

LAPORAN RESMI KEMANAN JARINGAN

Tugas 1



**Dosen :
Dr. Ferry Astika Saputra ST, M.Sc
Oleh :
Septiana Dyah Anissawati
D4 LJ Teknik Informatika B
3122640031**

**POLITEKNIK ELEKTRONIKA NEGERI SURABAYA
TAHUN AJARAN
2022/2023**

Perbedaan 3 web service (Apache, Nginx, IIS)

Apache, Nginx, dan IIS adalah tiga perangkat lunak server web yang populer digunakan untuk melayani aplikasi web dan situs web. Meskipun semuanya memiliki tujuan yang sama, yaitu menyajikan konten web kepada pengguna, ada beberapa perbedaan di antara ketiganya.

- Apache

Apache adalah server web open-source yang dikembangkan oleh Apache Software Foundation. Apache menjadi server web yang paling banyak digunakan di seluruh dunia. Beberapa fitur yang dimiliki oleh Apache antara lain kemampuan untuk memproses permintaan HTTP, dukungan untuk banyak bahasa pemrograman seperti PHP, Perl, dan Python, serta konfigurasi yang dapat disesuaikan dengan kebutuhan pengguna.

- Nginx

Nginx adalah server web open-source yang dikembangkan oleh Igor Sysoev pada tahun 2004. Nginx dirancang untuk melayani banyak permintaan dalam waktu yang bersamaan dengan menggunakan sedikit sumber daya. Nginx juga dapat berfungsi sebagai load balancer, HTTP cache, dan server proxy. Nginx diketahui lebih cepat dalam mengakomodasi banyak permintaan daripada Apache.

- IIS

IIS (Internet Information Services) adalah server web yang dikembangkan oleh Microsoft untuk digunakan pada sistem operasi Windows. IIS menyediakan dukungan untuk protokol seperti HTTP, HTTPS, FTP, SMTP, dan NNTP. IIS juga menyediakan dukungan untuk banyak bahasa pemrograman seperti ASP.NET, PHP, dan Python.

Perbedaan mendasar antara ketiga server web ini adalah bahasa pemrograman yang didukung, performa, dan platform yang didukung. Apache dan Nginx dapat digunakan pada sistem operasi Linux, MacOS, dan Windows, sedangkan IIS hanya dapat digunakan pada sistem operasi Windows. Apache dan Nginx dapat mendukung banyak bahasa pemrograman seperti PHP, Python, dan Perl, sedangkan IIS lebih terfokus pada bahasa pemrograman Microsoft seperti ASP.NET.

Berikut adalah contoh perbedaan dalam penggunaan antara Apache, Nginx, dan IIS:

Apache	Nginx	IIS
Situs web dengan trafik rendah atau sedang, seperti blog atau situs pribadi.	Situs web dengan trafik tinggi dan perlu melayani banyak permintaan dalam waktu yang bersamaan, seperti situs web e-commerce atau layanan berbasis cloud.	Situs web yang menggunakan bahasa pemrograman Microsoft, seperti ASP.NET.
Situs web yang memerlukan dukungan bahasa pemrograman seperti PHP, Python, atau Perl.	Situs web yang memerlukan load balancing atau proxy server.	Situs web yang perlu diintegrasikan dengan produk Microsoft, seperti SQL Server atau Exchange Server.
Situs web dengan konfigurasi kustom yang kompleks.	Situs web yang perlu dioptimalkan untuk kecepatan dan kinerja, terutama untuk penggunaan pada perangkat seluler.	Situs web yang memerlukan fitur keamanan khusus, seperti sertifikat digital atau autentikasi Windows.

RANGKUMAN Module 1: Cyber Security Fundamentals

Bab pertama dari Modul 1 APNIC tentang dasar-dasar keamanan siber membahas tiga topik utama, yaitu pengertian keamanan siber, pentingnya keamanan siber, dan ancaman serta risiko yang dapat mengancam keamanan jaringan.

Pertama-tama, modul ini mendefinisikan keamanan siber sebagai usaha untuk melindungi sistem komputer, jaringan, dan data dari akses tidak sah, penggunaan tidak sah, perubahan, pencurian, dan kerusakan. Keamanan siber mencakup semua tindakan yang dilakukan untuk melindungi jaringan dan sistem komputer dari ancaman dan risiko.

Nilai Data dan Informasi : Pada tingkat paling dasar, data dan informasi sangat berharga bagi organisasi. Ini dianggap sebagai aset untuk bisnis.

Data dan Informasi

- Laporan internal
- Data transaksi
- Informasi pengguna
- Desain produk atau resep rahasia

Ancaman Data & Informasi

- Modifikasi yang tidak sah
- Akses tidak sah
- Kehilangan informasi

Kemudian, modul ini membahas pentingnya keamanan siber. Jaringan dan sistem komputer sering kali menyimpan data sensitif seperti informasi pribadi, rahasia bisnis, dan informasi keuangan. Jika jaringan dan sistem tersebut tidak dilindungi dengan baik, maka data tersebut bisa diretas atau dicuri oleh pihak yang tidak bertanggung jawab. Oleh karena itu, penting untuk menjaga keamanan jaringan dan sistem komputer agar data tersebut tidak mudah diakses oleh pihak yang tidak berwenang.

Kebutuhan untuk Mengamankan Informasi : Data dan informasi dapat berada di banyak keadaan - diam, digunakan atau bergerak.

Data saat Istirahat (Data at Rest)

- Data tidak aktif disimpan secara fisik di database, gudang data, spreadsheet, arsip, kaset, cadangan di luar lokasi, dll.

Data dalam Gerakan (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) aset dan sistem informasi.

Confidentiality

- Properti bahwa informasi tidak tersedia atau diungkapkan kepada individu, entitas, atau proses yang tidak sah

Integrity

- Properti yang menjaga keakuratan dan kelengkapan harta kekayaan

Ketersediaan

Availability

- Properti yang dapat diakses dan digunakan sesuai permintaan oleh entitas resmi tanpa penundaan

Threat, Vulnerability and Risk

Dimensi lain yang harus kita pahami adalah hubungan Ancaman, 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: disengaja atau tidak disengaja.
- Ancaman Alam mengacu pada banjir, gempa bumi, angin puting beliung, tanah longsor, longsor salju, badai listrik, dan kejadian serupa lainnya.
- Ancaman Lingkungan mengacu pada kegagalan daya jangka panjang, polusi, bahan kimia, dan kebocoran cairan.
- Ancaman Manusia adalah peristiwa yang diaktifkan oleh atau disebabkan oleh manusia, seperti tindakan yang tidak disengaja (entri data yang tidak disengaja) atau tindakan yang disengaja (serangan berbasis jaringan, unggahan perangkat lunak berbahaya, akses tidak sah ke informasi rahasia).

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.

Risk

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

Terakhir, modul ini membahas ancaman dan risiko yang dapat mengancam keamanan jaringan. Ancaman siber dapat datang dari berbagai sumber, termasuk serangan peretas (hacker), malware, phishing, dan DoS (Denial of Service) attack. Ancaman-ancaman ini dapat menyebabkan kerusakan pada sistem, pencurian data, atau bahkan pencurian identitas. Risiko keamanan jaringan juga dapat muncul dari kelemahan pada sistem atau jaringan yang tidak diperbarui atau tidak dilindungi dengan baik.

Prinsip Keamanan

Seperti yang dapat kita lihat, ada berbagai jenis kontrol keamanan yang harus diterapkan berdasarkan penilaian risiko kami. Kontrol keamanan harus bekerja sama untuk mencapai tujuan keamanan kita. Dalam hal ini, ada dua prinsip keamanan yang sangat berguna untuk diingat:

Kontrol Keamanan

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

Kebijakan dan Prosedur

- Contoh kontrol : Kebijakan keamanan dunia maya, prosedur penanganan insiden
- Tujuan : untuk menyadarkan semua orang akan pentingnya keamanan, menentukan peran dan tanggung jawab, dan ruang lingkup masalah.

Teknis

- Contoh kontrol : Firewall, Sistem deteksi intrusi, perangkat lunak antivirus
- Tujuan : untuk mencegah dan mendeteksi potensi serangan, memitigasi risiko pelanggaran pada lapisan jaringan atau sistem.

Fisik

- Contoh kontrol : CCTV, Kunci, Ruang kerja yang aman
- Tujuan : untuk mencegah pencurian fisik aset informasi atau akses fisik yang tidak sah.

Prinsip Security

Principle of Weakest Link

- Prinsip tautan terlemah pada dasarnya berarti penyerang akan menemukan cara termudah untuk mencapai tujuannya. Misalnya, mungkin lebih mudah untuk menebak

kata sandi atau mengelabui karyawan untuk membagikan kata sandinya daripada mencoba memecahkan sesi jaringan terenkripsi.

Principle of Least Privilege

- Prinsip Keistimewaan Terkecil berarti 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 kontrol keamanan. Misalnya:

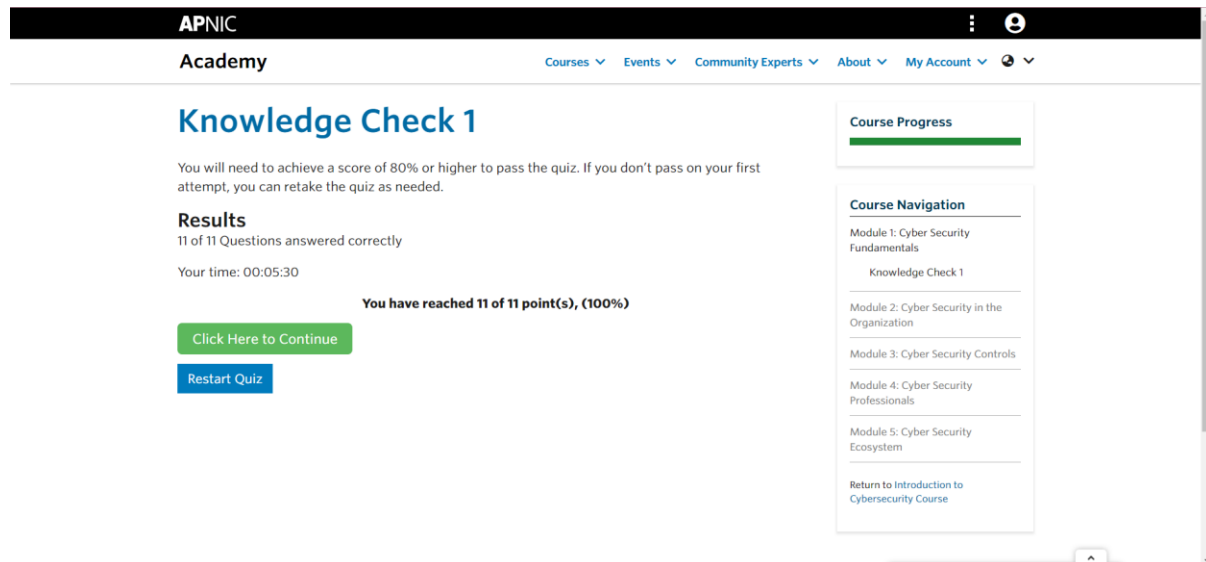
- Pengguna pada sistem hanya membutuhkan hak istimewa bagi diri mereka sendiri untuk menyelesaikan tugas mereka
- Jika akun pengguna telah disusupi, penyerang hanya memiliki akses ke aset informasi yang dapat diakses oleh pengguna tersebut.

Secara keseluruhan, bab pertama dari Modul 1 APNIC membahas dasar-dasar keamanan siber dengan menjelaskan pengertian keamanan siber, pentingnya keamanan siber, dan ancaman serta risiko yang dapat mengancam keamanan jaringan. Hal ini memberikan pemahaman dasar tentang mengapa keamanan siber penting dan mengapa tindakan yang tepat harus diambil untuk melindungi jaringan dan sistem komputer dari ancaman dan risiko tersebut.

Sumber terpercaya untuk informasi ini adalah dokumentasi resmi dari masing-masing perangkat lunak server web, yaitu:

- Apache: <https://httpd.apache.org/docs/>
- Nginx: <https://nginx.org/en/docs/>
- IIS: <https://docs.microsoft.com/en-us/iis/>

Hasil Kuis Modul 1



The screenshot shows the APNIC Academy interface for a 'Knowledge Check 1'. The page has a dark header with the APNIC logo and navigation links. The main content area is white and displays the quiz results. A green progress bar indicates 100% completion. The results section shows '11 of 11 Questions answered correctly' and 'Your time: 00:05:30'. A green button 'Click Here to Continue' and a blue button 'Restart Quiz' are visible. A sidebar on the right shows the course navigation menu with modules 1 through 5, and a link to 'Return to Introduction to Cybersecurity Course'.

APNIC Academy

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: 00:05:30

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
- Module 5: Cyber Security Ecosystem
- [Return to Introduction to Cybersecurity Course](#)