

IKI – 83408T
Proteksi dan Teknik Keamanan
Sistem Informasi

Topik: Operations Security

Kelompok 6:

Pranarendra Wibowo (7204000322)

Timor Setyaningsih (7204000381)

Program Magister Teknologi Informasi
Fakultas Ilmu Komputer
Universitas Indonesia

Daftar Isi

1. Pendahuluan
 - 1.1 Tujuan
 - 1.2 Definisi Domain
 - 1.2.1 Tiga Hal Utama
 - 1.2.2 C.I.A.
2. Kontrol dan Proteksi (Controls and Protections)
 - 2.1 Kontrol berdasarkan Kategori (Categories of Controls)
 - 2.2 Kontrol berdasarkan Orange Book (Orange Book Controls)
 - 2.2.1 Covert Channel Analysis
 - 2.2.2 Trusted Facility Management
 - 2.2.3 Trusted Recovery
 - 2.2.4 Configuration/Change Management Control
 - 2.3 Kontrol di tingkat Administratif (Administrative Controls)
 - 2.4 Kontrol di tingkat Operasi (Operations Controls)
 - 2.4.1 Pengamanan Sumberdaya (Resource Protection)
 - 2.4.2 Kontrol Perangkat Keras (Hardware Controls)
 - 2.4.3 Kontrol Perangkat Lunak (Software Controls)
 - 2.4.4 Kontrol Entitas-Kewenangan (Privileged-Entity Controls)
 - 2.4.5 Kontrol Media (Media Controls)
 - 2.4.6 Kontrol Terhadap Akses Fisik (Physical Access Controls)
3. Pengawasan dan Pengauditan (Monitoring and Auditing)
 - 3.1 Pengawasan (Monitoring)
 - 3.2 Pengauditan (Auditing)
 - 3.2.1 Audit Keamanan (Security Auditing)
 - 3.2.2 Jejak Audit (Audit Trails)
 - 3.2.3 Konsep Manajemen Masalah (Management Problem Concept)
4. Ancaman dan Kerawanan (Threats and Vulnerabilities)
 - 4.1 Ancaman (Threats)
 - 4.2 Kerawanan (Vulnerabilities)
5. Penutup
 - 5.1 Kesimpulan
 - 5.2 Saran

Draft Penulisan

1. Pendahuluan

Pada domain Keamanan Operasi (Operations Security) akan dibahas mengenai kontrol-kontrol apa saja yang diperlukan pada lingkungan operasi yang berhubungan dengan komputasi. Hal-hal tersebut harus mencakup tiga pilar dari keamanan informasi yaitu Kerahasiaan (Confidentiality), Integritas (Integrity), dan Ketersediaan (Availability).

1.1 Tujuan

Pendekatan yang akan dilakukan meliputi:

1. Kontrol dan Proteksi (Controls and Protections)
2. Pengawasan dan Pengauditan (Monitoring and Auditing)
3. Ancaman dan Kerawanan (Threats and Vulnerabilities)

1.2 Definisi Domain

Keamanan Operasi bermakna suatu tindakan untuk mengerti hal-hal yang menjadi ancaman dan hal-hal yang menjadi kerawanan dari operasi-operasi komputer yang bertujuan untuk secara rutin mendukung aktivitas operasional dari suatu sistem komputer agar dapat berfungsi dengan benar.

1.2.1 Tiga Hal Utama

Seperti domain keamanan lain, Keamanan Operasi juga memperhatikan tiga hal utama yaitu:

1. Ancaman (Threat)
Ancaman dalam domain Keamanan Operasi dapat didefinisikan sebagai adanya kejadian potensial yang dapat menyebabkan kerusakan dengan cara melanggar keamanan.
2. Kerawanan (Vulnerability)
Kerawanan dalam domain ini dapat didefinisikan sebagai titik lemah dalam sebuah sistem yang dapat mengakibatkan terjadinya pelanggaran keamanan.
3. Aset (Asset)
Aset adalah apa saja yang diyakini sebagai sumberdaya komputasi atau kemampuan, seperti perangkat keras, perangkat lunak, data, dan juga sumberdaya manusia (personel).

1.2.2 C.I.A.

Beberapa hal ini adalah beberapa dampak dari kontrol operasi pada C.I.A.:

1. **Konfidensialitas (Confidentiality)**
Kontrol Operasi memberi dampak pada sensitivitas dan kerahasiaan dari informasi.
2. **Integritas (Integrity)**
Bagaimana kontrol operasi diterapkan akan secara langsung berdampak pada akurasi data dan keotentikan.

3. Ketersediaan (Availability)
Kontrol ini memberi dampak pada tingkatan penanggulangan kesalahan (fault tolerance) organisasi dan kemampuannya untuk kembali dari kegagalan tersebut.

2. Kontrol dan Proteksi (Controls and Protections)

Domain Keamanan Operasi memperhatikan kontrol-kontrol yang akan digunakan untuk melindungi perangkat keras, perangkat lunak, dan sumberdaya media lainnya dari hal-hal sebagai berikut:

- Ancaman di sebuah lingkungan operasi
- Pihak pelanggar internal ataupun eksternal
- Operator yang tidak secara benar mengakses sumberdaya

Selain itu juga akan dibahas mengenai aspek kritical dari kontrol operasi yaitu:

1. Pengamanan sumberdaya, meliputi kontrol perangkat keras
2. Kontrol entitas-kewenangan (privileged-entity)

2.1 Kontrol berdasarkan Kategori (Categories of Controls)

Berikut ini beberapa kategori kontrol yang utama:

1. Kontrol Pencegahan (Preventative Controls)
Kontrol Pencegahan adalah kontrol yang dirancang untuk mencapai dua hal yakni untuk merendahkan jumlah dan akibat dari kesalahan yang tidak disengaja yang memasuki sistem dan untuk mencegah penerobos yang tidak berhak dari mengakses sistem melalui internal atau eksternal. Contohnya, urutan form atau validasi data dan prosedur pemeriksaan untuk mencegah duplikasi.
2. Kontrol Penyidikan (Detective Controls)
Kontrol Penyidikan digunakan untuk mendeteksi sebuah kesalahan tepat pada saat terjadi. Tidak seperti kontrol pencegahan, kontrol ini berjalan setelah kejadian dan dapat digunakan untuk melacak transaksi yang tidak berhak dan selanjutnya dituntut, atau untuk mengurangi akibat dari kesalahan pada sistem dengan mengidentifikasinya secara cepat. Contohnya, jejak audit (audit trails).
3. Kontrol Koreksi (Corrective/Recovery Controls)
Kontrol Koreksi diterapkan untuk membantu mitigasi dampak dari kejadian kehilangan melalui prosedur recovery. Kontrol ini dapat digunakan untuk recover setelah kerusakan, seperti mengembalikan kembali data yang secara tidak diingini terhapus dari floppy disk.

Sedangkan berikut ini adalah beberapa kontrol tambahan:

1. Kontrol Pengarah (Deterrent/Directive Controls)
Kontrol Pengarah digunakan untuk mendorong compliance dengan kontrol eksternal, seperti regulatory compliance. Kontrol ini ditujukan untuk melengkapi kontrol lain, seperti kontrol pencegahan dan penyidikan.
2. Kontrol Aplikasi (Application Controls)
Kontrol Aplikasi adalah kontrol yang dirancang ke dalam aplikasi perangkat lunak untuk mengurangi dan mendeteksi ketidakbiasaan operasi perangkat lunak.
3. Kontrol Transaksi (Transaction Controls)
Kontrol Transaksi digunakan untuk menyediakan kontrol pada berbagai tahapan peristiwa transaksi – dimulai dari inisiasi sampai output melalui kontrol pengujian dan perubahan.

Ada beberapa tipe Kontrol Transaksi:

- a. Kontrol Input (Input Controls)
Kontrol Input digunakan untuk memastikan bahwa transaksi-transaksi yang dilakukan, secara benar masuk ke dalam sistem satu kali saja. Unsur dari kontrol ini meliputi penghitungan data dan pemberian tanda waktu/tanggal data tersebut dimasukkan atau diubah.
- b. Kontrol Pemrosesan (Processing Controls)
Kontrol Pemrosesan digunakan untuk menjamin bahwa transaksi-transaksi yang dilakukan adalah valid dan akurat serta masukan-masukan yang salah diproses ulang secara benar dan diketahui.
- c. Kontrol Output (Output Controls)
Kontrol Output digunakan untuk dua hal yakni untuk melindungi kerahasiaan dari output dan untuk memverifikasi integritas dari output dengan cara membandingkan transaksi input dan data output.
- d. Kontrol Perubahan (Change Controls)
Kontrol Perubahan diimplementasikan untuk melindungi integritas data dalam sebuah sistem pada saat perubahan dilakukan terhadap konfigurasi. Prosedur dan standar akan diterapkan untuk mengelola perubahan tersebut dan modifikasi pada sistem dan konfigurasinya.
- e. Kontrol Uji (Test Controls)
Kontrol Uji dilaksanakan pada saat pengujian sebuah sistem untuk menghindari pelanggaran kerahasiaan dan untuk menjamin bahwa integritas transaksi.

2.2 Kontrol berdasarkan Orange Book (Orange Book Controls)

Trusted Computer Security Evaluation Criteria (TCSEC, Orange Book) mendefinisikan beberapa tingkat dari jaminan kebutuhan akan operasi komputer yang aman. Orange Book mendefinisikan dua tipe jaminan, yakni:

1. Operational Assurance, meliputi:
 - a. System Architecture
 - b. System Integrity
 - c. Covert Channel Analysis
 - d. Trusted Facility Management
 - e. Trusted Recovery
2. Life Cycle Assurance, meliputi:
 - a. Security Testing
 - b. Design Specification and Testing
 - c. Configuration Management
 - d. Trusted Distribution

Pada domain Kontrol Operasi, Operational Assurance meliputi Covert Channel Analysis, Trusted Facility Management, dan Trusted Recovery. Sedangkan Life Cycle Assurance meliputi Configuration Management.

2.2.1 Covert Channel Analysis

Covert channel adalah jalur informasi yang tidak normal digunakan untuk berkomunikasi dengan sistem; sehingga, jalur tersebut tidak dilindungi oleh

mekanisme keamanan normal sistem. Covert channel adalah cara rahasia untuk mengalihkan informasi ke orang atau program lain.

Ada dua tipe Covert channel:

1. Covert storage channels
Covert storage channels mengalihkan informasi dengan cara mengubah data tersimpan sistem. Contohnya, sebuah program dapat mengalihkan informasi ke program yang kurang-aman dengan cara mengubah jumlah atau pola free space dari sebuah hard disk.
2. Covert timing channels
Covert timing channels mengalihkan informasi dengan cara menghilangkan performa dari atau memodifikasi pewaktuan (timing) dari sumberdaya sistem dengan cara tertentu. Timing channels seringkali berhasil dengan mengambil keuntungan dari suatu clock sistem atau alat timing pada sistem. Informasi dialihkan dengan menggunakan unsur seperti elapsed time yang diperlukan untuk menjalankan suatu operasi, jumlah CPU time yang dihabiskan, atau waktu berjalannya antara dua kejadian.

2.2.2 Trusted Facility Management

Trusted Facility Management didefinisikan sebagai penugasan individu spesifik untuk melakukan administrasi fungsi-fungsi yang berhubungan dengan keamanan pada sebuah sistem. Trusted Facility Management erat hubungannya dengan konsep kewenangan terbatas (least privilege), dan juga dengan konsep administrasi pemisahan tugas (separation of duties) dan apa yang perlu diketahui (need to know). Adapun penjelasannya sebagai berikut:

1. Pemisahan Tugas (Separation of Duties)
Pemisahan Tugas dilaksanakan dengan cara menugaskan bagian-bagian dari suatu pekerjaan ke beberapa personel. Sehingga jika tidak ada satu orang yang memiliki kontrol total akan mekanisme keamanan suatu sistem, maka secara teori tidak akan ada satu orang yang juga dapat menggagalkan sistem.
2. Perotasian Tugas (Rotation of Duties)
Variasi lain dari pemisahan tugas adalah disebut dengan perotasian tugas. Didefinisikan sebagai proses pembatasan jumlah waktu yang diberikan pada seorang operator dalam melaksanakan suatu tugas berhubungan dengan keamanan sebelum selanjutnya dipindahkan ke tugas lain dengan klasifikasi keamanan yang berbeda pula. Kontrol ini mengurangi kesempatan berbuat kolusi diantara operator-operator pada fungsi-fungsi yang memungkinkan.

2.2.3 Trusted Recovery

Trusted Recovery menjamin bahwa keamanan tidak diterobos ketika sistem mengalami crash atau kegagalan sistem lain (seringkali disebut dengan “discontinuity”). Menjamin bahwa sistem di start ulang tanpa meninggalkan prosedur pengamanan yang diperlukan dan dapat recover dan roll back tanpa terkompromi setelah kegagalan. Contohnya, jika sistem crash saat data sensitif sedang dituliskan ke disk (di mana normalnya terlindungi oleh suatu kontrol), data mungkin tertinggal tidak terlindungi di memori dan mungkin dapat diakses oleh personel yang tidak berhak.

Trusted Recovery memiliki dua kegiatan utama:

1. Persiapan Kegagalan (Failure Preparation)
Persiapan Kegagalan yang dilakukan menghadapi suatu kegagalan sistem meliputi melakukan back up semua file yang kritikal secara teratur. Persiapan ini harus mencakup data recovery dalam cara yang terlindungi disamping juga menjamin keberlangsungan keamanan pada sistem. Prosedur-prosedur ini juga diperlukan apabila terjadi masalah dalam sistem seperti hilangnya sumberdaya, basisdata yang tidak konsisten, atau pelanggaran apa pun, yang terdeteksi, atau jika sistem memerlukan untuk dimatikan atau start ulang.
2. Pengembalian Sistem (System Recovery)
Jika prosedur-prosedur yang spesifik dari Trust Recovery bergantung secara langsung pada kebutuhan sistem, maka secara umum, prosedur Pengembalian Sistem meliputi hal-hal berikut:
 - a. Boot ulang sistem ke single user mode – sistem operasi dijalankan tanpa aktivasi sisi pengamanan muka – sehingga tidak ada user lain yang dapat mengakses sistem pada saat itu.
 - b. Recover semua sistem file yang aktif pada saat terjadinya kegagalan sisten
 - c. Restore semua file dan basisdata yang hilang atau rusak dari simpanan backup yang terbaru.
 - d. Recover semua karakteristik keamanan yang diperlukan, seperti label-label keamanan file.
 - e. Memeriksa semua file yang kritikal akan keamanan, seperti file password.

Setelah semua langkah tersebut dilakukan dan data sistem tidak dapat disalahgunakan, operator dapat kembali mengakses sistem.

Sebagai tambahan, Common Criteria juga mendeskripsikan tiga tipe hierarchical recovery yaitu:

1. Manual Recovery
Campur tangan administrator sistem diperlukan untuk mengembalikan sistem ke kondisi keamanan setelah sistem crash.
2. Automated Recovery
Recovery ke kondisi keamanan secara otomatis (tanpa campur tangan administrator sistem) ketika menangani satu kegagalan; namun, penanganan secara manual diperlukan untuk menangani beberapa kegagalan lainnya.
3. Automated Recovery without Undue Loss
Memiliki kemiripan dengan Automated Recovery, tipe recovery ini dikenal sebagai recovery tingkat tinggi karena mendefinisikan pencegahan terhadap undue loss dari objek-objek yang dilindungi.

2.2.4 Configuration/Change Management Control

Manajemen konfigurasi adalah proses pelacakan dan penyetujuan perubahan pada sebuah sistem. Meliputi pengidentifikasian, pengontrolan, dan pengauditan semua perubahan yang dilakukan terhadap sistem tersebut. Hal-hal yang terjadi dapat mencakup perubahan perangkat keras dan perangkat lunak, perubahan jaringan, atau perubahan lain yang memberi dampak pada keamanan. Manajemen konfigurasi juga dapat digunakan untuk melindungi sistem terpercaya pada saat dalam perancangan dan pengembangan.

Berikut ini adalah fungsi-fungsi utama kontrol konfigurasi atau perubahan:

- Untuk menjamin bahwa perubahan diterapkan dengan urutan cara yang benar dan telah melalui tahap pengujian formal
- Untuk menjamin bahwa pengguna dasar diinformasikan akan perubahan yang tertunda
- Untuk menganalisa akan dampak dari perubahan pada sistem setelah dilakukan implementasi
- Untuk mengurangi dampak negatif yang mungkin ditemukan pada suatu perubahan terutama pada layanan dan sumberdaya komputasi.

Lima prosedur umum yang ada dan dapat diterima untuk menerapkan dan mendukung proses kontrol perubahan:

1. Melakukan pengenalan perubahan
2. Mengkatalogkan perubahan yang ingin dilakukan
3. Menjadwalkan perubahan
4. Menerapkan perubahan
5. Melaporkan perubahan tersebut ke pihak yang berkepentingan

2.3 Kontrol di tingkat Administratif (Administrative Controls)

Kontrol di tingkat Administratif ini dapat didefinisikan sebagai kontrol yang dicanangkan dan dipelihara oleh pihak manajemen administratif untuk mengurangi ancaman atau dampak dari pelanggaran keamanan komputer. Kontrol ini terpisahkan dari kontrol operasi karena memiliki hubungan lebih banyak dengan administrasi personel sumberdaya manusia dan kebijakan (policy) dibandingkan dengan kontrol perangkat keras atau perangkat lunak.

Beberapa hal berikut adalah contoh dari kontrol administratif:

1. Keamanan Personel (Personnel Security)
Kontrol ini adalah kontrol sumberdaya manusia administratif yang digunakan untuk mendukung jaminan dari tingkat kualitas dari personel yang melakukan operasi-operasi komputer. Unsur-unsur dari kontrol ini meliputi:
 - a. Penyeleksian penerimaan pegawai atau pemeriksaan latar belakang
Penyeleksian pra-penerimaan untuk posisi-posisi yang sensitif layaknya dilakukan. Sedangkan untuk posisi yang kurang sensitif, pemeriksaan latar belakang pasca-penerimaan kiranya lebih layak dilakukan.
 - b. Libur yang wajib diambil dalam periode waktu satu minggu
Praktek ini adalah umum digunakan di institusi keuangan atau organisasi lain dimana operator memiliki akses ke transaksi finansial yang sensitif. Selama operator tersebut mengambil libur, dilakukan audit pada akun, proses, dan prosedur operator untuk mengungkapkan apabila ada bukti pelanggaran.
 - c. Peringatan kerja atau pemberhentian
Langkah ini diambil apabila pegawai melanggar standar kebiasaan komputer yang telah ditetapkan.
2. Pemisahan Tugas dan Tanggungjawab (Separation of Duties and Responsibilities)
Pemisahan Tugas dan Tanggungjawab adalah konsep dengan cara menugaskan bagian-bagian dari pekerjaan yang sensitif akan keamanan ke beberapa individu.
3. Kewenangan Terbatas (Least Privilege)
Kewenangan Terbatas memerlukan bahwa setiap subjek diberi set kewenangan terbatas yang diperlukan untuk melakukan tugas mereka. Apabila memungkinkan

diperlukan adanya pemisahan tingkat akses berdasarkan fungsi pekerjaan operator. Pendekatan yang efektif adalah pemberian kewenangan yang terbatas. Sebuah contoh penerapan kewenangan terbatas antara lain yakni konsep dari operator komputer yang tidak diperbolehkan mengakses sumberdaya komputer lain di tingkat yang melampaui apa yang dibutuhkan oleh tugas spesifik mereka. Pada contoh ini operator diorganisasikan ke dalam kelompok-kelompok tingkat-kewenangan (privilege-level). Setiap kelompok kemudian diberikan tingkat kewenangan paling terbatas yang mungkin diaplikasikan.

Tiga tingkat dasar dari kewenangan didefinisikan sebagai berikut:

- a. **Read Only**
Adalah tingkat paling bawah dari kewenangan dan juga merupakan satu kewenangan yang akan diberikan ke hampir semua operator. Operator diperbolehkan untuk melihat data tapi tidak diperbolehkan untuk menambahkan, menghapus, atau melakukan perubahan pada salinan asli dari data tersebut.
 - b. **Read/Write**
Adalah tingkat yang memungkinkan operator untuk membaca, menambahkan, atau menulis pada data apa saja yang memiliki otoritas bagi mereka. Operator biasanya hanya memiliki akses read/write akan data yang disalin dari tempat asalnya, mereka tidak dapat mengakses data asal/original.
 - c. **Access Change**
Adalah tingkat tertinggi yang memberikan operator hak untuk dapat memodifikasi data secara langsung ke tempat asal data tersebut, sebagai tambahan dari data yang disalin dari lokasi asalnya. Operator sebaiknya memiliki kewenangan untuk mengubah file dan hak akses operator di sistem (hak supervisor).
4. **Yang Perlu Diketahui (Need to Know)**
Yang Perlu Diketahui memiliki makna sebagai suatu akses ke, pengetahuan akan, atau kepemilikan dari informasi spesifik yang diperlukan untuk melakukan fungsi tugas tertentu. Akan memerlukan bahwa subjek tertentu diberikan informasi yang diperlukan saja untuk dapat melakukan suatu pekerjaan.
 5. **Kontrol Manajemen Perubahan/Konfigurasi (Change/Configuration Management Controls)**
Fungsi dari kontrol ini adalah untuk melindungi sistem dari masalah dan kesalahan yang dapat menyebabkan dijalankan secara tidak baik, atau untuk mengujicoba suatu perubahan di dalam sebuah sistem.
 6. **Pemeliharaan Rekaman dan Dokumentasi (Record Retention and Documentation)**
Administrasi dari kontrol keamanan pada dokumentasi dan prosedur-prosedur yang diterapkan untuk record retention memiliki dampak pada keamanan operasional.
 - a. **Data Remanence**
Memiliki makna suatu data yang tertinggal di media setelah media tersebut dihapus. Setelah penghapusan, dapat saja ada beberapa jejak fisik tertinggal, yang dapat menyebabkan data dapat disusun ulang bersama informasi yang sensitif.
 - b. **Due Care and Due Diligence**
Konsep dari due care dan due diligence membutuhkan sebuah organisasi untuk menjalankan praktek bisnis yang baik relatif ke industri organisasi. Contoh dari Due Care adalah pelaksanaan pelatihan pegawai dalam hal

kesadaran akan keamanan, bukan melainkan menyusun kebijakan tanpa adanya implementasi rencana dan follow-up. Contoh dari Due Diligence adalah kebutuhan akan banyak hukum di industri organisasi atau melalui compliance dengan standar regulasi pemerintah.

c. Documentation

Sistem keamanan memerlukan kontrol dokumen. Dokumen dapat mencakup beberapa hal seperti rencana keamanan, rencana kontijensi, analisa resiko, dan kebijakan dan prosedur. Sebagian besar dari dokumentasi ini harus dilindungi dari pengaksesan tidak berhak, dan juga harus tersedia pada saat kejadian suatu bencana.

2.4 Kontrol di tingkat Operasi (Operations Controls)

Kontrol di tingkat Operasi mencakup prosedur yang digunakan dari hari ke hari untuk melindungi operasi-operasi yang berhubungan dengan komputer. Konsep yang dibahas meliputi pengamanan sumberdaya, kontrol perangkat keras dan perangkat lunak, dan entitas kewenangan (privileged entity).

Beberapa hal berikut merupakan aspek-aspek penting dalam kontrol operasi:

1. Pengamanan sumberdaya (Resource protection)
2. Kontrol perangkat keras (Hardware controls)
3. Kontrol perangkat lunak (Software controls)
4. Kontrol entitas-kewenangan (Privileged-entity controls)
5. Kontrol media (Media controls)
6. Kontrol terhadap akses fisik (Physical access controls)

2.4.1 Pengamanan Sumberdaya (Resource Protection)

Pengamanan sumberdaya adalah merupakan arti sesungguhnya – konsep melindungi sumberdaya dan aset komputasi organisasi dari kehilangan dan penyalahgunaan. Sumberdaya komputasi didefinisikan sebagai seluruh perangkat keras, perangkat lunak, atau data yang dimiliki dan digunakan oleh organisasi. Pengamanan sumberdaya dirancang untuk membantu mengurangi kemungkinan kerusakan yang dihasilkan dari penggunaan tidak sah dan/atau penghapusan data dengan cara membatasi kesempatan untuk penyalahgunaan ini.

Beberapa contoh sumberdaya yang memerlukan pengamanan:

1. Sumberdaya perangkat keras, meliputi:
 - Komunikasi: router, firewall, gateway, switch, modem, access server
 - Media penyimpanan: floppy, removable drive, hard drive eksternal, tape, cartridge
 - Sistem pemrosesan: file server, mail server, internet server, backup server, tape drive
 - Perangkat standalone: workstation, modem, disk, tape
 - Printer dan mesin faks
2. Sumberdaya perangkat lunak, meliputi:
 - Program library dan source code
 - Vendor perangkat lunak atau paket-paket proprietary
 - Perangkat lunak sistem operasi dan utiliti sistem

3. Sumberdaya data, meliputi:
 - Data backup
 - File-file data pengguna
 - File-file password
 - Direktori-direktori data operasi
 - Log sistem dan jejak audit

2.4.2 Kontrol Perangkat Keras (Hardware Controls)

Kontrol perangkat keras yang dilakukan meliputi:

1. Pemeliharaan perangkat keras
Pemeliharaan sistem memerlukan akses secara fisik atau logik ke dalam sistem melalui staf pendukung dan operasi, vendor-vendor, atau penyedia layanan. Pemeliharaan mungkin dapat dilakukan di tempat itu langsung, atau dapat juga ditransportasi ke tempat khusus perbaikan. Bahkan dapat juga dilakukan melalui jarak jauh. Lebih jauh lagi, penyidikan terhadap personel layanan juga layak dilakukan. Penyuluhan dan penyaluran terhadap personel pemelihara saat mereka berada di tempat perbaikan juga layak dilakukan.
2. Akun pemeliharaan
Banyak sistem komputer menyediakan akun pemeriharaan. Akun di tingkat teratas ini diset dari pabrik dan menggunakan password yang diketahui oleh umum. Sangat penting untuk mengganti password tersebut atau sekurangnya mematikan akun tersebut sampai saatnya diperlukan. Apabila akun ini digunakan melalui jarak jauh, otentikasi dari penyedia pemelihara dapat dilakukan dengan cara callback atau enkripsi.
3. Kontrol port diagnosa
Banyak sistem memiliki port untuk melakukan diagnosa terhadap sistem yang dapat dilalui oleh pengkoreksi masalah untuk mengakses secara langsung ke perangkat keras. Port ini seharusnya hanya dapat digunakan oleh personel yang sah dan juga tidak membolehkan akses tidak sah baik secara internal maupun eksternal. Penyerangan port diagnosa adalah istilah yang menjelaskan tipe penyalahgunaan tersebut.
4. Kontrol perangkat keras fisik
Banyak area pemrosesan daya yang memiliki perangkat keras membutuhkan kunci dan alarm. Beberapa contohnya sebagai berikut:
 - Terminal dan keyboard operator yang sensitif
 - Kabinet atau ruangan media penyimpanan
 - Data center server atau perlengkapan komunikasi
 - Ruangan kumpulan modem atau sirkuit telekomunikasi

2.4.3 Kontrol Perangkat Lunak (Software Controls)

Unsur penting dari kontrol operasi adalah dukungan perangkat lunak – mengontrol perangkat lunak apa saja yang digunakan di dalam sistem. Unsur dari kontrol perangkat lunak, antara lain:

1. Manajemen anti-virus
Jika personel dapat menjalankan perangkat lunak apa saja yang ada di dalam sistem, maka sistem akan rawan terhadap virus, interaksi perangkat lunak yang tidak semestinya, dan juga perubahan paksa kontrol keamanan.

2. Uji perangkat lunak
Proses pengujian perangkat lunak yang kaku dan formal diperlukan untuk menentukan kompatibilitas dengan aplikasi khusus atau untuk mengidentifikasi interaksi lain yang tidak dikira sebelumnya. Prosedur ini sebaiknya diterapkan pada saat upgrade perangkat lunak.
3. Utiliti perangkat lunak
Utiliti sistem yang sangat berkuasa dapat menyalahgunakan integritas dari sistem pengoperasian dan kontrol akses logik. Sebaiknya dikontrol oleh kebijakan keamanan.
4. Penyimpanan perangkat lunak secara aman
Kombinasi dari kontrol logik dan fisik sebaiknya diterapkan untuk menjamin bahwa perangkat lunak dan salinan dari backup tidak dimodifikasi secara tidak sah.
5. Kontrol backup
Tidak hanya personel pendukung dan operasi melakukan backup perangkat lunak dan data, di lingkungan yang terdistribusi pengguna dapat juga melakukan backup terhadap data mereka sendiri. Adalah penting untuk secara rutin melakukan pengujian akurasi pengembalian (restore) dari suatu sistem backup. Suatu backup harus dapat disimpan secara aman untuk melindungi dari pencurian, pengrusakan, ataupun masalah lingkungan.

2.4.4 Kontrol Entitas-Kewenangan (Privileged-Entity Controls)

Kontrol entitas kewenangan didefinisikan sebagai akses lebih atau khusus ke suatu sumberdaya komputasi yang diberikan kepada operator dan administrator sistem. Banyak tugas kerja dan fungsi memerlukan akses tertentu.

Akses entitas kewenangan umumnya dipisahkan ke dalam kelas-kelas. Operator sebaiknya ditugaskan ke dalam kelas dengan berdasarkan job title mereka. Berikut ini adalah contoh dari fungsi operator dengan entitas kewenangnya:

- Akses khusus ke system command
- Akses ke parameter khusus
- Akses ke program kontrol sistem

2.4.5 Kontrol Media (Media Controls)

Pengamanan sumberdaya media dapat diklasifikasikan ke dalam dua area yaitu kontrol pengamanan media dan kontrol penanganan media. Kontrol pengamanan media diterapkan untuk mencegah ancaman pada C.I.A. dari pengungkapan data sensitif secara sengaja atau tidak disengaja. Kontrol ketersediaan media diterapkan untuk melindungi keadaan kerja yang benar dari media, khususnya untuk memfasilitasi pengembalian data (restore) secara akurat dan tepat waktu pada saat terjadi kegagalan sistem.

Berikut penjelasan klasifikasi kontrol media:

1. Kontrol Pengamanan Media (Media Security Controls)
Kontrol Pengamanan Media sebaiknya dirancang untuk mencegah hilangnya informasi sensitif ketika media dikirim keluar sistem.

Beberapa elemen kontrol pengamanan media:

- a. Pencatatan (Logging)
Pencatatan dengan menggunakan media data menghasilkan akuntabilitas. Pencatatan juga membantu di kontrol penyimpanan fisik dengan cara mencegah tape berpindah tempat dan juga memfasilitasi proses recovery yang diperlukan.
 - b. Kontrol akses (Access Control)
Akses kontrol fisik ke media digunakan untuk mencegah akses ke media oleh personel yang tidak sah. Prosedur ini juga merupakan kontrol penyimpanan fisik.
 - c. Pembuangan yang Benar (Proper Disposal)
Pembuangan media yang tepat dan bena diperlukan untuk menghindari adanya data yang tertinggal. Proses untuk menghilangkan informasi dari data media yang sudah terpakai disebut dengan sanitasi. Tiga teknik yang umum digunakan untuk sanitasi yaitu penulisan ulang, pen-degauss-an, dan penghancuran.
2. Kontrol Ketersediaan Media (Media Viability Controls)
Banyak kontrol fisik yang seharusnya digunakan untuk melindungi ketersediaan dari media penyimpanan data. Tujuannya adalah untuk mengamankan media dari kerusakan pada saat penanganan dan pemindahtempatan atau dalam jangka waktu pendek ataupun panjang. Penandaan yang benar dan pelabelan media diperlukan pada saat proses recovery sistem.

Beberapa elemen kontrol ketersediaan media:

- a. Penandaan (Marking)
Semua media penyimpanan data sebaiknya diberi tanda dan label dengan akurat. Label dapat digunakan untuk mengidentifikasi media dengan instruksi penanganan media tersebut atau untuk mencatat serial number atau bar code untuk penanganan pada saat recovery sistem.
- b. Penanganan (Handling)
Penanganan media dengan benar adalah penting. Beberapa hal yang berhubungan dengan penanganan media antara lain termasuk kebersihan media dan pengamanan dari pengrusakan secara fisik ke media pada saat pemindahan ke tempat pengumpulan media.
- c. Penyimpanan (Storage): Penyimpanan dari media adalah sangat penting untuk alasan keamanan dan lingkungan. Lingkungan yang memiliki panas tepat dan bebas kelembaban harus disediakan untuk media. Media data sensitif terhadap temperatur, cairan, medan magnet, asap, dan debu.

2.4.6 Kontrol Terhadap Akses Fisik (Physical Access Controls)

Kontrol pada akses fisik suatu sumberdaya adalah merupakan salah satu pembahasan utama di domain Keamanan Fisik (Physical Security). Secara tidak langsung domain Keamanan Operasi (Operations Security) juga memerlukan kontrol akses fisik.

Berikut ini mengandung beberapa contoh unsur dari sumberdaya operasi yang memerlukan kontrol akses fisik:

1. Perangkat keras, meliputi:
 - Kontrol komunikasi dan perlengkapan komputasi
 - Kontrol media penyimpanan

- Kontrol log dan report yang tercetak
2. Perangkat lunak, meliputi:
- Kontrol file backup
 - Kontrol log sistem
 - Kontrol aplikasi produksi
 - Kontrol data sensitif/kritikal

Secara tidak langsung, semua personel memerlukan suatu kontrol dan akuntabilitas ketika mengakses sumberdaya fisik, dan juga semua personel memerlukan akses fisik khusus untuk dapat melakukan fungsi pekerjaan mereka. Berikut ini contoh tipe dari personel-personel tersebut:

- Personel departemen Teknologi Informasi
- Staf kebersihan
- Personel pemelihara Heating Ventilation and Air Conditioning (HVAC)
- Personel pihak ketiga
- Konsultan, kontraktor, dan staf temporer

Perjanjian khusus untuk mengawasi sistem harus dibuat ketika ada personel pendukung luar yang memasuki data center.

3. Pengawasan dan Pengauditan (Monitoring and Auditing)

Pengawasan disini diimplementasikan pada fasilitas operasional dimana untuk mengidentifikasi penggunaan computer yang tidak semestinya. Mendeteksi kerusakan dan responnya, termasuk mekanisme pelaporan adalah bagian penting dari pengawasan.

3.1 Pengawasan (Monitoring)

Pengawasan terdiri mekanisme, peralatan dan teknik yang mengijinkan identifikasi dari kejadian keamanan yang dapat mempengaruhi operasi dari komputer. Konsep pengawasan termasuk pengawasan untuk instalasi perangkat lunak ilegal, memonitor perangkat keras untuk kesalahan, dan memonitor kegiatan operasional untuk anomali/keanehan.

Teknik-teknik dalam Pengawasan, antara lain sebagai berikut:

1. Intrusion Detection
Intrusion Detection adalah sarana sangat bermanfaat untuk dapat membimbing proses analisa dari gangguan yang terjadi, tidak hanya dapat digunakan untuk mengidentifikasi gangguan tapi juga untuk membuat contoh pola lalu lintas. Dengan menganalisa aktivitas yang terjadi di atas tingkat normal.
2. Penetration Testing
Penetration Testing adalah proses uji ketahanan jaringan dengan mencoba menerobos sistem dari luar dengan menggunakan teknik sama seperti yang digunakan oleh penerobos eksternal (contoh: cracker). Pengujian ini memberikan para profesional akan gambaran keadaan keamanan organisasi.

Dari berbagai macam teknik yang digunakan pada Penetration Testing terdapat beberapa teknik yang umum, antara lain:

- Scanning dan Probing
Berbagai macam scanner seperti port scanner, dapat memberikan informasi tentang infrastruktur jaringan komputer dan memungkinkan penerobos untuk mengakses port jaringan yang tidak diamankan.
- Demon Dialing
Demon (atau perang) dialer akan secara otomatis mengakses setiap sambungan telepon yang ada untuk mencoba menempatkan modem yang terhubung dengan jaringan. Informasi tentang modem ini kemudian dapat digunakan untuk akses dari luar secara tidak sah.
- Sniffing
Sebuah penganalisa protokol (protocol analyzer) dapat digunakan untuk menangkap (capture) paket data yang kemudian dapat dikodekan untuk mengumpulkan informasi seperti password atau konfigurasi infrastruktur.

Teknik lain yang tidak berbasiskan teknologi namun dapat digunakan untuk melengkapi Penetration Testing, antara lain :

- Dumpster Diving
Pencarian kertas-kertas berisi informasi berharga yang dibuang untuk mencari laporan-laporan penting yang tidak terpotong.
- Social Engineering
Teknik yang paling umum dan mudah digunakan untuk mendapatkan informasi seperti password yaitu dengan bertanya langsung kepada mereka yang memiliki password tersebut.

3. Violation Analysis

Salah satu teknik yang paling banyak digunakan untuk melacak perubahan aktivitas pengguna adalah pelacakan pelanggaran, pemrosesan, dan analisa. Agar penggunaan pelacakan pelanggaran efektif, clipping level harus ditetapkan terlebih dahulu. Clipping level adalah suatu dasar untuk aktivitas pengguna yang dipercayai sebagai kesalahan pengguna tingkat rutin. Clipping level digunakan agar sistem dapat mengabaikan kesalahan normal pengguna, namun ketika clipping level terlampaui maka catatan pelanggaran akan terbentuk. Clipping level juga digunakan untuk berbagai macam detektor.

Penggunaan clipping level dan deteksi anomali berdasarkan profil di bawah ini adalah tipe dari pelanggaran yang harus dilacak, diproses dan dianalisa:

- Kesalahan berulang-ulang yang melewati batas angka clipping level
- Individu yang melampaui otorisasinya
- Terlalu banyak orang yang memiliki akses tidak terbatas
- Pola-pola yang mengindikasikan percobaan penerobosan

3.2 Pengauditan (Auditing)

Implementasi dari audit sistem yang teratur adalah merupakan fondasi bagi pengawasan kontrol keamanan operasional. Sebagai tambahan dari dilakukannya pengecekan compliance baik internal maupun eksternal, pelaksanaan audit pada jejak audit (transaksi) dan log dapat membantu fungsi pengawasan dengan cara mengenali pola-pola yang abnormal dari kebiasaan pengguna.

3.2.1 Audit Keamanan (Security Auditing)

Auditor Teknologi Informasi (TI) sering dibagi menjadi dua tipe yaitu internal dan eksternal. Auditor internal biasanya bekerja untuk organisasi sedangkan eksternal tidak. Auditor eksternal sering bersertifikat Public Accountants atau Audit Professional yang lain yang diberi imbalan untuk melakukan audit independen pada organisasi finansial. Sedangkan auditor internal biasanya mempunyai cakupan pekerjaan yang lebih luas mengecek apakah standar yang ditetapkan telah terpenuhi, mengaudit efisiensi biaya operasi dan merekomendasikan kontrol yang tepat.

Auditor TI biasanya mengaudit hal-hal sebagai berikut:

- Kontrol backup
- Kontrol sistem dan transaksi
- Prosedur perpustakaan data
- Standar pengembangan sistem
- Keamanan data center
- Rencana keberlangsungan (contingency plan)

Auditor TI dapat juga merekomendasikan perbaikan kontrol dan mereka sering berpartisipasi dalam proses pengembangan sistem untuk membantu organisasi menghindari rekayasa ulang berbiaya besar setelah sistem diimplementasi.

3.2.2 Jejak Audit (Audit Trails)

Jejak audit memungkinkan praktisi keamanan untuk melacak sebuah sejarah transaksi. Jejak audit menyediakan informasi tentang penambahan, penghapusan dan modifikasi data dalam sistem yang seluruhnya disusun ulang menjadi suatu rangkaian kejadian menurut waktu. Jejak audit digunakan untuk membimbing mengidentifikasi problem dimana dapat membantu memecahkan problem tersebut.

Log audit sebaiknya mencatat hal-hal sebagai berikut:

- Tanggal dan waktu transaksi
- Siapa yang memproses transaksi tersebut
- Terminal mana transaksi tersebut di proses
- Berbagai macam kejadian keamanan yang berhubungan dengan transaksi

Auditor sebaiknya juga memeriksa log audit untuk hal-hal berikut:

- Amandemen ke pekerjaan produksi
- Pengerjaan ulang pekerjaan produksi
- Praktek operator komputer

Hal-hal lain yang juga penting untuk diperhatikan sehubungan dengan penggunaan media dan laporan audit adalah sebagai berikut:

- Retensi dan pengamanan dari media dan laporan audit ketika dikeluarkan dari tempat asalnya
- Pengamanan terhadap penghilangan audit atau log transaksi
- Pengamanan terhadap ketidaksediaan dari media audit pada suatu kejadian

3.2.3 Konsep Manajemen Masalah (Management Problem Concept)

Audit yang efektif mencakup konsep dari manajemen masalah. Manajemen masalah adalah cara untuk mengontrol proses isolasi masalah dan penyelesaian masalah. Auditor dapat juga menggunakan manajemen masalah untuk memecahkan isu yang berkembang seputar audit keamanan TI.

Ada tiga tujuan dari manajemen masalah:

1. Mengurangi kesalahan sampai ke tingkat yang dapat dikelola
2. Mencegah ulangan atau pengulangan dari masalah
3. Menangani dampak negatif dari masalah pada layanan komputasi dan sumberdaya

Langkah pertama dalam penerapan manajemen masalah adalah mendefinisikan area masalah yang potensial dan kejadian abnormal yang harus diselidiki. Beberapa contoh area masalah yang potensial, antara lain:

- Kemampuan dan ketersediaan dari sumberdaya komputasi dan layanan
- Infrastruktur sistem dan jaringan
- Prosedur dan transaksi
- Keselamatan dan keamanan personel

Beberapa contoh kejadian abnormal yang mungkin dapat ditemui pada saat audit, antara lain:

- Degradasi kemampuan perangkat keras atau lunak
- Deviasi dari prosedur standar transaksi
- Kejadian yang tidak dapat dijelaskan pada rantai proses

4. Ancaman dan Kerawanan (Threats and Vulnerabilities)

Ancaman adalah semua hal yang apabila terjadi dapat menyebabkan kerusakan pada sistem dan kehilangan kerahasiaan, kemampuan, dan integritas. Ancaman dapat berbahaya seperti merubah data-data yang sensitif atau dapat terjadi secara tidak sengaja seperti kesalahan pada kalkulasi transaksi atau penghapusan file yang tidak disengaja. Kerawanan adalah kelemahan yang terdapat pada sistem yang dapat dimanfaatkan oleh ancaman. Mengurangi aspek kerawanan pada sistem dapat mengurangi resiko dan efek dari ancaman pada sistem. Contohnya pada program password generation yang dapat membantu user memilih password robust (tidak mudah ditebak), yang dapat mengurangi kemungkinan user menggunakan password yang buruk (kerawanan) dan membuat password semakin susah untuk ditembus (ancaman).

4.1 Ancaman (Threats)

Ancaman dapat dikelompokkan menjadi beberapa macam, antara lain:

1. Kehilangan tidak disengaja (Accidental Loss)
Kehilangan tidak disengaja adalah kehilangan yang terjadi tidak secara terus-menerus dapat juga karena tidak adanya pelatihan terhadap operator atau kesalahan pada proses prosedur penggunaan aplikasi.

Beberapa contoh kehilangan tidak disengaja, antara lain:

- Kesalahan menginput pada operator atau kelalaian, hal ini dapat berupa kesalahan pada input transaksi, entri data ataupun penghapusan data dan kesalahan pada modifikasi data.
 - Kesalahan pada proses transaksi, kesalahan dapat terjadi pada data karena kesalahan pada program aplikasi atau prosedur proses.
2. Aktivitas tidak layak (Inappropriate Activities)
Kebiasaan menggunakan computer untuk aktivitas yang tidak layak selama itu bukan merupakan tindakan kriminal namun dapat dikenakan sanksi dari perusahaan pada pegawai yang melakukannya.

Beberapa contoh aktivitas yang tidak layak:

- Konten tidak layak
Menggunakan system perusahaan untuk menyimpan pornografi, hiburan, politik maupun muatan kekerasan
 - Sampah dari sumber perusahaan
Seseorang menggunakan perangkat keras maupun perangkat lunak, seperti mengadakan suatu bisnis pribadi dengan mempergunakan sistem komputer perusahaan
 - Kejahatan seksual ataupun rasial
Menggunakan email atau sumberdaya komputer lainnya untuk mendistribusikan material secara tidak layak.
 - Penyalagunaan kewenangan atau hak
Menggunakan level akses tidak sah untuk melanggar kerahasiaan informasi perusahaan
3. Operasi komputer ilegal dan Penyerangan yang disengaja (Illegal Computer Operations and Intentional Attacks)
Dibawah ini adalah kelompok area kegiatan yang dipertimbangkan sebagai kegiatan komputer ilegal yang disengaja untuk keuntungan financial pribadi dan untuk pengrusakan:
- Kegiatan memata-matai
Mengais-ngais data, lalu lintas data maupun analisa perkembangan, social engineering, ekonomi ataupun mata-mata politik, sniffing maupun pengamatan keystroke ataupun melakukan pemecahan terhadap segala jenis kegiatan mata-mata untuk mendapatkan informasi atau untuk menciptakan suatu pijakan untuk penyerangan berikutnya. Kegiatan memata-matai merupakan penyebab utama dari kegagalan kerahasiaan.
 - Penipuan
Contoh dari jenis penipuan adalah kolusi, transaksi fiktif, manipulasi data dan pengubahan data lainnya secara integritas untuk suatu keuntungan.
 - Pencurian
Contoh dari jenis pencurian adalah pencurian informasi atau rahasia perdagangan untuk keuntungan atau penyingkapan data secara tidak sah serta pencurian secara fisik perangkat keras maupun perangkat lunak.
 - Sabotase
Sabotase termasuk didalamnya Denial of Service (DoS), penundaan produksi dan sabotase data terintegritas.
 - Serangan Eksternal
Contoh dari serangan eksternal adalah cracking yang berbahaya, scanning dan probing yang berusaha untuk merusak infrastruktur informasi, demon dialing

untuk mencari sambungan modem yang tidak terlindungi, dan menyebarkan kode atau virus yang berbahaya.

4.2 Kerawanan (Vulnerabilities)

1. Analisa Tren/Lalu lintas (Traffic/Trend analysis)

Traffic analysis kadang kala disebut juga sebagai trend analysis, yaitu sebuah teknik yang digunakan oleh penerobos untuk menganalisa karakteristik data (panjang pesan, frekuensi pesan, dan sebagainya) dan pola pengiriman, untuk menjangkau informasi yang berguna untuk penerobos.

Untuk menangkalkan analisa lalulintas, digunakan cara yang mirip dengan untuk menangkalkan serangan terhadap kriptografi, antara lain:

- Padding message
Membuat semua message menjadi seragam bentuk datanya dengan menempatkan tempat kosong pada data.
- Sending noise
Memasukkan data yang tidak mengandung informasi apapun digabungkan ke dalam informasi yang sesungguhnya untuk mengacaukan pesan yang sesungguhnya.
- Covert channel analysis

2. Akun Pemeliharaan (Maintenance Account)

Salah satu cara untuk menerobos ke dalam sistem komputer adalah dengan menggunakan akun pemeliharaan yang masih memiliki password asal dari pabrik pembuatnya atau password yang mudah ditebak. Akses fisik ke perangkat keras yang diserahkan pengelolaannya pada perorangan juga dapat menyebabkan pelanggaran keamanan.

3. Penyerangan Pengaisan Data (Data-Scavenging Attacks)

Pengaisan data adalah salah satu teknik yang menyatukan kembali data-data informasi yang telah terpisah-pisah. Dimana ada dua tipe yang umum digunakan:

- Keyboard attacks
Data dikais melalui sumberdaya yang tersedia ke user sistem normal yang duduk di depan keyboard menggunakan peralatan normal untuk mengumpulkan informasi.
- Laboratory attacks
Data dikais dengan menggunakan peralatan elektronik yang canggih dan dengan perencanaan yang tepat.

4. Kerawanan IPL (IPL Vulnerabilities)

Dimulai dari sistem itu sendiri, Initial Program Load (IPL), adalah spesifik sistem kerawanan yang spesifik suatu sistem dimana tipe sistem mainframe tersentralisasi atau tipe LAN yang terdistribusi. Selama IPL, operator membawa fasilitas sistem. Operator ini mempunyai kemampuan membawa sistem ke dalam single user mode, tanpa adanya pengamanan secara penuh, disini terdapat kewenangan tidak terbatas. Pada keadaan ini operator dapat membawa banyak program atau data tanpa otorisasi, reset password, rename banyak sumberdaya, atau reset waktu dan tanggal sistem. Operator dapat juga menentukan data port atau jalur komunikasi yang digunakan untuk mengirimkan informasi pada sekutunya di luar data center. Pada sebuah LAN, administrator sistem dapat melihat bagian dari tape, CD-ROM atau floppy disk, melewati keamanan sistem operasi pada hard drive.

5. Pembajakan Alamat Jaringan (Network Address Hijacking)
Penerobos dapat melihat kembali data lalu lintas dari server atau perangkat jaringan ke komputer seseorang, demikian juga dengan memodifikasi alamat perangkat atau pembajakan alamat jaringan. Hal ini memungkinkan penerobos memantau lalu lintas dari dan keluar perangkat tersebut untuk analisa data atau modifikasi atau mencuri file password dari server dan memperoleh akses ke akun pengguna. Dengan menyelusuri output data, penerobos dapat mengabaikan pengawasan dari terminal dan mengelabui log sistem.

5. Penutup

5.1 Kesimpulan

5.2 Saran

Daftar Pustaka

- ICSA Labs. 2005. *Standards for commercial security products are set by ICSA Labs*. Diakses 27 Oktober 2005, dari <https://www.icsalabs.com/icsa/icsahome.php>
- Krutz, Ronald L., Russell Dean Vines. 2003. *The CISSP® Prep Guide: Gold Edition*. Indiana: Wiley Publishing, Inc.
- Microsoft Corporation. 2005. *Microsoft Small Business Center*. Diakses 27 Oktober 2005, dari <http://www.microsoft.com/smallbusiness/hub.mspx>
- Microsoft Corporation. 2005. *Security Bulletin Search*. Diakses 27 Oktober 2005, dari <http://www.microsoft.com/technet/security/current.aspx>
- Muhammad, Reza. 2003. *15 Jenis Serangan Cracker*. Indonesia: IlmuKomputer.Com. Diakses 27 Oktober 2005, dari <http://ilmukomputer.com/populer/reza-cracker.php>
- Purbo, Onno W. 2003. *Ensiklopedia Serangan Denial of Service*. Indonesia: IlmuKomputer.Com. Diakses 27 Oktober 2005, dari <http://ilmukomputer.com/populer/onno-dos.php>
- Purbosudibyo, Gani. 2003. *Mengenal Social Engineering*. Indonesia: IlmuKomputer.Com. Diakses 27 Oktober 2005, dari <http://ilmukomputer.com/populer/gani-socialeng.php>
- Sourcefire, Inc. 2005. *Snort Documents*. Diakses 27 Oktober 2005, dari <http://www.snort.org/docs/>
- Symantec Corporation. 2005. *Small Business - Symantec Corp*. Diakses 27 Oktober 2005, dari http://symantec.com/small_business/index.html
- Symantec Corporation. 2005. *The Critical Intrusion Detection Layer*. Diakses 27 Oktober 2005, dari <http://www.symantec.com/region/in/smallbiz/library/intrusion.html>
- Terpstra, John H. 2005. *Practical Exercises in Successful Samba Deployment*. Samba Team. Diakses 27 Oktober 2005, dari <http://us2.samba.org/samba/docs/man/Samba-Guide/>
- The OpenLDAP Project. 2005. *OpenLDAP Software 2.3 Administrator's Guide*. Diakses 27 Oktober 2005, dari <http://www.openldap.org/doc/admin23/>
- Ts, Jay, Robert Eckstein, David Collier-Brown. 2003. *Using Samba, 2nd Edition*. O'Reilly & Associates. Diakses 27 Oktober 2005, dari http://us2.samba.org/samba/docs/using_samba/toc.html
- Ziff Davis Publishing Holdings Inc. 2005. *PC Magazine Security Product Guide*. Diakses 27 Oktober 2005, dari <http://www.pcmag.com/category2/0,1874,4829,00.asp>