|  |  |  |  |
| --- | --- | --- | --- |
| C:\Users\Nabila Elshanum\Downloads\kad.jpg | **Tugas 6**  **Pemrograman Jaringan (CSH4V3)**  **------------------------------**  **Semester Genap 2018 - 2019**  **Dosen: Aulia Arif Wardana, S.Kom., M.T. (UIW)** | | |
| ***Berdo’alah sebelum mengerjakan. Dilarang berbuat curang.***  ***Tugas ini untuk mengukur kemampuan anda, jadi kerjakan dengan sepenuh hati.***  ***Selamat belajar, semoga sukses !*** | | | |
| **Nama Mahasiswa:**  **Taufik Rahmat Kurniawan** | | **NIM:**  **1301178601** | **Nilai:**  **……………………** |
| **Nama Mahasiswa:** | | **NIM:** | **Nilai:**  **……………………** |
| **Nama Mahasiswa:** | | **NIM:** | **Nilai:**  **……………………** |

|  |
| --- |
| **Siapkan tools berikut sebelum mengerjakan:** |
| 1. Go Programming Language (<https://golang.org/dl/>). 2. Visual Studio Code (<https://code.visualstudio.com/>) atau LiteIDE (<https://github.com/visualfc/liteide>). 3. Disarankan untuk menggunakan linux dengan distro fedora (<https://getfedora.org/id/workstation/>). 4. Buatlah git repository pada <https://github.com/> kemudian push semua kode dan hasil laporan anda ke dalam repository github yang sudah anda buat. Kumpulkan link repository github tersebut sebagai tanda bahwa anda mengerjakan tugas modul ini. 5. Buatlah Virtual Machine (VM) dengan virtualbox (<https://www.virtualbox.org/wiki/Downloads>). Gunakan operating system Centos (<https://www.centos.org/>) pada VM tersebut. VM yang sudah anda buat akan digunakan sebagai server. 6. Gunakan openssl (<https://www.openssl.org/>) untuk mengerjakan salah satu tugas pada modul ini. |

|  |
| --- |
| **Soal No 1 (Secure Web Server Design)** |
| Buatlah perancangan aplikasi Web Server yang dapat melakukan serve koneksi HTTPS menggunakan diagram FSM serta jelaskan cara kerjanya! |
| Jawaban:  Response request data  Response HTTP  Request data  Request HTTP  Cara kerja : sesuai dengan FSM yang telah dibuat kondisi awal browser akan meminta request dengan format Hyper Text Transfer Protocol (HTTP) kepada web server dan kemudian web server akan meneruskan request tersebut kepada data server untuk mencari data yang diinginkan dan sesuai setelah itu, data server akan mengirimkan respon yang akan dikirimkan terlebih dahulu ke web server sebelum diteruskan kembali ke browser. Hubungan antara web server dengan browser merupakan client-side sedangkan hubungan antara data server dengan web sever adalah server-side  Referensi : artikelteknologi.com   1. Browser mengunjungi suatu halaman website yang menggunakan SSL. 2. Secara bersamaan browser komputer client meminta komputer server memberikan identitas SSL website untuk memvalidasi status keamanan website tersebut. 3. Komputer server mengirim duplikat dari sertifikat SSL yang dimilikinya. 4. Browser komputer client memeriksa kebenaran sertifikat SSL yang dimiliki website tersebut. Jika benar, browser akan mengirim permintaan untuk melakukan koneksi terenskripsi kepada server. 5. Komputer server mengirim anak kunci berupa tanda tangan digital untuk melakukan melakukan transfer data dengan komputer client dengan identitas khusus (Private Key) yang hanya bisa digunakan komputer client tersebut. Anak kunci digital ini digunakan oleh browser membuka informasi yang diminta dari website tersebut serta mengamankan data yang dikirim ke website tersebut, karena setiap data yang dialirkan akan dibungkus oleh sistem SSL dengan identitas khusus. 6. Koneksi terenskripsi dapat dilakukan dan browser komputer client menampilkan status “Connection is secure”. Untuk memberi tahu pengguna bahwa website tersebut aman untuk melindungi datanya.   Referensi : mazayad github |

|  |
| --- |
| **Soal No 2 (Web Server Implementation)** |
| Implementasikan aplikasi secure web server dari design yang sudah anda buat, aplikasi harus mempunyai config file untuk melakukan konfigurasi aplikasi!  Anda bisa mengembangkan dari code berikut <https://github.com/aulwardana/simpe-web-server> |
| Jawaban: **HTTPS** HTTPS, Hyper Text Transfer Protocol Secure, adalah ekstensi dari HTTP yang berguna untuk pengamanan komunikasi lewat internet. Data atau informasi yang dikomunikasikan di-enkripsi menggunakan TLS. **TLS** TLS, Transport Layer Security, adalah versi yang lebih update dari SSL. **SSL** SSL, Secure Sockets Layer, adalah standar untuk pengamanan komunikasi lewat internet. Data atau informasi yang sedang dikomunikasikan dari sebuah system ke system lain akan di-proteksi, dengan cara adalah mengacak informasi tersebut menggunakan algoritma enkripsi. **HTML** HTML (HyperText Markup Language) adalah bahasa pemrograman standar yang digunakan untuk membuat sebuah halaman web, yang kemudian dapat diakses untuk menampilkan berbagai informasi di dalam sebuah penjelajah web Internet (Browser). Fungsi html yang pertama adalah untuk membuat suatu halaman website yang dapat dibaca dan dipahami oleh pengguna dengan lebih mudah. Lalu, menandai teks pada suatu laman. **HTTP** HTTP (Hypertext Transfer Protocol) merupakan istilah yang diberikan pada sebuah protokol dan dipergunakan untuk mengirimkan dokumen dari WWW (World Wide Web). HTTP dapat pula diartikan sebagai protokol jaringan untuk pendistribusian sistem informasi hypermedia secara kolaboratif. Fungsi utama dari protokol HTTP sebenarnya cukup sederhana, yaitu untuk mengkomunikasikan satu komputer dengan lainnya.Selain itu, HTTP juga berfungsi untuk menentukan bagaimana sebuah data atau pesan dapat ditransmisikan maupun diformat menjadi bentuk yang dapat merespon browser untuk menampilkan data-data tersebut.  Cara Kerja HTTP:   1. Pertama-tama, komputer klien (HTTP klien) membuat sambungan, lalu mengirimkan permintaan dokumen ke web server. 2. HTTP server kemudian memproses permintaan klien, sementara itu, HTTP klien menunggu respon dari server (berupa HTML) tersebut. 3. Web server merespon permintaan dengan kode status data, lalu barulah menutup sambungan ketika telah selesai memproses permintaan.     Implementation |