PROPOSAL PROYEK

“MEMBANGUN WEB SERVER BERBASIS LINUX (APACHE/NGINX+SSL)”

Disusun untuk memenuhi tugas mata kuliah Sistem Operasi

Dosen : Ferdi Cahyadi, S.Kom., M.Cs.

Disusun Oleh :

Kelompok 5

Siti Melka Rehngenana (2401020132)

Fitri Arfiana (2401020135)

Aisyah Nazwa Ramadhani (2401020136)

Christine Simbolon (2401020158)

Salsadilla Frisca Anjani (2401020164)

PRODI TEKNIK INFORMATIKA

FAKULTAS TEKNIK DAN TEKNOLOGI KEMARITIMAN

UNIVERSITAS MARITIM RAJA ALI HAJI

T.A 2024/2025

DAFTAR ISI

BAB I

PENDAHULUAN

1.1 LATAR BELAKANG

Perkembangan teknologi informasi mendorong kebutuhan akan layanan web yang stabil, cepat, dan aman. Web server menjadi bagian penting dalam infrastruktur jaringan karena berfungsi untuk menerima permintaan dari pengguna dan menyajikan konten melalui protokol HTTP. Namun, penggunaan HTTP yang tidak terenkripsi dapat menimbulkan berbagai risiko keamanan seperti penyadapan data (data sniffing) dan akses tidak sah terhadap informasi sensitif.

Untuk mengatasi risiko tersebut, diperlukan penggunaan protokol HTTPS dengan sertifikat SSL guna memastikan komunikasi antara klien dan server berlangsung secara terenkripsi. Selain itu, pengamanan jaringan melalui Firewall juga menjadi langkah penting untuk membatasi akses hanya pada port dan layanan yang diperlukan. Dengan cara ini, potensi serangan dari luar dapat diminimalkan.

Linux merupakan sistem operasi yang banyak digunakan pada server karena kestabilan, keamanan, dan fleksibilitasnya. Oleh karena itu, pembangunan web server berbasis Linux menjadi kesempatan yang baik bagi pemula untuk mempelajari manajemen sistem operasi, konfigurasi layanan jaringan, serta langkah-langkah pengamanan tingkat dasar. Melalui proyek ini, dilakukan instalasi dan konfigurasi web server Apache, penerapan SSL/HTTPS, serta pengaturan Firewall sebagai bentuk hardening. Proyek ini diharapkan dapat memberikan pemahaman praktis mengenai cara membangun layanan web yang aman dan dapat diandalkan.

1.2 RUMUSAN MASALAH

Rumusan masalah dalam proyek ini adalah sebagai berikut :

1. Bagaimana cara melakukan instalasi dan konfigurasi web server Apache pada sistem operasi Linux?
2. Bagaimana cara mengamankan transmisi data menggunakan protokol SSL/HTTPS dengan sertifikat self-signed?
3. Bagaimana menerapkan aturan Firewall (UFW/Iptables) untuk meningkatkan keamanan dan membatasi akses ke server?

1.3 TUJUAN PROYEK

Tujuan yang ingin dicapai melalui proyek ini meliputi :

1. Memahami implementasi layanan web yang aman pada sistem operasi Linux.
2. Mampu melakukan konfigurasi Virtual Host untuk mengelola domain lokal.
3. Mampu menerapkan teknik hardening dasar menggunakan Firewall (UFW/Iptables) dan sertifikat SSL.
4. Menghasilkan dokumentasi teknis mengenai proses instalasi, konfigurasi, dan pengamanan web server.

1.4 BATASAN MASALAH

Batasan masalah pada proyek ini adalah sebagai berikut :

1. Sistem operasi yang digunakan: Ubuntu Server 22.04 LTS.
2. Web server yang digunakan: Apache.
3. Jenis SSL yang digunakan: Self-signed Certificate.
4. Lingkungan implementasi menggunakan Virtual Machine (VirtualBox).
5. Pengujian layanan dilakukan pada jaringan lokal.

BAB II

LANDASAN TEORI

2.1 SISTEM OPERASI LINUX

Linux merupakan sistem operasi open source yang berbasis Unix dan banyak digunakan pada lingkungan server karena stabil, aman, dan memiliki fleksibilitas tinggi. Linux terdiri dari berbagai distribusi (distro) seperti Ubuntu, Debian, CentOS, Fedora, dan lainnya.

Pada proyek ini digunakan Ubuntu Server, salah satu distro Linux yang populer untuk kebutuhan server. Ubuntu dipilih karena memiliki :

- Komunitas besar dan dokumentasi lengkap.
- Pembaruan keamanan rutin.
- Kemudahan instalasi dan konfigurasi.
- Dukungan paket yang luas, termasuk Apache, Nginx, UFW, dan OpenSSL.

Server sering digunakan sebagai sistem operasi dasar untuk web server, database server, dan berbagai aplikasi jaringan lain.

2.2 WEB SERVER APACHE

Apache HTTP Server adalah web server open source yang dikembangkan oleh Apache Software Foundation. Apache menjadi salah satu web server paling banyak digunakan karena stabil, fleksibel, dan mendukung banyak modul tambahan.

Beberapa kelebihan Apache antara lain :

- Stabil dan handal dalam menangani lalu lintas tinggi.
- Mendukung modul seperti PHP, SSL/TLS, mod_rewrite, dan mod_security.
- Konfigurasi fleksibel melalui file virtual host.
- Komunitas besar, sehingga banyak tutorial dan solusi.
- Bersifat multiplatform, terutama optimal di Linux.

Dalam proyek ini Apache digunakan untuk:

1. Menyajikan halaman web melalui HTTP dan HTTPS.
2. Mengkonfigurasi virtual host.
3. Mengaktifkan modul SSL untuk keamanan.

2.3 SECURE SOCKET LAYER (SSL/HTTPS)

Secure Socket Layer (SSL) atau versi modernnya TLS (Transport Layer Security) adalah protokol keamanan yang mengenkripsi data antara klien dan server. Dengan SSL/TLS, data seperti username, password, atau informasi sensitif tidak dapat dibaca pihak ketiga.

Perbedaan HTTP dan HTTPS :

HTTP	HTTPS
Tidak terenkripsi	Terenkripsi dengan SSL/TLS
Rentan disadap (sniffing)	Aman dari penyadapan
Tidak memiliki sertifikat	Memerlukan sertifikat (CA/Let's Encrypt/self-signed)
Cocok untuk konten biasa	Wajib untuk login, transaksi, dan data sensitif

Dalam proyek ini digunakan SSL dari Let's Encrypt atau self-signed certificate untuk mengamankan koneksi ke web server.

2.4 FIREWALL (UFW/Iptables)

Firewall adalah mekanisme keamanan jaringan yang mengatur lalu lintas data masuk dan keluar. Firewall menentukan port mana yang boleh diakses dan mana yang harus diblok.

1. UFW (Uncomplicated Firewall)

   UFW adalah firewall bawaan Ubuntu yang dirancang mudah digunakan.

   Fungsinya antara lain :

   - Mengizinkan atau memblokir port tertentu.
   - Melihat status dan aturan firewall dengan mudah.
   - Melindungi server dari akses tidak sah.

   Contoh aturan : ufw allow 80 → membuka port HTTP
   ufw allow 443 → membuka port HTTPS
   ufw enable → mengaktifkan firewall

2. Iptables

   Iptables adalah firewall tingkat lanjut yang memberi kontrol detail terhadap paket jaringan.

   Keunggulan :

   - Bisa membuat aturan kompleks.
   - Mengontrol chain INPUT, OUTPUT, FORWARD.
   - Lebih fleksibel dibanding UFW.

BAB III

METODOLOGI PELAKSANAAN

3.1 ALAT DAN BAHAN

Untuk mendukung keberhasilan proyek ini, berikut perangkat keras dan perangkat lunak yang digunakan :

- Hardware : Laptop dengan spesifikasi RAM 16.0GB, Processor AMD Ryzen 7 7435HS.
- Software : Oracle VirtualBox (sebagai wadah virtualisasi), Sistem Operasi Ubuntu Server 22.04 LTS, Apache Web Server, OpenSSL.

3.2 PEMBAGIAN TUGAS DAN TANGGUNGJAWAB

Agar pengerjaan proyek berjalan efektif, tugas dibagi kepada lima anggota tim dengan rincian sebagai berikut :

1. Anggota Pertama

   Tugas Anggota Pertama adalah sebagau berikut :

   - Bertanggung jawab menyusun Proposal dan Laporan Akhir.
   - Mendokumentasikan setiap langkah pengerjaan, seperti Screenshoot hasil.
   - Menyusun materi Slide Presentasi untuk minggu ke-15.

2. Anggota Kedua

   Tugas Anggota Kedua adalah sebagai berikut :

   - Melakukan instalasi Sistem Operasi Ubuntu Server di Virtual Machine.
   - Melakukan konfigurasi jaringan dasar (IP Address statis/dinamis).
   - Melakukan update repository dan manajemen user Linux.

3. Anggota Ketiga

   Tugas Anggota ketiga adalah sebagai berikut :

   - Melakukan instalasi paket apache2.
   - Membuat halaman web statis (index.html) profil kelompok.
   - Melakukan konfigurasi Virtual Host agar web bisa diakses dengan domain lokal (kelompok.local).

4. Anggota Keempat

   Tugas Anggota keempat adalah sebagai berikut :

   - Melakukan instalasi modul SSL.

- Membuat sertifikat keamanan (Self-Signed Certificate) menggunakan OpenSSL.
- Mengkonfigurasi Apache agar berjalan di port 443 (HTTPS) dan redirect otomatis.

5. Anggota Kelima

   Tugas Anggota Kelima adalah sebagai berikut :

   - Melakukan instalasi dan konfigurasi Firewall (UFW).
   - Memastikan hanya port 22 (SSH), 80 (HTTP), dan 443 (HTTPS) yang terbuka.
   - Melakukan pengujian akses (Connectivity Test) dari komputer host (Windows) ke Server.

3.3 RENCANA PENGERJAAN (TIMELINE)

Berikut adalah jadwal pelaksanaan proyek yang disusun berdasarkan mingguan :

Minggu ke-	Kegiatan	Penanggungjawab
11	Penyusunan dan Pengajuan Proposal Proyek.	Anggota 1
12	1. Instalasi Linux server & Setup Jaringan. 2. Instalasi Apache Web server dasar. 3. Pembuatan SSL Certificate.	Anggota 2 dan 3
13	1. Konfigurasi Virtual Host (Domain lokal). 2. Implementasi HTTPS & Redirect SSL.	Anggota 3 dan 4
14	1. Konvigurasi Keamanan Firewall. 2. Pengujian Akses.	Anggota 5
15	Finalisasi Laporan Akhir dan Pembuatan PPT.	Anggota 1

BAB IV

TARGET LUARAN

Sesuai dengan panduan proyek Sistem Operasi (Advanced Project), target luaran yang akan dicapai dari Proyek Membangun Web Server Berbasis Linux (Apache/Nginx + SSL) adalah sebagai berikut :

4.1 SERVER WEB YANG BERJALAN STABIL (HTTP & HTTPS)

Server web dapat berjalan dengan protokol HTTP pada port 80 dan HTTPS pada port 443. Server harus dapat diakses secara konsisten dan memiliki service yang otomatis berjalan saat sistem boot.

Kriteria keberhasilan :

- Web server dapat diakses via http:// dan https://
- Status service "active (running)" pada systemctl
- Uptime minimal 99% selama periode testing

4.2 KONFIGURASI VIRTUAL HOST

Implementasi minimal 1 virtual host dengan domain lokal yang memungkinkan akses menggunakan nama domain (contoh: mywebsite.local) dengan konfigurasi DocumentRoot, ServerName, dan log file yang terpisah.

Kriteria keberhasilan :

- Website dapat diakses dengan nama domain lokal
- Dapat diakses dengan dan tanpa prefix "www"
- Log file mencatat aktivitas dengan benar

4.3 ATURAN FIREWALL YANG AKTIF

Implementasi firewall yang hanya membuka port-port yang diperlukan untuk keamanan server :

1. Port 22 (SSH) : Remote access dan administrasi
2. Port 80 (HTTP) : Layanan web standar
3. Port 443 (HTTPS) : Layanan web dengan enkripsi
4. Port lainnya : Tertutup (blocked)

Kriteria keberhasilan :

- Firewall aktif dan enabled pada boot
- Hanya port 22, 80, dan 443 yang dapat diakses
- Aturan persisten setelah reboot