



**ANALISIS SISTEM KEAMANAN PADA APACHE WEB
SERVER MENGGUNAKAN SELF SIGNED CA DI
WEBMIN**

**Buku Panduan: Mengamankan Apache Server Lokal
dengan Sertifikat Self-Signed via Webmin**

FAUZAN NUGROHO

1807422024

**PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK NEGERI JAKARTA**

2025

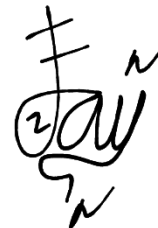
KATA PENGANTAR

Puji syukur kepada Allah SWT berkat Rahmat, Hidayah, dan Karunia-Nya kepada kita semua sehingga penulis dapat menyelesaikan Buku Panduan. Penulis menyadari dalam penyusunan skripsi ini tidak akan selesai tanpa bantuan dari berbagai pihak. Karena itu pada kesempatan ini penulis ingin mengucapkan terima kasih kepada:

1. Allah SWT tuhan yang maha esa, yang telah memberikan saya rizki berupa kesehatan dan akal pikiran yang sangat berharga bagi penulis sehingga laporan ini dapat terselesaikan dengan baik.
2. Orang tua dan keluarga penulis yang telah memberikan bantuan dukungan secara moral dan material.
3. Bapak Defiana arnaldy, S. Tp., M. Si. selaku pembimbing skripsi yang telah membimbing penulis dalam menyelesaikan skripsi ini.

Penulis menyadari skripsi ini tidak luput dari berbagai kekurangan. Penulis mengharapkan saran dan kritik demi kesempurnaan dan perbaikannya sehingga akhirnya laporan skripsi ini dapat memberikan manfaat bagi bidang pendidikan dan penerapan di lapangan serta bisa dikembangkan lagi lebih lanjut.

Depok, 6 Juli 2025

A handwritten signature in black ink, appearing to be 'Fauzan Nugroho', with a stylized flourish at the end.

(Fauzan Nugroho)

Kebutuhan Alat & Perangkat Lunak

Sebelum memulai, pastikan Anda memiliki perangkat lunak berikut:

- **VirtualBox:** Untuk membuat lingkungan server virtual.
- **ISO Ubuntu Server:** Sistem operasi untuk server.
- **Apache & Webmin:** Web server dan panel kontrol yang akan diinstal di Ubuntu.

Langkah 1: Persiapan Lingkungan Server

Langkah pertama adalah menyiapkan server dasar yang akan diamankan.

1. Instalasi OS: Instal Ubuntu Server 24.04 di dalam VirtualBox.
2. Konfigurasi Jaringan: Atur alamat IP statis untuk server agar mudah diakses, contohnya 192.168.57.2.
3. Instalasi Apache: Lakukan pembaruan sistem (`sudo apt update && sudo apt upgrade`) dan instal Apache Web Server (`sudo apt install apache2`).

Langkah 2: Instalasi dan Konfigurasi Webmin

Webmin digunakan untuk mempermudah manajemen server, termasuk konfigurasi SSL.

1. **Tambah Repository Webmin:** Tambahkan repository dan kunci GPG Webmin ke sistem Ubuntu Anda agar dapat melakukan instalasi.
2. **Instal Webmin:** Jalankan perintah `sudo apt install webmin` di terminal server.
3. **Buka Akses Firewall:** Izinkan koneksi ke port Webmin dengan perintah `sudo ufw allow 10000/tcp`.
4. **Akses Webmin:** Buka browser dan akses Webmin melalui `https://<IP-SERVER-ANDA>:10000`. Login menggunakan akun root atau sudo dari server Anda.

Langkah 3: Pembuatan dan Implementasi Sertifikat Self-Signed

Ini adalah inti dari proses pengamanan. Proses ini dilakukan sepenuhnya di dalam antarmuka Webmin.

1. Buat Certificate Authority (CA) Lokal:

- Di dashboard Webmin, navigasi ke menu **Webmin > Webmin Configuration**.
- Pilih **Certificate Authority**.
- Isi detail untuk CA baru Anda (misalnya, nama negara, nama domain lokal Anda seperti `zeins.local`) lalu klik "Create new CA certificate".

2. Aktifkan SSL pada Apache:

- Kembali ke dashboard utama, navigasi ke **Servers > Apache Webserver**.
- Pilih tab **Existing virtual hosts** dan klik pada *virtual host* yang ingin Anda amankan.
- Pilih tab **SSL Options**.
- Centang **Enable SSL?**, lalu pilih sertifikat yang baru saja Anda buat dari daftar.
- Simpan dan terapkan perubahan. Webmin akan secara otomatis me-restart Apache.

Langkah 4: Menambahkan Sertifikat ke Client (Browser)

Agar browser di mesin *client* (misalnya Windows) tidak menampilkan peringatan keamanan, Anda perlu membuatnya "mempercayai" sertifikat yang telah Anda buat.

1. **Unduh Sertifikat CA:** Kembali ke menu **Webmin > Webmin Configuration > Certificate Authority**. Unduh file sertifikat CA yang telah Anda buat ke komputer *client*.
2. **Impor Sertifikat di Browser:**

- Buka pengaturan browser di komputer *client* (misalnya Chrome atau Edge).
- Cari menu **Privacy and security**, lalu pilih **Manage certificates**.
- Pilih tab **Trusted Root Certification Authorities** dan klik tombol **Import**.
- Pilih file sertifikat CA yang telah Anda unduh sebelumnya dan selesaikan proses impor.

3. **Restart Browser:** Tutup dan buka kembali browser Anda.

Verifikasi dan Hasil Akhir

Setelah semua langkah selesai, akses web server Anda menggunakan HTTPS (contoh: <https://zeins.local>). Browser sekarang seharusnya menampilkan ikon gembok terkunci tanpa ada peringatan keamanan, yang menandakan komunikasi antara browser Anda dan server lokal telah berhasil dienkripsi dan aman.