Laporan Komprehensif Penilaian Keamanan Infrastruktur Server: Analisis Risiko dan Rekomendasi Mitigasi

---

Pendahuluan

Laporan ini berisi temuan yang diperoleh dari hasil pemindaian terhadap server yang menggunakan IP 103.146.62.138, yang meng-host berbagai layanan seperti Nginx, HTTP, POP3, IMAP, dan MySQL. Pemindaian dilakukan dengan menggunakan alat Nmap dan Nikto untuk mengidentifikasi kerentanannya, serta menganalisis potensi ancaman yang dapat dieksploitasi dari dalam jaringan (LAN). Berdasarkan hasil pemindaian ini, ditemukan beberapa celah yang berpotensi dimanfaatkan oleh penyerang yang sudah berada di dalam jaringan internal.

Tujuan Pengujian

- **Mengidentifikasi port yang terbuka pada server.**
- **Memeriksa konfigurasi server yang dapat menyebabkan kerentanannya, baik dari luar maupun dari dalam jaringan.**
- **Menilai efektivitas perlindungan firewall dan WAF (Web Application Firewall) terhadap ancaman eksternal serta ancaman yang berasal dari dalam jaringan (LAN).**

Metodologi

Pemindaian dilakukan dengan menggunakan alat:

- **Nmap: Digunakan untuk mendeteksi port terbuka dan layanan yang berjalan pada server.**
- **Nikto: Digunakan untuk memeriksa kerentanannya pada server web, termasuk potensi serangan XSS, clickjacking, dan kerentanannya terkait SSL/TLS.**

Hasil Pemindaian dengan Nmap

Berikut adalah hasil yang ditemukan setelah melakukan pemindaian dengan Nmap:

Port terbuka:

- **Port 21/tcp (FTP): Ditemukan dengan status tcpwrapped.**
- **Port 80/tcp (HTTP): Menggunakan Nginx.**
- **Port 443/tcp (HTTPS): SSL aktif.**
- **Port 110/tcp (POP3): Menggunakan Dovecot pop3d.**
- **Port 111/tcp (RPCBind).**
- **Port 3306/tcp (MySQL 5.7.20).**
- **Port 1234/tcp: Statusnya "hotline" yang mencurigakan.**
- **Port 1723/tcp: PPTP.**
- **Port 8081/tcp: Menggunakan Apache HTTPD 2.4.18.**

Peringatan Terkait Kerentanan:

- **SSL Server menggunakan sertifikat yang diterbitkan oleh Let's Encrypt, dengan waktu kedaluwarsa pada 2025-08-02.**
- **Teridentifikasi bahwa server web menggunakan Content-Encoding: deflate, yang bisa membuka potensi serangan BREACH.**
- **Beberapa header yang tidak ada, seperti X-Frame-Options, yang bisa membuka celah serangan clickjacking.**
- **Terdeteksi potensi kebocoran informasi terkait ETag dan inode (CVE-2003-1418).**

Metode HTTP yang Diizinkan:

- **Server mengizinkan metode GET, HEAD, POST, dan OPTIONS, yang dapat dimanfaatkan oleh penyerang jika tidak dikelola dengan baik.**

Hasil Pemindaian dengan Nikto

Nikto melakukan pemindaian terhadap aplikasi web pada https://bmt.darunnajah.com/#/login?returnUrl=%2Fdashboard, dan menemukan beberapa kerentanannya:

- **X-Frame-Options tidak ada, membuka kemungkinan serangan clickjacking.**

- **Strict-Transport-Security (HSTS) tidak didefinisikan, berarti server tidak mengharuskan penggunaan HTTPS untuk seluruh sesi.**

- **X-Content-Type-Options tidak diatur, yang dapat memungkinkan agen pengguna untuk merender konten web dalam cara yang tidak diinginkan.**

- **Inode Leakage via ETags: Server mengungkapkan informasi inode yang dapat digunakan oleh penyerang untuk merencanakan serangan lebih lanjut.**

- **Ditemukan file default seperti icons/README yang dapat diakses, menunjukkan bahwa konfigurasi Apache belum sepenuhnya diamankan.**

Analisis Keamanan

Berdasarkan hasil pemindaian:

- **Kerentanan WAF dan Firewall: Meskipun server memiliki lapisan perlindungan WAF dan firewall, perlindungannya terbatas hanya pada akses eksternal. Tidak ada pembatasan terhadap akses dari dalam jaringan internal, yang bisa dimanfaatkan oleh penyerang yang sudah berada di dalam jaringan.**

- **Akses dari Jaringan Lokal (LAN): Akses dari LAN dapat menghindari pembatasan yang ada pada WAF dan firewall, yang menunjukkan bahwa perlindungan dari dalam jaringan kurang ketat dibandingkan perlindungan dari luar. Ini dapat dimanfaatkan oleh penyerang yang sudah memiliki akses ke jaringan internal untuk melakukan eksploitasi lebih lanjut.**

  Potensi Ancaman dari Jaringan Internal:

  - **Worms dan RATs dapat menyebar secara otomatis melalui jaringan internal. Malware ini dapat mengeksploitasi kerentanannya pada perangkat yang terhubung dalam jaringan untuk menyebar dan merusak lebih banyak perangkat.**

  - **Malware seperti Ransomware dan Credential Dumping bisa digunakan untuk mengenkripsi file atau mencuri kredensial pengguna di dalam jaringan internal.**

  - **Serangan Man-in-the-Middle (MITM) dapat digunakan oleh penyerang di jaringan internal untuk mengakses dan memodifikasi data yang ditransmisikan antar perangkat.**

- **Dengan adanya port yang terbuka dan layanan yang terdeteksi, seperti Apache 2.4.18, MySQL 5.7.20, serta layanan yang tidak dikenal pada Port 1234/tcp, penyerang bisa mengeksploitasi layanan tersebut untuk bergerak lateral di dalam jaringan, mencari kelemahan lain, dan mengakses data sensitif.**

Rekomendasi Keamanan

Peningkatan Pengaturan WAF dan Firewall:

- **Meninjau dan meningkatkan pengaturan WAF untuk mencegah eksploitasi dari akses internal, serta memperkuat konfigurasi firewall agar membatasi lalu lintas yang datang dari LAN.**

Peningkatan Keamanan SSL:

- **Mengonfigurasi Strict-Transport-Security (HSTS) untuk memastikan seluruh komunikasi dilakukan melalui HTTPS.**
- **Memperbaiki header X-Frame-Options untuk mencegah clickjacking.**

Patch dan Pembaruan Sistem:

- **Melakukan pembaruan pada server yang menggunakan Apache 2.4.18 dan MySQL 5.7.20 untuk mengatasi kerentanannya, serta menutup celah yang bisa dimanfaatkan oleh malware dari dalam jaringan.**
- **Menyembunyikan atau mengamankan akses ke file default seperti icons/README yang ditemukan.**

Audit Layanan Terbuka:

- **Menonaktifkan atau memproteksi layanan yang tidak perlu, seperti port 1234/tcp (Hotline), serta port lainnya yang terdeteksi selama pemindaian.**

Deteksi Serangan:

- **Menyertakan Intrusion Detection System (IDS) untuk memantau lalu lintas mencurigakan baik dari jaringan internal maupun eksternal.**

Keamanan Jaringan Internal:

- **Melakukan segmentasi jaringan untuk membatasi pergerakan lateral malware di dalam jaringan.**
- **Implementasikan VPN dan MFA untuk membatasi akses hanya pada pengguna yang sah.**
- **Lakukan audit keamanan secara berkala dan edukasi pengguna tentang potensi serangan yang bisa terjadi dari dalam jaringan.**

Kesimpulan

Laporan ini menunjukkan bahwa meskipun firewall dan WAF memberikan perlindungan terhadap ancaman eksternal, mereka tidak cukup efektif dalam menangani potensi serangan dari dalam jaringan atau dari pengguna yang sudah mendapatkan akses. Oleh karena itu, tindakan tambahan seperti pembaruan perangkat lunak, penguatan konfigurasi server, serta penerapan kontrol akses yang lebih ketat sangat diperlukan untuk meningkatkan keamanan sistem ini. Perlindungan terhadap serangan dari jaringan internal harus menjadi perhatian utama dalam memperbaiki konfigurasi keamanan server ini.

Semoga laporan ini bisa membantu Anda dalam mengidentifikasi potensi kerentanannya dan memberikan langkah-langkah mitigasi yang tepat untuk meningkatkan keamanan server.