

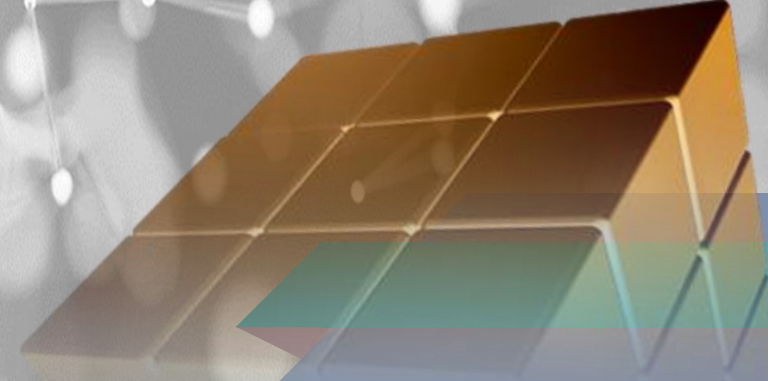


*Syahrul Imardi, MT*

# #4

## PENGANTAR MK KPL (Lanjutan)

KEAMANAN KOMPUTER





STMIK  
Amik Riau



# MATAKULIAH **KEAMANAN PERANGKAT LUNAK**

SYAHRUL IMARDI, M.T

Pertemuan 4 : **KEAMANAN KOMPUTER** (Lanjutan)



# OUTLINE

1. **Pendahuluan**
2. **Ancaman keamanan pada sistem berbasis komputer**
  - Social engineering
  - Keamanan fisik
  - Security hole pada sistem operasi dan servis
  - Serangan pada jaringan
  - DOS attack
  - Serangan via aplikasi berbasis web
  - Trojan, backdoor, rootkit, keylogger
  - Virus, worm
  - Anatomy of A Hack
3. **Hardening System**
  - Hardening System: Security Policy
  - Hardening System: Kriptografi
  - Hardening System: Firewall
  - Hardening System: IDS (Intrusion Detection System)
  - Hardening System: Backup
  - Hardening System: Auditing System
  - Hardening System: Digital Forensik dan Penanganan Pasca Insiden
4. **Ciber Law dan masa depan keamanan**

# PARADIGMA BELAJAR

1

**Dari Tidak Mengerti Menjadi sangat Mengerti**

2

**Dari Tidak Menguasai Menjadi Trampil**

3

**Dari Ugal-ugalan Menjadi Sopan**

4

**Dari Tidak Bisa Bergaul Menjadi Presenter**

Skill &  
Knowledge

Attitude /  
Karakter

# PENDAHULUAN

## □ Mengapa perlu aman?

- Resiko kerugian finansial
- Resiko kerugian kerahasiaan
- Resiko kerugian harga diri
- Dan lain-lain

## □ Motif-motif serangan pada sistem komputer

- Politis
- Finansial
- Dendam (sakit hati)
- Iseng
- Sebagai pekerjaan (cracker bayaran)
- Dan lain-lain

# PENDAHULUAN

## □ Aspek-aspek keamanan

- **Confidentiality**  
Informasi (data) hanya bisa diakses oleh pihak yang memiliki wewenang.
- **Integrity**  
Informasi hanya dapat diubah oleh pihak yang memiliki wewenang.
- **Availability**  
Informasi tersedia untuk pihak yang memiliki wewenang ketika dibutuhkan.
- **Authentication**  
Pihak yang terlibat dengan pertukaran informasi dapat diidentifikasi dengan benar dan ada jaminan bahwa identitas yang didapat tidak palsu.
- **Nonrepudiation**  
Pengirim maupun penerima informasi tidak dapat menyangkal pengiriman dan penerimaan pesan.

# PENDAHULUAN

## □ Aspek-aspek ketidakamanan (serangan)

### ▪ **Interruption**

Suatu aset dari suatu sistem diserang sehingga menjadi tidak tersedia atau tidak dapat dipakai oleh yang berwenang. Contohnya adalah kerusakan/modifikasi terhadap piranti keras atau saluran jaringan.

### ▪ **Interception**

Suatu pihak yang tidak berwenang mendapatkan akses pada suatu aset. Pihak yang dimaksud bisa berupa orang, program, atau sistem yang lain. Contohnya adalah penyadapan terhadap data dalam suatu jaringan.

### ▪ **Modification**

Suatu pihak yang tidak berwenang dapat melakukan perubahan terhadap suatu aset. Contohnya adalah perubahan nilai pada file data, modifikasi program sehingga berjalan dengan tidak semestinya, dan modifikasi pesan yang sedang ditransmisikan dalam jaringan.

### ▪ **Fabrication**

Suatu pihak yang tidak berwenang menyisipkan objek palsu ke dalam sistem. Contohnya adalah pengiriman pesan palsu kepada orang lain.



# PENDAHULUAN

## ❑ Hukum alam keamanan komputer

- Tidak ada sistem yang 100% aman
- Keamanan berbanding terbalik dengan kenyamanan

## ❑ Contoh insiden serangan pada sistem komputer

- Tahun 2004, situs KPU (<http://tnp.kpu.go.id>) dicrak sehingga content situs tersebut berubah
- Tahun 2001, Nasabah klickbca.com disadap identitas accountnya oleh seseorang yang membuat situs mirip (url dan tampilannya) dengan klickbca yang asli
- 10 Maret 1997. Seorang hacker dari Massachusetts berhasil mematikan sistem telekomunikasi di sebuah airport lokal (Worcester, Massachusetts) sehingga mematikan komunikasi di control tower dan menghalau pesawat yang hendak mendarat. Dia juga mengacaukan sistem telepon di Rutland, Massachusetts.
  - <http://www.news.com/News/Item/Textonly/0,25,20278,00.html?pfv>
  - <http://www.news.com/News/Item/0,4,20226,00.html>



# PENDAHULUAN

## □ Beberapa istilah-istilah keamanan komputer

- Hacker
- Cracker
- White hat
- Black hat
- Script kiddies
- Elite
- Vulnerable
- Security hole
- Bug
- Exploit (local, remote)
- Logical Bomb
- Penetration testing
- Dan lain-lain

# ANCAMAN KEAMANAN PADA SISTEM KOMPUTER

## ❑ Ancaman keamanan pada sistem Komputer antara lain:

- Social engineering
- Keamanan fisik
- Security hole pada sistem operasi dan servis
- Serangan pada jaringan
- DOS attack
- Serangan via aplikasi berbasis web
- Trojan, backdoor, rootkit, keylogger
- Virus, worm

## ❑ Anatomy of a hack

Langkah-langkah yang umum digunakan oleh hacker

# SOCIAL ENGINEERING

## ❑ Ancaman

- Mengaku sebagai penanggung jawab sistem untuk mendapatkan account user
- Mengaku sebagai user yang sah kepada pengelola sistem untuk mendapatkan account
- Mengamati user yang sedang memasukkan password
- Menggunakan password yang mudah ditebak
- Dan lain-lain

## ❑ Solusi

Mendidik seluruh pengguna sistem dari level manajer sampai operator akan pentingnya keamanan

# KEAMANAN FISIK

## ❑ Ancaman

- Pembobolan ruangan sistem komputer
- Penyalahgunaan account yang sedang aktif yang ditinggal pergi oleh user
- Sabotase infrastruktur sistem komputer (kabel, router, hub dan lain-lain)
- Dan lain-lain

## ❑ Solusi

- Konstruksi bangunan yang kokoh dengan pintu-pintu yang terkunci
- Pemasangan screen saver
- Pengamanan secara fisik infrastruktur sistem komputer
  - CPU ditempatkan di tempat yang aman
  - Kabel → direl
  - Router, hub → ditempatkan yang aman dari jangkauan
- Dan lain-lain

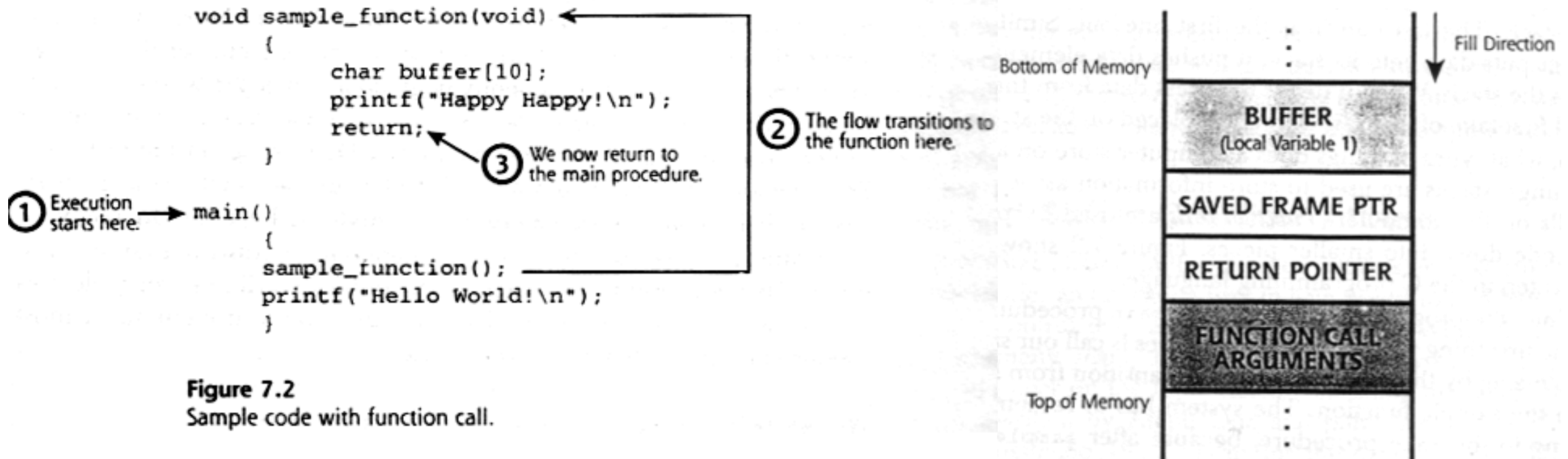
# SECURITY HOLE PADA OS DAN SERVIS

## □Ancaman

- Buffer over flow yang menyebabkan local/remote exploit
- Salah konfigurasi
- Instalasi default yang mudah diexploit
- Dan lain-lain

# BUFFER OVERFLOW (1)

❑ Mengapa bisa terjadi buffer over flow?



# BUFFER OVERFLOW (2)

```
void sample_function(char *string)
```

```
{
```

```
    char buffer[16];
```

```
    strcpy(buffer, string);
```

```
    return;
```

```
}
```

```
void main()
```

```
{
```

```
    char buffer[256];
```

```
    int i;
```

```
    for(i=0; i<255; i++)
```

```
        big_buffer[i]='A';
```

```
    sample_function(big_buffer);
```

```
}
```

④ The local variable "buffer" can hold 16 characters.

⑤ The strcpy function will load characters into buffer until it finds the end of the string... but the string is far longer than the buffer!

① Make a buffer that can hold 256 characters.

② Shove the character 'A' into big\_buffer... 255 times!

③ Send the big buffer to the function.

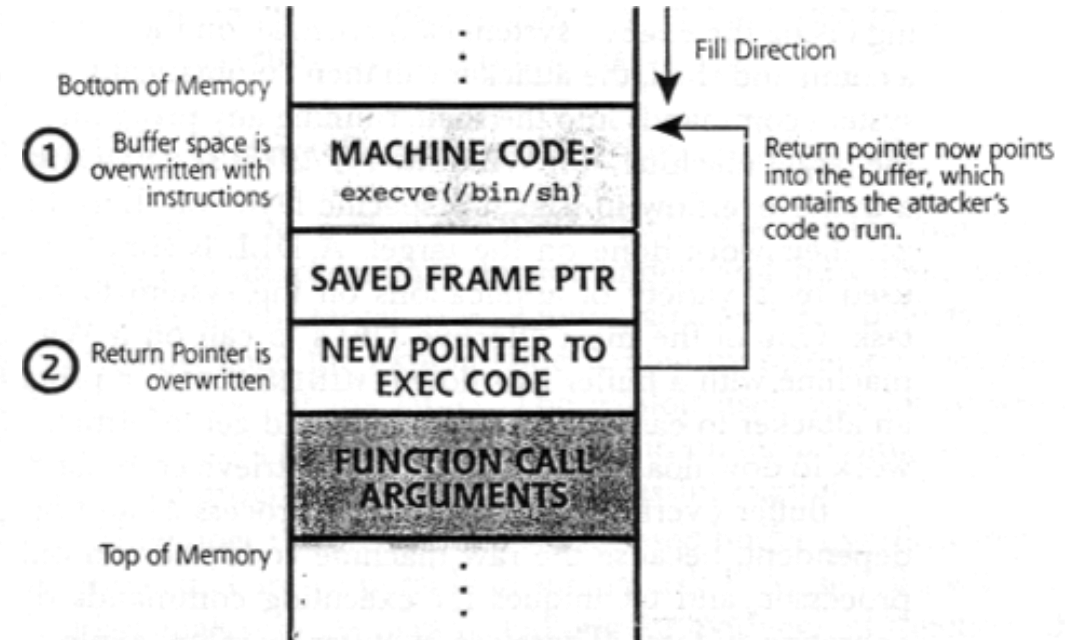


Figure 7.4  
Buffer overflow sample program.



# BUFFER OVERFLOW (3)

## □ Pencegahan

### ■ Sisi Programmer:

Coding dengan teliti dan sabar sehingga kemungkinan kekeliruan coding yang menyebabkan buffer over flow dapat dihindari

### ■ Sisi User

- Selalu mengikuti informasi bug-bug melalui milis dan situs-situs keamanan (Securityfocus.com dan lain-lain)
- Update..update...dan update!

# KESALAHAN KONFIGURASI

## ❑ Ancaman

- Sistem dapat diakses dari host yang tidak berhak
- *Privilege* yang dapat dieksploitasi
- Dan lain-lain

## ❑ Pencegahan

- Pengaturan hak akses host yang ketat
- Pengaturan *privilege* yang ketat
- Dan lain-lain

# INSTALLASI DEFAULT

## ❑ Ancaman

- Servis yang tidak diperlukan memakan *resource*
- Semakin banyak servis semakin banyak ancaman karena bug-bug yang ditemukan
- Servis-servis jaringan membuka port komunikasi
- Password default diketahui oleh khalayak
- Sample program dapat dieksploitasi
- Dan lain-lain

## ❑ Pencegahan

- Nyalakan servis yang diperlukan saja
- Konfigurasikan seaman mungkin
- Buang semua yang tidak diperlukan setelah instalasi
- Dan lain-lain

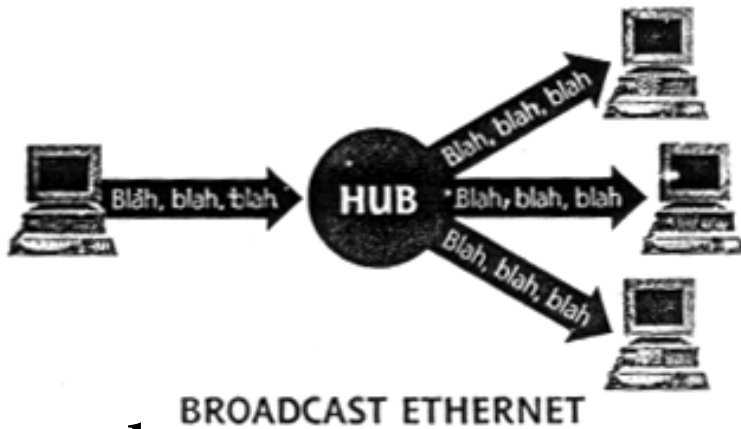
# ANCAMAN SERANGAN MELALUI JARINGAN

## □ Ancaman

- Sniffing (penyadapan)
- Spoofing (pemalsuan)
- Session hijacking (pembajakan)
- DOS attack
- Dan lain-lain

# SNIFFING

## ❑ Bagaimana Sniffing terjadi?



Sniffer mengubah mode ethernet untuk mendengarkan seluruh paket data pada jaringan yang menggunakan hub sebagai konsentrator

## ❑ Pencegahan

- Enkripsi (SSL, SSH, PGP, dan lain-lain)
- Penggunaan switch sebagai pengganti hub

# SPOOFING (PEMALSUAN)

## □ Jenis-jenis spoofing

- IP
- MAC address
- DNS
- Routing

## □ Pencegahan

- Implementasi firewall dengan benar
- Patch yang mencegah prediksi *sequence number*
- Mengeset router agar tidak bisa dilewatkan kecuali melalui rute yang telah ditentukan
- Dan lain-lain

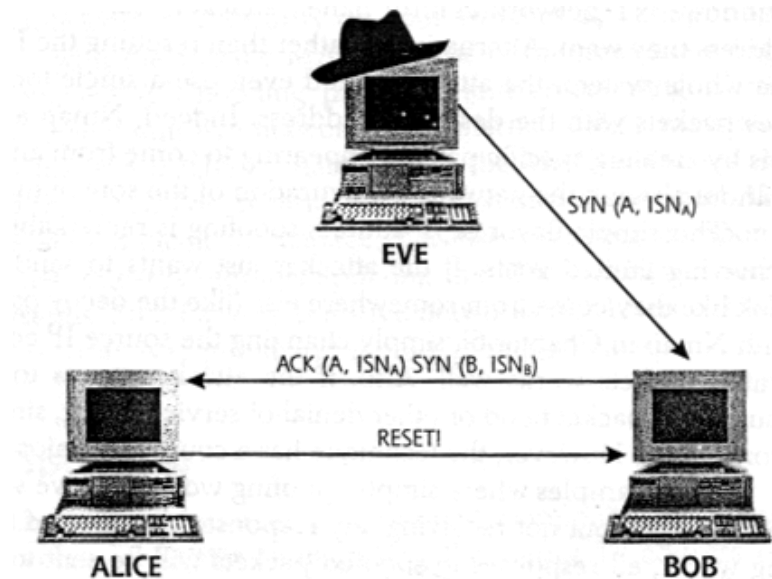


Figure 8.13

The TCP three-way handshake inhibits simple spoofing.

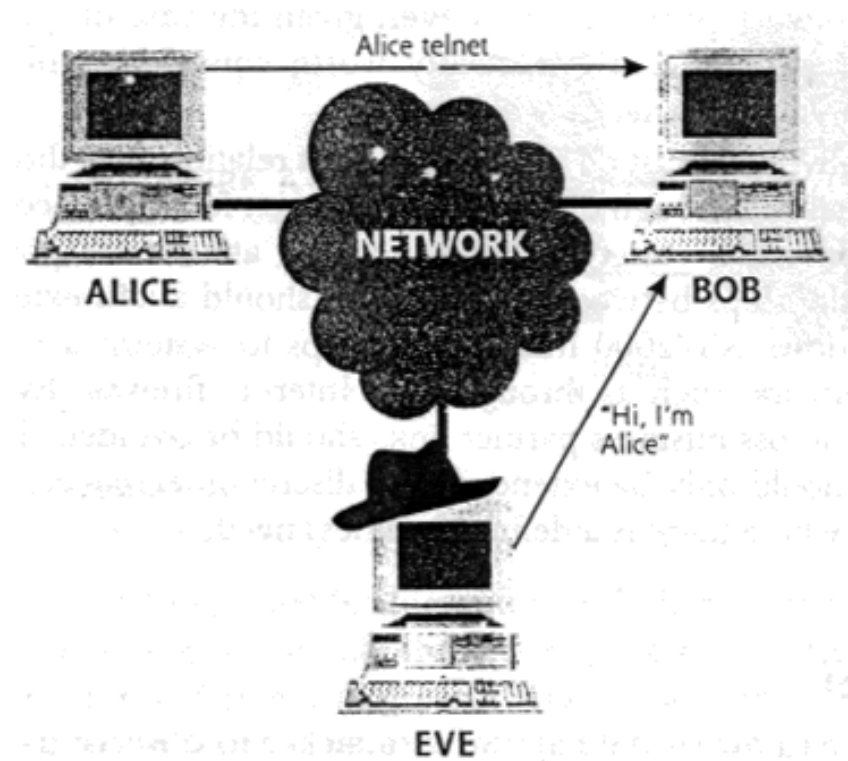
# SESSION HIJACKING (PEMBAJAKAN)

## □ Bagaimana Session Hijacking terjadi?

- Sniff
- Prediksi *sequence number*
- Spoof IP/MAC address

## □ Pencegahan

- Cegah sniffing
- Cegah spoofing





# DOS ATTACK(1)

## □DOS (Denial of Service)

Servis tidak mampu melayani sebagaimana mestinya

## □Jenis-jenis DOS Attack

- Mematikan servis secara local/remote
- Menguras resource: hardisk, memory, prosessor, bandwidth

# DOS ATTACK (2)

## ❑ Ancaman mematikan servis secara local

- Membunuh proses pada servis
- Mengubah konfigurasi servis
- Meng*crash*kan servis
- Dan lain-lain

## ❑ Pencegahan

- Patch terbaru
- Pengaturan *privilege* user dengan tepat
- Deteksi perubahan dengan program *integrity-checking*

# DOS ATTACK (3)

## ❑ Ancaman mematikan servis secara *remote*

- Mengirimkan *malformed* packet TCP/IP ke korban
- Spoofing
- Dan lain-lain

## ❑ Pencegahan

- Implementasi patch terbaru
- Cegah spoofing
- Dan lain-lain

# DOS ATTACK (4)

## ❑ Ancaman menguras resource secara local

- Menciptakan proses secara paralel
- Menulis file ke sistem
- Mengirimkan paket ke host lain
- Dan lain-lain

## ❑ Pencegahan

- Pengaturan *privilege* dengan tepat
- Penggunaan resource yang cukup untuk sistem yang sensitif
- Penggunaan bandwidth yang cukup
- Dan lain-lain

# DOS ATTACK (5)

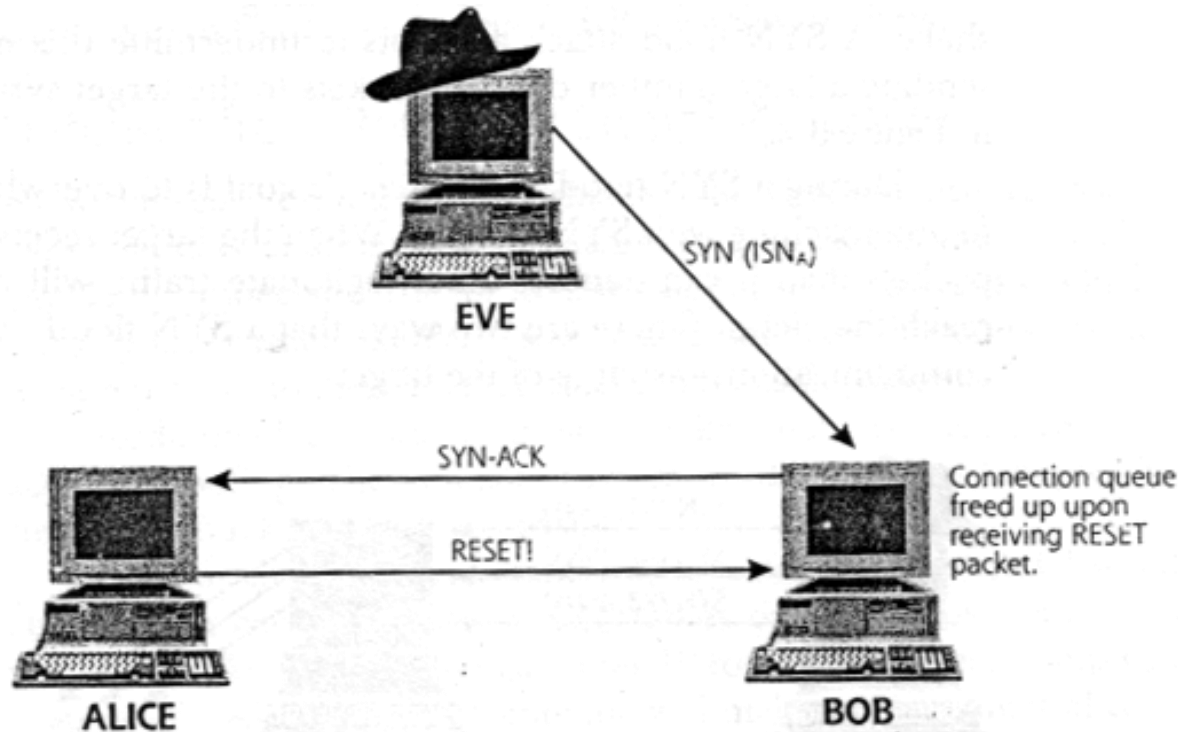
## □ Ancaman menguras resource secara remote

- Teknik Syn flood
- Teknik Smurf attack
- Teknik DDOS (Distributed DOS)
- Dan lain-lain

# DOS ATTACK (6)

## ❑ Ancaman SYN Flood

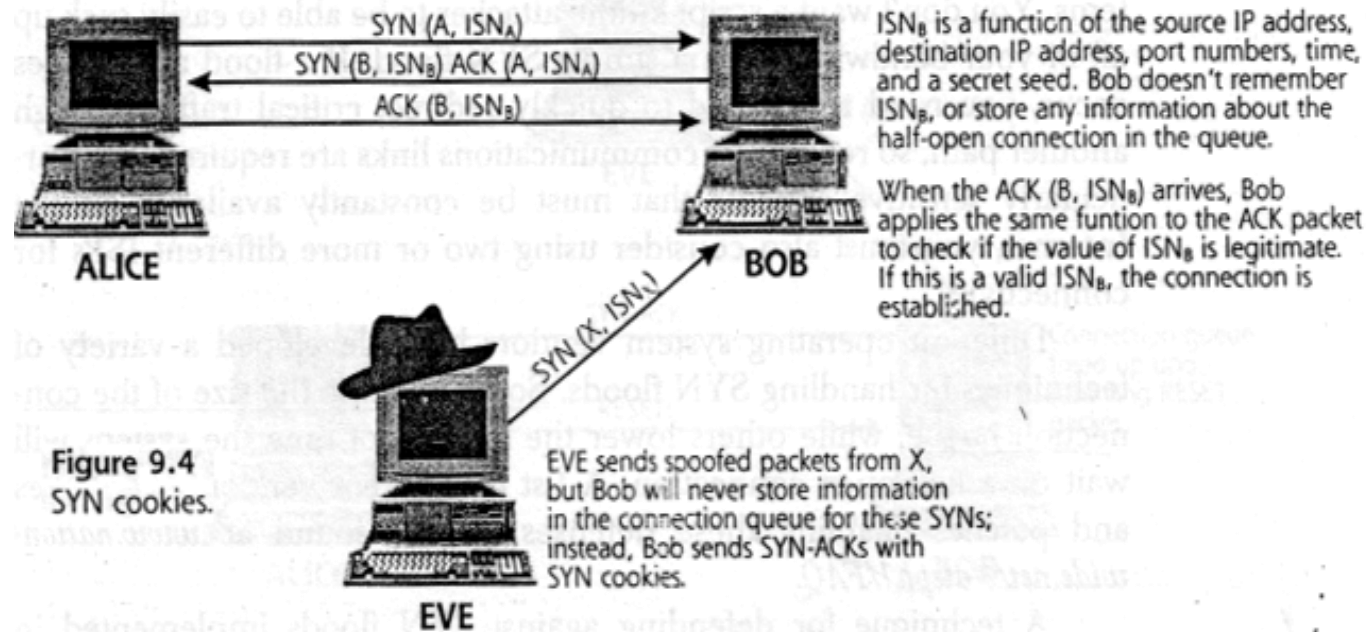
- Korban mengalokasikan memori untuk mengingat *sequence number* tiap paket data yang datang sampai *expired time* nya terlampaui
- Jaringan dipadati paket sampah



# DOS ATTACK (7)

## □ Pencegahan SYN Flood

- Pengalokasian *bandwidth* yang cukup
- Gateway/ISP cadangan
- Meningkatkan kemampuan jumlah antrian koneksi
- Perkecil *timeout* paket data
- Mengaktifkan SYN Cookies (Linux)





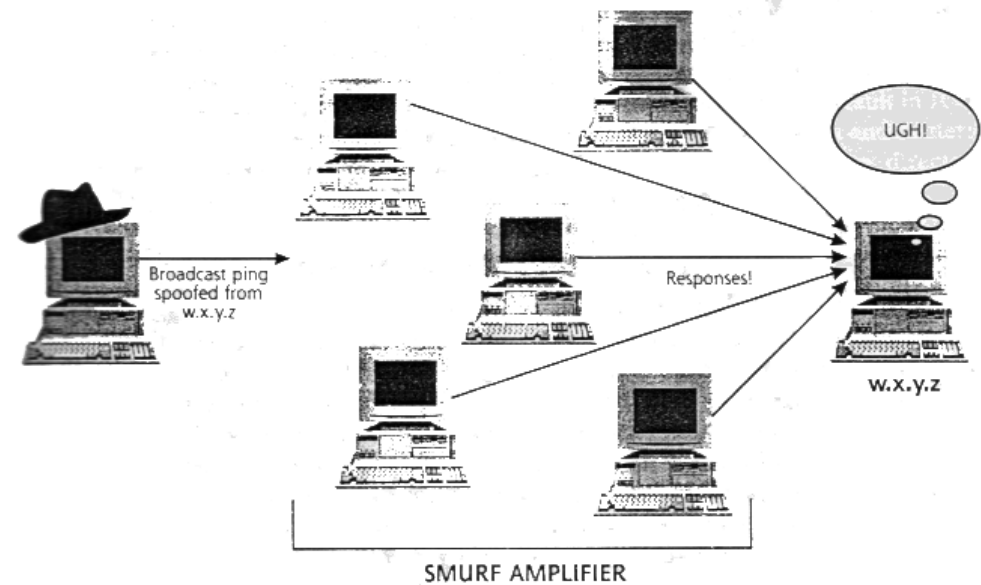
# DOS ATTACK (8)

## ❑ Ancaman Smurf attack

- Pengiriman paket spoof ke alamat broadcast
- Flooding paket ICMP
- Flooding paket UDP
- Dan lain-lain

## ❑ Pencegahan

- Bandwidth yang cukup
- Pemasangan firewall dengan benar
- Dan lain-lain



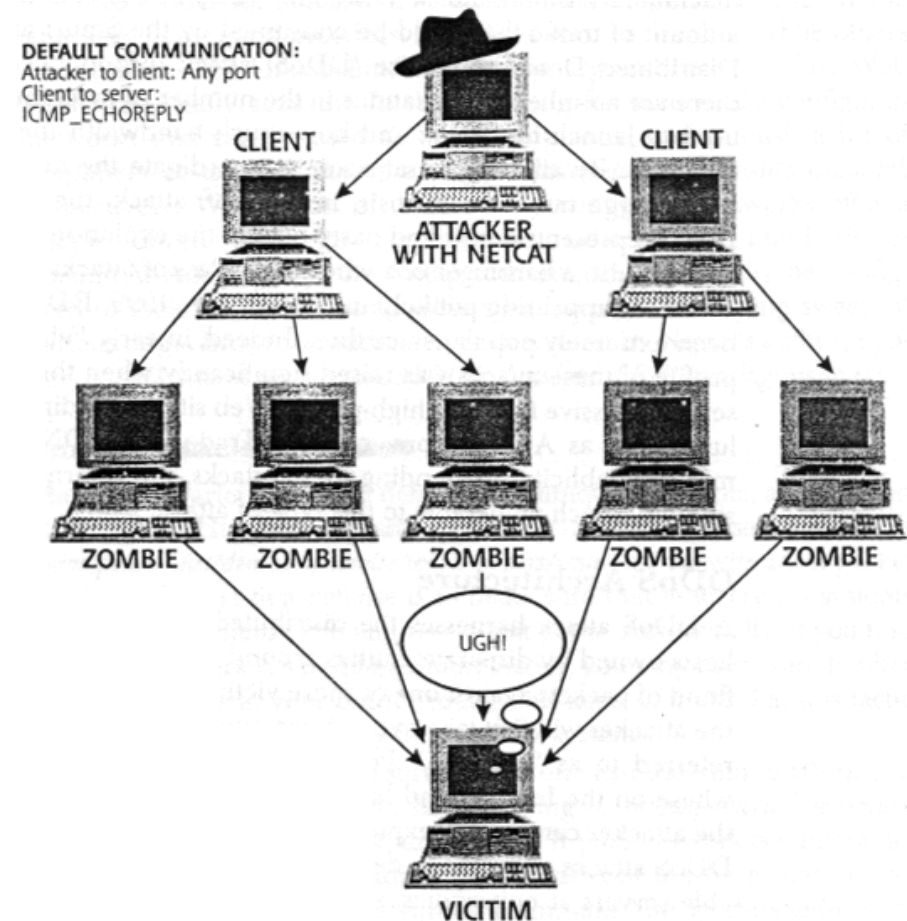
# DOS ATTACK (9)

## ❑ Ancaman DDOS (Distributed DOS)

Serangan DOS secara simultan dari banyak host

## ❑ Pencegahan

- Implementasikan patch terbaru
- Deteksi DDOS tools pada sistem
- Pemasangan firewall dengan benar
- Gateway/ISP cadangan
- Pemasangan IDS untuk deteksi DDOS
- Dan lain-lain



# ANCAMAN VIA APLIKASI BERBASIS WEB (1)

## □ Ancaman

- Serangan untuk mendapatkan account
- SQL injection
- Session hijacking
- Dan lain-lain

# ANCAMAN VIA APLIKASI BERBASIS WEB (2)

## ❑ Ancaman serangan account

- Analisa manajemen account untuk mendapatkan account
- Brute force attack
- Dan lain-lain

## ❑ Pencegahan

- Desain dan coding yang aman
- Mendisable pesan error sistem dan aplikasi yang tidak perlu
- Sanitasi nilai input dengan baik di sisi server
- Dan lain-lain

# ANCAMAN VIA APLIKASI BERBASIS WEB (3)

## ❑ Ancaman serangan SQL injection

Contoh:

- Query pada aplikasi database

```
select * from user where id=$id;
```

- Penyerang memasukan nilai variabel "id" dengan query yang "diinginkan"

```
$id=212; select * from admin
```

- Query akhir menghasilkan 2 buah query

```
select * from users where id=212;
```

```
select * from admin;
```

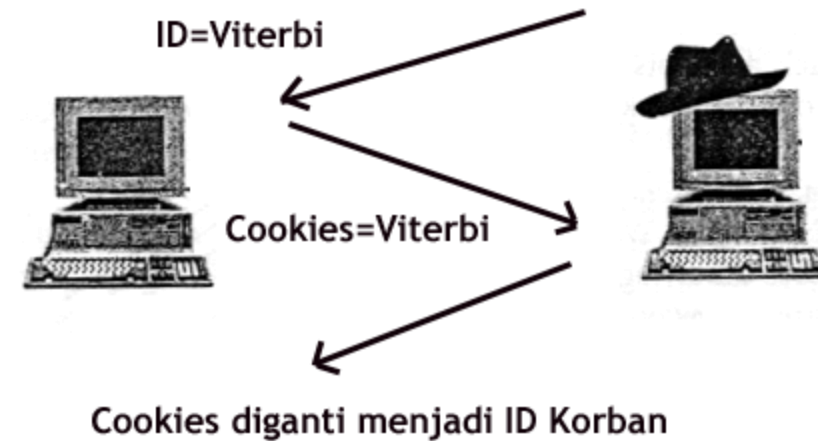
## ❑ Pencegahan

- Sanitasi nilai input dengan baik di sisi server

# ANCAMAN VIA APLIKASI BERBASIS WEB (4)

## ❑ Ancaman session hijacking

- HTTP adalah stateless
- Eksploitasi session



## ❑ Pencegahan

- Menggunakan session yang sulit ditebak, misalnya menyertakan id dan password
- Enkripsi nilai session

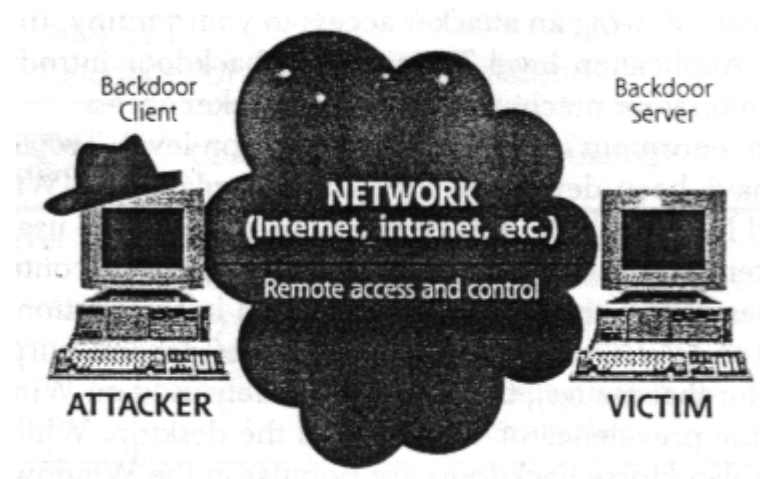
# BACKDOOR, TROJAN, ROOTKIT, KEYLOGGER

## ❑ Ancaman

- Penanaman trojan pada software-software gratisan dari internet dan CD bajakan
- Sistem dapat dikendalikan secara remote

## ❑ Pencegahan

- Gunakan scanner dengan database terbaru
- Jangan menginstall program yang belum dikenal betul
- Mendidik user tentang keamanan komputer





# VIRUS, WORM

## ❑ Ancaman

- Kerusakan, kehilangan data
- Menguras resource sistem (memory, prosessor, hardisk, bandwidth)
- Mengganggu/merusak sistem
- Dan lain-lain

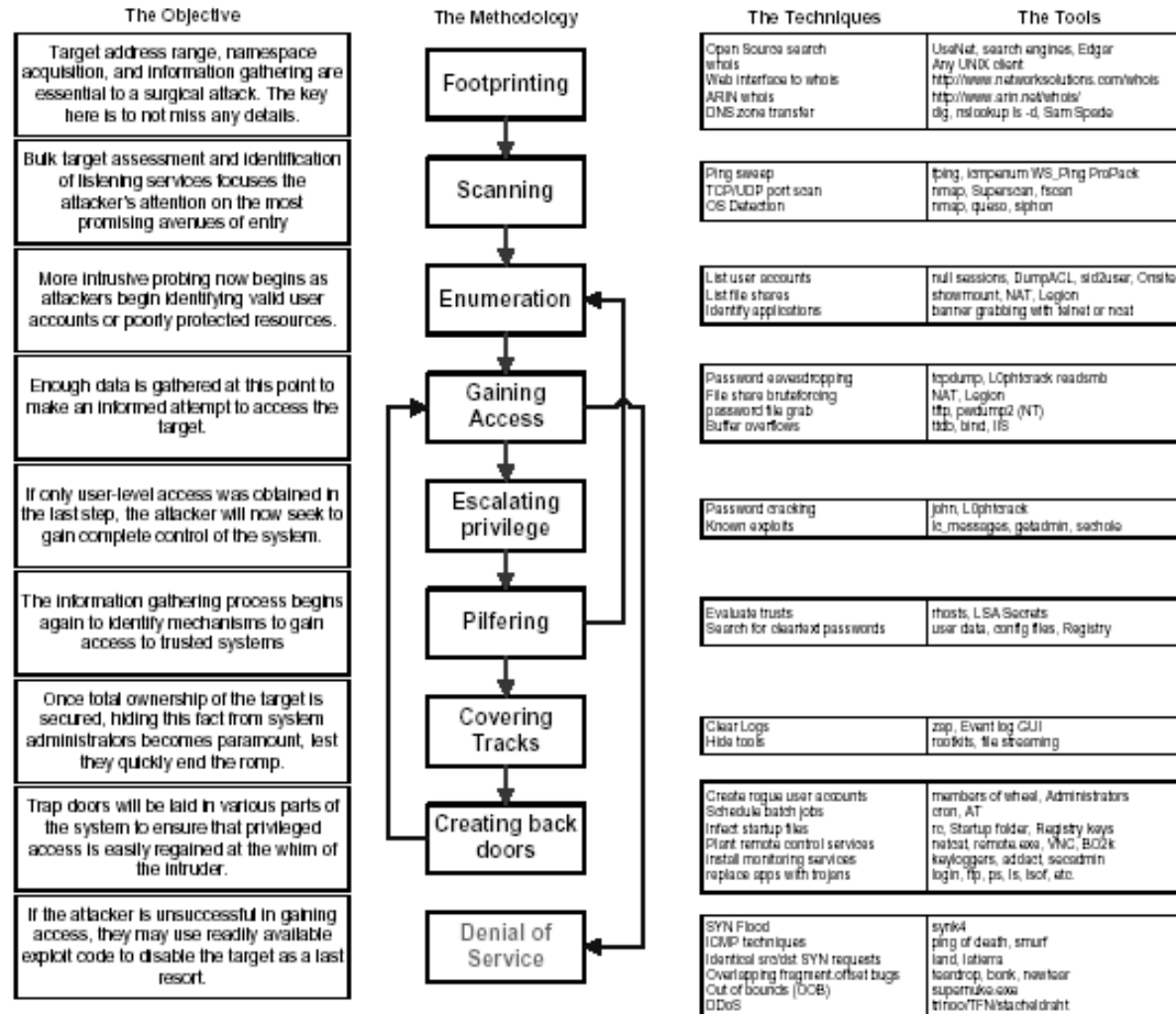
## ❑ Pencegahan

- Gunakan scan virus dengan database terbaru
- Jangan menginstall program yang belum dikenal betul
- Mendidik user tentang keamanan komputer
- Dan lain-lain

# ANATOMY OF A HACK

*“The only way to stop a hacker is to think like one”*

(Taken from “Network Hack Proofing Your Internet Tradedcraft”)



# SISTEM HARDENING

- Hardening System: Security Policy
- Hardening System: Kriptografi
- Hardening System: Firewall
- Hardening System: IDS (Intrusion Detection System)
- Hardening System: Backup
- Hardening System: Auditing System
- Hardening System: Digital Forensik dan Penanganan Pasca Insiden

# SECURITY POLICY

## ❑ Policy penggunaan komputer

- Tidak boleh meminjamkan account kepada orang lain
- Tidak boleh mengambil/menaruh file dari komputer kantor, dll

## ❑ Policy penggunaan Instalasi program

- Tidak boleh menginstall program tanpa seijin staff IT
- Tidak boleh menginstall program ilegal, dll

## ❑ Policy penggunaan Internet

- Tidak boleh menggunakan internet untuk kegiatan carding, hacking dkk
- Tidak boleh menggunakan internet untuk mengakses situs-situs yang berpotensi menyebarkan virus, dll

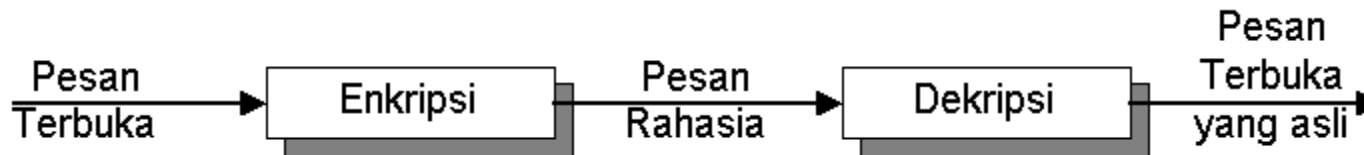
## ❑ Policy penggunaan Email

- Tidak boleh menggunakan email kantor untuk kegiatan milis, dll

# CRYPTOGRAFI (1)

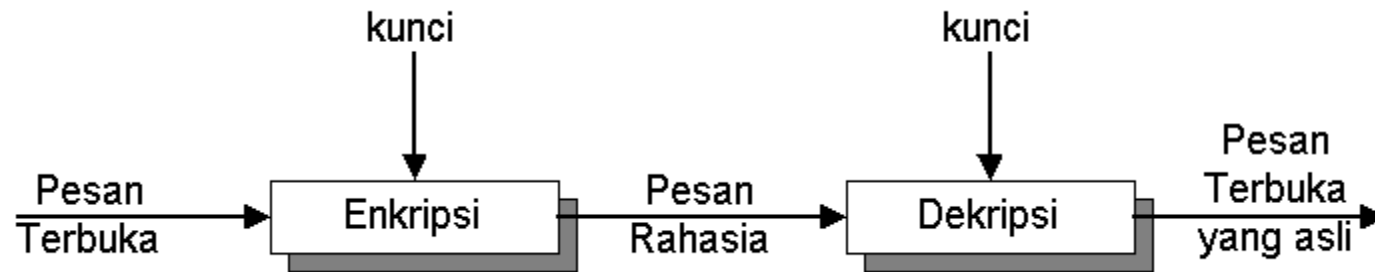
❑ Kriptografi (cryptography) adalah ilmu dan seni menyimpan suatu pesan secara aman

❑ Enkripsi dan Dekripsi

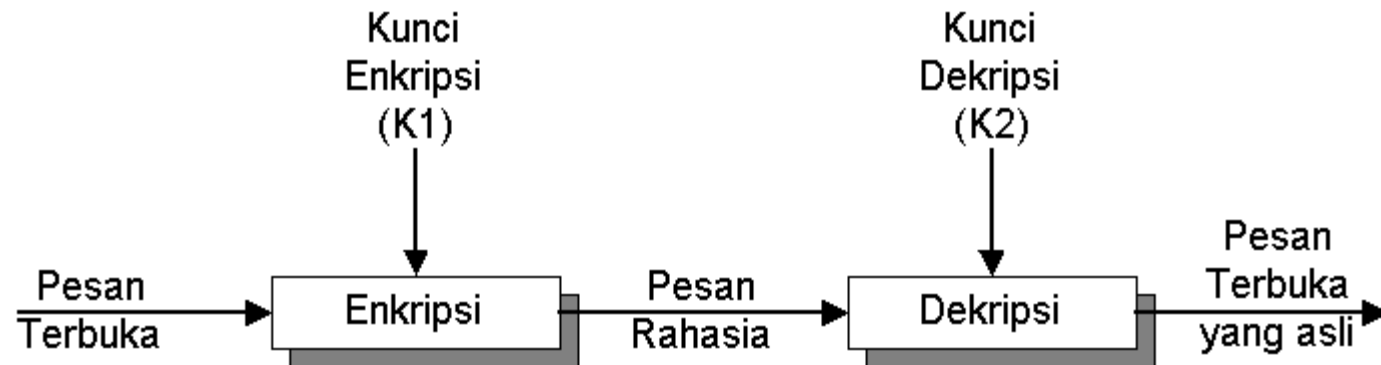


# CRYPTOGRAFI (2)

## ❑ Cryptografi Symetric

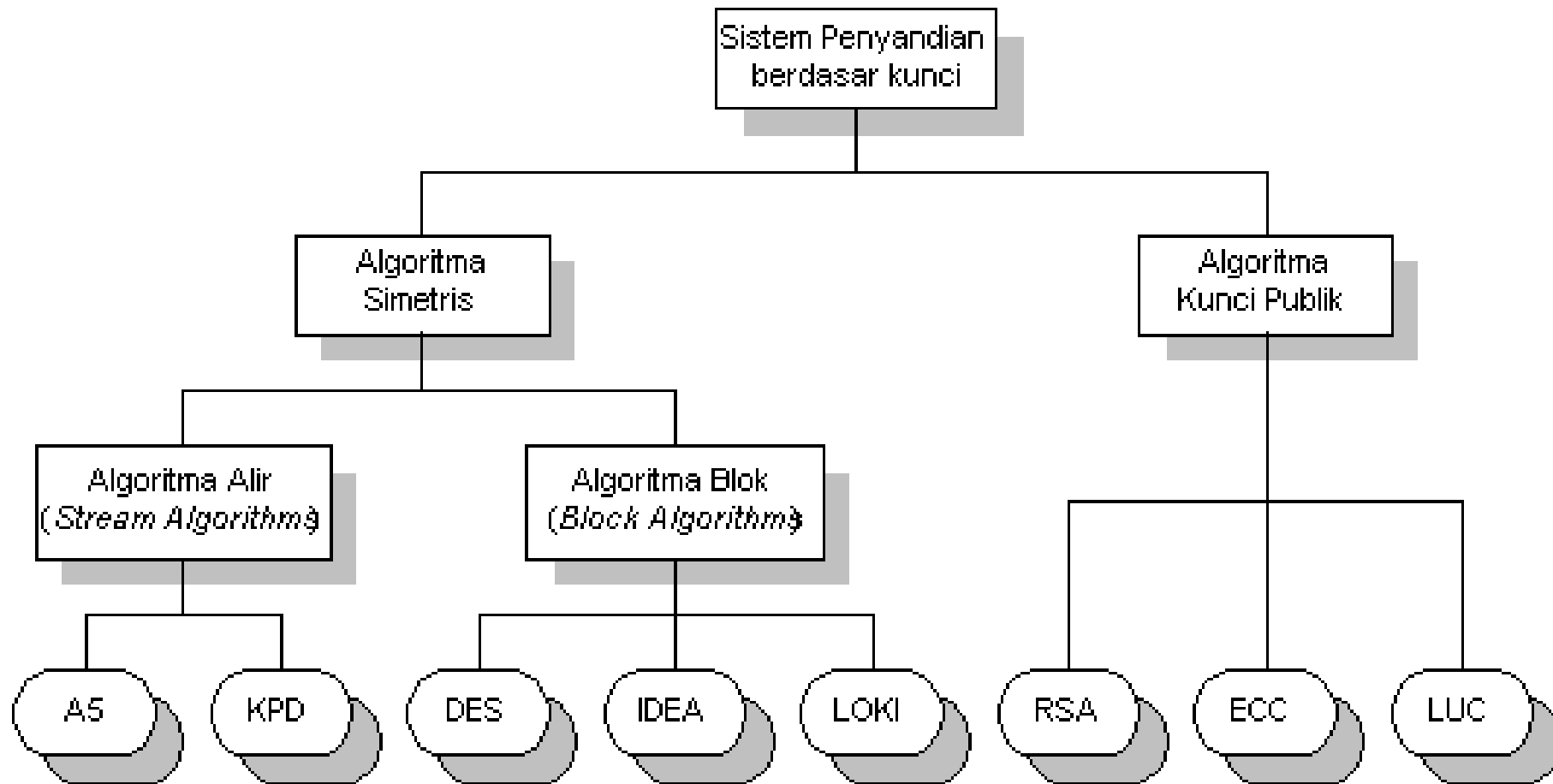


## ❑ Cryptografi Asymetric



# CRYPTOGRAFI (3)

□ Pembagian sistem kriptografi berdasarkan kunci



# CRYPTOGRAFI (4)

- Implementasi Cryptografi pada HTTP → SSL(Secure Socket Layer)
- Implementasi Cryptografi pada Remote Login → SSH (Secure Shell)
- Implementasi Cryptografi pada File Transfer → File transfer via SSH
- Implementasi Cryptografi pada Email → PGP (Pretty Good Privacy)



# CRYPTOGRAFI (5)

- ❑ Contoh penyadapan karena transmisi data dalam bentuk *clear text*

## Follow TCP stream

Stream Content

Content-Type: application/x-www-form-urlencoded

Content-Length: 45

user=jvandenbon%40jimiz.net&pass=Alice6232001HTTP/1.0 301 Moved

Server: cpsrvd/10.6.1

Set-Cookie: webmailsession=8TIU4895mwII9OmKBrt8k3TdsUIPTUfcvYP9Lk

Set-Cookie: webmailrelogin=no; path=

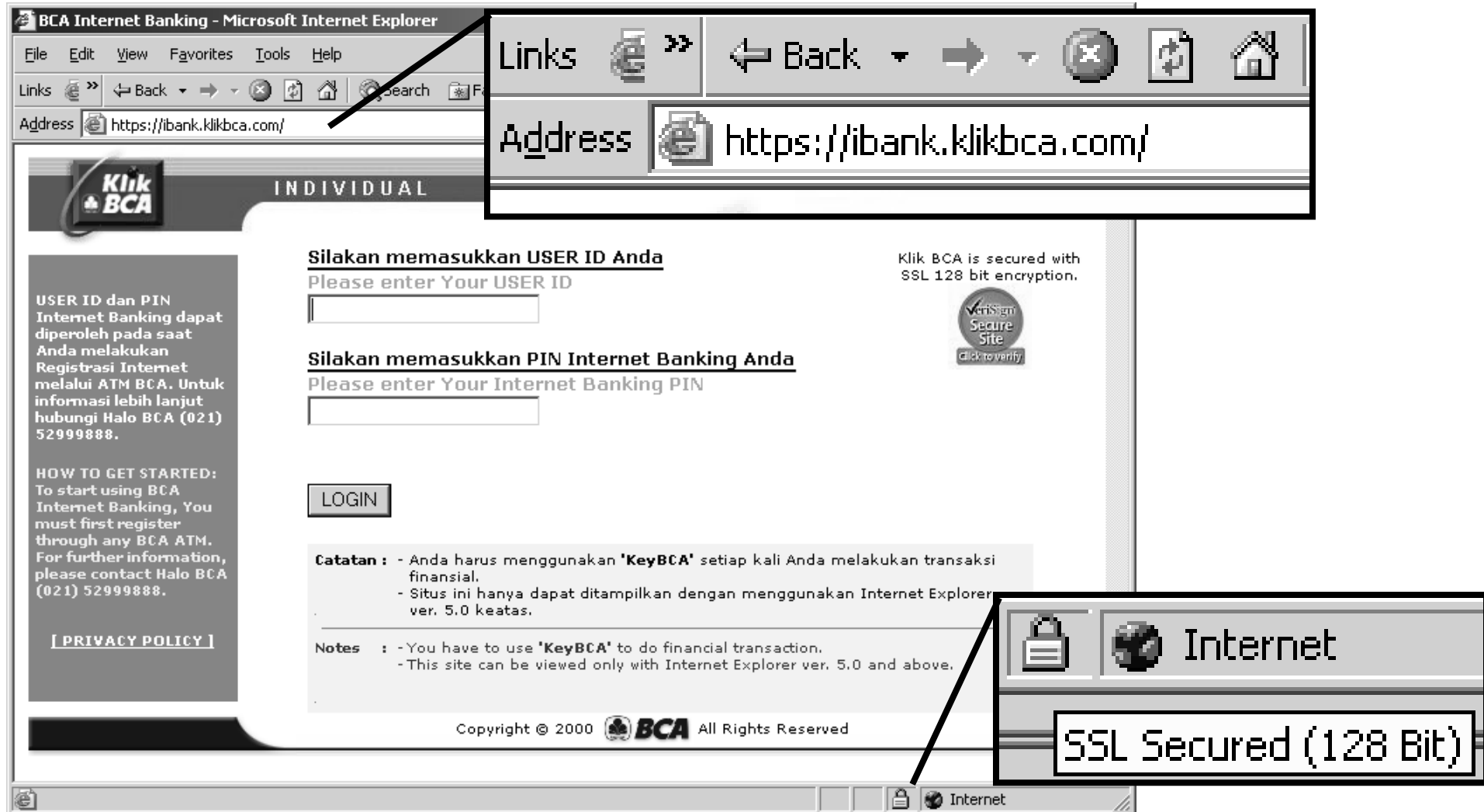
Location: /

Content-type: text/html

|

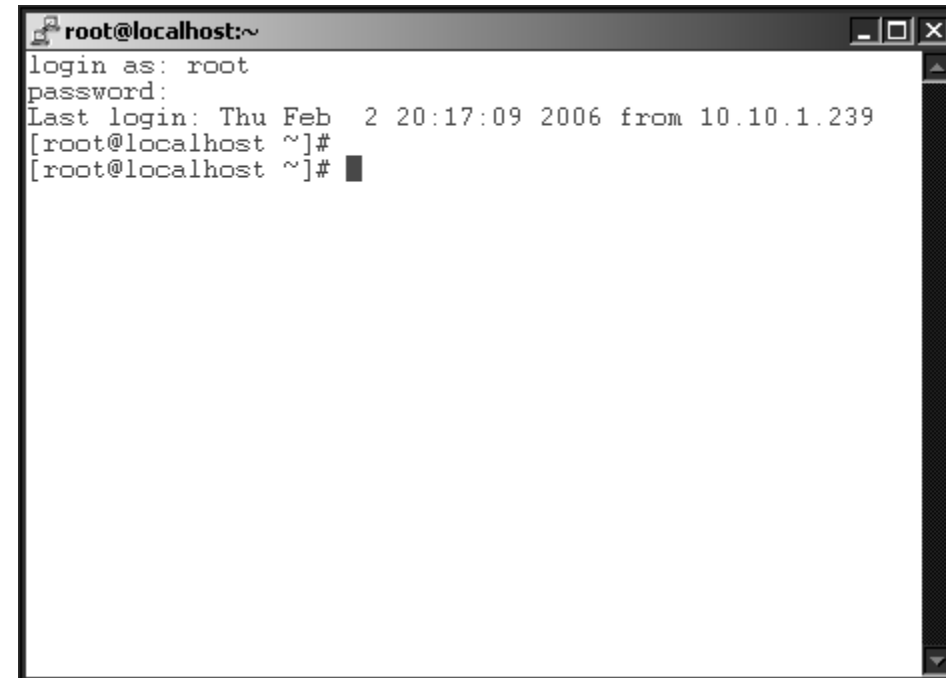
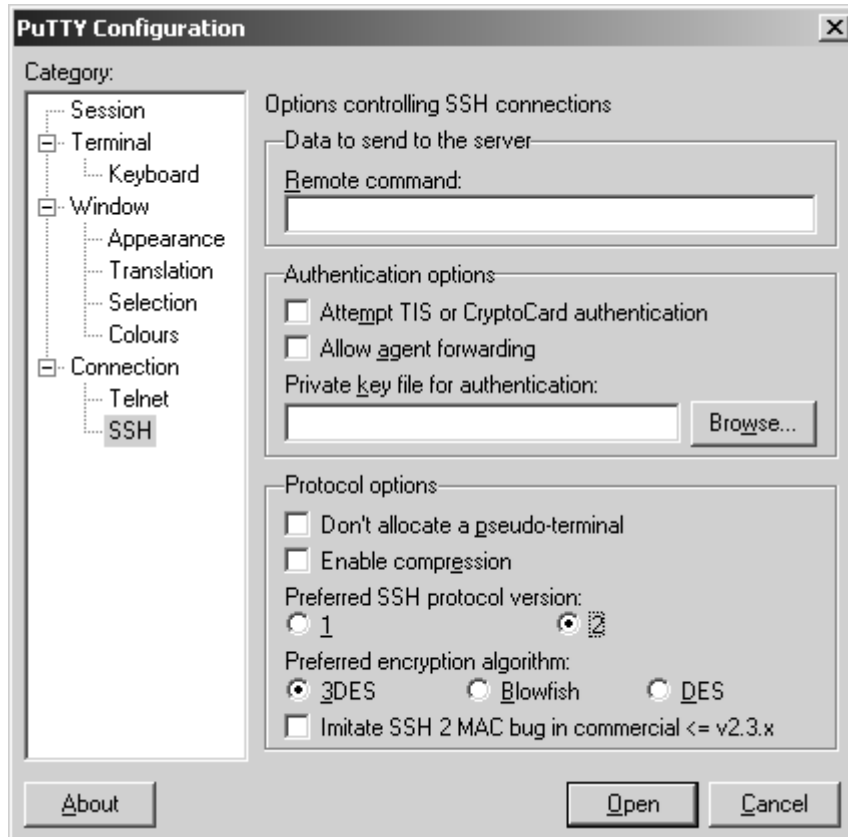
# CRYPTOGRAFI (6)

❑ Implementasi kriptografi pada protokol HTTP berupa SSL



# CRYPTOGRAFI (7)

## ❑ Implementasi kriptografi pada remote login dengan SSH



# FIREWALL (1)

## □Jenis-jenis

- Packet filtering
- Proxy based
- Statefull

## □Dimana?

- Host (Personal firewall)
- Router

□Efektifitas= 20% tools + 80% konfigurasi

# FIREWALL (2)

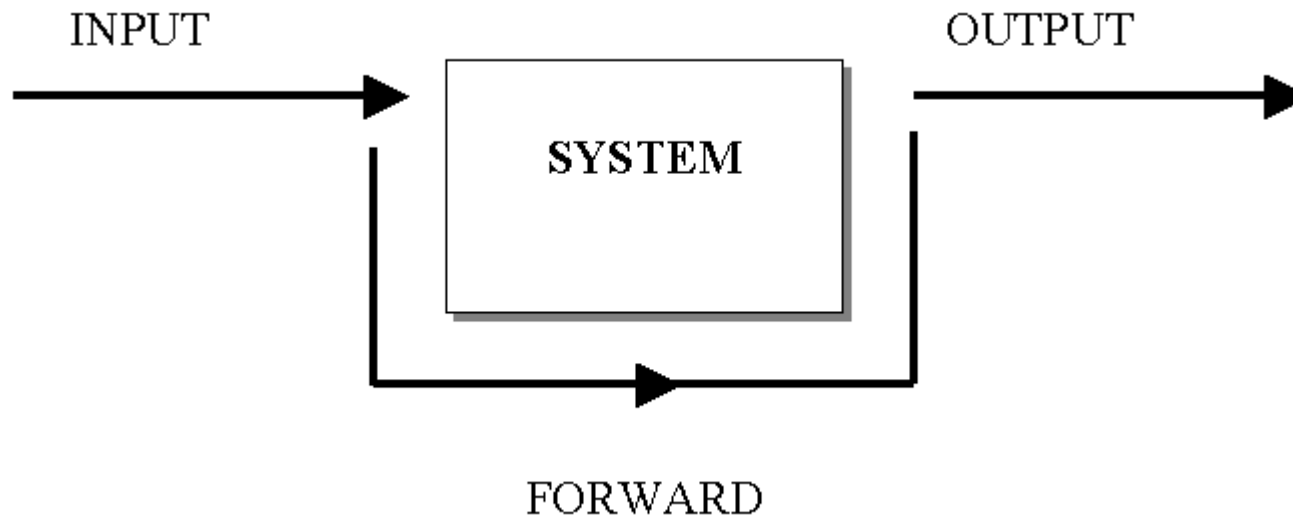
## □ Packet Filtering Firewall

- Parameter:
  - 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 (3)

## □ 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 (4)

## ❑ Statefull Packet Filter

- Packet filtering yang dikembangkan sehingga mampu “mengingat” paket yang diimplementasikan dalam *state tabel*
- Proses filtering sedang dibanding packet filtering dan proxy based

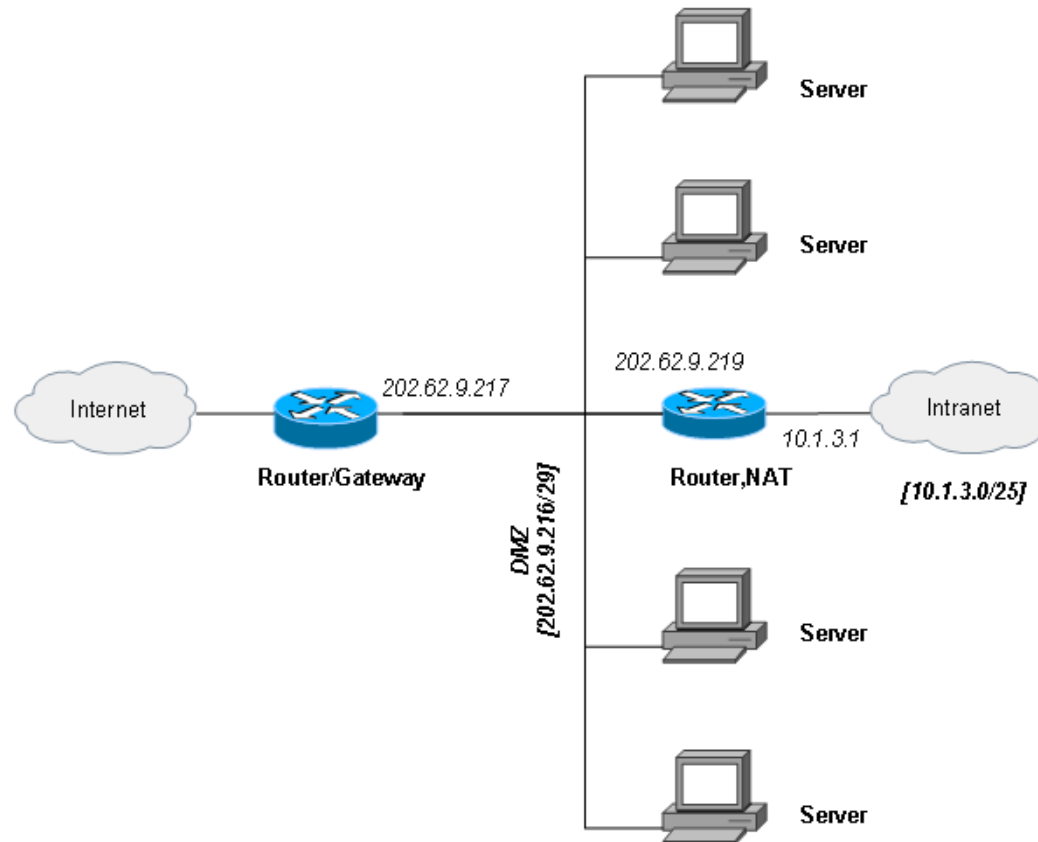
## ❑ Proxy Based

- Filtering di level aplikasi
- Proses filtering lebih lambat

# FIREWALL (5)

## □ 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 (6)

## □ 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 situs 71tahun.com (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) (1)

## ❑ Cara deteksi

- Deteksi anomaly (prosesor, bandwidth, memory dan lain-lain)
- Signature yang disimpan dalam database

## ❑ Serangan terdeteksi, lalu apa?

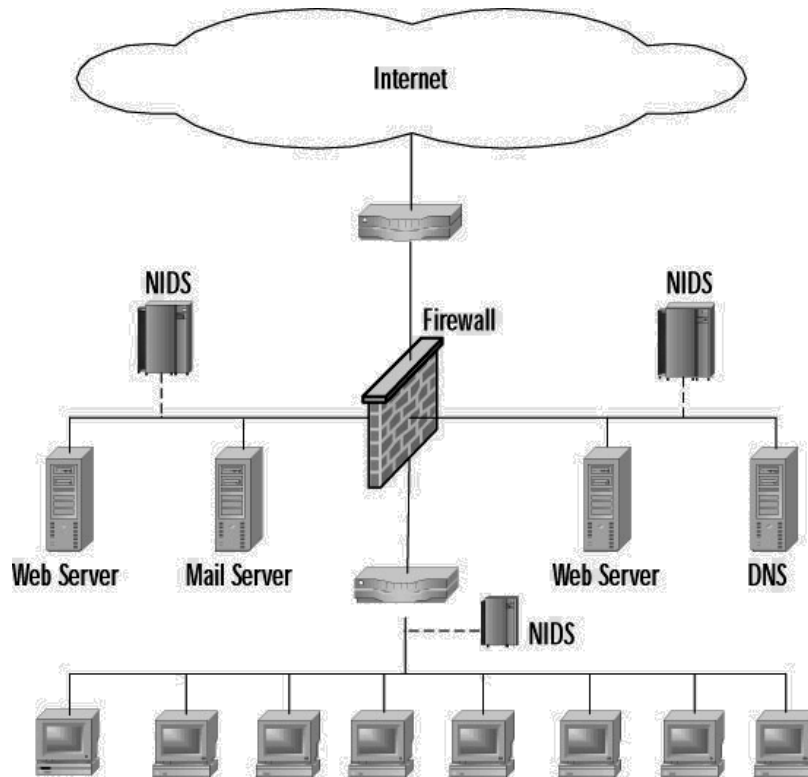
- Alert via SMS, email dan lain-lain
- Konfigurasi ulang firewall
- Menjalankan program respon terhadap serangan
- Logging serangan dan event

## ❑ Jenis-Jenis

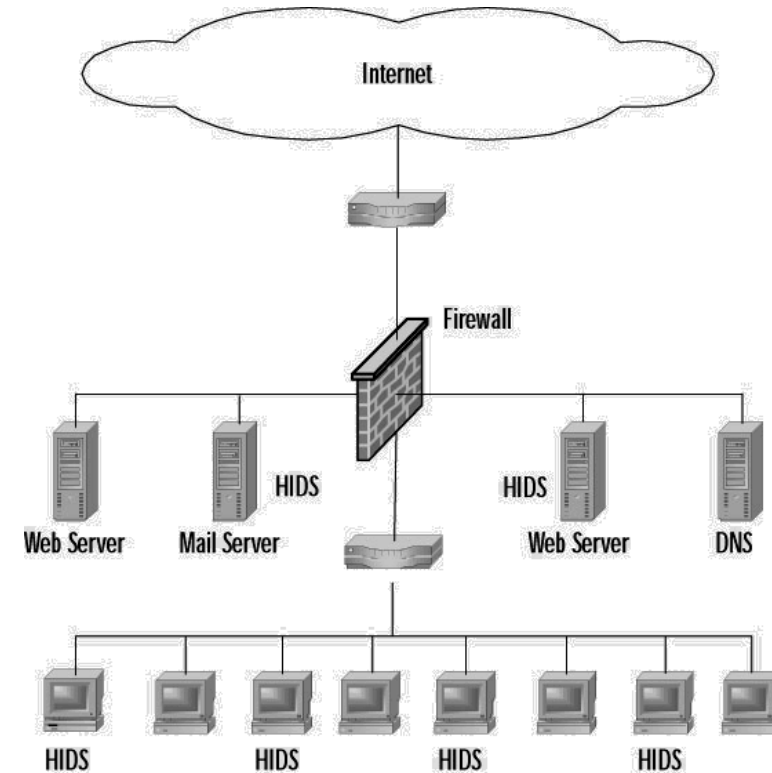
- Network IDS
- Host IDS

# IDS (INTRUSION DETECTION SYSTEM) (2)

## ❑ Network IDS vs Host IDS



NIDS



HIDS

# IDS (INTRUSION DETECTION SYSTEM) (3)

## ■ Contoh-contoh produk IDS-Snort

ACID Query Results

Home Search AG Maintenance [ Back ]

Added 0 alert(s) to the Alert cache

Queried DB on : Thu January 08, 2004 07:42:17

Meta Criteria	any
IP Criteria	any
TCP Criteria	any
Payload Criteria	any

Summary Statistics

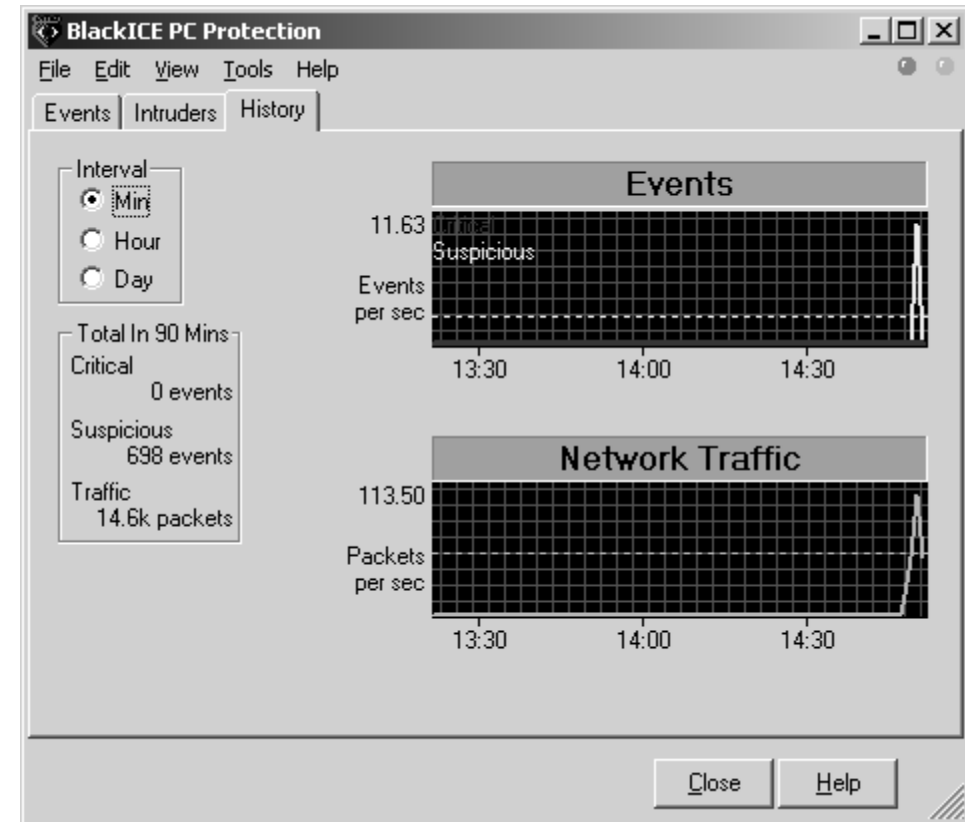
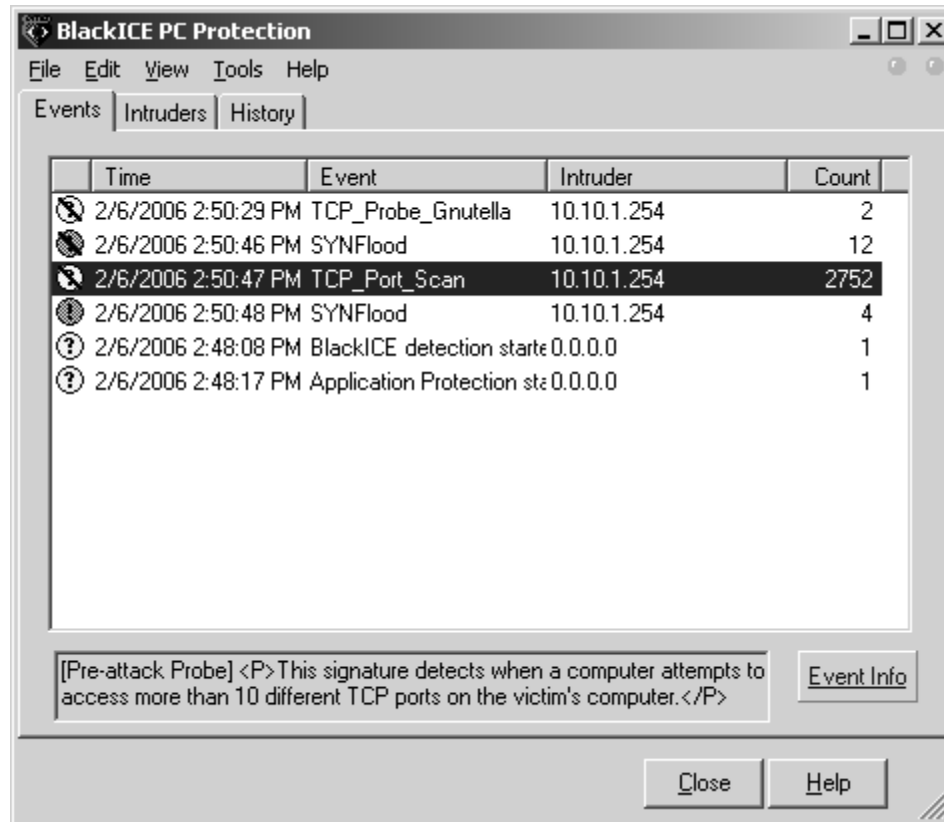
- Sensors
- Unique Alerts (classifications)
- Unique addresses: source | destination
- Unique IP links
- Source Port: TCP | UDP
- Destination Port: TCP | UDP
- Time profile of alerts

Displaying alerts 1-31 of 31 total

ID	Signature	Timestamp	Source Address	Dest. Address	Layer 4 Proto
#0-(1-849)	[snort] ATTACK-RESPONSES 403 Forbidden	2004-01-08 06:28:15	10.1.3.120:80	10.1.3.1:3422	TCP
#1-(1-848)	[snort] ATTACK-RESPONSES 403 Forbidden	2004-01-08 06:27:26	10.1.3.120:80	10.1.3.1:3401	TCP
#2-(1-	[snort] ATTACK-RESPONSES 403	2004-01-08 06:25:53	10.1.3.120:80	10.1.3.1:3355	TCP

# IDS (INTRUSION DETECTION SYSTEM) (4)

- Contoh-contoh produk IDS-BlackICE



# BACKUP

## ❑ Backuplah sebelum menyesal !

- Sistem Operasi dan Service
- Database
- Aplikasi
- Data-data penting lainnya

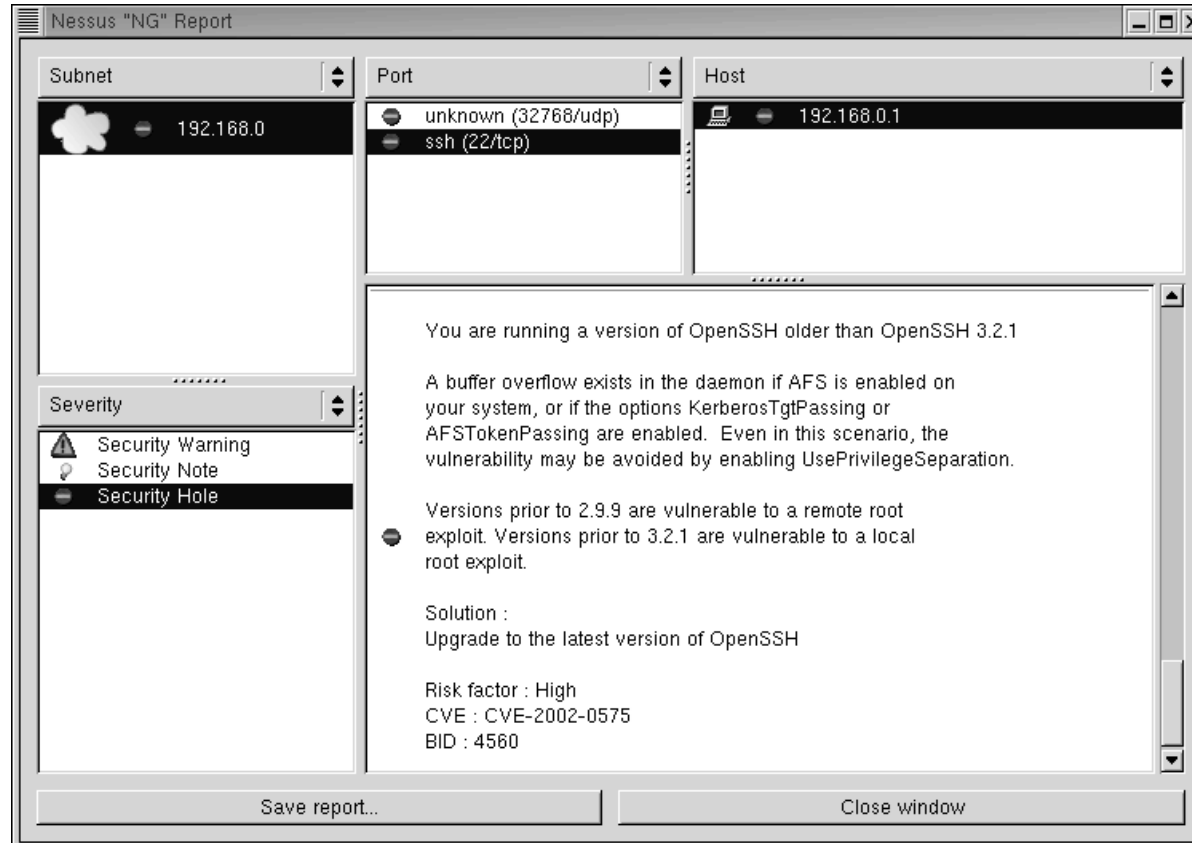
## ❑ Backup ke ..

- CD/DVDROM
- Hardisk yang diperuntukan khusus backup

# AUDITING SYSTEM

❑ Auditlah system Anda sebelum orang lain melakukannya 😊

- Hak akses
- Sistem
- Audit dengan Penetration testing



Contoh audit system  
dengan Nessus

# DIGITAL FORENSIK (1)

## □ 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

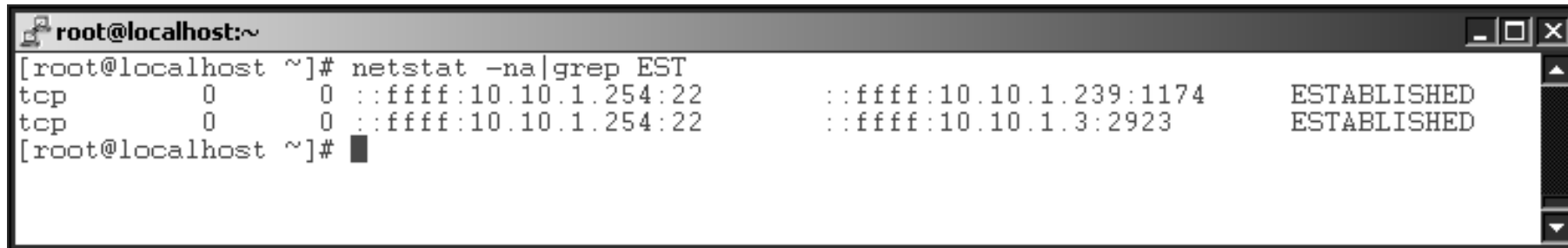
## □ Penanganan/pemulihan pasca insiden

- Pengecekan apakah ada backdoor yang ditanam
- Instalasi ulang sistem
- Tutup security hole yang ada
- Perbaiki konfigurasi firewall
- Dan lain-lain



# DIGITAL FORENSIK (2)

## □Pengecekan koneksi aktif

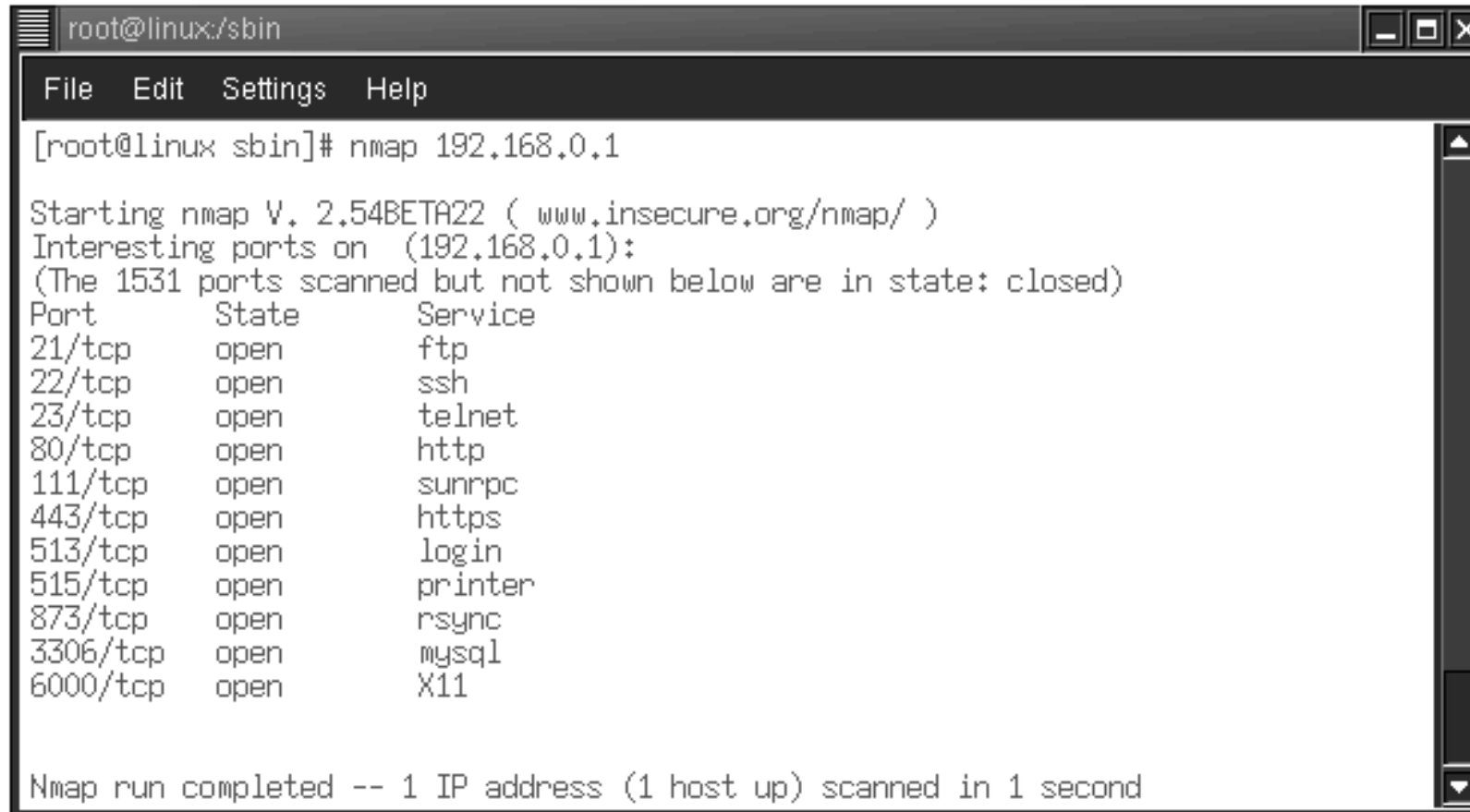


```
root@localhost:~  
[root@localhost ~]# netstat -na|grep EST  
tcp        0      0 :::ffff:10.10.1.254:22  :::ffff:10.10.1.239:1174  ESTABLISHED  
tcp        0      0 :::ffff:10.10.1.254:22  :::ffff:10.10.1.3:2923   ESTABLISHED  
[root@localhost ~]#
```

The image shows a terminal window with the command `netstat -na|grep EST` executed. The output displays two active TCP connections in the ESTABLISHED state. The first connection is between the local interface `:::ffff:10.10.1.254:22` and the remote address `:::ffff:10.10.1.239:1174`. The second connection is between the local interface `:::ffff:10.10.1.254:22` and the remote address `:::ffff:10.10.1.3:2923`. The terminal window has a title bar that reads `root@localhost:~` and standard window controls (minimize, maximize, close) on the right.

# DIGITAL FORENSIK (3)

## ❑ Koneksi listening port pasca insiden



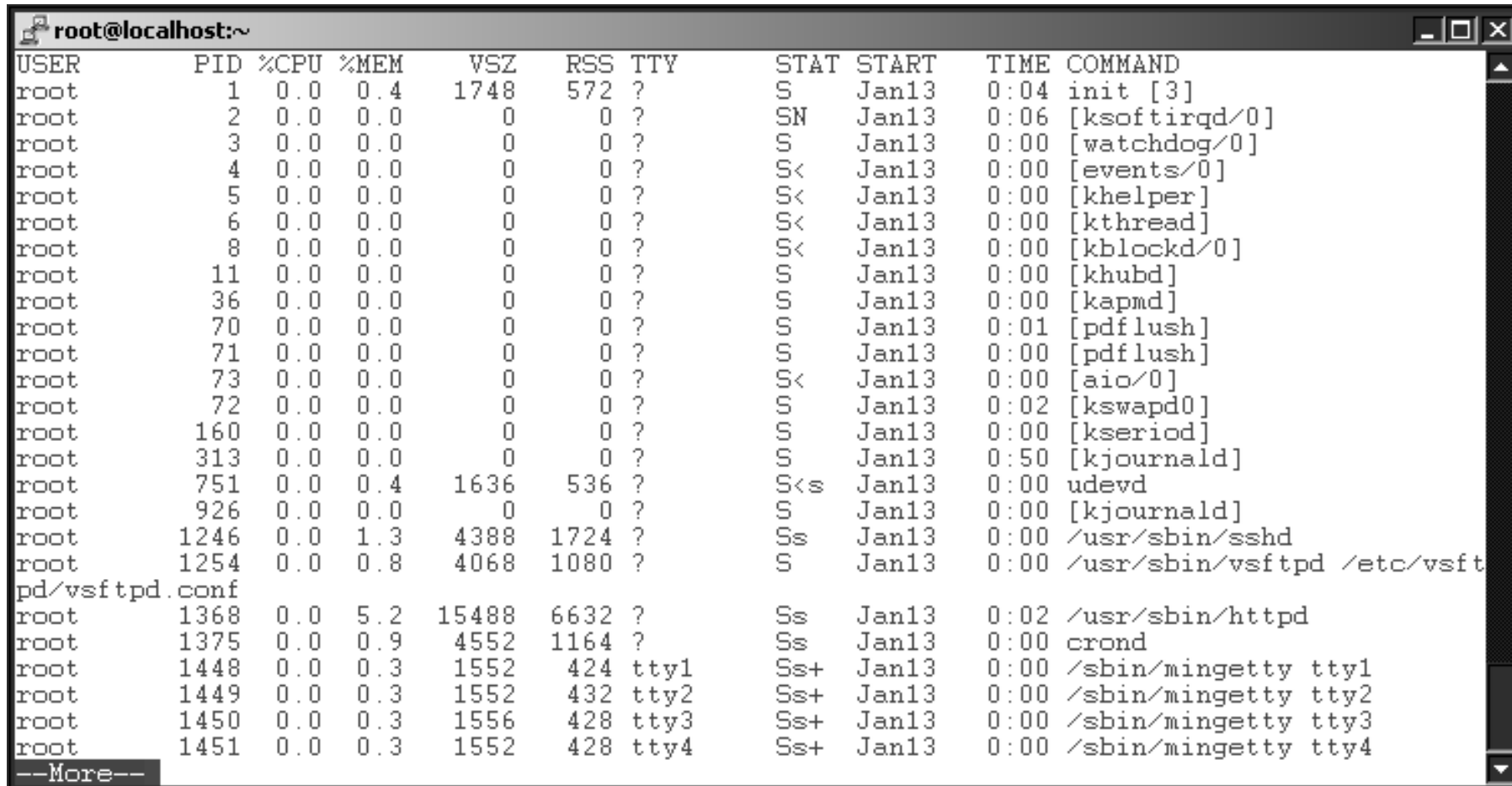
```
root@linux:/sbin
File Edit Settings Help
[root@linux sbin]# nmap 192.168.0.1

Starting nmap V. 2.54BETA22 ( www.insecure.org/nmap/ )
Interesting ports on (192.168.0.1):
(The 1531 ports scanned but not shown below are in state: closed)
Port      State      Service
21/tcp    open       ftp
22/tcp    open       ssh
23/tcp    open       telnet
80/tcp    open       http
111/tcp   open       sunrpc
443/tcp   open       https
513/tcp   open       login
515/tcp   open       printer
873/tcp   open       rsync
3306/tcp  open       mysql
6000/tcp  open       X11

Nmap run completed -- 1 IP address (1 host up) scanned in 1 second
```

# DIGITAL FORENSIK (4)

## □Pengecekan proses yang aktif pasca insiden



USER	PID	%CPU	%MEM	VSZ	RSS	TTY	STAT	START	TIME	COMMAND
root	1	0.0	0.4	1748	572	?	S	Jan13	0:04	init [3]
root	2	0.0	0.0	0	0	?	SN	Jan13	0:06	[ksoftirqd/0]
root	3	0.0	0.0	0	0	?	S	Jan13	0:00	[watchdog/0]
root	4	0.0	0.0	0	0	?	S<	Jan13	0:00	[events/0]
root	5	0.0	0.0	0	0	?	S<	Jan13	0:00	[khelper]
root	6	0.0	0.0	0	0	?	S<	Jan13	0:00	[kthreadd]
root	8	0.0	0.0	0	0	?	S<	Jan13	0:00	[kblockd/0]
root	11	0.0	0.0	0	0	?	S	Jan13	0:00	[khubd]
root	36	0.0	0.0	0	0	?	S	Jan13	0:00	[kapid]
root	70	0.0	0.0	0	0	?	S	Jan13	0:01	[pdflush]
root	71	0.0	0.0	0	0	?	S	Jan13	0:00	[pdflush]
root	73	0.0	0.0	0	0	?	S<	Jan13	0:00	[aio/0]
root	72	0.0	0.0	0	0	?	S	Jan13	0:02	[kswapd0]
root	160	0.0	0.0	0	0	?	S	Jan13	0:00	[kseriod]
root	313	0.0	0.0	0	0	?	S	Jan13	0:50	[kjournald]
root	751	0.0	0.4	1636	536	?	S<s	Jan13	0:00	udev
root	926	0.0	0.0	0	0	?	S	Jan13	0:00	[kjournald]
root	1246	0.0	1.3	4388	1724	?	Ss	Jan13	0:00	/usr/sbin/sshd
root	1254	0.0	0.8	4068	1080	?	S	Jan13	0:00	/usr/sbin/vsftpd /etc/vsft
pd/vsftpd.conf										
root	1368	0.0	5.2	15488	6632	?	Ss	Jan13	0:02	/usr/sbin/httpd
root	1375	0.0	0.9	4552	1164	?	Ss	Jan13	0:00	crond
root	1448	0.0	0.3	1552	424	tty1	Ss+	Jan13	0:00	/sbin/mingetty tty1
root	1449	0.0	0.3	1552	432	tty2	Ss+	Jan13	0:00	/sbin/mingetty tty2
root	1450	0.0	0.3	1556	428	tty3	Ss+	Jan13	0:00	/sbin/mingetty tty3
root	1451	0.0	0.3	1552	428	tty4	Ss+	Jan13	0:00	/sbin/mingetty tty4
--More--										

# DIGITAL FORENSIK (5)

## □Pengecekan log user yang login

```
root@localhost:/var/log
[root@localhost log]# last
root      pts/0      10.10.1.239      Mon Feb  6 15:51      still logged in
root      pts/0      10.10.1.239      Thu Feb  2 20:17 - 22:06      (01:49)
root      pts/3      10.10.1.158      Thu Feb  2 18:39 - 18:55      (00:16)
root      pts/2      10.10.1.58       Thu Feb  2 18:33 - 18:49      (00:16)
root      pts/2      10.10.1.173      Thu Feb  2 18:16 - 18:16      (00:00)
puji      pts/1      10.10.1.3        Thu Feb  2 17:56      still logged in
root      pts/0      10.10.1.239      Thu Feb  2 15:54 - 19:27      (03:32)

wtmp begins Thu Feb  2 15:54:53 2006
[root@localhost log]#
```

```
root@localhost:/var/log
pcap:x:77:77::/var/arpwatch:/sbin/nologin
nscd:x:28:28:NSCD Daemon::/sbin/nologin
named:x:25:25:Named:/var/named:/sbin/nologin
netdump:x:34:34:Network Crash Dump user:/var/crash:/bin/bash
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
rpc:x:32:32:Portmapper RPC user::/sbin/nologin
mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin
snmsp:x:51:51::/var/spool/mqueue:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
bblm:x:501:501::/home/bblm:/bin/bash
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
squid:x:23:23::/var/spool/squid:/sbin/nologin
puji:x:502:502::/home/puji:/bin/bash
virtual:x:503:503::/home/virtual:/bin/bash
[root@localhost log]#
```

# DIGITAL FORENSIK (6)

## □Pengecekan log pengakses service

```
root@localhost:~  
6.0; Windows NT 5.1)"  
[root@localhost ~]# tail /var/log/httpd/access_log  
202.51.210.116 - - [06/Feb/2006:17:10:08 +0700] "GET /images/dies.jpg HTTP/1.0" 200 5652 "http://www.bblm.go.id/m  
me=Pemesinan" "Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)"  
202.51.210.116 - - [06/Feb/2006:17:10:12 +0700] "GET /images/plastic_molds.jpg HTTP/1.0" 200 4930 "http://www.bbl  
es.php?name=Pemesinan" "Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)"  
202.51.210.116 - - [06/Feb/2006:17:10:21 +0700] "GET /images/casting_molds.jpg HTTP/1.0" 200 5923 "http://www.bbl  
es.php?name=Pemesinan" "Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)"  
202.51.210.116 - - [06/Feb/2006:17:10:35 +0700] "GET /images/jig.jpg HTTP/1.0" 200 4832 "http://www.bblm.go.id/mc  
e=Pemesinan" "Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)"  
202.51.210.116 - - [06/Feb/2006:17:10:38 +0700] "GET /images/las1.jpg HTTP/1.0" 200 6990 "http://www.bblm.go.id/m  
me=Pemesinan" "Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)"  
202.51.210.116 - - [06/Feb/2006:17:10:43 +0700] "GET /images/las3.jpg HTTP/1.0" 200 6457 "http://www.bblm.go.id/m  
me=Pemesinan" "Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)"  
202.51.210.116 - - [06/Feb/2006:17:10:45 +0700] "GET /images/las2.jpg HTTP/1.0" 200 5384 "http://www.bblm.go.id/m  
me=Pemesinan" "Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)"  
202.51.210.116 - - [06/Feb/2006:17:11:37 +0700] "GET /favicon.ico HTTP/1.0" 404 305 "-" "Mozilla/4.0 (compatible;  
indows NT 5.0)"  
81.215.209.113 - - [06/Feb/2006:17:47:58 +0700] "PUT /ayt.htm HTTP/1.0" 405 324 "-" "Microsoft Data Access Intern  
Provider DAV 1.1"  
202.73.103.42 - - [06/Feb/2006:17:59:39 +0700] "GET /heattreatment/heat.html HTTP/1.1" 404 317 "http://www.google  
?hl=id&q=hard+chrome&btnG=Telusuri+dengan+Google&meta=cr%3DcountryID" "Mozilla/4.0 (compatible; MSIE 6.0; Windows  
[root@localhost ~]#
```

# SISTEM HARDENING

- Hardening System: Security Policy
- Hardening System: Kriptografi
- Hardening System: Firewall
- Hardening System: IDS (Intrusion Detection System)
- Hardening System: Backup
- Hardening System: Auditing System
- Hardening System: Digital Forensik dan Penanganan Pasca Insiden

# SECURITY POLICY

## ❑ Policy penggunaan komputer

- Tidak boleh meminjamkan account kepada orang lain
- Tidak boleh mengambil/menaruh file dari komputer kantor, dll

## ❑ Policy penggunaan Instalasi program

- Tidak boleh menginstall program tanpa seijin staff IT
- Tidak boleh menginstall program ilegal, dll

## ❑ Policy penggunaan Internet

- Tidak boleh menggunakan internet untuk kegiatan carding, hacking dkk
- Tidak boleh menggunakan internet untuk mengakses situs-situs yang berpotensi menyebarkan virus, dll

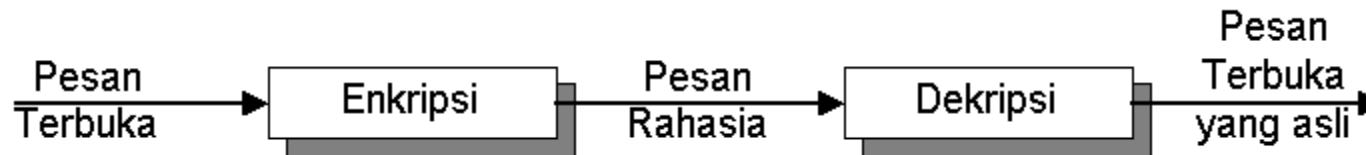
## ❑ Policy penggunaan Email

- Tidak boleh menggunakan email kantor untuk kegiatan milis, dll

# CRYPTOGRAFI (1)

❑ Kriptografi (cryptography) adalah ilmu dan seni menyimpan suatu pesan secara aman

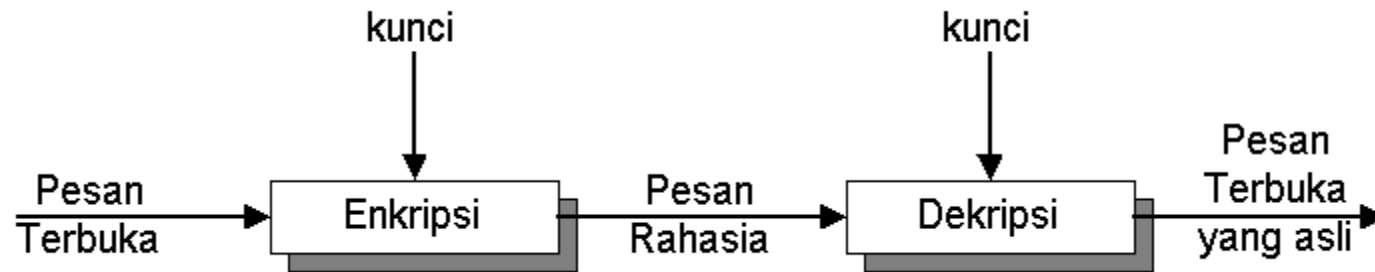
❑ Enkripsi dan Dekripsi



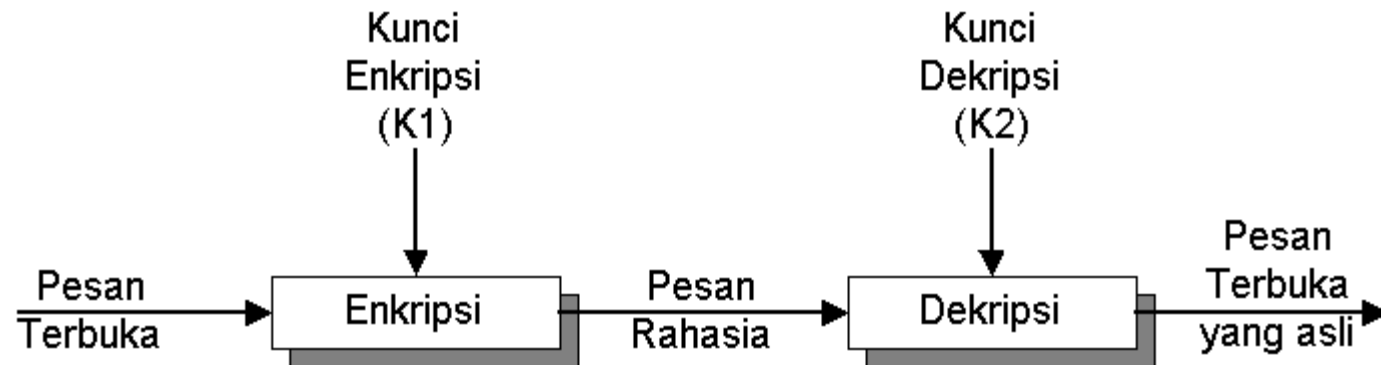


# CRYPTOGRAFI (2)

## □ Cryptografi Symetric

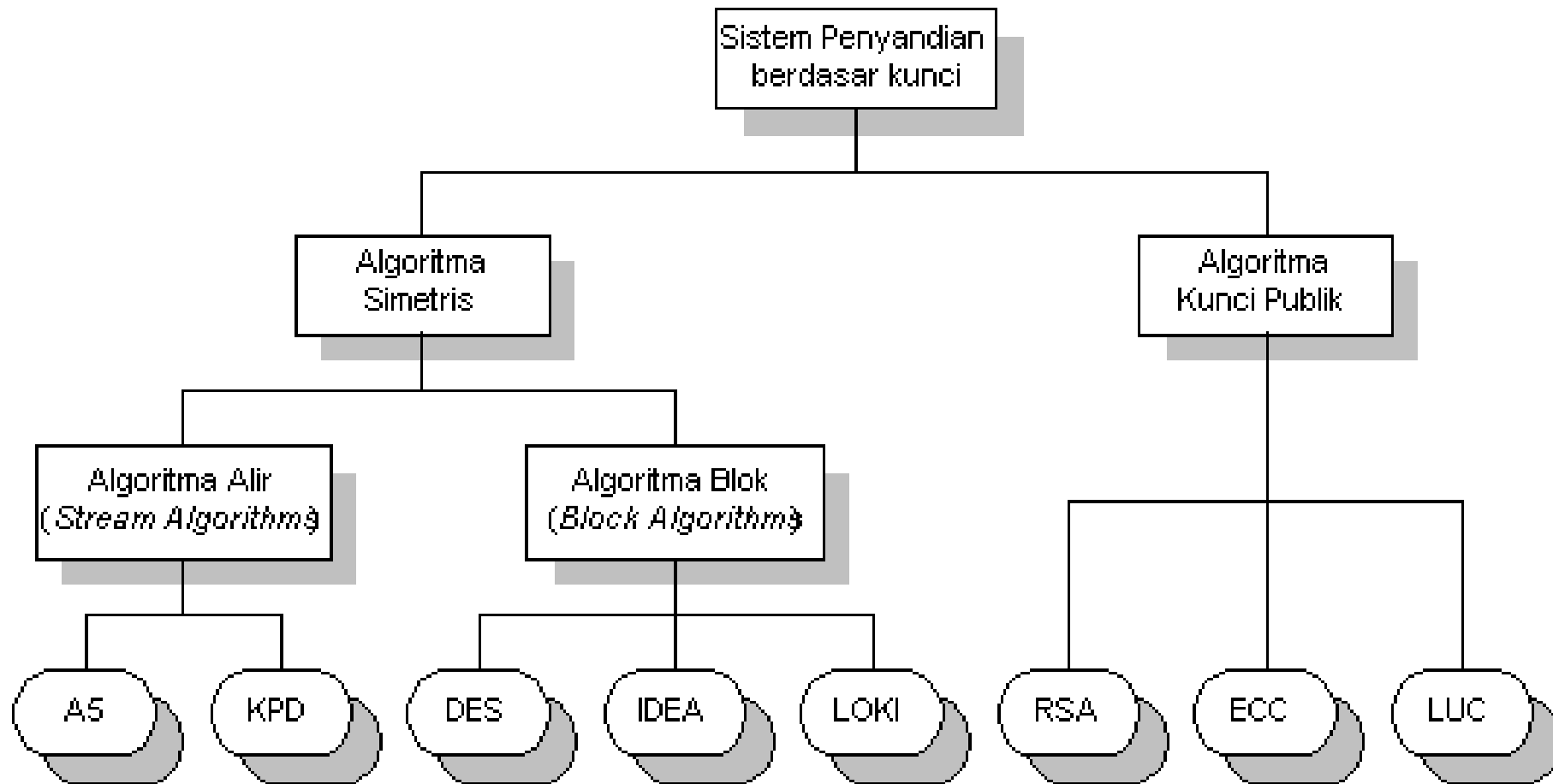


## □ Cryptografi Asymetric



# CRYPTOGRAFI (3)

□ Pembagian sistem kriptografi berdasarkan kunci



# CRYPTOGRAFI (4)

- Implementasi Cryptografi pada HTTP → SSL(Secure Socket Layer)
- Implementasi Cryptografi pada Remote Login → SSH (Secure Shell)
- Implementasi Cryptografi pada File Transfer → File transfer via SSH
- Implementasi Cryptografi pada Email → PGP (Pretty Good Privacy)

# CRYPTOGRAFI (5)

- ❑ Contoh penyadapan karena transmisi data dalam bentuk *clear text*

## Follow TCP stream

Stream Content

Content-Type: application/x-www-form-urlencoded

Content-Length: 45

user=jvandenbon%40jimiz.net&pass=Alice6232001HTTP/1.0 301 Moved

Server: cpsrvd/10.6.1

Set-Cookie: webmailsession=8TIU4895mwII9OmKBrt8k3TdsUIPTUfcvYP9Lk

Set-Cookie: webmailrelogin=no; path=

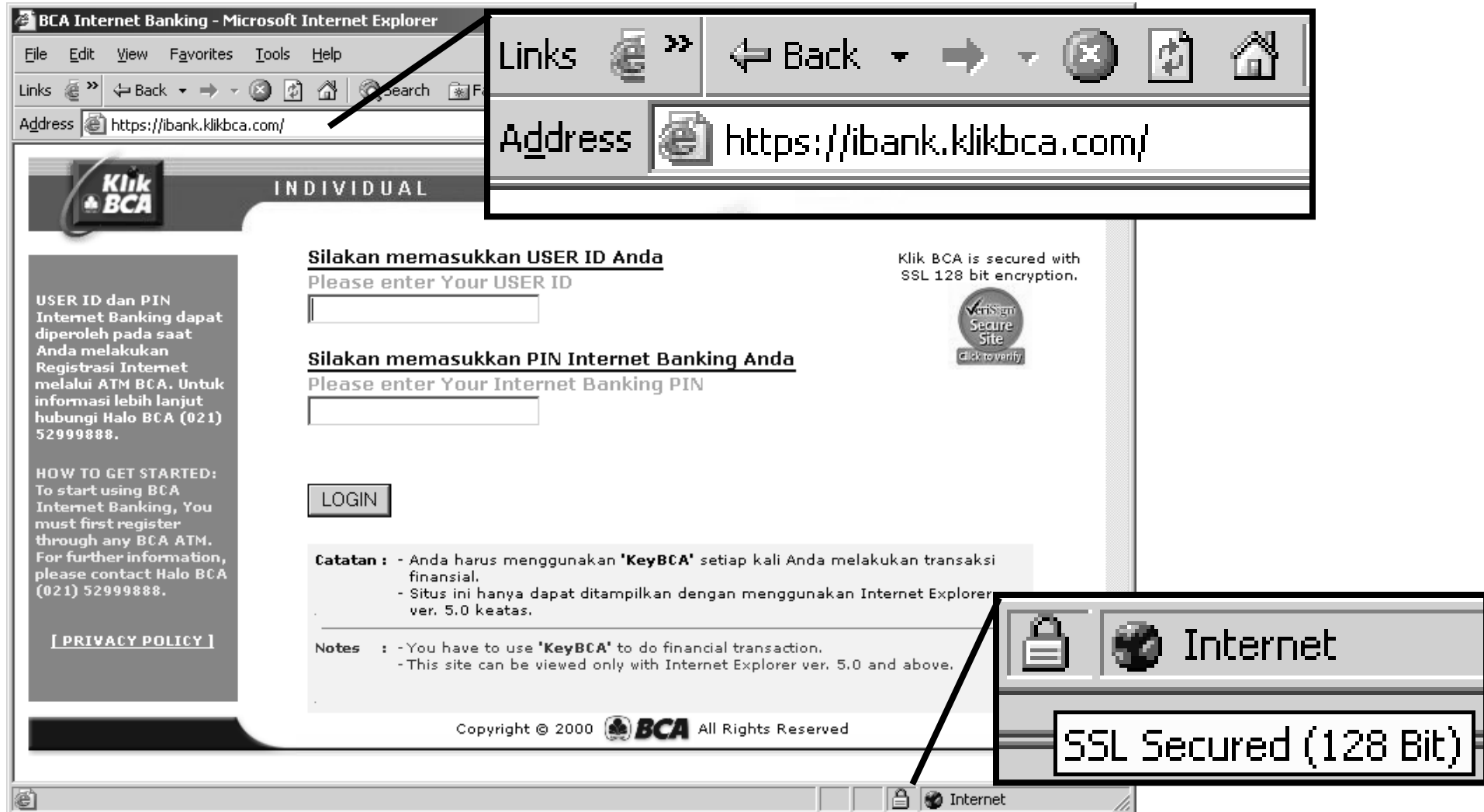
Location: /

Content-type: text/html

|

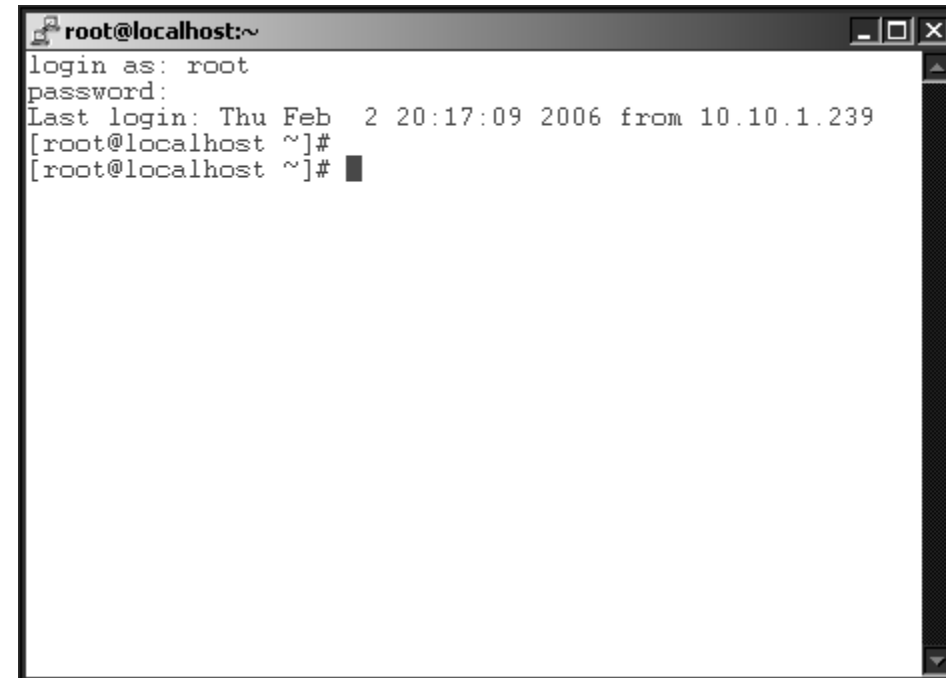
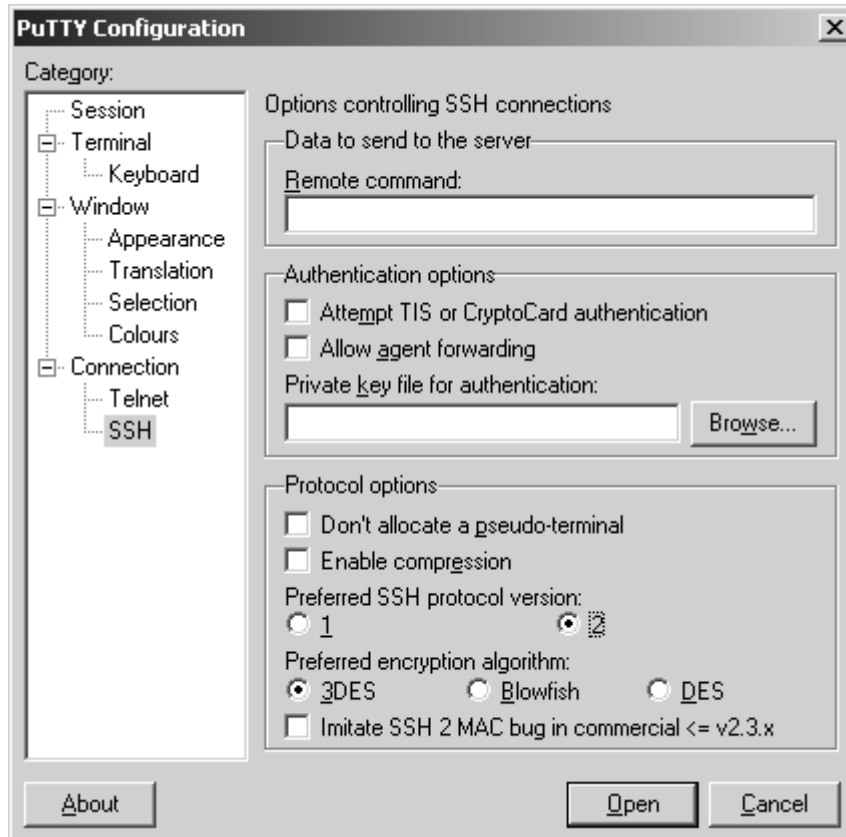
# CRYPTOGRAFI (6)

□ Implementasi kriptografi pada protokol HTTP berupa SSL



# CRYPTOGRAFI (7)

## ❑ Implementasi kriptografi pada remote login dengan SSH



# FIREWALL (1)

## □Jenis-jenis

- Packet filtering
- Proxy based
- Statefull

## □Dimana?

- Host (Personal firewall)
- Router

□Efektifitas= 20% tools + 80% konfigurasi

# FIREWALL (2)

## ❑ Packet Filtering Firewall

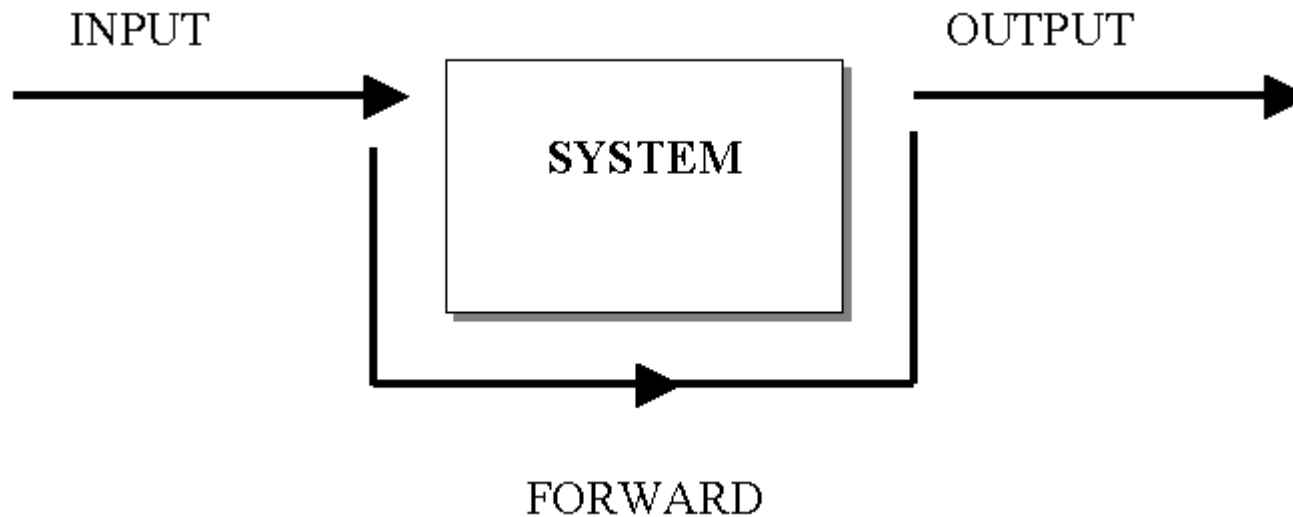
- Parameter:
  - Protokol, contoh TCP, UDP, ICMP
  - Port Asal, contoh 25, 1024:65536
  - Port Tujuan, contoh 25
  - IP Asal/Network tujuan, contoh 81.52.22.1, 81.52.22.0/29
  - IP Tujuan /Network tujuan , contoh 81.52.22.1, 81.52.22.0/29
  - Code bit, contoh ACK
  - Judge, contoh DROP, ACCEPT
- Proses filtering cepat



# FIREWALL (3)

## □ 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 (4)

## ❑ Statefull Packet Filter

- Packet filtering yang dikembangkan sehingga mampu “mengingat” paket yang diimplementasikan dalam *state tabel*
- Proses filtering sedang dibanding packet filtering dan proxy based

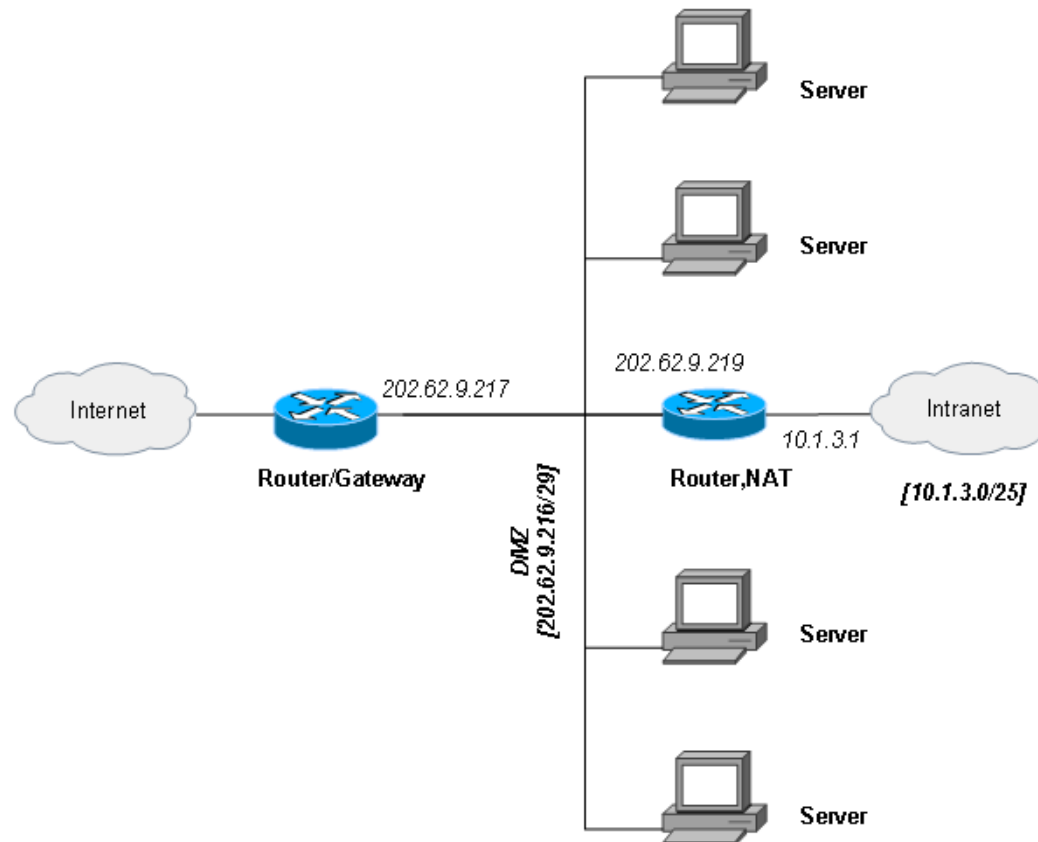
## ❑ Proxy Based

- Filtering di level aplikasi
- Proses filtering lebih lambat

# FIREWALL (5)

## □ 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 (6)

## □ 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 situs 71tahun.com (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) (1)

## ❑ Cara deteksi

- Deteksi anomaly (prosesor, bandwidth, memory dan lain-lain)
- Signature yang disimpan dalam database

## ❑ Serangan terdeteksi, lalu apa?

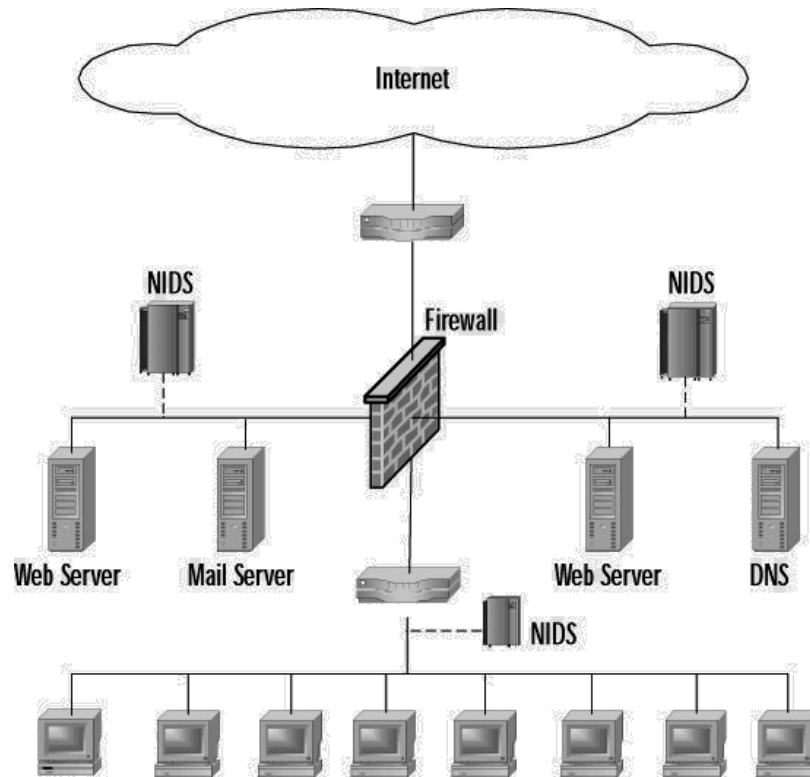
- Alert via SMS, email dan lain-lain
- Konfigurasi ulang firewall
- Menjalankan program respon terhadap serangan
- Logging serangan dan event

## ❑ Jenis-Jenis

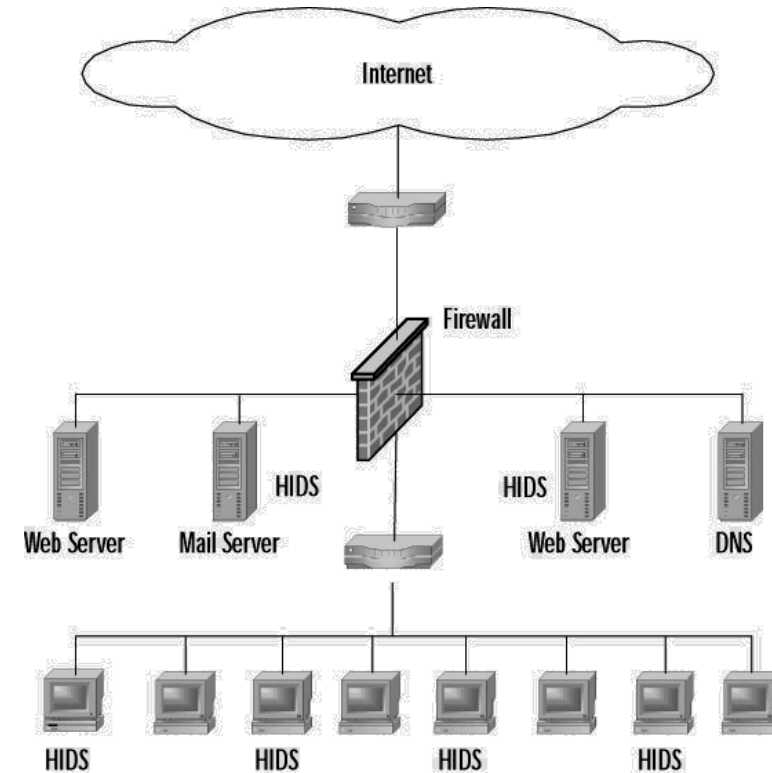
- Network IDS
- Host IDS

# IDS (INTRUSION DETECTION SYSTEM) (2)

## ❑ Network IDS vs Host IDS



NIDS



HIDS

# IDS (INTRUSION DETECTION SYSTEM) (3)

## ■ Contoh-contoh produk IDS-Snort

ACID Query Results

Home Search AG Maintenance [ Back ]

Added 0 alert(s) to the Alert cache

Queried DB on : Thu January 08, 2004 07:42:17

Meta Criteria	any
IP Criteria	any
TCP Criteria	any
Payload Criteria	any

Summary Statistics

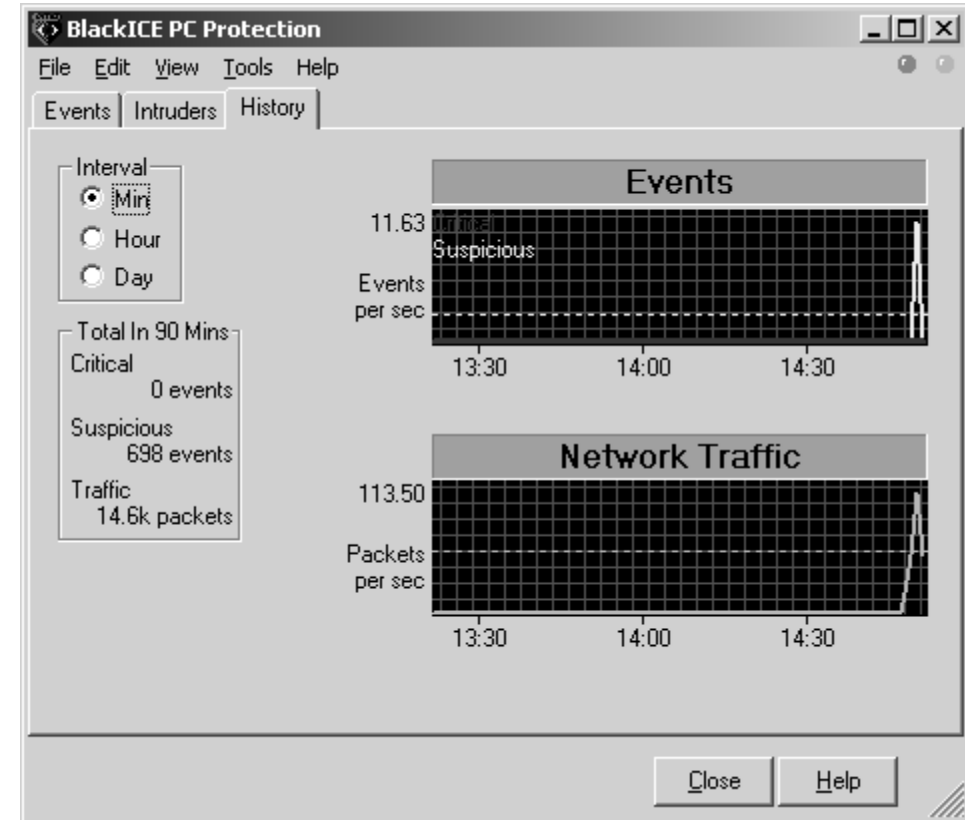
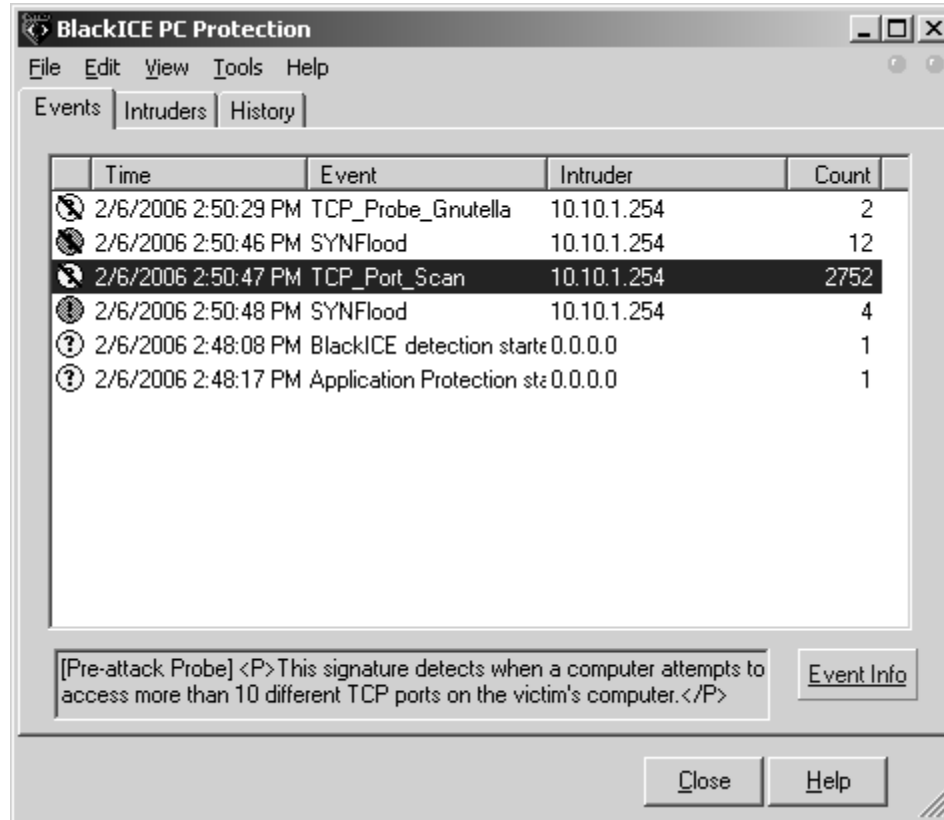
- Sensors
- Unique Alerts ( classifications )
- Unique addresses: source | destination
- Unique IP links
- Source Port: TCP | UDP
- Destination Port: TCP | UDP
- Time profile of alerts

Displaying alerts 1-31 of 31 total

ID	Signature	Timestamp	Source Address	Dest. Address	Layer 4 Proto
#0-(1-849)	[snort] ATTACK-RESPONSES 403 Forbidden	2004-01-08 06:28:15	10.1.3.120:80	10.1.3.1:3422	TCP
#1-(1-848)	[snort] ATTACK-RESPONSES 403 Forbidden	2004-01-08 06:27:26	10.1.3.120:80	10.1.3.1:3401	TCP
#2-(1-	[snort] ATTACK-RESPONSES 403	2004-01-08 06:25:53	10.1.3.120:80	10.1.3.1:3355	TCP

# IDS (INTRUSION DETECTION SYSTEM) (4)

- Contoh-contoh produk IDS-BlackICE





# BACKUP

## ☐ Backuplah sebelum menyesal !

- Sistem Operasi dan Service
- Database
- Aplikasi
- Data-data penting lainnya

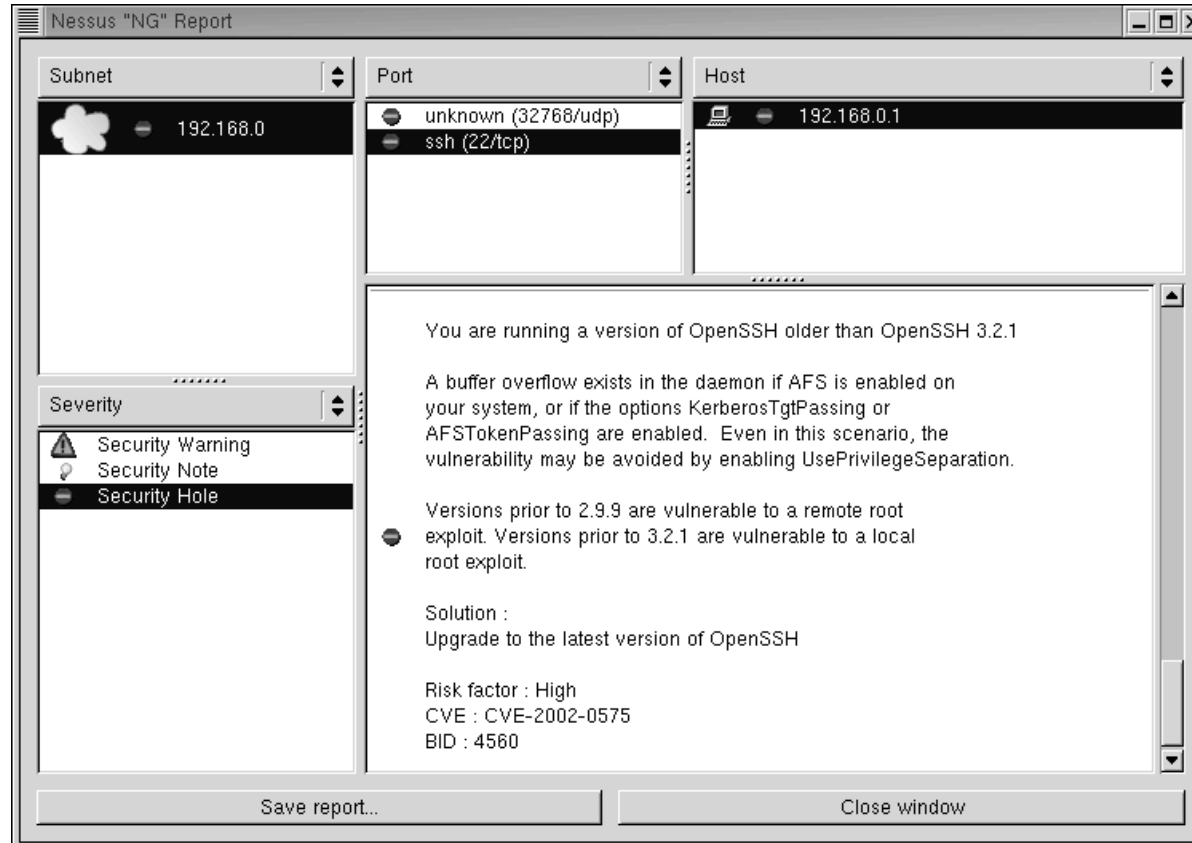
## ☐ Backup ke ..

- CD/DVDROM
- Hardisk yang diperuntukan khusus backup

# AUDITING SYSTEM

❑ Auditlah system Anda sebelum orang lain melakukannya 😊

- Hak akses
- Sistem
- Audit dengan Penetration testing



Contoh audit system  
dengan Nessus

# DIGITAL FORENSIK (1)

## □ Digital forensik pasca insiden

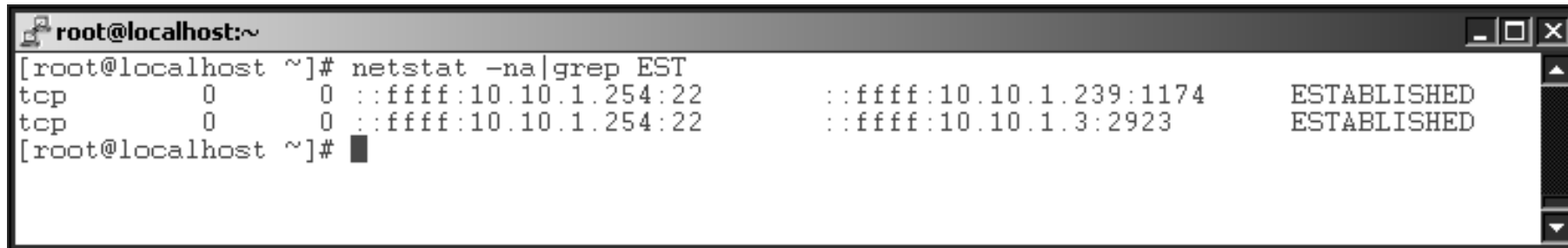
- Pengecekan koneksi aktif
- Pengecekan listening port pasca insiden
- Pengecekan proses yang aktif pasca insiden
- Pengecekan log user yang login
- Pengecekan log system
- Pengecekan log pengakses service
- Dan lain-lain

## □ Penanganan/pemulihan pasca insiden

- Pengecekan apakah ada backdoor yang ditanam
- Instalasi ulang sistem
- Tutup security hole yang ada
- Perbaiki konfigurasi firewall
- Dan lain-lain

# DIGITAL FORENSIK (2)

## □Pengecekan koneksi aktif

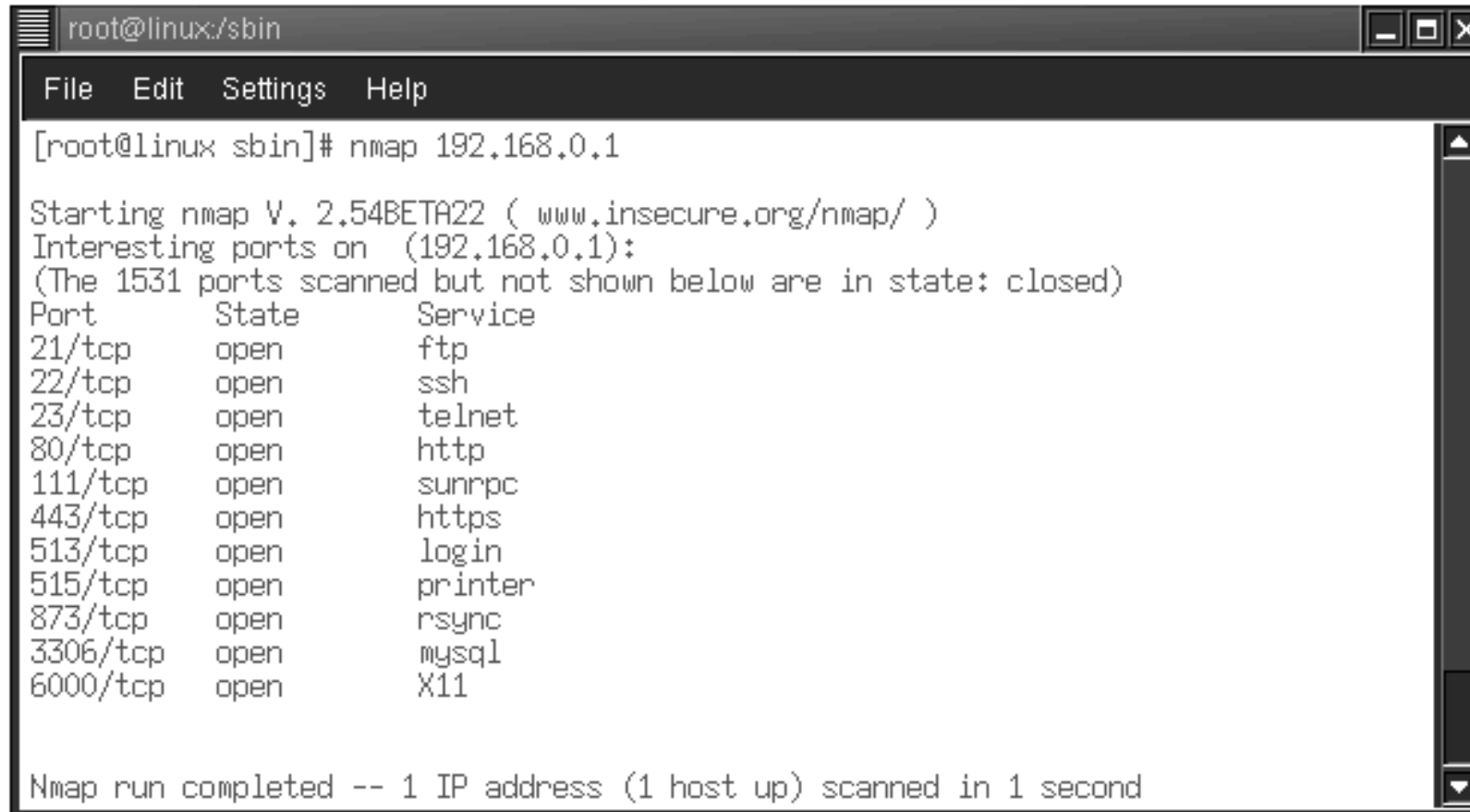


```
root@localhost:~  
[root@localhost ~]# netstat -na|grep EST  
tcp        0      0 :::ffff:10.10.1.254:22  :::ffff:10.10.1.239:1174 ESTABLISHED  
tcp        0      0 :::ffff:10.10.1.254:22  :::ffff:10.10.1.3:2923  ESTABLISHED  
[root@localhost ~]#
```

The image shows a terminal window with the command `netstat -na|grep EST` executed. The output displays two active TCP connections in the ESTABLISHED state. The first connection is between the local interface `:::ffff:10.10.1.254:22` and the remote address `:::ffff:10.10.1.239:1174`. The second connection is between the local interface `:::ffff:10.10.1.254:22` and the remote address `:::ffff:10.10.1.3:2923`. The terminal window has a title bar that reads `root@localhost:~` and standard window controls (minimize, maximize, close) on the right.

# DIGITAL FORENSIK (3)

## ❑ Koneksi listening port pasca insiden



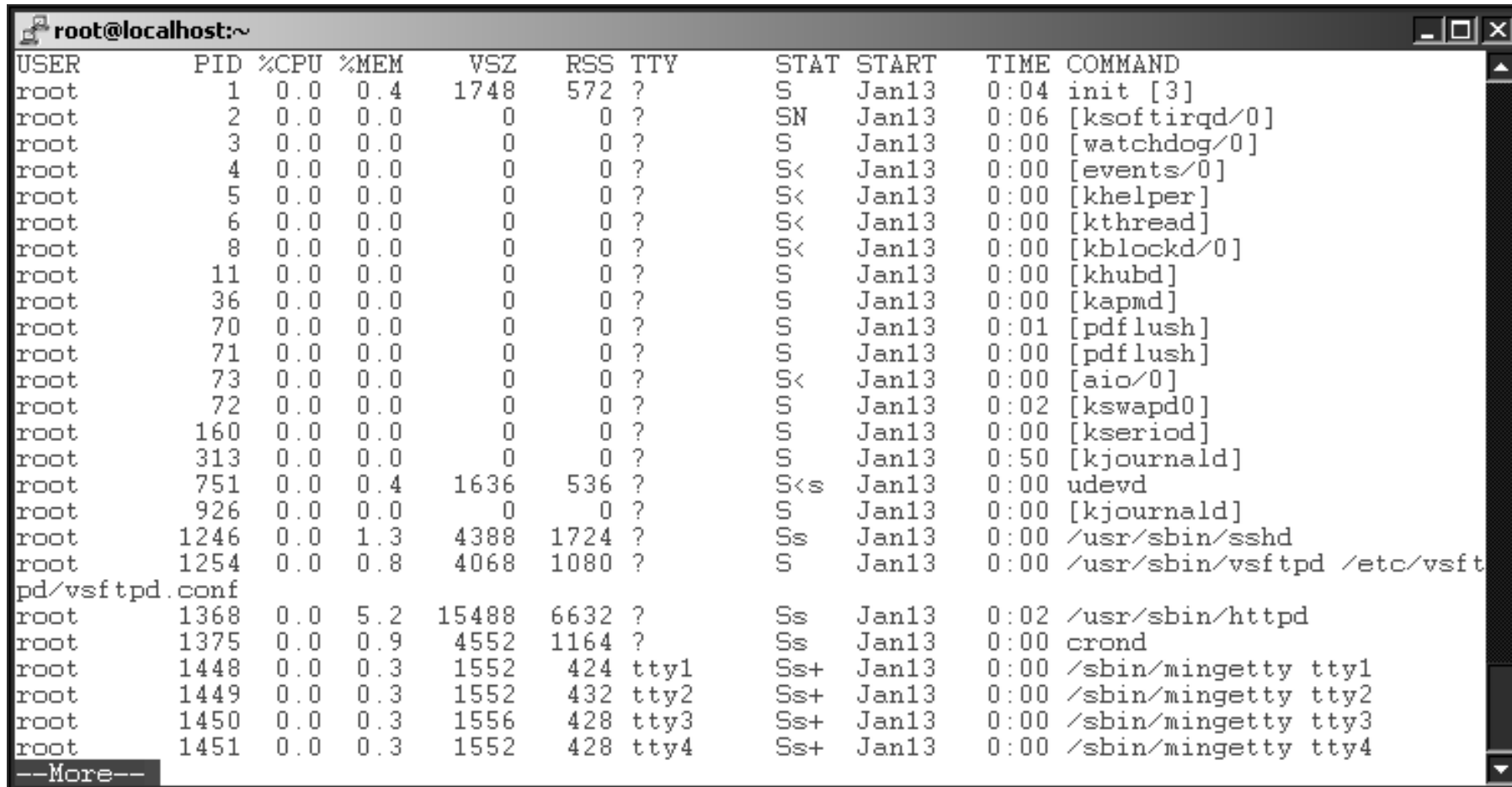
```
root@linux:/sbin
File Edit Settings Help
[root@linux sbin]# nmap 192.168.0.1

Starting nmap V. 2.54BETA22 ( www.insecure.org/nmap/ )
Interesting ports on (192.168.0.1):
(The 1531 ports scanned but not shown below are in state: closed)
Port      State      Service
21/tcp    open       ftp
22/tcp    open       ssh
23/tcp    open       telnet
80/tcp    open       http
111/tcp   open       sunrpc
443/tcp   open       https
513/tcp   open       login
515/tcp   open       printer
873/tcp   open       rsync
3306/tcp  open       mysql
6000/tcp  open       X11

Nmap run completed -- 1 IP address (1 host up) scanned in 1 second
```

# DIGITAL FORENSIK (4)

## □Pengecekan proses yang aktif pasca insiden



USER	PID	%CPU	%MEM	VSZ	RSS	TTY	STAT	START	TIME	COMMAND
root	1	0.0	0.4	1748	572	?	S	Jan13	0:04	init [3]
root	2	0.0	0.0	0	0	?	SN	Jan13	0:06	[ksoftirqd/0]
root	3	0.0	0.0	0	0	?	S	Jan13	0:00	[watchdog/0]
root	4	0.0	0.0	0	0	?	S<	Jan13	0:00	[events/0]
root	5	0.0	0.0	0	0	?	S<	Jan13	0:00	[khelper]
root	6	0.0	0.0	0	0	?	S<	Jan13	0:00	[kthread]
root	8	0.0	0.0	0	0	?	S<	Jan13	0:00	[kblockd/0]
root	11	0.0	0.0	0	0	?	S	Jan13	0:00	[khubd]
root	36	0.0	0.0	0	0	?	S	Jan13	0:00	[kapmd]
root	70	0.0	0.0	0	0	?	S	Jan13	0:01	[pdflush]
root	71	0.0	0.0	0	0	?	S	Jan13	0:00	[pdflush]
root	73	0.0	0.0	0	0	?	S<	Jan13	0:00	[aio/0]
root	72	0.0	0.0	0	0	?	S	Jan13	0:02	[kswapd0]
root	160	0.0	0.0	0	0	?	S	Jan13	0:00	[kseriod]
root	313	0.0	0.0	0	0	?	S	Jan13	0:50	[kjournald]
root	751	0.0	0.4	1636	536	?	S<s	Jan13	0:00	udev
root	926	0.0	0.0	0	0	?	S	Jan13	0:00	[kjournald]
root	1246	0.0	1.3	4388	1724	?	Ss	Jan13	0:00	/usr/sbin/sshd
root	1254	0.0	0.8	4068	1080	?	S	Jan13	0:00	/usr/sbin/vsftpd /etc/vsft
pd/vsftpd.conf										
root	1368	0.0	5.2	15488	6632	?	Ss	Jan13	0:02	/usr/sbin/httpd
root	1375	0.0	0.9	4552	1164	?	Ss	Jan13	0:00	crond
root	1448	0.0	0.3	1552	424	tty1	Ss+	Jan13	0:00	/sbin/mingetty tty1
root	1449	0.0	0.3	1552	432	tty2	Ss+	Jan13	0:00	/sbin/mingetty tty2
root	1450	0.0	0.3	1556	428	tty3	Ss+	Jan13	0:00	/sbin/mingetty tty3
root	1451	0.0	0.3	1552	428	tty4	Ss+	Jan13	0:00	/sbin/mingetty tty4
--More--										

# DIGITAL FORENSIK (5)

## □Pengecekan log user yang login

```
root@localhost:/var/log
[root@localhost log]# last
root      pts/0      10.10.1.239      Mon Feb  6 15:51      still logged in
root      pts/0      10.10.1.239      Thu Feb  2 20:17 - 22:06      (01:49)
root      pts/3      10.10.1.158      Thu Feb  2 18:39 - 18:55      (00:16)
root      pts/2      10.10.1.58       Thu Feb  2 18:33 - 18:49      (00:16)
root      pts/2      10.10.1.173      Thu Feb  2 18:16 - 18:16      (00:00)
puji      pts/1      10.10.1.3        Thu Feb  2 17:56      still logged in
root      pts/0      10.10.1.239      Thu Feb  2 15:54 - 19:27      (03:32)

wtmp begins Thu Feb  2 15:54:53 2006
[root@localhost log]#
```

```
root@localhost:/var/log
pcap:x:77:77::/var/arpwatch:/sbin/nologin
nscd:x:28:28:NSCD Daemon::/sbin/nologin
named:x:25:25:Named:/var/named:/sbin/nologin
netdump:x:34:34:Network Crash Dump user:/var/crash:/bin/bash
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
rpc:x:32:32:Portmapper RPC user::/sbin/nologin
mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin
snmsp:x:51:51::/var/spool/mqueue:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
bblm:x:501:501::/home/bblm:/bin/bash
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
squid:x:23:23::/var/spool/squid:/sbin/nologin
puji:x:502:502::/home/puji:/bin/bash
virtual:x:503:503::/home/virtual:/bin/bash
[root@localhost log]#
```

# DIGITAL FORENSIK (6)

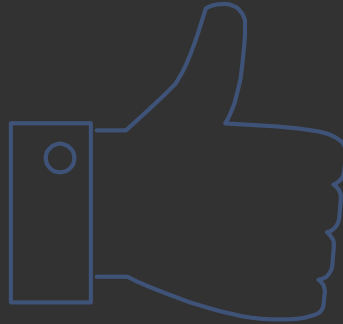
## □Pengecekan log pengakses service

```
root@localhost:~  
6.0; Windows NT 5.1)"  
[root@localhost ~]# tail /var/log/httpd/access_log  
202.51.210.116 - - [06/Feb/2006:17:10:08 +0700] "GET /images/dies.jpg HTTP/1.0" 200 5652 "http://www.bblm.go.id/m  
me=Pemesinan" "Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)"  
202.51.210.116 - - [06/Feb/2006:17:10:12 +0700] "GET /images/plastic_molds.jpg HTTP/1.0" 200 4930 "http://www.bbl  
es.php?name=Pemesinan" "Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)"  
202.51.210.116 - - [06/Feb/2006:17:10:21 +0700] "GET /images/casting_molds.jpg HTTP/1.0" 200 5923 "http://www.bbl  
es.php?name=Pemesinan" "Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)"  
202.51.210.116 - - [06/Feb/2006:17:10:35 +0700] "GET /images/jig.jpg HTTP/1.0" 200 4832 "http://www.bblm.go.id/mc  
e=Pemesinan" "Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)"  
202.51.210.116 - - [06/Feb/2006:17:10:38 +0700] "GET /images/las1.jpg HTTP/1.0" 200 6990 "http://www.bblm.go.id/m  
me=Pemesinan" "Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)"  
202.51.210.116 - - [06/Feb/2006:17:10:43 +0700] "GET /images/las3.jpg HTTP/1.0" 200 6457 "http://www.bblm.go.id/m  
me=Pemesinan" "Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)"  
202.51.210.116 - - [06/Feb/2006:17:10:45 +0700] "GET /images/las2.jpg HTTP/1.0" 200 5384 "http://www.bblm.go.id/m  
me=Pemesinan" "Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)"  
202.51.210.116 - - [06/Feb/2006:17:11:37 +0700] "GET /favicon.ico HTTP/1.0" 404 305 "-" "Mozilla/4.0 (compatible;  
indows NT 5.0)"  
81.215.209.113 - - [06/Feb/2006:17:47:58 +0700] "PUT /ayt.htm HTTP/1.0" 405 324 "-" "Microsoft Data Access Intern  
Provider DAV 1.1"  
202.73.103.42 - - [06/Feb/2006:17:59:39 +0700] "GET /heattreatment/heat.html HTTP/1.1" 404 317 "http://www.google  
?hl=id&q=hard+chrome&btnG=Telusuri+dengan+Google&meta=cr%3DcountryID" "Mozilla/4.0 (compatible; MSIE 6.0; Windows  
[root@localhost ~]#
```



### *Referensi utama :*

- >> Michael Felderer , Riccardo Scandariato (editor) - Exploring Security in Software Architecture and Design, 2018.*
- >> Nancy R. Mead, Carol Woody - Cyber Security Engineering\_ A Practical Approach for Systems and Software Assurance-Addison-Wesley Professional (2016)*
- >> James Helfrich - Security for Software Engineers-CRC Press (2019)*
- >> Pete Loshin - Simple Steps to Data Encryption\_ A Practical Guide to Secure Computing-Syngress (2013)*
- >> Tevfik Bultan,Fang Yu,Muath Alkhalaf,Abdulbaki Aydin (auth.) - String Analysis for Software Verification and Security (2017)*



# THANKS!

**Ada Pertanyaan?**