KEAMANAN JARINGAN

“RESUM MODUL 1 APANIC, NILAI KUIS APANIC DAN PERBEDAN NGINX DAN APACHE”

Nama : akhmad mufti ali wafa

Kelas : 1 D4 LJ Teknik Informatika

DEPARTEMEN TEKKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

Cyber security

Interdependensi Sistem

Internet adalah sebuah desa global yang besar, namun terdiri dari banyak sistem dan jaringan yang terpisah. Protokol umum digunakan untuk memungkinkan kerja sama dan pertukaran informasi antara sistem atau jaringan yang berbeda. Namun, ketergantungan ini dapat menimbulkan risiko ketika terjadi masalah seperti :

1. Efficiency
2. Reliability
3. Security

Nilai Data dan Informasi

Data dan informasi sangat berharga bagi organisasi karena dianggap sebagai aset bisnis. Data dan informasi ini dapat membantu organisasi dalam membuat keputusan yang tepat dan mengambil tindakan yang diperlukan untuk mencapai tujuan bisnis mereka. Dengan demikian, pengelolaan data dan informasi yang efektif menjadi sangat penting bagi kesuksesan organisasi.

Data dan informasi

- Laporan intern
- Informasi penguna
- Data transaksi
- Desain produk atau resep rahasia

Resiko data dan infromasi

- Modifikasi tanpa izin
- Kehilangan informasi
- Akses tidak sah

Kebutuhan untuk Mengamankan Informasi

Data dan informasi dapat berada di banyak keadaan - diam, digunakan atau bergerak.

a) **Data at rest**
   Data tidak aktif disimpan secara fisik di database, gudang data, spreadsheet. arsip, kaset cadangan di luar situs, dll.
b) **Data in motion**
   Data yang melintasi jaringan atau sementara berada di memori komputer untuk dibaca atau diperbarui.

Tujuan Utama Keamanan informasi adalah menjaga kerahasiaan integritas, dan ketersediaan (CIA) asset dan system informasi

1. Kerahasiaan
2. Intergritas
3. Ketersediaan

Ancaman, Kerentanan dan Risiko

Dimensi lain yang harus kita pahami adalah hubungan Ancaman, Kerentanan, Risiko dengan konteks melindungi aset informasi kita.

Ancaman (Threat)

Ancaman adalah penyebab potensial dari dampak yang tidak diinginkan pada sistem atau organisasi. Ada beberapa kategori ancaman seperti ancaman alam, ancaman manusia dan ancaman lingkungan.

Sumber Ancaman adalah:

1 Disengaja; atau

2. Kebetulan

kerentanan(Vulnerability)

Kerentanan adalah cacat atau kelemahan dalam prosedur keamanan sistem, desain, implementasi, atau kontrol internal yang dapat dilakukan (dipicu secara tidak sengaja atau dieksploitasi secara sengaja) dan mengakibatkan pelanggaran keamanan atau pelanggaran kebijakan keamanan sistem.

Resiko (Risk)

Risiko adalah kemungkinan sumber ancaman tertentu menggunakan kerentanan potensial, dan dampak yang dihasilkan dari kejadian buruk tersebut pada organisasi.

Kontrol Keamanan

Kontrol adalah penanggulangan yang dilakukan organisasi untuk melindungi aset informasi. Kontrol keamanan mengurangi risiko.

Kebijakan dan prosedur

Contoh control :

- Cyber security policy
- Incident handling procedure

Teknik

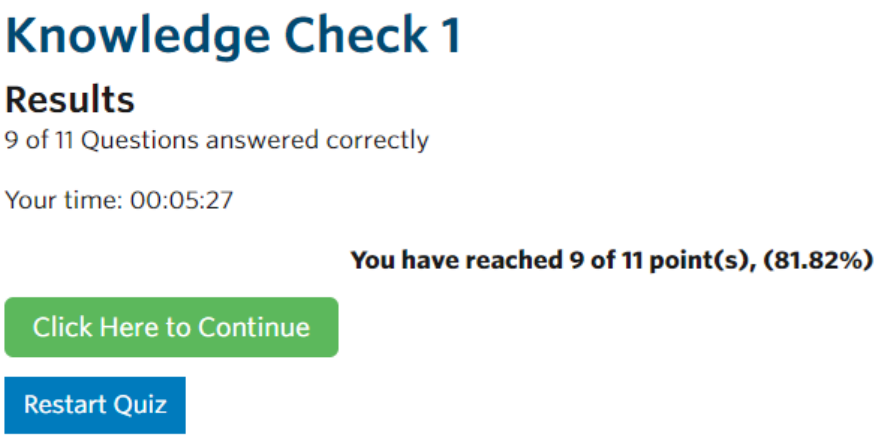
Contoh control :

- Fire wall
- Intrusion detection system
- Anti virus software

Physical

- CCTV
- Locks
- Secure working space

Hasil :



Perbedaan NginX dan Apache

Nginx dan Apache adalah dua server web populer yang digunakan untuk melayani konten web di internet. Berikut adalah perbedaan utama antara Nginx dan Apache:

1. Arsitektur: Nginx dikembangkan dengan desain yang lebih ringan dan modular, sedangkan Apache dikembangkan dengan desain yang lebih monolitik dan modularitas yang lebih rendah.
2. Kinerja: Nginx terkenal akan performa yang cepat dan efisien, terutama dalam menangani banyak permintaan secara bersamaan. Apache, di sisi lain, lebih cocok untuk memproses permintaan yang lebih sedikit dan lebih kompleks.

3. Konfigurasi: Apache menggunakan file konfigurasi berbasis teks yang mudah dibaca dan diubah oleh manusia. Nginx menggunakan sintaks konfigurasi yang sedikit lebih sulit dipahami, namun dapat diatur secara programatik.
4. Ketersediaan: Nginx sering digunakan sebagai reverse proxy, yang memungkinkan server web lainnya (termasuk Apache) untuk berjalan di belakangnya dan memanfaatkan kemampuan caching dan penanganan beban kerja yang efisien. Apache juga dapat berfungsi sebagai reverse proxy, tetapi lebih banyak digunakan sebagai server web utama.
5. Ekosistem: Apache telah menjadi server web yang dominan dalam beberapa dekade, sehingga memiliki ekosistem pengguna dan plugin yang luas. Nginx juga memiliki plugin dan modul yang berguna, namun lebih sedikit dibandingkan Apache.
6. Keamanan: Nginx umumnya dianggap lebih aman karena memiliki desain yang lebih sederhana dan fokus pada kinerja. Apache memiliki lebih banyak fitur dan kompleksitas, sehingga potensi untuk rentan terhadap serangan keamanan lebih besar.

Secara keseluruhan, Nginx dan Apache masing-masing memiliki kelebihan dan kekurangan, tergantung pada kebutuhan penggunaan dan lingkungan server yang digunakan.