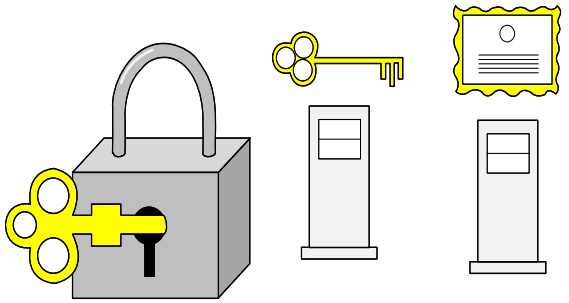
Pengantar Keamanan Sistem Informasi

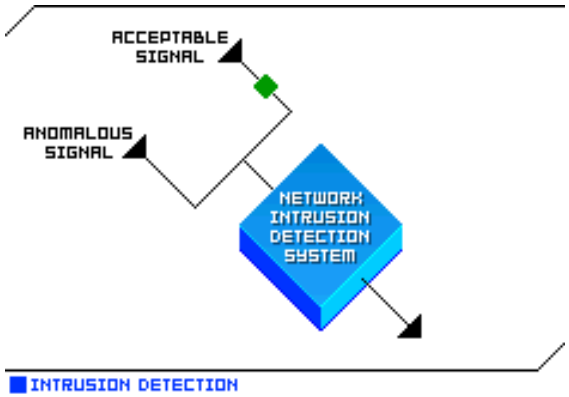
1. *Evaluasi Keamanan TI*
2. *Database*

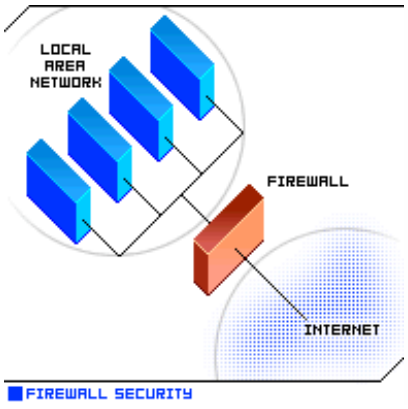
Mohammad Iqbal

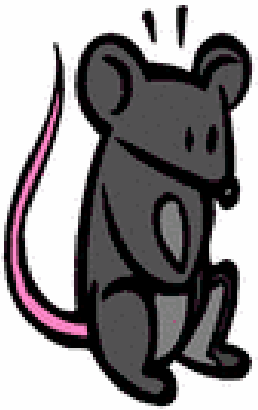
Evaluasi Keamanan TI

- Back-up
- Auditing System
- Firewall
- IDS (Intrusion Detection System)
- Digital Forensik









Back-up

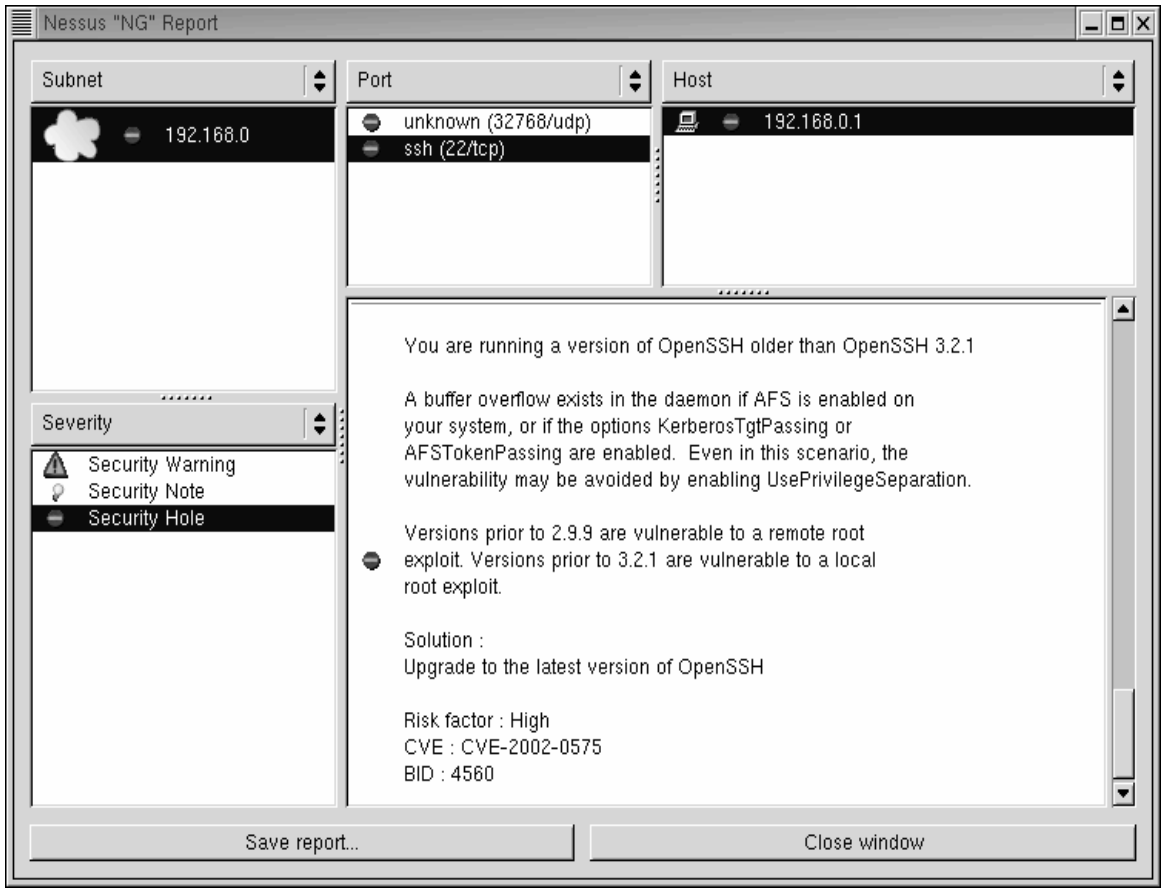
- **Backuplah sebelum menyesal !**
  - Sistem Operasi dan Service
  - Database
  - Aplikasi
  - Data-data penting lainnya

- Backup ke ..
  - CD/DVDROM
  - Harddisk khusus backup
  - Tape Back-up
  - Zip drive

Auditing System

- **Auditlah system Anda sebelum orang lain melakukannya ☺**
  - Hak akses
  - Sistem
  - Audit dengan Penetration testing

Contoh audit system dengan **Nessus**



Auditing System : Checklist

- ☑ Evaluasi topologi network
- ☑ *Penetration testing* dari luar dan dari dalam network
- ☑ Evaluasi network devices : routers, switches, firewalls, IDS, dll.
- ☑ Evaluasi *server*
- ☑ Evaluasi *software applications*
- ☑ Evaluasi policy (kebijakan) dan prosedur

Auditing System : Tools

Tools Terintegrasi

Perangkat lunak bantu	**Sistem Operasi**
Nessus	Windows
Cops	UNIX
Tripwire	UNIX
Satan/Saint	UNIX
SBScan: localhost security scanner	UNIX
Ballista <http://www.secnet.com>	Windows
Dan sebagainya… (cari sendiri!)	

Auditing System : Tools

Tools Parsial buatan 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
Dan sebagainya… (cari sendiri!)	

Auditing System : Tools

- **PROBING SERVICES** : “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.

Paket probe LINUX/UNIX
- nmap
- strobe
- tcpprobe

Paket Probe Windows
- NetLab
- Cyberkit
- Ogre

Program yang memonitor adanya probing ke system

Probing biasanya meninggalkan jejak di berkas log di system. Dengan mengamati entry di dalam berkas log dapat diketahui adanya probing.

Beberapa program untuk memonitor probe :

courtney, portsentry dan tcplogd.

Auditing System : Logging

Defenisi Logging :

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

- **Pencatatan logon dan logoff** termasuk pencatatan dalam **multi entry login**
- **Object access** (pencatatan akses obyek dan file)
- **Privilege Use** (pencatatan 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)

Auditing System : Logging

Contoh Pada LINUX : Semua file log linux disimpan di folder ***/var/log***,

- **Lastlog** : rekaman user login terakhir kali
- **last** : rekaman user yang pernah login dengan mencarinya pada file /var/log/wtmp
- **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.
- **Access_log** : rekaman layanan http / webserver.
- **Error_log** : rekaman pesan kesalahan atas service http / webserver berupa data jam dan waktu, tipe/alasan kesalahan
- **Messages** : rekaman kejadian pada kernel ditangani oleh dua daemon :
  - Syslog → merekam semua program yang dijalankan, konfigurasi pada syslog.conf
  - Klog → menerima dan merekam semua pesan kernel

Auditing System : Network Monitoring

- **Sistem pemantau jaringan** (network monitoring) digunakan untuk mengetahui adanya lubang keamaman → Memanfaatkan protokol SNMP (Simple Network Management Protocol).

Program network monitoring / management :

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

Program pemantau jaringan yang tidak menggunakan SNMP :

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
5. trafshow, menunjukkan traffic antar hosts dalam bentuk text-mode

Firewall

❑ Defenisi

- Firewall merupakan suatu mekanisme yang diterapkan baik terhadap hardware, software ataupun sistem itu sendiri
- dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan/kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkupnya.
- Segmen tersebut dapat merupakan sebuah workstation, server, router, atau local area network (LAN) anda.

Firewall

Keuntungan Firewall :

- Firewall merupakan fokus dari segala keputusan sekuritas. (fungsi sebagai satu titik tempat keluar masuknya trafik internet pada suatu jaringan)
- Firewall dapat menerapkan suatu kebijaksanaan sekuritas (fungsi sebagai penjaga untuk mengawasi service-service mana yang dapat digunakan untuk menuju dan meninggalkan suatu network)
- Firewall dapat mencatat segala aktivitas yang berkaitan dengan alur data secara efisien.
- Firewall dapat digunakan untuk membatasi pengunaan sumberdaya informasi.

Firewall

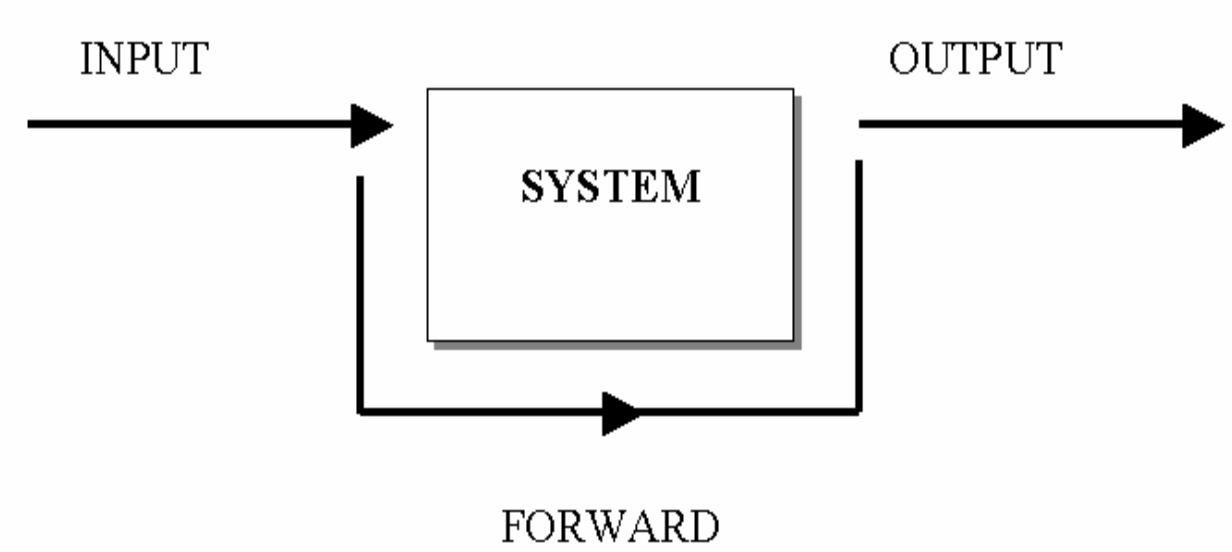
Kekurangan Firewall :

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

Firewall

Konsep Aliran paket data (chain)

- Input = rule untuk paket yang masuk
- Output = rule untuk paket yang keluar
- Forward = rule untuk paket yang diteruskan (khusus router)



Firewall

- **Jenis Firewall**
  1. Packet filtering
  2. Statefull Packet Filtering
  3. Proxy based (Application G

- **Dimana firewall dipasang ?**
  - Host (Personal firewall)
  - Router atau dedicated firewall

- **Efektifitas Firewall = 20% tools + 80%**

Firewall

Jenis Firewall

1. Packet Filtering Firewall

- Sistem paket *filtering* atau sering juga disebut dengan *screening router* adalah *router* yang melakukan routing paket antara internal dan eksternal *network* secara selektif sesuai dengan *security policy* yang digunakan pada *network* tersebut.
- Parameter yang di filter :
  - Protokol, contoh TCP, UDP, ICMP
  - Port Asal, contoh 25, 1024:65536
  - Port Tujuan, contoh 25
  - IP Asal/Network tujuan, contoh 81.52.22.1, 81.52.22.0/29
  - IP Tujuan /Network tujuan , contoh 81.52.22.1, 81.52.22.0/29
  - Code bit, contoh ACK
  - Judge, contoh DROP, ACCEPT
- Proses filtering cepat

Firewall
Jenis Firewall

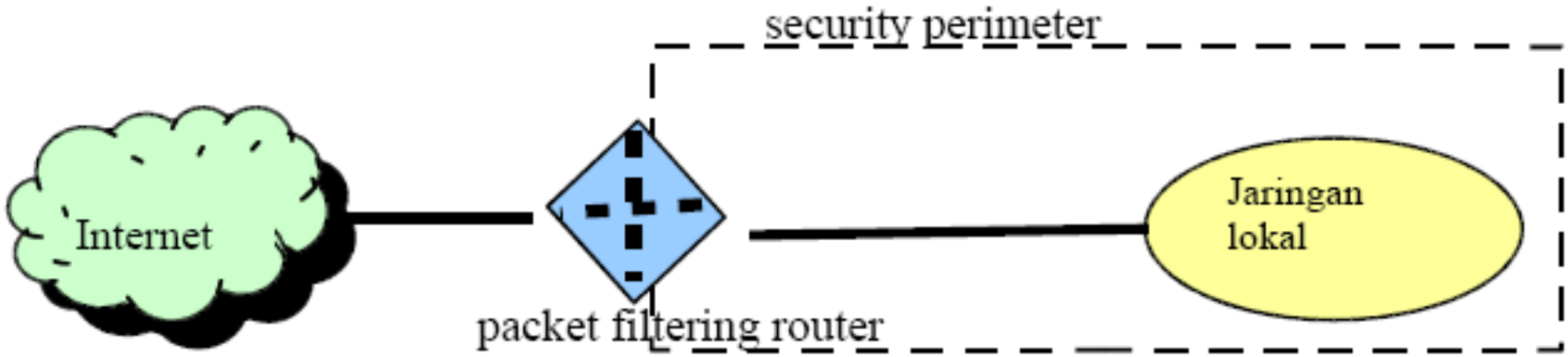
- Contoh policy selektif routing paket pada *Screening Router* :
  - Semua koneksi dari luar sistem yang menuju internal *network* diblokade kecuali untuk koneksi SMTP
  - Memperbolehkan *service* email dan FTP, tetapi memblok *service-service* berbahaya seperti TFTP, X Window, RPC dan 'r' *service* (rlogin, rsh, rcp, dan lain-lain).
- Kekurangan : tingkat *security*nya masih rendah, masih memungkinkan adanya IP Spoofing, tidak ada *screening* pada layer-layer di atas *network* layer.

Firewall

Jenis Firewall

2. Statefull Packet Filter

- Packet filtering yang dikembangkan sehingga mampu "mengingat" paket yang diimplementasikan dalam *state tabel*



Firewall

Jenis Firewall

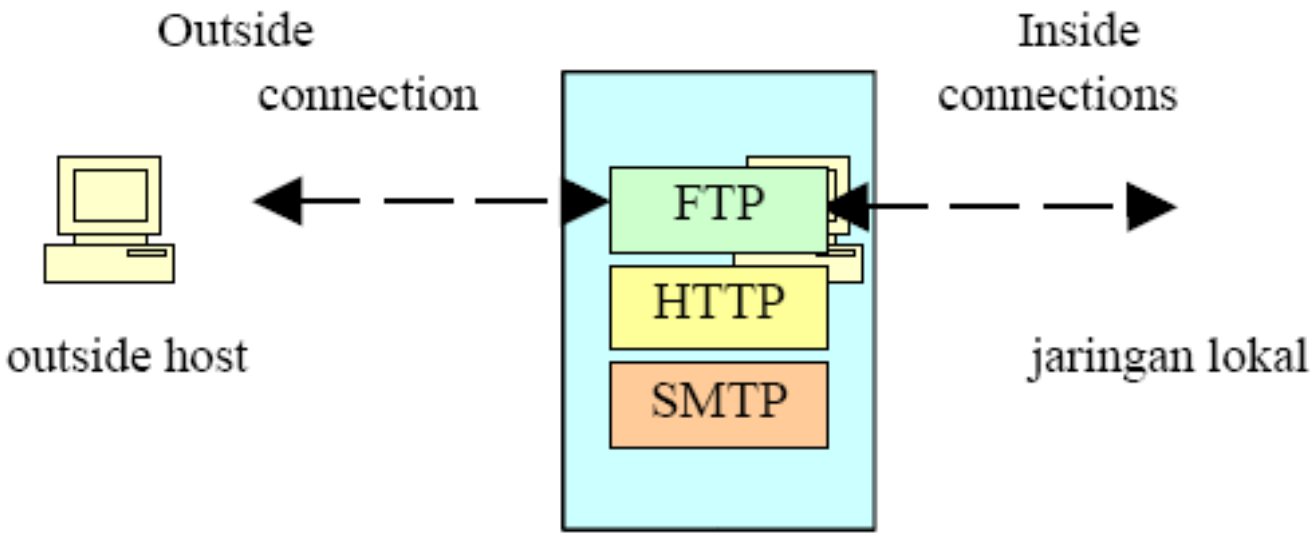
3. Application level Gateway - Proxy Based

- *Proxy service* merupakan aplikasi spesifik atau program server yang dijalankan pada mesin *Firewall*, program ini mengambil *user request* untuk Internet *service* (seperti FTP, telnet, HTTP) dan meneruskannya (bergantung pada *security policy*) ke *host* yang dituju. Dengan kata lain adalah *proxy* merupakan perantara antara internal *network* dengan eksternal *network* (Internet).
- Filtering di level aplikasi
- Kekurangan : Proses filtering lebih lambat karena terjadi penambahan *header* pada paket yang dikirim dan aplikasi yang di-*support* oleh *proxy* ini masih terbatas.

Firewall

Jenis Firewall

3. Application level Gateway - Proxy Based

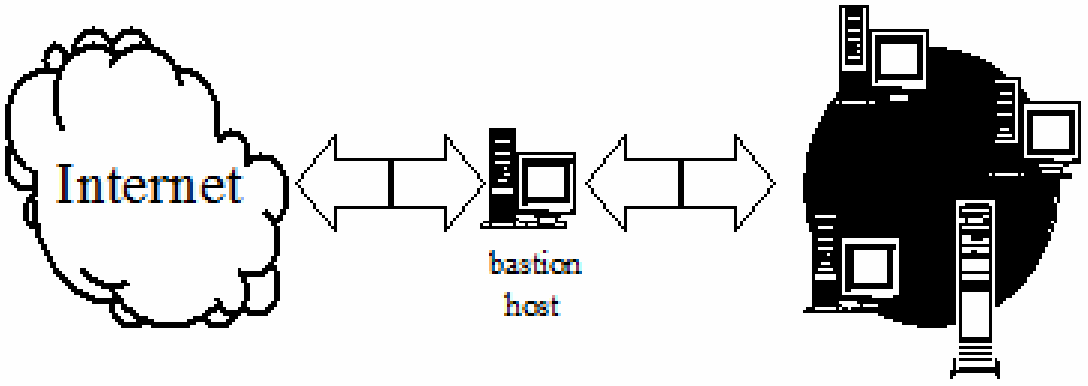


Firewall

Arsitektur Dasar

1. Dual homed gateway/ **DHG**

Sistem DHG menggunakan sebuah komputer dengan (paling sedikit) dua network-interface. Interface pertama dihubungkan dengan jaringan internal dan yang lainnya dengan Internet. Dual-homed host nya sendiri berfungsi sebagai bastion host (front terdepan, bagian terpenting dalam firewall).



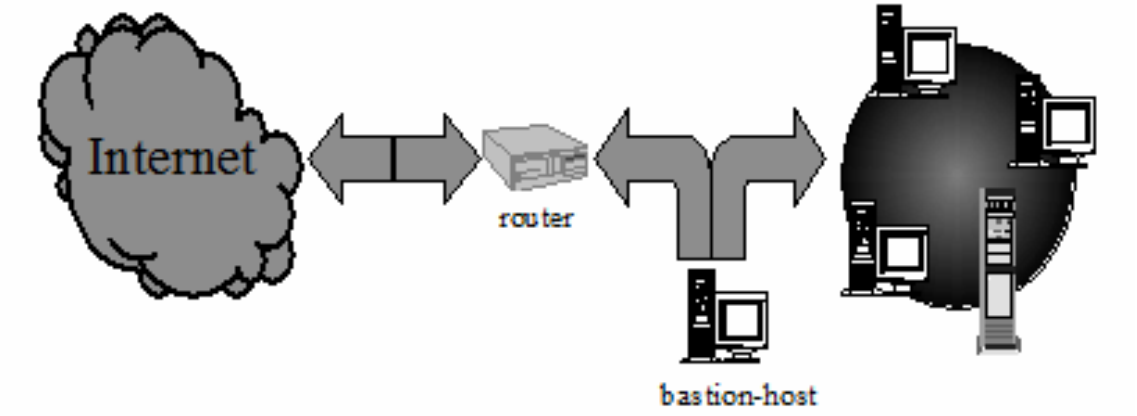
Arsitektur dengan dual-homed host

Firewall

Arsitektur Dasar

2. Screened-host (screened host gateway/ SHG)

Fungsi firewall dilakukan oleh sebuah screening-router dan bastion host. Router ini dikonfigurasi sedemikian sehingga akan menolak semua trafik kecuali yang ditujukan ke bastion host, sedangkan pada trafik internal tidak dilakukan pembatasan. Dengan cara ini setiap client servis pada jaringan internal dapat menggunakan fasilitas komunikasi standard dengan Internet tanpa harus melalui proxy.

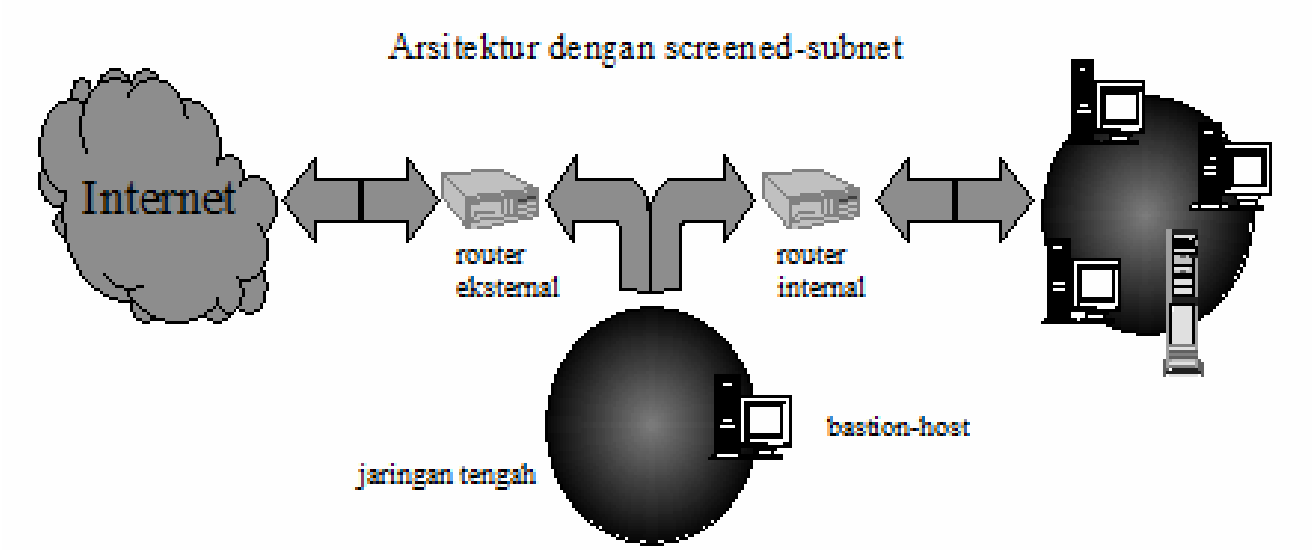


Arsitektur dengan screened-host

Firewall
Arsitektur Dasar

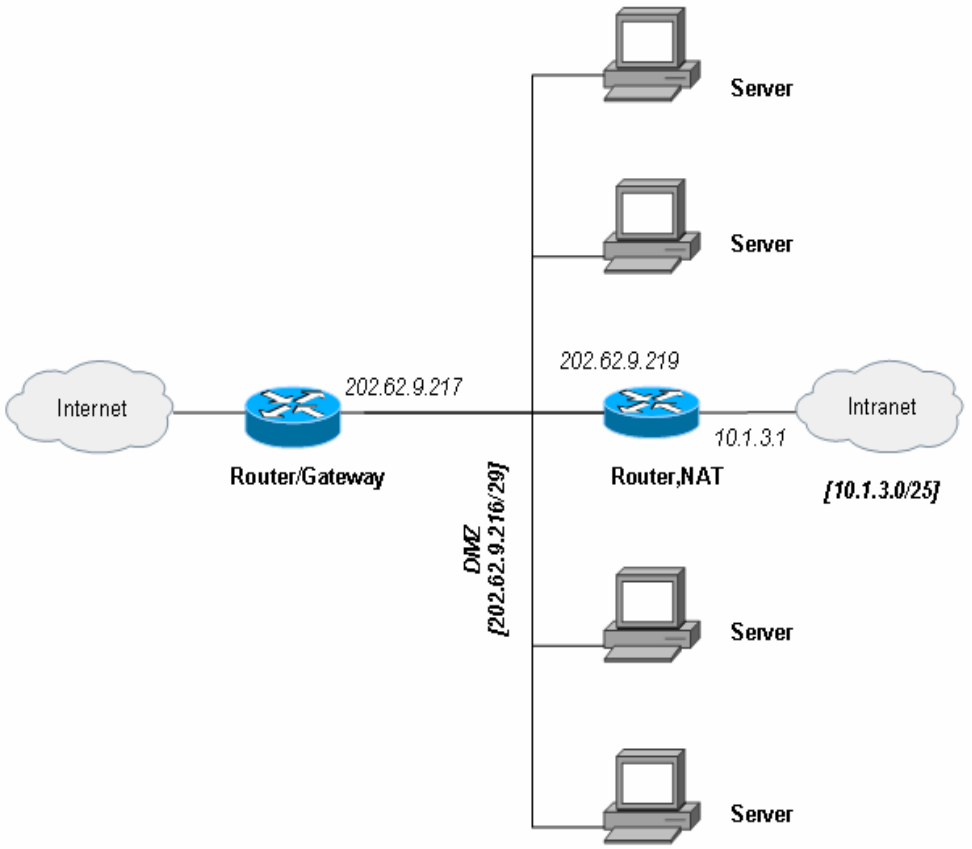
3. Screened-Subnet (screened subnet gateway/ SSG)

Firewall dengan arsitektur screened-subnet menggunakan dua screening-router dan jaringan tengah (*perimeter network*) antara kedua router tersebut, dimana ditempatkan bastion host. Kelebihan susunan ini akan terlihat pada waktu optimasi penempatan server.



Firewall

- **Posisi firewall yang optimal**
  - Firewall diletakkan di Router/Gateway untuk mengantisipasi serangan dari INTERNET
  - Firewall diletakkan di Router, NAT untuk mengantisipasi serangan dari INTRANET



Firewall

Membangun Firewall

1. Identifikasi bentuk jaringan yang dimiliki

- Mengetahui bentuk jaringan yang dimiliki khususnya toplogi yang di gunakan serta protocol jaringan, akan memudahkan dalam mendesain sebuah firewall

2. Penentuan Policy atau kebijakan : Baik buruknya sebuah firewall yang di bangun sangat di tentukan oleh policy/kebijakan yang di terapkan. Diantaranya:

- Menentukan apa saja yang perlu di layani. Artinya, apa saja yang akan dikenai policy atau kebijakan yang akan kita buat
- Menentukan individu atau kelompok-kelompok yang akan dikenakan policy atau kebijakan tersebut
- Menentukan layanan-layanan yang di butuhkan oleh tiap tiap individu atau kelompok yang menggunakan jaringan
- Berdasarkan setiap layanan yang di gunakan oleh individu atau kelompok tersebut akan ditentukan bagaimana konfigurasi terbaik yang akan membuatnya semakin aman
- Menerapkankan semua policy atau kebijakan tersebut

Firewall

Membangun Firewall

3. Menyiapkan Software atau Hardware yang akan digunakan
   - Baik itu operating system yang mendukung atau software-software khusus pendukung firewall seperti ipchains, atau iptables pada linux, dsb. Serta konfigurasi hardware yang akan mendukung firewall tersebut.

4. Melakukan test konfigurasi

- Pengujian terhadap firewall yang telah selesai di bangun haruslah dilakukan, terutama untuk mengetahui hasil yang akan kita dapatkan, caranya dapat menggunakan tool tool yang biasa dilakukan untuk mengaudit seperti nmap.

Firewall

❑ Contoh Firewall dengan IPTables

- 202.62.9.219 server yang didedikasikan khusus HANYA untuk Web Server, maka seluruh paket dari internet ditolak kecuali protokol TCP dengan destination port 80 dengan cara filtering paket di Router/Gateway (202.62.9.217)

```
#iptables –A FORWARD –p tcp –s 0.0.0.0/0 –d 202.62.9.219 –dport 80 –j
ACCEPT
#iptables –A FORWARD –p tcp –s 0.0.0.0/0 –d 202.62.9.219 –j DROP
#iptables –A FORWARD –p udp –s 0.0.0.0/0 –d 202.62.9.219 –j DROP
```

- Jaringan Intranet terkena virus brontok yang salah satu efeknya adalah client-client yang terkena virus ini melakukan flooding ICMP ke suatu situs (70.84.171.179)

```
#iptables –A FORWARD –p icmp –s 0.0.0.0/0 –d 70.84.171.179 –j DROP
```

IDS (Intrusion Detection System)

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

Tipe dasar IDS :

- 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 :
  - Preemptory (pencegahan) ; IDS akan memperhatikan semua lalu lintas jaringan, dan langsung bertindak jika dicurigai ada penyusupan.
  - Reactionary (reaksi) ; IDS hanya mengamati file log saja.
- Adaptive system : penerapan expert system dalam mengamati lalu lintas jaringan.

IDS (Intrusion Detection System)

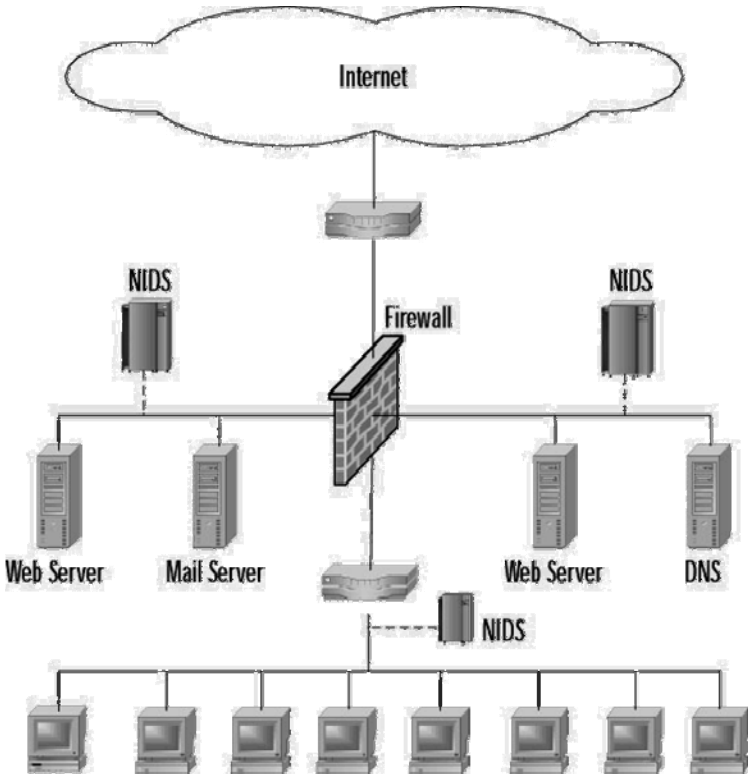
- **Cara deteksi**
  - Deteksi anomaly (prosessor, bandwidth, memory dan lain-lain)
  - Signature yang disimpan dalam database

- **Serangan terdeteksi, lalu apa?**
  - Alert via SMS, email dan lain-lain
  - Konfigurasi ulang firewall
  - Menjalankan program respon terhadap serangan
  - Logging serangan dan event

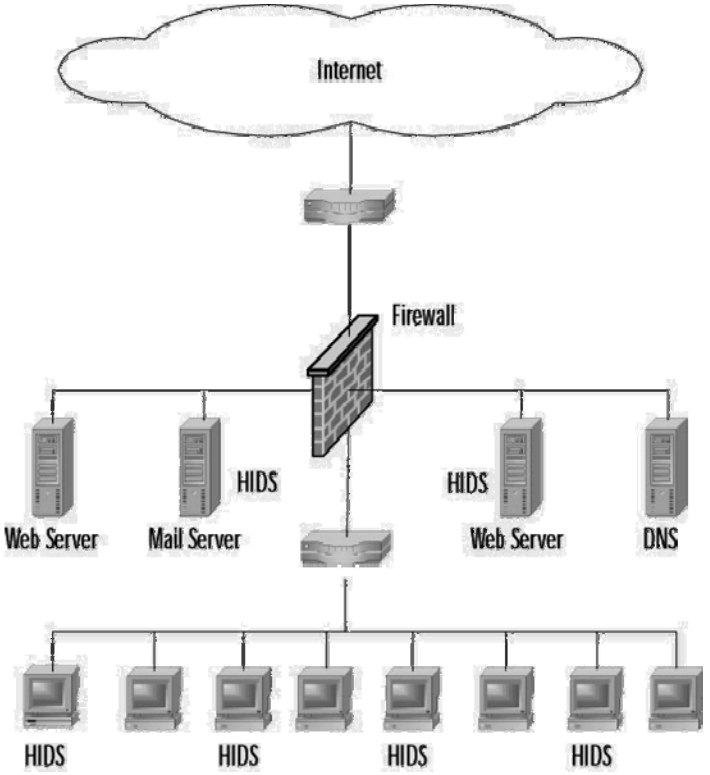
- **Jenis-Jenis**
  - Network IDS
  - Host IDS

IDS (Intrusion Detection System)

- **Networkdk IDS vs Host IDS**



NIDS



HIDS

IDS (Intrusion Detection System)

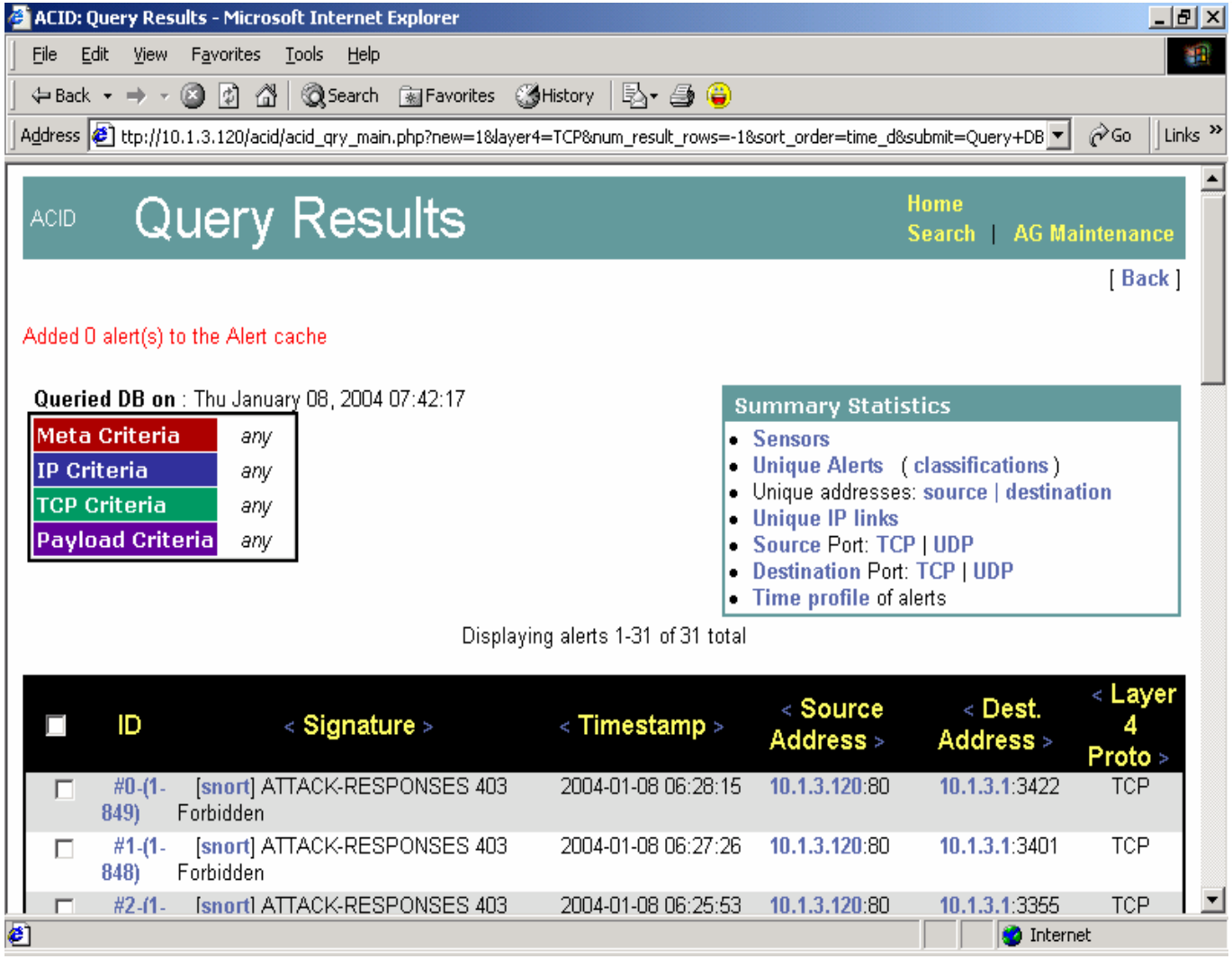
Contoh produk IDS

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

IDS (Intrusion Detection System)

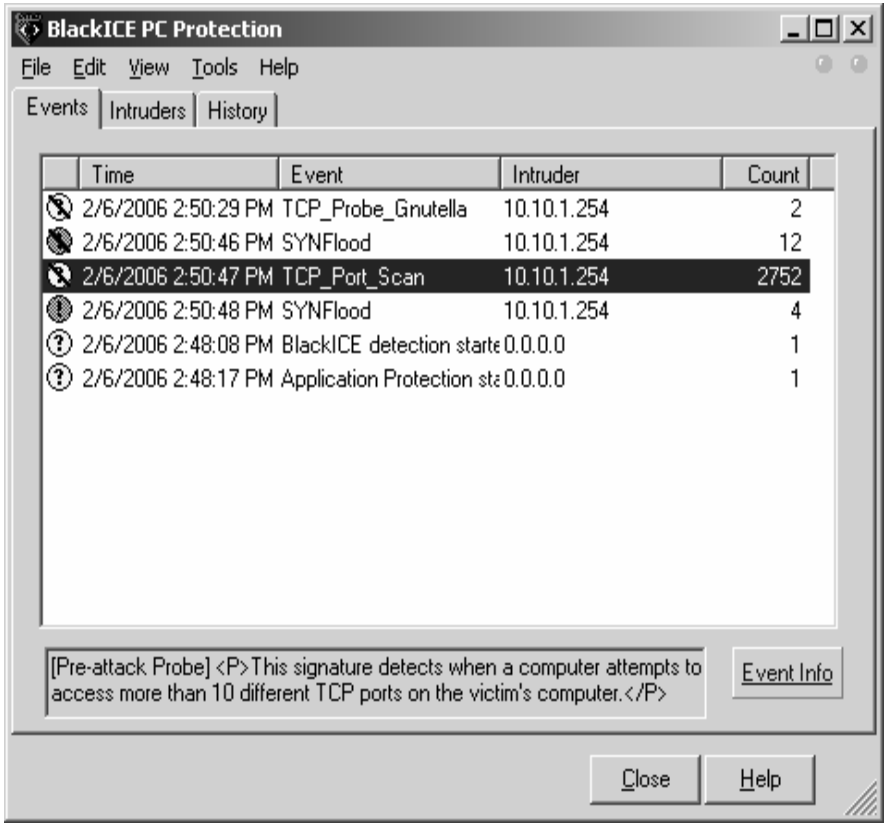
Contoh produk IDS

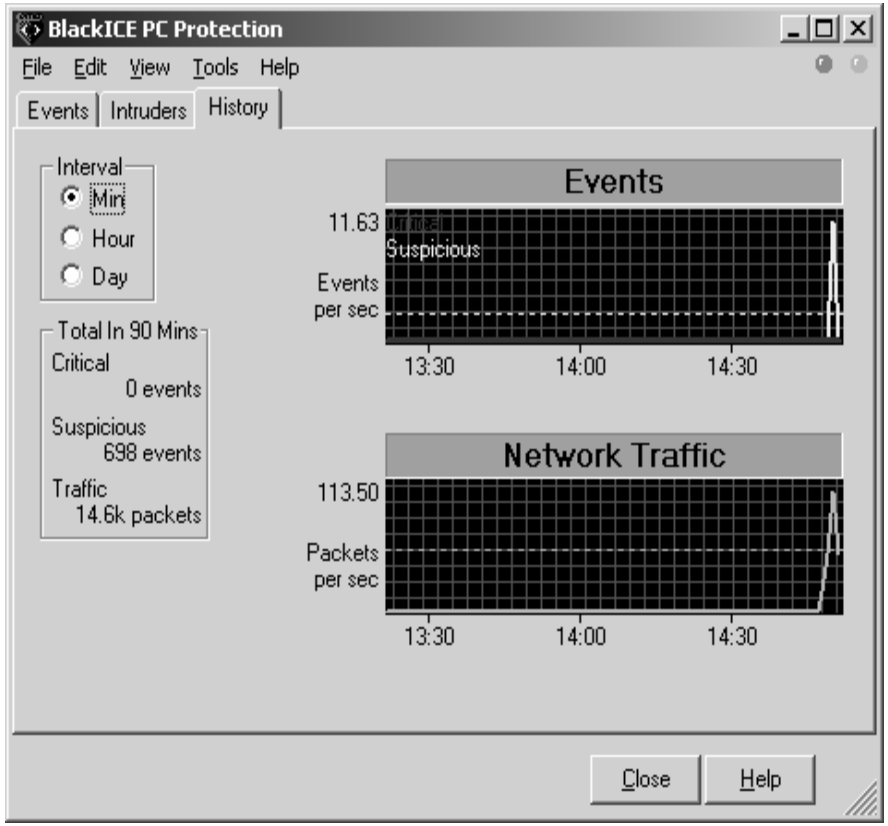
Snort



IDS (Intrusion Detection System)

- Contoh produk IDS : **BlackICE**





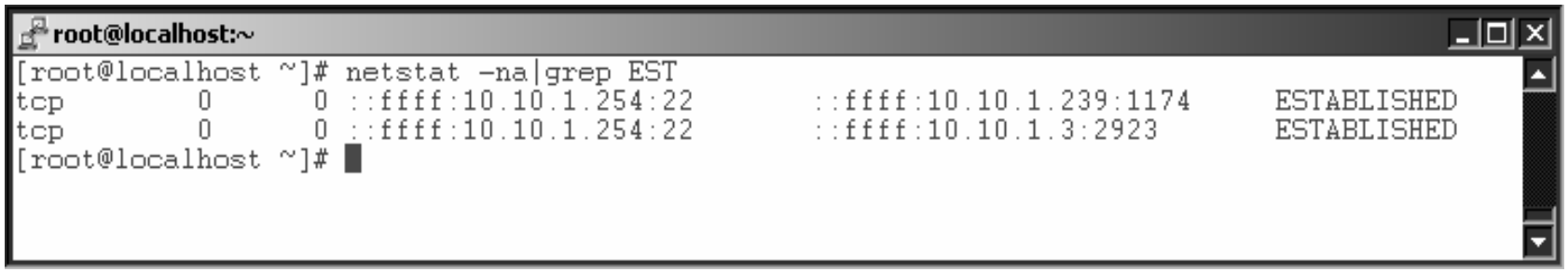
Digital Forensik

- **Digital forensik pasca insiden**
  - Pengecekan koneksi aktif
  - Pengecekan listening port pasca insiden
  - Pengecekan proses yang aktif pasca insiden
  - Pengecekan log user yang login
  - Pengecekan log system
  - Pengecekan log pengakses service
  - Dan lain-lain

- **Penanganan/pemulihan pasca insiden**
  - Pengecekan apakah ada backdoor yang ditanam
  - Installasi ulang sistem
  - Tutup security hole yang ada
  - Perbaiki konfigurasi firewall
  - Dan lain-lain

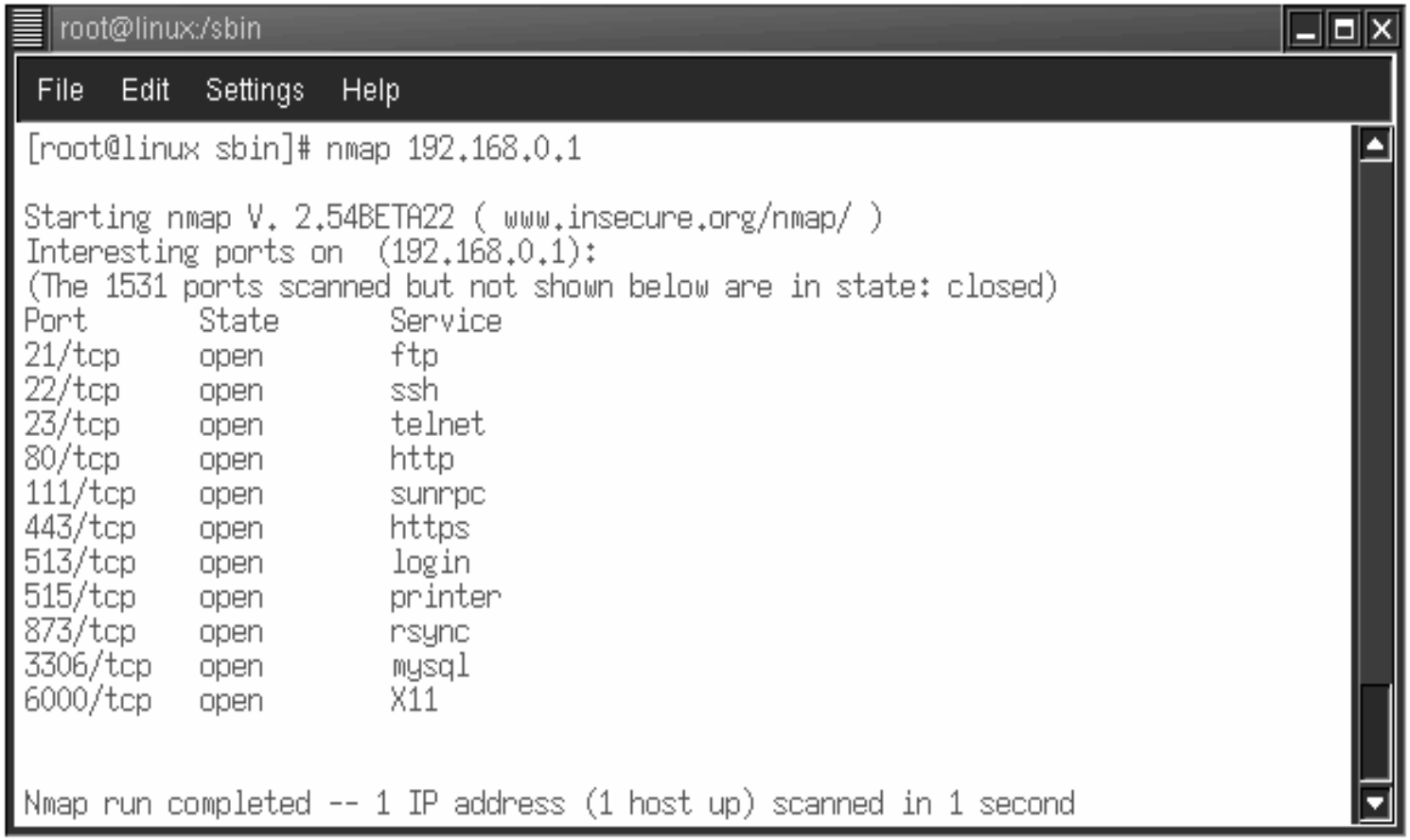
Digital Forensik

- **Pengecekan koneksi aktif**



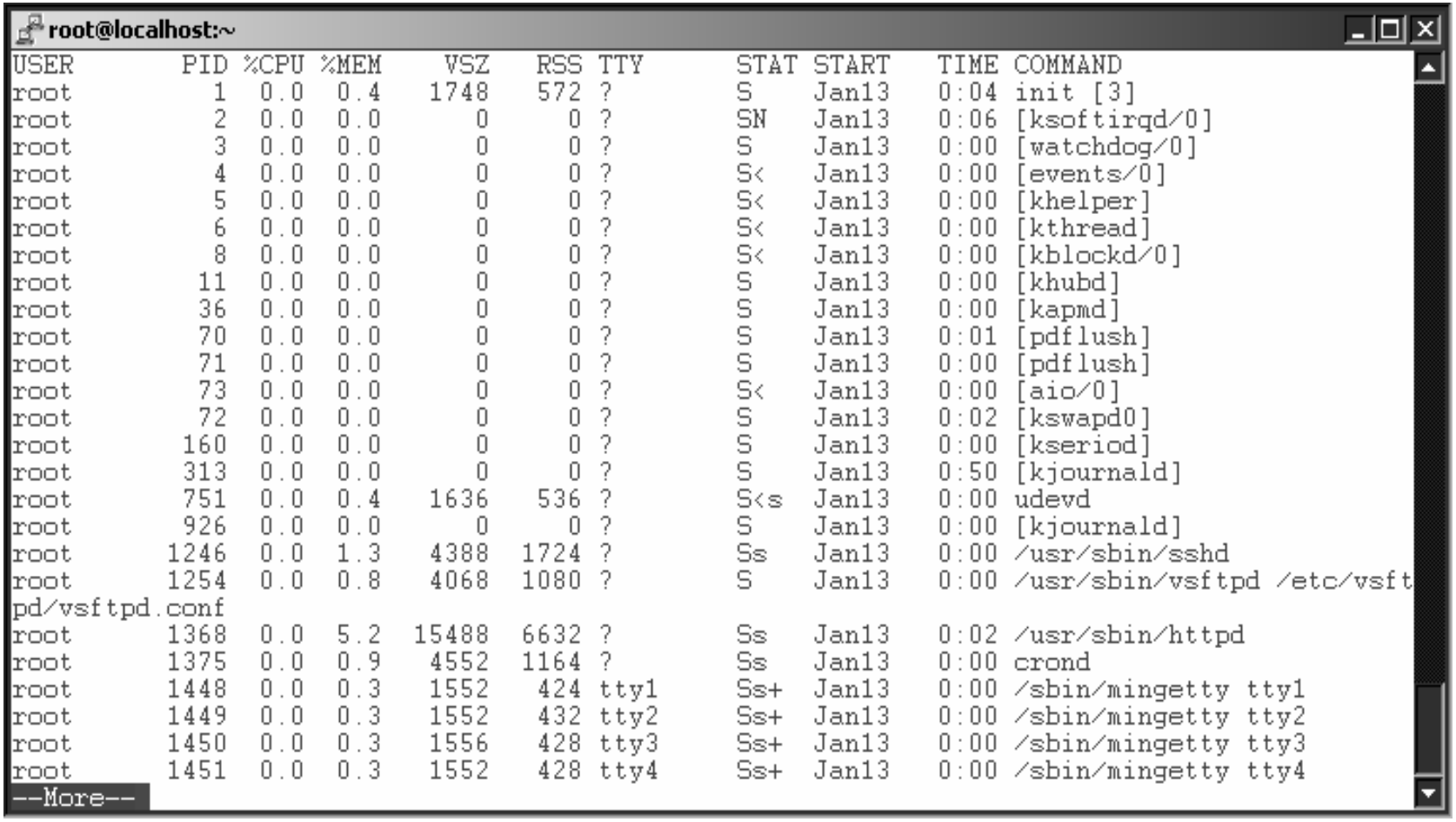
Digital Forensik

- **Koneksi listening port pasca insiden**



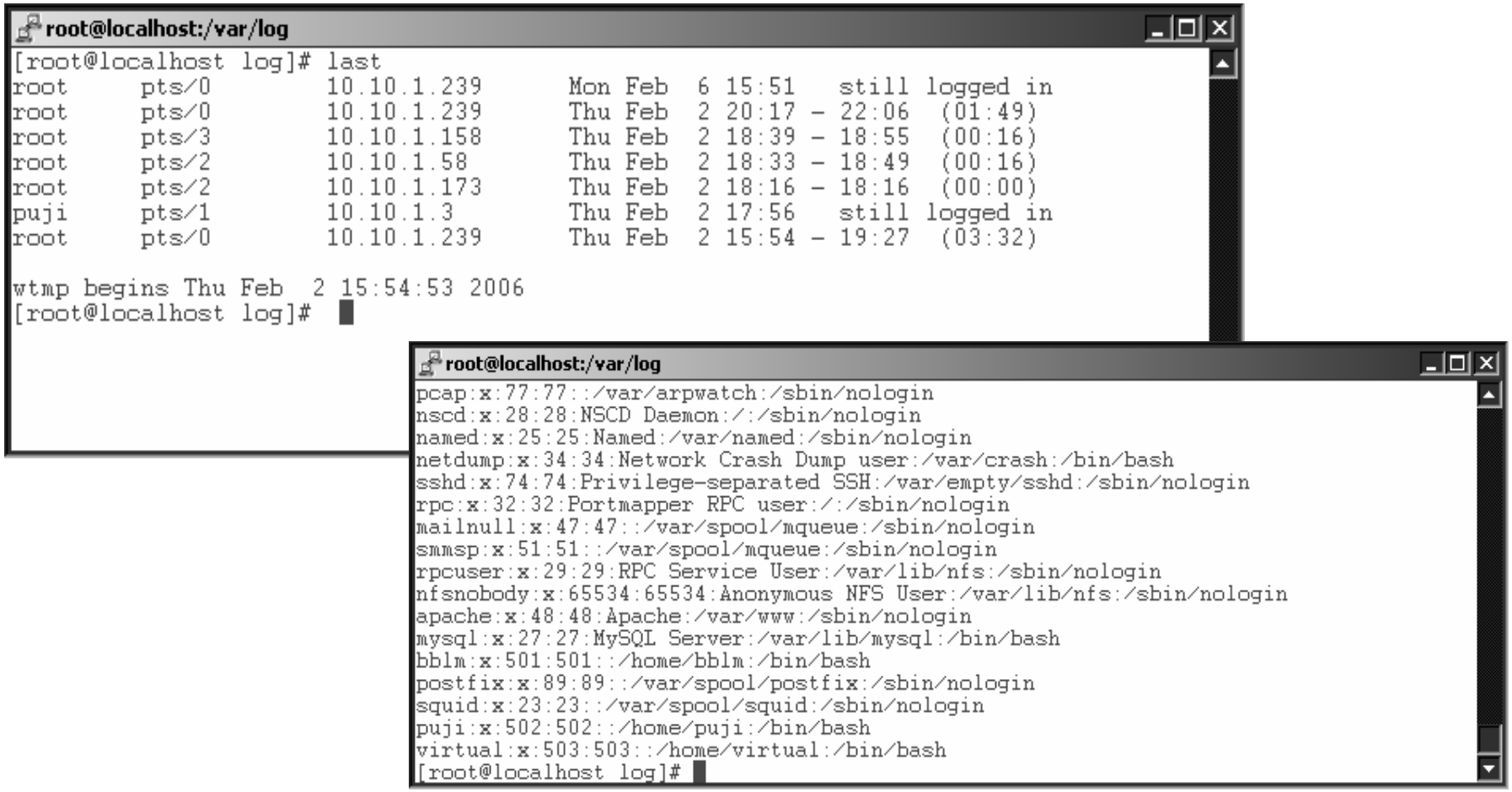
Digital Forensik

- **Pengecekan proses yang aktif pasca insiden**



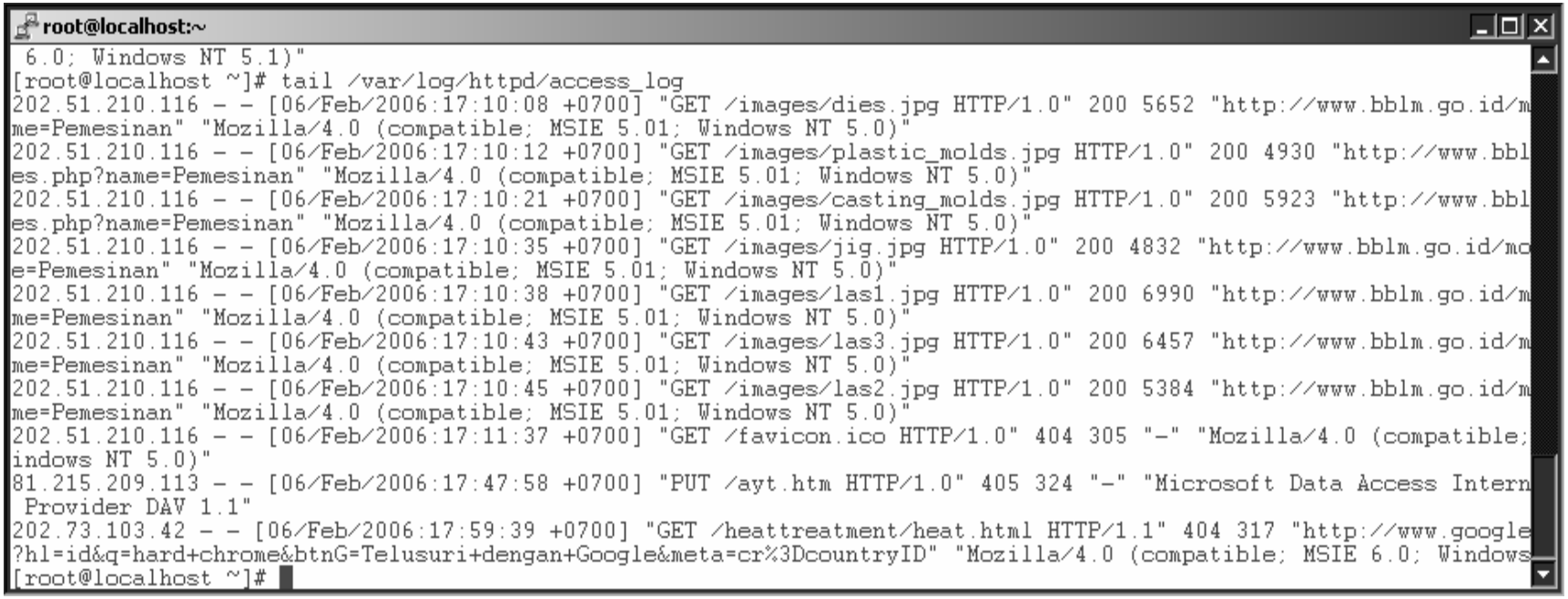
Digital Forensik

- **Pengecekan log user yang login**



Digital Forensik

- **Pengecekan log pengakses service**



Digital Forensik

PENYITAAN DIGITAL EVIDENCE

Analisa Barang Bukti Digital

BERKAS PERKARA

STATUS QUO

ANALISIS DIGITAL EVIDENCE SECARA LABORATORIK KRIMINALISTIK

KLONING

Alt 1 : BB Asli SITA
Alt 2 : Kloning diserahkan & BB asli : SITA

EnCASE IMAGE

+

FAST BLOCK

BAP
LABORATORIS KRIMINALISTIS
DIGITAL EVIDENCES

FORENSIC SOFTWARE ANALISIS

(EnCase, FTK, RunTime Software, dll)

Analisis

BB Digital

Terminologi Cyber Crime

Dalam dokumen konggres PBB ttg The Prevention of Crime and The Treatment of Offlenderes di Havana, Cuba pada tahun 1999 dan di Wina, Austria tahun 2000, menyebutkan ada 2 istilah yang dikenal :

a. ***Cyber crime in a narrow sense*** **is computer crime : *any illegal behaviour directed by means of electronic operation that target the secutity of computer system and the data processed by them.***
*(*Tindakan ilegal apapun yang terarah dengan maksud untuk eksploitasi elektronik yang menargetkan keamanan dari sistem komputer dan data yang telah diolah).

b. ***Cyber crime in a broader sense*** **is *computer related crime* : *any illegal behaviour committed by means on relation to, a computer system offering or system or network, including such crime as illegal possession in, offering or distributing information by means of computer system or network.***
(Tindakan ilegal apapun yang telah dilakukan sehubungan dengan, penawaran sistem komputer atau sistem atau jaringan, mencakup kepemilikan, penawaran atau distribusi informasi ilegal yang ditujukan untuk sistem komputer atau jaringan)

Terminologi Cyber Crime

SUBSTANTIVE CRIMINAL LAW

CONVENTION ON CYBERCRIME - BUDAPEST , 23 NOV 2001

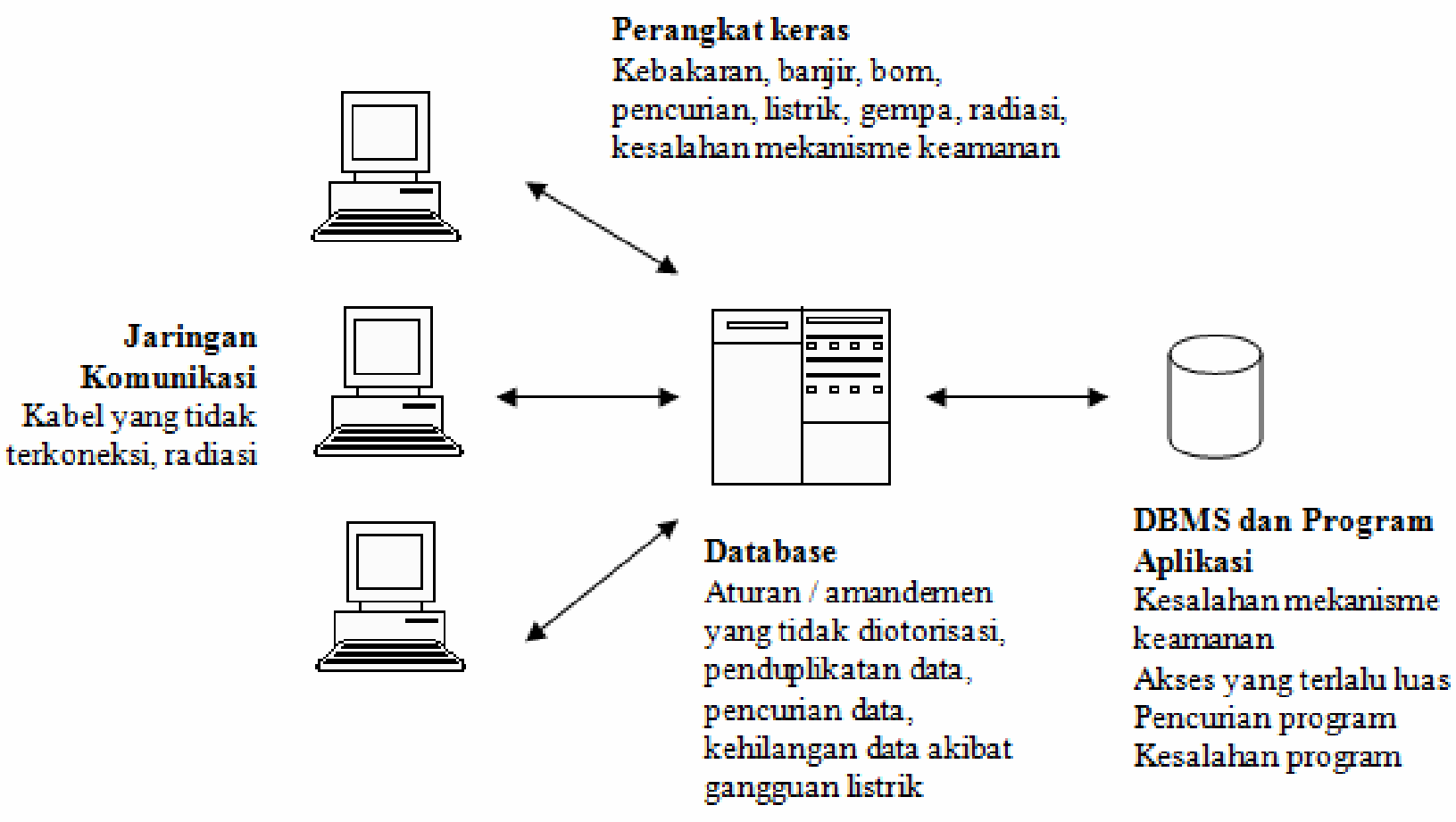
- OFFENCES AGAINST THE CONFIDENTIALITY , INTEGRITY AND AVAILABILITY OF COMPUTER DATA AND SYSTEMS
  - Illegal Access
  - Illegal Interception
  - Data interference
  - System Interference
  - Misuse of Devices
- COMPUTER RELATED OFFENCES
  - Computer related forgery
  - Computer related fraud
- CONTENT RELATED OFFENCES
  - offences related to child pornography
- OFFENCES RELATED TO INFRINGEMENTS OF COPYRIGHT AND RELATED RIGHTS
- ANCILLARY LIABILITY AND SANCTIONS
  - Attempt and aiding or abetting
  - corporate liability
  - Sanctions and measures

KEAMANAN DATABASE

Ancaman terhadap Sistem Database

- Informasi sensitif yang tersimpan di dalam database dapat terbuka (*disclosed*) bagi orang-orang yang tidak diizinkan (unauthorized).
- Informasi sensitif yang tersimpan di dalam database dapat *altered* dengan cara-cara ilegal.
- Informasi sensitif yang tersimpan di dalam database dapat *inaccessible* bagi orang-orang yang diizinkan.
- Mengawasi Sistem operating yang paling rentan diserang

Ancaman terhadap Sistem Database



Ancaman terhadap Sistem Database

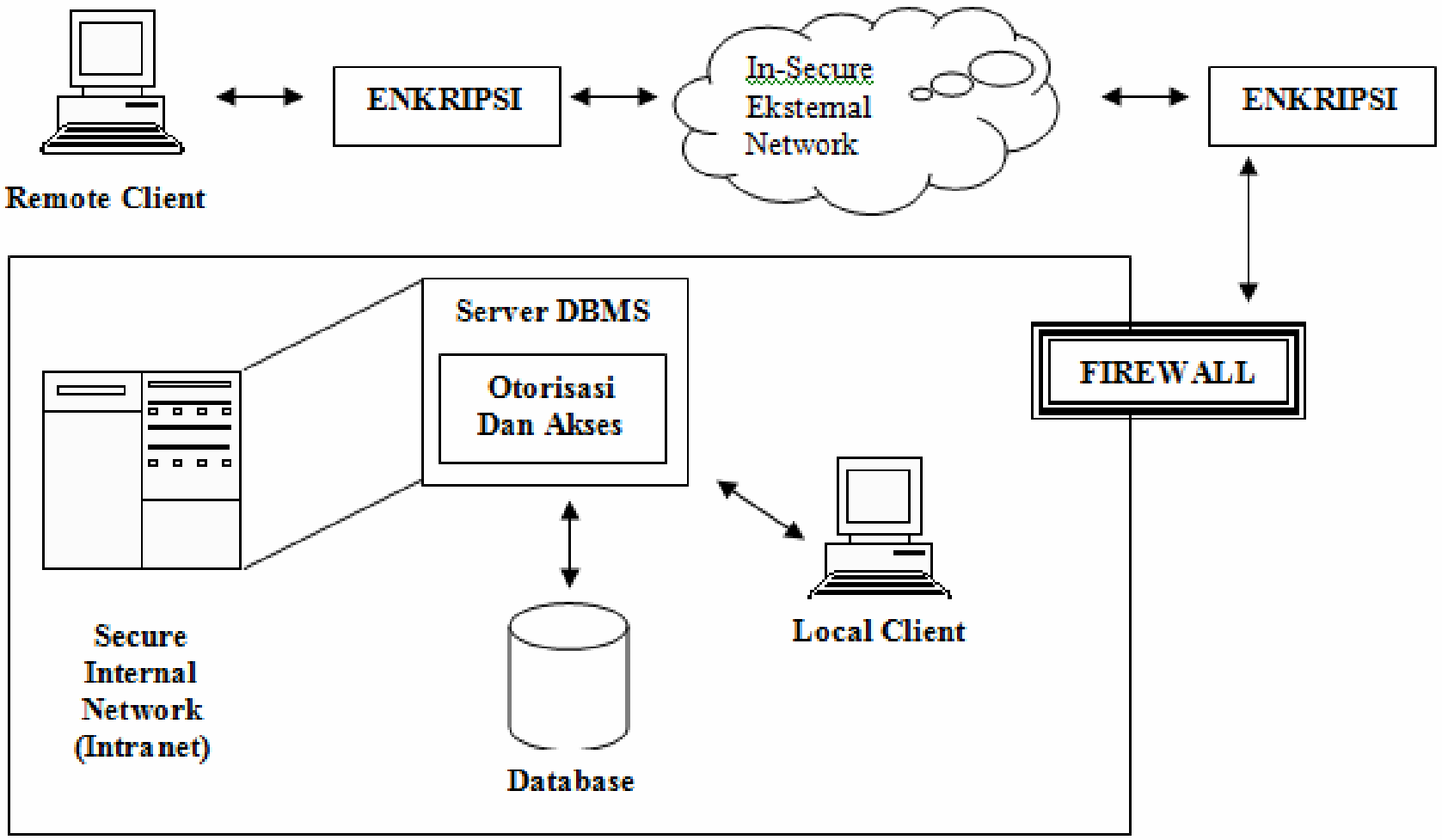
Penyalahgunaan Database

- Tidak disengaja, jenisnya :
  - kerusakan selama proses transaksi
  - anomali yang disebabkan oleh akses database yang konkuren (bersamaan)
  - anomali yang disebabkan oleh pendistribuasian data pada beberapa komputer
  - logika error yang mengancam kemampuan transaksi untuk mempertahankan konsistensi database.
- Disengaja, jenisnya :
  - Pengambilan data / pembacaan data oleh pihak yang tidak berwenang.
  - Pengubahan data oleh pihak yang tidak berwenang.
  - Penghapusan data oleh pihak yang tidak berwenang.

Tingkatan Pada Keamanan Database

- **Fisikal** → lokasi-lokasi dimana terdapat sistem komputer haruslah aman secara fisik terhadap serangan perusak.
- **Manusia** → wewenang pemakai harus dilakukan dengan berhati-hati untuk mengurangi kemungkinan adanya manipulasi oleh pemakai yang berwenang
- **Sistem Operasi** → Kelemahan pada SO ini memungkinkan pengaksesan data oleh pihak tak berwenang, karena hampir seluruh jaringan sistem database menggunakan akses jarak jauh.
- **Sistem Database** → Pengaturan hak pemakai yang baik.

Aktivitas Keamanan Database



Aktivitas Keamanan Database

1. 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 :
- Mengendalikan sistem atau obyek yang dapat diakses
- Mengendalikan bagaimana pengguna menggunakannya
- Sistem administrasi yang bertanggungjawab untuk memberikan hak akses dengan membuat account pengguna.

Aktivitas Keamanan Database

2. 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 :
  - Relasi → pengguna diperbolehkan atau tidak diperbolehkan mengakses langsung suatu relasi
  - View → pengguna diperbolehkan atau tidak diperbolehkan mengakses data yang terapat pada view
  - Read Authorization → pengguna diperbolehkan membaca data, tetapi tidak dapat memodifikasi.
  - Insert Authorization → pengguna diperbolehkan menambah data baru, tetapi tidak dapat memodifikasi data yang sudah ada.
  - Update Authorization → pengguna diperbolehkan memodifikasi data, tetapi tidak dapat menghapus data.
  - Delete Authorization → pengguna diperbolehkan menghapus data.

Aktivitas Keamanan Database

2. Tabel View (Lanjutan)

Untuk Modifikasi data terdapat otorisasi tambahan :

- Index Authorization → pengguna diperbolehkan membuat dan menghapus index data.
- Resource Authorization → pengguna diperbolehkan membuat relasi-relasi baru.
- Alteration Authorization → pengguna diperbolehkan menambah/menghapus atribut suatu relasi.
- Drop Authorization → pengguna diperbolehkan menghapus relasi yang sudah ada.

Aktivitas Keamanan Database

2. Tabel View (Lanjutan)

Contoh pada SQL

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

REVOKE : mencabut wewenang yang dimiliki oleh pemakai
Syntax : REVOKE <priviledge list> ON <nama relasi/view> FROM <pemakai>
Contoh :
REVOKE SELECT ON S TO BUDI
REVOKE SELECT,UPDATE (STATUS,KOTA) ON S TO ALI,BUDI

Aktivitas Keamanan Database

3. Backup data dan recovery :

- **Backup** : proses secara periodik untuk mebuat duplikat ari database dan melakukan logging file (atau program) ke media penyimpanan eksternal.
- **Jurnaling** : proses menyimpan dan mengatur log file dari semua perubahan yang dibuat di database untuk proses recovery yang efektif jika terjai kesalahan.

- **Isi Jurnal :**
  1. **Record transaksi**
     1. Identifikasi dari record
     2. Tipe record jurnal (transaksi start, insert, update, delete, abort, commit)
     3. Item data sebelum perubahan (operasi update dan delete)
     4. Item data setelah perubahan (operasi insert dan update)
     5. Informasi manajemen jurnal (misal : pointer sebelum dan record jurnal selanjutnya untuk semua transaksi
  2. **Record ceckpoint** : suatu informasi pada jurnal untuk memulihkan database dari kegagalan, kalau sekedar redo, akan sulit penyimpanan sejauh mana jurnal untuk mencarinya kembali, maka untuk membatasi pencarian menggunakan teknik ini.

Aktivitas Keamanan Database

3. Backup data dan recovery :

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

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

Aktivitas Keamanan Database

3. Backup data dan recovery :

Teknik Pemulihan :

- **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.
- **Immediate Update / 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.
- **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.

Aktivitas Keamanan Database

- **4. Kesatuan data dan Enkripsi :**
  - Enkripsi : keamanan data
  - Integritas :metode pemeriksaan dan validasi data (metode integrity constrain), yaitu berisi aturan-aturan atau batasan-batasan untuk tujuan terlaksananya integritas data.
  - Konkuren : mekanisme untuk menjamin bahwa transaksi yang konkuren pada database multi user tidak saling menganggu operasinya masing-masing. Adanya penjadwalan proses yang akurat (time stamping).

Selesai dulu untuk hari ini