KEAMANAN
JARINGAN KOMPUTER

Tim Penulis:
Aldo Eko Syaputra | Hedie Kristiawan
Agung Yuliyanto Nugroho | Eko Aziz Apriadi
Martono | Zumhur Alamin | Aliyah | Diki Arisandi
Lindung Siswanto | Hendri Julian Pramana
Muhammad Taher Jufri | Nungky Awang Chandra
Praditya Adi Nugroho | Dahlan | Rio Setiawan
Novi Aryani Fitri | Tarmin Abdulghani
Yosep Bustomi | Isminarti
Norbertus Tri Suswanto Saptadi

KEAMANAN JARINGAN KOMPUTER

Aldo Eko Syaputra
Hedie Kristiawan
Agung Yuliyanto Nugroho
Eko Aziz Apriadi
Martono
Zumhur Alamin
Aliyah
Diki Arisandi
Lindung Siswanto
Hendri Julian Pramana
Muhammad Taher Jufri
Nungky Awang Chandra
Praditya Adi Nugroho
Dahlan
Rio Setiawan
Novi Aryani Fitri
Tarmin Abdulghani
Yosep Bustomi
Isminarti
Norbertus Tri Suswanto Saptadi

sada
kurnia pustaka

KEAMANAN JARINGAN KOMPUTER

Tim Penulis:
Aldo Eko Syaputra
Hedie Kristiawan
Agung Yuliyanto Nugroho
Eko Aziz Apriadi
Martono
Zumhur Alamin
Aliyah
Diki Arisandi
Lindung Siswanto
Hendri Julian Pramana
Muhammad Taher Jufri
Nungky Awang Chandra
Praditya Adi Nugroho
Dahlan
Rio Setiawan
Novi Aryani Fitri
Tarmin Abdulghani
Yosep Bustomi
Isminarti
Norbertus Tri Suswanto Saptadi

Tata Letak : Asep Nugraha, S.Hum.
Desain Cover : Septimike Yourintan Mutiara, S.Gz.
Ukuran : UNESCO 15,5 x 23 cm
Halaman : x, 305
ISBN : 978-634-7021-46-5
Terbit Pada : Juni 2025
Anggota IKAPI : No. 073/BANTEN/2023

PENERBIT PT SADA KURNIA PUSTAKA
Jl. Warung Selikur Km.6 Sukajaya – Carenang, Kab. Serang-Banten
Email : sadapenerbit@gmail.com
Website : sadapenerbit.com & repository.sadapenerbit.com
Telpon/WA : +62 838 1281 8431

KATA PENGANTAR

Puji syukur kami panjatkan kehadirat Tuhan Yang Maha Esa atas rahmat dan karunia-Nya, sehingga buku yang berjudul "**Keamanan Jaringan Komputer**" ini dapat terselesaikan dengan baik. Buku ini disusun sebagai upaya untuk menyajikan panduan komprehensif mengenai aspek-aspek krusial dalam menjaga keamanan sistem dan jaringan komputer di era digital yang semakin kompleks dan sarat akan tantangan.

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan signifikan dalam berbagai sendi kehidupan. Jaringan komputer menjadi tulang punggung bagi hampir seluruh aktivitas, mulai dari komunikasi personal, transaksi bisnis, hingga operasional pemerintahan. Namun, seiring dengan kemudahan dan manfaat yang ditawarkan, muncul pula berbagai risiko dan ancaman keamanan yang terus berevolusi. Serangan siber seperti *malware*, *phishing*, DDoS, dan berbagai bentuk intrusi lainnya menjadi semakin canggih dan dapat menimbulkan kerugian yang besar, baik secara finansial maupun reputasi.

Oleh karena itu, pemahaman yang mendalam mengenai konsep dasar keamanan jaringan, identifikasi potensi ancaman, serta implementasi strategi pertahanan yang efektif menjadi suatu kebutuhan yang tidak dapat dihindari. Buku ini hadir untuk menjawab kebutuhan tersebut, dengan menyajikan pembahasan yang terstruktur, mulai dari pengenalan konsep dasar jaringan dan prinsip-prinsip keamanan, analisis berbagai jenis ancaman dan serangan, hingga langkah-langkah praktis dalam merancang, mengimplementasikan, dan mengelola sistem keamanan jaringan yang tangguh.

Buku ini ditujukan bagi para mahasiswa di bidang teknologi informasi, praktisi keamanan siber, administrator jaringan, pengembang sistem, serta siapa saja yang memiliki minat untuk memperdalam pengetahuan mengenai keamanan jaringan komputer.

Kami berupaya menyajikan materi dengan bahasa yang lugas dan disertai contoh-contoh relevan agar mudah dipahami oleh berbagai kalangan pembaca.

Kami menyadari bahwa buku ini masih jauh dari kesempurnaan. Oleh karena itu, kritik dan saran yang membangun dari para pembaca sangat kami harapkan demi perbaikan di masa mendatang. Semoga buku ini dapat memberikan kontribusi positif bagi pengembangan ilmu pengetahuan dan menjadi referensi yang bermanfaat dalam upaya menciptakan lingkungan siber yang lebih aman.

Akhir kata, selamat membaca dan semoga buku ini dapat memperkaya wawasan serta menjadi bekal berharga dalam menghadapi dinamika dunia keamanan jaringan komputer.

Selamat Membaca!

Penulis

DAFTAR ISI

KATA PENGANTAR ..... **iii**
DAFTAR ISI ..... **v**
BAB 1 KONSEP DASAR KEAMANAN JARINGAN **1**
Pendahuluan 2
Definisi Keamanan Jaringan 3
Ancaman dan Resiko pada Jaringan 6
Komponen Utama Dalam Keamanan Jaringan 9
Teknis dan Strategi Pengamanan Jaringan 12
Daftar Pustaka 14
Profil Penulis 16
BAB 2 ANCAMAN DAN SERANGAN JARINGAN **17**
Pendahuluan 18
Definisi Ancaman Jaringan 18
Jenis-Jenis Ancaman Jaringan 19
Kesimpulan 28
Daftar Pustaka 29
Profil Penulis 31
BAB 3 KRIPTOGRAFI DAN KEAMANAN JARINGAN **32**
Pendahuluan 33
Sejarah Kriptografi 35
Jenis-Jenis Kriptografi 36
Diagram Sederhana 39
Daftar Pustaka 41
Profil Penulis 42
BAB 4 AUTENTIKASI DAN OTORISASI **43**
Pendahuluan 44
Konsep Dasar Autentikasi 46
Konsep Dasar Otorisasi 48
Protokol dan Teknologi Pendukung 50
Tantangan dan Isu Keamanan 53
Tren dan Perkembangan Terkini 55
Daftar Pustaka 59
Profil Penulis 61

BAB 5 *FIREWALL* 62
Pengertian *Firewall* 63
Firewall Perangkat Keras dan Perangkat Lunak 64
Tujuan Dasar *Firewall* 64
Teknologi *Firewall* 65
Penyaringan Paket Berstatus (*Stateful Packet Inspection*) 67
Pembuatan Proksi (*Proxying*) 68
Penerjemahan Alamat Jaringan (*Network Address Translation*-NAT) 70
Penutup 73
Daftar Pustaka 75
Profil Penulis 76
BAB 6 *VIRTUAL PRIVATE NETWORK* (VPN) 77
Pendahuluan 78
Manfaat VPN 79
Berbagai Kasus Penggunaan VPN 81
Protokol Jaringan *Privat Virtual* (VPN) 82
Potensi Risiko dan Batasan Penggunaan VPN 86
Faktor-faktor Dalam Memilih Penyedia VPN 87
Aspek Legalitas Penggunaan VPN di Berbagai Negara 89
Perbandingan Layanan VPN Gratis dan Berbayar 90
Memaksimalkan Keamanan dan Privasi Dengan VPN 91
Daftar Pustaka 93
Profil Penulis 95
BAB 7 KEAMANAN PROTOKOL JARINGAN 96
Latar Belakang Keamanan Protokol Jaringan 97
Keamanan Protokol Jaringan Komputer 99
Ancaman Keamanan Protokol Jaringan 100
Protokol yang Aman dan Mekanismenya 103
Daftar Pustaka 104
Profil Penulis 105
BAB 8 SERANGAN *MAN IN THE MIDDLE* (MITM) DAN PENCEGAHANNYA 106
Pendahuluan 107
Apa Itu *Man In The Middle* (MITM)? 107
Motivasi Pelaku Melakukan Serangan MITM 108

Jaringan Publik yang Rawan Serangan MITM 110
Cara Kerja MITM dan Bagaimana *User* Bisa Terjebak 111
Bahaya yang Ditimbulkan dari Serangan MITM 112
Cara Pencegahan Serangan MITM 113
Hasil Riset Terbaru Deteksi dan Pencegahan MITM 115
Daftar Pustaka 118
Profil Penulis 121
BAB 9 *HARDENING SYSTEM* 122
Pengantar *Hardening System* 123
Teknik *Hardening System* 123
Daftar Pustaka 138
Profil Penulis 139
BAB 10 *ETHICAL HACKING* DAN *PENETRATION TESTING* 140
Pendahuluan 141
Apa Itu *Ethical Hacking* dan *Penetration Testing*? 142
Jenis-Jenis *Penetration Testing* 144
Tahapan *Ethical Hacking* dan *Penetration Testing* 146
Standar Umum *Penetration Testing* 149
Tools Populer *Ethical Hacking* 151
Sertifikasi dan Profesi di Bidang *Ethical Hacking* 152
Rangkuman 155
Daftar Pustaka 156
Profil Penulis 158
BAB 11 *PHISHING* DAN *SOCIAL ENGINEERING* 159
Pendahuluan 160
Definisi dan Konsep Dasar *Phishing* dan *Social Engineering* 160
Kesimpulan 167
Daftar Pustaka 169
Profil Penulis 170
BAB 12 MANAJEMEN RISIKO KEAMANAN SIBER 171
Latar Belakang Pentingnya Keamanan Siber 172
Jenis Ancaman Serangan Siber 173
Manajemen Risiko 175
Model dan Kerangka Kerja Manajemen Risiko Keamanan Siber 178

Proses Manajemen Risiko Keamanan Informasi 179
Daftar Pustaka 184
Profil Penulis 185
BAB 13 KEAMANAN NIRKABEL (*Wi-Fi*) 186
Pendahuluan 187
Arsitektur Jaringan Nirkabel 187
Ancaman Keamanan Nirkabel 189
Studi Kasus: Serangan "*Man-in-the-Middle*" Pada Jaringan *Wi-Fi* Publik di Kafe 191
Metode Pengamanan yang Dilakukan 192
Kesimpulan 193
Daftar Pustaka 194
Profil Penulis 195
BAB 14 KEAMANAN *INTERNET OF THINGS* (IOT) 196
Pendahuluan 197
Tantangan Keamanan *Internet of Things* (IoT) 198
Kriptografi Dalam Keamanan IoT 200
Model dan Strategi Keamanan IoT 202
Teknik dan Teknologi Pengamanan IoT 204
Daftar Pustaka 207
Profil Penulis 208
BAB 15 KEAMANAN PERANGKAT LUNAK 209
Pendahuluan 210
Ancaman Umum Pada Perangkat Lunak 210
Prinsip-Prinsip Keamanan Perangkat Lunak 213
Secure Software Development Life Cycle (SDLC) 215
Pengujian Keamanan Perangkat Lunak 217
Manajemen Kerentanan (*Vulnerability Management*) 219
Kesimpulan 220
Daftar Pustaka 221
Profil Penulis 222
BAB 16 SERANGAN DDoS DAN MITIGASINYA 223
Pendahuluan 224
Definisi *Denial of Service* (DDoS) 224
Cara Kerja Serangan DDoS 225
Jenis-Jenis Serangan DDoS 226

Para Penjahat Dapat Menyadap Paket 227
Penjahat Siber Dapat Menyerang *Server* dan Infrastruktur Jaringan 228
Teknik dan Strategi Mitigasi DDoS 229
Daftar Pustaka 232
Profil Penulis 234
BAB 17 *MALWARE* DAN *RONSOMWARE* 235
Definisi *Malware* (*Malicious Software*) 236
Klasifikasi dan Jenis *Malware* 238
Ransomware Bentuk Ancaman Modern 240
Skenario Penyebaran *Malware* dan *Ransomware* 243
Strategi Pencegahan dan Deteksi 246
Tindakan Respons Insiden Terhadap Serangan *Ransomware* 248
Kebijakan dan Kerangka Regulasi 250
Daftar Pustaka 253
Profil Penulis 255
BAB 18 *SECURE CODING* 256
Pendahuluan 257
Prinsip-prinsip Dasar *Secure Coding* 258
Kerentanan Umum Dalam Pengembangan Perangkat Lunak 263
Pengujian Keamanan Dalam Siklus Pengembangan 266
Kesimpulan 267
Daftar Pustaka 268
Profil Penulis 269
BAB 19 KEAMANAN JARINGAN 5G 270
Pendahuluan 271
Definisi dan Karakteristik 5G 272
Fitur Keamanan 275
Ancaman Keamanan Pada Jaringan 5G 276
Strategi Keamanan Untuk Jaringan 5G 277
Kebijakan dan Regulasi 281
Kesimpulan dan Rekomendasi 283
Daftar Pustaka 284
Profil Penulis 287

BAB 20 TREN TERKINI DALAM KEAMANAN JARINGAN KOMPUTER 288
Pendahuluan 289
Meningkatnya Serangan Berbasis AI dan Otomatisasi 290
Zero Trust Architecture (ZTA) 291
Keamanan Berbasis *Cloud* dan SASE 292
Deteksi dan Respons Ancaman Berbasis XDR 294
Penggunaan *Blockchain* Dalam Keamanan Jaringan 295
Keamanan Jaringan Untuk *Internet of Things* (IoT) 296
Ancaman Dari Dalam 298
Edukasi Keamanan Siber dan Kesadaran Pengguna 299
Kesimpulan 301
Daftar Pustaka 303
Profil Penulis 305

BAB 1
KONSEP DASAR KEAMANAN JARINGAN

Aldo Eko Syaputra, M.Kom.
Universitas Adzkia

Belum lagi ancaman serangan *Distributed Denial of Service* (DDoS) yang bisa melumpuhkan layanan sebuah situs dalam hitungan menit. Tak hanya ancaman dari luar, keamanan jaringan juga menghadapi tantangan dari dalam organisasi itu sendiri. Ancaman internal, baik yang disengaja maupun tidak disengaja, kerap kali menjadi penyebab utama kebocoran data. Karyawan yang lalai, tidak teredukasi, atau bahkan memiliki motif tertentu dapat menyebabkan kerugian yang sama besarnya seperti serangan dari luar (Amarudin et al., 2019).

Pentingnya keamanan jaringan juga semakin diperkuat oleh tingginya angka serangan siber di berbagai belahan dunia. Misalnya, serangan *ransomware* yang mengunci data perusahaan dan meminta tebusan dalam bentuk mata uang kripto telah menjadi fenomena global. Belum lagi ancaman serangan *Distributed Denial of Service* (DDoS) yang bisa melumpuhkan layanan sebuah situs dalam hitungan menit.

Tak hanya ancaman dari luar, keamanan jaringan juga menghadapi tantangan dari dalam organisasi itu sendiri. Ancaman internal, baik yang disengaja maupun tidak disengaja, kerap kali menjadi penyebab utama kebocoran data. Karyawan yang lalai, tidak teredukasi, atau bahkan memiliki motif tertentu dapat menyebabkan kerugian yang sama besarnya seperti serangan dari luar. Akhirnya, keamanan jaringan bukan sekadar urusan teknis, tetapi menyangkut aspek keberlangsungan operasional organisasi secara keseluruhan. Oleh karena itu, investasi pada pemahaman dan penerapan konsep dasar keamanan jaringan menjadi langkah awal yang strategis dalam membangun sistem teknologi informasi yang tangguh dan berkelanjutan.

Definisi Keamanan Jaringan

Dalam dunia yang semakin terdigitalisasi, arus informasi menjadi aset yang sangat berharga. Setiap data yang ditransmisikan, baik melalui jaringan internal perusahaan maupun melalui internet publik, memiliki nilai strategis. Oleh karena itu, penting bagi kita untuk memahami perlindungan terhadap data dan sistem, yang secara umum dikenal dengan istilah keamanan jaringan.

c. Antivirus dan *antimalware* melindungi perangkat *endpoint* dari *file* atau program yang mengandung virus. Tanpa antivirus, sistem bisa dengan mudah disusupi *malware* yang menyamar sebagai *file* biasa, lalu menyebar ke seluruh jaringan.
d. VPN menjamin kerahasiaan komunikasi data meskipun dilakukan melalui jaringan publik. Dengan VPN, koneksi antar pengguna atau antar cabang perusahaan akan tetap terenkripsi dan aman dari penyadapan.
e. Protokol keamanan menjamin bahwa setiap proses komunikasi dalam jaringan telah dienkripsi dan tervalidasi. Ini penting dalam transaksi *online*, pertukaran *file* sensitif, maupun pengiriman *email*. Protokol ini memastikan bahwa data hanya dapat diakses oleh penerima yang sah.

Teknis dan Strategi Pengamanan Jaringan

Mengamankan jaringan komputer bukanlah proses satu kali selesai, melainkan sebuah siklus berkelanjutan yang memerlukan teknik dan strategi yang tepat. Oleh karena itu, pengamanan jaringan menuntut perencanaan matang, penguasaan teknis, dan pemahaman menyeluruh terhadap infrastruktur yang digunakan. Strategi pengamanan jaringan dapat dibagi ke dalam dua pendekatan besar: pendekatan teknis dan pendekatan manajerial.

Pendekatan teknis berfokus pada perangkat, sistem, dan protokol yang digunakan untuk melindungi jaringan. Sedangkan pendekatan strategis (manajerial) lebih menitikberatkan pada kebijakan, prosedur, edukasi pengguna, serta pemantauan dan evaluasi berkelanjutan. Kedua pendekatan ini harus berjalan seimbang agar pengamanan dapat optimal (Fauzi et al., 2015).

Dalam konteks keamanan jaringan modern, keberhasilan perlindungan tidak hanya ditentukan oleh seberapa kuat firewall atau antivirus yang digunakan, tetapi juga oleh seberapa baik organisasi mengatur alur kerja, melatih staf, serta mendeteksi dan merespons insiden keamanan.

Tabel 1.2: Teknik dan Strategi Keamanan Jaringan

Kategori	Nama Teknik/Strategi	Deskripsi dan Manfaat
Teknik	Segmentasi Jaringan	Membagi jaringan menjadi beberapa segmen untuk membatasi dampak serangan dan memudahkan kontrol.
	Enkripsi Data	Mengamankan data selama transmisi atau penyimpanan agar tidak dapat dibaca oleh pihak tidak berwenang.
	Pembaruan Sistem (*Patching*)	Menutup celah keamanan dengan memperbarui sistem, aplikasi, dan perangkat secara rutin.
	Multi-Factor Authentication (MFA)	Menambah lapisan keamanan login untuk mencegah akses ilegal walau *password* diketahui.
	Monitoring & Logging	Mendeteksi aktivitas mencurigakan secara real-time dan mendukung analisis forensik insiden.
Strategi	Kebijakan Keamanan Informasi	Pedoman tertulis mengenai hak akses, penggunaan perangkat, dan tanggung jawab pengguna.
	Pelatihan & Edukasi Pengguna	Meningkatkan kesadaran pengguna terhadap ancaman siber dan praktik penggunaan yang aman.
	Risk Assessment & *Audit*	Mengidentifikasi area rentan dan mengevaluasi keamanan jaringan secara berkala.
	Rencana Tanggap Darurat (IRP)	Menyediakan alur penanganan insiden untuk mengurangi dampak dan mempercepat pemulihan.
	Keamanan Berlapis (*Defense in Depth*)	Menggunakan kombinasi berbagai sistem untuk perlindungan berlapis, meningkatkan resiliensi.

Sumber: Diolah Penulis.

Daftar Pustaka

Amarudin, Widyawan, & Najib, W. (2019). Analisis Keamanan Jaringan Single Sign On (SSO) Dengan Lightweight Directory Access Protocol (LDAP) Menggunakan Metode MITMA. *Analisis Keamanan Jaringan Single Sign On (SSO)*, *1*(2302–3805), 1–6.

Anugrah, I., & Rahmanto, R. H. (2018). Sistem Keamanan Jaringan Local Area Network Menggunakan Teknik De-Militarized Zone. *PIKSEL: Penelitian Ilmu Komputer Sistem Embedded and Logic*, *5*(2), 91–106. https://doi.org/10.33558/piksel.v5i2.271.

Dewi, S. (2020). Keamanan Jaringan Menggunakan VPN (Virtual Private Network) Dengan Metode PPTP (Point To Point Tunneling Protocol) Pada Kantor Desa Kertaraharja Ciamis. *EVOLUSI : Jurnal Sains Dan Manajemen*, *8*(1), 128–139. https://doi.org/10.31294/evolusi.v8i1.7658.

Fauzi, A., Setiawan, A., Hasta, A. B., Maulana, A., & Permana, R. (2015). *Introduction Cyber Security*. ELMARKAZI.

Gani, A. G. (2014). Konfigurasi Sistem Keamanan Jaringan. *Jurnal Sistem Informasi Universitas Suryadarma*, *6*(1), 134–149. https://doi.org/10.35968/jsi.v6i1.280.

Hayaty, N. (2020). *Buku Ajar: Sistem Keamanan*. 1–99.

Irfan, A., Nusri, A. Z., Rachmat, Z., & Wulandari, S. (2024). Analisis Keamanan Jaringan Nirkabel Menggunakan Wireless Intrusion Detection System (WIDS). *Jurnal Ilmiah Sistem Informasi Dan Teknik Informatika (JISTI)*, *7*(1), 110–119. https://doi.org/10.57093/jisti.v7i1.195.

Mamuriyah, N., Prasetyo, S. E., & Sijabat, A. O. (2024). Rancangan Sistem Keamanan Jaringan dari serangan DDoS Menggunakan Metode Pengujian Penetrasi. *Jurnal Teknologi Dan Sistem Informasi Bisnis*, *6*(1), 162–167. https://doi.org/10.47233/jteksis.v6i1.1124.

Muftiadi, A., Agustina, T. P. M., & Evi, M. (2022). Studi Kasus Keamanan Jaringan Komputer: Analisis Ancaman Phising Terhadap Layanan Online Banking. *Hexatech: Jurnal Ilmiah Teknik*, *1*(2), 60–65. https://doi.org/10.55904/hexatech.v1i2.346.

Munawar, Z., Kom, M., & Putri, N. I. (2020). Keamanan Jaringan Komputer Pada Era Big Data. *Jurnal Sistem Informasi-J-SIKA*, *02*(01), 14–20.

Palinggi, S., & Allolinggi, L. R. (2020). Analisa Deskriptif Industri Fintech di Indonesia: Regulasi dan Keamanan Jaringan dalam Perspektif Teknologi Digital. *Ekonomi Dan Bisnis*, *6*(2), 177–192. https://doi.org/10.35590/jeb.v6i2.1327.

Purba, W. W., & Efendi, R. (2021). Perancangan dan Analisis Sistem Keamanan Jaringan Komputer Menggunakan SNORT. *AITI: Jurnal Teknologi Informasi*, *17*(2), 143–158. https://doi.org/10.24246/aiti.v17i2.143-158.

Riska, P., Sugiartawan, P., & Wiratama, I. (2018). Sistem Keamanan Jaringan Komputer Dan Data Dengan Menggunakan Metode Port Knocking. *Jurnal Sistem Informasi Dan Komputer Terapan Indonesia (JSIKTI)*, *1*(2), 53–64. https://doi.org/10.33173/jsikti.12.

Santoso, N. A., Affandi, K. B., & Kurniawan, R. D. (2022). Implementasi Keamanan Jaringan Menggunakan Port Knocking. *Jurnal Janitra Informatika dan Sistem Informasi*, *2*(2), 90–95. https://doi.org/10.25008/janitra.v2i2.156.

Santoso, N. A., Ainurohman, M., & Kurniawan, R. D. (2022). Penerapan Metode Penetrasion Testing Pada Keamanan Jaringan Nirkabel. *Jurnal Responsif: Riset Sains Dan Informatika*, *4*(2), 162–167. https://doi.org/10.51977/jti.v4i2.831.

PROFIL PENULIS

Aldo Eko Syaputra, M.Kom.

Aldo Eko Syaputra, M.Kom. Lahir di Kota Depok Provinsi Jawa Barat pada tanggal 07 Juli 1996. Dalam menempuh Pendidikan dimulai dari Sekolah Dasar SDN 03 Taruang-Taruang Tamat 2008, MTsN Sungai Lasi tamat tahun 2011, SMAN 1 Sungai Lasi tamat tahun 2014. Lalu melanjutkan ke pendidikan tinggi swasta yaitu Sarjana (S1) Universitas Putra Indonesia YPTK Padang, lulus pada tahun 2018 dengan jurusan Sistem Informasi. Kemudian melanjutkan Program Pascasarjana (S2) di Universitas Putra Indonesia YPTK Padang dan lulus pada tahun 2020 Program Studi Teknik Informatika Konsentrasi Sistem Informasi. Penulis mengabdikan diri sebagai salah satu Dosen di Bidang Ilmu Komputer khususnya Program Studi Sistem Informasi di Universitas Adzkia dan menjadi Dosen tetap pada maret tahun 2021 di kampus tersebut. Penulis memiliki kepakaran dibidang Bisnis *Digital* dan *Data Science*. Dan untuk mewujudkan karir sebagai dosen profesional, penulis pun aktif sebagai peneliti di bidang kepakarannya tersebut. Beberapa penelitian yang telah dilakukan didanai oleh internal perguruan tinggi dan juga Kemenristek DIKTI. Selain peneliti, penulis juga aktif menulis buku dengan harapan dapat memberikan kontribusi positif bagi bangsa dan negara yang sangat tercinta ini.

Email Penulis: aldo@adzkia.ac.id.

BAB 2
ANCAMAN DAN SERANGAN JARINGAN

Hedie Kristiawan, S.Kom., M.M.
Universitas Santo Borromeus

Dalam konteks keamanan siber, ancaman ini mencakup berbagai jenis serangan yang dapat dilakukan oleh individu, kelompok atau bahkan negara dengan niat jahat (Fadhila Inas Pratiwi Citra Hennida, 2024).

Menurut laporan dari *Cybersecurity & Infrastructure Security Agency* (CISA), ancaman ini dapat berasal dari malware, serangan phishing, *ransomware*, dan serangan *Distributed Denial of Service* (DDoS) yang semuanya dapat menyebabkan kerugian finansial dan reputasi yang besar bagi organisasi menjadi target. Pentingnya memahami ancaman jaringan tidak bisa diabaikan, terutama di era digital sekarang ini di mana data menjadi aset yang sangat berharga.

Menurut laporan IBM, biaya rata-rata pelanggaran data pada tahun 2021 mencapai $4,24 Juta, yang menunjukan seberapa serius dampak dari serangan siber. (IBM Annual Report., 2017) Selain itu laporan lainnya menunjukan bahwa sebesar 43% dari semua pelanggaran data melibatkan serangan yang ditargetkan pada jaringan. Hal ini menekankan perlunya organisasi untuk memiliki pemahaman yang mendalam tentang ancaman yang ada dan untuk mengambil langkah-langkah pencegahan yang efektif.

Definisi ancaman jaringan dalam konteks keamanan siber mencakup semua potensi bahaya yang bisa memanfaatkan kelemahan dalam sistem jaringan. Ancaman ini tidak hanya mencakup serangan dari luar, tetapi juga ancaman yang berasal dari dalam organisasi, seperti *insider threats*. Dengan memahami berbagai jenis ancaman, organisasi bisa mengembangkan strategi keamanan yang lebih baik untuk melindungi data dan infrastruktur mereka. Oleh karena itu, kesadaran dan pendidikan tentang ancaman jaringan sangat penting untuk menciptakan lingkungan yang aman dan terlindungi dari serangan siber.

Jenis-Jenis Ancaman Jaringan

Di dunia yang semakin terhubung secara digital, ancaman jaringan menjadi salah satu tantangan utama bagi individu dan organisasi. Jenis ancaman ini bervariasi dari malware yang merusak sistem dan mencuri data. Selain itu teknik phishing yang canggih sering digunakan untuk menipu pengguna dengan disamarkan sebagai perusahaan terpercaya.

pencurian data. Kerusakan reputasi ini tidak hanya mempengaruhi hubungan dengan pelanggan yang sudah ada, tetapi juga dapat menghambat potensi pelanggan baru dan mengurangi daya tarik bisnis di mata investor.

Dalam jangka panjang, dampak reputasi dapat menyebabkan penurunan pangsa pasar dan kesulitan dalam menarik investasi, sehingga penting bagi organisasi organisasi yang tidak hanya berfokus pada aspek teknis keamanan siber, tetapi juga mempertimbangkan dampak reputasi yang dapat disebabkan oleh serangan siber. Oleh karena itu pendekatan komprehensif terhadap serangan siber menjadi sangat penting untuk melindungi aset berharga dan mempertahankan kelangsungan organisasi.

Kesimpulan

Dari pembahasan yang dijelaskan, kita dapat menyimpulkan bahwa dampak serangan *cyber* penting bagi individu dan organisasi di era *digital* saat ini. Kerugian finansial yang disebabkan oleh serangan siber, akan mencapai miliaran, termasuk biaya pemulihan, kehilangan pendapatan dan kerugian data.

Selain itu *downtime* karena serangan dapat mengganggu kegiatan dan mengancam kelangsungan hidup perusahaan terutama untuk bisnis yang merupakan sumber daya terbatas. Oleh karena itu, penting bahwa organisasi harus mengembangkan strategi mitigasi untuk melindungi aset berharga mereka terhadap ancaman yang terus berkembang. Selain kerugian finansial serangan dunia maya dapat menyebabkan kerusakan reputasi yang berkepanjangan, yang berdampak pada kepercayaan diri pelanggan dan hubungan perdagangan.

Keyakinan yang berkurang ini dapat menyebabkan hilangnya pelanggan dan kesulitan dalam menarik investasi, yang dapat mempengaruhi daya saing. Oleh karena itu pendekatan komprehensif untuk keamanan dunia maya, termasuk aspek teknis dan reputasi, sangat penting untuk mempertahankan integritas dan keberlanjutan kegiatan organisasi. Dengan menangani ancaman yang semakin kompleks, organisasi harus berkomitmen untuk memperkuat kesadaran keamanan siber dan menerapkan tahap aktif untuk melindungi diri dari serangan siber.

Daftar Pustaka

APWG. (2023). *Phishing Activity Trends Report_4th Quarter of 2023*. *February 2024*, 1–10. www.apwg.org,

Bustami, A., & Bahri, S. (2020). Ancaman, Serangan dan Tindakan Perlindungan Pada Keamanan Jaringan Atau Sistem Informasi: Systematic Review. *Unistek*, *7*(2), 59–70. https://doi.org/10.33592/unistek.v7i2.645.

Cekerevac, Z. (n.d.). *Man-In-The-Middle Attacks*. *January 2025*. https://doi.org/10.12709/mest.13.13.01.04.

Connolly, L. Y., & Wall, D. S. (2019). *Computers & Security The Rise Of Crypto-Ransomware In A Changing Cybercrime Landscape: Taxonomising Countermeasures*. *87*. https://doi.org/10.1016/j.cose.2019.101568.

Fadhila Inas PratiwiCitra Hennida, S. S. , N. B. D. Y. E. C. S. D. and A. A. I. (2024). *Cybersecurity Challenges In Indonesia: Threat and Responses Analysis*. *22*(3–4), 239–264. https://doi.org/https://doi.org/10.1163/15691497-12341660.

IBM Annual Report. (2017). *The Businesses Of The World Are Changing The Way They Work. We Have Prepared Your Company For This Moment.*

Leet, E. S. (2020). About The Cover. *Postmedieval*, *11*(1). https://doi.org/10.1057/s41280-020-00164-x.

Lidya Desy. (2015). *Analisa Malicious Code pada PDF Attack Menggunakan Teknik Reverse Engineering*. *672010031*.

Morgan, S. (2020). The 2020 Data Attack of Data by 2025 Oussama El-Hilali. *Arcserve*, 1–5.

Pratama, F. N. (2023). Perancangan Sistem Deteksi Dini Keamanan Informasi DISKOMINFO Kabupaten Bandung. *Jurnal Teknik Informatika Dan Sistem Informasi*, *10*(1), 808–820. http://jurnal.mdp.ac.id.

Yaspranika, Y., Setiawan, D., & Heryanto, A. (2020). *Sistem Deteksi Man*

in the Middle (MitM) Attack Pada Jaringan Supervisory Control and Data Acquisition (Scada) Menggunakan…. https://repository.unsri.ac.id/35878/.

Zidane, M. (2022). *Klasifikasi Serangan Distributed Denial-of-Service (DDoS) Menggunakan Metode Data Mining Naïve Bayes*. *6*(1), 172–180.

PROFIL PENULIS

Hedie Kristiawan, S.Kom., M.M.

Ketertarikan penulis terhadap ilmu manajemen dan sistem informasi dan komputer dimulai pada tahun 2000 silam. Hal tersebut membuat penulis memilih untuk masuk ke Perguruan Tinggi Sekolah Tinggi Ilmu Komputer (STMIK) LIKMI Bandung dengan memilih Manajemen Sistem Informasi (Manjemen Informasi) dan berhasil menyelesaikan studi pada tahun 2005. Penulis kemudian melanjutkan studi S2 pada tahun 2015 di prodi Manajemen Program Pasca Sarjana Universitas Pasundan Bandung dengan bidang minat Sistem Informasi Bisnis. Penulis memiliki kepakaran dibidang Manajemen dan Sistem Teknologi Informasi. Dan untuk mewujudkan karir sebagai dosen profesional, dan juga sebagai praktisi, penulis pun aktif sebagai peneliti di bidang kepakarannya tersebut dan penulis juga aktif menulis buku dengan harapan dapat memberikan kontribusi positif bagi bangsa dan negara yang sangat tercinta ini.

Email Penulis: hedie.kristiawan161@gmail.com.

BAB 3
KRIPTOGRAFI DAN KEAMANAN JARINGAN

Agung Yuliyanto Nugroho, M.Kom., M.Par.
Universitas Cendekia Mitra Indonesia

Sejarah Kriptografi

Kriptografi, sebagai ilmu untuk melindungi informasi, telah berkembang sejak ribuan tahun yang lalu. Pada awalnya, kriptografi digunakan terutama untuk menjaga kerahasiaan pesan dalam peperangan atau komunikasi penting. Sejarah kriptografi dapat dibagi ke dalam beberapa periode penting berikut:

1. **Kriptografi Kuno**

   Pada masa kuno, kriptografi digunakan untuk menyembunyikan pesan dalam bentuk yang sederhana. Salah satu metode tertua yang dikenal adalah sandi Caesar, yang digunakan oleh Julius Caesar untuk mengirim pesan rahasia kepada para jenderalnya. Teknik ini melibatkan pergeseran huruf dalam alfabet sejumlah langkah tertentu.

   Selain sandi Caesar, bangsa Mesir kuno dan Yunani juga mengembangkan metode kriptografi sederhana, seperti penggunaan hieroglif untuk menyamarkan pesan atau scytale di Sparta, yaitu teknik enkripsi dengan menggunakan batang kayu berdiameter tertentu.

2. **Kriptografi Abad Pertengahan**

   Pada abad pertengahan, kriptografi berkembang menjadi lebih kompleks. Salah satu perkembangan penting adalah penggunaan tabel substitusi dan transposisi. Di Eropa, kriptografi banyak digunakan dalam kegiatan diplomatik dan militer. Misalnya, *Vigenère cipher*, yang ditemukan pada abad ke-16, menggunakan serangkaian substitusi berbasis kunci untuk mengenkripsi teks.

   Meskipun dianggap "tak terpecahkan" selama berabad-abad, *Vigenère cipher* akhirnya berhasil dipecahkan pada abad ke-19.

3. **Kriptografi Pada Era Perang Dunia**

   Kriptografi memainkan peran krusial selama Perang Dunia I dan II. Salah satu contoh terkenal adalah mesin Enigma yang digunakan oleh Jerman. Mesin ini memungkinkan penyandian pesan yang sangat kompleks. Namun, upaya para kriptografer di Bletchley Park, Inggris termasuk tokoh penting seperti Alan Turing berhasil memecahkan kode Enigma, yang mempercepat akhir Perang Dunia II.

Algoritma *stream cipher* yang cepat, namun kini dianggap kurang aman untuk beberapa aplikasi. *Blowfish* dan *Twofish*: algoritma alternatif untuk AES dengan performa tinggi dan keamanan yang kuat. Aplikasi kriptografi simetris, pengamanan data di *database*, pengamanan komunikasi jaringan lokal (LAN/WLAN), Sistem pembayaran elektronik, Enkripsi *file* dan perangkat penyimpanan, ilustrasi sederhana. Misal, Alice ingin mengirim pesan ke Bob:

1. Alice mengenkripsi pesannya menggunakan kunci rahasia bersama.
2. Pesan terenkripsi dikirimkan ke Bob.
3. Bob menggunakan kunci yang sama untuk mendekripsi pesan dan membacanya.
4. Kriptografi Asimetris (*Asymmetric Cryptography*).

Kriptografi asimetris adalah metode enkripsi yang menggunakan sepasang kunci berbeda tetapi saling berhubungan:

1. Kunci Publik (*Public Key*): dapat dibagikan kepada siapa saja.
2. Kunci Privat (*Private Key*): harus dijaga kerahasiaannya oleh pemiliknya.

Data yang dienkripsi dengan kunci publik hanya dapat didekripsi dengan kunci privat yang sesuai, dan sebaliknya. Model ini mengatasi masalah distribusi kunci yang ada pada kriptografi simetris. Prinsip lerja:

1. Dalam kriptografi asimetris, terdapat dua operasi utama:
2. Enkripsi: pengirim menggunakan kunci publik penerima untuk mengenkripsi pesan.
3. Dekripsi: penerima menggunakan kunci privatnya sendiri untuk mendekripsi pesan tersebut.

Selain itu, kriptografi asimetris juga mendukung penandatanganan *digital*, yaitu:

1. Pengirim menggunakan kunci privat untuk menandatangani pesan.
2. Penerima menggunakan kunci publik pengirim untuk memverifikasi tanda tangan tersebut.
3. Kriptografi Hibrida (*Hybrid Cryptography*).

Kriptografi hibrida adalah metode yang menggabungkan keunggulan kriptografi simetris dan asimetris dalam satu sistem keamanan. Tujuannya adalah memanfaatkan:

1. Kecepatan kriptografi simetris untuk enkripsi data berukuran besar, dan
2. Keamanan kriptografi asimetris untuk pertukaran kunci.

Dengan kata lain, kriptografi hibrida menciptakan sistem yang lebih efisien dan aman dibandingkan hanya menggunakan satu jenis kriptografi saja. Prinsip kerja:

1. Negosiasi Kunci**:**
   a. Pengirim menggunakan algoritma kriptografi asimetris (seperti RSA) untuk mengenkripsi kunci simetris.
   b. Kunci ini disebut *session key* atau kunci sesi.
2. Enkripsi Data**:** setelah kunci simetris diterima oleh penerima, data sebenarnya (pesan, *file*, dll.) dienkripsi menggunakan algoritma simetris (seperti AES).
3. Dekripsi**:**
   a. Penerima mendekripsi *session key* menggunakan kunci privat asimetris.
   b. Setelah mendapatkan *session key*, data yang dienkripsi dengan algoritma simetris dapat didekripsi dengan cepat.

Diagram Sederhana

```
Data → [Enkripsi Simetris (AES)] → Ciphertext
Session Key → [Enkripsi Asimetris (RSA)] → Encrypted Session Key
```

Pengiriman ke penerima:

1. *Encrypted Session Key* + *Ciphertext* Penerima**:**
2. Deskripsi Session *Key* → Deskripsi *Ciphertext*.

Kelebihan Kriptografi Hibrida

1. Kinerja Tinggi: Data dienkripsi dengan algoritma simetris yang cepat.
2. Distribusi Kunci Aman: Kunci simetris dilindungi menggunakan kriptografi asimetris.

3. Skalabilitas Baik**:** Cocok untuk aplikasi yang membutuhkan pengamanan data dalam jumlah besar.

Kekurangan Kriptografi Hibrida

1. Kompleksitas Implementasi**:** sistem hibrida lebih kompleks daripada menggunakan satu metode saja.
2. *Overhead* Awal: proses pertukaran kunci asimetris memerlukan waktu lebih dibandingkan komunikasi biasa.

Daftar Pustaka

Diffie, W., & Hellman, M. (1976). *New Directions In Cryptography. IEEE Transactions On Information Theory*, 22(6), 644–654. https://doi.org/10.1109/TIT.1976.1055638.

Easttom, C. (2018). *Modern Cryptography: Applied Mathematics For Encryption And Information Security*. McGraw-Hill Education.

Kaufman, C., Perlman, R., & Speciner, M. (2011). *Network Security: Private Communication In A Public World (2nd ed.).* Prentice Hall.

Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook Of Applied Cryptography.* CRC Press.

Paar, C., & Pelzl, J. (2010). *Understanding Cryptography: A Textbook For Students And Practitioners*. Springer.

Singh, S. (2000). The *Code Book: The Science Of Secrecy From Ancient Egypt To Quantum Cryptography*. Anchor Books.

Stallings, W. (2017). *Cryptography And Network Security: Principles And Practice (7th Ed.).* Pearson.

PROFIL PENULIS

Agung Yuliyanto Nugroho, M.Kom., M.Par.

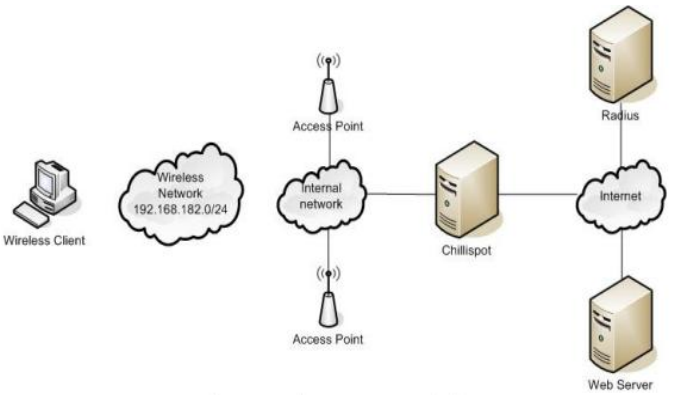
Ketertarikan penulis terhadap ilmu komputer dimulai pada tahun 2015 silam. Hal tersebut membuat penulis melanjutkan pendidikan ke Perguruan Tinggi dan berhasil menyelesaikan studi S1 di prodi Teknik Informatika Universitas Teknologi Yogyakarta pada tahun 2018. Dua tahun kemudian, penulis menyelesaikan studi S2 di prodi Teknik Informatika Program Pasca Sarjana Universitas Amikom Yogyakarta dan juga prodi Magister Pariwisata di Sekolah Tinggi Pariwisata Ambarrukmo Yogyakarta. Atas dedikasi dan kerja keras dalam membuat suatu karya, Republik Indonesia Kementerian Hukum Dan Hak Asasi Manusia sudah mencatat ada kurang lebih 100 karya yang sudah tercatat di surat pencatatan ciptaan sebagai salah satu kontribusi dalam melindungi hak kekayaan intelektual.

Email Penulis agungboiler11@gmail.com.

BAB 4
AUTENTIKASI DAN OTORISASI

Eko Aziz Apriadi, S.T., M.Kom.
Universitas Indonesia Mandiri

mengadaptasi dinamika ancaman serta kebutuhan pengguna yang beragam dan tersebar.



Gambar 4.1: Struktur Jaringan *Chillispot*
Sumber: Otentikasi & Pelaporan, 2006.

Keamanan jaringan yang efektif tidak hanya berfokus pada pencegahan akses ilegal, tetapi juga memastikan integritas, kerahasiaan, dan ketersediaan (CIA: *Confidentiality, Integrity, Availability*) dari informasi yang dikelola (Hermawan & Pasaribu, 2023). Autentikasi dan otorisasi yang dirancang dengan baik akan mencegah akses tidak sah, menghindari penyalahgunaan hak akses, dan memastikan bahwa sistem tetap dapat digunakan oleh pihak yang berhak pada waktu yang tepat (Fatman, 2020).

Selain itu, dengan semakin tingginya regulasi terkait perlindungan data pribadi seperti GDPR (*General Data Protection Regulation*) di Eropa dan UU Perlindungan Data Pribadi di Indonesia, penerapan autentikasi dan otorisasi yang kuat juga menjadi kewajiban hukum.

Organisasi dituntut untuk menjaga akuntabilitas dalam pengelolaan data pengguna, dan sistem keamanan jaringan yang andal menjadi instrumen utama dalam memenuhi tanggung jawab ini. Bab ini akan membahas secara komprehensif mengenai autentikasi dan otorisasi sebagai komponen utama dalam sistem keamanan jaringan komputer.

Pembahasan akan dimulai dari pemahaman konsep dasar, jenis-jenis mekanisme yang tersedia, hingga model dan protokol yang umum digunakan dalam implementasi nyata.

kombinasi yang lemah, mudah ditebak, dan digunakan ulang di banyak layanan. *Passwordless* authentication menghapus kebutuhan pengguna untuk mengingat atau mengetikkan kata sandi, dan menggantikannya dengan metode autentikasi berbasis biometrik, token *hardware*, atau verifikasi perangkat terpercaya.

Salah satu bentuk implementasi *passwordless authentication* yang paling umum adalah penggunaan autentikasi biometrik seperti sidik jari, pengenalan wajah, atau pemindaian retina. Metode ini menawarkan kenyamanan sekaligus peningkatan keamanan karena atribut biometrik sulit untuk diduplikasi. Selain itu, teknologi seperti *WebAuthn* dan FIDO2 menyediakan kerangka kerja terbuka yang memungkinkan verifikasi berbasis perangkat terpercaya, menjadikan proses autentikasi lebih aman dan *user-friendly*.

Dalam sistem berbasis *cloud* dan aplikasi modern, passwordless authentication juga diintegrasikan melalui perangkat lunak autentikator seperti *Microsoft Authenticator atau Google Authenticator*, serta token keamanan fisik seperti *YubiKey*. Sistem ini dapat menggabungkan autentikasi kontekstual, seperti lokasi dan perilaku pengguna, sehingga memberikan lapisan keamanan tambahan tanpa menambah beban kognitif kepada pengguna.

Penerapan teknologi-teknologi ini membutuhkan pondasi arsitektur dan kebijakan keamanan yang matang. Organisasi harus memastikan adanya integrasi yang mulus antara sistem autentikasi, kontrol akses, dan pengelolaan identitas yang adaptif. Penggunaan ZTA, AI, dan *passwordless authentication* harus didukung dengan pelatihan sumber daya manusia, pembaruan kebijakan keamanan, serta pemantauan berkelanjutan untuk memastikan efektivitas dan keberlanjutan penerapan (Apriadi et al., 2024).

Dari perspektif manajemen risiko, integrasi ketiga pendekatan ini ZTA, AI/ML, dan autentikasi tanpa kata sandi mewakili evolusi penting dalam menjaga keamanan jaringan. Mereka tidak hanya meningkatkan ketahanan terhadap serangan siber, tetapi juga mendorong pengalaman pengguna yang lebih baik, dengan mengurangi ketergantungan pada mekanisme autentikasi tradisional yang rentan dan tidak efisien.

Dengan demikian, transformasi keamanan jaringan menuju model yang lebih adaptif, cerdas, dan bebas kata sandi menjadi suatu keniscayaan dalam menjawab tantangan digital masa kini. Pendekatan ini menuntut organisasi untuk berpikir ulang tentang bagaimana mereka mendefinisikan kepercayaan, bagaimana mereka membangun sistem autentikasi dan otorisasi, serta bagaimana mereka melindungi data dan sumber daya yang semakin tersebar di berbagai lingkungan dan perangkat.

Daftar Pustaka

Apriadi, E. A., & Bisri, M. (2025). Optimization of BPJS Health Facility Distribution with K-Means Clustering Algorithm. *International Journal of Technology and Computer Science*, *1*(1), 1–13.

Apriadi, E. A., Lestari, S., & Irianto, S. Y. (2024). Comparison of Performance of K-Nearest Neighbors and Neural Network Algorithm in Bitcoin Price Prediction. *Sinkron: Jurnal Dan Penelitian Teknik Informatika*, *8*(2), 617–622.

Ardhana, V. Y. P., Hidayat, M. T., Jannah, M., Sumiati, S., Rini, P., & Sari, N. (2023). Implementasi RESTful API Pada Laravel dan Simulator IoT Wokwi Untuk Pengukuran Suhu dan Kelembaban Menggunakan Metode Waterfall. *Arcitech: Journal of Computer Science and Artificial Intelligence*, *3*(2), 93. https://doi.org/10.29240/arcitech.v3i2.9334.

Army, W. L., Ilham, W., & Syafrinal, I. (2023). *Mengoptimalkan Jaringan Hotspot Pada Kampus Upi "Yptk" Padang*. *13*(2), 124–133.

Fatman, Y. (2020). Implementasi Metode Open Authorization (OAUTH2) Untuk Pengelolaan Data Dosen di Universitas Islam Nusantara. *Ainet : Jurnal Informatika*, *2*(1), 10–18. https://doi.org/10.26618/ainet.v2i1.3212.

Fatwa, A. (2025). *Pengembangan Layanan Autentikasi dan Manajemen Akses Menggunakan Pendekatan Waterfall untuk Integrasi Aplikasi Fakultas berbasis Microservice (Studi Kasus: Fakultas Rekayasa Industri)*. *12*(1), 1634–1644.

Hermawan, F., & Pasaribu, A. F. O. (2023). Implementasi Web Service Sebagai Penyedia Informasi Untuk Aplikasi Pengelolaan Jadwal Pemberian Pakan Ikan (Studi Kasus: Pokdakan Karya Bersama). *Jurnal Informatika Dan Rekayasa Perangkat Lunak*, *4*(3), 335–341. https://doi.org/10.33365/jatika.v4i3.2720.

Kusuma, I. G. N. A. (2021). Perancangan Simple Stateless Autentikasi Dan Otorisasi Layanan Rest-Api Berbasis Protokol Http. *Jurnal Manajemen Informatika Dan Sistem Informasi*, *4*(1), 78–87.

Mahmudi, F. (2023). Analisis dan Perancangan Interoperabilitas Data Pemonitoran SPM (Standar Pelayanan Minimal) Bidang Kesehatan dengan Web Services. *Jurnal Rekam Medis Dan Informasi Kesehatan*, *6*(2), 126–132. https://doi.org/10.31983/jrmik.v6i2.10511.

Marisa Khairina, D. (2011). Analisis Keamanan Sistem Login. *Jurnal Informatika Mulawarman*, *Vol. 6 No. 2*(2), 64–67.

Nashikhuddin, A. Y., Karaman, J., & Litanianda, Y. (2023). Implementasi Api Restful Dengan Json Web Token (Jwt) Pada Aplikasi E-Commerce Thrifty Shop Untuk Otentikasi Dan Otorisasi Pengguna. *METHOMIKA Jurnal Manajemen Informatika Dan Komputerisasi Akuntansi*, *7*(2), 239–246. https://doi.org/10.46880/jmika.vol7no2.pp239-246.

Otentikasi, S., & Pelaporan, D. A. N. (2006). *Koneksi User Pada Jaringan Wireless*. *4*(1), 67–79.

PROFIL PENULIS

Eko Aziz Apriadi, S.T., M.Kom.

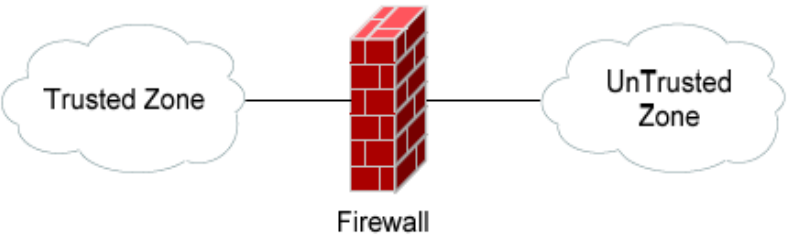
Penulis lahir di Bumi Pratama Mandara, Lampung, pada tanggal 14 April 1998. Sejak usia dini, penulis telah menunjukkan ketertarikan yang tinggi terhadap dunia teknologi dan komputer. Pendidikan formalnya dimulai di SD Negeri 1 Rantau Temiang yang diselesaikan pada tahun 2010. Selanjutnya, penulis melanjutkan pendidikan di SLTP Negeri 1 Banjit dan lulus pada tahun 2013, kemudian melanjutkan ke SMA Negeri 1 Banjit jurusan IPA dan menyelesaikannya pada tahun 2016. Minat dan kecintaan terhadap dunia teknologi informasi mengantarkan penulis untuk melanjutkan pendidikan tinggi di Universitas Lampung dan berhasil meraih gelar Sarjana Teknik (S.T.) dari Program Studi Teknik Elektro pada tahun 2021. Untuk memperdalam kompetensinya di bidang informatika, penulis kemudian melanjutkan studi pascasarjana di Institut Informatika dan Bisnis Darmajaya pada Program Studi Magister Teknik Informatika (M.Kom) dan saat ini tengah menyelesaikan studinya.

Pada tahun 2021, penulis mulai bergabung dengan Universitas Sang Bumi Ruwa Jurai sebagai Operator di Fakultas Ilmu Sosial dan Ilmu Politik. Pada tahun 2024, penulis diangkat menjadi Kepala Bagian Kemahasiswaan dan Alumni di Unit Wakil Rektor Bidang Kemahasiswaan dan Alumni. Selain itu, penulis juga sebagai dosen di Program Studi Hubungan Masyarakat dan Komunikasi Digital pada tahun yang sama, sebelum akhirnya berpindah mengajar di Universitas Indonesia Mandiri di Program Studi Informatika. Di sana, penulis kini menjabat sebagai Sekretaris LPPM (Lembaga Penelitian dan Pengabdian Masyarakat). Selain mengajar dan meneliti, penulis juga kerap menjadi narasumber dalam pelatihan dan seminar nasional.

Email Penulis: ekoazizapriadi72@gmail.com.

BAB 5
FIREWALL

Martono, S.Pd.Kim., M.TI.
Universitas Raharja



Gambar 5.1: *Firewall*
Sumber: *Introduction to Firewalls* v1.01-Aaron Balchunas.

Firewall Perangkat Keras dan Perangkat Lunak

Firewall dapat berupa perangkat keras atau perangkat lunak, tetapi konfigurasi *firewall* yang ideal akan terdiri dari keduanya. Selain membatasi akses ke komputer dan jaringan, *firewall* juga berguna untuk memungkinkan akses jarak jauh ke jaringan pribadi melalui sertifikat autentikasi dan *login* yang aman.

Firewall perangkat keras dapat dibeli sebagai produk yang berdiri sendiri, tetapi biasanya juga ditemukan di *broadband routers* dan harus diperhatikan sebagai bagian penting dari sistem dan pengaturan jaringan. Sebagian besar *firewall* perangkat keras akan memiliki minimal empat *port* jaringan untuk menghubungkan komputer lain. Tetapi untuk jaringan yang lebih besar, solusi *firewall* jaringan bisnis juga tersedia.

Firewall perangkat lunak diinstal pada komputer seperti perangkat lunak lainnya dan instalasinya dapat menyesuaikannya, memungkinkan pengguna untuk mengendalikan fungsi dan fitur perlindungannya. *Firewall* perangkat lunak akan melindungi komputer dari upaya eksternal untuk mengendalikan atau mendapatkan akses ke komputer secara ilegal.

Tujuan Dasar *Firewall*

Pada dasarnya, *firewall* melakukan tiga hal untuk melindungi jaringan:

1. Memblokir data masuk yang mungkin berisi serangan peretas.
2. Menyembunyikan informasi tentang jaringan dengan membuatnya seolah-olah semua lalu lintas keluar berasal dari *firewall* dan bukan dari jaringan. Ini disebut *Network Address Translation* (NAT).

NAT adalah proses di mana *router* menerjemahkan alamat IP pribadi menjadi alamat IP publik sehingga dapat mengirimkan lalu lintas komunikasi melalui internet dan melacak perubahan dalam proses tersebut. Saat informasi tersebut kembali ke *router, router* akan membalikkan perubahan tersebut dari alamat IP publik menjadi alamat IP pribadi dan meneruskan lalu lintas kembali ke komputer.

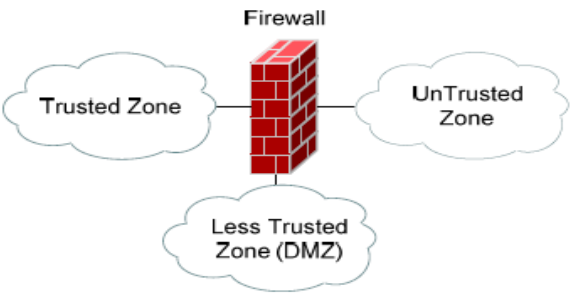
Penutup

Firewall tidak terbatas hanya pada dua zona, tetapi dapat berisi beberapa zona yang 'kurang terpercaya', yang sering disebut sebagai Zona Demiliterisasi (DMZ).

Untuk mengendalikan nilai kepercayaan setiap zona, setiap antarmuka *firewall* diberi tingkat keamanan, yang sering kali direpresentasikan sebagai nilai numerik atau bahkan warna. Misalnya, Zona Terpercaya dapat diberi nilai keamanan 100, Zona Kurang Terpercaya nilai 75, dan Zona Tidak Terpercaya nilai 0.

Lalu lintas dari zona keamanan yang lebih tinggi ke zona keamanan yang lebih rendah (umumnya) diizinkan secara *default*, sementara lalu lintas dari zona keamanan yang lebih rendah ke zona keamanan yang lebih tinggi memerlukan izin eksplisit.

Ada banyak cara untuk membangun jaringan dengan DMZ. Dua metode utama adalah *firewall* atau *firewall* ganda. Masing-masing sistem ini dapat diperluas untuk membuat arsitektur kompleks yang dibangun untuk memenuhi persyaratan jaringan. *Firewall* tunggal dengan beberapa *port* dapat digunakan untuk menerapkan DMZ logis.



Gambar 5.7: NAT *Terminology Example*
Sumber: *Introduction to Firewalls* v1.01-Aaron Balchunas.

DMZ yang lebih aman (disebut sebagai *subnet* yang disaring) menggunakan beberapa *firewall*:

Gambar 5.8: NAT *Terminology Example*
Sumber: *Introduction to Firewalls* v1.01-Aaron Balchunas.

Firewall adalah produk keamanan jaringan yang memantau dan menyaring lalu lintas jaringan internal atau keluar sesuai dengan kebijakan keamanan organisasi. *Firewall* merupakan dinding antara jaringan internal pribadi dan Internet publik. *Firewall* sangat penting untuk keamanan jaringan dan digunakan di lingkungan perusahaan dan pribadi. Sebagian besar sistem operasi memiliki *firewall* bawaan dasar. Namun, perlindungan menggunakan aplikasi *firewall* pihak ketiga lebih baik dan lebih bisa diandalkan.

Daftar Pustaka

Balchunas, Aaron., (2007). *Introduction to Firewalls v1.01,. [White Paper].* Retrieved from <http://www.routeralley.com/>.

https://www.geeksforgeeks.org/what-is-a-proxy-firewall/.

https://www.paloaltonetworks.com/cyberpedia/what-is-a-stateful-firewall.

https://www.tufin.com/blog/packet-filtering-firewall-basics-benefits.

https://www.vmware.com/topics/network-address-translation.

SS, Sweta., Rajita, G.Puspha., Sharma, Arkita., Krisna, G. Rama., *Network security and firewall. National Conference on Internet of Things* (IoT)-2K18. Retrived from https://www.smec.ac.in/assets/images/committee/research/17-18/514.Implementation%20and%20Management%20of%20framework%20for%20PaaS%20in%20Cloud%20Computing.pdf.

PROFIL PENULIS

Martono, S.Pd.Kim., M.TI.

Ketertarikan penulis pada bidang komputer awalnya hanya karena hobi dan iseng-iseng. Sambil menyelesaikan Pendidikan Kimia jenjang Diploma 3 di IKIP Jakarta pada saat itu penulis juga mengikuti pelatihan elektronika komputer. Belajar tentang jaringan komputer dimulai dari era *Novell Netware* dan *Microsoft NT 4.0* pada saat jaringan LAN yang masih populer menggunakan *Cable Coaxial* hingga kini era jaringan menggunakan *Wifi* dan *Fiber Optics*, hal tersebut lebih karena tuntutan pekerjaan. Pendidikan D3 diselesaikan di IKIP Jakarta dan S1 diselesaikan di Universitas Terbuka pada tahun 2006 masih pada Jurusan yang sama yakni Pendidikan Kimia. Penulis kemudian melanjutkan Pendidikan S2 di STMIK Raharja (sekarang sudah jadi Universitas Raharja) pada program studi Teknik Informatika dan selesai pada tahun 2017. Awalnya penulis bekerja di Perusahaan yang merupakan vendor di bidang Teknologi Informasi yang melayani berbagai organisasi pendidikan dan perusahaan.

Kemudian penulis berlanjut bergabung dengan perusahaan Teknologi Informasi yang memberikan pelatihan-pelatihan kepada sekolah-sekolah dan juga mengembangkan *Software-Software* Pendidikan dan Pelatihan Robotika. Dari sini penulis akhirnya banyak melakukan eksplorasi *software,* Mikrokontroler dan Robotika serta terlibat baik secara langsung maupun tidak langsung dalam pengembangan *software.* Beberapa tulisan ringan ditulis dalam bentuk *blog* dan sering menggunakan *nickname* martonokita. Adapun tulisan ilmiahnya telah diterbitkan dalam beberapa buku dan dalam beberapa Jurnal Ilmiah. Selain memberikan pelatihan, penulis juga mengajar di SMKN 4 Depok dan Universitas Raharja dan juga Kampus swasta lainnya.

Email Penulis: martono@raharja.info.

BAB 6
VIRTUAL PRIVATE NETWORK (VPN)

Zumhur Alamin, S.Kom., M.Kom.
Universitas Muhammadiyah Bima

Penggunaan internet sebagai tulang punggung komunikasi menjamin keandalan layanan. Jika sebuah *node* atau jalur antara *router* gagal, jalur logis secara sederhana dan transparan diubah untuk pengguna. Internet juga memberikan manfaat lebih lanjut bagi pengguna VPN, karena bahkan lokasi yang sangat terpencil pun memiliki akses ke internet melalui modem *dial-up*.

VPN menjamin komunikasi yang aman untuk pengguna *dial-in* (Alamin & Mu'min, 2024). Pengguna seluler mungkin tidak dapat menggunakan *leased lines* untuk terhubung dengan situs perusahaan, sehingga satu-satunya kebutuhan adalah terhubung ke internet dan menggunakan jaringan publik untuk melakukan *tunneling* koneksi privat dengan aman (Sharma & Kaur, 2020).

Manfaat VPN

Penggunaan VPN menawarkan berbagai manfaat signifikan, terutama dalam aspek peningkatan privasi, keamanan data, dan kemampuan untuk mengatasi pembatasan geografis. Di era *digital* saat ini, di mana sejumlah besar informasi pribadi tersebar di internet, perlindungan terhadap privasi daring menjadi semakin krusial guna menjaga keamanan aktivitas dan identitas pengguna (Cho, 2024).

VPN berperan dalam meningkatkan privasi *online* melalui enkripsi terhadap seluruh lalu lintas internet, sehingga data sensitif tetap terlindungi dan tidak dapat dipantau oleh pihak ketiga, termasuk penyedia layanan internet (ISP). Tanpa perlindungan dari VPN, situs *web*, pengiklan, dan ISP memiliki kemampuan untuk melacak lokasi serta kebiasaan penelusuran pengguna. Dengan menyamarkan alamat IP, VPN dapat mengurangi risiko iklan bertarget, pengawasan, dan praktik pengumpulan data yang invasif.

Alamat IP sendiri mengandung informasi tentang lokasi dan riwayat penelusuran yang dapat diakses oleh situs *web* melalui *cookie* dan teknologi pelacakan lainnya. Koneksi melalui VPN menyembunyikan alamat IP tersebut sehingga memungkinkan tingkat anonimitas yang lebih tinggi saat berselancar di internet (Stieglitz, 2025).

Meskipun demikian, perlu dicermati bahwa klaim sebagian penyedia layanan VPN mengenai kebijakan tanpa pencatatan data (*no-*

sebaliknya, umumnya memiliki fitur terbatas dan dukungan pelanggan yang minim atau tidak ada. Tabel 6.2. berikut merangkum perbandingan antara layanan VPN gratis dan berbayar:

Tabel 6.2: Perbandingan VPN Gratis dan Berbayar

Fitur	VPN Gratis	VPN Berbayar
Keamanan	Enkripsi lebih lemah, risiko *malware.*	Enkripsi kuat (AES-256), fitur keamanan canggih.
Privasi	Kebijakan *log* yang meragukan, penjualan data.	Kebijakan tanpa log yang ketat.
Kecepatan	Lebih lambat, *server* padat.	Lebih cepat, banyak *server.*
Batas Data	Seringkali terbatas.	Tidak terbatas.
Jumlah *Server*	Terbatas.	Banyak, di berbagai lokasi.
Dukungan Pelanggan	Minim atau tidak ada.	24/7 melalui berbagai saluran.
Fitur Tambahan	Terbatas.	Pemblokir iklan/*malware*, *split tunneling,* dll.

Sumber: Diolah Penulis.

Secara keseluruhan, meskipun VPN gratis mungkin cocok untuk penggunaan sesekali atau kebutuhan dasar, VPN berbayar umumnya merupakan pilihan yang lebih baik bagi pengguna yang memprioritaskan keamanan, privasi, kecepatan, dan fitur tambahan.

Memaksimalkan Keamanan dan Privasi Dengan VPN

Jaringan Privat Virtual (VPN) telah menjadi alat yang sangat diperlukan dalam lanskap *digital* saat ini, menawarkan pengguna kemampuan untuk meningkatkan keamanan, privasi, dan akses ke konten *online*.

Dari definisi dasarnya sebagai ekstensi jaringan privat melalui jaringan publik yang tidak terpercaya hingga berbagai manfaatnya seperti enkripsi data, penyembunyian alamat IP, dan melewati batasan geografis, VPN memainkan peran penting bagi individu dan organisasi. Berbagai kasus penggunaan VPN, mulai dari penjelajahan

pribadi yang aman dan akses ke konten yang dibatasi hingga akses jarak jauh yang aman untuk bisnis, menunjukkan fleksibilitas dan pentingnya teknologi ini.

Pemahaman tentang berbagai protokol VPN seperti *OpenVPN*, *WireGuard*, dan *IPsec*, bersama dengan kekuatan dan kelemahan masing-masing, memberdayakan pengguna untuk membuat pilihan yang tepat berdasarkan kebutuhan spesifik mereka. Namun, penting untuk menyadari potensi risiko dan batasan penggunaan VPN, termasuk potensi pencatatan aktivitas pengguna oleh beberapa penyedia dan kemungkinan penurunan kecepatan. Memilih penyedia VPN yang tepat memerlukan pertimbangan cermat terhadap faktor-faktor seperti fitur keamanan, kebijakan privasi, lokasi server, kecepatan, dan biaya.

Selain itu, kesadaran akan legalitas penggunaan VPN di berbagai negara sangat penting untuk menghindari potensi masalah hukum. Perbandingan antara layanan VPN gratis dan berbayar menyoroti *trade-off* penting dalam hal keamanan, kecepatan, dan batas data. Sementara VPN gratis mungkin menawarkan akses dasar, VPN berbayar umumnya memberikan pengalaman yang lebih aman, cepat, dan andal dengan fitur tambahan dan dukungan pelanggan yang lebih baik.

Ke depan, teknologi VPN terus berkembang, dengan penelitian dan pengembangan yang berfokus pada integrasi kecerdasan buatan (AI) untuk deteksi ancaman yang lebih baik dan peningkatan kinerja, serta pengembangan solusi VPN yang tahan terhadap ancaman komputasi kuantum di masa depan. Dengan tetap mengikuti perkembangan ini dan memilih penyedia VPN yang tepat, pengguna dapat memaksimalkan keamanan dan privasi mereka di lanskap *digital* yang terus berubah.

Daftar Pustaka

Alamin, Z., & Mu'min, M. A. (2024). *Memahami dan Menguasai Jaringan Komputer* (R. Missouri (ed.). PT. Mafy Media Literasi Indonesia.

Angelo, R. (2019). Secure Protocols And Virtual Private Networks: An Evaluation. *Issues In Information Systems*. https://doi.org/10.48009/3_iis_2019_37-46.

Cho, S. A. (2024). *The Power of Virtual Private Networks (VPN) in Privacy Protection | Office of Information Security | Washington University in St. Louis*. https://informationsecurity.wustl.edu/the-power-of-virtual-private-networks-vpn-in-privacy-protection/,

Ernszt, R. (2024). *Free VPN vs paid VPN: Why Pay When It's Free?* Comparitech.Com. https://www.comparitech.com/blog/vpn-privacy/free-vpn-vs-paid-vpn/.

Karuna Jyothi, K., & Reddy, B. I. (2018). Study on Virtual Private Network (VPN), VPN's Protocols And Security. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*.

Lamb, N. (2025). *Are VPNs Legal? Your Guide to VPN Legality*. ExpressVPN. https://www.expressvpn.com/blog/are-vpns-legal/.

Lekander, A. (2025). *VPN Protocols: OpenVPN vs IPSec, WireGuard, L2TP, & IKEv2 %*. Cyber Insider. https://cyberinsider.com/vpn/openvpn-ipsec-wireguard-l2tp-ikev2-protocols/.

Liu, Z. (2023). Application and Security Analysis of Virtual Private Network (VPN) in Network Communication. *Academic Journal of Computing & Information Science*, *6*(11). https://doi.org/10.25236/AJCIS.2023.061108.

Pattison, S. (2024). *Are VPNs Legal in 2025? It Depends on Where You Live*. Privacyjournal.Net. https://www.privacyjournal.net/are-vpns-legal/.

Sharma, Y. K., & Kaur, C. (2020). The Vital Role of Virtual Private Network (VPN) in Making Secure Connection Over Internet World. *International Journal of Recent Technology and Engineering (IJRTE)*, *8*(6), 2336–2339.

https://doi.org/10.35940/ijrte.F8335.038620.

Stieglitz, S. (2025). *7 Benefits of a VPN: Advantages of Using Virtual Private Networks*. ExpressVPN. https://www.expressvpn.com/blog/benefits-of-vpn/.

Triukose, S., Wen, Z., & Rabinovich, M. (2009). Content delivery networks. *ACM SIGMETRICS Performance Evaluation Review*, *37*(2), 59–60. https://doi.org/10.1145/1639562.1639585.

University, E.-C. (2025). *What Are the Downsides of Using a Free VPN? Are Free VPN Safe*. Eccu.Edu. https://www.eccu.edu/blog/cybersecurity/5-reasons-why-you-should-not-use-free-vpns/.

Venkateswaran, R. (2001). Virtual Private Networks. *IEEE Potentials*, *20*(1), 11–15.

Yang, H. (2022). Application of Hybrid Encryption Algorithm in Hardware Encryption Interface Card. *Security and Communication Networks*, *2022*, 1–11. https://doi.org/10.1155/2022/7794209.

PROFIL PENULIS

Zumhur Alamin, M.Kom.

Minat penulis terhadap ilmu komputer dimulai pada tahun 2005. Penulis memulai perjalanan pendidikan di Universitas Muhammadiyah Malang, mengambil jurusan Sarjana Teknik Informatika, dan berhasil meraih gelar sarjana pada tahun 2009. Pada tahun 2014 awal, penulis melanjutkan studi pada program magister Ilmu Komputer (M.Kom.) di Universitas Budi Luhur Jakarta dan berhasil menyelesaikan studi tahun 2015. Sebagai anak kedua dari enam bersaudara dari pasangan Ir. Zainuddin H. Hamzah dan Nurjanah, S.Sos, S.Pd., penulis telah menunjukkan komitmennya dalam dunia akademis. Kini, sebagai seorang dosen di Program Studi Ilmu Komputer di Universitas Muhammadiyah Bima sejak tahun 2022, penulis mengampu berbagai mata kuliah, termasuk Algoritma dan Pemrograman, serta memiliki ketertarikan di bidang *Software Engineering, Data Science* dan *Computer Network*. Untuk mewujudkan karir sebagai dosen profesional, penulis aktif sebagai peneliti di bidang kepakarannya tersebut. Selain peneliti, penulis juga aktif menulis buku dengan harapan dapat memberikan kontribusi positif bagi bangsa dan negara yang sangat tercinta ini.

Email Penulis: zumhur.alamin@gmail.com.

BAB 7
KEAMANAN PROTOKOL JARINGAN

Aliyah, S.Kom., M.T.I.
Universitas Cendekia Abditama

Latar Belakang Keamanan Protokol Jaringan

Penggunaan *firewall* menjadi krusial dalam mengurangi risiko keamanan jaringan. Ada tiga konfigurasi *firewall* utama: *firewall host system (single-homed bastion)*, *firewall host system (dual-homed bastion)*, dan *firewall subnet*. *Firewall* bekerja dengan menyaring paket data berdasarkan kebijakan yang telah ditetapkan, sehingga hanya koneksi yang diizinkan yang dapat melewati jaringan.

Proses *filtering* ini memungkinkan *firewall* untuk mengontrol akses internet dan memantau aktivitas jaringan. Penelitian menunjukkan bahwa *firewall* yang dikonfigurasikan dengan tepat, menggunakan teknik *filtering* dan *proxy*, mampu melindungi jaringan secara efektif. Tujuan utamanya adalah mengoptimalkan sistem keamanan firewall, terutama di jaringan *wide area* (WAN), dengan memanfaatkan konfigurasi *two host home*, *shrouded host*, dan *shrouded subnet*.

Protokol jaringan menjadi elemen penting dalam komunikasi digital karena mengatur bagaimana data dikemas, dikirim, diterima, dan ditafsirkan oleh perangkat yang terhubung. Namun, dalam praktiknya, protokol jaringan juga dapat menjadi pintu masuk bagi serangan siber jika tidak dirancang atau dikonfigurasi dengan benar. Adapun ruang lingkup pembahasan dalam tulisan ini meliputi:

1. **Pengenalan Protokol Jaringan**

   Pada bagian ini, akan dijelaskan tentang definisi protokol jaringan, serta peran dan fungsinya dalam sistem komunikasi data. Protokol seperti TCP/IP, HTTP, FTP, dan DNS akan diperkenalkan untuk memberikan gambaran mengenai bagaimana perangkat berkomunikasi satu sama lain dalam sebuah jaringan. Fokus juga akan diberikan pada bagaimana protokol-protokol tersebut menjadi fondasi dari internet dan jaringan lokal saat ini.

2. **Ancaman dan Kerentanan Dalam Protokol Jaringan**

   Bagian ini membahas berbagai serangan yang mengeksploitasi kelemahan protokol jaringan. Contohnya adalah:

   a. *Sniffing*, di mana penyerang menangkap data yang sedang ditransmisikan.

Protokol yang Aman dan Mekanismenya

Protokol jaringan yang aman dirancang untuk melindungi komunikasi data dari berbagai ancaman seperti penyadapan, pemalsuan data, dan penyusupan. Protokol ini mengandalkan berbagai mekanisme keamanan seperti enkripsi, otentikasi, dan integritas data. Penggunaan protokol aman sangat penting, terutama dalam:

1. Transaksi finansial.
2. Pengelolaan *server*.
3. Pengiriman data sensitif.
4. Akses ke sistem informasi organisasi.

Pemahaman dan implementasi yang tepat atas protokol keamanan ini akan secara signifikan menurunkan risiko kebocoran data, penyadapan, dan serangan siber lainnya.

Daftar Pustaka

Andri, A., Gunawan, I., & Kirana, I. O. (2022). Optimization of Computer Network Security System Against Malware Attacks Using Firewall Filtering with Port Blocking Method. *JOMLAI: Journal of Machine Learning and Artificial Intelligence*, *1*(2), 133-142.

Andri, I. G., & Kirana, I. O. (2022). Optimasi Sistem Keamanan Jaringan Komputer Terhadap Serangan Malware Menggunakan Filtering Firewall dengan Metode Port Blocking Optimization of Computer Network Security System Against Malware Attacks Using Firewall Filtering with Port Blocking Method Art. *JOMLAI J. Mach. Learn. Artif. Intell*, *1*(2), 2828-9099.

Dewi, S. (2020). Keamanan Jaringan Menggunakan VPN (Virtual Private Network) Dengan Metode PPTP (Point To Point Tunneling Protocol) Pada Kantor Desa Kertaraharja Ciamis. *EVOLUSI: Jurnal Sains dan Manajemen, 8(1).*

Fahmi, A. (2021). Rancang Bangun Sistem Keamanan Kapal Kargo Untuk Mendeteksi Pergerakan Mencurigakan Berbasis Internet of Thing. *(Doctoral Dissertation, Universitas Islam Negeri Sultan Syarif Kasim Riau*).

Nashrullah, M. R., Primananda, R., & Widasari, E. R. (2018). Implementasi Wireless Sensor Network Pada Keamanan Rumah Menggunakan Sensor Pir. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, *2*(12), 7322-7330.

Rolando, R. (2018). Analisis Kelemahan Protokol Wireless dengan Metode Brute Force Attack di Kali Linux. (Studi Kasus Jaringan Wireless di Kota Batam). (*Doctoral Dissertation, Prodi Teknik Informatika*).

Satria, D. E., Hanafi, F. W., San Putra, M. J., & Novantoro, Y. A. (2024). *Analisa Keamanan dan Privasi Data Pada Sistem Penyimpanan Icloud*.

Zaerani, A., Samsumar, L. D., Karim, M. N., & Suryadi, E. (2024). Analisis Sistem Keamanan Wireless Local Area Network (WLAN) Menggunakan Akses Tethering: Analisis Sistem Keamanan Wireless Local Area Network (WLAN) Menggunakan Akses Tethering. *Jurnal Rekayasa Sistem Informasi dan Teknologi*, *2*(1), 588-594.

PROFIL PENULIS

Aliyah, S.Kom., M.T.I.

Ketertarikan penulis terhadap ilmu komputer dimulai pada tahun 2000 silam. Hal tersebut membuat penulis memilih untuk masuk ke Sekolah Menengah Kejuruan di SMK Pelita Utama Gedung Tataan Kabupaten Pesawaran dengan memilih Jurusan Sekretaris dan berhasil lulus pada tahun 2003. Penulis kemudian melanjutkan pendidikan ke Perguruan Tinggi dan berhasil menyelesaikan studi S1 di prodi Sistem Informasi STMIK Insan Pembangunan dan berhasil lulus pada tahun 2018. Dua tahun kemudian, penulis menyelesaikan studi S2 di prodi Teknik Informatika Program Pascasarjana Universitas Raharja. Tiga tahun kemudian, penulis kuliah S3 ilmu komputer di Universitas. Penulis memiliki kepakaran dibidang *Web Technology* dan *Data Science*. Guna mewujudkan karir sebagai dosen profesional, penulis pun aktif sebagai peneliti di bidang kepakarannya tersebut. Beberapa penelitian yang telah dilakukan didanai oleh internal perguruan tinggi dan juga Kemenristek DIKTI. Selain peneliti, penulis juga aktif menulis buku dengan harapan dapat memberikan kontribusi positif bagi bangsa dan negara yang sangat tercinta ini. Atas dedikasi dan kerja keras dalam menulis buku, Perpustakaan Nasional RI memberikan penghargaan sebagai salah satu Pemenang Buku Terbaik Tahun 2018.

Email Penulis: aliyah@uca.ac.id.

BAB 8
SERANGAN *MAN IN THE MIDDLE* (MITM) DAN PENCEGAHANNYA

Diki Arisandi, S.Kom., M.Kom.
Universitas Muhammadiyah Riau

Pendahuluan

Perkembangan teknologi *digital* telah membawa kemudahan dalam berkomunikasi, bertransaksi, dan mengakses berbagai layanan daring. Namun, kemajuan ini juga diiringi oleh meningkatnya risiko keamanan informasi, terutama yang terkait dengan komunikasi data melalui jaringan. Salah satu ancaman yang semakin kompleks dan sulit dideteksi adalah serangan *Man In The Middle* (MITM).

Serangan ini memungkinkan pihak ketiga untuk menyusup ke dalam proses komunikasi dua arah tanpa sepengetahuan kedua pihak, dengan tujuan untuk menyadap, mencuri, bahkan memodifikasi informasi yang dipertukarkan. Fenomena MITM menjadi semakin relevan dalam penggunaan jaringan publik yang masif, serta rendahnya kesadaran keamanan *digital* di kalangan pengguna dan pengelola jaringan.

Bab ini akan mengulas secara komprehensif mengenai serangan MITM, mulai dari definisi, motivasi pelaku, kerentanan jaringan, hingga dampak serta strategi pencegahannya, termasuk pendekatan terkini berbasis kecerdasan buatan (AI).

Apa Itu *Man In The Middle* (MITM)?

Serangan MITM merupakan salah satu jenis serangan siber yang berbahaya karena dilakukan dengan menyusup ke jalur komunikasi antara dua pihak tanpa sepengetahuan mereka. Dalam skema ini, penyerang bertindak sebagai perantara yang tidak sah, namun mampu memantau, merekam, bahkan memodifikasi informasi yang ditransmisikan (Ylli & Fejzaj, 2021), seperti pada gambar 8.1. komunikasi tetap tampak normal di mata korban, padahal data yang dikirim dan diterima telah diakses atau diubah oleh pelaku.

Serangan ini bisa terjadi baik dalam jaringan lokal, seperti Wi-Fi publik, maupun dalam komunikasi berbasis internet melalui situs web dan aplikasi daring (Cekerevac et al., 2025). Kesulitan utama dalam menghadapi MITM terletak pada sifatnya yang diam-diam dan sulit dideteksi secara langsung oleh pengguna yang awam (Fereidouni et al., 2025).

Hasil Riset Terbaru Deteksi dan Pencegahan MITM

Dalam beberapa tahun terakhir, pendekatan berbasis kecerdasan buatan (*Artificial Intelligence*/AI) dengan merujuk kepada fitur, ciri unik, maupun pola perilaku MiTM mulai banyak diterapkan (Arisandi et al., 2021).

Berbeda dengan metode konvensional yang bergantung pada daftar tanda tangan (*signature-based detection*), metode AI mampu menganalisis pola lalu lintas jaringan secara *real-time* dan mengidentifikasi anomali yang mencurigakan meskipun belum pernah dikenali sebelumnya. Pendekatan ini memungkinkan sistem untuk mendeteksi serangan MITM yang bersifat baru dan kompleks (Ahmed, 2024).

Serangan MITM saat ini juga dikenal dalam bentuk *Rogue Access Point* (RAP). Beberapa studi menunjukkan bahwa algoritma pembelajaran mesin dan *Neural Networks* dapat digunakan untuk mendeteksi pola komunikasi yang tidak wajar, seperti perubahan mendadak dalam rute data atau kejanggalan dalam proses enkripsi. Sistem *Intrusion Detection System* (IDS) berbasis AI juga semakin banyak dikembangkan, sehingga dapat mendeteksi keberadaan MiTM ini.

Penelitian dari Arisandi (Arisandi et al., 2025) mengangkat permasalahan keamanan jaringan terkait keberadaan *Man-in-the-Middle* (MiTM) berwujud *Rogue Access Points* (RAP) yang dapat meniru jaringan Wi-Fi sah dan mengancam data sensitif pengguna. Untuk menjawab tantangan ini, dikembangkanlah mekanisme bernama *Invisible Scout* yang mampu mendeteksi RAP secara akurat dalam berbagai skenario, termasuk lingkungan terkendali, lingkungan nyata, serta saat terjadi serangan *de-authentication.*

Invisible Scout bekerja tanpa perangkat keras tambahan dengan mengandalkan model *decision tree* yang memanfaatkan fitur seperti OUI *Number, Retry Bit*, dan status IBS S untuk mengklasifikasikan AP sebagai sah atau *rogue*. Mekanisme ini terdiri dari modul *sniffer*, deteksi, *probing*, dan perbandingan terhadap basis data pola normal, dan terbukti efektif dengan akurasi klasifikasi mencapai 0,875 dan AUC sebesar 0,921, meskipun masih menghadapi tantangan dalam membedakan beberapa kelas RAP tertentu.

di lingkungan publik. Selanjutnya, Yang memperdalam pendekatan dengan memanfaatkan sidik jari fisik berbasis *Channel State Information* (CSI) dan algoritma *deep learning* untuk menjawab tantangan kompleksitas dan dinamika lingkungan IoT modern.

Sementara itu, Lu melengkapi arah tersebut dengan memperkuat aspek kestabilan dan keunikan sidik jari fisik melalui pemodelan rentang *drift* kesalahan fase, guna meningkatkan akurasi dan mengurangi kesalahan deteksi. Ketiganya bergerak ke arah yang sama: menciptakan sistem deteksi yang semakin cerdas, tangguh, dan adaptif terhadap kondisi dunia nyata, dengan tahapan peningkatan dari praktis, canggih, hingga stabil.

Daftar Pustaka

Ahmed, A. A. (2024). AI in Combatting Man-in-the-Middle Attacks: A Comprehensive Review. *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, 1–6. https://doi.org/10.1109/ICCCNT61001.2024.10725789.

Almon, L., Krause, A. M., Fietze, O., & Hollick, M. (2021). Desynchronization And MITM Attacks Against Neighbor Awareness Networking Using Opennan. *Proceedings of the 19th ACM International Symposium on Mobility Management and Wireless Access*, 97–105.

Arisandi, D., Ahmad, N. M., & Kannan, S. (2021). The Rogue Access Point Identification: A Model And Classification Review. *Indonesian Journal of Electrical Engineering and Computer Science*, *23*(3), 1527–1537. https://doi.org/10.11591/ijeecs.v23.i3.pp1527-1537.

Arisandi, D., Ahmad, N. M., & Kannan, S. (2025). Invisible Scout: A Layer 2 Anomaly System for Detecting Rogue Access Point (RAP). *Emerging Science Journal*, *9*(1), 284–310. https://doi.org/10.28991/ESJ-2025-09-01-016.

Astuti, N. R. D. P., Natsir, F., Haris, M. S., Ramdhani, Y., Aribowo, E., Anwar, N., Santoso, K. I., Rokhmah, S., Ismanto, E., & Hasan, F. N. (2025). *Keamanan Data dalam Revolusi Teknologi*. PT Penerbit Qriset Indonesia.

Budiyanto, B., & Iftitah, A. (2025). *Pengantar Cybercrime Dalam Sistem Hukum Pidana di Indonesia*. Sada Kurnia Pustaka.

Cekerevac, Z., Cekerevac, P., Prigoda, L., & Al-Naima, F. (2025). Security Risks From The Modern Man-In-The-Middle Attacks. *MEST Journal*, *13*(1), 34–51. https://doi.org/10.12709/mest.13.13.01.04.

Fereidouni, H., Fadeitcheva, O., & Zalai, M. (2025). IoT and Man-in-the-Middle Attacks. *Security and Privacy*, *8*(2), 1–19. https://doi.org/https://doi.org/10.1002/spy2.70016.

Kondracki, B., Azad, B. A., Starov, O., & Nikiforakis, N. (2021). Catching

Transparent Phish: Analyzing and Detecting MITM Phishing Toolkits. *Proceedings of the ACM Conference on Computer and Communications Security*, 36–50. https://doi.org/10.1145/3460120.3484765.

Lu, Q., Li, S., Zhang, J., & Jiang, R. (2022). PEDR: Exploiting Phase Error Drift Range To Detect Full-Model Rogue Access Point Attacks. *Computers and Security*, *114*, 102581. https://doi.org/10.1016/j.cose.2021.102581.

Mukhra, U., Makruf, J., Kesuma, T., Nizam, A., & Siregar, M. (2024). *Mobile Banking dalam Persepsi Privasi Nasabah*. Syiah Kuala University Press.

Panda, D., Kishore Mishra, B., & Sharma, K. (2022). A Taxonomy on Man-in-the-Middle Attack in IoT Network. *Proceedings - 2022 4th International Conference on Advances in Computing, Communication Control and Networking, ICAC3N 2022*, 1907–1912. https://doi.org/10.1109/ICAC3N56670.2022.10074170.

Sen, O., Van Der Veldc, D., Linnartz, P., Hacker, I., Henze, M., Andres, M., & Ulbig, A. (2021). Investigating Man-in-the-Middle-based False Data Injection in a Smart Grid Laboratory Environment. *Proceedings of 2021 IEEE PES Innovative Smart Grid Technologies Europe: Smart Grids: Toward a Carbon-Free Future, ISGT Europe 2021*. https://doi.org/10.1109/ISGTEurope52324.2021.9640002.

Shah, M. S. M., Leau, Y. B., Anbar, M., & Bin-Salem, A. A. (2023). Security and Integrity Attacks in Named Data Networking: A Survey. *IEEE Access*, *11*(January), 7984–8004. https://doi.org/10.1109/ACCESS.2023.3238732.

Steiner-Otoo, D., & Jahankhani, H. (2022). An Investigation Into How Smartphones Can Be Secured Against MiTM Attacks: Financial Sector. In *Blockchain And Other Emerging Technologies For Digital Business Strategies* (pp. 171–215). Springer.

Sulianta, F. (2025). *Literasi Digital Tingkat Lanjut - Computer Security*. Feri Sulianta.

Tommasi, F., Catalano, C., & Taurino, I. (2022). Browser-in-the-Middle (BitM) attack. *International Journal of Information Security*, *21*(2), 179–189.

Tyagi, V., Saraswat, A., Kumar, A., & Gambhir, S. (2024). Securing IoT Devices Against MITM and DoS Attacks. *Reshaping Intelligent Business and Industry*, 237–249. https://doi.org/10.1002/9781119905202.ch15.

Ul-Aaish, S., Pires, I. M., Godinho, A., Coelho, P. J., & Butt, P. K. (2024). Client Risk Assessment in a Network: An Examination of Man-in-the-Middle Attacks and Their Usage. *International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, *September*, 793–800. https://doi.org/10.1109/EECSI63442.2024.10776323.

Xhemajli, N., & Tafa, Z. (2024). Mobile Proxy in Public WiFi Networks: A Tool Against MITM Attacks. *2024 13th Mediterranean Conference on Embedded Computing, MECO 2024*, *June*, 1–5. https://doi.org/10.1109/MECO62516.2024.10577803.

Yang, Z., Lu, Q., Zhang, H., Chen, F., & Xian, H. (2024). Eliminating Rogue Access Point Attacks in IoT : A Deep Learning Approach With Physical-Layer Feature Purification and Device Identification. *IEEE Internet of Things Journal*, *11*(8), 14886–14900. https://doi.org/10.1109/JIOT.2023.3345378.

Ylli, E., & Fejzaj, J. (2021). Man in the Middle: Attack and Protection. *CEUR Workshop Proceedings*, *2872*(May), 198–204.

PROFIL PENULIS

Diki Arisandi, S.Kom., M.Kom.

Penulis memulai ketertarikan pada bidang ilmu komputer setelah menyelesaikan pendidikan menengah atas di SMA N 1 Bintan Timur, Kepulauan Riau. Saat ini penulis memiliki ketertarikan pada bidang IoT, jaringan nirkabel, keamanan siber, dan optimasi IT dalam bidang pendidikan. Penulis menyelesaikan pendidikan S1 di Universitas Abdurrab pada tahun 2010, dan memperoleh gelar Sarjana Komputer. Penulis melanjutkan studinya dan meraih gelar Magister Ilmu Komputer dari UPI "YPTK" Padang pada tahun 2013. Saat ini, penulis sedang menempuh studi S3 di Multimedia University, Malaysia, dengan riset terkait keamanan jaringan nirkabel.

Penulis saat ini ber homebase di Universitas Muhammadiyah Riau dan memiliki pengalaman mengajar di beberapa kampus diantaranya: Universitas Abdurrab, Universitas Islam Riau, AMIK Tri Dharma Pekanbaru, *President University*, serta Universitas Terbuka. Mata kuliah yang diajarkannya meliputi Jaringan Komputer, Komunikasi Data, Kemanan Komputer, Algoritma dan Struktur data, Bahasa Pemrograman, Media Pembelajaran, Sistem Informasi Manajemen, Matematika Bisnis, dan Kewirausahaan. Selain mengajar, penulis juga aktif dalam penelitian dan pengabdian masyarakat. Penulis telah menerima berbagai hibah penelitian dari pendanaan hibah internal universitas maupun dari Kementerian Riset, Teknologi, Pendidikan, dan Kebudayaan, seperti hibah dosen pemula, penelitian tingkat lanjut, penelitian fundamental, penelitian terapan, serta hibah pengabdian ipteks bagi masyarakat. Selain itu, penulis juga memiliki beberapa karya buku ajar dan buku referensi terkait dengan bidang informatika, yang berasal dari kegiatan tridharma penulis.

Email Penulis: diki1985@gmail.com.

BAB 9
HARDENING SYSTEM

Lindung Siswanto, S.Kom., M.Eng.
Politeknik Negeri Pontianak

Pengantar *Hardening System*

Hardening System merupakan upaya meningkatkan keamanan sistem komputer yang meliputi perangkat keras, perangkat lunak (sistem operasi, aplikasi, sistem informasi dll) dan jaringan komputer dengan cara mengurangi atau menghilangkan kerentanan dengan melakukan konfigurasi atau pengaturan tertentu secara ketat. Hal ini bertujuan untuk mengurangi atau menghilangkan potensi kerentanan/ *vulnerability*, akses tidak sah, eksploitasi yang dapat dilakukan oleh penyerang.

Manfaat *hardening system* yaitu mampu mengurangi serangan permukaan (*surface attack*) misalnya XSS, SQL *injection*, DOS, *Port Scanning* dll. Meningkatkan keberhasilan penanganan serangan, mencegah kebocoran data, atau gangguan operasional. Serangan permukaan sendiri merupakan jumlah titik awal yang dapat digunakan untuk melakukan penyerangan terhadap sistem, aplikasi atau jaringan. Semakin luas *surface attack*, semakin besar kemungkinan sistem dapat dieksploitasi dan begitu pula sebaliknya.

Manfaat lain dari *hardening system* adalah membantu organisasi untuk patuh terhadap regulasi keamanan seperti ISO 27001, PCI-DSS atau NIST. Kemudian meningkatkan kemudahan pengelolaan karena konfigurasi dan layanan yang berjalan disederhanakan dan difokuskan sesuai dengan tujuan organisasi. Dalam jangka panjang, mengurangi kerugian dan menurunkan biaya operasional akibat terjadinya insiden terkait keamanan.

Teknik *Hardening System*

Teknik *hardening system* merupakan serangkaian upaya atau proses untuk meningkatkan keamanan sistem komputer dari potensi ancaman dan kerentanan. Berikut ini beberapa langkah *best practices* untuk *hardening system* yang dapat dilakukan pada sistem operasi *Windows* dan *Linux*, aplikasi maupun jaringan.

Pada langkah-langkah praktik, penulis menggunakan Sistem Operasi *Windows* 11 dan *Kali Linux* 2023.

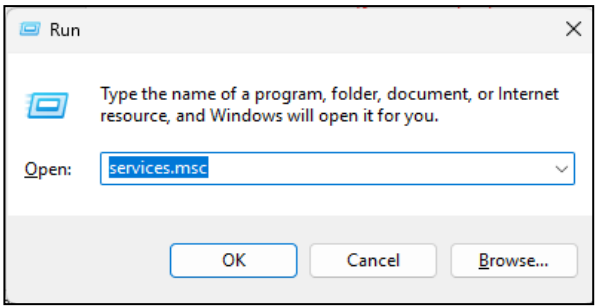
1. **Menonaktifkan Layanan yang Tidak dibutuhkan**

   Mengidentifikasi dan menonaktifkan layanan yang tidak diperlukan merupakan salah satu langkah penting untuk *hardening*

system, Berikut ini langkah-langkah yang dapat digunakan untuk mematikan layanan yang tidak dibutuhkan.

a. Sistem Operasi *Windows*

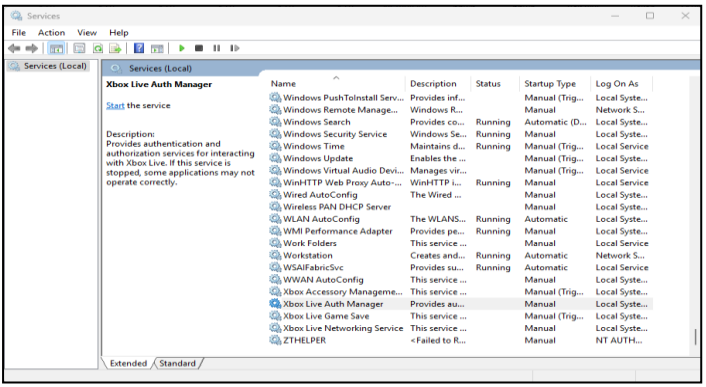
1) Tekan *Windows* + R, ketik *services.msc*, tekan *Enter*.



Gambar 9.1: Tampilan Menjalankan Perintah *Services.msc*

Sumber: Diolah Penulis.

2) Lakukan pengamatan daftar service yang sedang berjalan



Gambar 9.2: Tampilan Daftar Layanan yang ada di *Windows*

Sumber: Diolah Penulis.

Gambar 9.2 Merupakan contoh daftar layanan yang ada di sistem operasi *windows*. Jika pada bagian status terdapat "*Running*", berarti layanan tersebut sedang berjalan, dan sebaliknya jika tidak ada keterangan status maka layanan tidak sedang berjalan.

Daftar Pustaka

Fikri Muhammad Arifin. *Security Hardening*. i-3.co.id.

Linuxhackingid. *Practical Linux Security Hardening*. Kursus Online.

Muhammad Reza et al., (2024). Hardening Server Menggunakan Metode Port Knocking Pada Sistem Program Studi Teknik Informatika Universitas Muhammadiyah Ponorogo, *Jurnal Ilmiah Informatika Komputer*, Desember 2024.

Onno Center. *20 Linux Server Hardening Security Tips*. OnnoWiki.

Reza Rivaldo Fakhry. (2023). *Penerapan Keamanan Server dengan Teknik Hardening pada Sistem Operasi Ubuntu*, Eprints UMS, 2023.

Seth T. Ross. (1999). *Unix System Security Tools*.

Ubuntu Documentation. (n.d.). *File permissions. Ubuntu Community Help Wiki*. Retrieved May 19, 2025, from https://help.ubuntu.com/community/FilePermissions.

Windows & Linux Security Hardening: *Praktik Terbaik Untuk Perlindungan Data dan Sistem*. Academia.edu.

PROFIL PENULIS

Lindung Siswanto, S.Kom., M.Eng.

Merupakan salah satu dosen tetap di Politeknik Negeri Pontianak dengan keahlian di bidang pemrograman *web, cloud* computing, dan sistem keamanan informasi. Meraih gelar Sarjana Komputer dari Sekolah Tinggi Teknologi Informasi Respati Yogyakarta yang saat ini bernama Universitas Respati Yogyakarta, dan melanjutkan pendidikan Magister Teknologi Informasi di Universitas Gadjah Mada, Yogyakarta, dengan fokus pada pengembangan sistem informasi dan teknologi keamanan. Saat ini aktif mengembangkan metode pengajaran berbasis praktik, menyusun modul pembelajaran, serta membimbing mahasiswa dalam berbagai proyek teknologi informasi. Kerap menjadi pembicara dalam seminar dan pelatihan yang berkaitan dengan pengembangan aplikasi *web* modern, penerapan keamanan jaringan, serta integrasi teknologi *cloud* dalam sistem informasi. Selain mengajar, juga terlibat dalam kegiatan penelitian dan pengabdian masyarakat di bidang teknologi informasi, khususnya pada peningkatan literasi *digital* dan keamanan data di lingkungan pendidikan dan industri lokal.

Email Penulis: lindung_siswanto@yahoo.com.

BAB 10
ETHICAL HACKING DAN *PENETRATION TESTING*

Hendri Julian Pramana, S.Kom., M.Kom.
Universitas Garut

Apa Itu *Ethical Hacking* dan *Penetration Testing*?

1. Definisi *Ethical Hacking*

Secara sederhana, *ethical hacking* adalah proses mensimulasikan serangan siber terhadap sistem komputer, jaringan, atau aplikasi dengan tujuan mengidentifikasi kerentanan sistem yang berpotensi untuk dieksploitasi oleh pihak yang tidak berwenang.

Tujuannya adalah untuk memperkuat sistem sebelum celah tersebut dikuasai oleh orang atau kelompok yang tidak memiliki hak akses dan bertanggung jawab, misalnya seperti peretas berbahaya (Singh et al., 2024).

Ethical hacking juga dikenal dengan istilah *white hat hacking* atau *penetration testing*, meskipun ada perbedaan dalam ruang lingkupnya. Dalam keamanan jaringan komputer, terdapat beberapa kategori *hacker* berdasarkan niat dan metode yang digunakan, antara lain (Sinha, 2018).

a. *White Hat Hacker:* mereka adalah *ethical hacker* yang bekerja secara legal untuk mengamankan sistem.
b. *Black Hat Hacker:* peretas yang melakukan tindakan ilegal demi keuntungan pribadi, seperti mencuri data atau menyebarkan *malware*.
c. *Grey Hat Hacker*: *hacker* yang berada di wilayah abu-abu; mereka mungkin menemukan dan melaporkan celah tanpa izin, namun tanpa niat merusak.
d. *Green Hat Hacker*: peretas pendatang baru (*newbie*) dalam dunia *hacking* yang masih belajar namun sangat antusias.
e. *Blue Hat Hacker*: umumnya bekerja di luar organisasi dan diminta untuk menguji sistem sebelum dirilis untuk publik, misalnya dalam program *bug bounty*.

Sedangkan dalam penggunaan istilah, terdapat perbedaan pula antara makna dari kata *hacker*, *craker* dan *ethical hacker* yang perlu diluruskan, yaitu sebagai berikut (Pradeep & Sakthivel, 2021):

a. *Hacker* adalah seseorang yang memiliki kemampuan teknis untuk memahami sistem dan menemukan cara kerja internalnya. Tidak semua *hacker* bersifat merusak.

2. Profesi Dalam Bidang *Ethical Hacking*

Profesi di bidang *ethical hacking* sangat beragam, mulai dari teknis hingga manajerial. Beberapa jalur karier yang umum antara lain:

a. *Penetration Tester:* melakukan pengujian keamanan sistem secara proaktif dan menyeluruh.
b. *Security Analyst:* menganalisis lalu lintas jaringan dan insiden keamanan serta menyusun kebijakan mitigasi.
c. *Red Team Specialist:* menguji kekuatan pertahanan tim keamanan internal organisasi dengan simulasi serangan nyata.
d. *Bug Bounty Hunter:* bekerja secara independen atau melalui platform seperti *HackerOne* untuk menemukan *bug* dan mendapatkan imbalan.
e. *Cyber Security Consultant:* memberikan solusi keamanan strategis dan teknis kepada klien korporat.

3. *Roadmap* Profesi *Ethical Hacking*

Bagi pemula yang tertarik memulai karir di bidang *ethical hacking*, berikut adalah roadmap belajar secara umum:

a. Pemahaman Dasar: mulai dari jaringan komputer, sistem operasi (*Linux* dan *Windows*), dan konsep keamanan informasi.
b. Belajar *Tools*: praktik menggunakan *tools* seperti *Nmap, Wireshark,* dan *Metasploit.*
c. Pelatihan dan Sertifikasi: mengikuti kursus dan pelatihan, lalu mengambil sertifikasi seperti CEH atau *PenTest+.*
d. Pengalaman Praktis: mengikuti *Capture The Flag* (CTF), *bug bounty* program, atau proyek *open-source*.
e. Spesialisasi: menentukan bidang fokus seperti *mobile pentest, cloud security,* atau *industrial control systems.*

Langkah ini bersifat fleksibel, namun membantu individu membangun kompetensi secara bertahap dan terarah (Wylie & Crawley, 2021).

Rangkuman

Bab ini telah membahas secara tentang konsep dasar *ethical hacking* dan *penetration testing*. Melalui pendekatan sistematis dan legal, *ethical hacking* memberikan kontribusi besar dalam mendeteksi serta menanggulangi kerentanan sistem sebelum dimanfaatkan oleh pihak tidak bertanggung jawab. Beberapa poin penting yang dapat disimpulkan dari bab ini adalah:

1. *Ethical hacking* merupakan praktik legal dan etis untuk menguji keamanan sistem informasi. Seorang *ethical hacker* bekerja dengan izin resmi dan mengikuti prinsip-prinsip profesi seperti integritas, transparansi, dan tanggung jawab (Graham, 2021).
2. *Penetration testing* adalah simulasi serangan yang terstruktur untuk menemukan dan memperbaiki celah keamanan, yang terdiri dari berbagai tahapan, mulai dari perencanaan, pengumpulan informasi, eksploitasi, hingga pelaporan hasil pengujian (Weidman, 2014).
3. Terdapat berbagai standar dan *tools* yang mendukung *ethical hacking* secara profesional. Antara lain seperti standar NIST SP 800-115, OWASP, dan OSSTMM yang memberikan kerangka kerja yang valid. Sementara *tools* seperti *Kali linux*, *Nmap*, dan *Burp Suite* digunakan dalam berbagai tahap pengujian (Sinha, 2018).
4. Karir di bidang *ethical hacking* sangat terbuka dengan berbagai pilihan sertifikasi, seperti CEH, OSCP, dan *PenTest+* menjadi batu loncatan penting untuk memasuki profesi ini secara profesional dan diakui oleh industri (Wylie & Crawley, 2021).

Mempelajari *ethical hacking* bukan hanya tentang memahami teknik peretasan, tetapi juga tentang membangun budaya sadar keamanan dan tanggung jawab *digital* di era industri yang semakin terhubung ini.

Daftar Pustaka

Alhamed, M., & Rahman, M. M. H. (2023). A Systematic Literature Review on Penetration Testing in Networks: Future Research Directions. *Applied Sciences (Switzerland)*, *13*(12). https://doi.org/10.3390/app13126986.

Engebretson, P., & Kennedy, D. (2013). *The Basics of Hacking and Penetration Testing* (C. Katsaropoulos (ed.); 2nd ed.). Elsevier. http://scioteca.caf.com/bitstream/handle/123456789/1091/RED2017-Eng-8ene.pdf?sequence=12&isAllowed=y%0Ahttp://dx.doi.org/10.1016/j.regsciurbeco.2008.06.005%0Ahttps://www.researchgate.net/publication/305320484_SISTEM_PEMBETUNGAN_TERPUSAT_STRATEGI_MELESTARI.

Graham, D. G. (2021). *Ethical Hacking A Hands-on Introduction to Breaking In* (K. Andreadis & K. Taylor (ed.)). William Pollock. https://doi.org/10.2307/j.ctv5vdcsf.

Kho, Y., & Hernawan, F. Y. (2019). *Bug Hunting 101 (Web Application Security)*. https://alfursan.id.

Lewis, E. (2020). *Ethical Hacking Best Tips and Tricks of Ethical Hacking* (hal. 121). http://scioteca.caf.com/bitstream/handle/123456789/1091/RED2017-Eng-8ene.pdf?sequence=12&isAllowed=y%0Ahttp://dx.doi.org/10.1016/j.regsciurbeco.2008.06.005%0Ahttps://www.researchgate.net/publication/305320484_SISTEM_PEMBETUNGAN_TERPUSAT_STRATEGI_MELESTARI.

Pradeep, I., & Sakthivel, G. (2021). Ethical Hacking And Penetration Testing For Securing Us Form Hackers. *Journal of Physics: Conference Series*, *1831*(1). https://doi.org/10.1088/1742-6596/1831/1/012004.

Singh, T., Bajpai, A., & Shukla, S. (2024). Ethical Hacking and Penetration Testing. *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, *12*(IV), 2924–2930.

Sinha, S. (2018). *Beginning Ethical Hacking With Kali Linux: Computational Techniques For Resolving Security Issues*. Apress Media LLC. https://doi.org/10.1007/978-1-4842-3891-2.

Somani, A. (2024). Ethical Hacking and Penetration Testing. *Science*

Management Design Journal, *2*(6), 1–14. https://doi.org/10.70295/SMDJ.2412002.

Utomo, G. A. (2019). Ethical Hacking. *Cyber Security dan Forensik Digital*, *2*(1), 8–15. https://doi.org/10.14421/csecurity.2019.2.1.1418.

Weidman, G. (2014). *Penetration Testing A Hands-On Introduction To Hacking by*. William Pollock. http://scioteca.caf.com/bitstream/handle/123456789/1091/RED2017-Eng-8ene.pdf?sequence=12&isAllowed=y%0Ahttp://dx.doi.org/10.1016/j.regsciurbeco.2008.06.005%0Ahttps://www.researchgate.net/publication/305320484_SISTEM_PEMBETUNGAN_TERPUSAT_STRATEGI_MELESTARI.

Wylie, P. L., & Crawley, K. (2021). *The Pentester Blueprint (Starting a Career as an Ethical Hacker)*. WILEY.

PROFIL PENULIS

Hendri Julian Pramana, S.Kom., M.Kom.
adalah seorang akademisi di bidang pengembangan Rekayasa Perangkat Lunak (RPL). Ketertarikan penulis terhadap dunia komputer dan teknologi sudah tumbuh sejak masa sekolah menengah pertama. Belajar secara otodidak dan lembaga-informal yang terbatas tidak menghalangi keinginan untuk melanjutkan pendidikan tinggi di bidang Teknik Informatika setelah lulus Sekolah Menengah Atas di Kota Tasikmalaya. Penulis berhasil menyelesaikan studi Sarjana Komputer dan kemudian melanjutkan pendidikan Magister Komputer pada kampus UDINUS Semarang dan lulus pada tahun 2020. Saat ini, penulis menjadi dosen tetap untuk Prodi Rekayasa Perangkat Lunak, Fakultas Komunikasi dan Informasi (FKOMINFO), Universitas Garut (UNIGA). Penulis mengampu beberapa mata kuliah di antaranya: Sistem Terdistribusi, Pemrograman Bergerak, Sistem Pendukun Keputusan, Peretasan Beretika (*Ethical Hacking*), dan *Design Thinking*. Fokus dan ketertarikan penulis dalam bidang keilmuan meliputi *design thinking*, *decision support system*, *machine learning*, pengenalan objek menggunakan *computer vision*, serta *Internet of Things* (IoT). Selain mengajar, penulis juga berkomitmen untuk terus aktif melakukan penelitian dan meningkatkan pengetahuan melalui kegiatan menulis buku guna memperkuat kontribusi pada dalam pengembangan pengetahuan dan teknologi di Indonesia.

Email Penulis: hendri.jp@uniga.ac.id.

BAB 11
PHISHING DAN *SOCIAL ENGINEERING*

Muhammad Taher Jufri, S.T., M.T.
Universitas Garut

Pendahuluan

Dalam era *digital* yang semakin terkoneksi, keamanan informasi menjadi aspek krusial yang tidak dapat diabaikan. Ancaman terhadap sistem informasi tidak lagi terbatas pada kelemahan teknis semata, namun semakin berkembang dengan memanfaatkan kelemahan manusia sebagai titik masuk utama.

Serangan siber seperti *phishing* dan *social engineering* merupakan contoh nyata dari pendekatan ini, di mana pelaku mengeksploitasi kepercayaan, kelengahan, atau ketidaktahuan korban untuk mendapatkan akses tidak sah terhadap informasi atau sistem. Studi menunjukkan bahwa lebih dari 90% insiden pelanggaran keamanan informasi berawal dari kesalahan (Latifa, 2025), yang menunjukkan pentingnya memahami dimensi psikologis dari serangan ini.

Memahami aspek psikologis dalam serangan siber sangat penting karena sebagian besar teknik yang digunakan dalam *phishing* dan *social engineering* tidak memerlukan kecanggihan teknis, melainkan kemampuan untuk memanipulasi persepsi dan keputusan individu (Wicaksana, 2025). Pelaku sering kali menciptakan rasa urgensi, rasa takut, atau rasa percaya palsu untuk mengelabui korban. Hal ini menjadikan manusia sebagai titik lemah utama dalam sistem pertahanan keamanan *digital*, yang hanya dapat diperkuat melalui edukasi dan peningkatan kesadaran.

Bab ini bertujuan untuk mengenalkan konsep dasar dari *phishing* dan *social engineering*, menjelaskan berbagai teknik yang umum digunakan, menguraikan dampak yang ditimbulkan, serta menyajikan strategi pencegahan dan mitigasi yang dapat diterapkan oleh individu maupun organisasi. Dengan pemahaman yang menyeluruh, diharapkan pembaca dapat lebih siap menghadapi ancaman siber yang berbasis manipulasi sosial ini.

Definisi dan Konsep Dasar *Phishing* dan *Social Engineering*

1. *Phising*

Phishing adalah bentuk serangan siber yang bertujuan untuk mengelabui korban agar secara sukarela memberikan informasi

b) Memverifikasi permintaan informasi atau transaksi, terutama jika bersifat mendesak atau tidak biasa.
c) Melaporkan segera apabila menemukan email atau pesan mencurigakan.

2) Peran Organisasi:
a) Menyusun kebijakan keamanan informasi berdasarkan standar seperti ISO 27001.
b) Menetapkan tim keamanan informasi atau CSIRT (*Computer Security Incident Response Team*).
c) Menjalankan audit keamanan berkala dan meninjau kembali kebijakan berdasarkan hasil audit dan perkembangan ancaman terbaru.

e. Budaya Keamanan Siber
Organisasi perlu membangun budaya kerja yang mengutamakan keamanan, di mana setiap karyawan merasa memiliki tanggung jawab untuk menjaga integritas data dan sistem.

Kesimpulan

Phishing dan *social engineering* merupakan bentuk serangan siber yang terus berkembang dan menjadi ancaman signifikan bagi individu, organisasi, dan infrastruktur digital secara global. Serangan ini memanfaatkan kelemahan psikologis manusia untuk mengakses informasi sensitif, merusak sistem, atau mencuri identitas dan keuangan. Berdasarkan analisis yang telah dibahas, dapat disimpulkan bahwa:

1. Ancaman *phishing* dan *social engineering* bersifat dinamis dan semakin canggih, baik dari sisi teknik maupun pendekatan yang digunakan pelaku, seperti *spear phishing, vishing, smishing*, dan *baiting*.
2. Dampak serangan tidak hanya bersifat teknis, tetapi juga sosial dan ekonomi, seperti kehilangan data pribadi, kerugian finansial, reputasi organisasi yang tercemar, dan kepercayaan publik yang menurun.

3. Kesadaran dan edukasi merupakan strategi utama dalam pencegahan. Karyawan dan pengguna harus dibekali pemahaman yang kuat mengenai tanda-tanda serangan serta dilatih untuk merespons secara tepat.
4. Teknologi dan prosedur yang tepat dapat meminimalisir risiko dan mempercepat pemulihan dari insiden. Penggunaan teknologi seperti MFA, *email filtering*, dan IDS, serta adanya rencana penanganan insiden sangat penting untuk pertahanan yang komprehensif.
5. Keterlibatan aktif individu dan organisasi dalam membangun budaya keamanan siber menjadi pondasi dalam menciptakan lingkungan *digital* yang aman.

Sebagai penutup, penting bagi semua pihak untuk menyadari bahwa keamanan informasi bukan hanya tanggung jawab satu departemen, melainkan kolaborasi dari seluruh elemen dalam organisasi dan masyarakat. Dengan pendekatan menyeluruh dan berkelanjutan, risiko serangan *phishing* dan *social engineering* dapat ditekan secara signifikan.

Daftar Pustaka

Arafah, A. Y. (2024). *Teknik Phising (Pencurian Data Pribadi) Dalam Perspektif Hukum Pidana Islam Dan Hukum Fakultas Syariah Universitas Islam Negeri (UIN) Datokarama Palu*.

Interisle. (2024). *Phishing Landscape 2024 A Study of the Scope and Distribution of Phishing*.

Latifa, N. R. (2025). *Keuntungan Cyber Security Awareness Training Bagi Karyawan Perusahaan*. Siber Mate. https://sibermate.com/hrmi/keuntungan-cybersecurity-awareness-training-bagi-karyawan-perusahaan.

Maya Safitri, E., Ameilindra, Z., & Yulianti, R. (2023). Analisis Teknik *Social engineering* Sebagai Ancaman Dalam Keamanan Sistem Informasi: Studi Literatur. *Jurnal Ilmiah Teknologi Informasi Dan Robotika*, *2*(2), 21–26. https://doi.org/10.33005/jifti.v2i2.26.

Vadila, N., & Pratama, A. R. (2021). Analisis Kesadaran Keamanan Terhadap Ancaman *Phishing*. *Automata*, *2*(2), 1–4.

Wibowo Noor Fikri, A., Fauzi, A., Alfathur Rachman, A., Khaerunisa, A., Puspita Sari, D., Vernanda, P., Hikmah, R., & Putri Fadyanti, T. (2023). Analisis Keamanan Sistem Operasi dalam Menghadapi Ancaman *Phishing* dalam Layanan Online Banking. *Jurnal Ilmu Multidisiplin*, *2*(1), 84–91. https://doi.org/10.38035/jim.v2i1.228.

Wicaksana, S. A. (2025). *Hubungan antara Keamanan Siber dan Psikologi Dalam Konteks Organisasi The Relationship Between Cybersecurity and Psychology in Organizational Contexts*. *April*.

PROFIL PENULIS

Muhammad Taher Jufri, S.T., M.T. adalah seorang akademisi dan praktisi di bidang keamanan informasi dengan latar belakang pendidikan teknologi informasi dan sistem komputer. Saat ini, penulis aktif sebagai dosen tetap di Program Studi Rekayasa Sistem Komputer, Universitas Garut (UNIGA), serta terlibat dalam berbagai kegiatan penelitian dan pengabdian kepada masyarakat di bidang keamanan siber, *Internet of Things* (IoT), dan sistem tertanam. Penulis memiliki ketertarikan khusus pada isu-isu keamanan berbasis manusia (*human-centric cybersecurity*) seperti *phishing, social engineering*, dan literasi *digital*. Beberapa karya ilmiah dan artikel populer telah dipublikasikan dalam jurnal nasional maupun media online, dengan fokus pada edukasi dan peningkatan kesadaran masyarakat terhadap ancaman siber. Dengan semangat kolaboratif dan pendekatan berbasis edukasi, penulis berkomitmen untuk terus mengembangkan solusi keamanan yang tidak hanya berorientasi pada teknologi, tetapi juga pada pemberdayaan individu dan organisasi dalam menjaga integritas dan kerahasiaan informasi.

Email Penulis: jufri@uniga.ac.id.

BAB 12
MANAJEMEN RISIKO KEAMANAN SIBER

Dr. Nungky Awang Chandra, M.TI., S.Si.
Universitas Mercu Buana

Latar Belakang Pentingnya Keamanan Siber

Di era digital saat ini, teknologi informasi telah menjadi fondasi utama dalam menjalankan berbagai aktivitas, baik dalam lingkup individu, bisnis, maupun pemerintahan. Penggunaan sistem komputer, jaringan internet, dan penyimpanan data secara digital mempermudah proses komunikasi, transaksi, hingga pengambilan keputusan. Namun, ketergantungan yang tinggi terhadap teknologi juga membuka peluang bagi berbagai ancaman keamanan yang bersifat siber.

Keamanan siber (*cybersecurity*) menjadi aspek krusial untuk melindungi informasi dari akses tidak sah, perusakan, pencurian, atau gangguan terhadap sistem. Serangan siber seperti *phishing, malware*, *ransomware*, dan peretasan tidak hanya mengancam data pribadi, tetapi juga berdampak besar terhadap stabilitas operasional suatu organisasi dan bahkan keamanan nasional.

Laporan global menunjukkan bahwa kerugian akibat serangan siber terus meningkat setiap tahunnya, baik dari segi finansial maupun reputasi. Menurut Badan Siber dan Sandi Negara (BSSN), sepanjang 2023 ada 347 dugaan insiden siber di Indonesia. Insiden siber ini meliputi kebocoran data, *ransomware* (penyanderaan data), *web defacement* (peretasan situs *web*), dan serangan DDoS (gangguan terhadap fungsi situs *web*).

Jumlah serangan *phising* oleh *Kaspersky* juga meningkat, Kaspersky telah memblokir lebih dari 893 juta upaya *phishing* di seluruh dunia pada tahun 2024, meningkat 26% dibandingkan tahun 2023. Lonjakan signifikan terjadi antara Mei hingga Juli, bertepatan dengan musim liburan yang sering dimanfaatkan oleh pelaku kejahatan siber untuk menipu wisatawan melalui pemesanan palsu dan penawaran yang terlalu bagus untuk menjadi kenyataan.

Seiring berkembangnya kompleksitas teknologi dan metode serangan, pendekatan keamanan tradisional tidak lagi memadai. Oleh karena itu, dibutuhkan suatu sistem manajemen risiko keamanan siber yang mampu mengidentifikasi, menganalisis, dan mengendalikan potensi risiko secara proaktif. Dengan adanya manajemen risiko, organisasi dapat membuat keputusan yang lebih tepat dalam mengalokasikan sumber daya keamanan, serta meningkatkan ketahanan terhadap insiden siber.

melibatkan pemilihan dan penerapan kontrol dan tindakan yang tepat untuk mengurangi atau mengelola risiko yang teridentifikasi. Organisasi harus mempertimbangkan berbagai opsi, seperti menerapkan kontrol keamanan, mentransfer risiko melalui asuransi, atau menerima risiko berdasarkan keputusan yang matang.

6. Memantau dan Meninjau

Langkah terakhir dalam proses manajemen risiko ISO 27005:2022 adalah memantau dan meninjau efektivitas tindakan penanganan risiko yang diterapkan. Ini melibatkan penilaian kinerja kontrol secara berkala, memantau perubahan dalam lanskap risiko, dan meninjau proses manajemen risiko itu sendiri. Organisasi harus terus meningkatkan praktik manajemen risiko berdasarkan pelajaran yang dipelajari dan perubahan keadaan.

Penting untuk dicatat bahwa ISO 27005 selaras dengan standar lain seperti ISO/IEC 27001 dan ISO 31000, yang masing-masing menyediakan kerangka kerja komprehensif untuk manajemen keamanan informasi dan manajemen risiko umum.

Daftar Pustaka

Amin, H.E., Samhat, A.E., Chamoun, M., Oueidat, L., Feghali, A.(2024). An Integrated Approach to Cyber Risk Management with Cyber Threat Intelligence Framework to Secure Critical Infrastructure. *Journal of Cybersecurity and Privacy, MDPI,4,* 357-381.

Dosari, K.A., & Fetais, N.(2023). Risk-Management Framework and Information-Security Systems for Small and Medium Enterprises (SMEs): AMeta-Analysis Approach. *Journal of Electronics, MDPI,12,* 3629.

Garcia, I.D.S., Mejia, J., Gilabert, T.S.F. (2023). Cybersecurity Risk Assessment: A Systematic Mapping Review, Proposal, and Validation. *Journal of Applied Science, MDPI, 13,* 395.

Hodson, C.J. (2024). *Cyber Risk Management*. London EC1V3RS United Kingdom: Kogan Page Limited.

Leirvik, R. (2023). *Understand, Manage, and Measure Cyber Risk: Practical Solution for Creating a Sustainable Cyber Program*. Arlington, VA, USA: Apress.

Melaku, H.M.(2023). Context-Based and Adaptive Cybersecurity Risk Management Framework. *Journal of Risks, MDPI,11,* 101.

Nair, A., & Gresshman, M.R. (2023). *Mastering Information Security Compliance Management*. Birmingham, B3 2PB, UK: Packt Publishing Ltd.

PROFIL PENULIS

Dr. Nungky Awang Chandra, M.TI., S.Si.
Nungky Awang Chandra, lahir di Semarang 1973. Penulis selain dosen Teknik Informatika Fasilkom Universitas Mercubuana, juga berprofesi sebagai auditor sistem manajemen keamanan informasi ISO 27001, ISO 22301, ISO 27701, ISO 20000, ISO 42001 yang teregister di BSSN. Penulis merupakan lulusan pendidikan Sarjana S1 jurusan Fisika Komputasi Institut Teknologi Bandung pada tahun 1998. kemudian pada tahun 2007 melanjutkan pendidikan master di bidang Magister Teknologi Informasi Universitas Indonesia, menyelesaikan studinya pada tahun 2009. Pada tahun 2022 penulis juga menyelesaikan studi S3 di Universitas Indonesia dengan disertasi dan publikasi jurnal bereputasi internasional tentang keamanan siber dan manajemen risiko keamanan siber. Selain itu pada tahun 2023 penulis juga menyelesaikan studi *postgraduate cyber security* di *Massachusetts Institute of Technology* (MIT). Penulis memiliki kepakaran dibidang keamanan siber, pengembangann aplikasi, *drone*. Dan untuk mewujudkan karir sebagai dosen profesional, penulis pun aktif sebagai peneliti di bidang kepakarannya tersebut. Beberapa penelitian yang telah dilakukan didanai oleh internal perguruan tinggi dan juga Kemenristek DIKTI. Selain peneliti, penulis juga aktif menulis buku dengan harapan dapat memberikan kontribusi positif bagi bangsa dan negara yang sangat tercinta ini. Adapun untuk koresponden dengan penulis dapat email ke penulis dengan email: nungkyac707@gmail.com.

BAB 13
KEAMANAN NIRKABEL (*Wi-Fi*)

Praditya Adi Nugroho, S.T., M.T.
Politeknik PGRI Banten

Pendahuluan

Dengan berkembangnya teknologi nirkabel yang cepat, keamanan pada jaringan tanpa kabel muncul sebagai isu penting dalam bidang keamanan siber. Jaringan nirkabel seperti *Wi-Fi, Bluetooth*, dan Zigbee memiliki risiko tinggi terhadap serangan siber karena karakteristik komunikasinya yang tidak tertutup. Dalam bab ini, akan dibahas tentang konsep dasar keamanan nirkabel, berbagai ancaman yang sering dihadapi, serta langkah-langkah yang dapat diambil untuk melindungi infrastruktur nirkabel dari penyalahgunaan yang merugikan.

Gambar 13.1: Keamanan Jaringan Nirkabel (*Wi-Fi*)
Sumber: Kenali Sistem Jaringan WPA2-PSK Dalam Proteksi WiFi-Hosteko Blog.

Arsitektur Jaringan Nirkabel

Jaringan tanpa kabel menggunakan gelombang radio untuk mentransmisikan data. Beberapa standar penting yang sering diterapkan dalam kegiatan sehari-hari meliputi:

1. IEEE 802. 11 (*Wi-Fi*): digunakan untuk jaringan lokal tanpa kabel (WLAN).
2. *Bluetooth* (IEEE 802. 15. 1): digunakan untuk komunikasi dalam jarak dekat.
3. *Zigbee* (IEEE 802. 15. 4): sering dimanfaatkan dalam IoT (*Internet of Things*).

WiFi palsu dengan nama yang mirip dengan jaringan kafe tersebut (misalnya: "Kafe123_Free" padahal aslinya "Kafe123"). Andi terhubung ke jaringan palsu tersebut. Pelaku kemudian dapat:

a. Menyadap lalu lintas data dari dan ke perangkat Andi.
b. Mengakses kredensial login yang tidak dienkripsi.
c. Menyisipkan *malware* ke dalam situs yang dikunjungi.

3. **Dampak**
   a. Kredensial *email* dan akun perbankan Andi dicuri.
   b. Akun perusahaan digunakan untuk mengirim *email phishing*.
   c. Informasi sensitif perusahaan terpapar.

Metode Pengamanan yang Dilakukan

1. **Menggunakan VPN (*Virtual Private Network*)**
   a. Setelah insiden, perusahaan tempat Andi bekerja mewajibkan semua karyawan menggunakan VPN saat mengakses sistem internal, terutama dari jaringan publik.
   b. VPN mengenkripsi seluruh lalu lintas data sehingga tidak bisa dibaca oleh pihak ketiga meskipun terjadi penyadapan.
2. **Edukasi Pengguna**
   a. Karyawan diberi pelatihan tentang bahaya Wi-Fi publik dan cara mengenali jaringan palsu.
   b. Ditekankan pentingnya tidak melakukan transaksi penting melalui jaringan terbuka tanpa perlindungan.
3. ***Multi-Factor Authentication* (MFA)**: semua akun perusahaan dan layanan keuangan diaktifkan dengan autentikasi dua faktor untuk mencegah akses meski kata sandi bocor.
4. **HTTPS *Everywhere***
   a. *Browser* di perangkat kerja disetting agar selalu memaksa koneksi HTTPS.
   b. HTTPS melindungi data selama transmisi meskipun pengguna berada di jaringan publik.
5. **Pemantauan Keamanan dan Respons Insiden**
   a. Perusahaan memasang sistem pemantauan untuk mendeteksi *login* tidak biasa.
   b. Saat insiden terdeteksi, akses akun dibekukan dan kata sandi di reset secara otomatis.

Kesimpulan

Jaringan *Wi-Fi* yang bersifat publik rentan disalahgunakan untuk serangan seperti *Man-in-the-Middle*. Pencegahan yang berhasil melibatkan penggunaan teknologi seperti VPN, MFA, dan HTTPS, serta penerapan kebijakan keamanan dan pendidikan bagi pengguna.

Keamanan tanpa kabel membutuhkan strategi yang berlapis, mulai dari pengkodean hingga pengelolaan identitas. Pengetahuan yang mendalam mengenai ancaman dan solusinya berkontribusi dalam merancang jaringan yang lebih aman.

Daftar Pustaka

Abdillah, R. (2015). *Teknologi Jaringan Komputer Nirkabel (Standar IEEE 802.11b), Teknologi Jaringan Komputer Nirkabel, 1.*

Barki, A. (2019). WPA3 Security Analysis. *Journal of Network Security*.

Rerung, R. R., Fauzan, M., & Hermawan, H. (2020). Website Quality Measurement of Higher Education Services Institution Region IV Using Webqual 4.0 Method. *International Journal of Advances in Data and Information Systems*, *1*(2), 89-102.

Stewart, D. & Simmons, M. (2010). *The Business Playground: Where Creativity and Commerce Collide*. Berkeley, AS: New Riders Pres.

PROFIL PENULIS

Praditya Adi Nugroho, S.T., M.T.

Penulis menyelesaikan gelar Sarjana (S1) pada tahun 2010 di Program Studi Teknik Elektro, Fakultas Teknik Elektro, Universitas Sultan Ageng Tirtayasa (Untirta). Pada tahun 2016, Penulis melanjutkan pendidikan pascasarjana dan memperoleh gelar Magister dari Universitas Indonesia dengan fokus pada Manajemen Energi. Sejak tahun 2016, penulis telah terlibat secara aktif dalam kegiatan mengajar sebagai dosen Teknik Elektronika di Politeknik PGRI Banten. Selanjutnya, pada tahun 2018, Penulis juga memulai pengajaran di bidang Teknik Informatika, sehingga memperluas area pengajarannya sesuai dengan minat dan keterampilannya. Penulis menunjukkan minat yang besar terhadap bidang elektronik dan komputer. Kecenderungan itu mendorongnya untuk terus memperbaiki diri, baik melalui aktivitas penelitian maupun penulisan ilmiah. Penulis secara aktif menulis dan menerbitkan jurnal di bidang informatika, dengan harapan dapat memberikan sumbangan yang signifikan dalam pengembangan ilmu pengetahuan dan teknologi. Dengan dasar pendidikan dan pengalaman mengajar yang dimiliki, Penulis bertekad untuk terus membagikan pengetahuan demi kemajuan bersama, terutama dalam bidang pendidikan dan penelitian terapan di sektor teknik.

Email Penulis: praditya.energysolution@gmail.com.

BAB 14
KEAMANAN *INTERNET OF THINGS* (IOT)

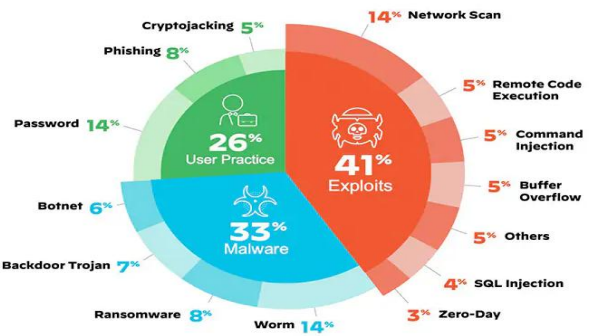
Ir. Dahlan, S.T., M.Kom.
Universitas Muhammadiyah Bima

Pendahuluan

Perkembangan teknologi *Internet of Things* (IoT) telah merevolusi cara manusia hidup, bekerja, dan berinteraksi dengan lingkungan. IoT memungkinkan berbagai perangkat fisik seperti sensor, kamera, kendaraan, bahkan peralatan rumah tangga terhubung dengan internet dan saling berkomunikasi secara otomatis. Dari rumah pintar, kota cerdas, hingga industri 4.0, teknologi ini terus memperluas peranannya dalam kehidupan modern.

Buku ini hadir untuk memberikan pemahaman menyeluruh mengenai keamanan *Internet of Things*, dimulai dari pengenalan tantangan utama, identifikasi ancaman umum, analisis kerentanan perangkat, hingga solusi teknis dan strategis yang dapat diterapkan untuk membangun sistem IoT yang aman. Buku ini juga mengulas pendekatan kriptografi modern, strategi otentikasi dan otorisasi, serta teknologi pengamanan seperti *blockchain, machine learning*, dan *edge security.*

Pembaca dari kalangan mahasiswa, dosen, peneliti, praktisi keamanan siber, maupun pengambil kebijakan akan mendapatkan panduan akademis dan praktis untuk menghadapi tantangan keamanan dalam penerapan IoT. Buku ini juga mendukung perkembangan literasi digital dalam upaya membangun ekosistem teknologi yang tangguh, terpercaya, dan berkelanjutan.



Gambar 14.1: Ancaman Keamanan IoT
Sumber: https://www-paloaltonetworks-com.translate.goog/cyberpedia/what-is-iot-security?_x_tr_sl=en&_x_tr_tl=id&_x_tr_hl=id&_x_tr_pto=imgs.

transaksi dicatat dalam blok yang saling terhubung dan tidak dapat diubah tanpa konsensus dari semua *node*, menjadikannya tahan terhadap manipulasi data.

Dalam IoT, *blockchain* dapat digunakan untuk autentikasi perangkat secara aman, pencatatan *log* komunikasi antar perangkat dan menjamin integritas *firmware* dan pembaruan. Namun, integrasi *blockchain* dalam IoT menghadapi tantangan seperti keterbatasan *bandwidth*, latensi, dan kapasitas penyimpanan perangkat.

Untuk itu, solusi seperti penggunaan *lightweight blockchain, side chains*, atau protokol konsensus yang efisien (misalnya PoS atau DAG) mulai dikembangkan agar cocok untuk lingkungan IoT.

3. *Artificial Intelligence* dan *Machine Learning* Untuk Deteksi Ancaman

AI dan ML menjadi alat penting dalam mendeteksi dan merespons ancaman pada sistem IoT secara cepat dan otomatis. Sistem keamanan berbasis ML dapat mengenali pola lalu lintas jaringan, mendeteksi anomali, dan memprediksi serangan sebelum terjadi. Contoh implementasi:

a. Deteksi DDoS dengan model *supervised learning*.
b. *Clustering* trafik jaringan untuk identifikasi perangkat kompromi.
c. Sistem prediksi kerentanan berbasis *historical data.*

Kelebihan AI/ML adalah kemampuan adaptasi terhadap ancaman baru yang belum terdefinisi (*zero-day*). Namun, pelatihan model membutuhkan *dataset* yang cukup dan validasi berkala untuk menghindari *false positive*/*negative*.

4. *Fog* dan *Edge Security*

Fog dan *edge computing* menghadirkan pemrosesan data lebih dekat ke sumber (perangkat IoT) sehingga mengurangi latensi dan risiko data dikirim ke *cloud*. Hal ini juga memberi kesempatan untuk mengimplementasikan keamanan lokal seperti, Enkripsi dan dekripsi data di *edge*, Autentikasi lokal terhadap perangkat baru dan IDS ringan berbasis *edge* untuk mendeteksi anomali lokal.

Keamanan pada *fog* dan *edge* sangat penting karena perangkat ini menjadi penghubung antara *cloud* dan *device*, sehingga sering menjadi target serangan.

5. Teknologi SDN dan NFV Dalam Keamanan IoT

Software Defined Networking (SDN) dan *Network Function Virtualization* (NFV) memberikan kontrol yang lebih besar atas infrastruktur jaringan dengan memisahkan fungsi kontrol dari perangkat keras. Dalam konteks IoT, SDN dan NFV memungkinkan segmentasi jaringan dinamis untuk memisahkan *traffic* IoT dan non-IoT, otomatisasi respons terhadap ancaman berdasarkan trafik abnormal dan penempatan fungsi keamanan (*firewall*, IDS) secara virtual dan fleksibel. Dengan arsitektur yang lebih terbuka dan terprogram, SDN/NFV memungkinkan pembaruan kebijakan keamanan secara *real-time.* Tantangannya terletak pada kompatibilitas perangkat IoT dengan infrastruktur virtual dan keamanan kontrol *plane* dari sistem SDN itu sendiri.

Daftar Pustaka

Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., & Al-Ali, A. R. (2023). Cybersecurity In The Internet of Things: A Survey on Threats and Defense Mechanisms. *Journal of Network and Computer Applications*, 213, 103560.

Alzu'bi, A., & El-Sayed, H. (2022). A Lightweight Cryptographic Scheme For IoT Devices Using Elliptic Curve And Hash-Based Signatures. *IEEE Access*, 10, 32650–32664.

Choudhary, G., Goudar, R. H., & Goudar, R. H. (2023). IoT Security: Recent Advances, Challenges, And Future Directions. *Computers & Security,* 125, 102954.

Hassan, M. S., Rehman, S. U., & Ghafoor, A. (2022). Secure Bootstrapping And Trust Management For IoT systems: A Blockchain-Based Approach. *Internet of Things*, 19, 100520.

Rahman, M. S., Hossain, M. S., Muhammad, G., & Alamri, A. (2022). A Secure And Privacy-Aware Fog-Based Framework For Internet Of Things. *Future Generation Computer Systems*, 128, 185–195.

Shrestha, R., Bajracharya, R., & Kim, S. W. (2022). Anomaly Detection In IoT Networks Using Federated Learning And Edge Intelligence. Sensors, 22(8), 3002.

Ullah, I., Naeem, M., & Alotaibi, E. (2023). Zero Trust Architecture for Securing Industrial IoT: Concepts, Framework, And Research Directions. *Computer Communications, 201*, 105–117.

Zhang, J., & He, H. (2022). Towards Secure Firmware Updates In IoT: Challenges And Recent Advances. *ACM Computing Surveys*, 55(1), 1–35.

PROFIL PENULIS

Ir. Dahlan, S.T., M.Kom.

Ketertarikan penulis terhadap ilmu komputer dimulai pada tahun 2011 silam. Hal tersebut membuat penulis memilih untuk masuk ke Sekolah Menengah Kejuruan di SMK Negeri 2 Kota Bima dengan memilih Jurusan Teknik Komputer dan Jaringan (TKJ) dan berhasil lulus pada tahun 2014. Penulis kemudian melanjutkan pendidikan ke Perguruan Tinggi dan berhasil menyelesaikan studi S1 di prodi Teknik Informatika Universitas Islam Makassar pada tahun 2019. Dua tahun kemudian, penulis melanjutkan studi S2 dan menyelesaikan studi di prodi Sistem Komputer Program Pasca Sarjana Universitas Handayani Makassar pada tahun 2024. Pada tahun 2024 penulis kemudian melanjutkan studi di Universitas Negeri Makassar pada program studi Profesi Insinyur BK Informatika dan menyelesaikan studi pada tahun 2025. Penulis memiliki kepakaran di bidang *Embedded Systems and Cloud Computing*. Guna mewujudkan karir sebagai dosen profesional, penulis pun aktif sebagai peneliti pada bidang kepakaran tersebut. Selain peneliti, penulis juga menulis buku dengan harapan dapat memberikan kontribusi positif bagi bangsa dan negara RI.

Email Penulis: dahlanlanggudu@gmail.com.

BAB 15
KEAMANAN PERANGKAT LUNAK

Rio Setiawan, S.T., M.T.
Universitas Garut

Pendahuluan

Keamanan perangkat lunak menjadi aspek yang sangat krusial untuk diperhatikan di era *digital* yang semakin berkembang. Perangkat lunak tidak hanya berfungsi sebagai pendukung operasional, tetapi juga menjadi bagian inti dari sistem informasi yang digunakan oleh perusahaan, lembaga, maupun organisasi.

Oleh karena itu, memastikan keamanan perangkat lunak dari berbagai ancaman siber merupakan langkah strategis yang tidak dapat diabaikan. Berikut alasan umum kenapa keamanan perangkat lunak itu penting:

1. Mencegah kehilangan dan kebocoran data.
2. Menghindari terjadinya kerugian *financial*.
3. Menjaga nama baik/reputasi perusahaan/lembaga/organisasi.
4. Memenuhi regulasi dan standar.

Salah satu contoh kasus yang sempat menghebohkan Negara Indonesia adalah serangan siber dalam bentuk *ransomware* terhadap Pusat Data Nasional yang membuat beberapa *server* lembaga dan kementrian lumpuh. Menurut Marsudi Wahyudi Kisworo (Guru Besar bidang IT dari Universitas Pancasila), dalam dunia keamanan komputer, di dunia ini tidak ada sistem yang dijamin pasti aman yang ada adalah sistem yang sudah diretas dan sistem belum diretas. Di negara-negara maju pun konon setiap 3-5 detik terjadi percobaan peretasan (Tempo.co, 2024).

Ancaman Umum Pada Perangkat Lunak

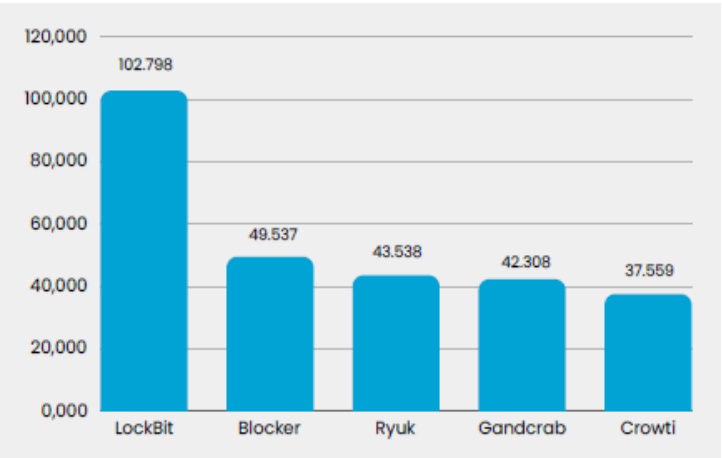
Jenis-jenis ancaman dalam perangkat lunak kedepannya akan semakin banyak, peretas akan melakukan upaya untuk mencari celah untuk bisa mencapai apa yang diinginkannya. Berikut adalah ancaman umum yang terjadi pada perangkat lunak.

1. *Malware*

Malware (*Malicious Software*) merupakan ancaman yang banyak terjadi di perangkat lunak, *malware* sendiri dibuat untuk merusak, mengganggu bahkan bisa mendapatkan akses yang tidak sah, Masuknya *malware* bisa dari *web* yang berbahaya, USB, *email*, atau celah celah yang lain.

Tujuannya bisa beragam, mulai dari mencuri data pribadi, mengganggu operasional sistem, hingga memeras korban untuk membayar tebusan. Salah satu jenis malware yang lagi trend pada saat ini adalah *Ransomware.*

Berdasarkan laporan tahunan ID_SIRTII *Indonesia Cyber Security Monitoring Report* 2024 tercatat terjadi aktivitas *Ransomware* sebanyak 514.508 aktivitas (ID-SIRTII, 2024), 5 *Ransomware* yang paling banyak ditemukan di laporan tersebut adalah:



Grafik 15.1: *Ransomware* Tahun 2024 di Indonesia
Sumber: Laporan Tahunan ID_SIRTII *Indonesia Cyber Security Monitoring Report* 2024.

2. *SQL Injection*

SQL *Injection* merupakan serangan keamanan yang memungkinkan penyerang menyisipkan perintah SQL berbahaya ke dalam *query* basis data. Dengan *SQL Injection*, penyerang bisa mendapatkan akses tidak sah ke data, memodifikasi isi basis data, atau bahkan menghapus seluruh tabel.

Dengan kata lain, penyerang bisa membobol sistem database dan memanipulasi data, membuat serangan serangan ini sangat berbahaya (Wiguna, 2020). Untuk mencegahnya, penting menggunakan *query* parameter (*prepared statements*), validasi input, dan membatasi hak akses basis data.

Daftar Pustaka

IDSIRTII. (2024). *Indonesia Cyber Security Monitoring Report 2024*. Jakarta: Indonesia Security Incident Response Team on Internet Infrastructure (IDSIRTII).

Mano Paul. (2008). The Ten Best Practices for secure software development. Information System Security Certification Consortium, Inc.

Tempo.co. (2024, Juni 24). *Pusat Data Nasional Lumpuh karena Serangan Ransomware, Apa Kata Akademisi dan Pakar IT?* https://www.tempo.co/digital/pusat-data-nasional-lumpuh-karena-serangan-ransomware-apa-kata-akademisi-dan-pakar-it--45107.

Wiguna, B., Prabowo, W.A. and Ananda, R., 2020. Implementasi Web Application Firewall Dalam Mencegah Serangan SQL Injection Pada Website. *Digital Zone: Jurnal Teknologi Informasi Dan Komunikasi*, *11*(2), pp.245-256.

PROFIL PENULIS

Rio Setiawan, S.T., M.T.
adalah seorang dosen tetap di program studi Rekayasa Perangkat Lunak Universitas Garut (UNIGA) dengan latar belakang pendidikan S1 di Teknik Elektro Universitas Indonesia dan S2 di Teknik Elektro Universitas Gunadarma dengan peminatan di Teknologi Informasi. Penulis aktif mengajar Sistem *Artificial Intelligence*, Jaringan Komputer, *Big Data* dan Analitik, *Evolution Configuration Management*, *Mikroprosesor*, dan *Mikrokontroler*, serta terlibat dalam berbagai kegiatan penelitian dalam rekayasa *software* dan pengabdian kepada masyarakat terhadap keamanan jaringan.

Penulis memiliki ketertarikan dalam *software development* dan isu-isu terkini terkait perkembangan dari *Artificial Intelegence*. Beberapa karya ilmiah dan artikel populer telah dipublikasikan dalam jurnal nasional dan media *online*, serta menjadi pembicara di seminar. Penulis akan selalu berupaya bisa berkontribusi dalam keamanan perangkat lunak dan inovasi teknologi lainnya dan sangat terbuka untuk bisa berkolaborasi dalam upaya mencari solusi dan inovasi kedepannya terhadap keamanan perangkat lunak. Tema Bab di Buku ini mengenai keamanan perangkat lunak ini ditulis sebagai bentuk kontribusi untuk meningkatkan literasi dan kesadaran praktis mengenai pentingnya keamanan dalam pengembangan sistem, baik di kalangan mahasiswa, dosen, maupun praktisi.

Email Penulis: rio.setiawan@uniga.ac.id.

BAB 16
SERANGAN DDoS DAN MITIGASINYA

Novi Aryani Fitri, S.T., M.Tr.Kom.
Politeknik Negeri Pontianak

Pendahuluan

Dalam era *digital* saat ini, ketersediaan layanan jaringan merupakan aspek krusial bagi kelangsungan operasional organisasi. Namun, ancaman terhadap ketersediaan ini semakin meningkat, salah satunya melalui serangan *Distributed Denial of Service* (DDoS). Serangan DDoS bertujuan untuk melumpuhkan layanan dengan membanjiri sistem target menggunakan lalu lintas yang sangat besar, sehingga menyebabkan gangguan atau penghentian layanan bagi pengguna yang sah.

Serangan DDoS telah berkembang dalam kompleksitas dan skala. Misalnya, pada tahun 2018, GitHub mengalami serangan DDoS terbesar yang pernah tercatat, dengan puncak lalu lintas mencapai 1,35 terabit per detik (Sam Kottler, 2018). Serangan ini memanfaatkan teknik amplifikasi melalui *server memcached* yang tidak aman, menunjukkan bagaimana infrastruktur yang rentan dapat dieksploitasi untuk melancarkan serangan besar-besaran.

Ancaman DDoS tidak hanya berasal dari volume lalu lintas yang besar, tetapi juga dari teknik yang semakin canggih, seperti serangan pada lapisan aplikasi (Layer 7) yang sulit dideteksi dan ditangani (Bhosale et al., 2017). Selain itu, kemunculan teknologi seperti *Internet of Things* (IoT) telah memperluas permukaan serangan, memungkinkan penyerang untuk mengendalikan sejumlah besar perangkat untuk digunakan dalam serangan DDoS.

Definisi *Denial of Service* (DDoS)

Distributed Denial of Service (DDoS) adalah jenis serangan siber yang bertujuan untuk mengganggu ketersediaan layanan jaringan atau sistem dengan membanjiri target dengan lalu lintas yang sangat besar dari banyak sumber secara simultan.

Tidak seperti serangan DoS (*Denial of Service*) konvensional yang biasanya berasal dari satu sumber, serangan DDoS menggunakan banyak perangkat yang telah dikompromikan (sering disebut bot atau zombie) dan dikendalikan oleh penyerang melalui sebuah jaringan *botnet*.

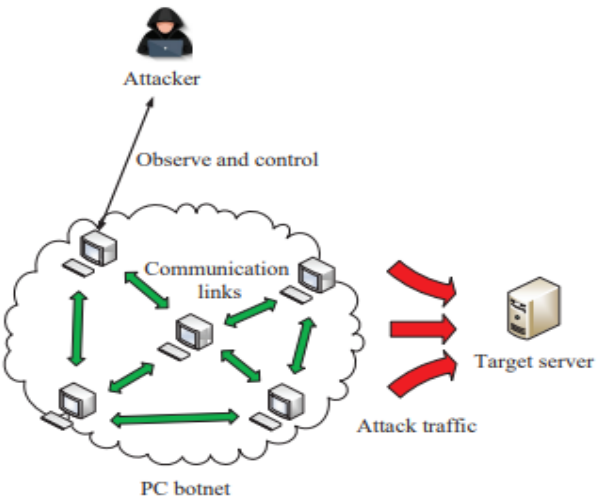
Menurut Mirkovic & Reiher, DDoS adalah salah satu serangan yang paling sulit untuk dicegah karena berasal dari sumber yang sah secara

tersebar, sehingga menyulitkan sistem untuk membedakan lalu lintas normal dan berbahaya (Mirkovic & Reiher, 2004).

Cara Kerja Serangan DDoS

Serangan DDoS pada umumnya terdiri dari tiga elemen utama yaitu:

1. ***Attacker* (Penyerang):** mengontrol *botnet* dan merencanakan serangan.
2. ***Botnet* (Jaringan *Zombie*):** sekumpulan perangkat (komputer, *server*, perangkat IoT) yang telah terinfeksi malware dan dapat diperintah untuk mengirim lalu lintas ke target.
3. ***Target* (Korban):** *server* atau layanan yang diserang, biasanya layanan publik seperti *website*, *DNS server*, *email server*, dll.



Gambar 16.1: Diagram Arsitektur Serangan DDoS Terdesentralisasi

Sumber: Huang et al., 2020.

Dalam serangan DDoS berbasis arsitektur *Peer-to-Peer* (P2P), semua perangkat dalam *botnet* saling terhubung dan menyebarkan perintah secara langsung antar sesama, tanpa pusat komando tetap. Ini membuat botnet lebih tangguh terhadap pemblokiran karena tidak bergantung pada satu titik kendali.

Namun, arsitektur ini juga memiliki kelemahan yaitu lebih mudah terdeteksi melalui pola komunikasi jaringan, lebih sulit dikelola, dan

Daftar Pustaka

Ajah, I. A. (2014). Evaluation of Enhanced Security Solutions in 802.11-Based Networks. *International Journal of Network Security & Its Applications*, *6*. https://doi.org/10.48550/ARXIV.1409.2261.

Azam, H., Tan, M., Pin, L. T., Syahmi, M. A., Qian, A. L. W., Jingyan, H., Uddin, M. F., & Sindiramutty, S. R. (2023). *Wireless Technology Security and Privacy: A Comprehensive Study*. Computer Science and Mathematics. https://doi.org/10.20944/preprints202311.0664.v1.

Bhosale, K. S., Nenova, M., & Iliev, G. (2017). The Distributed Denial Of Service Attacks (DDoS) Prevention Mechanisms On Application Layer. *2017 13th International Conference On Advanced Technologies, Systems And Services In Telecommunications (TELSIKS)*, 136–139. https://doi.org/10.1109/TELSKS.2017.8246247.

Government of Canada. (2024). *Defending Against Distributed Denial Of Service (DDoS) Attacks*. Communications Security Establishment = Centre De La Sécurité Des Telecommunications. https://www.cyber.gc.ca/en/guidance/defending-against-distributed-denial-service-ddos-attacks-itsm80110.

Guru Abhay Magapu. (2025). *Old Errors, New Threats: The Ongoing Impact of IP Spoofing in Modern Infrastructure*. Unpublished. https://doi.org/10.13140/RG.2.2.32467.69928.

Huang, K., Yang, L.-X., Yang, X., Xiang, Y., & Tang, Y. Y. (2020). A Low-Cost Distributed Denial-of-Service Attack Architecture. *IEEE Access*, *8*, 42111–42119. https://doi.org/10.1109/ACCESS.2020.2977112.

Joseph, G., Osamor, J., & Olajide, F. (2024). A Systematic Review of Network Packet Sniffing Tools for Enhancing Cybersecurity in Business Applications. *International Journal of Intelligent Computing Research*, *15*(1), 1292–1307. https://doi.org/10.20533/ijicr.2042.4655.2024.0157.

Kurose, J. F., & Ross, K. W. (2017). *Computer Networking: A top-down Approach* (7. edition). Pearson Education.

Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review*, *34*(2), 39–53. https://doi.org/10.1145/997150.997156.

Ouhssini, M., Afdel, K., Akouhar, M., Agherrabi, E., & Abarda, A. (2024a). Advancements in detecting, preventing, and mitigating DDoS attacks in cloud environments: A comprehensive systematic review of state-of-the-art approaches. *Egyptian Informatics Journal*, *27*, 100517. https://doi.org/10.1016/j.eij.2024.100517.

Ouhssini, M., Afdel, K., Akouhar, M., Agherrabi, E., & Abarda, A. (2024b). Advancements In Detecting, Preventing, And Mitigating DDoS Attacks In Cloud Environments: A Comprehensive Systematic Review Of State-Of-The-Art Approaches. *Egyptian Informatics Journal*, *27*, 100517. https://doi.org/10.1016/j.eij.2024.100517.

Sam Kottler. (2018). February 28th DDoS Incident Report [Company news]. The Incident. https://github.blog/news-insights/company-news/ddos-incident-report/

PROFIL PENULIS

Novi Aryani Fitri, S.T., M.Tr.Kom.

Buku ini secara khusus membahas serangan Distributed Denial-of-Service (DDoS), mencakup berbagai jenis serangan, dampaknya terhadap sistem dan organisasi, serta strategi mitigasi dan teknologi pertahanan yang dapat diterapkan untuk melindungi infrastruktur jaringan. Dengan penyajian materi yang komprehensif, diharapkan pembaca mampu memahami potensi ancaman DDoS dan menerapkan langkah-langkah pencegahan serta penanggulangan yang efektif. Penulis adalah dosen pada Program Studi Teknik Informatika, Politeknik Negeri Pontianak. Ia lahir di Sintang pada 13 November 1991. Pendidikan S1 diselesaikan di Teknik Elektro, Universitas Tanjungpura Pontianak pada tahun 2014, dan melanjutkan pendidikan S2 di Teknik Informatika dan Komputer, Politeknik Elektronika Negeri Surabaya, lulus pada tahun 2019. Penulis memiliki minat utama dalam bidang keamanan jaringan (*network security*). Selain mengajar, penulis juga aktif dalam kegiatan penelitian dan pengabdian kepada masyarakat, dengan fokus pada pengembangan solusi teknologi yang inovatif dan aplikatif untuk menjawab tantangan dunia nyata. Dapat menghubungi melalui email penulis: noviaryanif@polnep.ac.id.

BAB 17
MALWARE DAN *RONSOMWARE*

Tarmin Abdulghani, S.T., M.T., CITPM.
Universitas Suryakancana

Definisi *Malware* (*Malicious Software*)

Malware merupakan singkatan dari *malicious software*, yaitu perangkat lunak berbahaya yang diciptakan secara sengaja untuk mengganggu, merusak, mencuri, atau menyusup ke dalam sistem komputer, perangkat lunak, jaringan, atau perangkat pengguna.

Tidak seperti *bug* atau *error* yang terjadi karena kesalahan pemrograman yang tidak disengaja, *malware* dibuat secara sadar oleh pelaku (*attacker*) dengan maksud jahat. *Malware* dapat beroperasi secara tersembunyi atau terang-terangan, tergantung pada jenis dan tujuannya.

Jenis *malware* yang paling umum meliputi virus, *worm, trojan horse, ransomware*, *spyware, adware*, dan *rootkit*. Setiap jenis memiliki metode kerja dan dampak yang berbeda terhadap sistem dan jaringan.

1. **Jenis-Jenis *Malware* yang Paling Umum Antara Lain:**
   a. Virus: menyisipkan diri ke *file* atau program dan menyebar saat *file* tersebut dijalankan.
   b. *Worm*: menyebar melalui jaringan tanpa perlu interaksi pengguna.
   c. *Trojan Horse*: menyamar sebagai aplikasi sah untuk menipu pengguna agar menginstalnya.
   d. *Spyware*: mengumpulkan informasi pengguna secara diam-diam.
   e. *Ransomware*: mengenkripsi data dan menuntut tebusan untuk mengembalikannya.

2. **Pentingnya Memahami *Malware* dan *Ransomware* Dalam Konteks Keamanan Jaringan**
   Memahami *malware* dan *ransomware* menjadi sangat penting dalam konteks keamanan jaringan karena, beberapa alasan harus memahami hal ini:
   a. Ancaman Utama Terhadap Infrastruktur TI
      Malware dapat menembus jaringan perusahaan dan menyebabkan kerusakan serius, termasuk pencurian informasi sensitif, penghentian layanan, atau kontrol penuh atas sistem.
   b. *Ransomware* sebagai Modus Pemerasan *Digital*
      Ransomware semakin sering digunakan sebagai alat pemerasan terhadap organisasi, lembaga pendidikan, fasilitas kesehatan,

risiko *malware* dan *ransomware*, antara lain Undang-Undang ITE, Undang-Undang Perlindungan Data Pribadi (UU PDP), NIST *Cybersecurity Framework*, dan ISO/IEC 27001.

1. **Undang-Undang ITE (Indonesia)**

   Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya (UU No. 19 Tahun 2016) merupakan dasar hukum utama terkait kejahatan siber di Indonesia.

   Dalam konteks *malware* dan *ransomware*, UU ITE melarang perbuatan ilegal seperti akses tanpa izin, perusakan sistem elektronik, dan penyebaran program jahat. Pasal 30 hingga Pasal 34 mengatur ancaman pidana bagi pelaku kejahatan digital, termasuk penyisipan atau pengiriman *malware* yang mengganggu sistem elektronik (Republik Indonesia, 2008).

   UU ITE memberi landasan hukum bagi lembaga penegak hukum dan otoritas siber seperti BSSN (Badan Siber dan Sandi Negara) untuk melakukan investigasi dan penegakan hukum terhadap insiden *malware* dan *ransomware*.

2. **Undang-Undang Perlindungan Data Pribadi (UU PDP)**

   UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi memberikan fokus khusus terhadap keamanan data pribadi, termasuk dalam situasi insiden *ransomware*.

   Ketika data pribadi dienkripsi atau dicuri oleh *ransomware*, organisasi wajib melaporkan insiden tersebut kepada otoritas terkait dalam jangka waktu tertentu. UU PDP memperkuat prinsip keamanan dengan mewajibkan pengendali data melakukan tindakan teknis dan organisasi yang layak, termasuk proteksi terhadap *malware*. Hal ini mengaitkan keamanan jaringan (*cybersecurity*) dengan perlindungan hak privasi individu (Kemenkominfo, 2022).

3. **NIST *Cybersecurity Framework***

   National Institute of Standards and Technology (NIST) mengembangkan *Cybersecurity Framework* sebagai panduan manajemen risiko siber. *Framework* ini terdiri dari lima fungsi

utama: *Identify, Protect, Detect, Respond,* dan *Recover*. Dalam konteks *malware* dan *ransomware*:

a. *Identify*: mengenali aset, kerentanan, dan risiko yang berpotensi diserang *malware*.
b. *Protect*: implementasi kontrol akses, pelatihan keamanan, dan sistem antivirus.
c. *Detect*: mendeteksi anomali dan serangan *ransomware* melalui sistem *log* dan IDS/IPS.
d. *Respond*: prosedur tanggap insiden yang sesuai, termasuk isolasi dan pelaporan.
e. *Recover*: pemulihan data dan layanan secara aman pasca-serangan.

NIST CSF memberikan kerangka kerja terstandar yang dapat diadopsi oleh berbagai organisasi untuk memperkuat ketahanan terhadap *malware* (NIST, 2018).

4. ISO/IEC 27001

ISO/IEC 27001 merupakan standar internasional untuk sistem manajemen keamanan informasi (ISMS). Dalam standar ini, organisasi dituntut untuk mengidentifikasi risiko keamanan informasi, termasuk *malware* dan *ransomware*, dan menetapkan kontrol yang sesuai untuk menguranginya.

Salah satu kontrol penting adalah penggunaan kebijakan keamanan informasi, pelatihan karyawan, pengamanan teknis (misalnya: *firewall*, antivirus), serta audit dan pemantauan sistem. ISO/IEC 27001 membantu organisasi membangun budaya keamanan informasi yang berkelanjutan dan terukur (ISO, 2022).

Daftar Pustaka

Conti, G., & Raymond, D. (2021). *Cybersecurity for Executives: A Practical Guide*. Springer.

Europol. (2022). *No More Ransom Initiative*. https://www.nomoreransom.org.

Grimes, R. A. (2017). *Hacking the Hacker: Learn from the Experts Who Take Down Hackers*. Wiley.

Guide to Intrusion Detection and Prevention Systems (IDPS). NIST SP 800-94.

Hadnagy, C. (2018). *Social Engineering: The Science of Human Hacking* (2nd ed.). Wiley.

Internet Security Threat Report. Broadcom Inc. SANS Institute. (2020). *Incident Handler's Handbook.* https://www.sans.org.

ISO. (2022). *ISO/IEC 27001:2022-Information Security, Cybersecurity And Privacy Protection-Information Security Management Systems*. International Organization for Standardization.

Kaspersky. (2021). *Incident Response Playbook for Ransomware*. https://www.kaspersky.com.

Kaspersky. (2021). *Incident Response Playbook for Ransomware*. Retrieved From https://www.kaspersky.com Scarfone, K., & Mell, P. (2007).

Kaspersky. (2021). *Ransomware Prevention Guide*. Retrieved from https://www.kaspersky.com.

Kaspersky. (2023). *How Malware Spreads*. Retrieved from https://www.kaspersky.com.

Kaspersky. (2023). *Ransomware: What You Need to Know*. Retrieved From https://www.kaspersky.com.

Kementerian Komunikasi dan Informatika Republik Indonesia. (2022). *Undang-Undang No. 27 Tahun 2022 Tentang Perlindungan Data Pribadi*. https://pdp.id.

Kurose, J. F., & Ross, K. W. (2021). *Computer Networking: A Top-Down Approach* (8th ed.). Pearson.

Mitnick, K. D., & Vamosi, R. (2017). *The Art of Invisibility*. Little, Brown and Company.

National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. NIST. https://www.nist.gov/cyberframework.

NIST Special Publication 800-94.

Norton. (2022). *What is Malware? Definition and Types*. Retrieved from https://us.norton.com.

Republik Indonesia. (2008). *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. https://peraturan.bpk.go.id.

Scarfone, K., & Mell, P. (2007). *Guide to Intrusion Detection and Prevention Systems (IDPS)*. NIST Special Publication 800-94.

Skoudis, E., & Liston, T. (2006). *Malware: Fighting Malicious Code*. Prentice Hall.

Stallings, W., & Brown, L. (2018). *Computer Security: Principles and Practice* (4th ed.). Pearson Education.

Symantec. (2020). *Internet Security Threat Report*. Broadcom Inc.

Symantec. (2021). *Internet Security Threat Report*. Broadcom Inc.

Symantec. (2022). *Ransomware Threat Report*. Broadcom Inc.

Zetter, K. (2019). *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. Crown Publishing.

PROFIL PENULIS

Tarmin Abdulghani, S.T., M.T., CITPM.
Penulis lahir di Subang pada tanggal 1 Agustus 1975. Pendidikan menengah ditempuh di STM Prakarya Internasional pada Jurusan Mesin Produksi (1991–1994), kemudian melanjutkan pendidikan Sarjana (S1) di bidang Teknik Informatika di Sekolah Tinggi Sains dan Teknologi Indonesia (ST-INTEN) (1994–2000). Gelar Magister Teknik Informatika (S2) diperoleh dari Universitas Langlangbuana (2011–2015), dengan fokus keahlian pada bidang *Computer Security*, khususnya dalam pengembangan sistem keamanan jaringan dan perlindungan data *digital*.

Pengalaman profesional penulis dimulai di sektor industri sejak tahun 2001 hingga 2009, termasuk bekerja di perusahaan-perusahaan seperti PT. Perkasa Indobaja, PT. Perkasa *Heavy Engineering* (*Texmaco Group*), dan PT. *Stephalux*. Sejak 2010, penulis aktif mengembangkan solusi sistem informasi berbasis *web* dan *mobile* untuk mendukung proses bisnis dan pelayanan publik di berbagai institusi. Saat ini penulis mengajar sebagai dosen tetap di Program Studi Teknik Informatika, Fakultas Teknik, Universitas Suryakancana. Penulis juga merupakan anggota aktif organisasi profesi seperti APTIKOM dan EDU CSIRT, serta aktif dalam kegiatan pelatihan dan pendampingan keamanan siber. Minat riset penulis meliputi bidang *Internet of Things* (IoT), Keamanan Komputer, *Computer Network Security, Augmented Reality* (AR), *Virtual Reality* (VR), dan *Smart System,* dengan komitmen untuk terus berkontribusi dalam pengembangan teknologi informasi yang aman, adaptif, dan aplikatif bagi berbagai sektor.

Email Penulis: tarmin@artagani.com.

BAB 18
SECURE CODING

Yosep Bustomi, S.T., M.Kom.
Universitas Garut

keamanan yang tinggi (OWASP, 2024). Dengan hal tersebut diharapkan perangkat lunak yang dibangun memiliki keamanan yang dapat dipercaya pengguna.

Prinsip-prinsip Dasar *Secure Coding*

Keamanan dalam pengembangan perangkat lunak tidak dibangun secara kebetulan, melainkan melalui penerapan prinsip-prinsip yang kokoh. Beberapa prinsip dasar *secure coding* yang fundamental meliputi: melakukan implementasi *secure coding* yang efektif diperlukan pemahaman dari berbagai prinsip dasar.

Prinsip dasar ini menjadi landasan yang penting dalam membangun perangkat lunak yang aman terhadap berbagai ancaman keamanan. Berikut ini beberapa prinsip dasar keamanan dalam pembangunan perangkat lunak.

1. Validasi Input

Validasi input merupakan proses pengecekan bawah data yang diterima sistem sesuai dengan format, tipe, panjang dan batasan yang diharapkan sebelum sistem melakukan proses selanjutnya (Stuttard & Pinto, 2011)**.**

Prinsip validasi input ini sangat penting karena jika *input* yang diterima tidak valid dan berbahaya dapat digunakan peretas untuk melakukan serangan terhadap sistem seperti *buffer overflow, SQL Injection,* dan *cross-site scripting* (XSS) (OWASP, 2024). Sistem melakukan validasi input yang tepat, menjadi salah satu pencegahan dari potensi penyerangan. Berikut ini beberapa langkah dalam penerapan validasi input:

a. Validasi di Klien dan *Server*

Validasi dari sisi klien (*browser*) merupakan tahap awal dalam pencegahan data yang masuk, banyak pengembang aplikasi menerapkan validasi klien ini, namun kadang pengembang tidak menambahkan validasi dari sisi *server*.

Timbul masalah jika ada proses serangan MITM (*Man in The Middle Attack*) yang melakukan manipulasi data secara langsung ke *server* tanpa melewati aplikasi klien (*browser*) sehingga bisa melewati validasi tersebut (Howard & LeBlanc, 2003).

Berikut ini beberapa jenis pengujian keamanan pada sistem/perangkat lunak:

1. ***Static Application Security Testing* (SAST)**
   Jenis pengujian keamanan yang melakukan analisa kode program tanpa perlu menjalankan programnya (OWASP, 2023k). Jenis pengujian ini tujuannya untuk menghindari kerentanan *SQL Injection, Cross-site Scripting* (XSS), *buffer overflow,* dan pelanggaran aturan keamanan program.
2. ***Dynamic Application Security Testing* (DAST)**
   Jenis pengujian keamanan yang melakukan analisa aplikasi yang sedang berjalan (*runtime*) untuk mengidentifikasi kerentanan keamanan (OWASP, 2024). Jenis pengujian ini untuk menghindari dari kerentanan seperti *SQL Injection,* XSS, otentikasi yang lemah dan konfigurasi keamanan yang salah.
3. ***Software Composition Analysis* (SCA)**
   Jenis pengujian ini merupakan proses identifikasi dan analisis komponen perangkat lunak pihak ketiga (*framework*, *source-code library*, dan dependensi lainnya) dari kerentanan.
4. ***Fuzzing***
   Merupakan teknik pengujian keamanan yang memberikan sejumlah besar inputan acak, tidak valid atau tidak terduga ke dalam aplikasi atau sistem untuk mencoba menyebabkan kegagalan, pengecualian, atau perilaku yang tidak terduga.
5. ***Code Review***
   Merupakan praktik dimana pengembang lain memeriksa kode sumber yang sudah dibuat, identifikasi potensi masalah bugs, kinerja, ketidaksesuaian standar *coding* dan kerentanan terkait keamanan.

Kesimpulan

Secure coding merupakan pondasi penting dalam pengembangan perangkat lunak saat ini. Penerapan prinsip dasar keamanan, memahami kerentanan umum dan mengintegrasikan pengujian keamanan dalam proses SDLC, bisa mengurangi kerentanan secara signifikan. *Secure coding* harus dibudayakan apalagi dalam pengembang perangkat lunak sehingga keamanan bisa tercapai.

Daftar Pustaka

Bishop, M. (2003). Computer Security: Art And Science. *Addison-Wesley Professional*.

Brooks, & F. P., J. (1975). The Mythical Man-Month: Essays On Software Engineering. *Addison-Wesley*.

Dewi, E. K., & SN, A. (2012). Analisis Keamanan Sistem Perangkat Lunak. *Seminar Nasional Aplikasi Teknologi Informasi (SNATI)*, 15–16. https://journal.uii.ac.id/Snati/article/view/2945.

Howard, M., & LeBlanc, D. (2003). *Writing Secure Code (2nd ed.)* (*2nd ed).* Microsoft Press.

OWASP. (2024). *OWASP Top Ten*. Open Web Application Security Project. Diambil dari https://owasp.org/www-project-top-ten/.

Saltzer, J. H., & Schroeder, M. D. (1975). The Protection of Information in Computer Systems. *Proceedings of the IEEE*, *63*(9), 1278–1308. https://doi.org/10.1109/PROC.1975.9939.

Stuttard, D., & Pinto, M. (2011). The Web Application Hacker's Handbook: Finding And Exploiting Security Flaws (2nd ed.). *Wiley*.

Viega, J., & McGraw, G. (2001). Building Secure Software: How To Avoid The Most Common Security Problems. *Addison-Wesley Professional*.

Whitman, M. E., Mattord, H. J., Solutions, T., Garza, D., Marketing, C. E., Baker, J. A., Yarnell, D. S., Director, S. A., & Pendleton, J. (2012). Principles of Information Security. Dalam *Principles of Information Security* (International).

PROFIL PENULIS

Yosep Bustomi, S.T., M.Kom.

Seorang praktisi berpengalaman > 15 tahun bergelut di bidang pengembangan perangkat lunak. Selain menjadi praktisi saat ini penulis aktif juga sebagai akademisi menjadi dosen tetap di Program Studi Rekayasa Sistem Komputer, Universitas Garut (UNIGA). Berbagai proyek perangkat lunak yang sudah dikerjakan, baik untuk Perusahaan BUMN dan Perusahaan Swasta yang berfokus di bidang keuangan dan perbankan.

Email Penulis: yosep@uniga.ac.id.

BAB 19
KEAMANAN JARINGAN 5G

Dr. Ir. Isminarti, S.T., M.T.
Politeknik Bosowa

perangkat seperti *smartphone* akan menjadi target utama bagi penjahat dunia maya, kerentanan yang terkait dengan *malware* seluler dan potensi serangan terhadap jaringan 5G.

Masalah keamanan yang terkait dengan jaringan akses dalam komunikasi 5G. Hal ini menunjukkan bahwa integrasi teknologi akses ganda dapat mewarisi kerentanan keamanan dari sistem yang lebih lama, memerlukan mekanisme keamanan yang ditingkatkan untuk mengatasi berbagai tantangan. Studi kasus serangan tertentu, seperti serangan *Denial of Service* (DoS) dan *botnet* seluler, untuk menggambarkan jenis ancaman yang mungkin dihadapi sistem 5G (Mantas *et al.*, 2015).

Definisi dan Karakteristik 5G

1. Definisi 5G

5G atau generasi kelima jaringan seluler, merupakan kemajuan signifikan dalam teknologi komunikasi nirkabel. 5G direkayasa untuk mendukung beragam aplikasi, termasuk *broadband* seluler yang ditingkatkan, komunikasi kritis misi, dan konektivitas IoT.

Teknologi ini memanfaatkan inovasi seperti gelombang milimeter, MIMO masif, mikro sel, dan komputasi *edge* seluler untuk meningkatkan keandalan dan efisiensi. Kemampuan 5G untuk menghubungkan miliaran perangkat secara *real-time* menciptakan kemungkinan transformatif di seluruh industri, mulai dari manufaktur cerdas hingga pengalaman virtual dan *augmented reality* (AR). Seiring meningkatnya permintaan global untuk komunikasi berkecepatan tinggi dan andal, 5G siap untuk membentuk kembali cara kita hidup dan bekerja dengan memungkinkan lingkungan yang lebih efisien dan interaktif (Harish, Suriya and Velan, 2024)(Odida, 2024)(Tyokighir *et al.*, 2024).

2. Karakteristik Utama Teknologi 5G

a. Kecepatan Data Tinggi

Teknologi 5G mampu memberikan kecepatan data hingga 10 Gbps, secara signifikan lebih tinggi dari generasi sebelumnya. Konektivitas berkecepatan tinggi ini mendukung aplikasi

c. *GSM Association* (GSMA)
GSMA, bekerja sama dengan 3GPP, telah mengembangkan *Network Equipment Security Assurance Scheme* (NESAS) untuk menilai keamanan peralatan jaringan 5G. NESAS menyediakan kerangka kerja untuk evaluasi keamanan *vendor* dan *operator* jaringan.

2. Peraturan Lokal

a. Kementerian Komunikasi dan Informatika (KOMINFO) yang pada tahun 2025 telah resmi berganti nama menjadi Kementerian Komunikasi dan Digital (KOMDIGI). Perubahan ini ditetapkan melalui Peraturan Presiden Nomor 174 Tahun 2024 /KOMDIGI.

KOMDIGI bertanggung jawab atas regulasi dan pengawasan implementasi 5G di Indonesia. Beberapa inisiatif dan regulasi yang telah dikeluarkan meliputi:

1) Penetapan Standar Teknis: KOMINFO telah menerbitkan Keputusan Menteri Nomor 352 Tahun 2024 yang menetapkan standar teknis untuk perangkat LTE dan 5G NR,
2) Pengaturan Spektrum Frekuensi: KOMINFO mengatur alokasi spektrum frekuensi untuk layanan 5G, termasuk penambahan pita frekuensi baru untuk mendukung teknologi *Wireless Wide Area Network* (WWAN).

b. Objek Vital Nasional (Obvitnas)
Pemerintah Indonesia menetapkan infrastruktur telekomunikasi sebagai bagian dari Obvitnas, yang berarti:

1) Infrastruktur 5G mendapatkan perlindungan khusus dari potensi ancaman dan gangguan,
2) Pengelola Obvitnas di sektor telekomunikasi harus berkoordinasi dengan aparat keamanan seperti Kepolisian dan TNI untuk memastikan keamanan fisik dan siber.

c. Kolaborasi Internasional
Indonesia aktif dalam kolaborasi internasional untuk pengembangan dan implementasi 5G seperti:

1) KOMDIGI bekerja sama dengan GSMA untuk mempromosikan transformasi *digital* melalui 5G dan teknologi seluler lainnya,

2) Indonesia terlibat dalam forum-forum global yang membahas standar dan keamanan 5G untuk memastikan keselarasan dengan praktik terbaik internasional.

Kesimpulan dan Rekomendasi

5G mewakili lompatan signifikan dalam teknologi komunikasi seluler, menawarkan kecepatan yang lebih tinggi, latensi yang lebih rendah, dan kapasitas yang lebih besar dibandingkan dengan generasi sebelumnya. Kemajuan ini memungkinkan berbagai aplikasi, termasuk *broadband* seluler yang ditingkatkan dan komunikasi penting untuk perangkat IoT.

Terlepas dari manfaatnya, jaringan 5G menghadapi banyak tantangan keamanan termasuk kerentanan yang diwarisi dari sistem lama (2G/3G/4G) dan ancaman baru khusus untuk arsitektur 5G, seperti potensi serangan siber pada perangkat yang terhubung dan infrastruktur kritis. Buku ini menggarisbawahi perlunya memahami ancaman untuk mengembangkan strategi mitigasi yang efektif, membahas berbagai teknik, termasuk metode enkripsi yang lebih kuat dan integrasi kecerdasan buatan untuk deteksi ancaman.

Implementasi 5G harus dilengkapi dengan enkripsi *end-to-end* yang kuat seperti AES-256, kolaborasi lintas sektor, dan edukasi pengguna. Audit keamanan berkala, integrasi AI untuk deteksi ancaman, serta investasi riset keamanan 5G perlu ditingkatkan untuk menghadapi ancaman yang terus berkembang.

Daftar Pustaka

3GPP. (2019). *3GPP TS 33.210 version 15.2.2*, *European Telecommunications*.

Barker, E. *et al.* (2020). *Guide to IPsec VPNs*, *Special Publication (Nist SP)-800-77r1*. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-77r1.pdf%0Ahttp://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-77.pdf.

Bartock, M. *et al.* (2025). *5G Cybersecurity-Volume A: Executive Summary*.

Costa, C.E. and Granelli, F. (2023). Wireless 5G (The 5G mobile network standard), in *IEEE Technology and Engineering Management Society Body of Knowledge (TEMSBOK)*. Wiley Online Library, pp. 219–231. Available at: https://doi.org/10.1002/9781119987635.ch14.

Daemen, J. and Rijmen, V. (2020). *The Advanced Encryption Standard Process*, *Information Security And Cryptography*. Available at: https://doi.org/10.1007/978-3-662-60769-5_1.

ETSI. (2018). *Security Architecture And Procedures For 5G System (3GPP TS 33.501 version 15.2.0 Release 15)*. Available at: https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx.

Fowdur, T.P., Milovanovic, D.A. and Bojkovic, Z.S. (2025). 5G/6G-Based Sustainable Systems for Industry 4.0, in *Intelligent And Sustainable Engineering Systems For Industry 4.0 And Beyond*, pp. 29–58.

Ghosh, T. (2017). 5G Mobile Wireless Technology, *International Journal of Advance Research, Ideas and Innovations in Technology*, 3(6), pp. 71–75.

Harish, T., Suriya, V. and Velan, R. (2024). 5G/Next Generation Networks, *International Journal of Advanced Trends in Engineering and Management* (IJATEM), pp. 590–600.

Isminarti *et al.* (2023). Improved Data Security Using Advanced Encryption Standard Algorithm on Long-Range Communication System At Smart Grid, *ICIC Express Letters, Part B: Applications*, 14(5), pp. 499–508. Available at: https://doi.org/10.24507/icicelb.14.05.499.

M, K. and Bhuvana, D. (2024). 5G Wireless Networks, *International Journal of Innovative Research in Computer and Communication Engineering*, 12(05), pp. 6283–6286. Available at: https://doi.org/10.15680/ijircce.2024.1205190.

Malathi, P., Lydia, E.G. and Vidhyavathi, P. (2023). Exploring The Potential Of 5g Technologies: Navigating Opportunities And Challenges For Innovative Future Applications, *Industrial Engineering Journal*, 52(5), pp. 736–742.

Mantas, G. *et al.* (2015). Security for 5G Communications, in *Fundamentals of 5G Mobile Networks*, pp. 207–220.

National Institute of Standards and Technology. (2001). *197: Announcing The Advanced Encryption Standard* (AES), *Federal Information Processing Standards Publications* (FIPS PUBS). Available at: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf%5Cnhttp://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Announcing+the+ADVANCED+ENCRYPTION+STANDARD+(+AES+)#0.

Odida, M.O. (2024). The Evolution of Mobile Communication: A Comprehensive Survey on 5G Technology, *Journal of Sensor Networks and Data Communications*, 4(1), pp. 01–11. Available at: https://doi.org/10.33140/jsndc.04.01.06.

Omar, K.L. and Ong, R. (2024). Advancements in 5G Technology And Its Impact On Global Communication Networks, *International Journal of Communication and Information Technology*, 5(1), pp. 29–32. Available at: https://doi.org/10.33545/2707661x.2024.v5.i1a.76.

R. Indrajeet, M. and A. Anil, G. (2024). A Comprehensive Analysis of 5G Technology: Advancements, Challenges, and Implications, *International Journal of Advanced Research in Science, Communication and Technology*, 4(2), pp. 44–53. Available at: https://doi.org/10.48175/ijarsct-15206.

Sahu, V., Sahu, N. and Sahu, R. (2024). Challenges and Opportunities of 5G Network: A Review of Research and Development, *American Journal of Electrical and Computer Engineering*, 8(1), pp. 11–20. Available at: https://doi.org/10.11648/j.ajece.20240801.12.

Sheela, V. and Rathiga, D.P. (2024). Overview of Mobile Technologies in 5G Networking and Communication, *International Journal for*

Research in Applied Science and Engineering Technology, 12(3), pp. 1079–1085. Available at: https://doi.org/10.22214/ijraset.2024.58924.

Subramanian, B., Naamani, K.S.H. Al and Sagayee, G.M.A. (2024). Innovative Architectures and Management Strategies in 5G Communication Networks, *International Journal of Computational Mathematics and Computer Science*, 01(01). Available at: https://doi.org/10.69942/313319/20240101/02.

Tyokighir, S.S. *et al.* (2024). New Developments And Trends In 5G Technologies: Applications And Concepts, *Bulletin of Electrical Engineering and Informatics*, 13(1), pp. 254–263. Available at: https://doi.org/10.11591/eei.v13i1.6032.

PROFIL PENULIS

Dr. Ir. Isminarti, S.T., M.T.

Penulis lahir di Makassar, 30 Januari 1979. Penulis adalah dosen di Politeknik Bosowa, Kota Makassar Provinsi Sulawesi Selatan. Menyelesaikan pendidikan D3 pada Teknik Elektro Politeknik Negeri Ujung Pandang, S1 pada Teknik Elektro Universitas Hasanuddin, S2 pada Teknik Elektro Universitas Hasanuddin dan S3 pada Teknik Elektro Universitas Hasanuddin. Penulis menekuni bidang menulis setelah menempuh Pendidikan doktor. Penulis saat ini berstatus sebagai dosen tetap Yayasan Aksa Mahmud Program Studi Teknik Mekatronika Politeknik Bosowa sejak tahun 2013, sebelumnya pernah mengajar di Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) Dipanegara Makassar tahun 2011-2012, Dosen di Universitas Indonesia Timur tahun 2012-2013, dan pernah bekerja sebagai *Asisten Manager* di PT. Singa Langit tahun 2005-2013, serta sebagai *General Manager* di PT. Dhelmara Kurnia Raya Jakarta Selatan tahun 2000-2002. Beberapa artikel ilmiah internasional terindeks *Scopus*, terakreditasi sinta, buku referensi telah terbit dua tahun terakhir. Penulis memiliki kepakaran di bidang teknologi rekayasa otomasi meliputi Pemodelan dan Identifikasi Sistem, Elektronika Otomasi Industri, komunikasi data dan *Internet of Things* (IoT). Penulis juga telah mendapatkan hibah dari kemenristekDIKTI salah satunya adalah Penelitian Disertasi Doktor tahun 2022, Hibah Inovokasi dan Hibah Penelitian Produk Vokasi pada tahun 2024.

Email Penulis: isminarti@politeknikbosowa.ac.id.

BAB 20
TREN TERKINI DALAM KEAMANAN JARINGAN KOMPUTER

Dr. Ir. Norbertus Tri Suswanto Saptadi, S.Kom., M.T., M.M., IPM.
Universitas Atma Jaya Makassar

Gambar 20.1: Tren Keamanan Jaringan Komputer
Sumber: https://madhava.id/tren-keamanan-informasi-terbaru/.

Meningkatnya Serangan Berbasis AI dan Otomatisasi

Kecerdasan buatan (AI) yang awalnya dikembangkan untuk meningkatkan efisiensi dan kecerdasan sistem kini juga dimanfaatkan oleh pelaku kejahatan siber untuk memperkuat serangan (Subekti *et al.*, 2024). AI memungkinkan peretas untuk merancang *malware* yang dapat belajar dan beradaptasi dengan lingkungan target, serta menghindari sistem deteksi keamanan tradisional. Contohnya, AI digunakan untuk mengubah perilaku *malware* secara dinamis sehingga tampak seperti aktivitas normal dalam jaringan, menyulitkan sistem pertahanan untuk membedakan antara lalu lintas jaringan yang sah dan berbahaya.

Otomatisasi telah mempercepat dan memperluas skala serangan siber. *Botnet* otomatis mampu melakukan serangan *Distributed Denial of Service* (DDoS) dalam waktu singkat dan dengan dampak yang besar (Gelgi *et al.*, 2024). Alat peretasan berbasis skrip otomatis juga digunakan untuk mencari dan mengeksploitasi kerentanan sistem secara massal tanpa campur tangan manusia. Dengan kombinasi antara AI dan otomatisasi, serangan bisa berlangsung lebih cepat, lebih canggih, dan lebih sulit dilacak oleh tim keamanan.

Menghadapi ancaman ini, organisasi harus mulai mengadopsi strategi pertahanan yang juga memanfaatkan AI dan *machine learning* untuk memperkuat sistem deteksi dan respons. Teknologi seperti

behavior analytics, *threat intelligence* berbasis AI, serta *automated incident response* menjadi solusi yang semakin umum digunakan. Dengan membangun sistem pertahanan yang adaptif dan prediktif, organisasi dapat lebih siap menghadapi serangan siber generasi baru yang didorong oleh teknologi AI dan otomatisasi.

Gambar 20.2: AI *Cyberattack*
Sumber: https://mitraberdaya.id/id/news-information/ai-cyberattack.

Zero Trust Architecture (ZTA)

Zero Trust Architecture (ZTA) merupakan pendekatan keamanan jaringan yang menghapus asumsi bahwa semua entitas dalam jaringan dapat dipercaya. Berbeda dengan model tradisional yang mengandalkan perimeter keamanan, ZTA menekankan bahwa tidak ada pengguna, perangkat, atau aplikasi yang secara otomatis dipercaya, bahkan jika berada di dalam jaringan internal.

Prinsip utama ZTA adalah *"never trust, always verify"*, di mana setiap permintaan akses melalui proses verifikasi yang ketat berdasarkan identitas, perangkat, lokasi, dan konteks lainnya (Fitrian *et al.*, 2024). Penerapan ZTA menjadi sangat relevan seiring dengan meningkatnya mobilitas tenaga kerja, penggunaan perangkat pribadi (BYOD), serta adopsi layanan *cloud* yang tersebar.

Dalam lingkungan ini, batas jaringan menjadi kabur dan tidak lagi dapat dijaga hanya dengan *firewall* atau VPN tradisional. ZTA menyediakan kontrol akses berbasis kebijakan yang granular, dengan otorisasi berbasis identitas pengguna dan status perangkat yang digunakan, sehingga memberikan keamanan yang lebih dinamis dan

cenderung untuk mengenali dan menghindari ancaman. Sebagai bagian dari kesadaran keamanan siber, pengguna perlu dilibatkan dalam kebijakan dan praktik terbaik yang diterapkan oleh organisasi. Salah satunya adalah kebijakan kata sandi yang kuat dan pemantauan aktivitas akun pengguna yang mencurigakan. Pengguna yang memahami pentingnya menjaga kerahasiaan kata sandi dan menghindari penggunaan kata sandi yang sama di beberapa situs dapat secara signifikan mengurangi risiko akses tidak sah ke sistem perusahaan.

Penggunaan Autentikasi dua faktor (2FA) merupakan metode keamanan yang mengharuskan pengguna memasukkan dua bentuk identifikasi untuk mengakses akun di mana lapisan keamanan tambahan di atas kata sandi atau PIN untuk melindungi akun. Secara keseluruhan, kesadaran pengguna dan edukasi yang memadai merupakan komponen krusial dalam strategi keamanan siber yang menyeluruh.

Tanpa pemahaman yang baik dari para pengguna, teknologi keamanan yang paling canggih sekalipun tetap rentan terhadap kesalahan manusia, seperti kelalaian dalam mengelola kredensial atau tidak mengenali upaya rekayasa sosial. Organisasi secara konsisten berinvestasi dalam program pelatihan keamanan siber yang relevan dan berkelanjutan, serta menanamkan budaya kewaspadaan di lapisan struktur organisasi.

Pendekatan yang proaktif meminimalkan risiko kebocoran data dan dampak serangan siber dapat ditekan secara signifikan, menjadikan keamanan siber sebagai tanggung jawab bersama, bukan hanya tugas tim TI semata. Di era *digital* yang semakin kompleks, pendekatan edukasi keamanan siber juga perlu disesuaikan dengan perkembangan teknologi dan karakteristik generasi pengguna saat ini (Aska, Putta and Magdalena, 2024).

Metode pembelajaran interaktif seperti simulasi serangan *phishing*, gamifikasi, serta pelatihan berbasis skenario nyata terbukti lebih efektif dibandingkan pendekatan konvensional yang bersifat teoritis. Organisasi juga dapat memanfaatkan platform *e-learning* yang dapat diakses kapan saja untuk mendukung proses pembelajaran berkelanjutan.

Dengan pendekatan yang relevan dan adaptif, peningkatan literasi siber tidak hanya mencegah insiden, tetapi juga membentuk budaya kerja yang lebih waspada dan bertanggung jawab terhadap keamanan informasi.

Kesimpulan

Perkembangan teknologi informasi yang pesat turut mendorong transformasi dalam pendekatan terhadap keamanan jaringan komputer.

Ancaman siber kini menjadi semakin kompleks dan canggih, dengan kehadiran serangan berbasis AI, otomatisasi, serta pemanfaatan celah dari perangkat yang terus bertambah jumlahnya seperti IoT. Hal ini memaksa organisasi dan individu untuk terus memperbarui strategi keamanan agar tetap relevan dan efektif menghadapi berbagai risiko baru yang muncul.

Pendekatan keamanan tradisional yang hanya berfokus pada perimeter kini tidak lagi mencukupi. Arsitektur seperti *Zero Trust Architecture* (ZTA) dan *Secure Access Service Edge* (SASE) hadir sebagai solusi modern yang lebih fleksibel dan kontekstual dalam menghadapi lingkungan kerja *hybrid* serta penggunaan layanan cloud yang semakin meluas. Strategi ini tidak hanya meningkatkan kontrol akses, tetapi juga memperkuat pemantauan dan verifikasi secara menyeluruh terhadap setiap aktivitas di dalam jaringan.

Selain pendekatan arsitektural, inovasi teknologi seperti *Extended Detection and Response* (XDR) dan blockchain juga memberikan kontribusi besar dalam meningkatkan kapabilitas deteksi, respons, serta perlindungan terhadap integritas data dan komunikasi. Di saat yang sama, peningkatan kesadaran pengguna melalui edukasi dan pelatihan keamanan siber menjadi kunci penting dalam membangun lapisan pertahanan yang kuat.

Banyak insiden keamanan yang bisa dicegah apabila pengguna memahami peran dan tanggung jawab dalam menjaga keamanan sistem. Dengan menggabungkan teknologi canggih, kebijakan yang kuat, dan budaya keamanan yang menyeluruh, organisasi dapat membangun sistem pertahanan jaringan yang adaptif dan tahan terhadap berbagai ancaman.

Tren terkini dalam keamanan jaringan komputer tidak hanya menggambarkan tantangan baru, tetapi juga membuka peluang untuk menciptakan ekosistem *digital* yang lebih aman, terpercaya, dan berkelanjutan. Ke depan, kolaborasi antara penyedia teknologi, pemangku kepentingan, dan pengguna akan menjadi kunci utama dalam membentuk masa depan keamanan siber yang resilien.

Daftar Pustaka

Ade Irawan *et al.* (2024). Tantangan dan Strategi Manajemen Keamanan Siber di Indonesia berbasis IoT, *Journal Zetroem*, 6(1), pp. 114–119. Available at: https://doi.org/10.36526/ztr.v6i1.3376.

Arsa, I.G.N.W. (2019). Analisis sistem Cloud Computing IAAS Penyedia Server Cloud dengan Standar NIST Special Publication 800-145, *Jurnal Sistem Dan Informatika*, 13(2), pp. 52–58. Available at: https://jsi.stikom-bali.ac.id/index.php/jsi/article/view/200.

Aska, M.F., Putta, D. and Magdalena, C.J. (2024). Strategi Efektif Untuk Implementasi Keamanan Siber di Era Digital, *Journal of Information and Information Security (JIFORTY)*, 5(2), pp. 187–200.

Felicia. (2024). Tantangan dan Peluang Blockchain di Era Digital dalam Bidang Keamanan Data dan Transaksi Digital, *Journal of Comprehensive Science*, 3(11), pp. 5131–5147.

Fitrian, H.P. *et al.* (2024). Analisis Keamanan Cloud Dengan Zero Trust dan Blockchain yang Tangguh, *Journal Global Technology Computer*, 4(1), pp. 36–43.

Fuad, M.H. (2022). Serangan Man-In-The-Middle (MITM) menggunakan Open Source, *Indonesian Journal on Networking and Security*, 11(1), pp. 24–28.

Gelgi, M. *et al.* (2024). Systematic Literature Review of IoT Botnet DDOS Attacks and Evaluation of Detection Techniques, *Sensors*, 24(11). Available at: https://doi.org/10.3390/s24113571.

George, A.S. (2021). XDR: The Evolution of Endpoint Security Solutions - Superior Extensibility and Analytics to Satisfy the Organizational Needs of the Future, *International Journal of Advanced Research in Science Communication and Technology*, 8(1), pp. 493–501. Available at: https://doi.org/10.48175/568.

Hanhan Hanafiah Solihin, dkk. (2022). *Konsep Sistem Informasi di Era Digital*. Bandung: Kaizen Media Publishing.

Hartanto, B., Putra, A.S. and Fawaati, T.M. (2024). Analisis Dampak Implementasi Internet of Things (IoT) Terhadap Efisiensi Operasional di Industri Manufaktur, *Jurnal Multimedia dan Android (JMA)*, 5(1).

Hoshmand, M.O., Ratnawati, S. and Korespondensi, E.P. (2023).

Analisis Keamanan Infrastruktur Teknologi Informasi dalam Menghadapi Ancaman Cybersecurity, *Applied Information Technology and Computer Science (AICOMS)*, 2(2), pp. 9–18.

Kusnanto, Y., Nugroho, M.A. and Kartadie, R. (2024). Implementasi Zero Trust Architecture untuk Meningkatkan Keamanan Jaringan: Pendekatan Berbasis Simulasi, *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, 9(4), pp. 2357–2364.

Makani, S.T. (2024). Low-cost, Self-hosted Secure Access Service Edge (SASE) Solution using AWS Cloud Infrastructure, *International Journal of Cyber Security (IJCS)*, 2(1), pp. 34–44.

Nurain, A., Gultom, R.A.G. and Indrajit, R.E. (2024). Manajemen Ketahanan Risiko Siber pada Internet of Things dan Cyber Physical System, *Journal on Education*, 6(2), pp. 13271–13281.

Nurhidayat, T., Oktavianto, D. and Windarta, S. (2024). *Kajian Ketahanan Siber: Manajemen Kerentanan*. Bogor: Politeknik Siber dan Sandi Negara.

Shams, E.A. and Rizaner, A. (2018). A Novel Support Vector Machine Based Intrusion Detection System For Mobile Ad Hoc Networks, *Wireless Networks*, 24(5), pp. 1821–1829. Available at: https://doi.org/10.1007/s11276-016-1439-0.

Sinaga, N.H., Irmayani, D. and Hasibuan, M.N.S. (2024). Mengoptimalkan Keamanan Jaringan: Memanfaatkan Kecerdasan Buatan untuk Meningkatkan Deteksi dan Respon Ancaman, *Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI*, 7(2), pp. 364–369.

Soleman, D. and Soewito, B. (2024). Information Security System Design using XDR and EDR, *Inform: Jurnal Ilmiah Bidang Teknologi Informasi dan Komunikasi*, 9(1), pp. 51–57. Available at: https://doi.org/10.25139/inform.v9i1.7331.

Subekti, I. *et al.* (2024). Formulasi Kebijakan Kriminal Dalam Penanggulangan Kejahatan Berbasis Teknologi Kecerdasan Buatan, *Jurnal Ilmu Hukum*, 5(2), pp. 60–75.

Tanjung, A.M. *et al.* (2025). Keamanan Siber Dalam Sistem Informasi Berbasis Cloud: Tantangan dan Solusi, *DENTIK: Jurnal Ilmu Ekonomi, Pendidikan dan Teknik*, 2(1), pp. 127–133.

PROFIL PENULIS

Dr. Ir. Norbertus Tri Suswanto Saptadi, S.Kom., M.T., M.M., IPM.

Lahir di Cirebon, Jawa Barat, tanggal 7 Juni 1975. Memiliki Jabatan Fungsional Lektor Kepala, Pembina Tingkat I (IV/b). Berpendidikan Sarjana Komputer (S.Kom.) di Universitas Teknologi Digital Indonesia (UTDI) tahun 1998, Magister Manajemen (M.M.) di Universitas Hasanuddin (UNHAS) tahun 2004, Magister Teknologi Informasi (M.T.) di Universitas Gadjah Mada (UGM) tahun 2007, Insinyur (Ir.) di Pendidikan Profesi Insinyur UNHAS tahun 2020, Insinyur Profesional Madya (IPM.) di Persatuan Insinyur Indonesia (PII) tahun 2021, Doktor (Dr.) di Fakultas Teknik UNHAS tahun 2023, Kursus Kader Pimpinan (Suskapin) XXVI Menwa RI tahun 1997, dan Program Pendidikan Reguler Angkatan (PPRA) LX Lemhannas RI tahun 2020. Menjadi tenaga pengajar (Dosen) pada Program Studi Teknik Informatika Fakultas Teknologi Informasi Universitas Atma Jaya Makassar (UAJM). Peraih Poster terbaik DPRM Dikti tahun 2016. Dosen berprestasi IKDKI tahun 2020, 2021, dan 2024.

Pernah menjabat Kepala UPT Komputer, Kepala BAPSI, Wakil Dekan FT, Dekan FT dan FTI, Wakil Rektor III, Ketua Penjaminan Mutu. Tim PAK Dosen dan Asesor BKD UAJM. Reviewer International Conference dan Jurnal SINTA. Pemenang Hibah Kemdikbud Penelitian Dosen Pemula, Bersaing, Fundamental, dan Strategi Nasional. Penulis artikel media massa Tribun Timur, Koinonia, Bisnis Sulawesi, Sesawi.net, Mirifica.net, HidupKatolikCom, OMKNet, KatolikanaTV, Jalan Hidup Katolik, dll. Penulis Buku di Kanisius, Sada Kurnia Pustaka, Aksara Sastra Media, Future Science, HEI Publishing, Mifandi Mandiri Digital, Rey Media Grafika, Widina Salemba, Andi, dan Cendikia Mulia Mandiri. Aktifis organisasi IKA Lemhannas RI LX, IARMI, DPP ISKA, BAPOMI Sulsel, LP3KD Sulsel, IKDKI SulSelTraBar, Komkep KAMS, Komsos KAMS, PUKAT KAMS, TPP KAMS, FMKI KAMS, UPS KAMS, Pengurus Kebun Sawit Laimbo, FDI, PII Makassar, INAPR, Dewan Keuangan Paroki dan Program Ayo Sekolah Mariso, Animator Laudato Si', dll.

KEAMANAN
JARINGAN KOMPUTER

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan signifikan dalam berbagai sendi kehidupan. Jaringan komputer menjadi tulang punggung bagi hampir seluruh aktivitas, mulai dari komunikasi personal, transaksi bisnis, hingga operasional pemerintahan. Namun, seiring dengan kemudahan dan manfaat yang ditawarkan, muncul pula berbagai risiko dan ancaman keamanan yang terus berevolusi. Serangan siber seperti *malware, phishing,* DDoS, dan berbagai bentuk intrusi lainnya menjadi semakin canggih dan dapat menimbulkan kerugian yang besar, baik secara finansial maupun reputasi. Oleh karena itu, pemahaman yang mendalam mengenai konsep dasar keamanan jaringan, identifikasi potensi ancaman, serta implementasi strategi pertahanan yang efektif menjadi suatu kebutuhan yang tidak dapat dihindari. Buku ini hadir untuk menjawab kebutuhan tersebut, dengan menyajikan pembahasan yang terstruktur, mulai dari pengenalan konsep dasar jaringan dan prinsip-prinsip keamanan, analisis berbagai jenis ancaman dan serangan, hingga langkah-langkah praktis dalam merancang, mengimplementasikan, dan mengelola sistem keamanan jaringan yang tangguh. Untuk mengetahui penjelasan lebih rinci, penulis menyusun buku ini dalam 20 (dua puluh bab) sebagai berikut:

1. Konsep Dasar Keamanan Jaringan
2. Ancaman dan Serangan Jaringan
3. Kriptografi dan Keamanan Jaringan
4. Autentikasi dan Otorisasi
5. *Firewall*
6. *Virtual Private Network* (VPN)
7. Keamanan Protokol Jaringan
8. Serangan *Man in the Middle* (MITM) dan Pencegahannya
9. Hardening Sistem
10. *Ethical Hacking* dan *Penetration Testing*
11. *Phishing* dan *Social Engineering*
12. Manajemen Risiko Keamanan Siber
13. Keamanan Nirkabel (*Wi-Fi*)
14. Keamanan *Internet of Things* (IoT)
15. Keamanan Perangkat Lunak
16. Serangan DDoS dan Mitigasinya
17. *Malware* dan *Ransomware*
18. *Secure Coding*
19. Keamanan Jaringan 5G
20. Tren Terkini dalam Keamanan Jaringan

sada kurnia pustaka

ISBN 978-634-7021-46-5
9 786347 021465