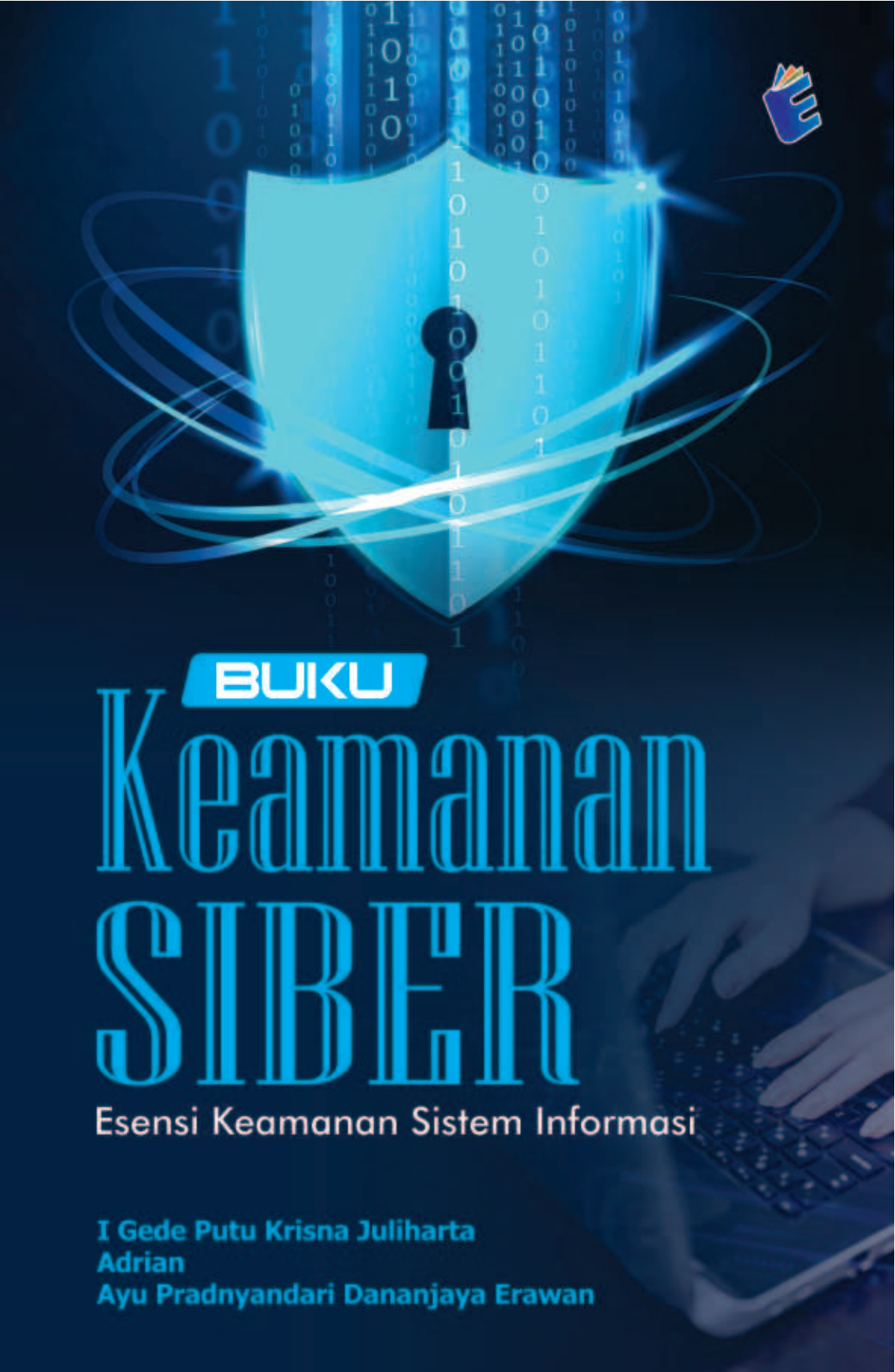


BUKU

Keamanan SIBER

Esensi Keamanan Sistem Informasi

I Gede Putu Krisna Juliharta
Adrian
Ayu Pradnyandari Dananjaya Erawan

Keamanan siber merupakan salah satu aspek penting dalam dunia teknologi informasi. Maka dari itu, Buku Keamanan Siber: Esensi Keamanan Sistem Informasi membahas tentang pentingnya keamanan siber di era digital saat ini. Buku ini relevan dengan berbagai permasalahan atau studi kasus yang dihadapi karena menjelaskan berbagai aspek keamanan siber seperti:

1. Pengantar Keamanan Sistem Informasi
2. Keamanan Sistem Operasi
3. Keamanan Jaringan dan Koneksi
4. Arsitektur Keamanan Pada *Website*
5. Keamanan *Database*
6. Aspek Keamanan Penggunaan Email
7. *Malware Analysis* dan Proteksi
8. Digital Forensik
9. Penilaian Risiko dan Manajemen Keamanan
10. Keamanan Dari Segi Pengguna
11. Etika dan Hukum dalam Keamanan Siber

Buku ini menggunakan pendekatan dari berbagai *framework* keamanan yang ada sehingga sangat cocok bagi siapapun yang ingin mempelajari dan mengimplementasikannya termasuk dengan latar belakang yang beragam baik dari level mendasar hingga menengah.

BUKU

Keamanan SIBER

Esensi Keamanan Sistem Informasi

eureka media aksara
Anggota IKAPI
No. 225/JTE/2021

0858 5343 1992
eurekamediaaksara@gmail.com
Jl. Banjaran RT.20 RW.10
Bojongsari - Purbalingga 53362

ISBN 978-623-516-106-8
9 786235 161068

BUKU KEAMANAN SIBER

Esensi Keamanan Sistem Informasi

I Gede Putu Krisna Juliharta
Adrian
Ayu Pradnyandari Dananjaya Erawan

PENERBIT CV. EUREKA MEDIA AKSARA

BUKU KEAMANAN SIBER
Esensi Keamanan Sistem Informasi

Penulis : I Gede Putu Krisna Juliharta
Adrian
Ayu Pradnyandari Dananjaya Erawan

Desain Sampul : Eri Setiawan

Tata Letak : Nadhifa Khairusyifa

ISBN : 978-623-516-106-8

Diterbitkan oleh : **EUREKA MEDIA AKSARA, JULI 2024**
ANGGOTA IKAPI JAWA TENGAH
NO. 225/JTE/2021

Redaksi:
Jalan Banjaran, Desa Banjaran RT 20 RW 10 Kecamatan Bojongsari
Kabupaten Purbalingga Telp. 0858-5343-1992
Surel : eurekamediaaksara@gmail.com
Cetakan Pertama : 2024

KATA PENGANTAR

Puji dan syukur kami panjatkan kepada Tuhan Yang Maha Esa yang telah memberikan rahmat dan karunianya, sehingga penulis dapat menyelesaikan "Buku Keamanan Siber: Esensi Keamanan Sistem Informasi".

Keamanan siber merupakan salah satu aspek penting dalam dunia teknologi informasi. Serangan siber telah menjadi ancaman yang nyata bagi berbagai organisasi, baik pemerintah, swasta, maupun individu. Serangan siber dapat menyebabkan kerugian finansial yang signifikan, gangguan operasional, dan bahkan kerusakan reputasi.

Buku ajar ini disusun untuk memberikan pemahaman yang komprehensif tentang esensi keamanan sistem informasi. Buku ini membahas berbagai aspek keamanan siber, mulai dari konsep dasar, ancaman dan kerentanan, hingga praktik terbaik dalam mengamankan sistem informasi.

Buku ini ditujukan untuk berbagai pembaca, termasuk:

- Mahasiswa dan profesional keamanan siber
- Praktisi keamanan siber
- Pemilik bisnis dan manajer TI
- Siapapun yang tertarik untuk belajar lebih lanjut tentang keamanan siber

Akhir kata, semoga buku ini dapat bermanfaat bagi pembaca dalam memahami dan menerapkan keamanan siber untuk melindungi sistem informasi. Kami mengucapkan terima kasih kepada semua pihak yang telah membantu dalam penyusunan buku ini. Semoga buku ini dapat memberikan kontribusi positif bagi peningkatan keamanan siber di Indonesia.

Denpasar, 31 Januari 2024

Tim Penulis

PRAKATA

Dalam era digital yang terus berkembang, tantangan keamanan siber menjadi semakin mendesak di tengah dinamika sistem informasi modern. Buku ini yang berjudul, "Buku Keamanan Siber: Esensi Keamanan Sistem Informasi", hadir sebagai panduan komprehensif yang mengurai inti keamanan sistem informasi dalam lingkup yang semakin kompleks. Melalui pembahasan yang mendalam, buku ini bertujuan untuk memberikan pemahaman yang kokoh tentang prinsip-prinsip keamanan siber yang krusial dalam menjaga keutuhan, kerahasiaan, dan ketersediaan data di era digital ini. Dari konsep dasar hingga isu-isu terkini, buku ini menawarkan wawasan yang berharga bagi para profesional, akademisi, serta siapa pun yang tertarik memahami dan mengimplementasikan praktik keamanan siber yang efektif.

Ketika teknologi informasi menjadi tulang punggung masyarakat global, tantangan keamanan siber pun menjadi semakin mendesak. Perkembangan sistem informasi yang pesat membuka pintu bagi peluang inovasi, tetapi juga meningkatkan risiko terhadap serangan siber yang merugikan. Oleh karena itu, pemahaman yang mendalam tentang keamanan siber menjadi suatu keharusan bagi siapa pun yang terlibat dalam dunia teknologi informasi.

Dalam buku ini, pembaca akan dibimbing melalui perjalanan mendalam dalam pemahaman konsep keamanan siber, mulai dari pemahaman dasar hingga konsep-konsep yang lebih kompleks. Penyajian materi-materi yang relevan dan praktis, dilengkapi dengan studi kasus, tip, dan praktik terbaik yang akan membantu pembaca memperkuat sistem informasi mereka.

Buku ini tidak hanya ditujukan untuk para profesional keamanan siber, tetapi juga bermanfaat bagi mahasiswa, praktisi teknologi informasi, pengusaha, dan siapa pun yang tertarik memahami pentingnya keamanan siber dalam era digital ini. Harapan untuk buku ini adalah tidak hanya menjadi sumber pengetahuan, tetapi juga menjadi panduan yang menginspirasi

pembaca dalam melangkah menuju keamanan siber yang lebih kokoh dan terpercaya.

Ucapan terima kasih sebesar-besarnya kepada semua pihak, yang telah menyumbangkan pengetahuan dan pengalaman mereka dalam pembuatan buku ini, serta kepada pembaca yang telah memberikan dukungan dan kesempatan bagi kelahiran karya ini. Semoga buku ini dapat memberikan kontribusi positif dalam upaya memperkuat keamanan sistem informasi di berbagai sektor.

Denpasar, 31 Januari 2024

Tim Penulis

HALAMAN PERSEMBAHAN

Puji syukur kepada Tuhan Yang Maha Esa, karena atas berkat dan Karunia-Nya penulis dapat menyelesaikan buku keamanan siber dengan judul "Buku Keamanan Siber : Esensi Keamanan Siber". Penulis menyadari dalam penyusunan buku ini tidak akan selesai tanpa bantuan dari berbagai pihak. Karena itu pada kesempatan ini penulis mengucapkan terima kasih kepada:

1. Tuhan Yang Maha Esa yang telah memberikan kesempatan dan kelancaran dalam pembuatan buku ini hingga selesai,
2. Segenap Tim Penulis, yang telah bekerja keras, bahu membahu, dalam menuangkan ide, gagasan, dan pengetahuan mereka, sehingga buku ini dapat tercipta dengan baik.
3. Masing - masing keluarga penulis yang telah memberikan doa, motivasi, serta kasih sayang.
4. Teman - teman, sahabat, dan kenalan yang telah memberikan semangat, dorongan, serta masukan sehingga buku ini dapat diselesaikan.
5. Semua pihak yang tidak dapat disebutkan satu persatu yang telah berkontribusi baik langsung maupun tidak langsung sehingga buku ini dapat terselesaikan.

Penulis menyadari buku ini tidak luput dari berbagai kekurangan. Penulis mengharapkan saran dan kritik demi meningkatkan kualitas buku ini sehingga buku ini dapat memberikan manfaat bagi bidang pendidikan dan penerapannya di lapangan serta bisa dikembangkan lagi lebih lanjut ataupun sebagai bahan referensi.

"Knowledge is of no value unless you put it into practice." – Anton Chekhov

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB 1 PENGANTAR KEAMANAN SISTEM INFORMASI

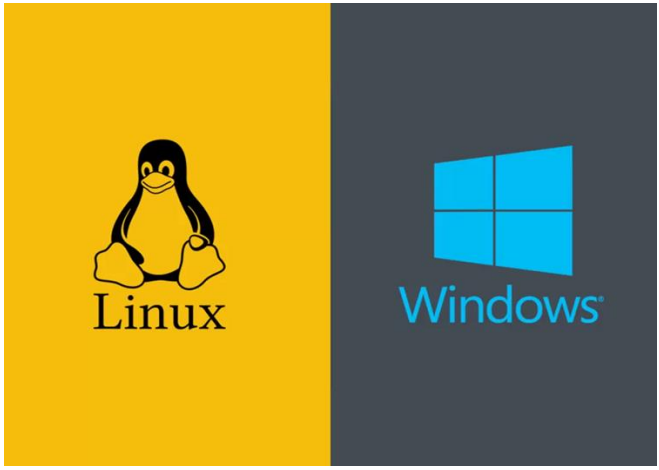
A. Pendahuluan

Pemanfaatan internet telah menjadi suatu hal yang umum dalam berbagai aspek kehidupan saat ini, memberikan kontribusi signifikan dalam mempermudah aktivitas manusia sehari-hari. Internet sendiri sudah seperti bagian penting dalam kehidupan manusia yang gunanya untuk berkomunikasi, berbagi informasi serta mengakses berbagai layanan *online*. Internet terkoneksi dengan perangkat yang biasa digunakan oleh manusia seperti laptop, komputer, gadget, *smartwatch* dan lain sebagainya. Dan tentunya pada perangkat - perangkat tersebut terpasang berbagai macam aplikasi yang memudahkan manusia untuk beraktivitas seperti berkomunikasi, berbisnis, berbelanja, mendapatkan informasi, belajar, hiburan dan berbagai macam lainnya. Dengan menjadi tulang punggung bagi revolusi digital, internet telah mengubah cara manusia hidup, bekerja, berinteraksi, dan menjadi peluang tak terbatas serta tantangan yang baru pula dalam era informasi modern.

Tantangan penggunaan internet yang dihadapi di era modern ini semakin kompleks dengan munculnya berbagai jenis kejahatan yang terus berkembang. Kasus kejahatan penggunaan komputer atau internet dalam melakukan aktivitas kejahatan disebut juga kejahatan siber (*cybercrime*). Dikarenakan kecepatan dan skala pertumbuhan teknologi juga menyebabkan perkembangan kejahatan siber menjadi lebih banyak dan canggih. Banyak kasus yang menyerang sistem informasi seperti

BAB 2 KEAMANAN SISTEM OPERASI

A. Mengamankan Sistem Operasi Windows & linux



Gambar 2. 1 Windows & Linux
Sumber : Indozone (2020)

Sebagai perangkat lunak vital dalam mengelola komputer, sistem operasi atau *system operation* (OS) berfungsi sebagai penghubung antara pengguna dan perangkat keras, mengatur eksekusi program, dan memberikan layanan umum. Dari segi keamanan, OS menjadi dasar utama dalam menjaga integritas dan keandalan sistem, mengkoordinasikan interaksi perangkat keras dan lunak, serta melindungi data dari ancaman siber. Maka, menjaga keamanan OS seperti Windows dan Linux menjadi langkah krusial di era ancaman siber yang beragam.

BAB 3 KEAMANAN JARINGAN DAN KONEKSI

A. Mengamankan Jaringan dan Infrastruktur TI dari Serangan Siber

Mengamankan jaringan dan infrastruktur Teknologi Informasi (TI) dari serangan siber adalah tugas krusial dalam era digital saat ini. Dengan kompleksitas teknologi yang semakin meningkat dan ancaman siber yang terus berkembang, organisasi harus fokus pada upaya perlindungan yang efektif untuk menjaga data, sistem, dan operasi bisnis mereka. Jaringan berperan sebagai jalur masuk dan keluar berbagai informasi, termasuk yang terhubung ke internet, memungkinkan transfer data yang cepat dan mendukung berbagai aplikasi. Namun, penggunaan jaringan ini juga membawa risiko, seperti *phising*, *hacking*, dan pencurian data sensitif. Dengan ketergantungan yang meningkat pada teknologi, pemahaman dan mitigasi risiko keamanan jaringan menjadi lebih penting daripada sebelumnya untuk menjaga keberlanjutan operasi di dunia digital yang penuh dengan ancaman.

Proxy server merupakan *software* atau *hardware* yang berguna sebagai perantara antara komputer atau perangkat pengguna (*client*) dan server yang menyediakan layanan atau sumber daya seperti situs web, *file*, atau layanan jaringan lainnya. *Proxy server* bertindak sebagai perantara untuk mengirimkan permintaan dan menerima respons atas nama *client*, dan ini dapat memberikan beberapa manfaat dan fungsi. *Proxy server* memberikan privasi dan anonimitas dengan

BAB 4 ARSITEKTUR KEAMANAN PADA WEBSITE

A. Pengamanan Pada Server

Pengamanan pada server adalah aspek yang tidak bisa diabaikan dalam konteks keamanan informasi. Dalam era di mana data menjadi aset yang sangat berharga, server merupakan pusat penyimpanan dan pengolahan informasi yang vital bagi berbagai entitas, mulai dari perusahaan hingga pemerintahan. Pengamanan server melibatkan serangkaian tindakan untuk melindungi infrastruktur jaringan dari ancaman dan serangan siber yang dapat mengancam keberlangsungan operasi dan keamanan data. Dengan memahami pentingnya pengamanan server, organisasi dapat mengurangi risiko terhadap pelanggaran keamanan dan kerugian yang mungkin timbul akibat akses yang tidak sah atau kebocoran informasi.

1. Apa itu Server

Server adalah sebuah sistem komputer yang menyediakan layanan kepada komputer lain atau perangkat lain dalam jaringan. Server umumnya memiliki spesifikasi yang lebih tinggi daripada komputer biasa, karena harus mampu menangani banyak permintaan dari klien. Server memiliki beberapa fungsi seperti menyimpan data, mengolah data, menjalankan aplikasi, menyediakan akses ke sumber daya atau perangkat yang lain dan sebagainya (Wang et al., 2015).

BAB 5 DATABASE

A. Ancaman Keamanan Database

Ancaman keamanan *database* dapat mempengaruhi keamanan dan sangat membahayakan serta merusak integritas, kerahasiaan, dan ketersediaan data dalam *database* (Ujung & Nasution, 2023). Ancaman ini dapat berasal dari dalam organisasi, seperti insiden dari karyawan yang tidak terpercaya atau kesalahan konfigurasi sistem. Termasuk adanya serangan terencana dari *hacker* menjadi salah satu ancaman yang berbahaya bagi keamanan data. Berikut adalah beberapa ancaman keamanan *database* :

Kesalahan Manusia (*Human Error*)

Kesalahan manusia dapat berupa kelalaian yang menyebabkan pelanggaran keamanan, sering kali karena kurangnya integritas karyawan dalam memberikan akses kepada pihak yang tidak bertanggung jawab. Hal ini dapat mengakibatkan eksposur kerahasiaan data dan kebocoran informasi penting yang merugikan pihak terkait. Selain itu, kelalaian juga dapat menyebabkan penghapusan atau kerusakan data yang merupakan ancaman serius.

Serangan Injeksi SQL/NoSQL

Serangan Injeksi SQL/NoSQL adalah jenis serangan siber yang disengaja untuk memanipulasi atau mengakses data dalam *database* melalui sejumlah kode berbahaya. Pelaku penyerangan akan memasukkan perintah tambahan atau mengubah perintah

BAB 6 ASPEK KEAMANAN PENGGUNAAN EMAIL

A. Pengenalan, Kegunaan Email, dan Ancaman

Email (*electronic mail*) adalah sarana komunikasi elektronik yang sangat umum dan efektif di dunia digital, memungkinkan pertukaran pesan dan file antara individu atau kelompok melalui internet, serta memberikan kemampuan untuk membuat, mengirim, menerima, dan menyimpan pesan-pesan elektronik.

Sebagai sarana komunikasi yang penting, email juga rentan terhadap berbagai ancaman keamanan. Beberapa ancaman seperti *spam*, *phishing, malware, spoofing,* dan lain-lain dapat saja dilakukan oleh pihak yang tidak bertanggung jawab untuk berbagai tujuan. Dalam menghadapi ancaman - ancaman, dibutuhkan penanganan dan keamanan yang baik dan tepat agar tidak terjadi hal yang tidak diinginkan.

BAB 7 MALWARE ANALYSIS DAN PROTEKSI

Dalam praktik meretas terdapat beberapa bentuk serangan dan cara yang dilakukan guna mencapai tujuan dari penyerang seperti menggunakan *virus*, *ransomware*, trojan dan lain-lain. Istilah dari berbagai jenis serangan ini adalah *malware* atau perangkat lunak yang berbahaya. Dalam memerangi ini dibutuhkan kemampuan untuk melindungi data atau sistem, identifikasi, pemahaman dan menganalisis serangan. Tujuan utamanya adalah untuk mengungkap cara kerja *malware*, mengidentifikasi ancaman potensial, serta mengembangkan taktik dan alat perlindungan yang efektif. Menganalisis *malware* akan membantu dalam mitigasi dan penanggulangan agar dapat melakukan langkah serta membuat kebijakan yang efektif dan efisien.

A. Serangan dan Macam-Macam Malware

Terdapat banyak sekali serangan yang terus berkembang hingga saat ini. Motif dari penyerang juga beragam mulai dari untuk hal baik seperti mengetes kerentanan sistem untuk meningkatkan keamanannya hingga mencuri atau tindak kejahatan berat lainnya. Serangan siber terbagi menjadi dua yaitu :

- Serangan Pasif, adalah serangan dengan tujuan untuk mengumpulkan informasi tanpa merusak data atau sistem. Serangan ini bersifat berhati-hati dan tidak diketahui korban atau dengan kata lain peretas menyembunyikan aktivitas mereka. Contoh dari serangan pasif adalah mencuri

BAB 8 DIGITAL FORENSIK

A. Konsep Dasar Forensik Digital dan Peran Dalam Penyelidikan Siber

1. Digital Forensik

Digital forensik secara umum diartikan sebagai penerapan ilmu pengetahuan untuk mengidentifikasi, mengumpulkan, memeriksa dan menganalisis data serta memastikan keutuhan informasi dan menjaga kredibilitas yang ketat terhadap data tersebut. Digital forensik dapat digunakan untuk berbagai tujuan, seperti melakukan penyelidikan kejahatan dan pelanggaran kebijakan internal, rekonstruksi insiden keamanan, pemecahan masalah operasional, dan memulihkan sistem dari kerusakan sistem yang tidak disengaja. Dalam dunia yang semakin terhubung secara digital, digital forensik menjadi kunci dalam menangani kejahatan siber. Seperti melindungi bukti elektronik dan memastikan bahwa data yang didapatkan bisa digunakan secara sah dalam pengadilan.

2. Peran digital forensik dalam penyelidikan siber

Dalam digital forensik, bukti elektronik dapat ditemukan dalam berbagai jenis penyelidikan kriminal, bukan hanya dalam kasus-kasus seperti pornografi anak dan pencurian identitas. Bukti digital, seperti pesan teks, email, data lokasi GPS, dan catatan panggilan, yang dihasilkan dari perangkat elektronik seperti komputer, ponsel, atau server, dapat digunakan sebagai bukti yang dapat diterima di

BAB 9 PENILAIAN RISIKO DAN MANAJEMEN KEAMANAN

A. Keamanan TI dan Penilaian Resiko

Penilaian risiko keamanan siber merupakan proses vital dalam mengidentifikasi, mengevaluasi, dan mengelola potensi ancaman serta kerentanan keamanan siber dalam lingkungan teknologi informasi. Tujuannya adalah memahami tingkat risiko yang dihadapi oleh organisasi dan mengambil langkah-langkah untuk menguranginya sejauh mungkin, sehingga langkah manajemen dapat diambil berdasarkan resiko yang mungkin terjadi. Dalam mengembangkan standar keamanan, relevansi terhadap apa yang dinilai dan diidentifikasi sangat penting, dan perlu memahami fundamental dalam manajemen dan penilaian risiko keamanan TI. Setiap organisasi memiliki keberagaman cara pandang dan pola pikir yang harus diidentifikasi untuk menghasilkan identifikasi dan mitigasi yang tepat.

1. Pentingnya Mengembangkan BIA

BIA (*Business Impact Analysis*) merupakan langkah kunci dalam mengimplementasikan kontrol dan proses perencanaan kontinjensi secara keseluruhan. BIA memungkinkan Koordinator untuk menggambarkan komponen sistem, proses misi/bisnis yang didukung, dan ketergantungannya. Tujuannya adalah menghubungkan sistem dengan proses misi/bisnis kritis dan layanan yang disediakan, serta menggambarkan konsekuensi dari gangguan. Hasil BIA digunakan koordinator untuk menentukan kebutuhan dan prioritas perencanaan

BAB 10 KEAMANAN DARI SEGI PENGGUNA

A. Keamanan Perangkat Mobile dan Aplikasi

Keamanan *mobile* adalah upaya yang dilakukan untuk menjaga perangkat seluler seperti ponsel cerdas, tablet, laptop, dan perangkat portabel lainnya, beserta jaringan yang terhubung dengannya, dari berbagai risiko dan kerentanan yang mungkin terjadi. Dalam era dimana perangkat *mobile* telah menjadi bagian tak terpisahkan dari kehidupan sehari-hari pengguna *device* digital, penting untuk memiliki pemahaman yang baik tentang keamanan perangkat *mobile* dan aplikasi yang berjalan di dalamnya. Faktor ini tidak hanya terkait dengan teknologi semata, melainkan juga melibatkan perlindungan data pribadi, finansial, dan informasi berharga yang sering disimpan di perangkat *mobile*. Dalam konteks ini, penting untuk menyadari bahwa jika perangkat *mobile* tidak aman, data sensitif dan privasi yang berisiko terkena ancaman. OWASP juga mengeluarkan daftar risiko yang dapat berdampak pada mobile, berikut 10 risiko teratas yang dikeluarkan pada tahun 2023.

BAB 11 ETIKA DAN HUKUM DALAM KEAMANAN SIBER

A. Etika Keamanan Siber dan Tanggung Jawab Profesional

Etika keamanan Siber dan tanggung jawab profesional memegang peran penting dalam menjaga integritas, kerahasiaan, dan ketersediaan data serta sistem informasi dalam lingkungan digital. Para profesional di bidang keamanan siber bertanggung jawab untuk melindungi informasi sensitif dan infrastruktur komputer dari serangan yang berpotensi merusak. Ini melibatkan pengembangan kebijakan yang sesuai, implementasi tindakan pengamanan yang efektif, dan pemeliharaan kesadaran tentang ancaman keamanan yang terus berkembang. Tanggung jawab profesional juga mencakup kesadaran akan konsekuensi dari tindakan mereka, termasuk dampak sosial, ekonomi, dan hukum. Mereka harus bertindak dengan integritas, mematuhi standar etika yang tinggi, dan selalu mengutamakan kepentingan klien, organisasi, dan masyarakat secara keseluruhan. Dengan mengikuti etika keamanan siber dan memahami tanggung jawab profesional mereka, para praktisi di bidang ini dapat memainkan peran yang krusial dalam menjaga keamanan dan keandalan dunia digital.

1. Prinsip Keamanan Siber

Keamanan siber merupakan aspek krusial dalam menjaga integritas, kerahasiaan, dan ketersediaan informasi di era digital. Agar keamanan siber efektif dan bermanfaat, pedoman etika yang jelas dan tanggung jawab profesional yang kuat menjadi landasan utama. Pada level fundamental,

DAFTAR PUSTAKA

42Gears Team (2018). BYOD, CYOD and COPE- Breaking Down Digital Workplace Programs. Diakses pada 6 April 2024 dari https://www.42gears.com/blog/byod-cyod-cope-breaking-digital-workplace-programs/

Aastha Thakker (2023). OWASP Top 10- Web Application Vulnerabilities (Part-2). Diakses pada 6 April 2024 dari https://medium.com/@aasthathakker/owasp-top-10-web-application-vulnerabilities-part-2-4f04bd5bf562

Abnormal Security (2021). PayPal Spoofed in Credential Phising Attack. Diakses pada 6 April 2024 dari https://abnormalsecurity.com/blog/spoofed-paypal-phishing-attack

Alotaibi, B., & Almagwashi, H. (2018, August 20). A Review of BYOD Security Challenges, Solutions and Policy Best Practices. 1st International Conference on Computer Applications and Information Security, ICCAIS 2018. https://doi.org/10.1109/CAIS.2018.8441967

Aloul, F., Zahidi, S., & El-Hajj, W. (2009). *IEEE/ACS International Conference on Computer Systems and Applications,* Rabat, Morocco, 2009, pp. 641-644, doi: https://doi.org/10.1109/AICCSA.2009.5069395

AMA Research & Media LLP (2024). Microsegmentation Market Giants Spending is Going to Boom. Diakses pada 6 April 2024 dari https://www.openpr.com/news/3373985/microsegmentation-market-giants-spending-is-going-to-boom

Amundrud, Ø., Aven, T., & Flage, R. (2017). How the definition of security risk can be made compatible with safety definitions. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, 231(3), 286–294. https://doi.org/10.1177/1748006X17699145

Andy Peterson (2021). The Pirate Bay is Using Visitors' Computers to Mine Monero Again. Diakses pada 6 April 2024 dari https://www.ccn.com/the-pirate-bay-is-using-visitors-computers-to-mine-monero-again/

Apurva Barve (2024). What is a S/MIME Certificate and How Does It Work?. Diakses pada 6 April 2024 dari https://www.ssl2buy.com/wiki/what-is-smime-certificate-how-does-it-work

Ardian Suhendra (2023). Perancangan Jaringan Komputer. Diakses pada 6 April 2024 dari https://homecare24.id/perancangan-jaringan-komputer/

Balthrop, J., Forrest, S., Newman, M. E. J., & Williamson, M. M. (2004). *Technological networks and the spread of computer viruses*. http://www.cs.unm.edu/

Barkah, A. S. (n.d.). *NIST SP 800-44v2: PEDOMAN PANDUAN SISTEM KEAMANAN PUBLIK WEB SERVER*. Retrieved January 22, 2024, from https://ejournal.amikompurwokerto.ac.id/index.php/telematika/article/view/188/163

Batool, H., & Masood, A. (2020). Enterprise Mobile Device Management Requirements and Features. In *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*.

Blatz, J. (n.d.). CSRF: Attack and Defense Managing Consultant McAfee ® Foundstone ® Professional Services.

Bunga, Dewi. (2019). *Legal Response to Cybercrime in Global and National Dimensions*. Journal of Law, 6(1). https://doi.org/10.22304/pjih.v6n1.a4

Carolina Turino (2024). Continous delivery, scalable design. Diakses pada 6 April 2024 dari https://medium.com/@carolinaturino/continuous-delivery-scalable-design-75d15ef7ecb5

Carvey, H. (n.d.). Windows Registry Forensics Advanced Digital Forensic Analysis of the Windows Registry.

Cawthra, J., Ekstrom, M., Lusty, L., Sexton, J., Sweetnam, J., & Townsend, A. (2020). Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events. https://www.nccoe.nist.gov/publication/1800-26/VolA/index.html

Chandramouli, R., & Rose, S. (2013). *Secure Domain Name System (DNS) Deployment Guide*. https://doi.org/10.6028/NIST.SP.800-81-2

Chinadaily (2004). Mydoom worm spreads as hunt for author intensifies. Diakses pada 6 April 2024 dari https://www.chinadaily.com.cn/en/doc/2004-01/31/content_301890.htm

Chiradeep BasuMallick (2023). What is MDM (Mobile Device Management)? Meaning, Working and Software. Diakses pada 6 April 2024 dari https://www.spiceworks.com/it-security/endpoint-security/articles/what-is-mobile-device-management/

Cichonski, Paul., Millar, T., Grance, Tim & Scarfone, K. (2012) Computer Security Incident Handling Guide NIST SP 800-61 Rev. 2. https://doi.org/10.6028/NIST.SP.800-61r2

CNN Indonesia (2020). Menguak Identitas Penjual 91 Juta Akun Tokopedia yang Bocor. Diakses 6 April 2024 dari https://www.cnnindonesia.com/teknologi/20200503155536-185-499571/menguak-identitas-penjual-91-juta-akun-tokopedia-yang-bocor

CRASHTEST SECURITY. (2022). GUIDE FOR PREVENTING CSRF ATTACKS WHAT ARE THE STEPS TO KEEP YOUR WEB APP OR API SAFE FROM SUCH VULNERABILITY. CRASHTEST SECURITY. www.crashtest-security.com

Cybersecurity Malaysia. (2020). Guidelines for Secure Software Development Life Cycle (SSDLC).

Dancho Danchev (2008). Sony Playstation's site SQL Injected, redirecting to rogue security software. Diakses pada 6 April 2024 dari https://www.zdnet.com/article/sony-playstations-site-sql-injected-redirecting-to-rogue-security-software/

Dermann, M., Dziadzka, M., Hemkemeier, B., Hoffmann, A., Meisel, A., Rohr, M., & Schreiber, T. (2008). OWASP Papers Program Best Practice: Use of Web Application Firewalls Best Practices: Use of Web Application Firewalls. http://www.webappsec.org/projects/threat/v1/WASC-TC-v1_0.de.doc

Do Son (2018). New Mirai botnet variant OMG turn IoT devices into proxy servers. Diakses pada 6 April 2024 dari https://securityonline.info/new-mirai-botnet-variant-omg-turn-iot-devices-into-proxy-servers/

Duyet Bui (2023). Part 9: Microsoft Sentinel Incident Response. Diakses pada 6 April 2024 dari https://medium.com/@phd8/part-9-microsoft-sentinel-incident-response-677810632754

Equitick (2023). The Importance of Secure Software Development Lifecycle (#SSDLC) in 21st Century Technologies . Diakses pada 6 April 2024 dari https://www.linkedin.com/pulse/importance-secure-software-development-lifecycle-ssdlc-21st

European Parliament. (2016), General Data Protection Regulation. https://gdpr-info.eu/

Fadilah, A., Aranggraeni R. & Putri, Sri. R. (2019). *EKSISTENSI KEAMANAN SIBER TERHADAP TINDAKAN CYBERSTALKING DALAM SISTEM PERTANGGUNGJAWABAN PIDANA CYBERCRIME*. (6)4. http:// 10.36418/syntax-literate.v6i4.2524

Faiz Iqbal Maulid (2022). Siapa MA, Penjual Es Thai Tea Asal Madiun yang Diduga Sosok di Balik Hacker Bjorka. Diakses pada 6 April 2024 dari https://pontianak.tribunnews.com/2022/09/17/siapa-ma-penjual-es-thai-tea-asal-madiun-yang-diduga-sosok-dibalik-hacker-bjorka

Forum null-byte.wonderhowto (2015). Zeus Malware. Diakses pada 6 April 2024 dari https://null-byte.wonderhowto.com/forum/zeus-malware-0166733/

Grossman, J., Hansen, R., D. Petkov, P., Rager, A., & Fogie, S. (2007). Cross Site Scripting Attacks Xss Exploits and Defense.

Gurneet Kaur (2023). What is DNS (Domain Name System) How It Works Explained. Diakses pada 6 April 2024 dari https://www.almabetter.com/bytes/articles/what-is-dns

Harris, M. A., & Patten, K. P. (2014). Mobile device security considerations for small- and medium-sized enterprise business mobility. In *Information Management and Computer Security* (Vol. 22, Issue 1, pp. 97–114). https://doi.org/10.1108/IMCS-03-2013-0019

Hive Systems (2023). Are Your Password in the Green. Diakses pada 6 April 2024 dari https://www.hivesystems.com/blog/are-your-passwords-in-the-green?utm_source=tabletext

IBM. (n.d.). What is patch management? Retrieved October 28, 2023, from https://www.ibm.com/topics/patch-management

Ilmu Bersama (2022). Cross Site Scripting (XSS). Diakses pada 6 April 2024 dari https://ilmubersama.com/2022/03/07/cross-site-scripting-xss/

Indozone (2020). Inilah Perbedaan Sistem Operasi Linux dan windows yang kamu harus tau. Diakses pada 6 April 2024 dari https://tech.indozone.id/gadget/921033691/inilah-perbedaan-sistem-operasi-linux-dan-windows-yang-kamuharustau

IntelliPaat (2024). What is Antivirus Software? – importance, Types, and Uses. Diakses pada 6 April 2024 dari https://intellipaat.com/blog/what-is-antivirus-software/

INTERPOL. (2021). *GUIDELINES FOR DIGITAL FORENSICS FIRST RESPONDERS*.

Intruder. (n.d.). The Ultimate Guide to Vulnerability Scanning. Diakses pada 19 April 2024 dari https://www.intruder.io/guides/the-ultimate-guide-to-vulnerability-scanning

Islem Othmani (2024). What is Cross-Site Request Forgery (CSRF). Diakses pada 6 April 2024 dari https://www.linkedin.com/pulse/what-cross-site-request-forgery-csrf-islem-othmani--18jwf?trk=public_post_main-feed-card_feed-article-content

Josh Frank (2021). June 9 : No, there's no evidence a hack called RockYou2021 exposed 8.4 bilion passwords. Diakses pada 6 April 2024 dari https://joshgoestoflatiron.medium.com/june-9-no-theres-no-evidence-a-hack-called-rockyou2021-exposed-8-4-billion-passwords-f65bbedf3ae4

Kaur, A. (2014). Methodology and Analysis for Various SQL Injection Techniques. http://www.banasthali.org/librarydetail.asp?catgory=book

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Special Publication 800-86 Guide to Integrating Forensic Techniques into Incident Response Recommendations of the National Institute of Standards and Technology.

Kime, C. (2023, May 16). How to Prevent SQL Injection: 5 Key Prevention Methods. https://www.esecurityplanet.com/threats/how-to-prevent-sql-injection-attacks/

Kurii, Y., & Opirskyy, I. (n.d.). *Analysis and Comparison of the NIST SP 800-53 and ISO/IEC 27001:2013*.

Lely Maulida (2017). Antivirus Bisa Hadang *Ransomware* WannaCry?. Diakses pada 6 April 2024 dari https://techno.okezone.com/read/2017/05/16/207/1692651/antivirus-bisa-hadang-ransomware-wannacry

Lu, C.-W., Chu, W. C., Chang, C.-H., Chung, Y.-C., Liu, X., & Yang, H. (1996). Reverse Engineering. In *Handbook of Software Engineering and Knowledge Engineering* (Vol. 2).

Mahkamah Konstitusi. (2008). Undang-undang (UU) Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Mahkamah Konstitusi. (2022). RUU tentang Perlindungan Data dan Informasi Pribadi.

Maison Sylvester Amanyi (2023). Keep Your Online Wolrd Safe ! CSRF. Diakses pada 6 April 2024 dari https://www.linkedin.com/posts/maisonarmani_csrf-cybersecurity-staysafeonline-activity-7122208257712037888-qL9T

Manico, J., M, J., Wall, K. W., & Heigh, S. Z. (n.d.). SQL Injection Prevention Cheat Sheet. Retrieved October 7, 2023, from

McGuire, M., & Downling, S. (2013). *Cyber crime: A review of the evidence Research Report 75 Cyber crime: A review of the evidence*.

Meghan Jacquot (2024). Differences of Stored XSS and Reflected XSS. Diakses pada 6 April 2024 dari https://www.inspectiv.com/articles/differences-of-stored-xss-and-reflected-xss

Milad et al (2018). AITSteg: An Innovative Text Steganography Technique for Hidden Transmission of Text Message via Social Media. Diakses pada 6 April 2024 dari https://www.researchgate.net/publication/327034906_AITSteg_An_Innovative_Text_Steganography_Technique_for_Hidden_Transmission_of_Text_Message_via_Social_Media?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6Il9kaXJlY3QiLCJwYWdlIjoiX2RpcmVjdCJ9fQ

Moira, W. B., Stikvoort, D., et. al. (2003). Handbook for Computer Security Incident Response Teams (CSIRTs). doi: 10.1184/R1/6574055.v1

Murphy, D. (2023, November 23). *What is a DNS Attack? Types and How to Prevent Them*. https://www.lepide.com/blog/what-is-a-dns-attack/

Natalie Polly (2023). Easy Tips to Stop Getting spam emails. Diakses pada 6 April 2024 dari https://setapp.com/how-to/stop-spam-emails

National Institute of Standards and Technology (2020). Data Integrity : Detecting and Responding to Ransomware and Other Destructive Events. Diakses pada 6 April 2024 dari https://www.nccoe.nist.gov/publication/1800-26/VolA/index.html

National Security Agency. (2021). *WHAT CAN I DO TO PRE VENT/MITIGATE?*

Neal Poole (2011). XSS Vulnerability in Facebook Translations. Diakses pada 6 April 2024 dari https://nealpoole.com/blog/2011/03/xss-vulnerability-in-facebook-translations/

Nera Besic (2021). How DOM Based XSS Attacks work. Diakses pada 6 April 2024 dari https://brightsec.com/blog/dom-based-xss/

NIJ. (n.d.). Forensic Examination of Digital Evidence: A Guide for Law Enforcement. http://www.ojp.usdoj.gov/nij

NIST. 5. (2020). *NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations*. https://doi.org/10.6028/NIST.SP.800-53r5

Nolan, R., O', C., Branson, S. J., & Waits, C. (2005). First Responders Guide to Computer Forensics.

NPS Power The Power Realible (2023). Data Center Service, Design & Engineering Services. Diakses pada 6 April 2024 dari

https://nps-power.com/data-center-design-engineering-service/

OKU-CSIRT. (2021, June 14). Mengenal Perintah Dasar Iptables pada Linux. https://csirt.okukab.go.id/2021/06/14/mengenal-perintah-dasar-iptables-pada-linux/

Orellano-Benancio, L., Muñoz-Canales, R., Rodriguez-Leon, P., & Huamaní, E. L. (2021). Integrity and authenticity of digital images by digital forensic analysis of metadata. International Journal of Emerging Technology and Advanced Engineering, 11(9), 38–45. https://doi.org/10.46338/IJETAE0921_05

OWASP. (2017). OWASP Top 10 - 2017 The Ten Most Critical Web Application Security Risks. https://github.com/OWASP/Top10/issues

OWASP. (n.d.). OWASP Top 10:2021. Retrieved October 10, 2023, from https://owasp.org/Top10/

Pasang Lama Tamang (2023). HomeLab : Exploring Apache Server, Firewall management, and Network Security with Iptables. Diakses pada 6 April 2024 dari https://medium.com/@pasanglamatamang/homelab-exploring-apache-server-firewall-management-and-network-security-with-iptables-cc7da731de49

Pieter Arntz (2015). Vonteera Adware Uses Certificates to Disable Anti-Malware. Diakses pada 6 April 2024 dari https://www.malwarebytes.com/blog/news/2015/11/vonteera-adware-uses-certificates-to-disable-anti-malware

Plotlights (2023). What is Threat Intelligence. Diakses pada 6 April 2024 dari https://www.plotlights.com/blog/what-is-threat-intelligence-update-for-communicators/

Podle Rose Barfield (2021). Computer Programing a Brief Story. Diakses pada 6 April 2024 dari https://www.bricsys.com/cs-cz/blog/computer-programing-a-brief-history

Point, P. (n.d.). OS Hardening: 15 Best Practices. Retrieved October 20, 2023, from https://perception-point.io/guides/os-isolation/os-hardening-10-best-practices/

Prahassacitta, Vidya. (2019). KONSEP KEJAHATAN SIBER DALAM SISTEM HUKUM INDONESIA. Diakses pada 7 April 2024 dari https://business-law.binus.ac.id/2019/06/30/konsep-kejahatan-siber-dalam-sistem-hukum-indonesia/

Ramadhan, R. A., Rachmat Setiawan, P., & Hariyadi, D. (2022). Digital Forensic Investigation for Non-Volatile Memory Architecture by Hybrid Evaluation Based on ISO/IEC 27037:2012 and NIST SP800-86 Framework. IT Journal Research and Development, 162–168. https://doi.org/10.25299/itjrd.2022.8968

Redaksi DDTCNews (2023). Hati – hati penipuan! Perhatikan Domain Email Resmi Kantor Pajak. Diakses pada 6 April 2024 dari https://news.ddtc.co.id/hati-hati-penipuan-perhatikan-domain-email-resmi-kantor-pajak-1793953

Redhat. (2019, July 30). What is SELinux? https://www.redhat.com/en/topics/linux/what-is-selinux

Rodríguez, G. E., Torres, J. G., Flores, P., & Benavides, D. E. (2020). Cross-site scripting (XSS) attacks and mitigation: A survey. Computer Networks, 166. https://doi.org/10.1016/j.comnet.2019.106960

RSI Security (2020). What Are The Different Types of Pen Testing?. Diakses pada 6 April 2024 dari https://blog.rsisecurity.com/what-are-the-different-types-of-pen-testing/

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. In *Future Internet* (Vol. 11, Issue 4). MDPI AG. https://doi.org/10.3390/FI11040089

Samonas, S., & Coss, D. (n.d.). *THE CIA STRIKES BACK: REDEFINING CONFIDENTIALITY, INTEGRITY AND AVAILABILITY IN SECURITY*. www.jissec.org

Scarfone, K. A., & Mell, P. (2007). *Intrusion Detection and Prevention Systems*.

Scarfone, K. A., Jansen, W., & Tracy, M. (2008). *Guide to general server security*. https://doi.org/10.6028/NIST.SP.800-123

Scarfone, K. A., Souppaya, M. P., Cody, A., & Orebaugh, A. D. (2008). Technical guide to information security testing and assessment. https://doi.org/10.6028/NIST.SP.800-115

Security National Bank (2021). Could a Thief Steal Your Phone Number? Here's How SIM Swap Scams Happen. Diakses pada 6 April 2024 dari https://www.snbonline.com/about/news/how-to-prevent-sim-swap-fraud

Shipley, T. G., & Reeve, H. R. (n.d.). Collecting Evidence from a Running Computer: A Technical and Legal Primer for the Justice Community. www.search.org

Siber, B., & Negara, D. S. (2019). MENGENAL SQL INJECTION DAN CARA MENCEGAHNYA.Souppaya, M., & Scarfone, K. (2022). Guide to enterprise patch management planning. https://doi.org/10.6028/NIST.SP.800-40r4

Siddiqui, R. A. (n.d.). Bring Your Own Device (BYOD) in Higher Education: Opportunities and Challenges Elliptic curve cryptography for embedded systems View project. *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*. www.ijettcs.org

Singgi, I G. A. S. K., Suryawan, I. G. B. & Sugiartha, I N. G. (2020). Penegakan Hukum Terhadap Tindak Pidana Peretasan sebagai Bentuk Kejahatan Mayantara (CYBER CRIME).

Jurnal Konstruksi Hukum. Vol. 1, No. 2, Oktober 2020, Hal. 334-339. https://doi.org/10.22225/jkh.1.2.2553.334-339

Souppaya, M., & Scarfone, K. (2022). Guide to enterprise patch management planning. https://doi.org/10.6028/NIST.SP.800-40r4

Stelian Pilici (2014). Remove "Superfish" adware (Virus Removal Guide). Diakses pada 6 April 2024 dari https://malwaretips.com/blogs/superfish-removal/

Subhas Patil (2020). Security implementation via AWS WAF for web application. Diakses pada 6 April 2024 dari https://medium.com/@subhas_51253/security-implementation-via-aws-waf-for-web-application-89fc62d1653e

Tasril, V., Br Ginting, M., & Putera Utama Siahaan, A. (2017). *Threats of Computer System and its Prevention*. *6*(10), 448–451. www.ijsrst.com

Tekiner, E., Acar, A., Uluagac, A. S., Kirda, E., & Selcuk, A. A. (2021). *SoK: Cryptojacking Malware*. http://arxiv.org/abs/2103.03851

TRAFFIC ANALYSIS EXERCISE - BURNINCANDLE. (2022). https://www.malware-traffic-analysis.net/2022/03/21/index3.html

Ujung, A. D. & Nasution, M. I. P. (2023). *Sistem Keamanan Database*. Jurnal Penelitian Teknologi Informasi Dan Sains, Vol. 1 No. 2 Juni 2023, 50-57. https://doi.org/10.54066/jptis.v1i2.480

Ujung, Adelia Marwah & Nasution, Muhammad Irwan Padli. (2023). Sistem Keamanan Database. Jurnal Penelitian Teknologi Informasi Dan Sains, 1(2), 50–57. https://doi.org/10.54066/jptis.v1i2.480

Urgent Home Work (2022). Business Continuity and Disaster Recovery Planning. Diakses pada 6 April 2024 dari https://www.urgenthomework.com/business-continuity-and-disaster-recovery-planning

Vasilena Markova (2023). Ping of Death (PoD) – What is it, and how does it work?. Diakses pada 6 April 2024 dari https://www.cloudns.net/blog/ping-of-death-pod-what-is-it-and-how-does-it-work/

Wack, J., Cutler, K., & Pole, J. (n.d.). *Special Publication 800-41 Guidelines on Firewalls and Firewall Policy Recommendations of the National Institute of Standards and Technology*.

Wang, D., Gu, Q., Cheng, H., & Wang, P. (2016). The request for better measurement: A comparative evaluation of two-factor authentication schemes. *ASIA CCS 2016 - Proceedings of the 11th ACM Asia Conference on Computer and Communications Security*, 475–486. https://doi.org/10.1145/2897845.2897916

Wang, T., Su, Z., Xia, Y., Muppala, J., & Hamdi, M. (2015). Designing efficient high performance server-centric data center network architecture. *Computer Networks*, *79*, 283–296. https://doi.org/10.1016/j.comnet.2015.01.006

Wang, Y., Wei, J., & Vangury, K. (n.d.). *Bring Your Own Device Security Issues and Challenges*.

William Baptist (2023). The Impressive Evolution of Ransomware Code. Diakses pada 6 April 2024 dari https://dev.to/baptistsec/the-impressive-evolution-of-ransomware-code-35ja

Yang, C.-Q. (2003). Global Information Assurance Certification Paper Operating System Security and Secure Operating Systems. http://www.giac.org/registration/gsec

Yudi Prayudi (2014). Metodologi Komputer Forensik. Diakses pada 6 April 2024 dari https://focuslearn.wordpress.com/metodologi-komputer-forensik/

Zeller, W., & Felten, E. W. (2008). Cross-Site Request Forgeries: Exploitation and Prevention. http://citp.princeton.edu/csrf/

GLOSARIUM

A

Adware : Perangkat lunak secara otomatis menampilkan iklan kepada pengguna tanpa izin mereka.

Algoritma : Serangkaian instruksi atau aturan yang digunakan untuk menyelesaikan masalah atau melakukan tugas tertentu dalam komputasi atau matematika.

Antivirus : Program komputer yang dirancang untuk mendeteksi, mencegah, dan menghapus perangkat lunak jahat atau virus dari sistem komputer.

Aplikasi : Perangkat lunak yang dirancang untuk melakukan tugas tertentu atau menyediakan layanan tertentu bagi pengguna.

AppArmor : Sistem keamanan yang memungkinkan administrator sistem membatasi kemampuan program dengan profil yang ditentukan.

Attack Vector : Serangan yang merujuk pada metode atau jalur yang digunakan oleh penyerang untuk memasuki atau mengeksploitasi kerentanan dalam sistem komputer atau jaringan.

Authentication : Proses validasi atau pembuktian terhadap identitas atau kredensial yang hendak memasuk sebuah sistem atau layanan yang penting.

Availability : Ketersediaan suatu sistem dalam keadaan berfungsi.

B

Black Box Testing : Pengujian yang dilakukan untuk mengamati hasil input dan output dari perangkat lunak tanpa mengetahui struktur kode dari perangkat lunak.

Bring Your Own Device (BYOD) : Kebijakan di tempat kerja yang memungkinkan karyawan untuk menggunakan perangkat pribadi mereka sendiri untuk aktivitas kerja.

Business Continuity Plan (BCP) : proses perencanaan yang dirancang untuk memastikan bahwa suatu organisasi dapat melanjutkan operasinya dalam menghadapi gangguan atau kejadian darurat yang tak terduga.

Botnet : Jaringan komputer yang terdiri dari sejumlah besar komputer yang telah diretas atau terinfeksi dengan malware tanpa sepengetahuan pemiliknya

C

Chain of Custody : Dokumen yang mencatat perjalanan barang bukti dari penemuan hingga penyimpanan, menjaga integritas dan keaslian bukti.

CIA Triad : Konsep dasar dalam keamanan informasi yang terdiri dari Kerahasiaan (*Confidentiality*), Integritas (*Integrity*), dan Ketersediaan (*Availability*).

Cloud Computing : Model komputasi dimana sumber daya komputer seperti penyimpanan data dan pemrosesan disediakan sebagai layanan melalui internet.

Cross-site Request Forgery (CSRF) : Sebuah serangan yang terjadi pada website, namun seringkali tidak disadari oleh para pengguna.

Cross-site Scripting (XSS) : Serangan keamanan web di mana penyerang menyuntikkan skrip berbahaya ke dalam halaman web yang dilihat oleh pengguna lain.

COBIT : Kerangka kerja manajemen TI yang membantu organisasi mengelola dan mengendalikan proses TI secara efektif.

Confidentiality : Upaya pencegahan bagi mereka yang tidak berkepentingan untuk dapat mencapai informasi.

Cryptojacking : Praktik ilegal di mana penyerang menggunakan sumber daya komputer orang lain untuk menambang kriptokurensi tanpa izin.

Cybersecurity : Praktik menjaga sistem komputer, jaringan, dan data tetap aman dari serangan dan akses yang tidak sah.

Cyber Attacks : Serangan yang dilakukan secara daring terhadap sistem komputer atau jaringan untuk merusak, mencuri data, atau menyebabkan gangguan lainnya.

D

Data : Fakta atau informasi yang diorganisir atau diolah sehingga memiliki makna.

Database : Kumpulan data yang diatur secara terstruktur dan dapat diakses oleh program komputer.

Denial of Service (DoS) : Serangan yang dilakukan untuk membuat layanan atau sumber daya komputer tidak tersedia bagi pengguna yang sah.

Distributed Denial of Service (DDoS) : Serangan yang dilakukan dengan cara membanjiri sistem atau jaringan dengan lalu lintas internet yang tidak valid, sehingga menyebabkan layanan menjadi tidak tersedia untuk pengguna yang sah.

Digital Forensik : Proses menyelidiki dan menganalisis bukti digital untuk keperluan hukum atau investigasi keamanan.

Disaster Recovery Plan (DRP) : Rencana yang disiapkan oleh organisasi untuk memulihkan operasi normal setelah terjadi kejadian bencana atau gangguan serius lainnya.

Domain name System (DNS) : Sistem yang menerjemahkan nama domain menjadi alamat IP untuk menghubungkan perangkat ke internet.

Dynamic Updates : Proses pembaruan yang terjadi secara otomatis dan dinamis pada suatu sistem atau perangkat lunak.

E

Eksploitasi IoT : Praktik penyalahgunaan atau penggunaan yang tidak sah terhadap perangkat *Internet of Things* (IoT)

Enkripsi : Proses mengkonversi data menjadi format yang tidak dapat dibaca atau dimengerti kecuali oleh penerima yang memiliki kunci dekripsi.

Email : Metode pengiriman pesan elektronik antara pengguna melalui jaringan komputer.

External Testing : Jenis pengujian yang dilakukan oleh pihak ketiga yang independen dari pengembang atau pemilik sistem.

Evidence Tree : Struktur hierarkis yang menampilkan seluruh isi dari drive atau media yang sedang dianalisis.

F

Firewall : Sistem keamanan yang digunakan untuk mengendalikan lalu lintas jaringan, memantau, dan memfilter data yang masuk dan keluar untuk melindungi jaringan dari serangan dan akses yang tidak sah.

Firmware : Perangkat lunak yang tertanam pada perangkat keras, seperti chip atau mikrokontroler, untuk mengontrol fungsionalitas dasar perangkat.

Framework : Kerangka kerja atau struktur yang menyediakan panduan, prinsip, dan alat untuk membangun dan mengembangkan aplikasi atau sistem.

H

Hardware : Bagian fisik dari sistem komputer yang dapat dilihat dan disentuh, seperti CPU, keyboard, mouse, dan monitor.

Hash : Fungsi matematika yang mengkonversi data menjadi nilai yang disebut hash, yang digunakan untuk mengenkripsi dan mengamankan data.

Honeypot : Sistem atau perangkat lunak yang sengaja dibuat untuk menarik serangan siber sehingga para peneliti keamanan dapat mempelajari taktik dan teknik penyerang

Hypertext Transfer Control Protocol (HTTP) : Protokol komunikasi yang digunakan untuk mentransfer data melalui internet, biasanya digunakan untuk mengakses situs web.

Hypertext Transfer Control Protocol Secure (HTTPS) : Versi aman dari protokol HTTP yang menggunakan enkripsi SSL/TLS untuk melindungi data yang ditransfer antara klien dan server.

I

Information Technology Infrastructure Library : Kerangka kerja yang menyediakan praktik terbaik dalam manajemen layanan TI untuk meningkatkan kualitas layanan dan efisiensi operasional.

Input Encoding : Proses mengubah data input menjadi format yang dapat dimengerti oleh sistem.

Integrity : Kualitas atau keadaan yang menunjukkan kesatuan yang utuh sehingga memiliki potensi dan kemampuan yang memancarkan kewibawaan atau kejujuran..

Internal Testing : Jenis pengujian perangkat lunak atau sistem yang dilakukan oleh tim atau individu yang terkait langsung dengan organisasi yang mengembangkan atau mengoperasikan sistem tersebut.

Internet Control Message Protocol : Rangkaian aturan komunikasi yang digunakan perangkat untuk mengomunikasikan kesalahan transmisi data dalam jaringan.

Internet Service Provider (ISP) : Sebuah layanan yang dikeluarkan oleh perusahaan tertentu untuk memberikan suplai Internet kepada masyarakat luas.

Internet Protocol (IP) : Protokol yang digunakan untuk mengirimkan data di jaringan komputer, termasuk di internet.

Intrusion Detection System (IDS) : Sistem keamanan komputer yang dirancang untuk mendeteksi aktivitas tidak sah atau mencurigakan pada sebuah

perangkat.

Intrusion Prevention System (IPS) : *Software* pencegahan penyusupan yang memadukan dua fungsi yaitu fungsi firewall dan Intrusion Detection system (IDS).

ISO 270001 : Standar internasional untuk manajemen keamanan informasi yang menyediakan kerangka kerja untuk melindungi kerahasiaan, integritas, dan ketersediaan informasi dalam suatu organisasi.

L

Least Privilege : Prinsip yang digunakan dalam keamanan komputer dan manajemen hak akses.

Linux : Sistem operasi berbasis kernel Linux yang bersifat open source, digunakan secara luas dalam pengembangan perangkat lunak dan sebagai platform server.

Local Area Network (LAN) : Suatu jaringan komputer yang cakupan wilayahnya hanya mencakup wilayah lokal saja atau terbatas.

Log : Catatan atau rekaman kronologis dari kegiatan yang terjadi dalam sistem komputer atau jaringan.

K

Kali Linux : Distribusi Linux khusus yang digunakan pengujian penetrasi dan keamanan komputer, dilengkapi dengan berbagai alat pengujian keamanan.

M

Malware : Perangkat lunak berbahaya yang dirancang untuk merusak, mengganggu, atau mencuri data dari sistem komputer tanpa izin pengguna.

Metadata : Informasi tentang data digital lainnya, termasuk file, pesan, gambar, suara, video, dll.

Monitoring : Pengawasan atau pemantauan terhadap suatu aktivitas, performa, atau kondisi suatu sistem.

N

Name Server : Server yang bertanggung jawab untuk menerjemahkan nama domain ke alamat IP yang sesuai.

National Institute of Standards and Technology (NIST) : Badan federal di Amerika Serikat yang mengembangkan dan menerapkan standar dan pedoman teknis mengenai teknologi.

Non-Volatile : Jenis penyimpanan data yang tidak memerlukan daya listrik untuk menyimpan data, seperti penyimpanan flash dan hard disk.

Nessus : Aplikasi Tenable Security untuk melihat *vulnerability* di dalam *network*.

O

Open Pretty Good Privacy (PGP) : Program komputer yang digunakan untuk melakukan pertukaran pesan rahasia melalui email.

OWASP (Open Web Application Security Project) : Organisasi *non-profit* yang berfokus pada keamanan aplikasi web.

OWASP Top 10 : Hasil publikasi terperinci dari penelitian yang relevan dan terkini serta didasarkan pada data yang terperinci di lebih dari 40 perusahaan mitra.

P

Password Cracking : Percobaan untuk memperoleh kata sandi seseorang dari data yang tersimpan dalam website, aplikasi, atau *database* lain.

Patch Management : proses mengelola dan menerapkan pembaruan atau "patch" ke perangkat lunak atau sistem operasi untuk memperbaiki kerentanan keamanan dan meningkatkan kinerja.

Penetration Testing : Metode untuk mengevaluasi sistem keamanan perangkat atau komputer dengan cara mensimulasikan serangan siber secara nyata.

Phising : Teknik serangan di mana penyerang mencoba memperoleh informasi sensitif seperti kata sandi atau informasi keuangan dengan menyamar sebagai entitas terpercaya melalui komunikasi elektronik.

Ping of Death : Serangan dengan cara eksploitasi program ping dengan memberikan packet yang ukurannya besar ke sistem yang dituju.

Prepared Statements : Fitur dalam pemrograman *database* yang digunakan untuk menjalankan pernyataan SQL yang telah dipersiapkan dan dioptimalkan sebelumnya oleh *database*.

Privileged Access Management (PAM) : Solusi keamanan identitas yang membantu melindungi organisasi dari ancaman *cyber* dengan memantau, mendeteksi, dan mencegah akses istimewa yang tidak sah ke sumber daya penting.

Programming : Proses membuat, merancang, dan menulis kode komputer untuk mengembangkan

aplikasi atau sistem perangkat lunak.

Proteksi : Tindakan atau mekanisme yang diimplementasikan untuk melindungi sistem komputer atau data dari akses yang tidak sah atau kerusakan.

Port : Mekanisme yang memungkinkan komputer terhubung dengan beberapa sesi koneksi dengan komputer dan program lainnya dalam jaringan.

Q

Query : Permintaan informasi atau pertanyaan tertentu dari sebuah data base yang ditulis dalam format tertentu.

R

Remote : Serangan atau perintah yang dapat dilakukan dari jarak jauh oleh penyerang.

Ransomware : Jenis malware yang mengenkripsi data pada sistem komputer korban dan meminta pembayaran tebusan (ransom) agar data tersebut dapat dipulihkan.

Resiko / Risk : Suatu kejadian yang mungkin terjadi, dan apabila terjadi akan memberikan dampak negatif pada pencapaian tujuan.

Resolver : Bagian dari sistem DNS yang bertanggung jawab untuk mengonversi nama domain ke alamat IP yang sesuai.

Resource Record (RR) : Bagian dari struktur data DNS yang menyimpan informasi tertentu terkait dengan suatu domain, seperti alamat IP atau informasi lainnya.

Response Policy Zones (RPZ) : Mekanisme yang digunakan dalam DNS untuk memberlakukan kebijakan khusus terkait resolusi nama domain.

Response Rate Limiting (RRL) : Teknik yang digunakan untuk membatasi tingkat respon dari server DNS terhadap permintaan yang berasal dari sumber yang sama dalam jangka waktu tertentu.

Reverse Engineering : Proses menganalisis produk atau sistem yang sudah ada untuk memahami cara kerjanya atau menciptakan versi baru yang serupa.

S

Sandboxes : Lingkungan terisolasi yang digunakan untuk menjalankan dan menguji perangkat lunak atau kode yang berpotensi berbahaya tanpa mempengaruhi sistem atau lingkungan produksi.

Secure / Multipurpose Internet Mail Extensions (S/MIME) : Peningkatan keamanan standar format e-mail internet MIME, yang didasarkan pada teknologi dari keamanan data RSA.

Secure Software Development Life Cycle (SSDLC) : Pendekatan pengembangan perangkat lunak yang memasukkan keamanan sebagai tanggung jawab bersama sepanjang siklus hidup pengembangan.

Security Enhanced Linux (SELinux) : Implementasi keamanan tambahan untuk kernel Linux yang menyediakan kontrol akses yang lebih ketat dan pencegahan eksploitasi.

Security Information and Event Management (SIEM) : Sistem yang mengumpulkan, menganalisis, dan melaporkan data keamanan dari berbagai sumber untuk mendeteksi dan merespons ancaman keamanan.

Security Testing : Istilah yang digunakan untuk mencari celah atau kerentanan keamanan pada perangkat lunak.

Segmentasi Jaringan	: Tindakan atau praktik membelah jaringan komputer menjadi Subnetwork, masing-masing menjadi segmen jaringan.
SELinux (Security-Enhanced Linux)	: Kerangka keamanan yang disisipkan ke dalam kernel Linux sehingga memberikan lapisan perlindungan tambahan terhadap ancaman keamanan dengan memungkinkan konfigurasi kebijakan keamanan yang ketat.
Server	: Komputer atau sistem yang menyediakan layanan, data, atau sumber daya kepada komputer atau perangkat lain dalam jaringan.
Service	: Program atau proses yang berjalan di latar belakang sebuah sistem komputer dan menyediakan fungsionalitas atau layanan tertentu kepada pengguna atau sistem lain.
Social Engineering	: Praktek manipulatif yang bertujuan untuk memanipulasi orang agar memberikan informasi rahasia atau melakukan tindakan tertentu yang menguntungkan penyerang.
Software	: Serangkaian instruksi atau program komputer yang memberikan perintah kepada perangkat keras untuk menjalankan tugas tertentu.
Spam	: Pengiriman pesan secara massal dan tidak dikehendaki penerima. Umumnya ini digunakan untuk menyebarkan konten yang tidak diinginkan, terutama iklan dan penipuan.
SSH Tunnel	: Teknik untuk memindahkan koneksi dari satu jaringan ke jaringan lain melalui koneksi SSH yang aman.

Spyware	: Salah satu ancaman yang paling umum bagi pengguna internet. Setelah diinstal, ia memantau aktivitas internet, melacak kredensial login, dan memata-matai informasi sensitif
Stored Procedures	: Suatu blok program yang dapat dipanggil secara berulang-ulang dalam bentuk script
SQL Injection	: Serangan keamanan di mana penyerang memanfaatkan celah keamanan pada aplikasi web untuk menyisipkan perintah SQL yang tidak sah dan mengeksploitasi basis data yang terhubung.

T

Teknologi Informasi (TI)	: penggunaan teknologi komputer dan komunikasi untuk memproses, mengirim, dan menyimpan informasi.
TCP/IP	: Protokol komunikasi yang digunakan untuk mentransmisikan data melalui internet, terdiri dari protokol kontrol transmisi (TCP) dan protokol internet (IP).
Trojan	: Jenis malware yang menyamar sebagai program yang berguna atau sah, tetapi sebenarnya mengandung kode berbahaya yang dapat merusak atau mencuri data.
Top-Level Domain (TLD)	: Bagian teratas dalam hierarki sistem nama domain internet, seperti .com, .org, atau .net.
Two-Factor Authentication (2FA)	: Metode keamanan yang memerlukan dua bentuk verifikasi identitas yang berbeda sebelum memberikan akses, seperti kombinasi kata sandi dan kode yang dikirimkan melalui SMS.

V

Virus : Jenis malware yang dapat menggandakan dirinya sendiri dan menyebar ke komputer lain, sering kali merusak atau mencuri data.

Virtual Private Network (VPN) : Jaringan pribadi virtual yang mengamankan koneksi internet dari mata-mata dan menyediakan akses ke jaringan pribadi secara aman melalui internet publik.

VirusTotal : Layanan online yang menyediakan pemindaian antivirus terhadap file atau URL untuk mendeteksi apakah mereka berisi malware.

Volatile : Jenis penyimpanan data yang memerlukan daya listrik untuk menyimpan data, seperti RAM, yang kehilangan data saat daya dimatikan.

Vulnerability : Kelemahan atau celah dalam perangkat lunak atau sistem yang dapat dieksploitasi oleh penyerang untuk merusak, mengganggu, atau mencuri data.

Vulnerability Assessment : Proses identifikasi, evaluasi, dan mitigasi kerentanan dalam perangkat lunak atau sistem komputer untuk meningkatkan keamanan.

W

Windows : Sistem operasi yang dikembangkan oleh Microsoft, digunakan secara luas di komputer pribadi dan server.

Wireshark : Perangkat lunak analisis jaringan yang memungkinkan pengguna untuk merekam dan menganalisis lalu lintas jaringan dalam waktu nyata

White Box Testing : Pengujian yang dilakukan untuk menguji perangkat lunak dengan cara menganalisa dan meneliti struktur internal dan kode dari perangkat lunak

Worm : Jenis *malware* yang dapat menyebar dan menggandakan dirinya sendiri secara otomatis melalui jaringan komputer, tanpa memerlukan bantuan pengguna.

Z

Zeus Trojan : Jenis *trojan* yang dirancang untuk mencuri informasi keuangan dari komputer korban, seperti detail login perbankan online.

Zone File : File yang menyimpan informasi konfigurasi tentang domain, termasuk catatan DNS yang menghubungkan nama domain dengan alamat IP.

Zone Transfer : Sebuah proses yang digunakan untuk meng-*copy* / meng-*update* informasi data zone file dari primary DNS server ke secondary DNS server

TENTANG PENULIS

I Gede Putu Krisna Juliharta
Lahir di Denpasar. Telah menempuh masa studi S1 Jurusan Teknik Informatika di Universitas Pembangunan Nasional (UPN) Yogyakarta, S2 Magister Manajemen Sistem Informasi di Universitas Udayana Bali. Terlibat dalam organisasi kerelawanan sebagai Ketua RTIK Bali. Saat ini, penulis fokus mengajar di bidang *cyber security* sebagai seorang Dosen di Universitas Primakara. E-mail : krisna.juliharta@gmail.com