunikasi dengan klien. Permintaan dari klien dikirim melalui HTTP kepada web server, dan server mengirimkan balasan HTTP yang sesuai.
C. **Menyajikan Konten:** Web server bertanggung jawab untuk menyajikan konten halaman web kepada pengguna. Ini dapat berupa halaman HTML, gambar, video, file CSS, JavaScript, dan banyak jenis konten lainnya.
D. **Routing dan Pengelolaan Permintaan:** Web server memiliki kemampuan untuk mengarahkan permintaan yang masuk ke aplikasi atau direktori yang tepat berdasarkan konfigurasi. Ini memungkinkan hosting beberapa situs web atau aplikasi di satu server fisik.
E. **Keamanan:** Web server memiliki fitur keamanan untuk melindungi situs web dari serangan, seperti Distributed Denial of Service (DDoS), serangan SQL injection, dan Cross-Site Scripting (XSS). Penggunaan SSL/TLS untuk enkripsi data juga merupakan bagian penting dari keamanan web server.
F. **Logging dan Analisis:** Web server biasanya mencatat aktivitas pengguna dalam file log. Ini membantu administrator server untuk memantau kinerja dan mengidentifikasi potensi masalah.
G. **Konfigurasi:** Administrasi web server melibatkan konfigurasi yang tepat untuk mengoptimalkan kinerja dan keamanan. Ini mencakup pengaturan seperti virtual host, izin akses, dan pengaturan jaringan.
H. **Skalabilitas:** Web server harus dapat menangani lalu lintas yang berfluktuasi. Ini dapat mencakup penambahan server secara horizontal (load balancing) atau vertikal (peningkatan daya komputasi) sesuai kebutuhan.
I. **Open Source vs. Proprietary:** Ada berbagai web server yang tersedia sebagai perangkat lunak sumber terbuka (open source) dan berbayar (proprietary).

Beberapa di antaranya gratis untuk digunakan, sementara yang lain memerlukan lisensi.

Web server merupakan komponen kritis dalam menjalankan aplikasi web dan situs web di internet. Pilihan web server yang tepat dan konfigurasi yang sesuai sangat penting untuk memastikan kinerja, keamanan, dan ketersediaan yang baik bagi pengguna situs web.

Pencegahan Web Defacement

Keamanan web server adalah aspek kunci dalam menjaga integritas dan ketersediaan situs web. Berikut adalah beberapa langkah yang dapat diambil untuk meningkatkan keamanan web server :

A. **Pembaruan Sistem:** Pastikan sistem operasi server dan perangkat lunak yang digunakan (termasuk server web) selalu diperbarui dengan patch keamanan terbaru. Perbaruan reguler sangat penting untuk mengatasi kerentanan keamanan yang telah ditemukan.
B. **Firewall:** Konfigurasi firewall untuk membatasi akses ke server. Serta dapat menggunakan firewall perangkat keras atau perangkat lunak seperti iptables (Linux), Windows Firewall (Windows), atau layanan cloud yang disediakan oleh penyedia cloud.
C. **Konfigurasi Keamanan:** Konfigurasikan server dengan kebijakan keamanan yang ketat. Matikan atau batasi fitur dan modul yang tidak diperlukan. Pastikan izin akses terbatas dan hanya diberikan kepada pengguna yang berwenang.[3]
D. **Enkripsi:** Gunakan protokol enkripsi seperti SSL/TLS untuk mengamankan data yang ditransmisikan antara klien dan server. Instal sertifikat SSL yang valid untuk situs web.
E. **Pemantauan Keamanan:** Aktifkan sistem pemantauan dan logging keamanan pada server. Ini akan membantu mendeteksi aktivitas mencurigakan dan melacak serangan potensial.[3]
F. **Pemutusan Jaringan (Isolasi):** Isolasikan aplikasi web dari komponen server lainnya dengan menggunakan teknik seperti kontainerisasi atau virtualisasi. Ini dapat mencegah serangan yang berhasil memanfaatkan celah di satu aplikasi web dari mengakses sumber daya server lainnya.[3]
G. **Pemantauan dan Analisis Log:** Perhatikan log keamanan server dan analisis mereka secara rutin untuk mendeteksi t-t aktivitas mencurigakan. Penggunaan alat SIEM (Security Information and Event Management) dapat membantu dalam mengelola log dengan efisien.[3]
H. **Kunci Akses:** Pastikan kunci akses (seperti kunci SSH) yang digunakan untuk mengakses server dengan sangat aman dan hanya dipegang oleh orang-orang yang berwenang. Pertimbangkan penggunaan otentikasi dua faktor (2FA) untuk lapisan tambahan keamanan.[3]
I. **Manajemen Akses:** Kelola akses pengguna dengan bijak. Berikan hak akses minimum yang diperlukan kepada pengguna dan prinsip kebutuhan-berdasarkan (principle of least privilege).[3]
J. **Pemantauan Jejaring Sosial:** Pantau media sosial dan platform komunikasi lainnya untuk melihat apakah ada klaim defacement atau tindakan mencurigakan terhadap situs web.
K. **Perangkat Keamanan Tambahan:** Pertimbangkan untuk menggunakan perangkat keamanan tambahan seperti Web Application Firewall (WAF), Intrusion Detection System (IDS), atau Intrusion Prevention System (IPS) untuk mendeteksi dan mencegah serangan.

III. METODOLOGI PENELITIAN

Metode penelitian yang digunakan pada penelitian ini adalah Metode penelitian tindakan (action research) yang merupakan pendekatan penelitian yang fokus pada pemecahan masalah dan perbaikan praktis dalam konteks situasi nyata. Tujuannya adalah untuk memahami, merencanakan, bertindak, dan merefleksikan kembali tindakan yang dilakukan untuk mengatasi masalah atau meningkatkan kualitas suatu situasi atau praktis tertentu. Melalui Metode action research, sebuah konsep/model/prototype benar-benar diuji-cobakan di dalam Subyek Penelitian dalam Konteks sesungguhnya. Metode Action Research menggunakan Dunia Praktis sebenarnya sebagai “Laboratorium” untuk menguji Teori. Secara umum Penelitian Tindakan (Action Research) ini masuk dalam kelompok Metodologi Penelitian Kualitatif karena data yang diamati dan dikumpulkan umumnya Bukan hanya data dalam bentuk angka.[9] Deskripsi tahapan Penelitian Tindakan yang paling populer disampaikan oleh Susman and Evered (1978), yakni bahwa sebuah Penelitian Tindakan (Action Research) dilakukan dengan melakukan 5 Tahapan yang bersifat siklus iteratif, yakni:

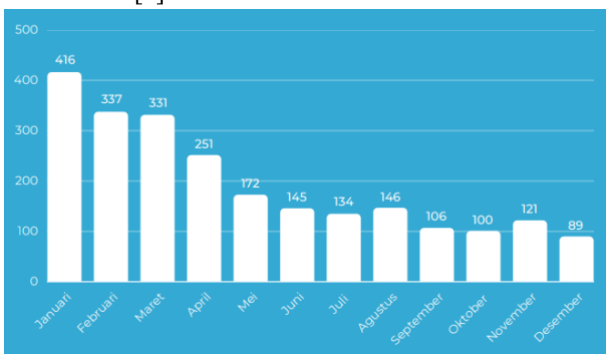
1. Diagnosing
2. Action Planning
3. Action Taking
4. Evaluating
5. Specifying Learning

IV. HASIL DAN PEMBAHASAN

Jurnal Esensi Infokom Vol 8 No. 1 Mei 2024
e-ISSN: 2828-6707
https://esensijournal.com/index.php/infokom
DOI: 10.55886/infokom.v8i1.816

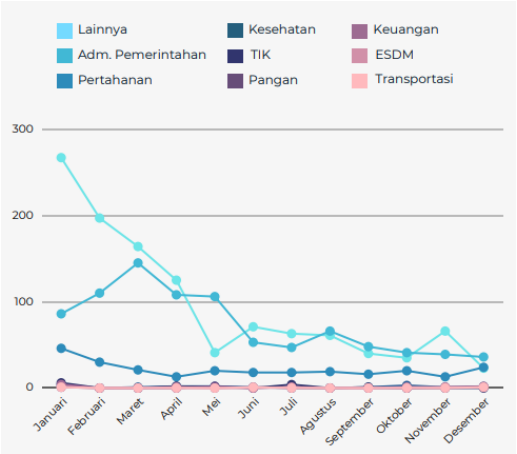
Diagnosing

Serangan web defacement merupakan serangan yang dilakukan untuk mengeksploitasi situs web atau server web yang rentan dengan memanfaatkan kerentanan dari sistem sehingga penyerang dapat merusak, memodifikasi, atau menghapus konten halaman web yang telah diretas. Insiden web defacement merupakan insiden yang terjadi pada tampilan website dimana threat actor melakukan perubahan tampilan website sehingga dapat merusak reputasi pemilik sistem. Umumnya web defacement memanfaatkan kerentanan pada sistem website seperti CMS, Plugin, dan Web Engine yang tidak dilakukan update. Walaupun metode serangan yang digunakan dikategorikan sederhana dan mudah, namun insiden web defacement dapat dimanfaatkan sebagai awalan pintu masuk insiden lainnya dan bahkan server yang terkompromi dapat digunakan sebagai botnet untuk melakukan serangan ke sistem/infrastruktur lainnya. Selama tahun 2022, BSSN telah mencatat terdapat 2.348 kasus web defacement yang terjadi di situs-situs Indonesia dengan kasus terbanyak terjadi pada bulan Januari dengan jumlah kasus sebanyak 416 kasus web defacement.[1]



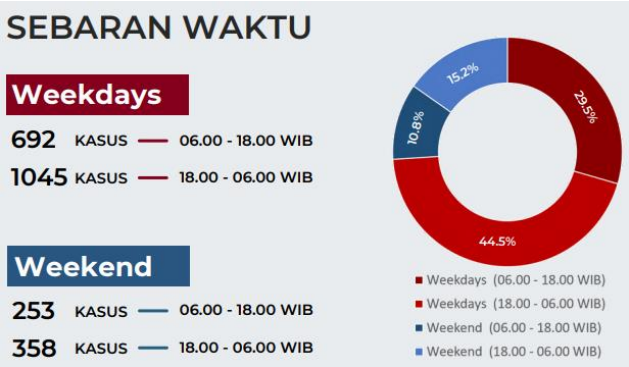
Gambar 1. Web Defacement di Indonesia
Sumber : Lanskap Keamanan Siber Indonesia, BSSN, 2022.

Selama tahun 2022, sektor yang paling banyak terkena serangan web defacement adalah sektor Administrasi Pemerintahan dengan jumlah kasus sebanyak 885 kasus.[1]



Gambar 2. Sektor terdampak Web Defacement
Sumber : Lanskap Keamanan Siber Indonesia, BSSN, 2022.

Pengelompokan kasus web defacement berdasarkan sebaran waktu bertujuan untuk mengetahui waktu terbanyak terjadinya web defacement. Berdasarkan hasil pengelompokan tersebut diketahui bahwa kasus web defacement paling banyak terjadi pada Weekdays (SeninJumat) pada pukul 18.00 – 06.00 WIB dengan jumlah kasus sebanyak 1045 kasus.[1]



Gambar 3. Sebaran waktu Web Defacement
Sumber : Lanskap Keamanan Siber Indonesia, BSSN, 2022.

Website www.arya.one dipasang pada Virtual Private Server (VPS) dan Server tersebut menggunakan web kontrol panel PLESK. Virtual Private Server (VPS) adalah bentuk virtualisasi yang memungkinkan sejumlah besar server virtual berjalan di dalam satu server fisik tunggal. Setiap VPS memiliki lingkungan server yang terisolasi, yang membuatnya tampak dan berperilaku seperti server fisik yang independen. VPS sering digunakan sebagai alternatif yang lebih terjangkau dibandingkan dengan menyewa server fisik secara penuh.

Vektor Serangan Web Defacement

Berdasarkan hasil Asistensi Tanggap Insiden dari Badan Siber dan Sandi Negara, diketahui attack vector yang dimanfaatkan threat actor sebagai berikut:

1. **Exploit Public-Facing Application**
   Threat actor memanfaatkan kelemahan yang terdapat pada situs web untuk melakukan berbagai percobaan serangan seperti SQL Injection, File Upload, XSS, dan lain sebagainya.
2. **Active Scanning**
   Threat actor melakukan scanning untuk mengumpulkan informasi yang dapat dilakukan eksploitasi dari sistem target.
3. **Compsomised Account**
   Threat actor memanfaatkan akun-akun yang telah terkompromi oleh malware stealer untuk masuk ke sistem.

Action Planning

Website www.arya.one menggunakan web kontrol panel Plesk. Plesk adalah sebuah platform kontrol hosting web yang digunakan untuk mengelola server web dan hosting situs web. Salah satu panel kontrol hosting web yang populer dan memiliki banyak fitur yang memudahkan pengelolaan server web, situs web, database, dan aplikasi. Plesk digunakan oleh penyedia hosting web, administrator sistem, dan pemilik situs web untuk mengatur berbagai aspek hosting web.[8]

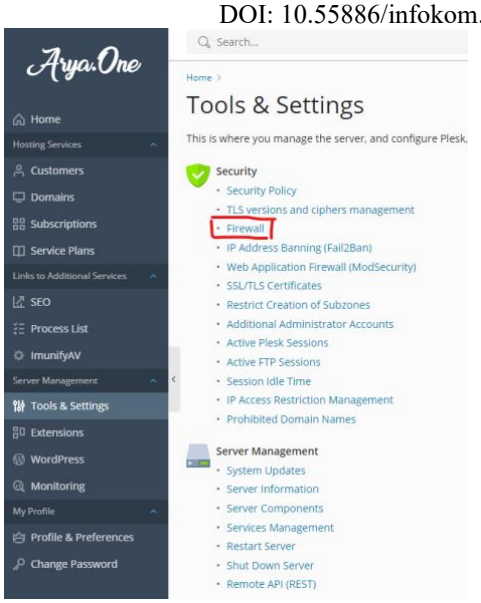
Beberapa fitur utama dari Plesk meliputi:

1. **Manajemen Domain:** Plesk memungkinkan untuk dengan mudah menambahkan, menghapus, dan mengelola domain dan subdomain pada server .
2. **Manajemen Aplikasi:** dapat menginstal, mengelola, dan memantau aplikasi web seperti WordPress, Joomla, dan Drupal dengan mudah melalui Plesk.
3. **Manajemen Database:** Plesk mendukung berbagai jenis database seperti MySQL, PostgreSQL, dan Microsoft SQL Server, memungkinkan untuk membuat, mengelola, dan membackup database.
4. **Keamanan:** Plesk dilengkapi dengan alat keamanan seperti firewall, deteksi malware, dan sertifikat SSL, yang membantu melindungi situs web dan data .
5. **Manajemen Server:** dapat mengelola server melalui Plesk, termasuk manajemen pengguna, izin, dan konfigurasi server.
6. **Statistik dan Analitik:** Plesk menyediakan statistik lalu lintas web dan alat analitik untuk membantu memahami kinerja situs web .
7. **Otomatisasi:** Plesk menyediakan alat otomatisasi untuk tugas-tugas seperti pencadangan, pemulihan, dan pemantauan, yang menghemat waktu administrator.

Action Taking

Pada tahap ini dilakukan beberapa implementasi keamanan untuk pencegahan web defacement pada website www.arya.one:

1. **Firewall:** Plesk dilengkapi dengan firewall yang dapat dikonfigurasi untuk melindungi server dari serangan jaringan dan mencoba akses yang tidak sah. Pada Plesk dapat mengatur aturan firewall sesuai kebutuhan. Berikut langkah-langkah untuk mengkonfigurasi firewall pada Plesk:



Gambar 4. Konfigurasi Firewall pada Plesk

A. Masuk ke Plesk:
Buka browser web dan akses antarmuka Plesk dengan mengunjungi URL seperti https://alamat-ip-server:8443 (ganti alamat-ip-server dengan alamat IP atau nama domain server Plesk).
Masukkan kredensial administrator (username dan password) untuk masuk.

B. Buka Modul Firewall:
Setelah berhasil masuk, klik pada tab "Tools & Settings" (Alat dan Pengaturan) di sisi kiri.

C. Pilih "Firewall":
Di bawah bagian "Security", dapat menemukan opsi "Firewall". Klik pada opsi ini untuk membuka modul firewall.

D. Atur Aturan Firewall:
Di dalam modul Firewall, dapat melihat daftar aturan yang ada dan status firewall saat ini. Dapat mengonfigurasi aturan firewall dengan mengklik "Enable Firewall" (Aktifkan Firewall) jika belum aktif.
Selanjutnya, dapat menambahkan, menghapus, atau mengedit aturan-aturan firewall sesuai kebutuha. Ini termasuk mengizinkan atau memblokir port, protokol, atau alamat IP tertentu. Pastikan untuk mengklik tombol "Apply" (Terapkan) setelah membuat perubahan pada aturan firewall.

E. Atur Jenis Firewall:
Plesk mendukung dua jenis firewall, yaitu "Basic Firewall Rules" (Aturan Firewall Dasar) dan

"Advanced Firewall Rules" (Aturan Firewall Lanjutan).

F. **Monitor Log Firewall:**
Plesk juga menyediakan opsi untuk memantau log firewall melalui antarmuka web. Ini memungkinkan melihat catatan aktivitas firewall untuk mengidentifikasi percobaan akses yang tidak sah atau ancaman keamanan lainnya.

G. **Simpan Konfigurasi:**
Pastikan untuk menyimpan semua perubahan yang dibuat pada konfigurasi firewall dengan mengklik tombol "Apply" atau "OK" yang sesuai.

2. **Web Application Firewall:** ModSecurity adalah sebuah aplikasi keamanan open-source yang berfungsi sebagai firewall aplikasi web (WAF) untuk melindungi server web dari serangan siber. ModSecurity dapat digunakan dengan panel kontrol web seperti Plesk untuk meningkatkan keamanan situs web. Berikut langkah-langkah mengaktifkan ModSecurity pada Plesk:

Masuk ke Plesk:
Masuk ke Plesk Control Panel sebagai administrator.
Aktifkan ModSecurity:
Di dashboard Plesk, buka tab "Server Management".
Pilih "Tools & Settings".
Pilih ModSecurity:
Di bawah "Security", klik "Web Application Firewall (ModSecurity)".
Aktifkan ModSecurity:
Pastikan "Web application firewall mode" diatur ke "On".
Klik "Apply" untuk menyimpan perubahan.
Konfigurasi ModSecurity:
Setelah mengaktifkan ModSecurity, dapat mengonfigurasinya lebih lanjut sesuai dengan kebutuhan. Dan dapat menambahkan aturan kustom, mengonfigurasi tindakan yang diambil saat serangan terdeteksi, dan lainnya. Ini bergantung pada preferensi keamanan.
Lihat Laporan dan Log:
ModSecurity akan mencatat aktivitas firewall dan serangan yang terdeteksi. Dapat mengakses laporan dan log melalui Plesk untuk memeriksa aktivitas yang terkait dengan keamanan situs web.
Uji ModSecurity:
Setelah mengaktifkan ModSecurity, penting untuk menguji situs web untuk memastikan bahwa tidak ada kesalahan atau blokir yang tidak diinginkan yang terjadi. Pastikan situs web berfungsi seperti seharusnya.
Perbarui dan Pantau:
Terus perbarui ModSecurity dan peraturannya secara berkala untuk menjaga perlindungan terhadap serangan yang baru muncul. Selain itu, monitor log keamanan secara teratur untuk mendeteksi aktivitas mencurigakan.

3. **Antivirus dan Antimalware:** Plesk dapat memindai file dan situs web untuk deteksi virus dan malware. Plesk tidak menyediakan antivirus built-in secara default, tetapi dapat menginstal perangkat lunak antivirus pihak ketiga pada server yang dihosting pada Plesk. Beberapa antivirus yang umum digunakan dan dapat diintegrasikan dengan Plesk diantaranya ClamAV dan Kaspersky Antivirus. Berikut adalah langkah-langkah untuk menginstal dan mengkonfigurasi ClamAV pada Plesk:

A. **Masuk ke Server:** Pastikan telah masuk ke server yang dihosting Plesk dengan akses root atau hak administrator.

B. Instal ClamAV:
Untuk sistem berbasis Linux, dapat menggunakan manajer paket seperti apt (untuk Debian/Ubuntu) atau yum (untuk CentOS/RHEL) untuk menginstal ClamAV. Contoh perintah untuk instalasi di Ubuntu adalah:

```arduino
sudo apt-get install clamav
```

Gambar 5. Konfigurasi AntiVirus pada Plesk

C. Konfigurasi ClamAV:

D. Setelah ClamAV terinstal, dapat mengkonfigurasi pengaturannya. File konfigurasi ClamAV biasanya berada di **/etc/clamav/clamd.conf** dan **/etc/clamav/freshclam.conf**.

E. **Update Database Virus:** ClamAV memerlukan database virus yang diperbarui secara teratur. Dapat mengupdate database ini dengan menjalankan perintah:

Jurnal Esensi Infokom Vol 8 No. 1 Mei 2024
e-ISSN: 2828-6707
https://esensijournal.com/index.php/infokom
DOI: 10.55886/infokom.v8i1.816

```
sudo freshclam
```

Gambar 6. Update Antivirus Database

F. Integrasikan ClamAV dengan Plesk:

1) Buka antarmuka web Plesk.
2) Di bagian "Server Management" (Manajemen Server), klik "Tools & Settings" (Alat dan Pengaturan).
3) Di bawah "Security", pilih "Antivirus".
4) Aktifkan opsi "Switch on antivirus protection" (Aktifkan perlindungan antivirus).
5) Pilih ClamAV sebagai "Antivirus server" dari daftar drop-down.

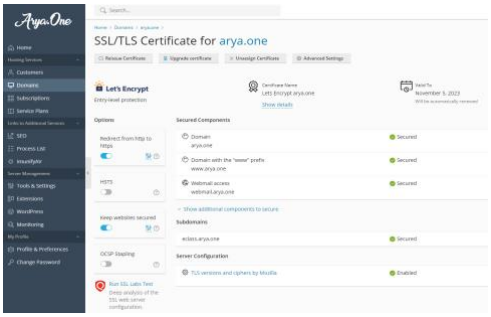
G. Konfigurasi Antivirus Pada Mail Server (Opsional):

Jika ingin memeriksa email dengan ClamAV, dapat juga mengonfigurasi Mail Server untuk menggunakan ClamAV. Pilih "Mail Server Settings" (Pengaturan Server Email) di Plesk dan aktifkan "Switch on antivirus protection" (Aktifkan perlindungan antivirus) di bagian "Antivirus Settings" (Pengaturan Antivirus).

H. Simpan Perubahan:

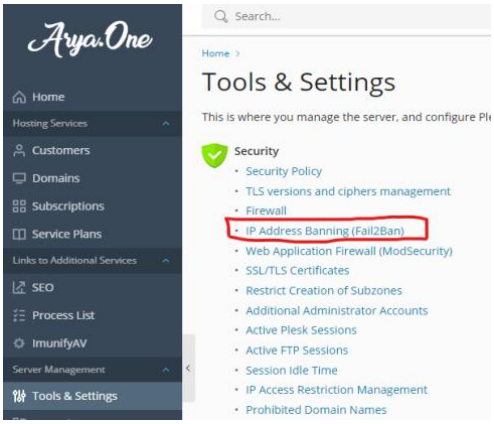
Jangan lupa untuk menyimpan perubahan yang dibuat dalam antarmuka web Plesk.

4. **Pengendalian Akses Pengguna:** Plesk memiliki fitur mengelola izin dan hak akses pengguna secara rinci, membatasi akses mereka ke bagian-bagian tertentu dari server dan situs web. Ini membantu mengurangi risiko akses yang tidak sah.
5. **Sertifikat SSL:** Plesk menyediakan dukungan untuk instalasi dan manajemen sertifikat SSL. Ini membantu menjaga koneksi ke situs web aman dengan enkripsi data.



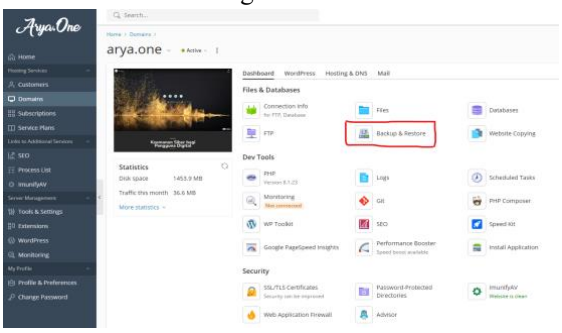
Gambar 6. Konfigurasi SSL pada Plesk

6. **Deteksi Intrusi:** Plesk dapat memonitor aktivitas server dan mendeteksi aktivitas yang mencurigakan atau potensi serangan. Ini membantu dalam respons cepat terhadap ancaman. Deteksi intrusi (Intrusion Detection System atau IDS) adalah salah satu elemen penting dalam menjaga keamanan server Plesk. IDS berfungsi untuk mendeteksi aktivitas mencurigakan atau serangan keamanan pada server. Plesk memiliki fitur IDS yang disebut "Fail2Ban" yang dapat membantu dalam mendeteksi dan merespons serangan brute force atau percobaan akses yang tidak sah. Fail2Ban adalah alat yang berguna untuk membantu melindungi server Plesk dari serangan brute force dan serangan berbasis pola tertentu. Dengan konfigurasi yang benar dan pemantauan IDS secara berkala, dapat memitigasi risiko keamanan.



Gambar 7. Konfigurasi IDS Fail2Ban pada Plesk

7. **Pencadangan dan Pemulihan:** Melakukan pencadangan rutin dari situs web dan data-data penting adalah langkah keamanan yang diharuskan. Plesk menyediakan alat pencadangan otomatis yang dapat membantu memulihkan data jika terjadi kerusakan atau serangan.



Gambar 8. Backup dan Restore pada Plesk

8. **Keamanan Email:** Plesk memiliki fitur keamanan email yang dapat memeriksa email masuk untuk ancaman malware dan spam, serta menyediakan opsi

pengaturan filter email yang disesuaikan. Untuk menjaga keamanan email pada Plesk, ada beberapa langkah yang dapat melindungi komunikasi email dan menghindari serangan spam atau malware. Berikut adalah beberapa langkah konfigurasi keamanan email pada Plesk:

A. **Aktifkan Antivirus dan Antispam:**
   Pastikan telah mengaktifkan antivirus dan antispam pada server Plesk. Konfigurasinya melalui antarmuka Plesk di bagian "Mail Server Settings" (Pengaturan Server Email).
B. **Gunakan Protokol Keamanan:**
   Selalu gunakan protokol keamanan seperti SSL/TLS saat mengakses email. Ini akan mengenkripsi komunikasi email, dan menjaga kerahasiaan data.
C. **Atur SPF dan DKIM:**
   SPF (Sender Policy Framework) dan DKIM (DomainKeys Identified Mail) adalah metode otentikasi email yang membantu mencegah spoofing email.
D. **Blokir Akses untuk IP Mencurigakan:**
   Plesk memiliki fitur yang untuk memblokir akses dari IP yang mencurigakan. Terdapat padai "Tools & Settings" > "IP Access Restrictions."
E. **Gunakan Filter Email:**
   Mengonfigurasi filter email untuk menghapus atau memindahkan email spam ke folder spam. Ini membantu mengurangi kemungkinan penerimaan email berbahaya.
F. **Buat Kebijakan Keamanan Email:**
   Buat dan terapkan kebijakan keamanan email yang ketat untuk pengguna. Beri tahu mereka untuk tidak membuka lampiran yang mencurigakan atau mengklik tautan yang tidak dikenal.
G. **Pembaruan Rutin:**
   Pastikan perangkat lunak server Plesk dan komponen email yang digunakan selalu diperbarui dengan patch keamanan terbaru.
H. **Backup Email:**
   Selalu buat cadangan email yang penting. Ini membantu dalam mengatasi kehilangan data email akibat serangan atau kesalahan manusia.

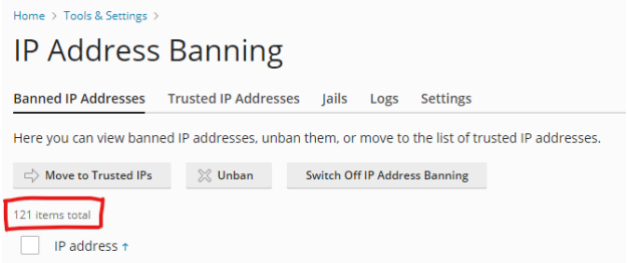
9. **Update Otomatis:** Plesk dapat mengotomatisasi pembaruan perangkat lunak server dan aplikasi web untuk memastikan bahwa server selalu diperbarui dengan patch keamanan terbaru.

Evaluating

Pada tahap ini dievaluasi kinerja dari konfigurasi keamanan yang telah dilakukan pada tahap action taking, berikut adalah beberapa kinerja konfigurasi keamanan yang telah berhasil mencegah serangan serangan ke web server www.arya.one :

Intrusion Detection System (IDS) Fail2Ban:

Intrusion Detection System (IDS) Fail2Ban berhasil mencegah ratusan serangan ke webserver www.arya.one beserta Log pencacatannya seperti pada gambar berikut :

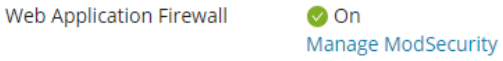


Gambar 9. Instrusion Detection System

Gambar 10. Log Fail2Ban

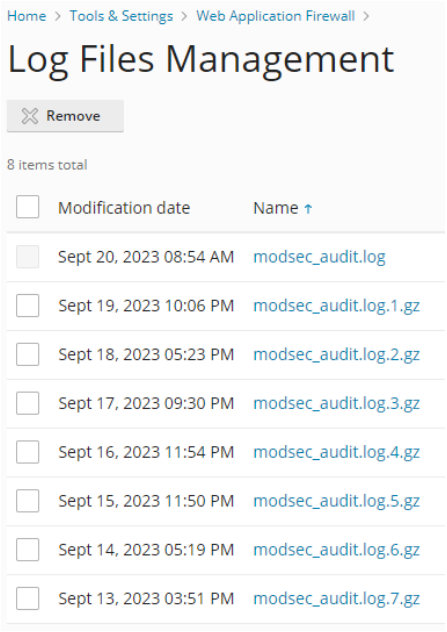
Web Appplication Firewall

Modsecurity telah diaktivasi dan berjalan dengan baik untuk mencegah beberapa serangan ke web server beserta Log nya, seperti pada gambar berikut.



Gambar 11. Web Application Firewall

e-ISSN: 2828-6707
https://esensijournal.com/index.php/infokom
DOI: 10.55886/infokom.v8i1.816



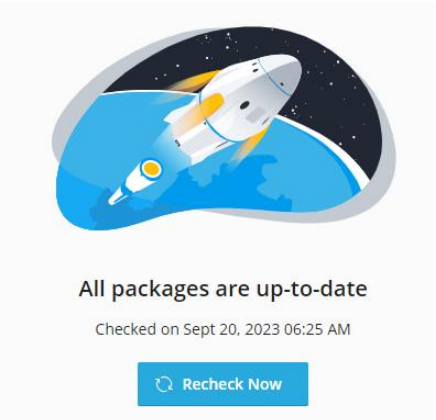
Gambar 12. Log Web Application Firewall

Berikut adalah beberapa jenis serangan dan ancaman yang dapat dicegah oleh ModSecurity:

1. **SQL Injection:** ModSecurity dapat mencegah serangan SQL injection dengan memantau permintaan HTTP dan mendeteksi upaya untuk memasukkan perintah SQL berbahaya ke dalam input yang disampaikan ke server web.
2. **Cross-Site Scripting (XSS)**: ModSecurity dapat mengidentifikasi dan mencegah serangan XSS dengan memeriksa apakah ada skrip berbahaya yang mencoba dieksekusi pada halaman web.
3. **Local File Inclusion (LFI) dan Remote File Inclusion (RFI):** ModSecurity dapat mencegah upaya pengguna untuk mengakses atau menyisipkan file lokal atau remote ke dalam aplikasi web, yang dapat digunakan untuk mendapatkan akses yang tidak sah.
4. **Cross-Site Request Forgery (CSRF):** ModSecurity dapat mengenali serangan CSRF dengan melacak permintaan yang tidak sah yang mencoba melakukan tindakan tidak diinginkan atas nama pengguna yang sah.
5. **Brute Force Attacks:** ModSecurity dapat mengidentifikasi upaya brute force untuk menebak kata sandi dengan memblokir alamat IP yang mencoba login secara berulang kali dengan kombinasi yang salah.
6. **Serangan HTTP DoS (Denial of Service):** ModSecurity dapat menghadapi serangan DoS dengan mendeteksi dan memblokir upaya yang mencoba menghabiskan sumber daya server dengan permintaan yang berlebihan.
7. **Perlindungan terhadap Akses Berlebihan dan Scan Port:** ModSecurity dapat mencegah akses berlebihan atau scan port dengan memblokir permintaan yang mencurigakan atau yang tidak diinginkan.
8. **Perlindungan terhadap Serangan Nol Hari (Zero-Day Attacks):** ModSecurity dapat memberikan perlindungan tambahan terhadap serangan yang belum dikenal atau serangan nol hari dengan mengidentifikasi pola perilaku mencurigakan.
9. **Pengendalian Akses:** ModSecurity dapat digunakan untuk mengendalikan akses ke situs web dengan berbasis aturan, misalnya, hanya mengizinkan akses dari wilayah geografis tertentu atau memblokir alamat IP yang mencurigakan.
10. **Perlindungan terhadap Hotlinking:** ModSecurity dapat mencegah situs web dari hotlinking, yaitu ketika situs web lain mencoba menggunakan sumber daya gambar atau media secara tidak sah.
11. **Perlindungan terhadap Skrip Berbahaya:** ModSecurity dapat mendeteksi dan memblokir upaya untuk mengunggah atau menjalankan skrip berbahaya pada server web.
12. **Perlindungan terhadap Vulnerability Scanning:** ModSecurity dapat mencegah upaya pemindaian kelemahan yang mencari titik masuk potensial pada server web.

Pembaruan Rutin

Perangkat lunak server Plesk dan komponen-komponen lain selalu diperbaharui dengan patch keamanan yang terbaru.



Gambar 13. Pembaruan

Specifying Learning

Pencegahan Web defacement meliputi berbagai langkah-langkah penerapan keamaan untuk melindungi integritas dan tampilan situs web dari perubahan yang tidak sah. “Learning” pada konteks web deafecent mengacu pada proses pemantauan

situs web dari potensi perubahan anomali sehingga sistem keaman dapat beradaptasi dan merespon ancaman yang muncul. Dengan mempelajari "Lesson Learned" dalam pencegahan Web Defacement kita dapat membuat sistem pertahanan dinamis yang dapat beradaptasi dari ancaman baru. Diperlukan juga peninjauan dan selalu memperbaharui langkah-langkah keamanan pada web server.

V. KESIMPULAN

Kesimpulan dari upaya pencegahan web defacement yaitu bahwa pencegahan harus menjadi bagian integral dari strategi keamanan website. Defacement adalah tindakan merusak dan mengubah tampilan website, dan dapat merusak reputasi bisnis serta mengancam kepercayaan pengunjung. Dengan menerapkan langkah-langkah pencegahan yang efektif seperti pada pembahasan, menjadi suatu keharusan dan sangat penting. Diperlukan juga kombinasi berbagai langkah pencegahan untuk dapat membuat lapisan perlindungan yang kuat serta terus menerus memperbaharuin dan memantau keamanan website secara berkala.

.

UCAPAN TERIMA KASIH

Terima kasih Kepada Pengelola Jurnal Esensi Komputasi Institut Bisnis Nusantara, yang telah memberikan kesempatan dalam publikasi jurnal ini, Harapan jurnal ini dapat memberikan pengetahuan dan manfaat. Terima kasih.

REFERENSI

[1] Lanskap Keamanan Siber Indonesia, Badan Siber dan Sandi Negara, 2022.

[2] Pusiknas Polri : https://pusiknas.polri.go.id/detail_artikel/kejahatan_siber_di_indonesia_naik_berkali-kali_lipat (September 2023)

[3] The Ten Most Critical Web Application Security Risks, OWASP (Open Web Application Security Project), 2017.

[4] HTML (Hypertext Markup Language): https://developer.mozilla.org/en-US/docs/Web/HTML (September 2023)

[5] CSS (Cascading Style Sheets): https://developer.mozilla.org/en-US/docs/Web/CSS (September 2023)

[6] JavaScript:https://developer.mozilla.org/en-US/docs/Web/JavaScript (September 2023)

[7] HTTP (Hypertext Transfer Protocol): https://www.ietf.org/rfc/rfc2616.txt (September 2023)

[8] Plesk Web Control Panel : https://www.plesk.com/ (September 2023)

[9] Susanto, Tony Dwi, Metode Penelitian Tindakan (Action Research) : https://notes.its.ac.id/tonydwisusanto/2020/09/05/metode-penelitian-tindakan-action-research/