

KEAMANAN JARINGAN DAN SISTEM INFORMASI

Agung Yuliyanto Nugroho

Apriyanto

Edy Wihardjo

Edy Prayitno

Muhammad Munsarif



NEXUSBOOKS.ID



CV PUSTAKA BUKU NUSANTARA

KATA PENGANTAR

Puji syukur kami panjatkan ke hadirat Tuhan Yang Maha Esa atas terselesaikannya buku KEAMANAN JARINGAN DAN SISTEM INFORMASI. Buku ini disusun untuk memberikan pemahaman mengenai konsep dasar keamanan informasi, kriptografi, protokol jaringan, ancaman siber, serta keamanan web dan aplikasi. Dengan meningkatnya ancaman terhadap sistem informasi, pemahaman tentang metode perlindungan data dan sistem menjadi sangat penting bagi individu, organisasi, dan infrastruktur nasional.

Kami berharap buku ini dapat menjadi referensi yang bermanfaat bagi mahasiswa, akademisi, dan praktisi IT dalam memahami dan menerapkan keamanan jaringan serta sistem informasi dengan lebih baik. Ucapan terima kasih kami sampaikan kepada semua pihak yang telah mendukung penyusunan buku ini. Kritik dan saran yang membangun sangat kami harapkan untuk penyempurnaan buku ini di masa mendatang..

NEXUSBOOKS.ID

Jakarta, Maret 2025

Penulis

DAFTAR ISI

KATA PENGANTAR.....	i
DAFTAR ISI	ii
DAFTAR TABEL	v
BAB 1 PENDAHULUAN KEAMANAN INFORMASI.....	1
1.1 Pengertian Keamanan Informasi.....	1
1.2 Konsep Dasar Keamanan Informasi.....	7
1.3 Jenis Ancaman terhadap Keamanan Informasi ..	13
1.4 Prinsip-Prinsip Keamanan Informasi.....	18
1.5 Komponen Keamanan Informasi	23
1.6 Manajemen Risiko Keamanan Informasi.....	30
Langkah-langkah dalam Manajemen Risiko Keamanan Informasi	31
DAFTAR PUSTAKA	36
BAB 2 DASAR - DASAR KRIPTOGRAFI.....	37
2.1 Pengertian Kriptografi	37
2.2 Algoritma Kriptografi	40
2.3 Protokol dan Teknik Kriptografi	44
2.4 Kriptografi dalam IoT dan Keamanan Jaringan ..	48
2.5 Kriptografi dan Keamanan Perangkat Mobile.....	52
2.6 Keamanan Kriptografi di Media Digital	56
DAFTAR PUSTAKA	61
BAB 3 PROTOKOL KEAMANAN JARINGAN.....	61
3.1 Pengantar Protokol Keamanan Jaringan	63
3.2 Dasar-Dasar Protokol Keamanan.....	64
3.3 Analisis Protokol Keamanan Jaringan	67
3.4 Protokol Keamanan untuk Jaringan Nirkabel	69
3.5 Pengelolaan dan Pemeliharaan Protokol	70
3.6 Keamanan Lanjutan dan Tren Terbaru	73
3.7 Sumber Daya dan Alat Pembelajaran	75
DAFTAR PUSTAKA	78

BAB 1

PENDAHULUAN KEAMANAN INFORMASI

Oleh Agung Yuliyanto Nugroho

1.1 Pengertian Keamanan Informasi

Keamanan Informasi dalam konteks **Keamanan Jaringan** dan **Sistem Informasi** merujuk pada langkah-langkah yang diambil untuk melindungi data dan informasi yang disimpan, diproses, atau ditransmisikan dalam sistem informasi dan jaringan komputer. Keamanan informasi ini melibatkan pengelolaan dan penerapan kebijakan, prosedur, dan teknologi untuk memastikan bahwa informasi yang ada dalam sistem dan jaringan tetap aman, terjaga kerahasiaannya, integritasnya, dan dapat diakses dengan benar oleh pihak yang berwenang.

Keamanan Informasi dalam Konteks Keamanan Jaringan:

Keamanan jaringan berfokus pada perlindungan terhadap data yang ditransmisikan melalui jaringan dan infrastruktur jaringan itu sendiri dari ancaman seperti penyusupan, peretasan, serangan DDoS (Distributed Denial of Service), dan pencurian data. Keamanan informasi dalam konteks jaringan memastikan bahwa komunikasi antar perangkat dan server terlindungi dengan baik agar data

BAB 5

KEAMANAN WEB DAN APLIKASI WEB

Oleh Muhammad Munsarif

5.1 Pengertian Kemanan Web

Keamanan web merupakan elemen esensial dalam melindungi situs web dan data pengguna dari ancaman siber yang semakin kompleks. Dalam era digital yang semakin tergantung pada teknologi, keamanan web menjadi fondasi penting bagi keberlanjutan layanan digital serta perlindungan privasi pengguna [1]. Keamanan web, atau web security, mencakup serangkaian tindakan yang bertujuan melindungi situs web dari ancaman seperti peretasan, pencurian data, atau serangan siber lainnya. Ancaman-ancaman ini dapat merusak sistem, mencuri informasi pribadi, atau bahkan membuat situs tidak dapat diakses. Oleh karena itu, dengan menerapkan langkah-langkah seperti enkripsi data, penggunaan firewall, autentikasi dua faktor, dan konfigurasi server yang aman, pemilik situs dapat mengurangi risiko serangan siber dan menjaga kepercayaan pengguna[2].

Langkah-langkah keamanan yang canggih seperti pemantauan rutin dan teknologi enkripsi juga menjadi bagian dari keamanan siber yang lebih luas. Fokusnya