PERBEDAAN 3 WEB SERVICES

DAN RESUME SUMMARY MODUL 1 APNIC

DI SUSUN OLEH :

Nadya Indah Trisnawati

3122640034

PROGRAM STUDI TEKNIK INFORMATIKA

DEPARTEMEN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

1. PERBEDAAN 3 WEB SERVICES YAITU APACHE, NGINX DAN IIS.

Apache, Nginx, dan IIS (Internet Information Services) adalah tiga jenis web server yang berbeda. Meskipun ketiganya berfungsi sebagai server web, namun ada beberapa perbedaan utama di antara mereka:

1. Apache

Apache adalah salah satu web server open-source yang paling populer dan umum digunakan. Apache didukung oleh banyak sistem operasi, termasuk Linux, UNIX, dan Windows. Apache juga memiliki fleksibilitas yang tinggi dan sangat mudah dikonfigurasi, sehingga sering menjadi pilihan utama bagi pengembang web.

2. Nginx

Nginx juga merupakan web server open-source yang populer. Nginx lebih dikenal karena kinerjanya yang sangat cepat dan ringan, serta kemampuannya untuk menangani jumlah permintaan yang sangat besar secara bersamaan. Nginx lebih cocok untuk digunakan dalam pengembangan aplikasi web modern yang berbasis mikroserfis.

3. IIS

IIS adalah web server yang dikembangkan oleh Microsoft untuk digunakan pada sistem operasi Windows. IIS memiliki beberapa kelebihan, termasuk integrasi yang kuat dengan teknologi Microsoft, seperti ASP.NET, dan kemampuan untuk melakukan manajemen dan administrasi server yang mudah dan terintegrasi.

Secara umum, perbedaan utama di antara ketiga web server ini terletak pada platform yang digunakan (Apache dan Nginx multi-platform, sedangkan IIS hanya tersedia di platform Windows), kinerja (Nginx lebih cepat daripada Apache), dan fitur dan integrasi (IIS terintegrasi dengan teknologi Microsoft). Pemilihan web server tergantung pada kebutuhan pengguna dan karakteristik proyek web yang sedang dikembangkan

2. RESUME SUMMARY MODUL 1 CYBER SECURITY FUNDAMENTAL

1. Sistem Indenpendencies
   Internet memiliki banyak sistem yang umumnya dapat bekerja dengan menggunakan sebuah protocol yang dapat menjelaskan bagaimana sistem dan jaringan yang berbeda namun dapat bekerja sama saling berbagi informasi.
2. Nilai Dari Sebuah Data dan Informasi
   Yang dimaksud nilai dari sebuah data informasi disini adalah data yang diantaranya adalah laporan internal, informasi costumer, design produk atau resep rahasia pada suatu produk. Beberapa ancaman dari sebuah data dan informasi adalah akses tidak sah, modifikasi data yang tidak sah dan juga hilangnya suatu informasi.
3. Pentingnya Mengamankan Sebuah Data
   Data dan informasi terbagi menjadi 2 state, yaitu :
   a. **Data Istirahat**
      Merupakan data yang sedang dalam keadaan yang tidak aktif dan disimpan dalam database, data warehouse, spreadsheet atau yang lainnya.
   b. **Data Bergerak**
      Merupakan data yang sedang melewati sebuah jaringan atau tinggal sebentar pada memori computer yang berguna untuk dilihat dan diperbarui.
4. Tujuan utama keamanan informasi adalah menjaga kerahasiaan, integritas dan ketersediaan (CIA) pada sebuah asset dan sistem.

   a. **Kerahasiaan**
      Setiap organisasi berusaha melindungi data dan informasinya dari pengungkapan kepada pihak-pihak yang tidak berwenang.
   b. **Integritas**
      Sistem dimaksudkan untuk selalu siap menyediakan data dan informasi bagi mereka yang berwenang untuk menggunakannya. Tujuan ini penting khususnya bagi sistem yang berorientasi informasi seperti SIM, DSS dan sistem pakar (ES).
   c. **Ketersediaan**
      Semua sistem dan subsistem yang dibangun harus mampu memberikan gambaran yang lengkap dan akurat dari sistem fisik yang diwakilinya.
5. Pada konteks pengamanan sebuah informasi terdapat 3 macam :

a. **Ancaman**
   Memiliki potensi untuk memberikan dampak yang tidak di inginkan pada sebuah sistem organisasi, ancaman tersebut dapat terjadi yang disebabkan oleh ancaman alami, lingkungan dan ancaman dari manusia.
b. **Kerentanan**
   Merupakan kekurangan pada keamanan prosedur sistem, design, pengimplementasian dan control dari dalam yang dapat mengakibatkan pelanggaran keamanan pada peraturan keamanan sistem.
c. **Resiko**
   Hasil yang didapat dari kegiatan ancaman dan memberikan dampak pada organisasi.

6. Kontrol Security (digunakan organisasi untuk melindungi asset informasi dan juga untuk mengurangi dampak resiko)
   Kontrol security dibagi menjadi 3 :

a. **Peraturan atau Prosedur**
   Dibuat untuk memberikan kesadaran pada semua orang akan pentingnya keamanan, tanggung jawab dan juga melihat cakupan dari masalah yang di alami.
b. **Technical**
   Digunakan untuk pencegahan dan mendeteksi adanya potensi serangan, serta mengurangi dampak resiko pada jaringan.
c. **Physical**
   Digunakan untuk mencegah pencurian informasi fisik dan akses yang tidak sah.

7. Prinsip keamanan
   Terdapat 2 prinsip keamanan yaitu :

a. **Principle of Weakest Link**
   Adalah penyerang akan mencari cara yang paling mudah untuk melakukan penyerangan
b. **Principle of Least Privilage**
   Adalah entitas (manusia, program atau sistem) harus dapat mampu mengakses informasi atau sumber daya yang dibutuhkan oleh bisnisnya.