

Nama : Baiquni Krisna Adyarta

NIM : 105221037

SOAL

1. Apa itu HTTP (Hypertext Transfer Protocol) dan bagaimana cara kerjanya dalam komunikasi web?
2. Apa perbedaan utama antara HTTP dan HTTPS (Hypertext Transfer Protocol Secure), dan mengapa HTTPS lebih aman?
3. Bagaimana DNS (Domain Name System) berperan dalam penggunaan internet, dan mengapa penting untuk mengonfigurasi DNS dengan benar?
4. Apa fungsi utama dari sebuah server dalam konteks teknologi informasi, dan bagaimana server berinteraksi dengan permintaan dari klien?
5. Bagaimana protokol HTTP digunakan dalam konteks server? Jelaskan aliran komunikasi antara klien dan server ketika mengakses sebuah situs web.
6. Mengapa enkripsi data sangat penting dalam HTTPS dan bagaimana SSL/TLS (Secure Sockets Layer/Transport Layer Security) berperan dalam mengamankan koneksi web?
7. Bagaimana DNS meresolusi nama domain menjadi alamat IP, dan mengapa proses ini penting dalam navigasi web?
8. Apa peran DNS server dan recursive DNS server dalam proses resolusi nama domain?
9. Apa yang dimaksud dengan server fisik dan server virtual, dan apa kelebihan serta kekurangannya masing-masing?
10. Bagaimana arsitektur klien-server berperan dalam distribusi tugas dan sumber daya dalam sebuah jaringan komputer?

JAWABAN

1. protokol komunikasi yang digunakan untuk mengirim dan menerima data. Cara kerjanya adalah dimulai ketika seorang user memasukkan URL (Uniform Resource Locator) atau mengklik tautan di browser mereka.
2. HTTP adalah protokol standar untuk komunikasi web, tetapi tidak menawarkan keamanan tambahan. Data yang dikirim melalui HTTP tidak dienkripsi, yang berarti dapat dengan mudah dibaca oleh pihak ketiga yang dapat mengintip lalu lintas internet. Sedangkan HTTPS adalah versi aman dari HTTP. Ini menggunakan lapisan keamanan tambahan yang disebut SSL/TLS (Secure Sockets Layer/Transport Layer Security) untuk mengenkripsi data yang dikirim antara server web dan klien web.

3. DNS sangat penting dalam penggunaan internet karena berperan sebagai "buku telepon" internet. Ini menghubungkan alamat IP numerik (yang digunakan oleh komputer untuk mengidentifikasi satu sama lain di jaringan) dengan nama domain yang lebih mudah diingat oleh manusia.

DNS dapat Menerjemahkan Nama Domain ke Alamat IP.

Konfigurasi DNS yang buruk atau tidak aman dapat memungkinkan serangan seperti serangan cache poisoning atau man-in-the-middle attacks, yang dapat merusak integritas dan kerahasiaan data.

4. Fungsi utama dari server adalah akan melayani segala permintaan dari klien untuk diproses. Baik itu permintaan data atau aplikasi untuk dijalankan oleh klien.

Klien (seperti komputer pengguna atau perangkat) membuat permintaan ke server. Permintaan ini dapat berupa permintaan untuk halaman web, pengiriman email, mengambil data dari basis data, atau layanan lainnya.

5. HTTP digunakan dalam konteks server sebagai cara untuk mengelola komunikasi antara klien (biasanya seorang pengguna dengan perangkat seperti browser web) dan server web yang menyimpan dan mengelola situs web atau aplikasi web.

6. Enkripsi data sangat penting dalam HTTPS karena itu adalah salah satu cara terpenting untuk melindungi kerahasiaan dan integritas data saat berkomunikasi melalui internet.

HTTPS menggunakan protokol SSL/TLS untuk mengenkripsi data yang dikirim antara klien (seperti browser web pengguna) dan server web.

Untuk Kerahasiaan Data, Integritas Data, dan Autentikasi Server.

7. DNS meresolusi nama domain menjadi alamat IP dengan menggunakan hierarki sistem yang terdiri dari berbagai komponen, seperti server DNS dan catatan DNS.

Untuk Skalabilitas, Pembaruan Alamat IP, dan Lokalitas Geografis.

8. DNS server adalah server yang bertanggung jawab untuk menyimpan catatan DNS yang merujuk ke alamat IP yang sesuai dengan nama domain tertentu. Setiap situs web atau layanan internet biasanya memiliki setidaknya satu DNS server otoritatif yang mengelola catatan DNS untuk domain mereka.