KEBIJAKAN DALAM PENGUJIAN KEAMANAN DAN TATA KELOLA JARINGAN

NAMA: AMANDA
NIM: 2344390004
JURUSAN: SISTEM INFORMASI (S1)
KODE/NAMA MK: 246/KEAMANAN INFORMASI

PROGRAM STUDI SISTEM INFORMASI DAN FAKULTAS TEKNIK
UNIVERSITAS PERSADA INDONESIA
2025

DAFTAR ISI

DAFTAR GAMBAR

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa, karena atas rahmat dan karunia-Nya, makalah ini dapat diselesaikan dengan baik. Makalah ini disusun sebagai salah satu tugas mata kuliah terkait keamanan informasi dan teknologi jaringan.

Penulis menyadari bahwa keamanan informasi dan jaringan merupakan aspek penting dalam pengelolaan sistem teknologi saat ini. Oleh sebab itu, makalah ini berfokus pada kebijakan keamanan dan tata kelola, konsep model jaringan dan proteksi, serta pengujian keamanan sistem secara etis.

Penulis menyadari bahwa makalah ini masih jauh dari sempurna. Kritik dan saran yang membangun sangat diharapkan untuk perbaikan di masa yang akan datang. Ucapan terima kasih juga disampaikan kepada dosen pembimbing, teman-teman dan semua pihak yang telah memberikan dukungan dan bantuan selama proses penyusunan makalah ini.

Akhir kata, penulis berharap makalah ini bermanfaat bagi pembaca dalam menambah pemahaman mengenai keamanan informasi, tata kelola, serta praktik pengujian keamanan yang aman dan etis.

Jakarta, 1 Oktober 2025

Amanda

Kebijakan Keamanan & Tata Kelola

Minggu 3 Kebijakan keamanan & tata kelola: ISMS, peran, tanggung jawab; pengantar ISO/IEC 27001. (ISO)

A. Konsep Dasar Keamanan Informasi

Keamanan informasi adalah sebuah disiplin penting dalam manajemen teknologi dan organisasi yang bertujuan utama untuk menjaga kerahasiaan, integritas dan ketersediaan informasi, baik dalam bentuk data, sistem, infrastruktur, maupun proses bisnis, dari ancaman yang dapat menimbulkan risiko bagi keberlangsungan operasional. Fokus utamanya adalah melindungi informasi dari akses tidak sah, penggunaan tanpa izin, pengungkapan data yang tidak semestinya, perubahan atau manipulasi yang berbahaya, serta gangguan hingga perusakan baik yang disengaja maupun tidak disengaja.

Gambar 1. 1 Konsep Dasar Keamanan Informasi

Sumber : https://www.agus-hermanto.com/blog/detail/definisi-keamanan-informasi-3-aspek-di-dalamnya

Aspek perlindungan dalam keamanan informasi mencakup pencegahan terhadap berbagai ancaman yang berpotensi muncul, baik dari internal maupun

eksternal. Ancaman tersebut bisa berupa akses tidak sah, penggunaan informasi tanpa izin, pengungkapan data secara ilegal, hingga manipulasi yang dapat merusak keaslian informasi. Untuk mengantisipasi hal ini, organisasi membutuhkan kebijakan, prosedur, serta penerapan teknologi yang tepat agar keamanan data tetap terjamin.

Keamanan informasi juga berkaitan dengan upaya menjaga kelancaran operasional dari berbagai gangguan. Gangguan dapat terjadi dalam bentuk serangan siber, kerusakan perangkat keras, kesalahan manusia, maupun bencana yang menimbulkan dampak signifikan. Strategi pengamanan biasanya mencakup kontrol akses, enkripsi, sistem cadangan, serta audit berkala guna memastikan kesiapan menghadapi berbagai situasi darurat. Dengan langkah tersebut, organisasi tetap mampu mempertahankan fungsionalitas meskipun menghadapi insiden keamanan. (Nieles, 2017)

Selain aspek teknis, keamanan informasi menekankan pentingnya keterlibatan manajemen dan kesadaran seluruh anggota organisasi. Budaya keamanan perlu ditanamkan melalui edukasi, pelatihan dan kepatuhan terhadap kebijakan yang berlaku. Integrasi antara teknologi, tata kelola dan perilaku manusia akan membentuk fondasi yang kuat bagi keberlanjutan bisnis, menjaga kepercayaan pemangku kepentingan, sekaligus meningkatkan daya saing organisasi di era digital.(Alraja et al., 2023b)

Menurut standar *National Institute of Standards and Technology* (NIST), keamanan informasi mencakup perlindungan menyeluruh terhadap "unauthorized access, use, disclosure, alteration, disruption, or destruction" yang dapat memengaruhi informasi maupun sistem pendukungnya, sehingga aspek ini tidak hanya berkaitan dengan teknologi, tetapi juga menyangkut kebijakan, prosedur dan kontrol yang terintegrasi demi menciptakan sistem informasi yang andal(Nieles, 2017)

Dalam praktik keamanan informasi modern, tidak cukup hanya memperkuat aspek teknis seperti enkripsi atau firewall; aspek manusia dan struktur organisasi juga harus menjadi perhatian utama, karena faktor manusia adalah salah satu vektor risiko terbesar dalam sistem keamanan (Di Nocera et al., 2023). Sebuah

objek abaik berupa data, sistem, atau proses dapat dikatakan aman bagi pemangku kepentingan (*stakeholder*) apabila setiap agen (aktor manusia ataupun sistem) diberikan akses yang sesuai terhadap bagian sistem terkait tidak terlalu sedikit yang menghambat fungsionalitas dan tidak terlalu banyak sehingga menimbulkan risiko penyalahgunaan atau eskalasi hak akses (James, 2021). Kontrol akses yang efektif tidak hanya mengatur apa yang boleh dilakukan oleh agen, tetapi juga menjamin bahwa hak akses tersebut proporsional dan sesuai dengan peran dan tanggung jawab mereka dalam organisasi.

B. Ancaman & Risiko Keamanan Informasi

Keamanan informasi adalah suatu kerangka kegiatan, kebijakan dan kontrol yang dirancang untuk melindungi aset informasi organisasi agar tetap rahasia, utuh dan tersedia (CIA) serta tidak disalahgunakan, diubah tanpa izin, atau hilang karena gangguan. Dalam pengertian modern, keamanan informasi mencakup tidak hanya aspek teknis (seperti firewall, enkripsi, kontrol akses), tetapi juga aspek manusia dan organisasi (kebijakan, pelatihan, budaya keamanan).(Alraja et al., 2023a)

Dalam sebuah organisasi menetapkan kontrol akses hanya bagi staf tertentu berdasarkan peran mereka, serta melaksanakan audit berkala untuk memeriksa apakah akses yang ada masih sesuai kebutuhan.(AL-Dosari & Fetais, 2023)

Gambar 1. 2 Ancaman & Risiko Keamanan Informasi

Sumber : https://www.batumenyan.desa.id/memahami-risiko-keamanan-digital-panduan-literasi-untuk-semua/

Keamanan informasi juga berkaitan dengan identifikasi dan pengelolaan risiko yang dihadapi oleh organisasi yaitu kemungkinan ancaman terhadap aset informasi yang memanfaatkan kerentanan. Saat sebuah organisasi menjalankan sistem manajemen keamanan informasi (ISMS), mereka melakukan penilaian risiko, menetapkan kontrol mitigasi dan memantau efektivitasnya. Keberhasilan keamanan informasi tergantung pada keseimbangan antara keamanan dan operasional: kontrol tidak boleh terlalu ketat sehingga menghambat kerja, tapi cukup kuat untuk mengurangi risiko. Contoh-contoh penerapan keamanan informasi

a) Penggunaan autentikasi multi-faktor (MFA) untuk akses sistem kritikal
b) Penerapan kebijakan password: panjang minimal, kompleksitas, masa berlaku
c) Enkripsi data sensitif (data di dalam database, data dalam perjalanan)
d) Pemisahan hak akses (role-based access control)
e) Audit dan pencatatan log (logging) aktivitas pengguna
f) Pelatihan kesadaran keamanan (security awareness) bagi semua pegawai
g) Backup dan pemulihan bencana (disaster recovery)
h) Pengelolaan patch dan pembaruan sistem
i) Pengamanan fisik (ruang server terkunci, akses terbatas)
j) Pengujian kerentanan dan penilaian penetrasi (vulnerability assessment / penetration testing)

C. Prinsip Tata Kelola Keamanan Informasi

Berikut beberapa prinsip utama dalam tata kelola keamanan informasi:(Magnusson et al., 2025)

1. Akuntabilitas (*Accountability*) menetapkan siapa bertanggung jawab atas kebijakan, pengawasan dan keputusan keamanan
2. Transparansi (*Transparency*) proses dan kebijakan keamanan dapat dipahami dan diaudit
3. Kepatuhan (*Compliance*) mematuhi regulasi, standar dan peraturan yang relevan
4. Keterpaduan strategis (*Strategic Alignment*) keamanan informasi harus selaras dengan visi & strategi organisasi
5. Pengelolaan risiko (*Risk Management*) identifikasi, evaluasi, mitigasi risiko keamanan
6. Alokasi sumber daya (*Resource Allocation*) menyediakan anggaran, SDM, teknologi yang memadai
7. Monitoring & pengukuran (*Monitoring & Metrics*) memantau efektivitas kontrol keamanan lewat indikator (KPI)
8. Perbaikan berkelanjutan (*Continuous Improvement*) mengevaluasi dan memperbarui kebijakan & kontrol berdasarkan hasil audit & perubahan ancaman(Mishra, 2023)
9. Kepemimpinan & komitmen manajemen puncak (*Leadership & Top Management Commitment*) dukungan manajemen sangat penting
10. Integrasi GRC (*Governance, Risk, Compliance*) mengaitkan aspek keamanan informasi dengan manajemen risiko dan kepatuhan.

D. Kerangka Sistem Manajemen Keamanan Informasi (ISMS)

Kerangka Sistem Manajemen Keamanan Informasi (ISMS) adalah struktur formal yang digunakan organisasi untuk mengelola risiko keamanan informasi melalui proses yang sistematis: mulai dari identifikasi aset, penilaian risiko, perlakuan risiko, hingga monitoring dan perbaikan berkelanjutan (Fajri & Harwahyu, 2024). ISMS menyertakan kebijakan, prosedur, kontrol dan peran & tanggung jawab yang jelas untuk menjamin bahwa informasi organisasi tetap

rahasia, utuh dan tersedia sesuai kebutuhan bisnis dan peraturan yang berlaku. ISMS juga harus disesuaikan dengan konteks organisasi: pemahaman tentang internal (struktur organisasi, budaya, teknologi) dan eksternal (regulasi, ancaman) sangat penting.

Salah satu elemen penting dalam kerangka ISMS adalah siklus *Plan-Do-Check-Act* (PDCA), yaitu perencanaan *(Plan*) pengelolaan keamanan informasi, pelaksanaan (Do) kontrol & prosedur, pemeriksaan (*Check*) efektivitas dan kepatuhan, lalu tindakan (Act) untuk perbaikan. Kerangka ini memastikan ISMS tidak statis tetapi berevolusi mengikuti perubahan risiko, teknologi dan kebutuhan organisasi. Selain PDCA, standar seperti ISO/IEC 27001 mengatur klausul-klausul yang menjadi bagian inti dari ISMS (contoh: konteks organisasi, kepemimpinan, dukungan, operasi, evaluasi kinerja, perbaikan) yang diikuti annex kontrol untuk mitigasi risiko.(Jevelin & Faza, 2023)

Komponen teknis dan non-teknis harus berjalan bersama di dalam ISMS. Komponen teknis meliputi penggunaan kontrol administratif, teknis dan fisik: kontrol akses, enkripsi, manajemen patch, keamanan fisik, keamanan operasional, dll. Sedangkan komponen non-teknis meliputi kebijakan keamanan, pelatihan dan kesadaran pegawai, struktur organisasi, dokumentasi, audit internal dan manajemen insiden. Keberhasilan ISMS tergantung integrasi semua elemen ini serta koordinasi antar bagian: TI, manajemen, sumber daya manusia, compliance, dsb.

Implementasi ISMS juga memerlukan mekanisme evaluasi dan pengukuran: organisasi harus menetapkan metrik keamanan, mengaudit internal secara berkala, melakukan review manajemen dan memperbarui kebijakan dan kontrol berdasarkan feedback serta hasil audit. Di samping itu, harus ada Statement of Applicability (SoA) yang mendokumentasikan kontrol-kontrol yang dipilih dan alasannya, serta ruang lingkup ISMS yang jelas. Tanpa pengukuran dan dokumentasi, sulit untuk membuktikan bahwa ISMS bekerja atau bahwa organisasi memenuhi standar seperti ISO/IEC 27001.

Berikut kerangka komponen utama ISMS secara sistematis:

1. Konteks Organisasi (Organizational Context)
2. Kepemimpinan & Komitmen Manajemen Puncak
3. Kebijakan Keamanan Informasi
4. Penilaian Risiko (Risk Assessment)
5. Penanganan Risiko (Risk Treatment)
6. Kontrol Keamanan (Technical, Fisik, Administratif)
7. Sumber Daya & Kompetensi (Resources & Competence)
8. Dokumentasi & Komunikasi
9. Operasional (implementasi kontrol, prosedur operasional)
10. Pemantauan & Pengukuran (Monitoring & Metrics)
11. Audit Internal & Review Manajemen
12. Perbaikan & Tindakan Korektif / Preventif

E. Siklus PDCA dalam ISMS

Siklus PDCA (*Plan-Do-Check-Act*) merupakan fondasi metodologis dalam penerapan sistem manajemen, termasuk ISMS (*Information Security Management System*). ISMS, fase Plan meliputi penetapan kebijakan keamanan, identifikasi konteks organisasi, identifikasi aset informasi, penilaian risiko dan perencanaan kontrol dan tindakan mitigasi yang sesuai untuk mengelola risiko keamanan. Fase ini memastikan bahwa organisasi memahami apa yang harus dilindungi dan bagaimana cara merancang kerangka kontrol.(Sevgi, 2021)

Fase Do adalah pelaksanaan atau implementasi kontrol, prosedur dan kebijakan yang telah direncanakan misalnya penerapan kontrol akses, enkripsi, monitoring sistem, pelatihan pegawai, serta operasional rutin sistem keamanan. Kemudian, fase Check meliputi pengukuran, audit internal, peninjauan kontrol untuk mengevaluasi sejauh mana efektivitas kontrol dan kepatuhan terhadap kebijakan dan tujuan keamanan. Fase Act adalah tindakan korektif dan pencegahan berdasarkan hasil evaluasi dan audit, serta revisi kebijakan / kontrol

agar ISMS terus berkembang dan menyesuaikan dengan perubahan risiko atau lingkungan. PDCA menjamin bahwa ISMS bersifat dinamis, adaptif dan berorientasi pembaruan berkelanjutan (*continuous improvement*).(Górka–Chowaniec & Popek, 2025)

Berikut adalah fase-fase PDCA dan aktivitas utama di tiap fase dalam ISMS:

1. Plan
    a) Menetapkan cakupan ISMS
    b) Menyusun kebijakan keamanan informasi
    c) Identifikasi aset & konteks organisasi
    d) Penilaian risiko (risk assessment)
    e) Merencanakan kontrol & tindakan mitigasi
    f) Menetapkan tujuan keamanan & indikator (KPI)
2. Do
    a) Mengimplementasikan kontrol (teknis, administratif, fisik)
    b) Menjalankan prosedur operasional keamanan
    c) Pelatihan & kesadaran keamanan (security awareness)
    d) Pengelolaan insiden keamanan
    e) Backup & pemeliharaan
3. Check
    a) Audit internal keamanan
    b) Pemantauan & pengukuran metrik keamanan
    c) Evaluasi kepatuhan terhadap kebijakan & standar
    d) Pelaporan hasil ke manajemen
4. Act

a) Menetapkan tindakan korektif & preventif

b) Meninjau dan memperbarui kebijakan dan kontrol

c) Review manajemen

d) Meningkatkan proses keamanan dan adaptasi terhadap perubahan

F. Peran Manajemen dalam ISMS

Manajemen puncak memiliki peran kunci dalam keberhasilan implementasi ISMS karena mereka yang menetapkan arah strategis, mendukung budaya keamanan dan menyediakan sumber daya yang dibutuhkan. Pertama, manajemen mesti menetapkan kebijakan keamanan informasi yang jelas dan selaras dengan tujuan bisnis dan visi organisasi. Mereka juga harus menjamin bahwa tujuan keamanan (*security objectives*) ditetapkan, dipahami oleh seluruh tingkat organisasi dan diukur efektivitasnya. Tanpa komitmen dari atas, kebijakan dan kontrol yang dibuat seringkali tidak akan diikuti atau diabaikan karena anggaran, prioritas, atau konflik dengan kebutuhan operasional.(Fajri & Harwahyu, 2024)

Peran manajemen dalam Information Security Management System (ISMS) adalah tanggung jawab strategis untuk memastikan bahwa keamanan informasi menjadi bagian integral dari tata kelola organisasi. Manajemen memiliki kewenangan untuk menetapkan arah, tujuan, serta kebijakan yang berkaitan dengan perlindungan aset informasi. Manajemen berfungsi sebagai pengambil keputusan utama yang menentukan prioritas keamanan dan memastikan alokasi sumber daya yang memadai dalam penerapan ISMS. peran manajemen dalam ISMS mencakup keterlibatan aktif dalam menetapkan visi serta strategi keamanan informasi yang selaras dengan tujuan bisnis organisasi.

Manajemen juga berperan dalam memberikan arahan kebijakan, menyetujui prosedur operasional, serta memastikan seluruh unit kerja memahami dan menjalankan standar keamanan yang telah ditentukan. Tanpa komitmen dari tingkat manajerial, ISMS tidak akan dapat berjalan efektif karena kurangnya legitimasi dan dukungan struktural.

Manajemen bertanggung jawab untuk melakukan evaluasi dan perbaikan berkelanjutan terhadap penerapan ISMS. Hal ini dilakukan melalui proses audit, tinjauan manajemen, serta pengelolaan risiko secara berkala untuk menyesuaikan dengan perkembangan ancaman maupun perubahan regulasi. Dengan keterlibatan tersebut, manajemen tidak hanya memastikan kepatuhan terhadap standar internasional, tetapi juga membangun budaya keamanan informasi yang berkesinambungan di seluruh lapisan organisasi.

Manajemen bertanggung jawab dalam menyediakan dukungan nyata bukan hanya formalitas. Dukungan nyata bisa berupa alokasi anggaran, sumber daya manusia, pelatihan, infrastruktur teknologi, pengawasan secara langsung dan peninjauan berkala terhadap performa ISMS. Manajemen juga harus mengambil peran aktif dalam "leadership & commitment" seperti yang dituntut dalam klausa 5.1 ISO/IEC 27001: memastikan bahwa sistem keamanan informasi terintegrasi dalam proses organisasi dan bahwa ada komunikasi yang efektif mengenai pentingnya keamanan informasi(Jevelin & Faza, 2023). Mereka harus meminta laporan performa ISMS, menindaklanjuti temuan audit dan mendorong perbaikan berkelanjutan agar ISMS tidak menjadi dokumen mati.

G. Tanggung Jawab Individu & Tim Keamanan

Keamanan informasi dalam organisasi bukan hanya menjadi tanggung jawab manajemen, tetapi juga setiap individu yang terlibat dalam proses bisnis. Individu memiliki peran penting dalam menjaga kerahasiaan, integritas dan ketersediaan informasi. Kesadaran terhadap ancaman siber, kepatuhan pada kebijakan organisasi, serta disiplin dalam penggunaan perangkat digital merupakan aspek mendasar yang harus dimiliki setiap karyawan. Tanpa keterlibatan individu, penerapan ISMS akan sulit mencapai efektivitas yang maksimal.(Melaku, 2023)

Selain individu, tim keamanan memiliki tanggung jawab yang lebih luas dalam mengkoordinasikan upaya perlindungan data. Mereka bertugas memastikan penerapan kebijakan keamanan, melakukan evaluasi risiko, serta memberikan pelatihan dan bimbingan kepada seluruh anggota organisasi. Tim ini juga berfungsi sebagai penghubung antara manajemen dan staf operasional

dalam menjaga sistem tetap berjalan aman(Savaş & Karataş, 2022). Tanggung jawab tim keamanan dapat dirinci dalam bentuk berikut:

1. Melaksanakan monitoring dan audit keamanan secara berkala.
2. Mengidentifikasi serta menanggapi insiden keamanan informasi.
3. Mengembangkan dan memperbarui kebijakan serta prosedur keamanan.
4. Memberikan pelatihan keamanan bagi seluruh karyawan.
5. Menyediakan laporan dan rekomendasi kepada manajemen terkait risiko keamanan.

Perpaduan antara tanggung jawab individu dan koordinasi tim menjadi fondasi keberhasilan dalam menjaga keamanan informasi. Kolaborasi yang kuat memungkinkan organisasi memiliki sistem pertahanan berlapis yang mampu mengantisipasi ancaman, sekaligus meningkatkan budaya kesadaran keamanan. ISMS dapat berjalan selaras dengan tujuan organisasi dan memberikan perlindungan yang berkesinambungan.

H. Kebijakan Keamanan Informasi Organisasi

Kebijakan keamanan informasi organisasi adalah dokumen formal yang menetapkan tujuan, prinsip dan aturan yang mengarahkan bagaimana organisasi menjaga kerahasiaan, integritas dan ketersediaan aset informasi. Kebijakan ini menjembatani strategi bisnis dengan tindakan operasional keamanan, memastikan bahwa setiap aktivitas TI dan non-TI berada dalam kerangka yang konsisten dan aman. Kebijakan memuat ruang lingkup (scope), tanggung jawab, persyaratan kepatuhan, serta mekanisme pelaporan dan pengendalian.(Nagata, 2024)

Kebijakan keamanan informasi berperan penting dalam menghubungkan strategi bisnis dengan tindakan operasional keamanan sehari-hari. Hal ini mencakup penentuan prosedur yang harus diikuti oleh seluruh unit kerja, mulai dari tata cara penggunaan sistem informasi, perlindungan data pelanggan, hingga mekanisme pencegahan ancaman digital. Keberadaan kebijakan yang terintegrasi membantu memastikan bahwa semua aktivitas yang berkaitan

dengan informasi organisasi tetap berjalan secara konsisten, terkendali dan terlindungi dari potensi risiko. .(Nagata, 2024)

Dokumen kebijakan juga berisi rincian ruang lingkup yang menjelaskan area mana saja yang harus dijaga, serta menetapkan tanggung jawab masing-masing pihak dalam pelaksanaan keamanan. Di dalamnya termasuk ketentuan mengenai kepatuhan terhadap regulasi, standar industri, maupun aturan internal organisasi. Selain itu, terdapat pula mekanisme pengawasan dan pelaporan yang dirancang agar setiap pelanggaran atau insiden keamanan dapat segera teridentifikasi dan ditindaklanjuti secara cepat.

Evaluasi dan pembaruan kebijakan menjadi faktor yang tidak bisa diabaikan, sebab ancaman keamanan informasi terus berkembang seiring kemajuan teknologi. Organisasi yang mampu menyesuaikan kebijakan dengan kondisi terbaru akan lebih siap dalam menghadapi tantangan serta mempertahankan kepercayaan stakeholder. Kebijakan keamanan informasi bukan hanya dokumen statis, melainkan sebuah kerangka dinamis yang mendukung keberlangsungan dan ketahanan organisasi di era digital.

Kebijakan keamanan juga harus bersifat adaptif terhadap perubahan lingkungan ancaman dan evolusi teknologi. Organisasi perlu melakukan review berkala dan pembaruan kebijakan ketika terjadi perubahan risiko, regulasi, atau struktur organisasi(Alraja et al., 2023b). Dengan kebijakan yang diperbarui secara kontinu, organisasi mampu merespon ancaman baru, memperbaiki kelemahan dan menjaga relevansi kontrol keamanan dalam jangka panjang.

I. Pengenalan ISO/IEC 27001

Kebijakan keamanan informasi organisasi adalah seperangkat aturan, pedoman dan prosedur formal yang ditetapkan untuk melindungi kerahasiaan, integritas, serta ketersediaan informasi. Kebijakan ini menjadi kerangka acuan utama bagi seluruh aktivitas yang berkaitan dengan pengelolaan data dan sistem informasi, sehingga setiap anggota organisasi memiliki pemahaman yang sama mengenai cara melindungi aset informasi dari ancaman internal maupun eksternal.(Nagata, 2024)

Kebijakan keamanan informasi juga berperan dalam mengatur mekanisme kontrol akses, manajemen risiko, serta strategi respons insiden ketika terjadi pelanggaran keamanan. Hal ini mencakup bagaimana organisasi mendefinisikan hak dan kewajiban pengguna, prosedur otorisasi, serta metode pemantauan terhadap aktivitas sistem. Dengan adanya kebijakan yang jelas, organisasi mampu meminimalkan risiko kebocoran data, serangan siber, maupun penyalahgunaan informasi oleh pihak yang tidak berwenang.

Gambar 1. 3 Pengenalan ISO/IEC 27001

Sumber : https://izinusaha.id/iso-iec-27001-indonesia-manfaat-dan-penerapannya/

Keberhasilan implementasi kebijakan keamanan informasi sangat bergantung pada dukungan manajemen puncak serta kepatuhan seluruh anggota organisasi. Kebijakan ini perlu dievaluasi secara berkala untuk menyesuaikan dengan dinamika ancaman baru, perkembangan teknologi, serta kebutuhan bisnis yang terus berubah. Dengan pendekatan yang adaptif dan komprehensif, kebijakan keamanan informasi dapat menjadi fondasi kuat dalam memastikan kelangsungan operasional organisasi sekaligus menjaga kepercayaan dari mitra bisnis maupun pelanggan.

Kebikan keamanan informasi organisasi adalah instrumen strategis yang memastikan keselarasan antara tujuan bisnis dengan praktik keamanan yang diterapkan(PROTHRO, 2022). Dengan adanya kebijakan yang jelas dan terdokumentasi, organisasi dapat meningkatkan kepatuhan terhadap standar,

mengurangi risiko kebocoran data, serta membangun budaya keamanan yang berkesinambungan di antara seluruh karyawan.

J. Manfaat & Tantangan Implementasi ISO/IEC 27001

Implementasi ISO/IEC 27001 memberikan manfaat strategis dan operasional yang signifikan bagi organisasi. Standar ini membantu memperjelas kebijakan dan prosedur keamanan informasi, menguatkan kepercayaan pelanggan, mitra bisnis dan pemangku kepentingan melalui bukti kepatuhan terhadap standar internasional.

Penggunaan ISMS yang sesuai ISO/IEC 27001 juga memungkinkan organisasi melakukan identifikasi dan mitigasi risiko secara sistematis, mengurangi kemungkinan insiden keamanan seperti kebocoran data atau serangan siber. Penerapan kontrol-terkontrol yang relevan juga meningkatkan efisiensi operasional karena proses keamanan lebih terstruktur dan terdokumentasi.(Intan Mafiana et al., 2023)

A. Manfaat

1. Perlindungan aset informasi dari kebocoran, penyalahgunaan dan ancaman siber.
2. Kepatuhan regulasi serta standar industri terkait keamanan data.
3. Meningkatkan kepercayaan stakeholder melalui sertifikasi resmi.
4. Efisiensi operasional dengan prosedur yang terdokumentasi dan terstandar.
5. Pengelolaan risiko sistematis melalui identifikasi dan kontrol risiko.
6. Keunggulan kompetitif di pasar karena komitmen pada keamanan.
7. Budaya keamanan yang lebih kuat di dalam organisasi.

B. Tantangan

1. Biaya tinggi untuk implementasi, pelatihan dan sertifikasi.
2. Proses kompleks dengan dokumentasi dan kontrol berlapis.

3. Resistensi karyawan terhadap perubahan kebijakan.
4. Keterbatasan sumber daya terutama di organisasi kecil.
5. Ancaman siber yang terus berkembang membutuhkan pembaruan.
6. Waktu implementasi panjang tergantung skala organisasi.
7. Ketergantungan pada dukungan manajemen agar berjalan efektif.

Implementasi ISO/IEC 27001 juga menghadapi sejumlah tantangan. Organisasi sering mengalami keterbatasan sumber daya, baik dari sisi dana, infrastruktur TI, maupun tenaga ahli yang memahami standar dan kontrol keamanan. Perubahan budaya organisasi dapat menjadi hambatan signifikan, terutama ketika staf merasa kebijakan baru mengganggu kebebasan kerja atau menambah beban(Apriany & Wibowo, 2024). Ddokumentasi dan audit kepatuhan memerlukan waktu dan usaha besar. Adaptasi terhadap versi terbaru standar juga menjadi tantangan karena organisasi harus memperbarui kontrol dan prosedur agar tetap sesuai dengan revisi standar.

Aspek lain yang menjadi kendala adalah perubahan budaya kerja di dalam organisasi. Kebijakan baru terkait keamanan informasi sering kali dianggap mengganggu fleksibilitas karyawan atau menambah beban administratif, sehingga menimbulkan resistensi. Kurangnya kesadaran akan pentingnya keamanan informasi menyebabkan sebagian staf tidak mematuhi prosedur yang ada, padahal kepatuhan menjadi kunci dalam keberhasilan implementasi (Apriany & Wibowo, 2024).

Proses dokumentasi menjadi salah satu tantangan besar dalam penerapan ISO/IEC 27001. Standar ini menuntut dokumentasi yang lengkap, mulai dari kebijakan, prosedur, catatan aktivitas, hingga bukti penerapan kontrol keamanan. Proses tersebut tidak hanya memakan waktu, tetapi juga membutuhkan konsistensi dalam pengelolaan dokumen agar selalu siap untuk dilakukan audit internal maupun eksternal.

Audit kepatuhan sendiri menjadi pekerjaan yang memerlukan tenaga, biaya dan fokus manajemen. Organisasi harus memastikan bahwa seluruh aktivitas

berjalan sesuai dengan standar yang berlaku. Ketika ditemukan ketidaksesuaian, tindakan korektif harus segera dilakukan, yang pada praktiknya sering menimbulkan tekanan tambahan bagi tim manajemen maupun staf operasional.

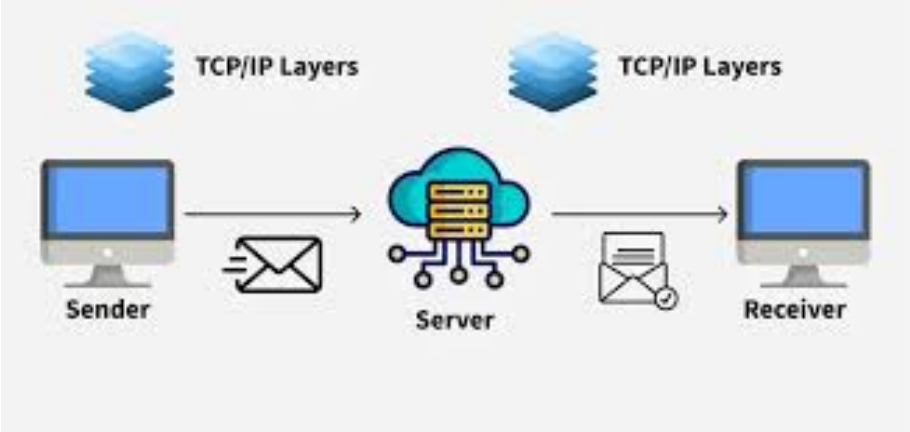
Tantangan berikutnya muncul ketika terjadi revisi standar ISO/IEC 27001. Organisasi dituntut untuk segera melakukan penyesuaian terhadap kontrol, prosedur dan kebijakan yang sudah ada. Hal ini membutuhkan evaluasi menyeluruh serta pembaruan dokumentasi, yang berarti tambahan biaya, waktu, serta pelatihan bagi karyawan. Adaptasi yang lambat dapat menyebabkan organisasi kehilangan sertifikasi atau menghadapi risiko tidak patuh terhadap persyaratan terbaru.

Keamanan Jaringan

Minggu 7 Keamanan jaringan I: model TCP/IP, ancaman jaringan, firewall, IDS/IPS.

A. Konsep Model TCP/IP

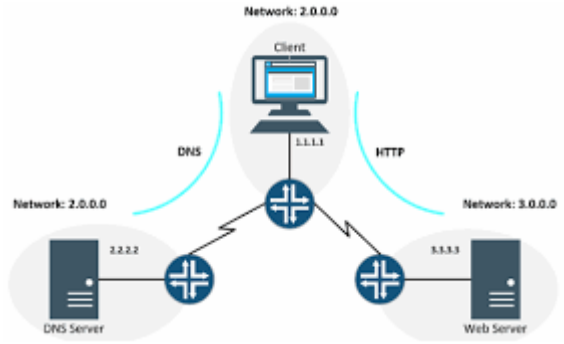
Model TCP/IP (Transmission Control Protocol / Internet Protocol) adalah kerangka protokol komunikasi yang digunakan untuk mentransmisikan data antar perangkat di jaringan berdasarkan prinsip layering. Model ini mengelompokkan fungsi komunikasi ke dalam lapisan-lapisan yang saling berinteraksi; setiap lapisan memiliki tanggung jawab spesifik dalam proses pengiriman data dari pengirim ke penerima. (Saide, 2024)



Gambar 1. 4 Konsep Model TCP/IP

Sumber : https://jakarta.telkomuniversity.ac.id/perbedaan-model-osi-dan-tcp-ip-dalam-jaringan-komputer/

Model TCP/IP lebih praktis dibanding OSI karena dirancang berdasarkan protokol nyata yang digunakan di Internet, sehingga ia menggabungkan beberapa fungsi lapisan untuk menyederhanakan struktur. Dalam model ini, protokol-protokol seperti IP, TCP, UDP, serta protokol aplikasi (HTTP, DNS, FTP) bekerja bersama untuk menjamin bahwa data dikemas, dialamatkan, dikirim, dirutekan dan diterima dengan benar. (Ezeagwu et al., 2021)



Gambar 1. 5 Model TCP/IP

Sumber : https://blog.unmaha.ac.id/peran-protokol-tcp-ip-dalam-jaringan-fondasi-komunikasi-modern/

Model TCP/IP juga mencerminkan filosofi "end-to-end" dalam hal keandalan dan penanganan kesalahan: kestabilan dan kontrol kesalahan sebagian besar diatur di lapisan transport, bukan di setiap lapisan. Karena itu, model ini tidak memaksakan setiap lapisan bertanggung jawab penuh atas reliabilitas; fungsi kontrol kesalahan dan retransmisi dikembalikan ke lapisan transport. Pendekatan ini memungkinkan fleksibilitas dan modularitas protokol baru bisa ditambahkan atau diganti di lapisan tertentu tanpa merombak seluruh sistem. Artikel "*Exploring the TCP/IP Protocol Suite: Architecture, Dominance, and Future Challenges*" menjelaskan bagaimana struktur modular model TCP/IP sangat berkontribusi terhadap dominasi model ini di dunia komunikasi modern.

Model TCP/IP (Transmission Control Protocol / Internet Protocol) adalah kerangka protokol komunikasi yang digunakan untuk mentransmisikan data antar perangkat di jaringan berdasarkan prinsip layering. Model ini mengelompokkan fungsi komunikasi ke dalam lapisan-lapisan yang saling berinteraksi; setiap lapisan memiliki tanggung jawab spesifik dalam proses pengiriman data dari pengirim ke penerima.

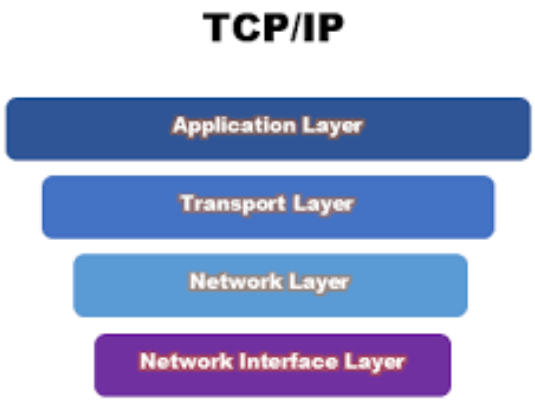
Secara konseptual, model TCP/IP terdiri dari empat lapisan utama, yaitu Application Layer, Transport Layer, Internet Layer dan Network Access Layer. Masing-masing lapisan memiliki peran tersendiri: lapisan aplikasi menangani antarmuka dengan pengguna atau program, lapisan transport mengatur segmentasi dan reliabilitas data, lapisan internet bertanggung jawab pada

pengalamatan dan routing paket, sedangkan lapisan akses jaringan berhubungan dengan media fisik untuk transmisi data. Pemisahan ini memungkinkan komunikasi berjalan lebih terstruktur, terstandarisasi, serta memudahkan interoperabilitas antar perangkat dan sistem yang berbeda.

Selain sebagai dasar komunikasi internet modern, model TCP/IP juga menjadi landasan dalam pengembangan teknologi jaringan baru. Dengan adanya standar ini, produsen perangkat keras, penyedia layanan jaringan dan pengembang perangkat lunak dapat merancang produk yang kompatibel satu sama lain. Hal ini menjadikan TCP/IP sebagai model dominan dalam jaringan global, menggantikan model sebelumnya seperti OSI yang meskipun lebih rinci, namun kurang diimplementasikan dalam praktik nyata.

B. Lapisan TCP/IP

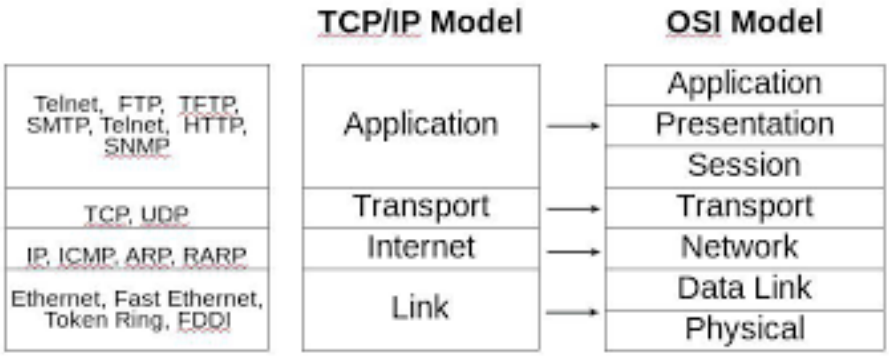
Model TCP/IP (Internet Protocol Suite) menyusun fungsi komunikasi jaringan ke dalam beberapa lapisan, dimana setiap lapisan memiliki tanggung jawab tersendiri untuk menjaga agar data dapat dikirim dari satu host ke host lain dengan benar. Pada dasarnya, model ini membagi arsitektur komunikasi jaringan ke dalam empat (kadang lima, tergantung varian) lapisan: *Network Interface / Link*, *Internet*, *Transport* dan *Application*. Setiap paket data "dibungkus" (encapsulation) dan "dibuka bungkusnya" (decapsulation) secara berurutan oleh lapisan-lapisan ini sepanjang pengiriman antara pengirim dan penerima.(Ezeagwu et al., 2021)



Gambar 1. 6 Lapisan TCP/IP

Sumber : https://www.arduinoindonesia.id/2023/05/pengertian-dan-penjelasan-tentang-tcpip.html

Dalam praktiknya, protokol-protokol seperti IP, TCP, UDP, ARP, ICMP, DNS, HTTP dan lain-lain berfungsi di lapisan-lapisan TCP/IP tersebut. Lapisan *Network Interface* bertanggung jawab menangani pengiriman fisik di media, framing dan pengalamatan fisik. Lapisan *Internet* (atau Network) mengatur pengalamatan logika (IP), routing, fragmentasi paket dan kontrol kongesti. Lapisan *Transport* memastikan koneksi antara aplikasi, pengendalian aliran (flow control), retransmisi paket yang hilang dan multiplexing antar aplikasi. Akhirnya, lapisan *Application* menyediakan antarmuka bagi aplikasi pengguna (web, email, DNS, FTP) untuk berkomunikasi melalui jaringan.(Saide, 2024)



Gambar 1. 7 Network Interface

Sumber : https://www.fathurhoho.id/2017/08/penjelasan-tentang-tcp-ip.html

Fungsi & Protokol di Tiap Lapisan TCP/IP(Tyagi, 2020)

1) Network Interface / Link Layer

   Mengelola framing, pengalamatan fisik (MAC), pengendalian akses media; protokol: Ethernet, Wi-Fi, ARP, PPP.

2) Internet / Network Layer

   Menangani pengalamatan logika, routing, fragmentasi, ICMP, IP (IPv4/IPv6).

3) Transport Layer

Mengatur transport end-to-end; protokol: TCP (transmission control), UDP (user datagram).

4) Application Layer

Menangani fungsi aplikasi dan layanan; protokol: HTTP, HTTPS, DNS, FTP, SMTP, SSH, DHCP.

C. Fungsi Protokol TCP/IP

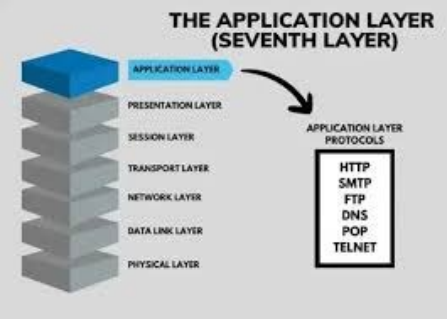
Protokol TCP/IP menyediakan seperangkat aturan komunikasi digital yang memungkinkan perangkat di jaringan saling bertukar data. Setiap protokol dalam *suite* TCP/IP memiliki tugas khusus: pengalamatan, pengiriman, pengaturan aliran data, serta ketahanan terhadap kesalahan. (Tyagi, 2020)

Protokol ini bekerja secara berlapis aplikasi, transport, internet dan link sehingga tugas kompleks komunikasi jaringan terbagi menjadi fungsi-fungsi modular. Modularitas ini memungkinkan pengembang untuk memperbarui atau menggantikan protokol di satu lapisan tanpa memengaruhi keseluruhan sistem. Fungsi Protokol TCP/IP / Contoh Protokol & Fungsi Utama

1) IP: pengalamatan logis, routing, fragmentasi
2) ICMP: pesan kontrol, diagnostik jaringan
3) TCP: koneksi andal, retransmisi, kontrol aliran & kesalahan
4) UDP: pengiriman cepat tanpa overhead reliabilitas
5) HTTP: komunikasi web, permintaan & respon halaman
6) FTP: transfer file antar host
7) SMTP / IMAP / POP: pengiriman dan penerimaan email
8) DNS: resolusi nama domain → alamat IP
9) SSH: akses jarak jauh aman
10) DHCP: pengalokasian alamat IP dinamis

Pada lapisan *Internet*, protokol IP mengatur pengalamatan dan routing paket dari sumber ke tujuan melalui berbagai jaringan dan perangkat perantara (router). Fungsi penting IP meliputi fragmentasi paket agar cocok ukuran MTU, kontrol kesalahan dasar (melalui header checksum) dan pengenalan alamat logis (IPv4/IPv6). Protokol ICMP juga menjadi bagian integral, memberikan mekanisme pengiriman pesan diagnostik dan kontrol (misalnya pesan "ping" atau laporan error rute).(Saide, 2024)

Lapisan *Transport* mengandung protokol seperti TCP (Transmission Control Protocol) dan UDP (User Datagram Protocol). TCP bertugas menjamin pengiriman data secara andalan, melalui mekanisme *handshake*, *flow control*, *retransmission* dan penomoran urutan (sequence). Sementara UDP menyediakan pengiriman cepat tanpa overhead reliabilitas, cocok untuk aplikasi real-time seperti video streaming atau VoIP. Beberapa ekstensi seperti SCTP atau DCCP juga hadir sebagai alternatif untuk kebutuhan khusus jaringan modern.(Saide, 2024)



Gambar 1. 8 Lapisan Application

Sumber : https://medium.com/@kavyanshgandhi/the-application-layer-internets-postal-service-bdbc7dcd1173

Lapisan *Application* berisi protokol yang langsung digunakan oleh aplikasi akhir: HTTP, FTP, SMTP, DNS, SSH dan lain-lain. Protokol ini menyederhanakan komunikasi pengguna dengan jaringan: HTTP untuk web, FTP untuk transfer file, SMTP/IMAP/POP untuk email, DNS untuk penerjemahan nama domain menjadi alamat IP dan SSH untuk akses aman ke

sistem remote. Protokol aplikasi ini memanfaatkan layanan transport (TCP/UDP) agar pesan pengguna dikemas, dikirim dan diterima dengan benar.

D. Jenis Ancaman Jaringan

Ancaman jaringan (network threats) merujuk pada segala bentuk potensi gangguan, serangan, atau penyalahgunaan terhadap infrastruktur jaringan dan data yang melewatinya. Ancaman ini dapat bersifat pasif (passive) maupun aktif (active). Ancaman pasif melibatkan pengintaian atau pengumpulan data tanpa mengubah data tersebut, sementara ancaman aktif mencakup tindakan yang mengganggu, merusak, atau menyuntikkan perubahan dalam sistem jaringan. Karakteristik ancaman jaringan mencakup skala serangan (lokal hingga global), kompleksitas teknik yang digunakan (dari serangan sederhana hingga serangan canggih seperti APT) dan sifatnya yang adaptif terhadap teknik pertahanan.(Tyagi, 2020)

Seiring meningkatnya konektivitas dan penggunaan berbagai perangkat IoT, ancaman jaringan menjadi semakin beragam dan kompleks. Serangan tidak hanya datang dari luar, tetapi juga dari dalam (insider). Beberapa ancaman modern juga memanfaatkan kelemahan protokol, kesalahan konfigurasi dan celah keamanan aplikasi. Dalam konteks organisasi, ancaman jaringan bisa berdampak besar pada kerahasiaan, integritas dan ketersediaan layanan TI. Studi "Threats and Mitigation Techniques in Network Security" menguraikan berbagai ancaman seperti serangan data modification, denial-of-service dan eskalasi hak akses, serta strategi mitigasi yang diperlukan.(Andersson & Seid, 2024)

Ancaman jaringan kadang muncul secara terkoordinasi dan sistematis, seperti *Advanced Persistent Threats (APT)*, di mana penyerang menyusup ke jaringan dan mempertahankan keberadaan mereka dalam waktu lama tanpa terdeteksi. Selain itu, serangan berbasis web (web threats), supply chain attacks, serta serangan berbasis malware dan ransomware merupakan bagian dari ancaman jaringan kontemporer. Adaptasi teknik serangan seperti evasion, polymorphic malware dan serangan zero-day membuat pertahanan jaringan harus terus diperbarui. Artikel "A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks and Solutions" menekankan bahwa peran

teknologi baru seperti pembelajaran mesin dan blockchain dapat membantu mendeteksi serangan baru yang sulit diantisipasi. Jenis-Jenis Ancaman Jaringan sebagai berikut :

1) Sniffing / Eavesdropping (pengintaian data)
2) Man-in-the-Middle (MITM)
3) Denial of Service (DoS) / Distributed DoS (DDoS)
4) Serangan Modifikasi Data (Data Modification)
5) Spoofing / IP Spoofing
6) Session Hijacking
7) Malware / Ransomware / Trojan / Worm
8) Advanced Persistent Threat (APT)
9) Web threats (SQL injection, XSS, CSRF)
10) Serangan pada rantai pasokan (Supply Chain Attack)
11) Insider Threat (serangan dari dalam organisasi)
12) Serangan berbasis protokol / kelemahan konfigurasi jaringan

Organisasi perlu mengenali bahwa ancaman bukan hanya berupa upaya teknis semata tetapi juga sosial dan manusiawi (social engineering). Penyerang dapat memanipulasi pengguna agar membocorkan kredensial atau akses ke sistem. Pertahanan jaringan harus mencakup kontrol teknis, kebijakan, pelatihan, serta pemantauan..

E. Dampak Serangan Jaringan

Serangan jaringan dapat menimbulkan dampak serius pada berbagai aspek organisasi mulai dari aspek teknis hingga bisnis dan reputasi. Dari sisi teknis, serangan seperti DDoS atau malware dapat membuat sistem tidak responsif atau bahkan mati total (downtime), mengganggu layanan dan menyebabkan kerusakan perangkat keras atau perangkat lunak. Serangan yang berhasil menyusup ke dalam sistem mungkin menyebarkan malware atau backdoor,

sehingga merusak integritas data atau memberikan akses jangka panjang kepada penyerang. Dalam banyak kasus, serangan tersebut juga menimbulkan beban operasional karena tim TI harus melakukan investigasi, pemulihan sistem dan patching yang memerlukan waktu dan biaya.(Andersson & Seid, 2024)

Gambar 1. 9 Dampak Serangan Jaringan

Sumber : https://puskomedia.id/blog/apa-itu-serangan-ddos-dan-mengapa-penting-untuk-diperhatikan/

Dampaknya bisa berupa kerugian finansial langsung dan tak langsung. Organisasi mungkin mengalami kehilangan pendapatan akibat layanan tidak tersedia, denda regulasi karena pelanggaran data, atau tuntutan hukum dari klien atau pemangku kepentingan. Biaya pemulihan (forensik, penggantian sistem, audit keamanan) dapat sangat tinggi. Serangan jaringan juga sering menyebabkan hilangnya kepercayaan pelanggan atau mitra bisnis, yang lama-kelamaan dapat merusak citra organisasi. Karena reputasi tercemar, pelanggan bisa berpindah ke penyedia lain dan memengaruhi pangsa pasar organisasi.(Andersson & Seid, 2024)

Serangan jaringan juga memiliki implikasi terhadap kepatuhan terhadap regulasi dan aspek hukum. Jika data pribadi bocor karena serangan, organisasi dapat dikenai sanksi atau denda berdasarkan undang-undang perlindungan data (misalnya GDPR atau regulasi lokal). Organisasi juga mungkin diwajibkan melaporkan insiden keamanan, melakukan audit eksternal, atau menghadapi litigasi dari pihak yang dirugikan. Dalam kasus infrastrukur kritikal, serangan jaringan bisa membawa dampak sosial yang lebih luas: misalnya jika layanan

telekomunikasi, listrik, atau sistem kesehatan terganggu, maka masyarakat luas bisa ikut merasakan kerugian.

Gambar 1. 10 Serangan Jaringan

Sumber : https://digitalsolusigrup.co.id/evil-twin-attack-adalah/

Secara strategis, dampak serangan jaringan dapat menggangu kontinuitas bisnis dan memperlambat inovasi teknologi. Organisasi yang sering diserang mungkin menjadi enggan mengadopsi teknologi baru atau transformasi digital karena kekhawatiran keamanan yang tinggi.(Franken & Reuter, 2024)

Jaringan kemitraan dan kolaborasi juga bisa terganggu karena mitra tidak mau bekerja sama jika mereka merasa resiko keamanan terlalu besar. serangan jaringan yang berat bisa memicu krisis bisnis yang memerlukan pengambil keputusan strategis untuk merombak model operasional dan keamanan organisasi. Contoh Dampak Serangan Jaringan :

1) Layanan tidak bisa diakses (downtime)
2) Modifikasi atau penghapusan data
3) Pencurian data rahasia / bocornya data pribadi
4) Kehilangan pendapatan & biaya pemulihan tinggi
5) Denda regulasi & litigasi
6) Kerusakan infrastruktur TI & perangkat keras
7) Kerusakan reputasi & kepercayaan publik

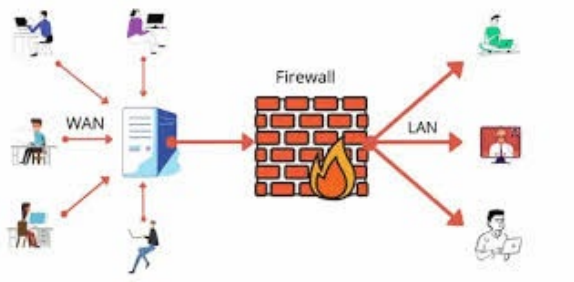
8) Gangguan operasional, termasuk pemulihan manual

9) Gangguan terhadap layanan kritikal (kesehatan, listrik, telekomunikasi)

10) Hambatan pertumbuhan dan investasi teknologi

F. Mekanisme Firewall

Firewall adalah perangkat atau sistem yang berfungsi sebagai garis pertahanan antara jaringan internal dan eksternal, dengan tujuan mengendalikan lalu lintas data berdasarkan kebijakan keamanan yang telah ditetapkan. Mekanisme dasar mencakup *packet filtering*, *stateful inspection* dan *application-level filtering*. *Packet filtering* memeriksa header paket seperti alamat IP sumber dan tujuan, port, serta protokol untuk menentukan apakah paket tersebut boleh diteruskan atau harus diblokir (Lo Giudice & Ghafir, 2024). *Stateful inspection* bekerja lebih cerdas karena mampu melacak status koneksi, memastikan bahwa hanya paket yang sesuai dengan sesi komunikasi yang sah yang dapat melewati firewall. Sedangkan *application-level filtering* atau *proxy firewall* beroperasi pada lapisan aplikasi dengan memeriksa konten lalu lintas, misalnya pada protokol HTTP atau FTP, untuk mendeteksi aktivitas mencurigakan.



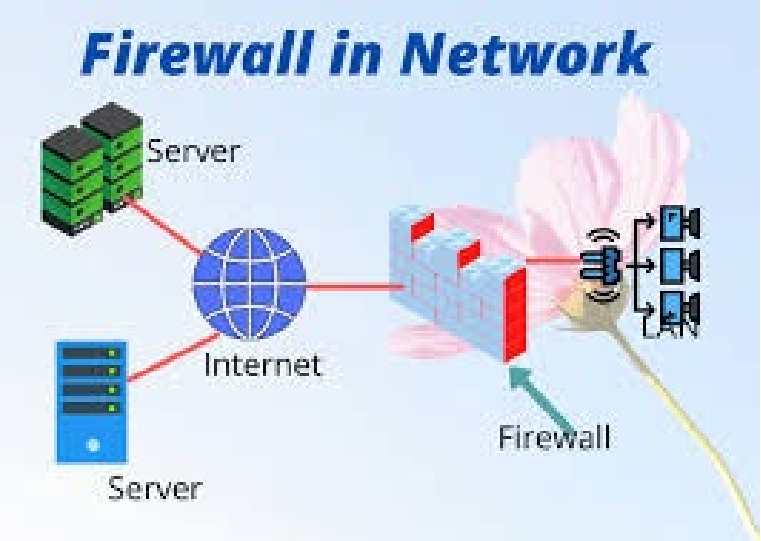
Gambar 1. 11 Firewall

Sumber : https://medium.com/@shyamsandeep28/introduction-of-aws-web-application-firewall-layer-7-firewall-a-step-by-step-guide-096b3d5b49e3

Seiring dengan perkembangan teknologi dan meningkatnya ancaman siber, firewall modern dikembangkan menjadi *Next-Generation Firewall (NGFW)*. Firewall jenis ini tidak hanya melakukan penyaringan pada header paket, tetapi juga mampu melakukan *deep packet inspection* (DPI), yaitu menganalisis isi paket secara lebih mendalam hingga ke lapisan aplikasi. Dengan mekanisme ini,

firewall dapat mengenali aplikasi, mendeteksi pola berbahaya dan mencegah serangan yang lebih kompleks seperti malware, serangan berbasis payload, atau upaya intrusi yang tersembunyi dalam lalu lintas terenkripsi.(Wang, 2022)

Terdapat konsep *distributed firewall* yang dirancang untuk lingkungan komputasi modern seperti cloud, virtualisasi dan jaringan berbasis perangkat mobile. Firewall jenis ini bekerja secara terdistribusi dengan menempatkan aturan keamanan lebih dekat ke sumber lalu lintas, sehingga perlindungan dapat diberikan secara menyeluruh di berbagai titik jaringan. Pendekatan ini menjawab kebutuhan keamanan pada sistem yang bersifat dinamis, skalabel dan tersebar di berbagai lokasi.(Patel, 2024)



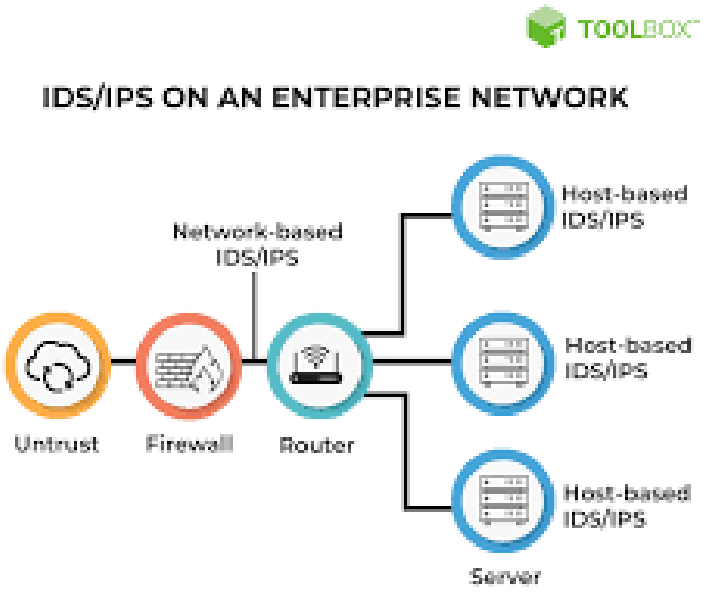
Gambar 1. 12 Distributed Firewall

Sumber : https://puskomedia.id/blog/firewall-pada-server-membangun-zona-aman-dalam-infrastruktur-anda/

Firewall juga semakin cerdas dengan mengadopsi teknologi berbasis kecerdasan buatan dan otomatisasi. Dengan integrasi analisis perilaku dan *machine learning*, firewall mampu mendeteksi pola lalu lintas abnormal, melakukan penyesuaian aturan secara otomatis, serta merespons ancaman baru dengan lebih cepat. Penerapan otomatisasi ini mengurangi ketergantungan pada konfigurasi manual, meminimalkan kesalahan manusia, serta meningkatkan efisiensi dalam pengelolaan keamanan jaringan.

G. IDS vs IPS

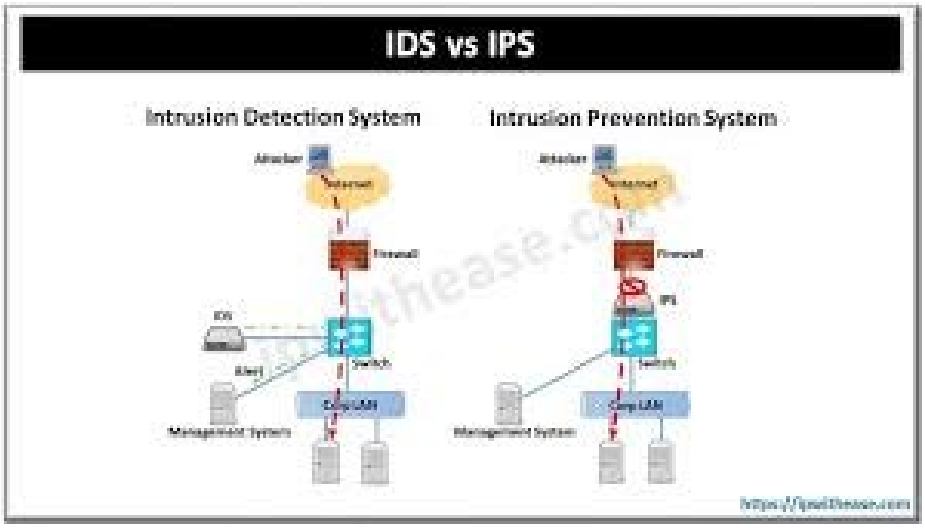
Intrusion Detection System (IDS) adalah sistem yang dirancang untuk memantau lalu lintas jaringan atau aktivitas sistem dan mendeteksi kejadian yang mencurigakan atau melanggar kebijakan keamanan. Ketika sistem menemukan pola serangan atau anomali, ia menghasilkan alarm atau log untuk memberi tahu administrator bahwa terjadi potensi ancaman, tetapi tidak mengambil tindakan aktif untuk menghentikannya. IDS bekerja “pasif”mereka berada di luar jalur (out-of-band) dan hanya menganalisis salinan trafik, sehingga tidak memblokir paket secara langsung.



Gambar 1. 13 Intrusion Detection System

Sumber : https://www.spiceworks.com/it-security/network-security/articles/ids-vs-ips/

Sebaliknya, Intrusion Prevention System (IPS) memperluas fungsi IDS dengan kemampuan preventif yaitu tidak hanya mendeteksi tetapi juga merespons kejadian ancaman secara real time. IPS ditempatkan “in-line” dalam jalur trafik, sehingga bisa langsung memblok paket jahat, memutus koneksi, atau menerapkan aturan mitigasi secara otomatis. Dengan demikian, IPS bersifat proaktif dalam mencegah serangan menyebar atau merusak sistem lebih jauh.



Gambar 1. 14 Perbedaan utama antara IDS dan IPS

Sumber : https://ipwithease.com/difference-between-ips-and-ids-in-network-security/

Perbedaan utama antara IDS dan IPS terletak pada aspek lokasi, tindakan respons dan resiko false positive. Karena IPS dijalankan pada jalur utama trafik, kesalahan dalam mengenali lalu lintas bisa menyebabkan paket sah yang sebenarnya tidak berbahaya diblokir, yang pada gilirannya mungkin mengganggu operasi normal sistem. Beban kinerja sistem lebih tinggi karena semua paket melewati IPS dan harus dianalisis. Sementara itu, IDS tidak menghadapi konsekuensi langsung terhadap trafik normal apabila terjadi false alarm, karena hanya memberi peringatan.

Dalam implementasi nyata, organisasi sering menggunakan kombinasi IDS dan IPS (atau IDPS) untuk mendapatkan keseimbangan antara deteksi dan pencegahan. Model hibrid memungkinkan sistem mendeteksi potensi ancaman dan mengambil tindakan preventif hanya pada kondisi tertentu (misalnya ketika tingkat ancamannya tinggi atau terjadi pola yang jelas). Dengan pendekatan ini, kelemahan masing-masing sistem dapat dikompensasi IDS menyediakan visibilitas dan logging yang lebih aman dan IPS menambahkan lapisan respons otomatis terhadap serangan nyata.

Contoh Fungsi / Perbedaan IDS vs IPS :

1. IDS mendeteksi (monitoring & alert), sementara IPS mendeteksi + mencegah (block/drop)
2. IDS bersifat pasif (out-of-band), IPS aktif (in-line)
3. IDS tidak mengganggu trafik normal meskipun false alarm; IPS bisa memblokir trafik valid jika false positive
4. IPS butuh kinerja lebih tinggi karena analisis real time terhadap paket yang lewat
5. IDS cocok untuk audit, forensik dan visibilitas
6. IPS cocok untuk proteksi real time dan mitigasi langsung

Keamanan jaringan modern menghadapi ancaman yang semakin kompleks dan beragam, mulai dari serangan berbasis malware hingga serangan terdistribusi seperti DDoS. Untuk itu, organisasi memerlukan mekanisme yang tidak hanya mampu mendeteksi ancaman, tetapi juga mencegah dampaknya secara langsung. Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS) berkembang sebagai dua komponen vital dalam arsitektur pertahanan jaringan. Keduanya sering digunakan bersama untuk menciptakan lapisan proteksi berlapis (defense in depth).(Wang, 2022)

Secara historis, IDS muncul lebih dulu sebagai solusi untuk memberikan visibilitas terhadap lalu lintas jaringan dan mendeteksi pola serangan. Namun, seiring dengan meningkatnya volume dan kecepatan serangan, kebutuhan munculnya sistem yang lebih aktif akhirnya mendorong lahirnya IPS. Dengan sifatnya yang proaktif, IPS mampu mencegah kerusakan yang ditimbulkan serangan sebelum mencapai target, yang membuatnya lebih relevan pada lingkungan bisnis dengan kebutuhan uptime tinggi.(Thapa & Akalanka, 2020)

Perkembangan teknologi analisis data, seperti machine learning dan behavioral analysis, telah meningkatkan kemampuan IDS maupun IPS. IDS modern tidak lagi hanya berbasis signature, melainkan mampu mengenali pola anomali dan aktivitas mencurigakan yang belum pernah terdaftar sebelumnya. IPS semakin cerdas dalam mengurangi false positive dengan menilai konteks

lalu lintas jaringan secara lebih akurat. Hal ini menjadikan kombinasi IDS/IPS sebagai alat yang lebih adaptif dalam menghadapi ancaman siber kontemporer.

Pengujian Keamanan

Minggu 11 Pengujian keamanan (non-exploitative): vulnerability scanning, pentest etika (konsep, hukum, batas) dan metode mitigasi.

A. Konsep Pengujian Keamanan

Pengujian keamanan (*security testing*) adalah proses evaluasi sistem, jaringan, atau perangkat lunak untuk mengidentifikasi kelemahan atau celah keamanan sebelum pihak jahat mengeksploitasinya. Tujuan utamanya bukan untuk menyerang, tetapi menguji secara terkendali dan etis sejauh mana sistem rentan terhadap ancaman. Proses ini membantu organisasi memahami titik lemah mereka dari perspektif penyerang, tetapi tetap berada dalam batas aman sehingga tidak merusak sistem atau mengganggu operasional.(Subhangani & Chaudhary, 2020)

Gambar 1. 15 Konsep Pengujian Keamanan

Sumber : https://www.testingxperts.com/blog/security-testing-guide

Dalam non-exploitative, pengujian keamanan meliputi teknik-teknik yang tidak menggunakan eksploit langsung (tidak mengeksploitasi celah menjadi serangan aktif), melainkan mendeteksi dan mendiagnosa potensi kelemahan. Teknik seperti *vulnerability scanning*, *configuration review*, *security auditing*, atau *code analysis statis* sering digunakan. Pendekatan ini memungkinkan organisasi menemukan risiko sebelum terjadi eksploitasi, sekaligus menjaga integritas sistem selama pengujian.(Bennouk et al., 2024)

Pendekatan non-exploitative memberikan keuntungan signifikan bagi organisasi, karena risiko gangguan terhadap operasi normal sistem dapat diminimalkan. Proses ini menekankan pada identifikasi celah dan rekomendasi mitigasi tanpa menimbulkan kerusakan atau kehilangan data. Dengan menggunakan teknik seperti *vulnerability scanning* dan *code analysis statis*, organisasi dapat mengidentifikasi konfigurasi yang lemah, patch yang belum diterapkan, atau kesalahan pemrograman yang berpotensi dimanfaatkan oleh pihak yang tidak bertanggung jawab.

Evaluasi berbasis audit dan review konfigurasi membantu membangun kesadaran tim TI dan pemangku kepentingan terhadap risiko keamanan. Hasil pengujian dapat dijadikan dasar untuk memperbaiki kebijakan, prosedur dan kontrol teknis yang ada. Pendekatan ini tidak hanya mendeteksi kelemahan, tetapi juga mendorong peningkatan berkelanjutan pada praktik keamanan informasi, sehingga menciptakan sistem yang lebih tahan terhadap ancaman masa depan.

Pengujian keamanan juga harus mempertimbangkan aspek legal dan etika. Meskipun pengujian dilakukan untuk tujuan perlindungan, jika tidak ada izin atau batasan yang jelas, maka aktivitas tersebut bisa dianggap sebagai serangan ilegal atau pelanggaran hukum. Prosedur pengujian umumnya melibatkan persetujuan tertulis, ruang lingkup yang disepakati dan dokumentasi lengkap agar tidak terjadi kesalahpahaman atau dampak negatif terhadap sistem yang diuji.

Setelah kelemahan ditemukan, hasil pengujian harus ditindaklanjuti dengan analisis, prioritisasi dan mitigasi yang sesuai. Hasil laporan keamanan akan menyajikan rekomendasi perbaikan, seperti patch perangkat lunak, perubahan konfigurasi, atau penerapan kontrol tambahan. Dengan demikian, pengujian keamanan menjadi bagian integral dalam siklus keamanan bukan sekadar aktivitas satu kali demi meningkatkan postur keamanan organisasi dari waktu ke waktu.

Contoh Teknik Non-Exploitative Pengujian Keamanan :

1. Vulnerability scanning (menggunakan tool otomatis untuk mendeteksi celah yang dikenal)
2. Static code analysis / review kode sumber
3. Audit konfigurasi sistem dan keamanan
4. Security audit / compliance check
5. Assessment kerentanan aplikasi web (non-intrusive)
6. Analisis dependency & komponen (software composition analysis)
7. Review kebijakan & prosedur keamanan
8. Assessment arsitektur dan desain keamanan

B. Prinsip Non-Exploitative

Prinsip non-exploitative dalam pengujian keamanan menekankan bahwa pengujian dilakukan dengan cara aman dan tidak merusak sistem. Artinya, saat pengujian, penguji tidak akan menggunakan eksploit aktif yang bisa mengubah sistem, mencuri data, atau menimbulkan downtime. Tujuannya adalah menemukan kelemahan tanpa memicu kerusakan. Penguji harus menghindari tindakan yang bersifat destruktif, seperti eksekusi exploit berbahaya, injeksi skrip yang merusak, atau modifikasi database. Dengan prinsip ini, pengujian tidak mengganggu layanan nyata dan meminimalkan risiko bagi organisasi. Prinsip Non-Exploitative sebagai berikut :

1. Pengujian aman tanpa merusak sistem
2. Tidak menggunakan exploit aktif yang mengubah data
3. Otorisasi & kesepakatan ruang lingkup (scope)
4. Penjagaan kerahasiaan data pengujian
5. Pencatatan aktivitas & dokumentasi (audit trail)
6. Pelaporan hasil kepada pihak berwenang
7. Rekomendasi mitigasi tanpa memperlemah

Prinsip berikutnya adalah pengujian harus dilakukan dengan otorisasi dan batas cakupan yang jelas. Sebelum pengujian non-exploitative dijalankan, organisasi dan penguji harus menyepakati ruang lingkup (scope), sistem mana saja yang boleh diuji dan teknik mana yang diizinkan. Jika tanpa izin atau melewati batas, pengujian bisa dianggap tindakan ilegal. Selain itu, penguji perlu menjaga kerahasiaan data yang ditemukan selama pengujian, serta memastikan integritas sistem tetap terjaga. Laporan hasil pengujian harus disampaikan ke pihak yang berwenang dan tidak disalahgunakan.

Prinsip non-exploitative juga mengedepankan verifikasi dan pertanggungjawaban. Setiap aktivitas pengujian harus dicatat metode, waktu, alat yang digunakan dan hasilnya sehingga bisa diaudit kembali jika ada masalah. Penguji harus menunjukkan dokumentasi bahwa mereka bertindak sesuai kesepakatan dan bila ditemukan kelemahan, langkah mitigasi harus direkomendasikan tanpa menimbulkan kerentanan baru. Keberhasilan pengujian non-exploitative terletak pada sikap tanggung jawab tinggi dari penguji agar pengujian membawa manfaat tanpa konsekuensi buruk bagi sistem.

Prinsip non-exploitative menekankan pentingnya transparansi kepada pemilik sistem dan pihak terkait. Setiap temuan harus dilaporkan secara rinci, mencakup tingkat risiko, lokasi celah dan rekomendasi perbaikan. Hal ini memungkinkan manajemen untuk mengambil keputusan berbasis informasi yang akurat mengenai prioritas mitigasi dan alokasi sumber daya. Dengan dokumentasi yang lengkap, organisasi dapat menunjukkan kepatuhan terhadap kebijakan keamanan dan peraturan yang berlaku.(Gani, 2024)

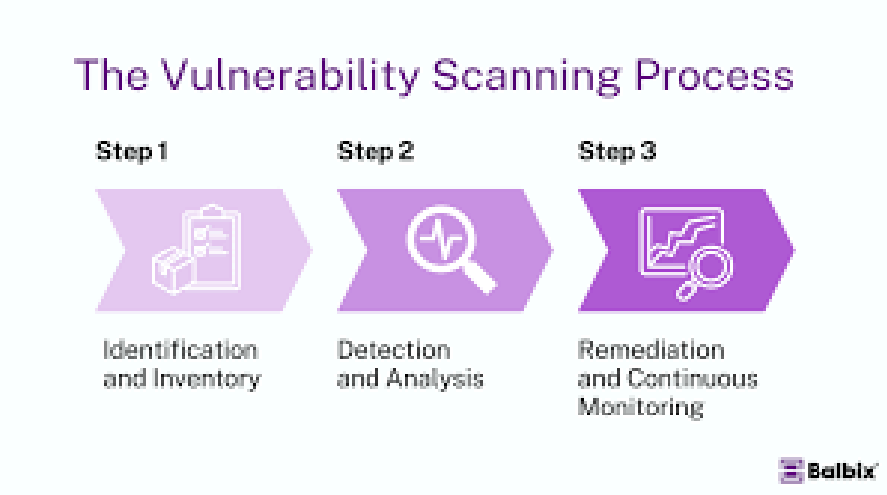
Prinsip ini juga mendorong penerapan proses audit internal dan evaluasi berkelanjutan. Penguji non-exploitative harus memastikan bahwa tindakan mereka dapat direplikasi dan diverifikasi oleh tim lain, sehingga hasil pengujian menjadi bukti sahih untuk perbaikan sistem. Dengan pendekatan ini, pengujian keamanan tidak hanya fokus pada identifikasi risiko, tetapi juga membangun budaya tanggung jawab, akuntabilitas dan

keamanan proaktif dalam seluruh organisasi.(Tabitha Fransisca Romauli Nababan & Shevanna Putri Cantiqa, 2024)

C. Vulnerability Scanning

Vulnerability scanning adalah metode sistematis untuk mendeteksi kelemahan atau celah keamanan pada sistem, jaringan, atau aplikasi tanpa melakukan eksploitasi langsung. Tujuannya adalah menemukan potensi titik lemah (vulnerabilities) seperti port terbuka, layanan yang usang atau tidak aman, konfigurasi software yang salah sebelum penyerang mengambil keuntungan darinya (Bennouk et al., 2024).

Proses ini biasanya memakai alat otomatis (scanner) yang membandingkan kondisi target dengan basis data kelemahan yang diketahui dan standar keamanan, lalu menghasilkan laporan tentang temuan, tingkat keparahan dan rekomendasi perbaikan.



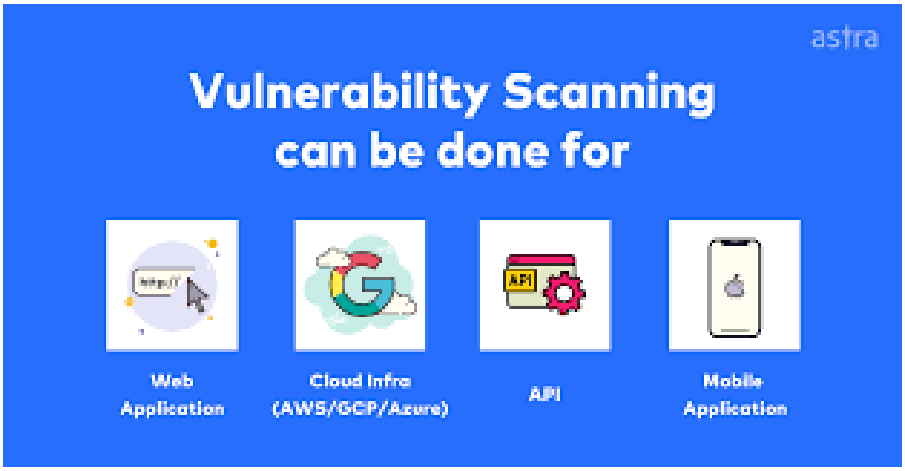
Gambar 1. 16 Vulnerability Scanning

Sumber : https://www.balbix.com/insights/what-is-vulnerability-scanning/

Proses vulnerability scanning bisa dilakukan dalam berbagai jenis: scan eksternal (dari luar jaringan), scan internal (dari dalam jaringan), scan host, scan web aplikasi, serta scan konfigurasi. Setiap jenis memberi sudut pandang yang berbeda: scan eksternal mengidentifikasi apa yang tampak dari luar (exposed services), sedangkan scan internal mengungkapkan kelemahan dalam lingkungan tertutup, seperti sistem yang terlindung di balik firewall.

Intensitas, cakupan dan frekuensi scanning juga mempengaruhi efektivitasnya scan berkala membantu mendeteksi kelemahan baru yang muncul akibat pembaruan software, perubahan konfigurasi, atau update keamanan.(I.Mohaidat & Al-Helali, 2024)

Keunggulan vulnerability scanning termasuk kecepatan dalam mendeteksi masalah umum, efisiensi biaya karena banyak proses diotomatisasi dan kemudahan memperoleh gambaran general keamanan sebuah sistem. Namun scanner otomatis punya keterbatasan: sering gagal mendeteksi kelemahan logika aplikasi yang kompleks, false positives dan false negatives, atau celah yang hanya muncul di kondisi tertentu (misalnya setelah interaksi manusia atau data spesifik). Laporan scanning harus dianalisis dan terkadang dikombinasikan dengan metode pengujian lain seperti pentest untuk menguji exploitasi nyata.



Gambar 1. 17 Keunggulan Vulnerability Scanning

Sumber : https://www.getastra.com/blog/security-audit/vulnerability-scanning-process/

Keamanan organisasi, vulnerability scanning harus dilakukan secara terstruktur: setiap hasil scanning diperiksa, diprioritaskan berdasarkan risiko, lalu mitigasi dilaksanakan dan setelah itu dipantau ulang. Aspek dokumentasi, persetujuan ruang lingkup, otorisasi dan dampak operasional harus diperhatikan agar scanning tidak mengganggu layanan penting (I.Mohaidat & Al-Helali, 2024). Monitoring hasil perbaikan dan peninjauan berkala sangat

penting agar sistem tetap aman seiring perubahan teknologi, threat landscape dan kondisi operasional.

D. Etika Pentest

Etika dalam penetration testing merujuk pada seperangkat pedoman yang harus diikuti oleh profesional keamanan siber untuk memastikan bahwa pengujian dilakukan dengan cara yang sah, aman dan bertanggung jawab. Tujuan utama dari pentest adalah untuk menilai dan meningkatkan keamanan sistem informasi tanpa menyebabkan kerusakan atau pelanggaran terhadap privasi individu atau organisasi (Patel, 2024). Etika dalam pentest sangat penting untuk menjaga integritas profesi dan kepercayaan klien.

Gambar 1. 18 Etika Pentest

Sumber : https://www.getastra.com/blog/security-audit/penetration-testing/

Salah satu aspek utama dari etika pentest adalah mendapatkan izin eksplisit dari pemilik sistem sebelum melakukan pengujian. Tanpa izin yang jelas, tindakan tersebut dapat dianggap sebagai peretasan ilegal. Selain itu, penting untuk menetapkan ruang lingkup pengujian secara rinci, termasuk sistem, data dan metode yang akan digunakan, untuk menghindari pelanggaran terhadap data atau sistem yang tidak terkait. Kejelasan ini juga membantu dalam mengelola ekspektasi klien dan meminimalkan risiko.(Lo Giudice & Ghafir, 2024)

Selama proses pengujian, profesional pentest harus menghormati privasi dan kerahasiaan data yang diakses. Informasi sensitif yang ditemukan selama pengujian harus dijaga kerahasiaannya dan hanya dibagikan dengan pihak yang berwenang. Pengujian harus dilakukan dengan cara yang tidak merusak sistem atau data, memastikan bahwa operasi normal tidak terganggu dan tidak ada data yang hilang atau rusak.(Wang, 2022)

Gambar 1. 19 Etika Pentest 1

Sumber : https://www.getastra.com/blog/security-audit/third-party-penetration-testing/

Setelah pengujian selesai, hasilnya harus disampaikan dalam laporan yang jelas dan objektif, mencakup temuan, potensi risiko dan rekomendasi perbaikan. Laporan ini harus disusun dengan bahasa yang mudah dipahami oleh pihak non-teknis, seperti manajemen, untuk memastikan bahwa rekomendasi dapat diimplementasikan dengan efektif.(Lo Giudice & Ghafir, 2024)

Profesional pentest harus terus memperbarui pengetahuan dan keterampilan mereka untuk mengikuti perkembangan terbaru dalam teknologi dan ancaman siber. Prinsip Etika dalam Pentest sebagai berikut :

1. Izin eksplisit: Mendapatkan persetujuan tertulis dari pemilik sistem sebelum melakukan pengujian.

2. Ruang lingkup yang jelas: Menetapkan batasan pengujian untuk menghindari akses ke sistem atau data yang tidak sah.
3. Kerahasiaan data: Menjaga informasi sensitif yang ditemukan selama pengujian agar tidak jatuh ke tangan yang salah.
4. Non-destruktif: Melakukan pengujian tanpa menyebabkan kerusakan atau gangguan pada sistem atau data.
5. Laporan yang objektif: Menyusun laporan yang akurat dan tidak bias mengenai temuan dan rekomendasi.
6. Pembaruan pengetahuan: Terus belajar dan beradaptasi dengan perkembangan terbaru dalam keamanan siber.

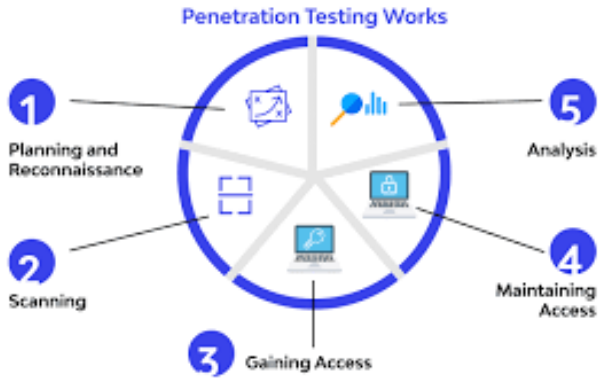
E. Aspek Hukum Pentest

Penetration testing (pentest) adalah metode untuk mengidentifikasi kerentanan dalam sistem informasi dengan tujuan meningkatkan keamanan. Aktivitas ini harus dilaksanakan dengan izin tertulis dari pemilik sistem agar legal dan sah secara hukum. Tanpa izin, pentest dapat dikategorikan sebagai akses ilegal yang melanggar Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan perubahannya melalui UU Nomor 27 Tahun 2022. Persetujuan resmi menjadi landasan hukum agar pengujian dapat dilakukan tanpa risiko konsekuensi pidana atau perdata.

Dasar hukum pentest menegaskan bahwa setiap akses sistem elektronik tanpa izin, meskipun bertujuan pengujian keamanan, dapat dianggap sebagai tindakan melanggar hukum. Pasal 30 UU ITE secara spesifik melarang akses tanpa otorisasi, sehingga pentester harus memahami batasan legal sebelum melakukan pengujian. Kepatuhan terhadap regulasi ini menjadi syarat mutlak agar aktivitas pentest tetap diakui secara profesional dan etis.

Selain aspek izin, pentester juga bertanggung jawab secara etis dan hukum untuk menjaga integritas, kerahasiaan dan ketersediaan data yang diakses. Semua temuan harus didokumentasikan dan dilaporkan kepada

pemilik sistem, tanpa memanfaatkan kelemahan untuk tujuan pribadi atau merusak sistem. Etika profesi mengatur bahwa tujuan pentest adalah memperkuat keamanan, bukan menimbulkan risiko baru atau kerugian bagi organisasi.



Gambar 1. 20 Penetration Testing

https://www.wowrack.com/id-id/blog/compliance-id/apa-itu-penetration-testing-dan-manfaat-untuk-perusahaan/

1. Legalitas Penetration Testing di Indonesia

   Penetration testing adalah metode yang sah dan penting dalam mengidentifikasi kerentanan sistem informasi. Namun, untuk memastikan legalitasnya, pengujian ini harus dilakukan dengan izin tertulis dari pemilik sistem yang diuji. Tanpa izin tersebut, aktivitas pentest dapat dianggap sebagai akses ilegal dan melanggar hukum.Penting bagi pentester untuk memperoleh persetujuan resmi sebelum melaksanakan pengujian.(Tabitha Fransisca Romauli Nababan & Shevanna Putri Cantiqa, 2024)

2. Dasar Hukum Penetration Testing

   Dasar hukum yang mengatur aktivitas pentest di Indonesia adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang telah diperbarui dengan UU Nomor 27 Tahun 2022. Pasal 30 UU ITE mengatur tentang larangan akses sistem elektronik tanpa izin, yang mencakup aktivitas pentest tanpa persetujuan.

Penting bagi pentester untuk memahami dan mematuhi ketentuan hukum yang berlaku.(Rusman & Kamaludin, 2024)

3. Tanggung Jawab dan Etika Pentester

   Pentester memiliki tanggung jawab untuk menjaga integritas dan kerahasiaan data yang diakses selama pengujian. Mereka harus menjalankan tugasnya sesuai dengan etika profesi, yaitu dengan tujuan untuk meningkatkan keamanan sistem, bukan untuk merusak atau mengeksploitasi kelemahan yang ditemukan. Dokumentasi yang jelas dan laporan yang transparan kepada pemilik sistem juga merupakan bagian dari tanggung jawab profesional pentester.(Gani, 2024)

Pelaksanaan pentest yang sesuai hukum juga mendorong organisasi untuk menyusun perjanjian formal dengan pihak penguji. Perjanjian ini mencakup lingkup pengujian, metode yang digunakan, batasan aktivitas, serta mekanisme pertanggungjawaban jika terjadi insiden. Dengan pendekatan ini, pengujian keamanan dapat dijalankan secara profesional, transparan dan memberikan manfaat nyata bagi perlindungan aset informasi organisasi.

F. Batasan Pengujian Sistem

Pengujian penetrasi (penetration testing) merupakan metode yang sah dan penting dalam mengidentifikasi kerentanan sistem informasi. Untuk memastikan legalitasnya, pengujian ini harus dilakukan dengan izin tertulis dari pemilik sistem yang diuji.

Gambar 1. 21 Batasan Pengujian Sistem

Sumber : https://www.compassitc.com/blog/penetration-testing-phases-steps-in-the-process

Tanpa izin tersebut, aktivitas pentest dapat dianggap sebagai akses ilegal dan melanggar hukum. Penting bagi pentester untuk memperoleh persetujuan resmi sebelum melaksanakan pengujian.(Rhogust & Sekayu, 2024)

1. Dasar Hukum Penetration Testing

   Dasar hukum yang mengatur aktivitas pentest di Indonesia adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang telah diperbarui dengan UU Nomor 27 Tahun 2022. Pasal 30 UU ITE mengatur tentang larangan akses sistem elektronik tanpa izin, yang mencakup aktivitas pentest tanpa persetujuan. Penting bagi pentester untuk memahami dan mematuhi ketentuan hukum yang berlaku.
2. Tanggung Jawab dan Etika Pentester

   Pentester memiliki tanggung jawab untuk menjaga integritas dan kerahasiaan data yang diakses selama pengujian. Mereka harus menjalankan tugasnya sesuai dengan etika profesi, yaitu dengan tujuan untuk meningkatkan keamanan sistem, bukan untuk merusak atau mengeksploitasi kelemahan yang ditemukan. Dokumentasi yang jelas dan laporan yang transparan kepada pemilik sistem juga merupakan bagian dari tanggung jawab profesional pentester.(Tobondo et al., 2024)

G. Metode Mitigasi Temuan

Setelah melakukan penetration testing, langkah selanjutnya adalah mitigasi terhadap temuan yang ditemukan. Mitigasi ini bertujuan untuk mengurangi atau menghilangkan risiko yang ditimbulkan oleh kerentanan yang teridentifikasi.

Beberapa metode mitigasi yang umum diterapkan antara lain:

1. Penerapan Patch dan Pembaruan Sistem

Melakukan pembaruan perangkat lunak dan sistem operasi untuk menutup celah keamanan yang ditemukan. Penerapan patch secara rutin dapat mencegah eksploitasi oleh pihak yang tidak bertanggung jawab.

2. Penguatan Konfigurasi Sistem

   Mengubah konfigurasi sistem agar lebih aman, seperti menonaktifkan layanan yang tidak diperlukan, mengubah pengaturan default dan membatasi akses hanya kepada pengguna yang berwenang.

3. Implementasi Kontrol Akses yang Ketat

   Menerapkan kebijakan kontrol akses berbasis peran (role-based access control/RBAC) untuk memastikan bahwa pengguna hanya memiliki akses sesuai dengan kebutuhan tugas mereka.

4. Penerapan Keamanan Jaringan

   Menggunakan firewall, sistem deteksi dan pencegahan intrusi (IDS/IPS), serta enkripsi untuk melindungi data yang ditransmisikan melalui jaringan.

5. Pelatihan dan Kesadaran Pengguna

   Memberikan pelatihan kepada pengguna mengenai praktik keamanan terbaik dan meningkatkan kesadaran mereka terhadap potensi ancaman.

H. Evaluasi & Tindak Lanjut

Setelah melakukan penetration testing, evaluasi terhadap temuan yang diperoleh sangat penting untuk menentukan tingkat keparahan dan prioritas penanganannya. Metode yang umum digunakan dalam evaluasi ini adalah Risk Assessment Matrix, yang mengklasifikasikan temuan berdasarkan dampak dan kemungkinan terjadinya. Temuan dengan dampak tinggi dan kemungkinan besar harus menjadi prioritas utama untuk ditindaklanjuti.(Sholawati et al., 2024)

1. Tindak Lanjut dan Mitigasi

Tindak lanjut terhadap temuan meliputi langkah-langkah mitigasi untuk mengurangi atau menghilangkan risiko yang ditimbulkan. Langkah-langkah tersebut antara lain:

a) Penerapan Patch dan Pembaruan Sistem: Melakukan pembaruan perangkat lunak dan sistem operasi untuk menutup celah keamanan yang ditemukan.

b) Penguatan Konfigurasi Sistem: Mengubah konfigurasi sistem agar lebih aman, seperti menonaktifkan layanan yang tidak diperlukan dan mengubah pengaturan default.

c) Implementasi Kontrol Akses yang Ketat: Menerapkan kebijakan kontrol akses berbasis peran (RBAC) untuk memastikan bahwa pengguna hanya memiliki akses sesuai dengan kebutuhan tugas mereka.

d) Penerapan Keamanan Jaringan: Menggunakan firewall, sistem deteksi dan pencegahan intrusi (IDS/IPS), serta enkripsi untuk melindungi data yang ditransmisikan melalui jaringan.

e) Pelatihan dan Kesadaran Pengguna: Memberikan pelatihan kepada pengguna mengenai praktik keamanan terbaik dan meningkatkan kesadaran mereka terhadap potensi ancaman.

2. Verifikasi dan Pengujian Ulang

Setelah langkah mitigasi diterapkan, penting untuk melakukan verifikasi dan pengujian ulang untuk memastikan bahwa celah keamanan telah tertutup dan tidak ada kerentanan baru yang muncul. Metode yang digunakan dalam pengujian ulang ini adalah Regression Testing, yang memastikan bahwa perubahan yang dilakukan tidak mempengaruhi fungsionalitas sistem secara keseluruhan.(Rhogust & Sekayu, 2024)

3. Dokumentasi dan Pelaporan

Seluruh proses evaluasi, tindak lanjut dan pengujian ulang harus didokumentasikan dengan baik. Dokumentasi ini mencakup laporan

temuan, langkah-langkah mitigasi yang diambil, hasil pengujian ulang, serta rekomendasi untuk perbaikan lebih lanjut. Dokumentasi yang baik akan menjadi referensi penting untuk audit keamanan di masa depan dan membantu dalam perencanaan strategi keamanan jangka panjang.

DAFTAR PUSTAKA

AL-Dosari, K., & Fetais, N. (2023). Risk-Management Framework and Information-Security Systems for Small and Medium Enterprises (SMEs): A Meta-Analysis Approach. *Electronics (Switzerland)*, *12*(17). https://doi.org/10.3390/electronics12173629

Alraja, M. N., Butt, U. J., & Abbod, M. (2023a). Information security policies compliance in a global setting: An employee's perspective. *Computers and Security*, *129*, 103208. https://doi.org/10.1016/j.cose.2023.103208

Alraja, M. N., Butt, U. J., & Abbod, M. (2023b). Information security policies compliance in a global setting: An employee's perspective. *Computers and Security*, *129*(April), 103208. https://doi.org/10.1016/j.cose.2023.103208

Andersson, J., & Seid, E. (2024). The Classification and Impact of Cyber Attacks Targeting Critical Service Providers. *International Conference on Information Systems Security and Privacy*, *1*(Icissp), 137–145. https://doi.org/10.5220/0012374500003648

Apriany, A., & Wibowo, A. (2024). Analysis of the Implementation of ISO 27001: 2022 and KAMI Index in Enhancing the Information Security Management System in Consulting Firms. *IJCCS (Indonesian Journal of Computing and Cybernetics Systems)*, *18*(4), 417–428. https://doi.org/10.22146/ijccs.100385

Bennouk, K., Ait Aali, N., El Bouzekri El Idrissi, Y., Sebai, B., Faroukhi, A. Z., & Mahouachi, D. (2024). A Comprehensive Review and Assessment of Cybersecurity Vulnerability Detection Methodologies. *Journal of Cybersecurity and Privacy*, *4*(4), 853–908. https://doi.org/10.3390/jcp4040040

Di Nocera, F., Tempestini, G., & Orsini, M. (2023). Usable Security: A Systematic Literature Review. *Information (Switzerland)*, *14*(12). https://doi.org/10.3390/info14120641

Ezeagwu, E., Ndubuisi Nnamani, K., Tochukwu Onyia, C., Alagbu, E. E., & Author, C. (2021). Comparative Analysis of OSI and TCP/IP Models in Network Communication. *Quest Journals Journal of Software Engineering and Simulation*, *7*(6), 2321–3809. www.questjournals.org

Fajri, K. S. Al, & Harwahyu, R. (2024). Information Security Management System Assessment Model by Integrating ISO 27002 and 27004. *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, *4*(2), 498–506. https://doi.org/10.57152/malcom.v4i2.1245

Franken, J., & Reuter, C. (2024). *Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure*. 279–301. https://doi.org/10.1007/978-3-658-44810-3_13

Gani, N. (2024). Legal Politics and Data Protection in Indonesia: A Case Study of the National Data Center Hacking. *Sasi*, *30*(3), 296. https://doi.org/10.47268/sasi.v30i3.2213

Górka–Chowaniec, A., & Popek, A. (2025). Attempt To Use the Deming Cycle (Pdca) in the Process of Implementing an Information Security Management System. *International Journal for Quality Research*, *19*(2), 371–386. https://doi.org/10.24874/IJQR19.02-01

I.Mohaidat, A., & Al-Helali, D. A. (2024). Web Vulnerability Scanning Tools: A Comprehensive Overview, Selection Guidance, and Cyber Security Recommendations. *International Journal of Research Studies in Computer Science and Engineering*, *10*(1), 8–15. https://doi.org/10.20431/2349-4859.1001002

Intan Mafiana, A., Hanum, L., Ilmi, H. M., & Febriliani, S. (2023). Implementasi Manajemen Keamanan Informasi Berbasis Iso 27001 Pada Sistem Informasi Akademik. *Journal of Digital Business and Innovation Management*, *2*(2), 139–163. https://doi.org/10.26740/jdbim.v2i2.57580

James, L. (2021). *Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis By Liu Hua Yeo, MS, and James Banfield, PhD*.

Jevelin, J., & Faza, A. (2023). Evaluation the Information Security Management System: A Path Towards ISO 27001 Certification. *Journal of Information Systems and Informatics*, *5*(4), 1240–1256. https://doi.org/10.51519/journalisi.v5i4.572

Lo Giudice, F. G., & Ghafir, I. (2024). Firewalls: Types, Policies, Security Issues and Best Practices. *SSRN Electronic Journal*, *February*. https://doi.org/10.2139/ssrn.4709034

Magnusson, L., Iqbal, S., Elm, P., & Dalipi, F. (2025). Information security governance in the public sector: investigations, approaches, measures, and trends. *International Journal of Information Security*, *24*(4). https://doi.org/10.1007/s10207-025-01097-x

Melaku, H. M. (2023). A Dynamic and Adaptive Cybersecurity Governance Framework. *Journal of Cybersecurity and Privacy*, *3*(3), 327–350. https://doi.org/10.3390/jcp3030017

Mishra, S. (2023). Principles of organizational security governance. *Issues in Information Systems*, *24*(3), 116–131. https://doi.org/10.48009/3_iis_2023_111

Nagata, K. (2024). *Establishing Information Security Policy as an Organizational Risk Management*. https://doi.org/10.5772/intechopen.1004563

Nieles, M. (2017). An introduction to information security evaluation. *Journal of Information Processing and Management*, *48*(6), 320–332. https://doi.org/10.1241/johokanri.48.320

Patel, U. (2024). Based on Google Scholar Citation) Cite this Article: Udit Patel, The Role of Next-Generation Firewalls in Modern Network Security: A Comprehensive Analysis. *International Journal of Advanced Research in Engineering and Technology (IJARET)*, *15*(4), 135–154. https://iaeme.com/MasterAdmin/Journal_uploads/IJARET/VOLUME_15_ISSUE_4/IJARET_15_04_012.pdf

PROTHRO, J. B. (2022). The Importance and Challenges of Paul. *The Apostle Paul*

and His Letters, 1–10. https://doi.org/10.2307/j.ctv289dp17.6

Rhogust, M., & Sekayu, I. R. (2024). Legal Framework for Cybersecurity in the Digital Economy: Challenges and Prospects for Indonesia. *Social Science*, *1*(2), 166–180. https://myjournal.or.id/index.php/JLSSH

Rusman, R., & Kamaludin, A. (2024). Investigation of Cyber Crime in the Indonesian Legal Framework. *Journal La Sociale*, *5*(6), 1576–1586. https://doi.org/10.37899/journal-la-sociale.v5i6.1367

Saide, M. (2024). *Exploring the TCP / IP Protocol Suite : Architecture , Dominance , and Future Challenges in Data Communication International Open University Department of Information Technology Exploring the TCP / IP Protocol Suite : Architecture , Dominance , and Future*. *August*. https://doi.org/10.2139/ssrn.4885418

Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. *International Cybersecurity Law Review*, *3*(1), 7–34. https://doi.org/10.1365/s43439-021-00045-4

Sevgi. (2021). Governing Information Security In Conjunction With Cobit And Iso 27001. *International Journal of Network Security & Its Applications*, *3*(4), 111–116. https://doi.org/10.5121/ijnsa.2011.3410

Sholawati, A., Setyadi, H. J., & Masa, A. P. A. (2024). Implementasi Penetration Testing Pada Sistem Informasi Terpadu Layanan Prodi Menggunakan Framework Issaf. *Techno (Jurnal Fakultas Teknik, Universitas Muhammadiyah Purwokerto)*, *25*(2), 73. https://doi.org/10.30595/techno.v25i2.21140

Subhangani, F. A., & Chaudhary, S. B. A. (2020). *Vulnerability Scanning System Diagram*. www.nessus.org.

Tabitha Fransisca Romauli Nababan, & Shevanna Putri Cantiqa. (2024). Mengoptimalkan Implementasi UU No. 27 Tahun 2022 Dengan Penetration Test Dan Vulnerability Assessment Pada Kasus Pembobolan Data Aplikasi

Dana. *Jurnal Hukum, Politik Dan Ilmu Sosial*, *3*(3), 155–161. https://doi.org/10.55606/jhpis.v3i3.3900

Tobondo, Y. A., Juliana, S. F., Ruagadi, H. A., Tondowala, S. F. H., & Ngguna, Y. (2024). Analysis of Cybersecurity Implementation in Indonesia Based on the Framework of Administrative Law. *Interdisciplinary Journal (IDe)*, *2*(2), 83–94. https://doi.org/10.61254/idejournal.v2i2.55

Tyagi, A. (2020). TCP/IP Protocol Suite. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *July 2020*, 59–71. https://doi.org/10.32628/cseit206420

Wang, P. (2022). Research on firewall technology and its application in computer network security strategy. *Frontiers in Computing and Intelligent Systems*, *2*(2), 42–46. https://doi.org/10.54097/fcis.v2i2.3931