|  |  |  |  |
| --- | --- | --- | --- |
| 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:**  **Ahmad Fathan Afdhali**  **……………………………..................................................** | | **NIM:**  **1301164220**  **…………………….............................** | **Nilai:**  **……………………** |
| **Nama Mahasiswa:**  **Yudi Kurniawan**  **……………………………..................................................** | | **NIM:**  **1301154143**  **…………………….............................** | **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:  Request Key/HTTPS  Request SSL/Data  Response Key/HTTPS  Response SSL/Data  Cara Kerja :  Browser akan meminta request SSL berupa key Hyper Text Transfer Protocol Secure (HTTPS) kepada web server yang akan meneruskan request tersebut untuk autentifikasi.  Lalu pada server untuk mencari key yang dapat berupa public key dan private key yang di request oleh pengguna, setelah itu server akan mengirimkan data response yang akan dikirimkan ke pengguna dengan dilakukan (decryption) yaitu menguraikan kembali "kode" rahasia yang sudah didapat, sebelum dikirim kembali response kepada browser. Hubungan antara web server dengan browser merupakan client-side sedangkan hubungan antara data server dengan web sever adalah server-side |

|  |
| --- |
| **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: |