

**KEAMANAN JARINGAN  
(SUMMARY MODUL DAN PERBEDAAN APACHE WEB  
SERVER NGINX IIS)**



Fifin Nur Rahmawati  
Dosen : Dr. Ferry Astika Saputra ST, M.Sc  
3122640040  
D4 LJ-Teknik Informatika

**PROGRAM STUDI TEKNIK INFORMATIKA  
DEEPARTEMEN TEKNIK INFORMATIKA DAN KOMPUTER  
POLITEKNIK ELEKTRONIKA NEGERI SURABAYA  
2023/2024**

## Perbedaan Apache, Nginx, IIS

- **Apache HTTP Server** adalah perangkat lunak web server sumber terbuka dan gratis yang digunakan untuk melayani permintaan dari klien untuk mengakses halaman web atau file lainnya
- **NGINX** adalah perangkat lunak web server sumber terbuka yang dapat digunakan untuk memproses permintaan HTTP, TCP, dan UDP. NGINX dapat dikonfigurasi dengan file konfigurasi teks sederhana atau melalui antarmuka pengguna yang disediakan oleh pihak ketiga. NGINX juga dapat digunakan sebagai server proxy, load balancer, dan cache, sehingga membuatnya sangat fleksibel dan dapat dikustomisasi sesuai kebutuhan pengguna. Selain itu, NGINX juga dilengkapi dengan fitur-fitur keamanan seperti proteksi terhadap serangan DDoS dan serangan XSS (Cross-Site Scripting).
- **Microsoft IIS** adalah server web bawaan dari sistem operasi Windows Server. IIS dapat digunakan untuk menjalankan aplikasi web yang dibangun dengan teknologi Microsoft seperti ASP.NET.

Perbedaan	Apache	Nginx	IIS
<u>Penanganan Traffic</u>	<u>Menggunakan MPM untuk pemrosesan traffic. Ada 3 MPM dengan tingkatan efisiensi yang berbeda, diantaranya mpm_prefork, mpm_worker dan mpm_event</u>	<u>Menggunakan algoritma bersifat asinkrot, event-driven dan non blocking untuk pemrosesan traffic</u>	NginX lebih unggul dari Apache dari segi <i>penanganan</i> website dengan <i>traffic</i> yang tinggi.
<u>Pemrosesan Konten Dinamis</u>	<u>Memiliki modul untuk memproses konten dinamis, konfigurasinya mudah</u>	<u>Bergantung pada software tambahan untuk memproses konten dinamis. Harus menghubungkan dengan NGINX terlebih dahulu</u>	Seperti pada IIS 6.0, situs berisi semua konten, baik statis maupun dinamis, yang terkait dengan situs tersebut. Namun, setiap situs harus berisi setidaknya satu aplikasi, yang diberi nama aplikasi root
<u>Akses Konfigurasi tingkat direktori</u>	<u>Menggunakan file htaccess, memungkinkan kustomisasi server tanpa mengubah konfigurasi utama</u>	<u>Tidak menawarkan akses konfigurasi di tingkat direktori</u>	menggunakan jalur di dalam file Metabase untuk menentukan <i>tingkat konfigurasi</i> (layanan, <i>direktori</i> virtual, <i>direktori</i> fisik).
<u>Cara mencari File yang diminta Request</u>	<u>Mencari file yang diminta request melalui document tree</u>	<u>Meminta request dengan mengurai URL</u>	Fungsi pertama dari IIS adalah memproses permintaan data yang masuk dari klien ke server. Setelah itu IIS akan mengirimkan data dari server ke klien

			sesuai apa yang diminta.
<u>Kemampuan Caching</u>	<u>Menggunakan modul mod_cache atau Varnish</u>	<u>Melakukan caching menggunakan FastCGI dan mampu menangani lebih banyak request daripada Varnish milik apache</u>	Untuk lebih meningkatkan performa untuk aplikasi dinamis, cache output <i>IIS</i> memberi administrator <i>kemampuan</i> untuk menyimpan konten dinamis
Keamanan	Rentan terhadap serangan DDoS dan serangan web lainnya	Cukup aman terhadap serangan web, namun tetap rentan terhadap serangan DDoS	Cukup aman terhadap serangan web dan DDoS, namun memerlukan konfigurasi yang tepat

## **Summary Modul 1**

### A. System Interdependencies

Jaringan yang dapat digunakan untuk bekerja sama dengan penggunaan protocol bagaimana system tersebut dan jaringan .

Pengamanan sebuah data informasi , diantaranya :



- Data istirahat, → data yang sedang tidak aktif dan disimpan pada database,
- Data bergerak → data yang tertinggal pada memori computer untuk dibaca dan melakukan pembaruan .

## What are the Main Objectives of Security?

The main objectives of information security is the preservation of confidentiality, integrity, and availability (CIA) of information assets and systems.



CONFIDENTIALITY



INTEGRITY



AVAILABILITY

Tujuan utama keamanan informasi adalah menjaga kerahasiaan, integritas, dan ketersediaan(CIA) aset dan sistem informasi.



CONFIDENTIALITY

The property that information is not made available or disclosed to unauthorized individuals, entities, or processes

### Kerahasiaan

Informasi tidak tersedia atau dipublikasikan kepada individu, entitas, atau proses yang tidak berwenang. Contohnya adalah : Nama pengguna dan kata sandi (atau kredensial pengguna) untuk mengakses email web hanya boleh diketahui oleh pengguna. Isi komunikasi email hanya boleh tersedia bagi penerima yang dituju.



INTEGRITY

The property of safeguarding the accuracy and completeness of assets

### Integritas

Menjaga keakuratan dan kelengkapan aset. Contohnya adalah : Email yang diterima atau dikirim tidak diubah dari bentuk aslinya.



AVAILABILITY

The property of being accessible and usable on demand by an authorized entity without delay

### Ketersediaan

Dapat diakses dan digunakan sesuai permintaan oleh entitas yang berwenang tanpa penundaan.

Contohnya adalah : Karena komunikasi email sangat penting bagi perusahaan, layanan email ini harus tersedia setiap saat.

## **Ancaman, Kerentanan, dan Risiko**

**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 potensi untuk memberikan dampak yang tidak diinginkan pada sebuah system organisasi, ancaman dapat terjadi disebabkan oleh ancaman alami, ancaman lingkungan, dan ancaman dari manusia

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

**Risiko** adalah kemungkinan sumber ancaman tertentu menjalankan potensi kerentanan, dan dampak yang dihasilkan dari peristiwa buruk tersebut pada organisasi.

## **Security Controls**

**Security Controls** adalah tindakan pencegahan yang dilakukan organisasi untuk melindungi aset informasi. Security Controls juga dapat mengurangi risiko. Beberapa kategori Security Controls diantaranya adalah Policy and Procedures, Technical, dan Physical. Kontrol security dibagi menjadi 3 diantaranya, peraturan dan prosedur, technical, dan physical

**Policy and Procedures** → membuat semua orang sadar akan pentingnya keamanan, menentukan roles serta tanggung jawab, dan ruang lingkup masalah.



**Policy and Procedures**

**Examples of Controls:**

-  Cyber Security Policy
-  Incident Handling Procedure

**Purpose:**  
To make everyone aware of the importance of security, define roles and responsibilities, and scope of the problem.

**Technical** → mencegah dan mendeteksi potensi serangan, mengurangi risiko pelanggaran pada layer network atau system.



**Technical**

**Examples of Controls:**

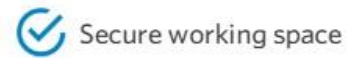
-  Firewall
-  Anti Virus Software
-  Intrusion Detection System

**Purpose:**  
To prevent and detect potential attacks, mitigate risk of breach at the network or system layer.

**Physical** → mencegah pencurian fisik aset informasi atau akses fisik yang tidak sah



Examples of Controls:



**Purpose:**

To prevent physical theft of information assets or unauthorized physical access.

## Prinsip Keamanan

Dua prinsip keamanan yang sangat berguna yaitu Principle of Weakest Link dan Principle of Least Privilege.



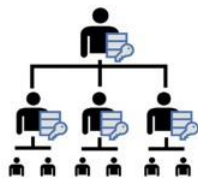
Principle of Weakest Link basically means that an attacker will find the easiest way to achieve their goals.

For example, it might be easier to guess passwords or trick an employee to share his or her password instead of trying to crack an encrypted network session.

## **Principle of Weakest Link**

Principle of Weakest Link pada dasarnya berarti bahwa penyerang akan menemukan cara termudah untuk mencapai tujuan mereka.

Misalnya, mungkin lebih mudah untuk menebak kata sandi atau mengelabui karyawan untuk membagikan kata sandinya daripada mencoba memecahkan jaringan yang terenkripsi.



Principle of Least Privilege means that entities (person, program, or system) must be able to access only the information and resources that are necessary for its business needs.

This principle is important for limiting the damage or impact of the breach and is applied to security controls.

For instance:

- Users on a system only need privileges for themselves to accomplish their tasks
- If users' accounts have been compromised, then the attacker only has access to information assets accessible to that user.

## **Principle of Least Privilege**

Prinsip of Least Privilege pada dasarnya berarti bahwa entitas (orang, program, atau sistem) harus dapat mengakses hanya informasi dan sumber daya yang diperlukan untuk kebutuhan bisnisnya. Prinsip ini penting untuk

membatasi kerusakan atau dampak pelanggaran dan diterapkan pada Security Controls.

Misalnya, pengguna pada suatu sistem hanya membutuhkan hak istimewa bagi diri mereka sendiri untuk menyelesaikan tugas-tugas mereka. Jika akun pengguna telah disusupi, penyerang hanya memiliki akses ke aset informasi yang dapat diakses oleh pengguna tersebut.

**APNIC**

Academy

Courses ▾Events ▾Community Experts ▾About ▾My Account ▾👤 ▾

# Knowledge Check 1

You will need to achieve a score of 80% or higher to pass the quiz. If you don't pass on your first attempt, you can retake the quiz as needed.

## Results

11 of 11 Questions answered correctly

Your time: 00:02:28

**You have reached 11 of 11 point(s), (100%)**

Click Here to Continue

Restart Quiz

Course Progress

Course Navigation

Module 1: Cyber Security Fundamentals

Knowledge Check 1

Module 2: Cyber Security in the Organization

Module 3: Cyber Security Controls

Module 4: Cyber Security Professionals