

Perlindungan Sistem Elektronik: Khususnya Infrastruktur Informasi

Onno W. Purbo

onno@indo.net.id

X: Onno Purbo

Institut Teknologi Tangerang Selatan (ITTS)

Abstrak

Vital Information Infrastructure (VII) dan **Critical Information Infrastructure (CII)** adalah komponen esensial yang mendukung sektor-sektor penting seperti energi, transportasi, kesehatan, keuangan, dan pemerintahan. **VII** mencakup sistem dan aset teknologi informasi yang esensial bagi kelangsungan operasional suatu organisasi atau sektor tertentu, seperti sistem perbankan internal atau basis data rumah sakit. Gangguan pada VII dapat menyebabkan kerugian operasional atau finansial bagi organisasi terkait, namun biasanya tidak berdampak pada skala nasional. Sebaliknya, **CII** meliputi infrastruktur yang sangat krusial bagi keberlangsungan ekonomi, keamanan nasional, dan kesejahteraan masyarakat secara luas, seperti jaringan listrik nasional, sistem komunikasi darurat, atau infrastruktur keuangan negara. Karena dampaknya yang lebih luas dan kritis, **CII** biasanya dilindungi oleh regulasi keamanan nasional, sementara VII lebih bergantung pada kebijakan internal atau standar industri masing-masing sektor. Ancaman terhadap infrastruktur ini mencakup serangan siber seperti Distributed Denial of Service (DDoS), ransomware, phishing, dan eksploitasi zero-day, serta gangguan teknologi dan ancaman fisik seperti bencana alam. Dampak dari ancaman tersebut meliputi kerugian ekonomi, ketidakstabilan sosial, ancaman terhadap keamanan nasional, dan hilangnya kepercayaan publik. Untuk mengatasi tantangan ini, diperlukan strategi komprehensif yang mencakup penerapan siklus **Plan-Do-Check-Act (PDCA)**, peningkatan kesadaran keamanan siber, investasi dalam teknologi pertahanan, dan kerjasama antara sektor publik dan swasta. Selain itu, implementasi arsitektur Zero Trust, penggunaan enkripsi data, sistem deteksi dan pencegahan intrusi, serta **pengembangan sumber daya manusia** di bidang keamanan siber menjadi langkah penting dalam memperkuat ketahanan VII dan CII.

Lisensi

Creative Commons Attribution 4.0 International (CC BY 4.0): Karya ini dilisensikan di bawah Lisensi Atribusi 4.0 Internasional Creative Commons. Anda bebas untuk berbagi, mengadaptasi, dan menyebarkan materi ini dalam bentuk apapun atau media apapun, termasuk untuk tujuan komersial, selama Anda menyebutkan **nama penulis aslinya**.

Kata Pengantar

Dalam era digital yang semakin maju, ancaman terhadap keamanan informasi menjadi semakin kompleks dan beragam. Berbagai insiden siber yang terjadi telah menimbulkan kerugian signifikan bagi organisasi, perusahaan, dan individu. Oleh karena itu, penanganan insiden siber yang efektif dan efisien menjadi kebutuhan yang mendesak. Buku ini hadir sebagai panduan komprehensif untuk membantu para profesional keamanan siber, praktisi TI, pengelola jaringan, dan semua pihak yang terlibat dalam menjaga keamanan sistem informasi.

Melalui buku ini, pembaca akan memperoleh pemahaman mendalam tentang konsep Vital Information Infrastructure (VII) dan Critical Information Infrastructure (CII), termasuk perbedaan, karakteristik, serta contoh kasus yang relevan. Selain itu, buku ini membahas berbagai ancaman dan dampak yang mungkin terjadi pada infrastruktur informasi, serta strategi perencanaan, implementasi, dan perlindungan yang dapat diterapkan. Pembahasan mengenai siklus Plan-Do-Check-Act (PDCA) dan pentingnya sumber daya manusia dalam keamanan informasi juga disajikan secara detail.

Kami berharap buku ini dapat menjadi referensi yang bermanfaat dalam meningkatkan kesiapan dan respons terhadap insiden siber. Dengan pengetahuan dan strategi yang tepat, diharapkan para pembaca dapat mengidentifikasi, merespons, dan memitigasi ancaman siber dengan lebih efektif, sehingga keamanan dan integritas sistem informasi dapat terjaga dengan baik.

Jakarta, Februari 2025
Onno W. Purbo

Daftar Isi

Abstrak.....	1
Lisensi.....	1
Kata Pengantar.....	2
Daftar Isi.....	3
BAB 1: Pendahuluan.....	5
Snapshot Terkini.....	5
Definisi Vital Information Infrastructure (VII).....	6
Karakteristik Vital Information Infrastructure (VII).....	6
Contoh Infrastruktur yang Termasuk dalam VII.....	7
Definisi Critical Information Infrastructure (CII).....	7
CII Menurut Beberapa Sumber Resmi.....	7
Karakteristik Critical Information Infrastructure.....	8
Sektor yang Termasuk dalam CII.....	9
Regulasi dan Perlindungan CII.....	9
Perbedaan antara Vital Information Infrastructure (VII) dan Critical Information Infrastructure (CII).....	10
Kasus Vital Information Infrastructure (VII).....	11
Kasus Critical Information Infrastructure (CII).....	11
Summary Vital Information Infrastructure (VII) dan Critical Information Infrastructure (CII). 12	
Referensi Tambahan.....	13
BAB 2: Ancaman & Dampak terhadap Infrastruktur Informasi.....	14
Ancaman Siber.....	14
Gangguan Teknologi.....	15
Ancaman Fisik.....	15
Dampak dari Ancaman terhadap VII / CII.....	15
Ancaman Cyber Attack terhadap Infrastruktur Informasi.....	16
Dampak dari Serangan Siber.....	17
Catatan SDM Cyber Security.....	18
BAB 3: Strategi untuk Perencanaan & Implementasi Information Infrastructure.....	19
Siklus Plan-Do-Check-Act (PDCA).....	19
Lebih Detail untuk Mendukung PDCA di CII.....	20
Sumber Daya Manusia Information Infrastructure.....	22
BAB 4: Strategi Perlindungan Infrastruktur Informasi.....	23
Contoh Software / Aplikasi Open Source.....	24
BAB 5: Backup.....	26
Backup - Rsync dan Cronopete.....	27
Backup - Bera.....	28
Backup - Tar.....	29
Backup - Cpio.....	30
Backup - DD Command.....	30
Backup - SCP dan Timeshift.....	30
Backup - Profesional Backup & Recovery.....	32

Backup - MySQL database.....	32
Backup - Cron dan scheduling.....	33
Backup - Checksum check.....	35
Apa itu hashing?.....	35
Jenis kriptografi hash apa yang mungkin Anda gunakan dengan Linux?.....	36
Generate checksum secara manual:.....	37
Check dan bandingkan checksum.....	37
Backup -Shell Script.....	38
BAB 6: Wazuh.....	40
Wazuh Kebutuhan Hardware dan Pendukungnya.....	41
Wazuh Manager Install Script.....	41
Wazuh Agent Install Script.....	43
Wazuh GUI Dashboard.....	46
BAB 7: Open Course.....	49
BAB 8: Kesimpulan.....	53
Referensi.....	55
Tentang Penulis.....	56

BAB 1: Pendahuluan

Vital Information Infrastructure (VII) dan Critical Information Infrastructure (CII) merupakan dua (2) jenis infrastruktur informasi yang memiliki peran penting dalam mendukung operasional berbagai sektor, tetapi dengan tingkat dampak dan perlindungan yang berbeda. VII merujuk pada sistem dan aset teknologi informasi yang sangat penting bagi kelangsungan bisnis atau sektor tertentu, seperti sistem perbankan internal atau database rumah sakit. Gangguan pada VII dapat menyebabkan kerugian operasional atau finansial bagi organisasi terkait, tetapi tidak selalu berdampak pada skala nasional. Sementara itu, CII mencakup infrastruktur yang sangat krusial bagi keberlangsungan ekonomi, keamanan nasional, dan kesejahteraan masyarakat secara luas, seperti jaringan listrik nasional, sistem komunikasi darurat, atau infrastruktur keuangan negara. Karena dampaknya yang lebih luas dan kritis, CII biasanya dilindungi oleh regulasi keamanan nasional, sedangkan VII lebih bergantung pada kebijakan internal atau standar industri masing-masing sektor.

Snapshot Terkini

Indonesia saat ini menghadapi tantangan serius dalam hal keamanan siber, terutama terkait dengan Critical Information Infrastructure. Serangan siber yang menargetkan sektor-sektor vital seperti energi, keuangan, dan kesehatan telah meningkat secara signifikan. Misalnya, serangan ransomware baru-baru ini berhasil melumpuhkan Pusat Data Nasional Sementara (PDNS) di Surabaya, mengganggu layanan untuk hampir 300 instansi pemerintah pusat dan daerah, termasuk layanan imigrasi dan operasional bandara.

<https://csirt.or.id/berita/keamanan-siber-indonesia>

Selain itu, Indonesia mengalami lonjakan serangan siber yang signifikan. Menurut laporan dari ESET, sebuah perusahaan antivirus ternama, Indonesia mencatat lebih dari 13,6 juta insiden siber hanya dalam bulan Juni 2024.

<https://cyberhub.id/berita/lonjakan-serangan-siber-indonesia>

Kerugian ekonomi akibat serangan siber mencapai proporsi yang sangat besar, dengan Indonesia mencatat kerugian finansial tertinggi di Asia, mencapai angka yang signifikan.

<https://pustanas.unas.ac.id/2024/06/04/lonjakan-serangan-siber-ancam-infrastruktur-vital-indonesia/>

Salah satu faktor yang memperburuk situasi ini adalah kurangnya sumber daya manusia (SDM) yang kompeten di bidang keamanan siber. Badan Siber dan Sandi Negara (BSSN) mengungkapkan bahwa Indonesia membutuhkan sekitar 8.000 SDM dengan kualifikasi keamanan siber, namun saat ini hanya mampu mencetak sekitar **100 lulusan per tahun**.

<https://validnews.id/nasional/bssn-ungkap-indonesia-kekurangan-sdm-keamanan-siber>

Kekurangan ini menyebabkan banyak instansi pemerintah dan perusahaan swasta rentan terhadap serangan siber karena kurangnya tenaga ahli yang mampu mengidentifikasi dan menangani ancaman tersebut.

Untuk mengatasi tantangan ini, diperlukan upaya kolaboratif antara pemerintah, sektor swasta, dan institusi pendidikan. Peningkatan investasi dalam pendidikan dan pelatihan keamanan siber menjadi krusial untuk membangun SDM yang kompeten. Selain itu, implementasi kebijakan keamanan siber yang komprehensif dan peningkatan kesadaran akan pentingnya perlindungan data di kalangan masyarakat juga menjadi langkah penting dalam memperkuat ketahanan siber Indonesia.

Definisi Vital Information Infrastructure (VII)

Vital Information Infrastructure (VII) adalah sistem, jaringan, atau aset informasi yang sangat penting bagi kelangsungan operasional suatu organisasi, industri, atau sektor tertentu. Meskipun gangguan pada VII dapat menyebabkan kerugian finansial atau operasional yang signifikan, dampaknya tidak selalu berskala nasional atau mengancam keamanan publik secara luas seperti **Critical Information Infrastructure (CII)**.

Karakteristik Vital Information Infrastructure (VII)

- **Penting untuk Kelangsungan Bisnis atau Organisasi**
 - VII mendukung operasi inti perusahaan atau institusi dan berfungsi sebagai aset strategis.
- **Dampak Gangguan Terbatas pada Organisasi atau Sektor Tertentu**
 - Jika VII terganggu, efeknya akan terasa di tingkat organisasi atau industri tertentu, tetapi tidak selalu mempengaruhi keamanan nasional.
- **Perlindungan Bergantung pada Kebijakan Internal atau Standar Industri**
 - VII biasanya dilindungi oleh protokol keamanan internal perusahaan atau standar keamanan yang berlaku di sektor industri terkait.
- **Tidak Selalu Masuk dalam Regulasi Keamanan Nasional**
 - Berbeda dengan CII yang mendapatkan perlindungan dari undang-undang pemerintah, VII sering kali berada di bawah kendali organisasi itu sendiri.

Contoh Infrastruktur yang Termasuk dalam VII

Sektor	Contoh Vital Information Infrastructure (VII)
Keuangan	Sistem perbankan internal, aplikasi mobile banking, jaringan ATM lokal
Kesehatan	Database pasien rumah sakit, sistem rekam medis elektronik, perangkat IoT medis
Pendidikan	Sistem e-learning universitas, database akademik, portal administrasi kampus
Telekomunikasi	Jaringan internal penyedia layanan internet, pusat data penyedia hosting
Transportasi	Sistem manajemen tiket kereta, aplikasi ride-hailing, sistem navigasi bandara
E-commerce & Retail	Server transaksi toko online, sistem CRM pelanggan, gateway pembayaran digital
Media & Hiburan	Platform streaming video/audio, sistem manajemen konten berita
Energi & Utilitas	Sistem manajemen jaringan listrik lokal, sistem pemantauan distribusi air
Pemerintahan	Database kependudukan daerah, sistem administrasi pajak daerah

Tabel ini mencerminkan bahwa **VII** bersifat vital untuk operasional sektor tertentu tetapi tidak selalu memiliki dampak keamanan nasional seperti **CII**.

Definisi Critical Information Infrastructure (CII)

Critical Information Infrastructure (CII) adalah sistem, jaringan, dan aset teknologi informasi yang sangat penting bagi kelangsungan hidup suatu negara, ekonomi, dan keamanan nasional. Gangguan, kerusakan, atau eksploitasi terhadap infrastruktur ini dapat menyebabkan **konsekuensi serius**, termasuk gangguan layanan publik, krisis ekonomi, ketidakstabilan sosial, atau ancaman terhadap keamanan nasional.

CII Menurut Beberapa Sumber Resmi

- **International Telecommunication Union (ITU)**

*Critical Information Infrastructure refers to systems and assets, whether physical or virtual, that are essential for the functioning of a society and economy, and whose failure would have a significant impact on **national security, economic security, or public health and safety**.*

- **European Union Agency for Cybersecurity (ENISA)**
*CII includes information and communication technology systems that support critical sectors such as energy, finance, health, and government. The security and resilience of these infrastructures are **vital to national stability**.*
- **National Institute of Standards and Technology (NIST), USA**
*CII is composed of information systems and networks that underpin the critical infrastructure sectors, providing essential services that, if disrupted, would have a debilitating **impact on national security and economic continuity**.*

Karakteristik Critical Information Infrastructure

- **Berkaitan dengan Layanan Publik dan Keamanan Nasional**
 - CII mencakup sistem yang mendukung **fungsi penting negara** dan masyarakat luas.
- **Memiliki Dampak Besar jika Terkena Gangguan**
 - Serangan atau kegagalan sistem CII dapat menyebabkan **pemadaman listrik massal, gangguan perbankan, atau kegagalan sistem transportasi**.
- **Menjadi Target Utama Ancaman Siber**
 - Aktor jahat, termasuk hacker, kelompok kriminal, dan aktor negara (state-sponsored actors) sering menyerang CII untuk spionase, sabotase, atau keuntungan finansial.
- **Memerlukan Proteksi dan Regulasi Ketat**
 - **Pemerintah** biasanya memiliki kebijakan dan regulasi untuk melindungi, mendeteksi, dan merespons ancaman terhadap CII.

Sektor yang Termasuk dalam CII

Menurut banyak negara dan organisasi keamanan siber global, **Critical Information Infrastructure** mencakup sektor-sektor berikut:

Sektor	Contoh CII dalam Sektor Tersebut
Energi	Sistem SCADA untuk jaringan listrik, jaringan tegangan tinggi 150 KV dan 500 KV, pembangkit listrik, dan pipa gas.
Keuangan	Infrastruktur perbankan, sistem pembayaran elektronik, dan pasar saham.
Telekomunikasi	Jaringan telepon, internet, penyedia layanan cloud, dan pusat data nasional.
Transportasi	Sistem navigasi udara, pengendalian lalu lintas, infrastruktur kereta api, dan pelabuhan.
Kesehatan	Database rekam medis elektronik, jaringan rumah sakit, dan sistem distribusi obat.
Pemerintahan	Infrastruktur e-Government, sistem militer, dan layanan administrasi publik.
Air dan Sanitasi	Sistem pengolahan air minum dan limbah.
Keamanan Publik	Jaringan komunikasi polisi, sistem darurat 911/112, dan sistem pemantauan keamanan nasional.

Regulasi dan Perlindungan CII

Banyak negara telah mengadopsi kebijakan khusus untuk melindungi Critical Information Infrastructure. Beberapa di antaranya:

1. **Amerika Serikat** – *Cybersecurity and Infrastructure Security Agency (CISA)* mengawasi keamanan infrastruktur kritis di AS.
2. **Uni Eropa** – *NIS Directive (Network and Information Systems Directive)* yang mengatur perlindungan infrastruktur digital.
3. **Indonesia** – Peraturan terkait keamanan siber dalam **Peraturan Presiden No. 82 Tahun 2022 tentang Perlindungan Vital Information Infrastructure** yang menetapkan sektor-sektor prioritas dan tanggung jawab pemangku kepentingan.

Perbedaan antara Vital Information Infrastructure (VII) dan Critical Information Infrastructure (CII)

Meskipun kedua istilah ini sering digunakan dalam konteks **keamanan siber dan perlindungan infrastruktur**, terdapat perbedaan dalam cakupan, dampak, dan tingkat kepentingannya. Berikut adalah perbandingan utama:

Aspek	Vital Information Infrastructure (VII)	Critical Information Infrastructure (CII)
Definisi	Infrastruktur informasi yang penting bagi organisasi atau industri tertentu, tetapi tidak selalu berdampak luas jika terganggu.	Infrastruktur informasi yang sangat penting bagi keamanan nasional, ekonomi, dan kesejahteraan publik, di mana gangguan dapat menyebabkan konsekuensi besar.
Dampak jika terganggu	Gangguan dapat mempengaruhi operasi bisnis atau layanan tertentu, tetapi tidak selalu menimbulkan dampak nasional yang luas.	Gangguan dapat mengancam keamanan nasional, stabilitas ekonomi, kesehatan masyarakat, atau bahkan menyebabkan bencana besar.
Cakupan	Fokus pada sektor atau organisasi tertentu (misalnya, perusahaan teknologi, manufaktur, atau layanan finansial tertentu).	Meliputi sektor-sektor strategis seperti energi, transportasi, layanan kesehatan, pemerintahan, dan komunikasi publik.
Contoh Infrastruktur	- Server internal perusahaan - Sistem perbankan dalam suatu cabang bank - Pusat data layanan cloud - Sistem reservasi maskapai penerbangan	- Jaringan listrik nasional - Infrastruktur telekomunikasi negara - Sistem pembayaran dan perbankan nasional - Sistem pertahanan militer dan keamanan negara
Regulasi dan Perlindungan	Mungkin memiliki kebijakan keamanan internal atau diatur oleh standar industri, tetapi tidak selalu menjadi prioritas utama bagi pemerintah.	Dilindungi oleh kebijakan keamanan nasional dan regulasi yang ketat karena dampaknya yang lebih luas terhadap masyarakat dan negara.
Prioritas dalam Keamanan Siber	Keamanan tetap penting, tetapi pendekatan yang diterapkan lebih berfokus pada mitigasi risiko spesifik untuk organisasi atau industri.	Keamanan sangat ketat dengan pendekatan " defense-in-depth ", sering melibatkan kolaborasi antara sektor publik dan swasta untuk menjaga ketahanan infrastruktur.

Kasus Vital Information Infrastructure (VII)

- **Gangguan pada Pusat Data E-commerce**
 - Jika server suatu perusahaan e-commerce mengalami downtime karena kegagalan sistem atau serangan siber, perusahaan tersebut akan mengalami kerugian finansial dan terganggunya operasional bisnis. Namun, dampaknya tidak akan meluas ke sektor publik atau keamanan nasional.
 - **Contoh:** Serangan DDoS terhadap marketplace online yang menyebabkan situs tidak bisa diakses selama beberapa jam, merugikan penjual dan pembeli tetapi tidak mempengaruhi pelayanan publik secara luas.
- **Serangan Ransomware pada Rumah Sakit Lokal**
 - Jika sistem rekam medis elektronik di rumah sakit tertentu terkena serangan ransomware, layanan kesehatan di rumah sakit tersebut akan terganggu, tetapi dampaknya hanya terbatas pada pasien dan staf di rumah sakit itu sendiri, tidak secara nasional.
 - **Contoh:** Serangan ransomware pada rumah sakit di kota kecil yang menyebabkan keterlambatan dalam pelayanan pasien dan pengelolaan data medis, tetapi tidak berdampak pada sistem kesehatan nasional.
- **Gangguan pada Sistem Perbankan Internal**
 - Jika sistem perbankan internal sebuah bank mengalami gangguan, pelanggan bank tersebut tidak dapat melakukan transaksi sementara. Namun, jika tidak melibatkan sistem perbankan nasional, dampaknya hanya terbatas pada nasabah bank tersebut.
 - **Contoh:** Server mobile banking bank swasta mengalami downtime selama beberapa jam, menyebabkan nasabah kesulitan bertransaksi tetapi tidak berdampak pada stabilitas ekonomi nasional.

Kasus Critical Information Infrastructure (CII)

- **Serangan terhadap Sistem Kelistrikan Nasional**
 - Jika sistem kelistrikan nasional mengalami serangan siber, hal ini dapat menyebabkan pemadaman listrik berskala luas, yang berpotensi mengganggu layanan publik, transportasi, komunikasi, hingga keamanan negara.
 - **Contoh:** Serangan siber terhadap sistem kelistrikan nasional yang menyebabkan pemadaman listrik di berbagai kota, berdampak pada rumah sakit, layanan darurat, dan infrastruktur transportasi.
- **Serangan terhadap Infrastruktur Transportasi Nasional**
 - Jika sistem manajemen lalu lintas udara atau transportasi publik diserang, hal ini dapat menyebabkan kekacauan besar dalam mobilitas masyarakat dan aktivitas ekonomi.
 - **Contoh:** Serangan terhadap sistem kontrol lalu lintas udara yang menyebabkan pesawat mengalami penundaan atau kegagalan komunikasi dengan pilot, membahayakan keselamatan penerbangan.

- **Serangan terhadap Jaringan Bahan Bakar atau Pasokan Energi**
 - Jika jaringan distribusi bahan bakar atau sistem penyediaan energi nasional diserang, dapat menyebabkan krisis energi yang berdampak luas pada masyarakat dan perekonomian.
 - **Contoh:** Serangan terhadap **Colonial Pipeline** di AS (2021) yang menyebabkan gangguan pasokan bahan bakar di berbagai wilayah, memicu kepanikan masyarakat dan lonjakan harga bahan bakar.

Perbedaan utama antara VII dan CII terletak pada cakupan dampaknya—VII berdampak pada organisasi atau sektor tertentu, sedangkan CII memiliki konsekuensi yang lebih luas terhadap keamanan nasional dan kesejahteraan publik.

Summary Vital Information Infrastructure (VII) dan Critical Information Infrastructure (CII)

- **Perbedaan Fokus dan Dampak:**
 - **VII** lebih berfokus pada kepentingan sektor atau organisasi tertentu, sedangkan **CII** memiliki cakupan lebih luas dan berdampak langsung pada keamanan nasional serta masyarakat.
 - Semua **CII** adalah **VII**, tetapi tidak semua **VII** adalah **CII** karena tidak semua infrastruktur vital bagi organisasi memiliki dampak nasional.
- **Perlindungan dan Regulasi:**
 - **VII** memiliki perlindungan yang lebih fleksibel dan bergantung pada kebijakan internal organisasi atau standar industri.
 - **CII** memiliki regulasi ketat karena dampaknya yang luas terhadap ekonomi, keamanan, dan kesejahteraan publik.
- **Tanggung Jawab Keamanan:**
 - Perusahaan atau organisasi bertanggung jawab atas keamanan **VII** mereka sendiri.
 - **CII** diawasi oleh otoritas nasional dan mendapat perlindungan dari regulasi serta teknologi keamanan mutakhir.
- **Risiko dan Konsekuensi Gangguan:**
 - Gangguan terhadap **VII** dapat menghambat operasi bisnis atau sektor tertentu tanpa dampak luas secara nasional.
 - Gangguan terhadap **CII** dapat menyebabkan konsekuensi besar, seperti pemadaman listrik, gangguan perbankan, atau krisis keamanan nasional.
 - **CII** menjadi target utama serangan siber dan harus dilindungi melalui kerja sama antar-lembaga serta negara.
- **Sumber daya manusia (SDM) yang kompeten** dalam bidang keamanan siber memainkan peran krusial dalam melindungi Vital Information Infrastructure (VII) dan Critical Information Infrastructure (CII). Kekurangan SDM yang berkualitas dapat meningkatkan kerentanan terhadap serangan siber, yang berpotensi mengganggu

operasional sektor-sektor penting dan mengancam keamanan nasional. Oleh karena itu, investasi dalam pengembangan dan pelatihan SDM keamanan siber menjadi sangat penting untuk memastikan ketahanan infrastruktur informasi yang vital.

Referensi Tambahan

Sulit untuk menjelaskan dengan detail berbagai hal teknis terkait pengamanan infrastruktur informasi dalam tulisan terbatas ini. Sangat disarankan untuk membaca lebih detail tentang teknik penanganan dan keamanan Internet dari buku berikut:

- Onno W. Purbo, Jimmy Alberto, Hafizhan Irawan, Bagus Gede Arta Perdana, Aolia Ikhwanudin, Muhamad Yusuf, Agianto Syamhalim, Tubagus Toifur, Ibnu Mas'ud, Dimaz Arno Prasetyo, Tubagus Asep Nurdin. Buku Pegangan Penanganan Insiden Siber. Yogyakarta: Andi Publisher; 2023.
- Hartono, Onno W. Purbo. Membangun dan Menguji Keamanan Website. Yogyakarta: Andi Publisher; 2022.

Untuk icip2 tersedia Bab tentang Backup dan Wazuh. Tentunya materi yang lebih lengkap dapat di baca di buku di atas. Juga sangat disarankan untuk enroll dan membaca kuliah online FREE di

opencourse.itts.ac.id

BAB 2: Ancaman & Dampak terhadap Infrastruktur Informasi

Vital Information Infrastructure (VII) dan **Critical Information Infrastructure (Critical Information Infrastructure/CII)** adalah komponen esensial yang mendukung fungsi utama masyarakat, termasuk sektor energi, transportasi, kesehatan, keuangan, dan pemerintahan. Karena peranannya yang krusial, infrastruktur ini sering menjadi target berbagai ancaman yang dapat mengganggu operasional dan menimbulkan dampak signifikan. Berikut adalah beberapa ancaman utama yang dihadapi oleh **VII** dan **CII**:

Ancaman Siber

- **Serangan DDoS (Distributed Denial of Service):** Penyerang membanjiri jaringan atau server dengan lalu lintas palsu, menyebabkan layanan tidak dapat diakses.
Contoh: Serangan DDoS terhadap Dyn DNS pada tahun 2016 yang mengakibatkan gangguan pada layanan seperti Twitter, GitHub, dan Netflix.
- **Ransomware:** Peretas mengenkripsi data penting dan meminta tebusan untuk memulihkan akses.
Contoh: Serangan ransomware WannaCry pada tahun 2017 yang menginfeksi rumah sakit, perusahaan, dan organisasi pemerintah di seluruh dunia.
- **Phishing & Rekayasa Sosial:** Penipuan yang mengelabui pengguna untuk mengungkapkan informasi sensitif atau kredensial akses.
Contoh: Email phishing yang menyamar sebagai institusi terpercaya untuk mencuri data login pengguna.
- **Eksplorasi Zero-Day:** Penyerang memanfaatkan celah keamanan yang belum diketahui atau belum diperbaiki.
Contoh: Eksplorasi EternalBlue oleh WannaCry yang memanfaatkan kerentanan di sistem Windows.
- **Serangan Supply Chain:** Menargetkan pihak ketiga atau vendor yang memiliki akses ke sistem utama.
Contoh: Serangan SolarWinds pada tahun 2020 yang berhasil menyusup ke banyak instansi pemerintah dan perusahaan melalui pembaruan perangkat lunak yang disusupi.

Gangguan Teknologi

- **Kegagalan Perangkat Keras & Perangkat Lunak:** Masalah seperti bug, crash, atau pemeliharaan yang buruk dapat menyebabkan gangguan operasional.
- **Ketergantungan pada Vendor Pihak Ketiga:** Jika vendor mengalami gangguan atau masalah keamanan, sistem utama dapat terkena dampaknya.

Ancaman Fisik

- **Bencana Alam:** Peristiwa seperti gempa bumi, banjir, dan kebakaran dapat merusak pusat data dan jaringan komunikasi.
- **Aksi Terorisme dan Sabotase:** Serangan fisik yang ditujukan pada infrastruktur teknologi, seperti pemadaman listrik skala besar atau perusakan fasilitas penting.

Dampak dari Ancaman terhadap VII / CII

Serangan dan gangguan terhadap infrastruktur ini dapat menimbulkan berbagai dampak serius, antara lain:

- **Kerugian Ekonomi:** Gangguan operasional dapat menyebabkan kerugian finansial yang signifikan dan biaya pemulihan yang tinggi.
- **Ketidakstabilan Sosial:** Gangguan pada layanan penting seperti listrik atau sistem keuangan dapat memicu kepanikan dan ketidakpercayaan di masyarakat.
- **Ancaman terhadap Keamanan Nasional:** Serangan yang menargetkan sistem pertahanan atau komunikasi dapat melemahkan keamanan suatu negara.
- **Hilangnya Kepercayaan Publik:** Kebocoran atau manipulasi data sensitif dapat menurunkan kepercayaan masyarakat terhadap institusi terkait.

Untuk mengatasi ancaman-ancaman tersebut, diperlukan pendekatan keamanan yang komprehensif, termasuk peningkatan kesadaran keamanan siber, investasi dalam teknologi pertahanan, dan kerjasama antara sektor publik dan swasta.

Ancaman Cyber Attack terhadap Infrastruktur Informasi

Vital Information Infrastructure (VII) dan **Information Informasi Kritis (CII)** adalah komponen esensial yang mendukung berbagai sektor penting seperti energi, transportasi, kesehatan, keuangan, dan pemerintahan. Karena peranannya yang krusial, **VII / CII** sering menjadi target utama serangan siber yang dapat mengakibatkan dampak signifikan terhadap stabilitas dan keamanan suatu negara. Berikut adalah beberapa ancaman siber utama yang mengincar **VII / CII**:

- **Serangan DDoS (Distributed Denial of Service):** Penyerang membanjiri server atau jaringan dengan lalu lintas berlebihan, menyebabkan pelayanan menjadi tidak dapat diakses oleh pengguna yang sah. Serangan semacam ini dapat melumpuhkan operasi layanan publik dan sektor bisnis yang bergantung pada infrastruktur digital.
Contoh: Serangan DDoS terhadap Dyn DNS (2016) yang menyebabkan gangguan pada layanan seperti Twitter, GitHub, dan Netflix.
- **Ransomware:** Peretas menginfeksi sistem dengan malware yang mengenkripsi data penting, kemudian menuntut tebusan untuk memulihkan akses tersebut. Serangan ransomware dapat menyebabkan gangguan operasional yang parah, terutama jika data yang disandera berkaitan dengan layanan kritis.
Contoh: Serangan ransomware WannaCry (2017) yang menginfeksi rumah sakit, perusahaan, dan organisasi pemerintah di seluruh dunia.
- **Phishing dan Rekayasa Sosial:** Melalui teknik manipulasi psikologis, penyerang mengelabui pengguna untuk mengungkapkan informasi sensitif seperti kredensial akses. Metode ini sering digunakan sebagai langkah awal untuk mendapatkan akses tidak sah ke sistem **VII / CII**.
- **Eksplotasi Zero-Day:** Penyerang memanfaatkan kerentanan perangkat lunak yang belum diketahui atau belum diperbaiki oleh pengembang. Eksplotasi semacam ini berpotensi menyebabkan kerusakan besar sebelum patch keamanan tersedia.
Contoh: Eksplotasi EternalBlue oleh WannaCry, yang menggunakan kerentanan di Windows untuk menyebar secara luas.
- **Ancaman Persisten Lanjutan (Advanced Persistent Threats/APT):** Serangan jangka panjang yang dilakukan oleh kelompok peretas profesional dengan tujuan mencuri data sensitif atau mengganggu sistem kritis. APT sering kali sulit dideteksi karena penyerang berusaha tetap tersembunyi dalam sistem untuk waktu yang lama.
Contoh: APT29 (Cozy Bear) yang diyakini berafiliasi dengan Rusia dan menargetkan lembaga pemerintah serta sektor energi.
- **Serangan Supply Chain:** Penyerang menargetkan vendor atau pihak ketiga yang memiliki akses ke sistem utama. Dengan mengeksploitasi hubungan ini, mereka dapat menyusup ke dalam Vital Information Infrastructure tanpa terdeteksi.
Contoh: Serangan SolarWinds (2020) yang berhasil menyusup ke banyak instansi pemerintah dan perusahaan melalui pembaruan perangkat lunak yang disusupi.

- **Manipulasi Data dan Disinformasi:** Penyerang tidak hanya mencuri data tetapi juga mengubahnya, yang dapat merusak kredibilitas organisasi.
Contoh: Serangan terhadap sektor perbankan atau pemilu yang **bertujuan menciptakan ketidakpercayaan publik.**

Dampak dari Serangan Siber

Serangan siber dapat menimbulkan berbagai dampak serius, antara lain:

- **Gangguan Operasional:** Layanan publik dan sektor bisnis dapat terhenti, mengakibatkan kerugian ekonomi yang signifikan.
- **Kerugian Finansial:** Biaya pemulihan sistem, kehilangan pendapatan, dan potensi pembayaran tebusan dapat membebani organisasi secara finansial.
- **Kehilangan Data Sensitif:** Informasi penting dapat dicuri atau dirusak, yang dapat mengancam privasi dan keamanan nasional.
- **Penurunan Kepercayaan Publik:** Insiden keamanan dapat mengurangi kepercayaan masyarakat terhadap kemampuan institusi dalam melindungi data dan menyediakan layanan yang andal.

Untuk mengatasi ancaman-ancaman tersebut, diperlukan pendekatan keamanan yang komprehensif, termasuk peningkatan kesadaran keamanan siber, investasi dalam teknologi pertahanan, dan kerjasama antara sektor publik dan swasta.

Catatan SDM Cyber Security

Kekurangan sumber daya manusia (SDM) yang kompeten di bidang keamanan siber di Indonesia telah menjadi perhatian serius. Badan Siber dan Sandi Negara (BSSN) mengungkapkan bahwa Indonesia membutuhkan sekitar 10.000 SDM keamanan siber setiap tahun untuk mengimbangi peningkatan anomali siber dan aktivitas digital masyarakat. Namun, saat ini, kapasitas pendidikan dan pelatihan hanya mampu menghasilkan sekitar **100 lulusan per tahun**, menciptakan kesenjangan yang signifikan antara kebutuhan dan ketersediaan tenaga ahli.

<https://mediaindonesia.com/teknologi/671079/kasus-serangan-siber-strategi-perlindungan-sdm-dan-regulasi-keamanannya>

Untuk mengatasi tantangan ini, diperlukan strategi pengembangan SDM yang komprehensif dan berkelanjutan. Salah satu langkah penting adalah meningkatkan kerjasama dengan pihak swasta dalam upaya mencapai pengembangan SDM siber nasional yang lebih maksimal. <https://jurnalprodi.idu.ac.id/index.php/MP/article/view/630> Perlu menginisiasi pembentukan **Lembaga Sertifikasi Profesi (LSP) sebagai langkah strategis untuk meningkatkan kualitas SDM**. LSP ini bertujuan memastikan bahwa tenaga kerja di bidang keamanan siber memiliki kompetensi yang profesional dan berdaya saing.

<https://institute.ojk.go.id/ojk-institute/id/news/read/1503/hadapi-serangan-siber-bssn-siapkan-ribuan-sdm-yang-kompeten-lewat-hal-ini> Dengan implementasi strategi-strategi tersebut, diharapkan Indonesia dapat membangun SDM keamanan siber yang kompeten, profesional, dan mampu menghadapi berbagai ancaman siber yang semakin kompleks.

BAB 3: Strategi untuk Perencanaan & Implementasi Information Infrastructure

Siklus Plan-Do-Check-Act (PDCA)

Siklus **Plan-Do-Check-Act (PDCA)** adalah kerangka kerja iteratif yang digunakan untuk perbaikan berkelanjutan dalam berbagai proses, termasuk perencanaan, implementasi, dan operasionalisasi **Critical Information Infrastructure (CII)** dan **Vital Information Infrastructure (VII)**. Dengan menerapkan PDCA, organisasi dapat memastikan bahwa infrastruktur informasi mereka tetap aman, andal, dan sesuai dengan kebutuhan yang terus berkembang. Berikut adalah penerapan siklus PDCA dalam konteks CII dan VII:

- **Plan (Perencanaan)** - Tahap ini melibatkan identifikasi dan analisis aset kritis serta potensi ancaman yang mungkin dihadapi. Langkah-langkah spesifik meliputi:
 - **Pemetaan Infrastruktur Kritis:** Mengidentifikasi aset, sistem, dan jaringan yang memiliki dampak signifikan terhadap keamanan nasional, ekonomi, dan layanan publik.
 - **Analisis Risiko & Dampak:** Mengevaluasi kemungkinan ancaman seperti serangan siber, bencana alam, kegagalan teknis, atau sabotase, serta menganalisis skenario gangguan dan dampaknya terhadap layanan publik serta keamanan negara.
- **Do (Pelaksanaan)** - Pada tahap ini, rencana yang telah disusun diimplementasikan dengan fokus pada penguatan keamanan infrastruktur. Langkah-langkah yang diambil antara lain:
 - **Penerapan Kebijakan & Regulasi Keamanan:** Mengikuti standar keamanan global seperti ISO 27001, NIST Cybersecurity Framework, dan menyesuaikan dengan regulasi nasional terkait keamanan siber dan perlindungan infrastruktur kritis.
 - **Keamanan Jaringan & Sistem:** Menerapkan arsitektur Zero Trust untuk mengamankan akses ke sistem CII, penggunaan enkripsi data, firewall tingkat tinggi, serta sistem deteksi & pencegahan intrusi (IDS/IPS).
 - **Redundansi & Rencana Pemulihan Bencana:** Membangun infrastruktur cadangan seperti backup data, server mirror, dan sistem failover, serta membuat prosedur pemulihan bencana untuk memastikan kelangsungan layanan dalam kondisi darurat.
- **Check (Pemeriksaan)** - Setelah implementasi, penting untuk memantau dan menilai efektivitas langkah-langkah yang telah diambil. Ini melibatkan:
 - **Sistem Pemantauan & Deteksi Dini:** Mengimplementasikan Security Information and Event Management (SIEM) untuk deteksi ancaman secara real-time, serta menggunakan Artificial Intelligence (AI) & Machine Learning untuk mendeteksi anomali dalam jaringan.
 - **Simulasi & Pengujian Keamanan:** Melakukan **penetration testing** dan **red teaming** untuk menguji ketahanan sistem, serta mengadakan latihan

tabletop dengan skenario ancaman untuk meningkatkan respons keamanan.

- **Act (Tindakan)** - Berdasarkan hasil evaluasi, organisasi harus mengambil tindakan korektif atau preventif untuk meningkatkan sistem. Langkah-langkah ini meliputi:
 - **Manajemen Krisis & Respons Insiden:** Membentuk **Cyber Emergency Response Team (CERT)**, **Computer Security Incident Response Team (CSIRT)** atau **Security Operation Center (SOC)** untuk menangani serangan siber, serta menyusun protokol komunikasi darurat untuk memastikan koordinasi antar-lembaga dalam penanganan insiden.
 - **Peningkatan Kesadaran & Pelatihan:** Melatih staf dan pemangku kepentingan tentang cyber hygiene, kesadaran phishing, dan keamanan sistem informasi, serta mengadakan pelatihan berkala untuk meningkatkan kesiapan terhadap serangan siber dan gangguan operasional.

Dengan menerapkan siklus PDCA secara konsisten, organisasi dapat memastikan bahwa CII dan VII mereka tetap aman, efisien, dan mampu beradaptasi dengan ancaman serta perubahan yang terjadi. Pendekatan ini mendukung perbaikan berkelanjutan dan memastikan bahwa langkah-langkah keamanan selalu relevan dan efektif.

Lebih Detail untuk Mendukung PDCA di CII

Untuk memastikan keamanan dan ketahanan **Critical Information Infrastructure (CII)**, perencanaan dan implementasi harus dilakukan dengan strategi yang sistematis dan berbasis risiko. Berikut adalah strategi utama dalam perencanaan dan implementasi CII:

- **Identifikasi & Klasifikasi Infrastruktur Kritis** - Analisis skenario gangguan dan dampaknya terhadap layanan publik serta keamanan negara.
 - **Pemetaan Infrastruktur Kritis**
 - Identifikasi aset, sistem, dan jaringan yang memiliki dampak signifikan terhadap keamanan nasional, ekonomi, dan layanan publik.
 - Kategorisasi berdasarkan sektor (keuangan, energi, telekomunikasi, transportasi, dll.).
 - **Analisis Risiko & Dampak** - Evaluasi kemungkinan ancaman seperti serangan siber, bencana alam, kegagalan teknis, atau sabotase.
- **Penguatan Keamanan Infrastruktur**
 - **Penerapan Kebijakan & Regulasi Keamanan**
 - Mengikuti standar keamanan global seperti ISO 27001, NIST Cybersecurity Framework, dan GDPR (jika berlaku).
 - Menyesuaikan dengan regulasi nasional terkait keamanan siber dan perlindungan infrastruktur kritis.
 - **Keamanan Jaringan & Sistem**
 - Menerapkan Zero Trust Architecture untuk mengamankan akses ke sistem CII.
 - Penggunaan enkripsi data, firewall tingkat tinggi, sistem deteksi & pencegahan intrusi (IDS/IPS).
 - **Redundansi & Disaster Recovery Plan**

- Membangun infrastruktur cadangan (backup data, server mirror, failover system).
 - Membuat prosedur pemulihan bencana (**Disaster Recovery Plan – DRP**) untuk memastikan kelangsungan layanan dalam kondisi darurat.
- **Monitoring & Manajemen Ancaman**
 - **Sistem Pemantauan & Deteksi Dini**
 - Implementasi **Security Information and Event Management (SIEM)** untuk deteksi ancaman secara real-time.
 - Menggunakan **Artificial Intelligence (AI) & Machine Learning** untuk mendeteksi anomali dalam jaringan.
 - **Simulasi & Pengujian Keamanan**
 - Melakukan **penetration testing** dan **red teaming** untuk menguji ketahanan sistem.
 - Mengadakan **tabletop exercises** dengan skenario ancaman untuk meningkatkan respons keamanan.
 - **Manajemen Krisis & Respons Insiden**
 - Membentuk **Cyber Emergency Response Team (CERT)**, **Computer Security Incident Response Team (CSIRT)** atau **Security Operation Center (SOC)** untuk menangani serangan siber.
 - Menyusun protokol komunikasi darurat untuk memastikan koordinasi antar-lembaga dalam penanganan insiden.
- **Kolaborasi & Kesadaran Keamanan**
 - **Kerja Sama dengan Pemerintah & Swasta**
 - Melibatkan otoritas nasional, sektor swasta, dan penyedia layanan infrastruktur dalam membangun ketahanan CII.
 - Mengembangkan kebijakan berbasis Public-Private Partnership (PPP) untuk meningkatkan efektivitas keamanan.
 - **Peningkatan Kesadaran & Pelatihan**
 - Melatih staf dan stakeholder tentang cyber hygiene, phishing awareness, dan keamanan sistem informasi.
 - Mengadakan pelatihan berkala untuk meningkatkan kesiapan terhadap serangan siber dan gangguan operasional.
- **Evaluasi & Pengembangan Berkelanjutan**
 - **Audit & Peninjauan Berkala**
 - Melakukan audit keamanan infrastruktur secara rutin untuk menyesuaikan dengan ancaman terbaru.
 - Mengevaluasi efektivitas kebijakan keamanan dan memperbarui framework berdasarkan pembelajaran dari insiden sebelumnya.
 - **Adopsi Teknologi Baru**
 - Menggunakan **Blockchain** untuk meningkatkan transparansi dan keamanan data.
 - Mengembangkan **AI-driven security** untuk respons otomatis terhadap ancaman siber.

Sumber Daya Manusia Information Infrastructure

Untuk memastikan perencanaan, implementasi, dan operasionalisasi infrastruktur informasi di Indonesia berjalan efektif, diperlukan strategi investasi yang komprehensif dalam pengembangan sumber daya manusia (SDM) di bidang keamanan siber. Langkah-langkah berikut dapat diambil untuk mencapai tujuan tersebut:

- **Perencanaan (Plan):**
 - **Analisis Kebutuhan SDM:** Identifikasi kebutuhan spesifik terkait jumlah dan kompetensi SDM keamanan siber yang diperlukan untuk mendukung Vital Information Infrastructure dan kritis.
 - **Pengembangan Kurikulum Pendidikan:** Bekerja sama dengan institusi pendidikan untuk mengembangkan kurikulum yang relevan dengan perkembangan teknologi dan ancaman siber terkini.
 - **Kemitraan dengan Sektor Swasta:** Meningkatkan kerja sama dengan pihak swasta untuk mendukung pengembangan SDM siber nasional yang lebih maksimal.
- **Implementasi (Do):**
 - **Program Pelatihan dan Sertifikasi:** Menyelenggarakan pelatihan berkelanjutan dan sertifikasi kompetensi untuk memastikan SDM memiliki keahlian yang diakui secara profesional.
 - **Peningkatan Kesadaran Keamanan Siber:** Melaksanakan program edukasi untuk meningkatkan kesadaran akan pentingnya keamanan siber di kalangan pegawai dan pemangku kepentingan terkait.
 - **Pengembangan Lembaga Sertifikasi Profesi (LSP):** Membentuk LSP untuk memastikan standarisasi kompetensi SDM di bidang keamanan siber.
- **Pengoperasian (Operate):**
 - **Pembentukan Tim Tanggap Insiden Siber:** Membentuk tim khusus yang bertugas memantau, mendeteksi, dan merespons insiden siber secara efektif.
 - **Pengembangan Pusat Operasi Keamanan (Security Operation Center/SOC):** Membangun SOC untuk memantau aktivitas jaringan dan mengidentifikasi potensi ancaman secara real-time.
 - **Kolaborasi Antar Lembaga:** Mendorong kerja sama antara pemerintah, sektor swasta, dan akademisi untuk berbagi informasi dan sumber daya dalam menghadapi ancaman siber.

Dengan menerapkan strategi di atas, Indonesia dapat membangun fondasi SDM keamanan siber yang kuat, memastikan infrastruktur informasi nasional terlindungi, dan meningkatkan ketahanan terhadap berbagai ancaman siber.

Perencanaan dan implementasi **Critical Information Infrastructure (CII)** harus dilakukan dengan pendekatan berbasis risiko, pemantauan berkelanjutan, dan kerja sama lintas sektor. Dengan strategi yang matang, **CII** dapat lebih tahan terhadap ancaman dan tetap beroperasi meskipun menghadapi gangguan atau serangan.

BAB 4: Strategi Perlindungan Infrastruktur Informasi

Untuk melindungi Infrastruktur Informasi di Indonesia dari berbagai ancaman siber, diperlukan strategi dan langkah taktis yang komprehensif. Berikut adalah beberapa pendekatan yang dapat diterapkan:

- **Penerapan Cyber Hygiene**
 - **Pembaruan Perangkat Lunak Secara Berkala:** Pastikan semua sistem dan aplikasi diperbarui dengan patch keamanan terbaru untuk menutup celah yang dapat dieksploitasi oleh penyerang.
 - **Penggunaan Autentikasi Multi-Faktor (MFA):** Terapkan MFA untuk menambahkan lapisan keamanan ekstra pada proses login, sehingga mengurangi risiko akses tidak sah.
 - **Pemantauan Jaringan Secara Real-Time:** Implementasikan sistem pemantauan yang mampu mendeteksi aktivitas mencurigakan secara real-time, memungkinkan respons cepat terhadap potensi ancaman.
- **Penggunaan Arsitektur Zero Trust**
 - **Verifikasi Setiap Akses:** Dalam pendekatan Zero Trust, tidak ada entitas yang dipercaya secara otomatis. Setiap permintaan akses harus diverifikasi, baik berasal dari dalam maupun luar jaringan organisasi.
- **Implementasi Sistem Deteksi dan Respons**
 - **Penggunaan Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS):** IDS dan IPS membantu dalam mendeteksi dan mencegah aktivitas berbahaya di jaringan.
 - **Pemanfaatan AI dan Machine Learning:** Gunakan teknologi AI dan machine learning untuk mengidentifikasi pola anomali dalam lalu lintas jaringan, sehingga ancaman dapat dideteksi lebih awal.
- **Backup dan Rencana Pemulihan Bencana**
 - **Backup Data Secara Rutin:** Lakukan backup data secara berkala dan simpan salinan tersebut di lokasi yang terpisah, termasuk backup offline untuk melindungi dari serangan ransomware.
 - **Latihan Simulasi Insiden Siber:** Adakan latihan rutin untuk mensimulasikan insiden siber, memastikan tim siap merespons dan memulihkan sistem dengan efisien.
- **Kolaborasi Internasional**
 - **Kerja Sama Antar Negara:** Bangun kerja sama dengan negara lain untuk berbagi informasi mengenai ancaman terbaru dan praktik terbaik dalam keamanan siber.
 - **Partisipasi dalam Forum Keamanan Siber:** Ikuti forum seperti FIRST, Europol EC3, dan ASEAN Cybersecurity Forum untuk tetap terinformasi dan

terlibat dalam diskusi keamanan siber global.

- **Kebijakan dan Regulasi**
 - **Penerapan Standar Keamanan:** Adopsi standar keamanan internasional seperti ISO 27001 dan NIST Cybersecurity Framework untuk memastikan praktik keamanan yang konsisten.
 - **Regulasi untuk Penyedia Layanan Infrastruktur Kritis:** Terapkan regulasi yang mewajibkan penyedia layanan infrastruktur kritis mematuhi standar keamanan yang ditetapkan.
- **Pengembangan dan Peningkatan SDM Keamanan Siber**
 - **Pendidikan dan Pelatihan:** Investasikan dalam program pendidikan dan pelatihan untuk menghasilkan profesional keamanan siber yang kompeten.
 - **Sertifikasi Profesional:** Dorong SDM untuk memperoleh sertifikasi internasional di bidang keamanan siber guna meningkatkan kredibilitas dan keahlian.
 - **Kesadaran Keamanan Siber:** Tingkatkan kesadaran akan pentingnya keamanan siber di seluruh level organisasi melalui kampanye dan workshop.

Dengan mengimplementasikan strategi dan langkah-langkah di atas, Indonesia dapat memperkuat perlindungan terhadap infrastruktur informasinya dan meningkatkan ketahanan terhadap ancaman siber yang terus berkembang.

Contoh Software / Aplikasi Open Source

Untuk mengimplementasikan strategi perlindungan infrastruktur informasi, berikut adalah beberapa perangkat lunak open source yang dapat digunakan:

- **Penerapan Cyber Hygiene**
 - **Pembaruan Perangkat Lunak Secara Berkala:** Menggunakan sistem manajemen patch seperti **OpenVAS** untuk mengidentifikasi kerentanan dan memastikan semua sistem diperbarui dengan patch keamanan terbaru.
 - **Penggunaan Autentikasi Multi-Faktor (MFA):** **PrivacyIDEA** adalah solusi open source yang memungkinkan implementasi MFA untuk meningkatkan keamanan akses sistem.
 - **Pemantauan Jaringan Secara Real-Time:** **Nagios**, **Zabbix**, atau **Wazuh** dapat digunakan untuk memantau jaringan dan sistem secara real-time, mendeteksi aktivitas mencurigakan, dan memberikan notifikasi dini.
- **Penggunaan Arsitektur Zero Trust**
 - **Verifikasi Setiap Akses:** **Keycloak** adalah alat open source untuk manajemen identitas dan akses yang mendukung prinsip Zero Trust dengan memastikan setiap permintaan akses diverifikasi secara ketat.
- **Implementasi Sistem Deteksi dan Respons**
 - **Penggunaan Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS):** **Snort** dan **Suricata** adalah IDS/IPS open source yang efektif untuk mendeteksi dan mencegah aktivitas berbahaya di jaringan.

- **Pemanfaatan AI dan Machine Learning: Elastic Stack (ELK Stack)** dengan modul seperti Machine Learning for ELK dapat digunakan untuk menganalisis lalu lintas jaringan dan mendeteksi anomali menggunakan teknik pembelajaran mesin.
- **Backup dan Rencana Pemulihan Bencana**
 - **Backup Data Secara Rutin: Bacula** adalah solusi backup open source yang memungkinkan penjadwalan backup rutin dan penyimpanan salinan data di lokasi terpisah.
 - **Latihan Simulasi Insiden Siber: Metasploit Framework** dapat digunakan untuk mensimulasikan serangan siber dan menguji kesiapan tim dalam merespons insiden.
- **Kolaborasi Internasional**
 - **Kerja Sama Antar Negara:** Berpartisipasi dalam komunitas open source global seperti **Open Source Security Foundation (OpenSSF)** untuk berbagi informasi mengenai ancaman terbaru dan praktik terbaik dalam keamanan siber.
- **Kebijakan dan Regulasi**
 - **Penerapan Standar Keamanan:** Mengadopsi kerangka kerja seperti **OpenSCAP** untuk memastikan kepatuhan terhadap standar keamanan seperti **ISO 27001** dan **NIST Cybersecurity Framework**.

Dengan memanfaatkan perangkat lunak open source di atas, organisasi dapat meningkatkan keamanan infrastruktur informasi mereka secara efektif dan efisien.

BAB 5: Backup

Backup dan pemulihan data memiliki peran penting dalam menjaga keamanan dan keberlanjutan operasional data. Berikut adalah penjelasan singkat tentang pentingnya backup dan pemulihan data:

- **Perlindungan terhadap Kehilangan Data:** Backup data adalah salinan cadangan dari informasi yang berharga. Jika terjadi kegagalan perangkat keras, serangan malware, bencana alam, atau kesalahan manusia, data utama dapat hilang atau rusak. Dengan adanya backup, data yang hilang dapat dipulihkan, dan kehilangan informasi yang berharga dapat diminimalkan.
- **Pemulihan Setelah Serangan Ransomware:** Serangan ransomware dapat mengenkripsi data dan meminta tebusan untuk mendapatkan kunci dekripsi. Dengan backup yang baik, Anda dapat mengabaikan permintaan tebusan dan memulihkan data dari salinan cadangan yang tidak terpengaruh oleh serangan.
- **Enkripsi semua file yang di backup:** Serangan ransomware juga akan mengcopy semua file di komputer kita ke control center attacker. Jika file tersebut tidak di enkripsi maka attacker dengan mudah membaca dan menggunakan informasi yang ada di file untuk melakukan tindak kejahatan. Jadi ransomware juga sering berfungsi sebagai extortionware juga. Untuk mengatasi ini sebaiknya semua file yang penting sebaiknya di enkripsi; semua public key kita tidak terambil oleh attacker juga.
- **Kelancaran Operasional:** Ketika data hilang atau rusak, bisnis atau organisasi dapat mengalami gangguan signifikan. Dengan backup dan pemulihan yang efektif, data dapat dipulihkan dengan cepat, memungkinkan bisnis untuk melanjutkan operasional tanpa terhenti.
- **Perlindungan terhadap Kesalahan Manusia:** Kesalahan manusia seperti penghapusan tidak sengaja atau penimpaan file dapat menyebabkan kehilangan data yang tidak dapat dipulihkan. Backup yang rutin dapat menyediakan salinan data yang dapat dikembalikan dalam kasus seperti ini.
- **Perlindungan terhadap Bencana Alami dan Kegagalan Perangkat Keras:** Bencana alam seperti kebakaran, banjir, atau gempa bumi dapat merusak perangkat keras dan menyebabkan kehilangan data. Backup offsite atau di cloud dapat memberikan perlindungan terhadap kerusakan fisik dan memungkinkan pemulihan data dari lokasi yang aman.
- **Kesempatan untuk Eksperimen dan Pengembangan:** Dengan backup yang tersedia, Anda memiliki kebebasan untuk bereksperimen dengan perubahan dalam sistem atau melakukan pengembangan baru tanpa resiko kehilangan data yang tak tergantikan. Jika ada masalah, Anda dapat dengan mudah mengembalikan sistem ke keadaan sebelumnya.
- **Kepercayaan dan Ketentuan:** Backup data memberikan rasa percaya diri dan ketenangan pikiran bahwa jika sesuatu terjadi pada data, ada cadangan yang dapat dipulihkan. Hal ini juga mendukung kepatuhan terhadap persyaratan hukum dan regulasi yang membutuhkan pemulihan data dalam jangka waktu tertentu.

Secara keseluruhan, backup dan pemulihan data adalah langkah penting dalam menjaga keberlanjutan bisnis, melindungi informasi berharga, dan mengurangi resiko kehilangan data akibat kegagalan perangkat keras, serangan malware, atau bencana alam.

Sebagai salah satu kolaborasi perangkat lunak open-source yang paling menonjol, Linux adalah sistem operasi terkemuka di 3 jenis server termasuk Linux File Server, Linux Web Server, dan Linux Database Server dengan distribusi yang luas seperti Debian, openSUSE, Fedora Linux, Ubuntu, dan ratusan lainnya.

Dikenal karena skalabilitas, keamanan kelas atas, dan fleksibilitasnya, server Linux digunakan secara luas di antara lebih dari 1 juta organisasi, yang memerlukan perlindungan data yang lengkap dan andal terhadap ancaman seperti kegagalan perangkat keras, waktu henti sistem, atau serangan dunia maya.

Cadangan adalah praktik yang terbukti untuk menghindari kehilangan data dalam bencana. Tidak hanya penting tetapi juga perlu untuk mengetahui opsi pencadangan dan pemulihan tertentu yang efektif untuk server Linux. Anda dapat mencadangkan file/folder dan server Linux ke berbagai tujuan dengan berbagai cara. Pada kesempatan ini akan dibahas tujuh (7) cara untuk melakukan backup data di Linux.

Backup - Rsync dan Cronopete

Rsync is a Linux-based utility often used to transfer and synchronize files and directories locally, to and from another host using any remote shell or to and from a remote rsync daemon.

Parameters:

-verbose, -v	increase verbosity.
-stderr=e a c	change stderr output mode (default: errors).
-quiet, -q	suppress non-error messages.
-backup, -b	create backups (see --suffix & --backup-dir).
-backup-dir=DIR	create backups into a hierarchy based on DIR.
-suffix=SUFFIX	backup suffix (default ~ w/o --backup-dir).
-update, -u	exclude files that are newer on the receiver.
-checksum, -c	skip based on checksum.
-fake-super	store/restore privileged attrs using xattrs.
-exclude=PATTERN	rule out files matching PATTERN.
-exclude-from=FILE	read exclude patterns from FILE.
-include=PATTERN	include files matching PATTERN.
-include-from=FILE	read include patterns from FILE.

Untuk melihat semua option, silahkan cek di Rsync website.

Linux Server Backup

- Insert backup medium dan locate drive menggunakan “**fdisk -l**” command.
- Buka terminal dan jalankan,
 `sudo rsync -aXv /`
 `--exclude={"/dev/*","/proc/*","/sys/*","/tmp/*","/run/*","/mnt/*","/media/*","/lost+found"} /target_folder`

Perintah ini akan mem-backup keseluruhan directory root kecuali /dev, /proc, /sys, /tmp, /run, /mnt, /media, /lost+found dan menyimpannya di folder /target_folder.

- Backup home directory dengan MS Word file yang besar dan mail folder:
rsync -aiz . bkhost:backup/user_name/

Linux Server Recovery

Cronopete adalah Linux clone dari Time Machine dan backup tool for Mac. Kita dapat mengcopy dan restore semua user file di harddisk yang berbeda, tapi tidak untuk membackup seluruh sistem operasi.

- Install Cronopete dan ketik perintah berikut di terminal:
cronopete
- Click Configure now di welcome page.
- Masukkan external HDD or USB dan click Change disk.
- Choose USB disk dan click Select. Ulangi langkah tersebut untuk backup disk lainnya.
- Klik Format disk untuk memformat disk untuk backup.
- Tool segera mulai membackup seluruh direktori \$HOME secara default. Anda dapat menentukan objek backup dari bagian Opsi dan menentukan interval waktu antar backup.
- Untuk memulihkan data, klik kanan ikon Cronopete pada menu dan pilih Restore file. Selanjutnya, pilih file atau folder sumber dari USB backup dan klik Restore file di kiri atas.

Backup - Bera

Bera adalah sistem backup untuk dengan mudah membackup semua file dan folder penting, melayani konfigurasi, dan memulihkannya di server yang sama atau memindahkannya ke server lain. Tool ini dapat melakukan backup dan pemulihan penuh, dan memigrasikan server kompleks dalam waktu 10 menit. Itu juga dapat mengecualikan domain, file, dan folder, dan menggunakan SSH untuk mengamankan transmisi.

Parameters:

backupOrigin	refers to local if the backup is on the server or SSH if it is from other locations.
backupLocalDir	local directory where the backup is located.
backupRemoteUser	connect to the backup server via SSH.
Backupremoteserver	remote SSH backup server.
backupRemotePort	SSH server port.
backupRemoteDir	remote backup directory.

Linux Server Backup

Preparation:

- Linux server
- Rsync
- SSH

Root access pada source dan target system.

- Instal sistem operasi, konfigurasi network, instal package, sampai mengkonfigurasi server.
- Download service config, file, folder dan lainnya menggunakan Bera.

```
chmod +x bera-backup.sh
chmod +x bera-restore.sh
```

- Config file dari masing-masing script perlu seperti `_bera_restore_config_example` dan `_bera_backup_config_example`
- Backup Linux server di folder yang dituju
`./bera-backup.sh PATH_TO_CONFIG_FILE`

Linux Server Recovery

- Download backup dari server dan restore,
`./bera-restore.sh PATH_TO_CONFIG_FILE`

Backup - Tar

Tar, kependekan dari tape archive, adalah untuk mengompres dan mengarsipkan beberapa file dan direktori untuk distribusi penyimpanan yang mudah, yang dikenal sebagai tarball. Itu membuat backup menggunakan tar, gzip, dan bzip.

Parameters:

- c create a new archive.
- v offer verbose output.
- f define the archive file to be used.
- t make a list of the files in an archive.
- x extract the backup.
- z zip.

Linux Server Backup

- Buat tar backup
`tar -cvf backup_name.tar /home/user`
- Buat tar.gz backup
`tar -cvfz backup_name.tar.gz /home/user`
- Exclude files
`tar --exclude file.txt --exclude file.sh -cvfz backup_name.tar.gz`
- Extract content dari backup.
`tar -xvfz backup_name.tar.gz /backup/directory/file.txt`
- Arsipkan semua file di server ke dalam format gzip, kecuali backup yang dibuat sebelumnya, dan buat direktori baru untuk backup. Pastikan server tidak dalam maintenance mode.
`sudo tar -cvpzf backup_name.tar.gz --exclude=/home/server/backup.tar.gz --one-file-system`

Linux Server Recovery

- Restore tar.gz backup.
tar -xvpf /media/your_harddisk/backup.tar.gz

Backup - Cpio

Cpio, copy in/out, adalah utilitas pengarsipan file untuk membuat dan mengekstrak arsip atau menyalin file ke tempat lain.

Parameters:

- O read the standard input.
- i extract files from the standard input.
- c read or write the header information in ASCII character.
- d create directories if needed.
- u copy unconditionally so the new file won't overwrite the older file.

Linux Server Backup

- Backup files
ls file * /cpio -acvf >/root/backup.cpio
- Lihat content backup
cpio -it </root/backup.cpio
cpio -it -l /root/backup .cpio

Linux Server Recovery

- Restore backup file
cpio -icuvd </root/backup.cpio

Backup - DD Command

DD (Disk to Disk) buat backup dari satu partisi ke partisi yang lain.

Linux Server Backup

- Buat backup.
dd if=source_partition of=destination_partition
- Buat duplicate partition dengan existing partition tanpa membuat backup file.
dd if=existing_source_partition of=destination_partition

Linux Server Recovery

- Restore backup partition ke partisi empty.
dd if=destination_partition of=another_empty_partition

Backup - SCP dan Timeshift

SCP (Secure Copy) menyalin data dari satu sistem Unix/Linux ke sistem lain di mesin yang sama, dari mesin lokal ke mesin jarak jauh dan sebaliknya, atau antara server jarak jauh yang berbeda.

Parameters:

- r recursively.
- q no progress indicator is shown.
- v verbose mode.
- p copy files with the specified port number.

Linux Server Backup

Persiapan:

- Memiliki izin untuk menyalin file pada sistem target.
- Miliki akun di mesin target atau kunci publik resmi di dalamnya.
- Memiliki izin baca pada mesin sumber dan izin tulis pada target.

Backup:

- Copy file dari local ke remote server.
scp filename root@serverxxx.example.com:/root
- Copy file dari remote ke local server.
scp root@serverxxx.example.com:/root/backup*
- Replicate directory,
scp -r directory root@serverxxx.example.com: /root
- Use blowfish atau arcfour encryption untuk improve performance,
scp -c blowfish filename root@serverxxx.example.com.com:
- Specify nomor port.
scp -p xxxx backup_file root@serverxxx.example.com:/tmp

Linux Server Recovery

Timeshift adalah tool pemulihan sistem yang sudah diinstal sebelumnya di beberapa distro Linux dan memungkinkan recovery waktu tertentu.

Recovery:

- Install Timeshift di terminal.

On Ubuntu and derivatives:

```
sudo add-apt-repository -y ppa:teejee2008/timeshift
sudo apt-get update
sudo apt-get install timeshift
```

On Fedora, CentOS, and RHEL:

```
sudo dnf install timeshift
```

On Arch Linux and Manjaro:

```
yay -S timeshift
```

- Buka Applications menu, search, dan launch Timeshift. Masukkan credential / password dan press Authenticate.
- Set setting preferences pada Setup Wizard.
 - Pilih snapshot type antara Rsync dan Btrfs dan click Next.
 - Specify lokasi untuk Timeshift snapshot dan click Next.
 - Pilih snapshot frequency tergantung seberapa sering perubahan di elemen sistem kita.

- Pilih snapshot level dan click Next.
- Pilih backup home folder ke snapshot atau tidak dan Next.
- Click Finish.
- Click Restore di main window saat sistem bekerja, dan select snapshot yang akan di restore restore.

Backup - Profesional Backup & Recovery

Menggunakan jasa profesional Backup & Recovery yang mampu untuk 12 virtual machine platform (seperti VMware, Hyper-V, Xen, Oracle OLVM, dll.), 6 databases, NAS, dan Windows/Linux Server. Dia menyediakan backup yang cepat dan efektif dan worry-free recovery option dengan extremely affordable dan flexible pricing model.

Profesional backup support platform Linux berikut:

- File backup:
 - Debian Linux 10.1 to 11.5
 - Ubuntu Linux 14 to 22
- Server backup:
 - RedHat Enterprise Linux 6(6.0/6.8), 7(6.2/7.6), 8(8.0/8.1)
 - CentOS Linux 6(6.5/6.9), 7(7.2/7.6/7.7/7.9), 8(8.0/8.3)

Fitur yang didukung:

- Automatic data backup: otomatiskan semuanya dengan jadwal pencadangan yang disesuaikan dan pemberitahuan email tentang kasus yang tidak biasa.
- Different backup type: pilihan termasuk Full, Differential, Incremental, dan Forever Incremental Backup.
- Smart strategies: aktifkan deduplikasi dan kompresi data untuk mengurangi setengah dari ukuran cadangan dan Transfer Terenkripsi dengan teknik SSL untuk keamanan data selama transfer.
- Server recovery: memulihkan cadangan Server Linux dengan cepat melalui multiple transfer thread dan mengenkripsi transmisi untuk keamanan.
- Anti-ransomware protection: lindungi semua cadangan yang disimpan di server cadangan milik provider pada account user yang mencurigakan dan tidak sah.
- Offsite backup copy: simpan salinan cadangan di luar lokasi di lokasi terpencil untuk mempersiapkan yang terbaik.

Pencadangan dan pemulihan server sangat penting bagi organisasi jika terjadi kasus kehilangan data. Walaupun ada beberapa cara backup di Linux. Karena command line sering kali terlalu banyak untuk dibaca, dan ada risiko korupsi disk cadangan dan penyimpanan yang rusak, pengguna server dapat menggunakan solusi cadangan server profesional dengan GUI manajemen, berbagai opsi cadangan, dan pemulihan data.

Backup - MySQL database

Selain file / disk kita seringkali harus membackup database. Salah satu database yang banyak digunakan adalah MySQL. Berikut ini adalah cara dump database.

Dump isi database ke file.

```
/usr/bin/mysqldump -u usernamemysql -ppasswordmysql namadb -c  
/usr/bin/mysqldump -u usernamemysql -ppasswordmysql namadb -c > isidatabase.sql
```

jika kita menginginkan agar file yang dihasilkan langsung di gz, kita dapat menggunakan perintah

```
/usr/bin/mysqldump -u usernamemysql -ppasswordmysql namadb -c | /bin/gzip -9 > isidatabase.sql.gz
```

Database akan tersimpan di file

isidatabase.sql.gz

Restore Database dari backup database adalah drop database

```
mysqladmin --user=usernamemysql --password=passwordmysql --force drop namedb  
mysqladmin --user=usernamemysql --password=passwordmysql create namedb
```

contoh

```
mysqladmin --user=root --password=123456 --force drop dvwa  
mysqladmin --user=root --password=123456 create dvwa
```

restore database

```
gunzip isidatabase.sql.gz  
mysql -u usernamemysql -ppasswordmysql namedb < isidatabase.sql
```

contoh

```
mysql -u root -p123456 dvwa < backup-dvwa.sql
```

Backup - Cron dan scheduling

Cron adalah penjadwal pekerjaan di sistem operasi komputer seperti Unix. "cron" adalah singkatan dari "chronograph".

Cron memungkinkan pengguna untuk menjadwalkan pekerjaan (perintah atau shell script) untuk berjalan secara otomatis pada waktu atau tanggal tertentu. Hal ini umumnya digunakan untuk melakukan pemeliharaan atau administrasi sistem, meskipun mempunyai tujuan yang bersifat umum, cron dapat digunakan untuk keperluan lain, seperti menghubungkan ke internet dan download email.

Tabel cron biasanya dimasukkan di bawah folder

```
/var/spool/cron/crontabs/
```

Misalnya untuk user root maka file tersebut adalah

```
/var/spool/cron/crontabs/root
```

Mengedit tabel cron bisa langsung ke folder / file yang bersangkutan, atau menggunakan perintah

```
crontab -e
```

dari user yang kita inginkan

Beberapa operator / sintaks cron - ada beberapa cara untuk menentukan waktu

- koma (',') menentukan daftar nilai, contoh: "1,3,4,7,8" (spasi tidak digunakan dalam sebuah daftar).
- dash ('-') menentukan sebuah range dari nilai, contoh: "1-6", equivalen dengan "1,2,3,4,5,6"
- asterisk (*) menentukan semua nilai yang mungkin. Contoh, asterisk pada kolom jam akan sama dengan setiap jam.
- slash (/) biasa di sebut "step", biasa digunakan untuk meloncati nilai tertentu. Contoh: "*/3" dalam jam artinya sama dengan "0,3,6,9,12,15,18,21".
- Contoh berikut akan membersihkan Apache error log setiap satu menit melewati tengah malam setiap hari.

```
1 0 * * * echo "" > /www/apache/logs/error_log
```

- Contoh slash: script /home/user/test.pl akan dijalankan setiap 5 menit.

```
* /5 * * * * /home/user/test.pl
```

Format secara umum

```
.----- menit (0 - 59)
| .----- jam (0 - 23)
| | .----- hari dalam bulan (1 - 31)
| | | .----- bulan (1 - 12) ATAU jan,feb,mar,apr ...
| | | | .---- hari dalam minggu (0 - 6) (Sunday=0 or 7) ATAU
sun,mon,tue,wed,thu,fri,sat
| | | | |
* * * * * perintah yang dijalankan
```

Beberapa entry khusus yang mungkin akan berguna

Entry	Keterangan	Ekuivalen
@reboot	Run satu kali, saat start	None
@yearly	Run setahun sekali	0 0 1 1 *
@annually	(sama dengan @yearly)	0 0 1 1 *
@monthly	Run sebulan sekali	0 0 1 * *
@weekly	Run seminggu sekali	0 0 * * 0
@daily	Run sehari sekali	0 0 * * *

@midnight	(sama dengan @daily)	0 0 * * *
@hourly	Run setiap jam	0 * * * *

@reboot akan berguna jika user perlu merestart server atau daemon, atau jika user tidak dapat mengakses ke file di bawah /etc/init.d/

Menjalankan Cron melalui CLI

```
start cron
stop cron
restart cron
```

Backup - Checksum check

Cryptography pada dasarnya mempunyai tiga (3) goal / objektif / tujuan:

- Confidentiality - menjaga agar konten tidak bisa dibaca oleh unauthorized user
- Authenticity - membuktikan daripada file berasal
- Integrity - membuktikan bahwa file tidak diubah

Konsep ketiga, integritas, yang kita minati di sini. Dalam konteks ini, integritas berarti membuktikan bahwa data tidak berubah secara tiba-tiba. Membuktikan integritas berguna dalam banyak skenario:

- Unduhan internet seperti distribusi Linux, perangkat lunak, atau file data
- Transfer file jaringan melalui NFS, SSH, atau protokol lainnya
- Memverifikasi instalasi perangkat lunak
- Membandingkan nilai tersimpan, seperti kata sandi, dengan nilai yang dimasukkan oleh pengguna
- Backup yang dapat membandingkan dua file untuk melihat apakah mereka telah berubah

Apa itu hashing?

Kriptografi menggunakan hashing untuk mengonfirmasi bahwa file tidak berubah.

Penjelasan sederhananya adalah metode hashing yang sama digunakan pada file di setiap akhir unduhan Internet. File di-hash di server web oleh administrator web, dan hasil hash dipublikasikan. Seorang pengguna mengunduh file dan menerapkan metode hash yang sama. Hasil hash, atau checksum, dibandingkan. Jika checksum dari file yang diunduh sama dengan file aslinya, maka kedua file tersebut identik, dan tidak ada perubahan yang tidak terduga karena kerusakan file, serangan man-in-the-middle, dll.

Hashing adalah proses satu arah. Hasil hash tidak dapat dibalik untuk mengekspos data asli. Checksum adalah string output yang merupakan ukuran yang ditetapkan. Secara teknis, itu berarti hashing bukanlah enkripsi karena enkripsi dimaksudkan untuk dibalik (didekripsi).

Jenis kriptografi hash apa yang mungkin Anda gunakan dengan Linux?

Message Digest dan Secure Hash Algorithm:

Di Linux, Anda cenderung berinteraksi dengan salah satu dari dua metode hashing:

- MD5
- SHA256

Tool kriptografi ini dibangun di sebagian besar distribusi Linux, serta macOS. Windows biasanya tidak menyertakan utilitas ini, jadi Anda harus mengunduhnya secara terpisah dari vendor pihak ketiga jika ingin menggunakan teknik keamanan ini.

Message Digest versus Secure Hash Algorithm:

Apa perbedaan antara intisari pesan dan algoritma hash yang aman? Perbedaannya terletak pada matematika yang terlibat, tetapi keduanya mencapai tujuan yang sama. Sysadmin mungkin lebih memilih yang satu daripada yang lain, tetapi untuk sebagian besar tujuan, fungsinya serupa. Namun, mereka tidak dapat dipertukarkan. Hash yang dibuat dengan MD5 di salah satu ujung koneksi tidak akan berguna jika SHA256 digunakan di ujung lainnya. Metode hash yang sama harus digunakan di kedua sisi.

SHA256 menghasilkan hash yang lebih besar, dan mungkin membutuhkan lebih banyak waktu dan daya komputasi untuk menyelesaikannya. Ini dianggap sebagai pendekatan yang lebih aman. MD5 mungkin cukup baik untuk sebagian besar pemeriksaan integritas dasar, seperti pengunduhan file.

Kapan hashing digunakan di Linux:

Linux menggunakan hash di banyak tempat dan situasi. Checksum dapat dibuat secara manual oleh pengguna. Anda akan melihat dengan tepat bagaimana melakukannya nanti di artikel. Selain itu, kemampuan hash disertakan dengan `/etc/shadow`, `rsync`, dan utilitas lainnya.

Misalnya, kata sandi yang disimpan di file `/etc/shadow` sebenarnya adalah hash. Saat Anda masuk ke sistem Linux, proses autentikasi membandingkan nilai hash yang disimpan dengan versi hash dari kata sandi yang Anda ketikkan. Jika kedua checksum identik, maka kata sandi asli dan yang Anda ketikkan juga identik. Dengan kata lain, Anda memasukkan kata sandi yang benar. Ini ditentukan, bagaimanapun, tanpa pernah benar-benar mendekripsi kata sandi yang tersimpan di sistem Anda. Periksa dua karakter pertama dari bidang kedua untuk akun pengguna Anda di `/etc/shadow`. Jika dua karakter adalah `$1`, kata sandi Anda dienkripsi dengan MD5. Jika karakternya adalah `$5`, kata sandi Anda dienkripsi dengan SHA256. Jika nilainya `$6`, SHA512 sedang digunakan.

Hashing untuk melawan ransomware:

Untuk melawan ransomware, sebaiknya semua file yang di backup di hash. Sehingga kita dapat mengecek apakah sebuah file masih bersih dari ransomware

atau sudah terkontaminasi. Ini diperlukan untuk menentukan apakah backup tersebut masih bisa dipercaya atau tidak.

Generate checksum secara manual:

Penggunaan hash utility sangat sederhana. Berikut adalah sedikit howto-nya,

Buat file:

Buat sebuah file

```
mkdir percobaan
cd percobaan
touch original.txt
echo "informasi asli" > original.txt
```

generate MD5 checksum

```
md5sum original.txt
hasilnya,
340e9898ce273c93c5f648e49c88fa60 original.txt
```

Perhatikan nilai checksum yang dihasilkan. Simpan nilai tersebut di file untuk digunakan di kemudian hari,

```
md5sum original.txt > hashes.txt
cat hashes.txt
outputnya,
340e9898ce273c93c5f648e49c88fa60 original.txt
```

Check dan bandingkan checksum

check dua file yang sama persis:

Copy ke /tmp dan bandingkan

```
cd ~/percobaan
cp original.txt /tmp/duplicate.txt
```

check MD5

```
md5sum /tmp/duplicate.txt
Output,
340e9898ce273c93c5f648e49c88fa60 /tmp/duplicate.txt
```

check MD5 duplicate.txt masukan ke hashes.txt

```
md5sum /tmp/duplicate.txt >> hashes.txt
```

Bandingkan dua hash,

```
cat hashes.txt
```

Output,

```
340e9898ce273c93c5f648e49c88fa60 original.txt
```

```
340e9898ce273c93c5f648e49c88fa60 /tmp/duplicate.txt
```

Terlihat dengan jelas kedua hash, sama persis walaupun nama file berbeda. Artinya ke dua file sama persis.

Check dua file yang beda:

Ubah /tmp/duplicate.txt

```
echo tambahkata >> /tmp/duplicate.txt
```

check MD5

```
md5sum /tmp/duplicate.txt
```

Output,

```
6579964edfc3f80dea0463726eea8aee /tmp/duplicate.txt
```

Check otomatis dari kumpulan hashes.txt

Gunakan hashes.txt

```
md5sum --check hashes.txt
```

Hasilnya

```
original.txt: OK
```

```
/tmp/duplicate.txt: FAILED
```

```
md5sum: WARNING: 1 computed checksum did NOT match
```

Anda dapat mengulangi langkah-langkah di atas dengan mengganti perintah md5sum sha256sum untuk melihat bagaimana proses bekerja menggunakan algoritma SHA. Perintah sha256sum juga menyertakan opsi --check checksum yang membandingkan hasil hash dan menampilkan pesan apakah file berbeda.

Backup -Shell Script

Tentunya banyak hal yang harus dikerjakan adalah proses backup dapat berjalan secara periodik dibantu dengan crontab. Berikut adalah contoh shell script di linux untuk melakukan backup menggunakan rsync, generate MD5 checksum dan menambahkan timestamp di backup folder,

```
#!/bin/bash
```

```
# Source and destination directories
```

```

source_dir="/path/to/source"
destination_parent_dir="/path/to/backup"

# Rsync options
rsync_options="-av --delete"

# Create a timestamp for the backup folder
timestamp=$(date +"%Y-%m-%d_%H-%M-%S")
destination_dir="$destination_parent_dir/backup_$timestamp"

# Temporary file to store MD5 checksums
md5_file="/tmp/md5_$timestamp.txt"

# Perform the backup using rsync
rsync $rsync_options --checksum --out-format="%n" "$source_dir" "$destination_dir"

# Generate MD5 checksums for transferred files
cd "$destination_dir"
find . -type f -exec md5sum {} + > "$md5_file"

# Print the path and MD5 checksum of each file
echo "MD5 checksums:"
cat "$md5_file"

# Print the timestamp
echo "Backup timestamp: $timestamp"

# Clean up temporary file
rm "$md5_file"

```

Keterangan script:

- Variabel `destination_parent_dir` menset parent directory dimana backup folder akan dibuat. Pastikan anda mengubahnya dengan path yang kita inginkan.
- Variable `timestamp` menggunakan `date` command untuk men-generate timestamp dalam format "YYYY-MM-DD_HH-MM-SS".
- Timestamp ditambahkan ke variable `destination_parent_dir`, membuat unique backup folder setiap kali run.
- Variable `md5_file` memasyjab timestamp di filename, pastikan setiap backup run mempunyai MD5 file sendiri.
- Setelah backup dan MD5 di generate, script akan menulis MD5 checksum dan backup timestamp.
- Temporary MD5 file di bersihkan di akhir.

Ingat untuk mengganti direktori sumber dan sesuaikan `destination_parent_dir` sesuai dengan kebutuhan Anda. Anda dapat menyesuaikan format stempel waktu dengan memodifikasi argumen ke perintah tanggal.

BAB 6: Wazuh

Wazuh dapat digunakan untuk memantau titik akhir, layanan dan kontainer cloud, serta untuk menggabungkan dan menganalisis data dari sumber eksternal. Wazuh penting untuk memonitor keamanan jaringan karena memiliki beberapa keunggulan dan manfaat berikut:

- **Deteksi Ancaman Real-Time:** Wazuh menyediakan deteksi ancaman real-time yang aktif dan responsif terhadap serangan yang terjadi di jaringan. Melalui fitur deteksi Intrusion Detection System (IDS), Wazuh dapat memantau lalu lintas jaringan untuk mendeteksi aktivitas mencurigakan atau ancaman yang mungkin tidak terdeteksi oleh sistem keamanan tradisional.
- **Pengumpulan dan Analisis Log:** Wazuh mengumpulkan dan menganalisis log dari berbagai sumber di jaringan, seperti log system, log aplikasi, dan log perangkat jaringan. Dengan analisis log yang terpusat, Wazuh dapat mengidentifikasi pola dan tanda-tanda serangan yang mungkin terlewatkan, serta memberikan wawasan tentang keadaan keamanan jaringan secara menyeluruh.
- **Penyelidikan Kejadian Keamanan:** Wazuh menyediakan kemampuan untuk menyelidiki kejadian keamanan dengan melacak dan merekam aktivitas di jaringan. Hal ini memungkinkan administrator untuk menganalisis serangan yang terjadi, mengidentifikasi sumbernya, dan mengambil langkah-langkah yang tepat untuk merespons serangan tersebut.
- **Pemantauan Kepatuhan:** Wazuh dapat membantu dalam pemantauan kepatuhan terhadap kebijakan keamanan dan peraturan yang berlaku. Dengan memeriksa kepatuhan terhadap standar keamanan yang ditetapkan, seperti CIS Benchmark atau GDPR, Wazuh dapat membantu organisasi menjaga kepatuhan dan mengidentifikasi ketidaksesuaian yang mungkin mengarah pada kerentanan atau pelanggaran keamanan.
- **Integrasi dengan Solusi Keamanan Lainnya:** Wazuh dapat diintegrasikan dengan berbagai solusi keamanan lainnya, seperti SIEM (Security Information and Event Management), Endpoint Protection, atau Sistem Manajemen Keamanan (Security Management Systems). Integrasi ini memungkinkan pertukaran informasi dan koordinasi antara berbagai tool keamanan, meningkatkan kemampuan deteksi dan respons terhadap ancaman.

Secara keseluruhan, Wazuh memberikan pandangan yang komprehensif tentang keamanan jaringan, membantu mengidentifikasi ancaman yang mungkin terlewatkan, merespons serangan dengan cepat, dan menjaga kepatuhan terhadap kebijakan dan peraturan keamanan. Dengan demikian, Wazuh menjadi penting dalam menjaga dan meningkatkan keamanan jaringan suatu organisasi.

Untuk memanfaatkan sepenuhnya kemampuan manajer Wazuh dan memiliki UI yang bagus untuk visualisasi, Wazuh harus terintegrasi dengan Elastic Stack dan Kibana. Kibana untuk visualisasi, Elasticsearch untuk penyimpanan data dan mesin pencari, Filebeat untuk

mengumpulkan data manajemen Wazuh dan push data ke mesin pencari Elasticsearch. Jadi, untuk menginstal dan mengkonfigurasi pengelola Wazuh di Ubuntu 22.04, kita harus mulai dengan menyiapkan Elastic Stack; Kibana, Elasticsearch dan Filebeat.

Wazuh Kebutuhan Hardware dan Pendukungnya

Persyaratan perangkat keras sangat bergantung pada jumlah endpoint yang dilindungi dan beban kerja cloud. Angka ini dapat membantu memperkirakan berapa banyak data yang akan dianalisis dan berapa banyak peringatan keamanan yang akan disimpan dan diindeks.

Mengikuti quickstart ini berarti menerapkan Wazuh server, Wazuh indexer, dan Wazuh dashboard pada host yang sama. Ini biasanya cukup untuk memantau hingga 100 titik akhir dan selama 90 hari data peringatan yang dapat di query/ indeks. Tabel di bawah menunjukkan perangkat keras yang direkomendasikan untuk penerapan quickstart:

Tabel 6.1. Keperluan Hardware

Agent	CPU	RAM	Storage (90 hari)
1-25	4 vCPU	8 GB	50 GB
25-50	8 vCPU	8 GB	100 GB
50-100	8 vCPU	8GB	200 GB

Untuk lingkungan yang lebih besar, kami merekomendasikan penerapan terdistribusi. Konfigurasi cluster multi-node tersedia untuk Wazuh server dan Wazuh indexer, menyediakan ketersediaan tinggi dan load balancing.

Komponen utama Wazuh dapat diinstal pada sistem operasi Linux 64-bit. Wazuh merekomendasikan salah satu versi sistem operasi berikut:

- Amazon Linux 2
- CentOS 7, 8
- Red Hat Enterprise Linux 7, 8, 9
- Ubuntu 16.04, 18.04, 20.04, 22.04

Wazuh dashboard mendukung web browser berikut:

- Chrome 95 or later
- Firefox 93 or later
- Safari 13.7 or later

Browser berbasis Chromium lainnya mungkin juga berfungsi. Internet Explorer 11 tidak didukung

Wazuh Manager Install Script

Jika dibutuhkan, biasanya tidak perlu, kita dapat menginstall Wazuh GPG key

```
curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | apt-key add -
```

Unduh dan jalankan asisten instalasi Wazuh.

```
curl -sO https://packages.wazuh.com/4.4/wazuh-install.sh && sudo bash  
./wazuh-install.sh -a
```

Jika hardware yang digunakan menggunakan spec di bawah standar kita dapat memaksa installer untuk ignore hardware spec (-i)

```
curl -sO https://packages.wazuh.com/4.4/wazuh-install.sh && sudo bash  
./wazuh-install.sh -a -i
```

Setelah asisten menyelesaikan penginstalan, output menampilkan kredensial akses dan pesan yang mengonfirmasi bahwa penginstalan berhasil.

```
INFO: --- Summary ---  
INFO: You can access the web interface https://<wazuh-dashboard-ip>  
User: admin  
Password: <ADMIN_PASSWORD>  
INFO: Installation finished.
```

Contoh,

```
INFO: --- Summary ---  
INFO: You can access the web interface https://<wazuh-dashboard-ip>  
User: admin  
Password: 337SaXHs4YdC90sRhnuBzUMnrEmfVyo+  
INFO: Installation finished.
```

Anda sekarang telah menginstal dan mengkonfigurasi Wazuh.

Sebaiknya cek konfigurasi supaya bisa di akses dari remote di ossec.conf menggunakan <remote> XML tag. Secara default, akan monitor apapun IP address-nya. Jika dibutuhkan, kita dapat ubah IP address service untuk listen, sebagai berikut,

```
<ossec_config>  
  <remote>  
    <local_ip>192.168.0.65</local_ip>  
  </remote>  
</ossec_config>
```

Ini akan menset manager listen ke IP address 192.168.0.65.

Jika kita mengubah nilai parameter ossec.conf , kita perlu me-restart service.

```
systemctl restart wazuh-indexer
```

```
systemctl restart wazuh-manager
systemctl restart filebeat.service
systemctl restart wazuh-dashboard
```

Akses interface web Wazuh dengan `https://<wazuh-dashboard-ip>` dan kredensial Anda:

```
Username: admin
Password: <ADMIN_PASSWORD>
```

Saat Anda mengakses dasbor Wazuh untuk pertama kali, browser menampilkan pesan peringatan yang menyatakan bahwa sertifikat tidak dikeluarkan oleh otoritas terpercaya. Hal ini diharapkan dan pengguna memiliki opsi untuk menerima sertifikat sebagai pengecualian atau, alternatifnya, mengkonfigurasi sistem untuk menggunakan sertifikat dari otoritas terpercaya.

Anda dapat menemukan kata sandi untuk semua pengindeks Wazuh dan pengguna API Wazuh di file `wazuh-passwords.txt` di dalam `wazuh-install-files.tar`. Untuk mencetaknya, jalankan perintah berikut:

```
sudo tar -O -xvf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt
```

Jika Anda ingin menghapus instalasi komponen utama Wazuh, jalankan asisten instalasi Wazuh menggunakan opsi `-u` atau `--uninstall`.

Wazuh Agent Install Script

Agent run di host yang ingin Anda pantau dan berkomunikasi dengan server Wazuh, mengirimkan data hampir secara real-time melalui saluran terenkripsi dan diautentikasi.

Pada kesempatan ini, hanya akan diberikan catatan untuk deploy agent Wazuh pada sistem Linux menggunakan variabel penerapan yang memfasilitasi tugas penginstalan, pendaftaran, dan konfigurasi agen. Atau, jika Anda ingin menginstalasi di berbagai OS lainnya dan mengunduh langsung paket agen Wazuh, lihat bagian daftar packages <https://documentation.wazuh.com/current/installation-guide/packages-list.html>

Catatan Anda memerlukan hak pengguna root untuk menjalankan semua perintah yang dijelaskan di bawah ini.

Tambahkan Wazuh repository:

- Tambahkan repository Wazuh untuk mengunduh paket resmi.
- Install GPG key:

```
curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg
--no-default-keyring --keyring gnupg-ring:/usr/share/keyrings/wazuh.gpg
--import && chmod 644 /usr/share/keyrings/wazuh.gpg
```

- Tambahkan repository:

```
echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg]
https://packages.wazuh.com/4.x/apt/ stable main" | tee -a
/etc/apt/sources.list.d/wazuh.list
```

- Update package:

```
apt-get update
```

Deploy Wazuh agent:

Untuk men-deploy Wazuh agent pada endpoint, pilih package manager dan edit WAZUH_MANAGER variable agar berisi Wazuh manager IP address atau hostname, misalnya 192.168.0.187.

```
WAZUH_MANAGER="192.168.0.187" apt-get -y install wazuh-agent
```

atau bisa juga di ambil dari dashboard Wazuh > menu Setup Agent seperti,

```
curl -so wazuh-agent.deb
https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_
4.4.5-1_amd64.deb && sudo WAZUH_MANAGER='192.168.0.187'
WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='agent-187'
dpkg -i ./wazuh-agent.deb
```

Pastikan konfigurasi MANAGER IP di wazuh agent, di file /var/ossec/etc/ossec.conf sudah benar.

```
<ossec_config>
<client>
  <server>
    <address>192.168.0.187</address>
    <port>1514</port>
    <protocol>tcp</protocol>
  </server>
  <config-profile>ubuntu, ubuntu22, ubuntu22.04</config-profile>
  <notify_time>10</notify_time>
  <time-reconnect>60</time-reconnect>
  <auto_restart>yes</auto_restart>
  <crypto_method>aes</crypto_method>
</client>
```

Untuk opsi penerapan tambahan seperti nama agen, grup agen, dan password pendaftaran, lihat bagian Variabel penerapan untuk Linux <https://documentation.wazuh.com/current/user-manual/deployment-variables/deployment-variables-linux.html>

Catatan Selain itu, jika Anda ingin menginstal agen tanpa mendaftarkannya, abaikan variabel penerapan. Untuk mempelajari lebih lanjut tentang berbagai metode

pendaftaran, lihat bagian pendaftaran agent Wazuh
<https://documentation.wazuh.com/current/user-manual/agent-enrollment/index.html>

Aktifkan dan mulai service agent Wazuh:

```
systemctl daemon-reload
systemctl enable wazuh-agent
systemctl start wazuh-agent
systemctl status wazuh-agent
```

Proses deployment selesai, dan Wazuh agent berhasil jalan di Linux system.

Recommended Disable Wazuh update:

Kompatibilitas antara agent Wazuh dan manajer Wazuh dijamin ketika versi manajer Wazuh lebih baru atau sama dengan versi agen Wazuh. Oleh karena itu, kami menyarankan untuk menonaktifkan repositori Wazuh untuk mencegah upgrade yang tidak disengaja. Untuk melakukannya, gunakan perintah berikut:

```
sed -i "s/^deb/#deb/" /etc/apt/sources.list.d/wazuh.list
apt-get update
```

Atau, Anda dapat mengatur status paket untuk di hold. Tindakan ini menghentikan upgrade tetapi Anda masih dapat upgrade secara manual menggunakan apt-get install.

```
echo "wazuh-agent hold" | dpkg --set-selections
```

Uninstall Wazuh agent:

Jika diperlukan, untuk uninstall agent, run command berikut:

```
apt-get remove wazuh-agent
```

Beberapa file ditandai sebagai file konfigurasi. Karena penunjukan ini, pengelola paket tidak menghapus file-file ini dari sistem file. Jika Anda ingin menghapus semua file sepenuhnya, jalankan perintah berikut:

```
apt-get remove --purge wazuh-agent
```

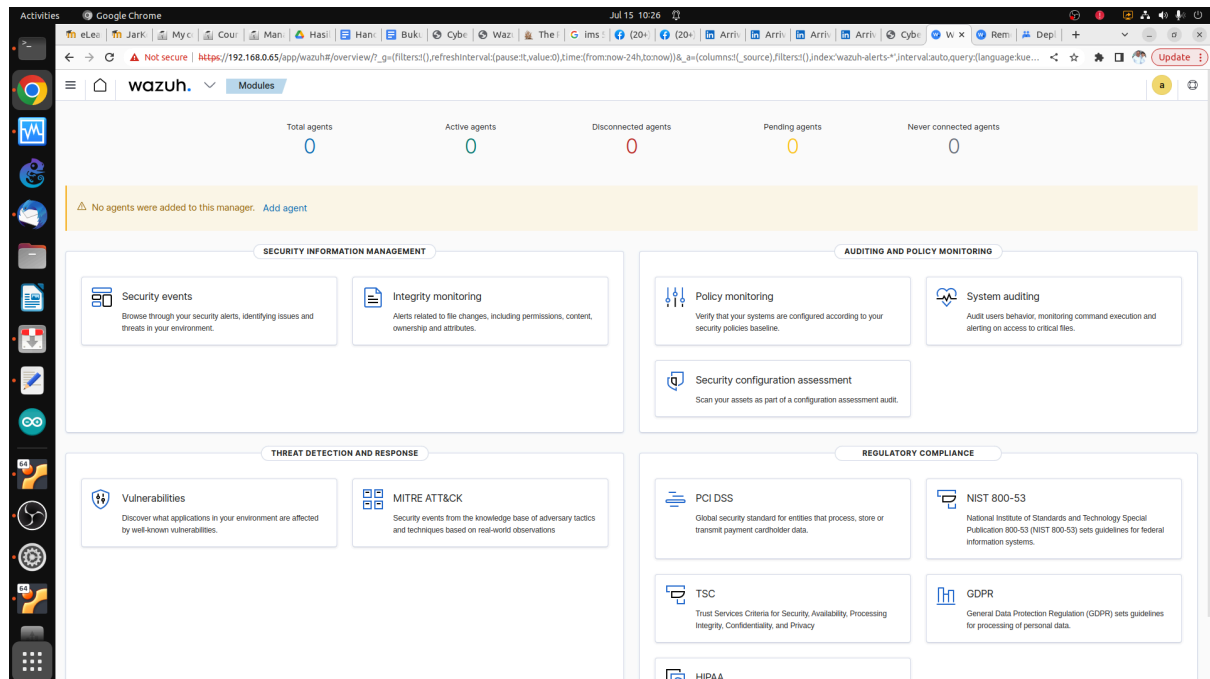
Disable Wazuh agent service:

```
systemctl disable wazuh-agent
systemctl daemon-reload
```

Sekarang, Wazuh agent berhasil di uninstall secara penuh dari Linux endpoint.

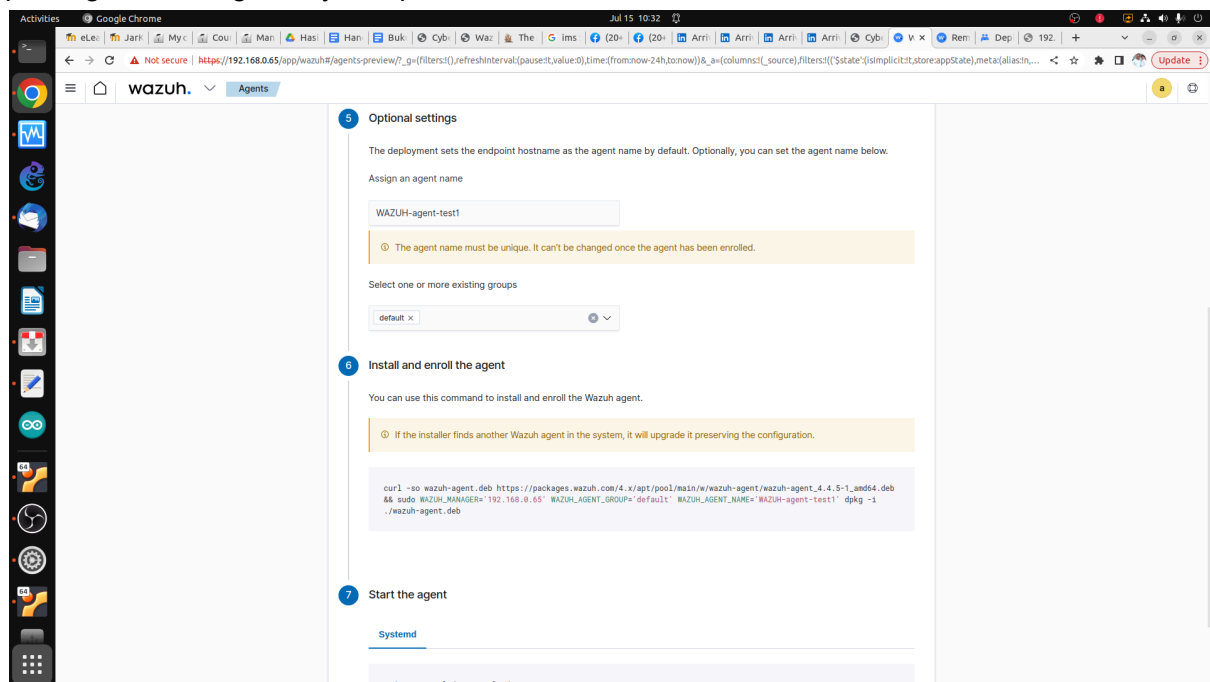
Wazuh GUI Dashboard

Berikut ini adalah beberapa penampakan GUI Web dari Wazuh.



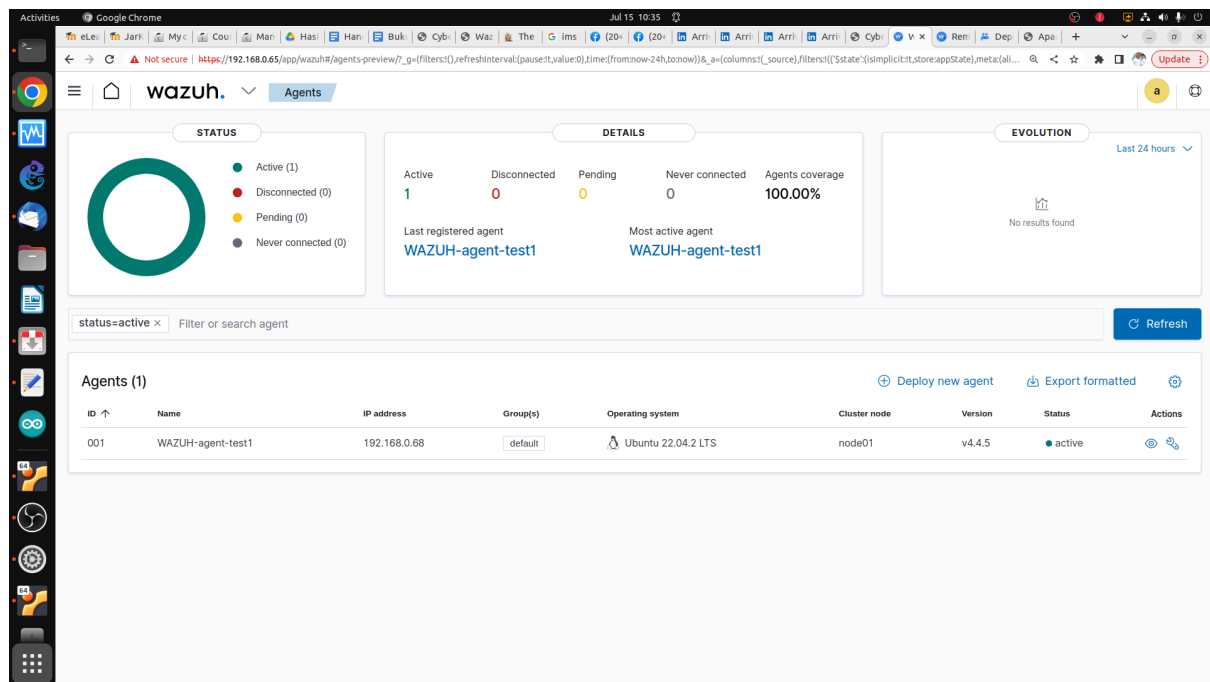
Gambar 6.1: Home Page Wazuh Manager

Gambar diatas memperlihatkan tampilan home page wazuh manager. Kita dapat melihat gambaran umum kondisi agent wazuh yang terpasang di jaringan, security information management, audit & policy monitoring, threat detection & response, dan yang tidak kalah penting adalah regulatory compliance.



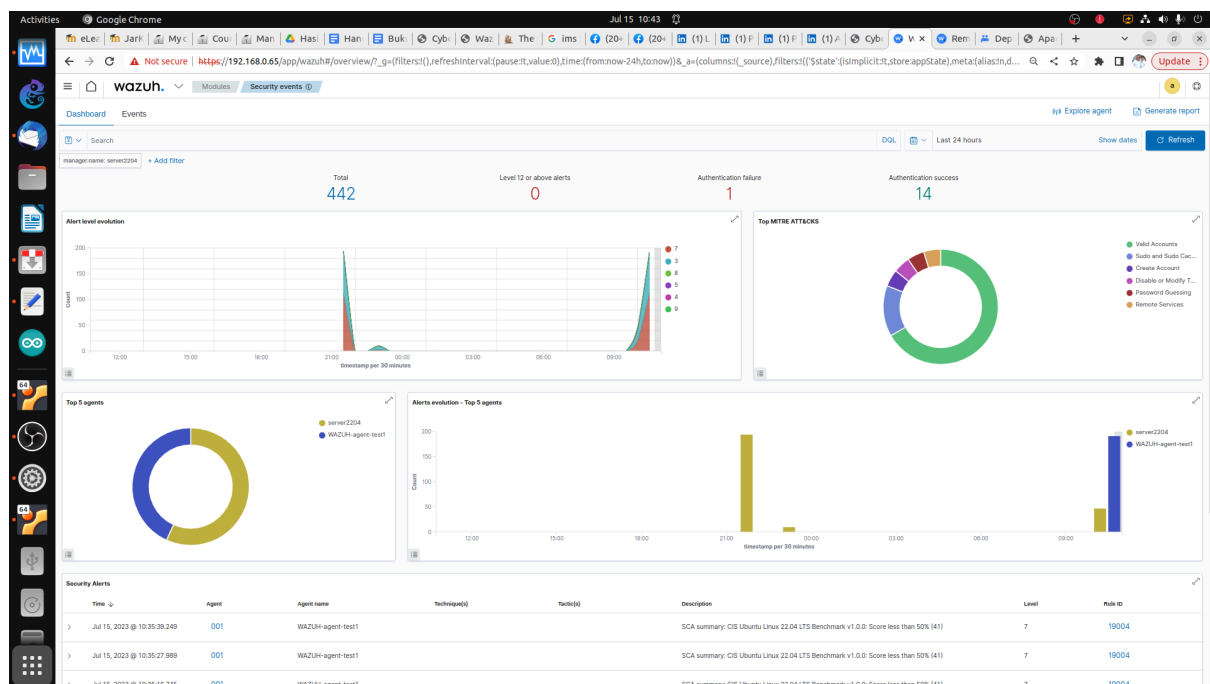
Gambar 6.2: Fitur menambahkan Agent Wazuh

Pada Wazuh terdapat fitur yang akan sangat memudahkan kita dalam menambahkan agen wazuh. Bahkan script yang perlu di paste di server yang mengoperasikan agen wazuh juga sudah tersedia.



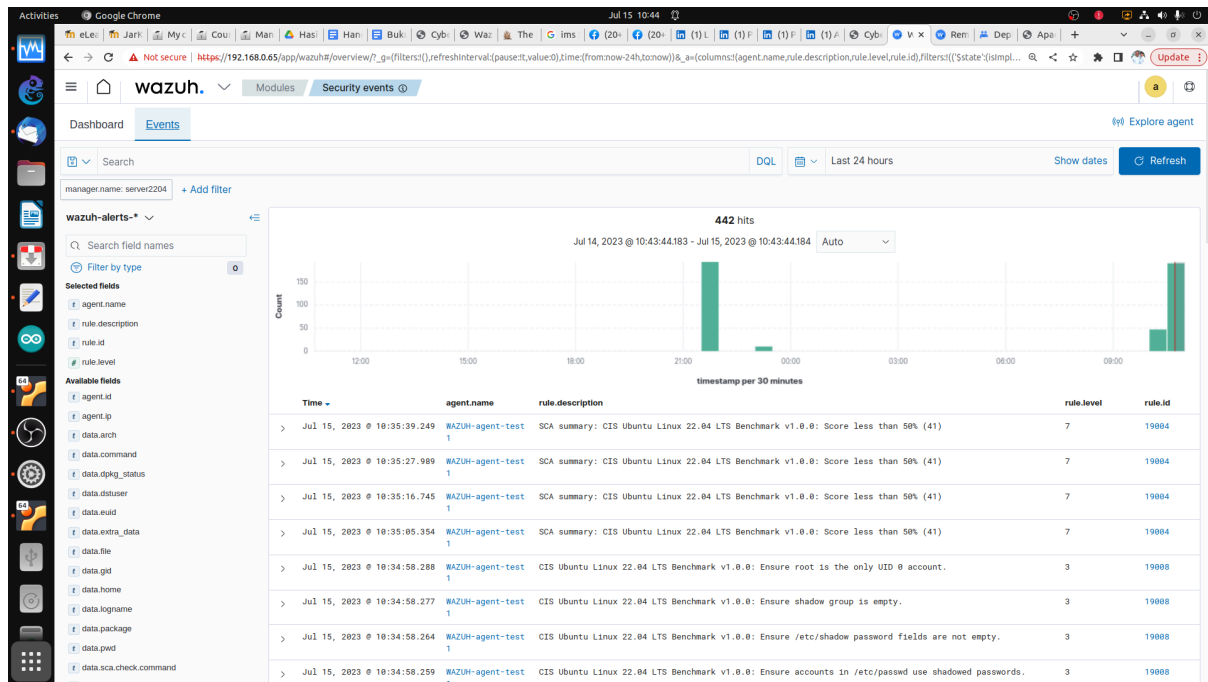
Gambar 6.3: Tampilan Monitoring Agent Wazuh.

Pada gambar di atas di perlihatkan kondisi / status agen yang sudah beroperasi di salah satu server yang sedang kita monitoring. Akan terlihat dengan jelas jika ada event yang berbahaya yang terjadi pada server yang kita monitor.



Gambar 6.4: Dashboard Event pada jaringan yang dimonitor.

Pada gambar diatas diperlihatkan tampilan dashboard event security yang terjadi di jaringan. Disini hanya dilakukan port scanning nmap pada server yang tertanam agent, sehingga tampilan tidak terlalu heboh.

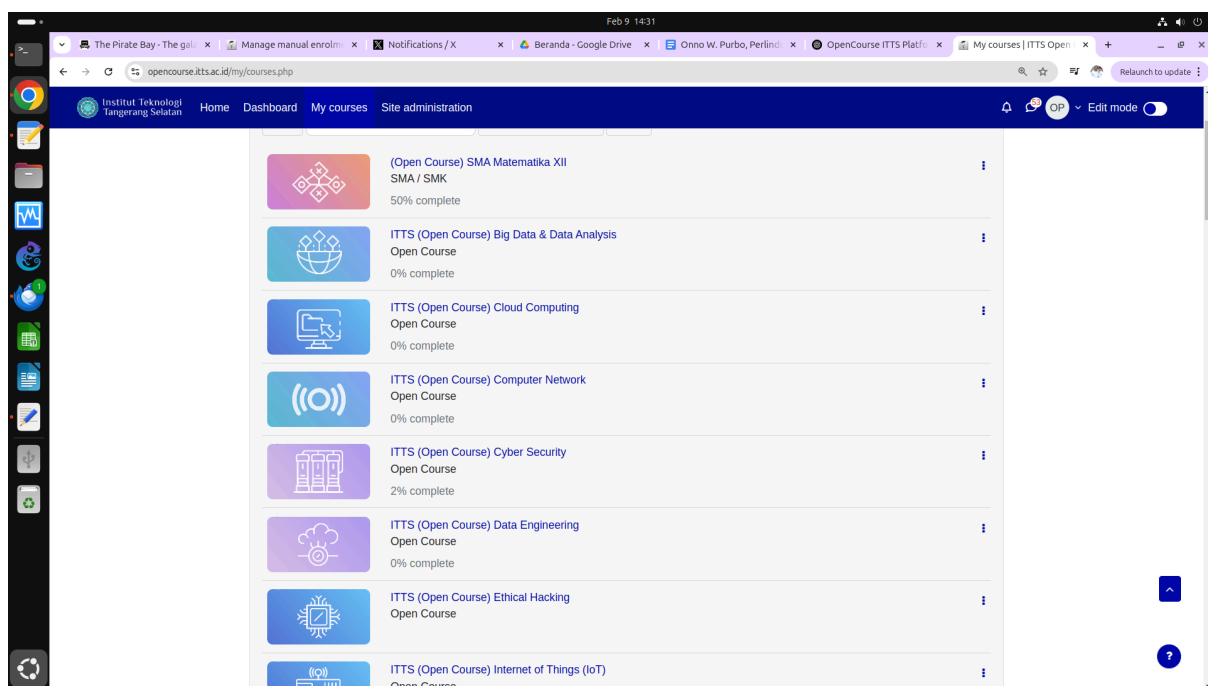


Gambar 6.5: Detail Security Event yang Terjadi.

Detail event juga dapat dilihat melalui dashboard seperti tampak pada gambar. Disini kita dapat melihat waktu (time), nama agent, level severity, ID. Ini akan dibutuhkan untuk mengejar attacker yang masuk.

BAB 7: Open Course

OpenCourse ITTS (opencourse.itts.ac.id) adalah platform e-learning gratis yang dikembangkan oleh Institut Teknologi Tangerang Selatan untuk menyediakan akses luas terhadap pendidikan berkualitas di bidang teknologi informasi. Sejak beroperasi lebih dari tiga tahun lalu, platform ini telah menarik lebih dari **30.000 mahasiswa** yang ingin memperdalam pemahaman mereka dalam berbagai disiplin ilmu teknologi. Dengan sistem pembelajaran berbasis daring, OpenCourse ITTS memungkinkan siapa saja, dari pelajar hingga profesional, untuk meningkatkan keahlian mereka tanpa biaya, menjadikannya salah satu sumber belajar terbuka khususnya bidang jaringan, cyber security yang terbaik di Indonesia.



Gambar 7.1. Tampilan Halaman Muka Open Course

Salah satu keunggulan OpenCourse ITTS adalah koleksi kursusnya yang berfokus pada teknologi open source, jaringan komputer, keamanan siber, forensik digital, dan **ethical hacking**. Semua materi perkuliahan inti di bidang ini dapat diakses secara bebas, memberikan peluang bagi siapa saja untuk memahami konsep fundamental hingga praktik lanjutan tanpa hambatan finansial. Dengan pendekatan berbasis komunitas dan kurikulum yang diperbarui secara berkala, platform ini terus berkembang sebagai pusat pembelajaran yang mendukung pengembangan keterampilan digital di era modern.

Pola belajar di **OpenCourse ITTS** dirancang untuk memberikan kebebasan penuh bagi mahasiswa dalam mengakses ilmu pengetahuan. Semua mata kuliah tersedia dengan **materi yang terstruktur**, memungkinkan mahasiswa untuk belajar secara mandiri sesuai dengan tempo dan kebutuhan mereka sendiri. Selain itu, seluruh rekaman kuliah dapat diakses melalui **YouTube**, sehingga mahasiswa dapat mengulang pembelajaran kapan saja

dan dari mana saja. Dengan sistem ini, siapa pun dapat meningkatkan pemahaman mereka tanpa batasan waktu dan tempat, menjadikannya solusi ideal bagi mereka yang ingin belajar dengan fleksibilitas tinggi.

Salah satu fitur menarik dari **OpenCourse ITTS** adalah sistem **quiz yang fleksibel**, di mana mahasiswa dapat mengerjakan soal berkali-kali **tanpa batasan waktu dan pengawasan**, dengan nilai tertinggi yang akan diambil. Kebebasan ini memungkinkan mahasiswa untuk terus mencoba dan memperbaiki pemahaman mereka. Namun, konsekuensinya, mereka bisa saja **mencari jawaban melalui Google, ChatGPT, atau copy-paste saat ujian**. Meskipun begitu, pendekatan ini lebih menekankan pada **eksplorasi dan pemecahan masalah**, mendorong mahasiswa untuk aktif mencari solusi dengan berbagai cara—sebuah keterampilan yang sangat relevan di dunia kerja.

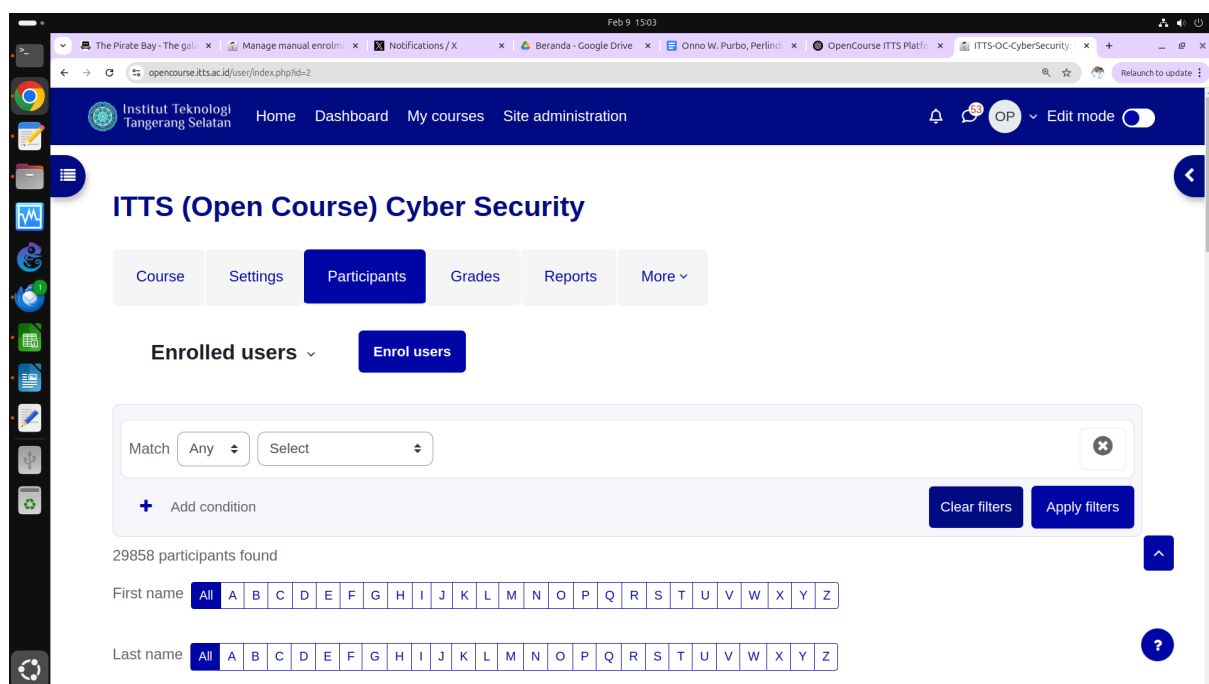
Lebih dari sekadar kursus online, **OpenCourse ITTS** juga memberikan akses luas ke **perpustakaan digital**. Mahasiswa bahkan dapat **mengirimkan harddisk 500GB** untuk meng-copy ribuan **file PDF** yang mencakup berbagai topik seperti **jaringan, sistem operasi, teknik hacking, cyber security, forensic, dan cryptography**—semuanya **gratis**. Dengan harga harddisk yang kini hanya sekitar **Rp. 65.000 – 75.000 di e-commerce**, mahasiswa bisa memperoleh banyak referensi berkualitas tanpa biaya besar. Ditambah lagi, interaksi dengan pengajar melalui **email, Twitter, dan media sosial** sepenuhnya **terbuka dan gratis**, menjadikan **OpenCourse ITTS** sebagai ekosistem pembelajaran yang inklusif dan mudah diakses oleh siapa saja.

Pengalaman dari **OpenCourse ITTS** menunjukkan bahwa meskipun semua **materi diberikan secara gratis** dan mahasiswa dapat mengulang **quiz/ujian tanpa batas** dengan sistem nilai tertinggi, hasil yang diperoleh tetap jauh dari optimal. Dari **30.000 mahasiswa** yang terdaftar, hanya segelintir yang berhasil mencapai nilai di atas 90 di berbagai mata kuliah. Hal ini menyoroti tantangan dalam kualitas **SDM Indonesia**, di mana akses ke materi dan fasilitas belajar yang luas ternyata **tidak serta-merta menghasilkan lulusan yang unggul**.

Tabel 7.1. Mahasiswa Bernilai Baik

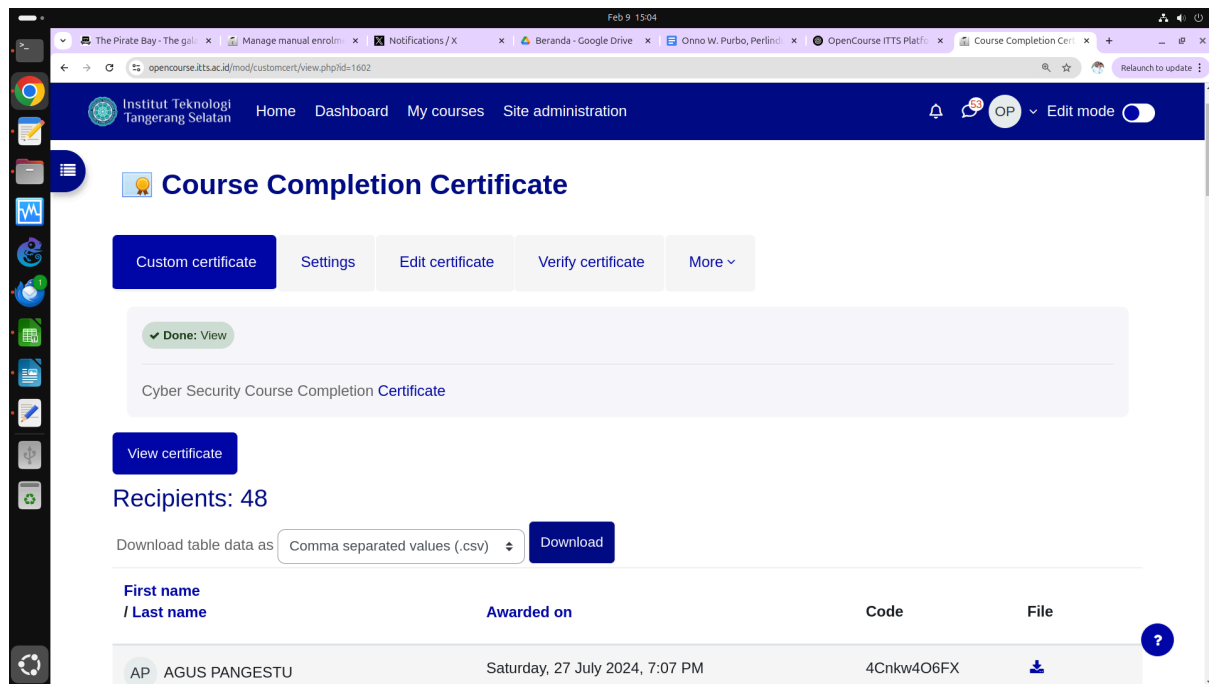
Mata Kuliah	Mahasiswa dengan Nilai >90
Jaringan Komputer	70
Cyber Security	54
IPv6	15
Microprocessor	24
Data Science	26
IoT	5
Ethical Hacking	5
Linux	52

Data yang tersedia menunjukkan bahwa hanya **70 orang** yang mampu meraih nilai tinggi di mata kuliah **Jaringan Komputer**, sementara bidang penting seperti **Cyber Security** hanya memiliki **54 orang**, **IPv6** hanya **15 orang**, dan **Ethical Hacking** hanya **5 orang**. Bahkan dalam topik fundamental seperti **Linux**, hanya **52 orang** yang berhasil mencapai nilai di atas 90. Ini menunjukkan bahwa **minat atau akses terhadap ilmu saja tidak cukup**, tetapi dibutuhkan juga **motivasi, kedisiplinan, dan kemauan untuk benar-benar memahami materi secara mendalam**.



Gambar 7.2 Tampilan Jumlah Mahasiswa Cyber Security di Open Course

Fenomena ini menggambarkan tantangan besar dalam pengembangan SDM berbasis teknologi di Indonesia. Banyak mahasiswa mungkin hanya mengejar sertifikat atau nilai, tetapi tidak berusaha memahami materi secara serius. Padahal, di dunia kerja, keahlian di bidang **jaringan, keamanan siber, data science, dan IoT** sangat dibutuhkan, dan penguasaan ilmu ini seharusnya menjadi prioritas utama. Oleh karena itu, meskipun **OpenCourse ITTS memberikan akses pendidikan tanpa hambatan biaya**, tantangan sebenarnya terletak pada **motivasi dan kesiapan individu untuk belajar secara mandiri dan mendalam**.



Gambar 7.3. Sedikitnya Mahasiswa yang Lulus Cyber Security.

Melihat kenyataan bahwa sangat sedikit mahasiswa yang dapat menyelesaikan **OpenCourse ITTS** dengan hasil yang baik, perlu ada langkah konkret untuk meningkatkan kualitas SDM di bidang teknologi. Salah satu solusi yang bisa dilakukan adalah **menyiapkan guru-guru SMP, SMA, dan SMK agar mampu menyampaikan materi dengan lebih baik**. Dengan bimbingan yang tepat sejak dini, siswa akan lebih siap menghadapi tantangan dalam bidang **jaringan, keamanan siber, forensic, dan data science**. Selain itu, penting untuk **memberikan gambaran yang jelas tentang persaingan dunia kerja**, agar mahasiswa dan siswa memahami bahwa hanya mereka yang benar-benar menguasai keterampilan teknis yang akan bertahan dan berkembang di industri.

Selain penguatan tenaga pengajar, langkah lain yang bisa dilakukan adalah **mendistribusikan materi dan kurikulum OpenCourse ITTS ke SMK dan kampus-kampus lain** agar lebih banyak institusi pendidikan yang dapat menyiapkan SDM dengan standar yang lebih baik. Namun, hal ini juga harus dibarengi dengan peningkatan **kompetensi dosen dan pengajar** di bidang **jaringan, keamanan siber, forensic, dan sistem operasi open-source**, agar mereka mampu membimbing mahasiswa dengan lebih efektif. Tidak kalah pentingnya, dukungan **peralatan komputer yang mumpuni** juga harus diperhatikan, tetapi pengadaannya **sebaiknya dilakukan secara kompetitif**, agar hanya institusi yang benar-benar serius dalam meningkatkan kualitas pendidikan yang mendapatkan akses ke sumber daya tersebut.

BAB 8: Kesimpulan

Vital Information Infrastructure (VII) dan **Critical Information Infrastructure (CII)** adalah dua komponen penting yang mendukung berbagai sektor esensial seperti energi, transportasi, kesehatan, keuangan, dan pemerintahan. Perbedaan utama antara keduanya terletak pada tingkat dampak dan skala pengaruhnya. **VII** mencakup sistem dan aset teknologi informasi yang esensial bagi operasional suatu organisasi atau sektor tertentu. Gangguan pada **VII** dapat menyebabkan kerugian operasional atau finansial bagi organisasi terkait, namun biasanya tidak berdampak pada skala nasional. Sebaliknya, **CII** meliputi infrastruktur yang sangat krusial bagi keberlangsungan ekonomi, keamanan nasional, dan kesejahteraan masyarakat secara luas. Karena dampaknya yang lebih luas dan kritis, **CII** biasanya dilindungi oleh regulasi keamanan nasional, sementara **VII** lebih bergantung pada kebijakan internal atau standar industri masing-masing sektor.

Indonesia saat ini menghadapi tantangan serius dalam hal keamanan siber, terutama terkait dengan **Critical Information Infrastructure**. Serangan siber yang menargetkan sektor-sektor vital seperti energi, keuangan, dan kesehatan telah meningkat secara signifikan. Misalnya, serangan ransomware baru-baru ini berhasil melumpuhkan Pusat Data Nasional Sementara (PDNS) di Surabaya, mengganggu layanan untuk hampir 300 instansi pemerintah pusat dan daerah, termasuk layanan imigrasi dan operasional bandara. Selain itu, Indonesia mengalami lonjakan serangan siber yang signifikan, dengan lebih dari 13,6 juta insiden siber tercatat hanya dalam bulan Juni 2024. Kerugian ekonomi akibat serangan siber mencapai proporsi yang sangat besar, dengan Indonesia mencatat kerugian finansial tertinggi di Asia.

Salah satu faktor yang memperburuk situasi ini adalah kurangnya sumber daya manusia (SDM) yang kompeten di bidang keamanan siber. Badan Siber dan Sandi Negara (BSSN) mengungkapkan bahwa Indonesia membutuhkan sekitar 8.000 SDM dengan kualifikasi keamanan siber, namun saat ini hanya mampu mencetak sekitar **100 lulusan per tahun**. Kekurangan ini menyebabkan banyak instansi pemerintah dan perusahaan swasta rentan terhadap serangan siber karena kurangnya tenaga ahli yang mampu mengidentifikasi dan menangani ancaman tersebut.

Untuk mengatasi tantangan ini, diperlukan upaya kolaboratif antara pemerintah, sektor swasta, dan institusi pendidikan. Peningkatan investasi dalam pendidikan dan pelatihan keamanan siber menjadi krusial untuk membangun SDM yang kompeten. Selain itu, implementasi kebijakan keamanan siber yang komprehensif dan peningkatan kesadaran akan pentingnya perlindungan data di kalangan masyarakat juga menjadi langkah penting dalam memperkuat ketahanan siber Indonesia.

Siklus **Plan-Do-Check-Act (PDCA)** adalah kerangka kerja iteratif yang digunakan untuk perbaikan berkelanjutan dalam berbagai proses, termasuk perencanaan dan implementasi **Critical Information Infrastructure (CII)** dan **Vital Information Infrastructure (VII)**. Dengan menerapkan **PDCA**, organisasi dapat memastikan bahwa infrastruktur informasi mereka tetap aman, andal, dan sesuai dengan kebutuhan yang terus berkembang. Tahap pertama, **Plan (Perencanaan)**, melibatkan identifikasi dan analisis aset kritis serta potensi ancaman yang mungkin dihadapi. Setelah perencanaan, tahap **Do (Pelaksanaan)** dilakukan dengan mengimplementasikan rencana yang telah disusun, fokus pada penguatan

keamanan infrastruktur. Tahap berikutnya, **Check (Pemeriksaan)**, melibatkan pemantauan dan penilaian efektivitas langkah-langkah yang telah diambil. Terakhir, tahap **Act (Tindakan)** melibatkan pengambilan tindakan korektif atau preventif berdasarkan hasil evaluasi untuk meningkatkan sistem.

Dengan menerapkan siklus **PDCA** secara konsisten, organisasi dapat memastikan bahwa **CII** dan **VII** mereka tetap aman, efisien, dan mampu beradaptasi dengan ancaman serta perubahan yang terjadi. Pendekatan ini mendukung perbaikan berkelanjutan dan memastikan bahwa langkah-langkah keamanan selalu relevan dan efektif.

Perlindungan **Vital Information Infrastructure (VII)** di Indonesia memerlukan pendekatan strategis yang komprehensif untuk menghadapi berbagai ancaman siber. Salah satu langkah penting adalah penerapan cyber hygiene, seperti pembaruan perangkat lunak secara berkala untuk menutup celah keamanan, penggunaan **otentikasi multi-faktor (MFA)** guna menambah lapisan keamanan pada proses login, dan pemantauan jaringan secara real-time untuk mendeteksi aktivitas mencurigakan dengan cepat. Selain itu, implementasi **arsitektur Zero Trust** memastikan setiap permintaan akses diverifikasi tanpa memandang asalnya, baik dari dalam maupun luar jaringan organisasi.

Penggunaan sistem deteksi dan respons juga krusial dalam strategi perlindungan. Penerapan **Intrusion Detection System (IDS)** dan **Intrusion Prevention System (IPS)** membantu mendeteksi serta mencegah aktivitas berbahaya di jaringan. Pemanfaatan teknologi **kecerdasan buatan (AI)** dan **pembelajaran mesin (machine learning)** dapat mengidentifikasi pola anomali dalam lalu lintas jaringan, memungkinkan deteksi ancaman lebih dini. Selain itu, melakukan backup data secara rutin dan menyimpan salinan di lokasi terpisah, termasuk backup offline, penting untuk melindungi data dari serangan seperti ransomware. Latihan simulasi insiden siber secara berkala memastikan tim siap merespons dan memulihkan sistem dengan efisien.

Kolaborasi internasional juga menjadi elemen kunci dalam memperkuat pertahanan VII. Kerja sama dengan negara lain memungkinkan berbagi informasi mengenai ancaman terbaru dan praktik terbaik dalam keamanan siber. Partisipasi dalam forum keamanan siber global, seperti **FIRST**, **Europol EC3**, dan **ASEAN Cybersecurity Forum**, membantu Indonesia tetap terinformasi dan terlibat dalam diskusi keamanan siber internasional.

Dari sisi kebijakan dan regulasi, adopsi standar keamanan internasional seperti **ISO 27001** dan **NIST Cybersecurity Framework** memastikan praktik keamanan yang konsisten. Regulasi yang mewajibkan adopsi standar keamanan yang baik.

Referensi

Sulit untuk menjelaskan dengan detail berbagai hal teknis terkait pengamanan infrastruktur informasi dalam tulisan terbatas ini. Sangat disarankan untuk membaca lebih detail tentang teknik penanganan dan keamanan Internet dari buku berikut:

- Onno W. Purbo, Jimmy Alberto, Hafizhan Irawan, Bagus Gede Arta Perdana, Aolia Ikhwanudin, Muhamad Yusuf, Agianto Syamhalim, Tubagus Toifur, Ibnu Mas'ud, Dimaz Arno Prasetio, Tubagus Asep Nurdin. Buku Pegangan Penanganan Insiden Siber. Yogyakarta: Andi Publisher; 2023.
- Hartono, Onno W. Purbo. Membangun dan Menguji Keamanan Website. Yogyakarta: Andi Publisher; 2022.

Juga sangat disarankan untuk enroll dan membaca kuliah online FREE di

opencourse.itts.ac.id

Tentang Penulis

Onno W. Purbo, saat ini bertugas sebagai Rektor di Institut Teknologi Tangerang Selatan (ITTS). Onno memperoleh gelar Ph.D bidang Electrical Engineering dari University of Waterloo, Canada, adalah seorang copyleft, educator dan ICT evangelist. Dia sudah mempublikasikan 60+ buku, termasuk free ICT ebook untuk sekolah tahun 2008. Beberapa buku terakhirnya adalah "Internet-TCP/IP: Konsep Dan Implementasi", 2018; "Sistem Operasi, Konsep Dan Membuat Linux OpenWRT Dan ROM Android", 2019; "IPv6 Untuk Mendukung Operasi Jaringan Dan Domain Name System", 2019; "Kubernetes untuk Pemula", 2024 dan "Membuat Operator Seluler 5G Sendiri", 2024. Dia memimpin sambungan pertama Internet di Institut Teknologi Bandung, tahun 1993-2000, dan menggunakannya untuk membuat jaringan Internet pendidikan yang pertama di Indonesia. Dia membebaskan frekuensi WiFi, memperkenalkan RT/RW-net, antenna Wajanbolic dan jaringan selular OpenBTS. Dia memimpin jaringan telepon pertama di atas Internet, VoIP Merdeka, yang kemudian hari dikenal sebagai VoIP Rakyat berbasis SIP dan menggunakan kode area +62520 dan +62521. Dia saat ini aktif memperkenalkan e-Learning, dan menjalankan server e-Learning di <http://lms.onnocenter.or.id/moodle/> 65,000++ siswa / mahasiswa dan <https://opencourse.itts.ac.id> 30.000+ mahasiswa secara gratis.