

KEAMANAN SIBER PADA SISTEM KOMPUTER DAN JARINGAN

Setiya Nugroho, S.T., M.Eng., Verra Budhi Lestari, S.Kom., M.Kom.,
Dr. Ir. Muhammad Salman, S.T., MIT., Ali Muhammad, S.Kom., M.Kom.,
Sabrina Adela Br Sibarani, S.Kom., M.Kom.,
Fadil Aulia Rahman, S.Kom., M.Kom., Sri Wahyuningsih, S.Kom., M.Kom.,
Siti Aminah, M.Kom., dan Kiky Rizky Nova Wardani, M.Kom.



Keamanan Siber pada Sistem Komputer dan Jaringan

Setiya Nugroho, S.T., M.Eng.

Verra Budhi Lestari, S.Kom., M.Kom.

Dr. Ir. Muhammad Salman, S.T., MIT.

Ali Muhammad, S.Kom., M.Kom.

Sabrina Adela Br Sibarani, S.Kom., M.Kom.

Fadil Aulia Rahman, S.Kom., M.Kom.

Sri Wahyuningsih, S.Kom., M.Kom.

Siti Aminah, M.Kom.

Kiky Rizky Nova Wardani, M.Kom.



Keamanan Siber pada Sistem Komputer dan Jaringan

Penulis : Setiya Nugroho, S.T., M.Eng., Verra Budhi Lestari, S.Kom., M.Kom., Dr. Ir. Muhammad Salman, S.T., MIT., Ali Muhammad, S.Kom., M.Kom., Sabrina Adela Br Sibarani, S.Kom., M.Kom., Fadil Aulia Rahman, S.Kom., M.Kom., Sri Wahyuningsih, S.Kom., M.Kom., Siti Aminah, M.Kom., dan Kiky Rizky Nova Wardani, M.Kom.

ISBN : 978-634-7670-96-0 (PDF)

Penyunting Naskah : Endah Romadhon

Tata Letak : Endah Romadhon

Desain Sampul : Novikean Keysah Sanisri

Penerbit

PT Cipta Digital Edukasi

Jl. Wijaya Ii/Wijaya Grand Centre Blok G-15, Desa/Kelurahan Pulo, Kec. Kebayoran Baru, Kota Adm. Jakarta Selatan, Provinsi DKI Jakarta, Kode Pos: 1216

E-Mail : penerbitcde@gmail.com

Website : cideka.com

© Hak cipta dilindungi oleh undang-undang

Berlaku selama 50 (lima puluh) tahun sejak Ciptaan tersebut pertama kali dilakukan pengumuman.

Dilarang mengutip atau memperbanyak sebagian atau seluruh isi buku ini tanpa izin tertulis dari penerbit. Ketentuan Pidana Sanksi Pelanggaran Pasal 2 UU Nomor 19 Tahun 2002 Tentang Hak Cipta.

1. Barang siapa dengan sengaja dan tanpa hak melakukan perbuatan sebagaimana dimaksud dalam Pasal 2 ayat (1) atau Pasal 49 ayat (1) dan ayat (2) dipidana dengan pidana penjara masing-masing paling singkat 1 (satu) bulan dan/atau denda paling sedikit Rp1.000.000,00 (satu juta rupiah), atau pidana penjara paling lama 7 (Tujuh) tahun dan/atau denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).
2. Barang siapa dengan sengaja menyerahkan, menyiarkan, memamerkan, mengedarkan atau menjual kepada umum suatu Ciptaan atau barang hasil pelanggaran Hak Cipta atau Hak Terkait sebagaimana dimaksud pada ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau denda paling banyak Rp500.000.000,00 (lima ratus juta rupiah)

KATA PENGANTAR

Puji syukur ke hadirat Tuhan Yang Maha Esa atas tersusunnya buku *Keamanan Siber pada Sistem Komputer dan Jaringan* ini. Perkembangan teknologi informasi dan komunikasi yang begitu pesat telah membawa banyak kemudahan dalam berbagai aspek kehidupan. Namun, di balik kemajuan tersebut, muncul pula berbagai ancaman siber yang semakin kompleks dan beragam. Oleh karena itu, pemahaman yang mendalam mengenai keamanan sistem komputer dan jaringan menjadi suatu kebutuhan yang tidak dapat diabaikan.

Buku ini disusun untuk memberikan landasan teoritis sekaligus panduan praktis dalam memahami konsep keamanan siber, jenis-jenis ancaman, serta strategi mitigasi dan perlindungan sistem. Pembahasan mencakup prinsip dasar keamanan informasi, kriptografi, pengamanan jaringan, manajemen risiko, hingga praktik terbaik dalam menjaga keamanan infrastruktur digital. Penulis berharap buku ini dapat menjadi referensi yang bermanfaat bagi pendidik serta praktisi teknologi informasi dalam meningkatkan kesadaran dan kompetensi di bidang keamanan siber.

Jakarta, Maret 2026

Tim Penyusun

DAFTAR ISI

KATA PENGANTAR.....	iii
DAFTAR ISI.....	iv
BAB 1. PERAN KEAMANAN SIBER DALAM TEKNOLOGI INFORMASI	7
1.1 Konsep Dasar Keamanan Siber	7
1.2 Evolusi dan Sejarah Keamanan Siber	10
1.3 Ancaman dan Risiko Keamanan Informasi	13
1.4 Peran Keamanan Siber dalam Organisasi	17
1.5 Aspek Hukum dan Etika Keamanan Siber	19
1.6 Tantangan dan Perkembangan Keamanan Siber	22
1.7 Latihan Soal (Esai)	24
BAB 2. KONSEP DASAR KEAMANAN INFORMASI.....	25
2.1 Pengertian Keamanan Informasi	25
2.2 Prinsip Dasar Keamanan Informasi.....	28
2.3 Ancaman terhadap Keamanan Informasi	30
2.4 Pengelolaan Keamanan Informasi	32
2.5 Latihan Soal (Esai)	34
BAB 3. ANCAMAN, SERANGAN, DAN KERENTANAN.....	35
3.1 Konsep Ancaman Keamanan Informasi.....	35
3.2 Jenis-Jenis Serangan Siber	38
3.3 Kerentanan Sistem Informasi	41
3.4 Hubungan Ancaman, Serangan, dan Kerentanan	43
3.5 Latihan Soal (Esai)	46
BAB 4. KRIPTOGRAFI DASAR.....	47
4.1 Pengertian dan Tujuan Kriptografi.....	47

4.2 Jenis-Jenis Kriptografi.....	51
4.3 Algoritma Kriptografi Populer	54
4.4 Penerapan Kriptografi dalam Keamanan Informasi.....	56
4.5 Latihan Soal (Esai)	59
BAB 5. KEAMANAN JARINGAN	60
5.1 Konsep Dasar Keamanan JaringanKeamanan jaringan.....	60
5.2 Ancaman terhadap Keamanan Jaringan	63
5.3 Mekanisme dan Teknologi Keamanan Jaringan	65
5.4 Pengelolaan dan Kebijakan Keamanan Jaringan.....	67
5.5 Latihan Soal (Esai)	70
BAB 6. KEAMANAN SISTEM OPERASI DAN APLIKASI..	71
6.1 Konsep Keamanan Sistem Operasi	71
6.2 Ancaman terhadap Sistem Operasi dan Aplikasi	74
6.3 Mekanisme Keamanan Sistem Operasi dan Aplikasi.....	76
6.4 Praktik Terbaik Keamanan Sistem Operasi dan Aplikasi	79
6.5 Pemantauan dan Pengujian Keamanan Sistem Operasi dan Aplikasi	81
6.6 Manajemen Insiden Keamanan pada Sistem Operasi dan Aplikasi	83
6.7 Latihan Soal (Esai)	84
BAB 7. KEAMANAN DATA DAN BASIS DATA	85
7.1 Konsep Keamanan Data	85
7.2 Ancaman terhadap Data dan Basis Data	88
7.3 Mekanisme Keamanan Basis Data	90
7.4 Pengelolaan dan Kebijakan Keamanan Data.....	92
7.5 Latihan Soal (Esai)	95
BAB 8. MANAJEMEN RISIKO DAN AUDIT KEAMANAN	96
8.1 Konsep Manajemen Risiko Keamanan Informasi.....	96

8.2 Identifikasi dan Analisis Risiko	99
8.3 Pengendalian dan Penanganan Risiko	101
8.4 Audit Keamanan Informasi	104
8.5 Manajemen Risiko Keamanan pada Sistem dan Infrastruktur Digital	106
8.6 Audit Keamanan Berbasis Risiko dan Perbaikan Berkelanjutan.....	108
8.7 Latihan Soal (Esai)	110
BAB 9. KEAMANAN SIBER PADA CLOUD DAN IoT	111
9.1 Konsep Keamanan Cloud Computing	111
9.2 Ancaman Keamanan pada Cloud	114
9.3 Keamanan Internet of Things (IoT).....	116
9.4 Strategi dan Praktik Keamanan Cloud dan IoT	119
9.5 Latihan Soal (Esai)	121
BAB 10. ASPEK HUKUM DAN ETIKA KEAMANAN SIBER	122
10.1 Pengantar Aspek Hukum Keamanan Siber	122
10.2 Regulasi dan Kebijakan Keamanan Siber	127
10.3 Etika dalam Keamanan Siber	132
10.4 Tantangan Hukum dan Etika di Era Digital	136
10.5 Latihan Soal (Esai)	139
PROFILE PENULIS.....	141
DAFTAR PUSTAKA	150

Buku Keamanan Siber pada Sistem Komputer dan Jaringan membahas secara komprehensif konsep, ancaman, serta strategi perlindungan terhadap sistem komputer dan infrastruktur jaringan di era digital. Perkembangan teknologi informasi yang pesat telah meningkatkan risiko serangan siber, mulai dari malware, phishing, ransomware, hingga serangan berbasis jaringan seperti DDoS dan intrusi sistem. Buku ini menguraikan prinsip dasar keamanan informasi, termasuk kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) sebagai fondasi dalam membangun sistem yang aman dan andal.

Selain teori dasar, buku ini juga membahas teknik pengamanan seperti kriptografi, firewall, sistem deteksi dan pencegahan intrusi (IDS/IPS), manajemen akses, serta praktik keamanan jaringan dan sistem berbasis cloud. Disertai contoh kasus, ilustrasi arsitektur keamanan, dan pendekatan praktis, buku ini dirancang untuk membantu dosen serta praktisi teknologi informasi memahami dan menerapkan strategi keamanan siber secara efektif dalam menghadapi tantangan ancaman digital yang terus berkembang.