



1

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

Dikti MONKS MERDEKA BELAJAR Kampus Merdeka

## MENGAPA DIBUTUHKAN

- Information-based society, menyebabkan nilai informasi menjadi sangat penting dan menuntut kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat efisien bagi sebuah organisasi.
- Infrastruktur jaringan komputer, Seperti LAN dan Internet, memungkinkan untuk menyediakan informasi secara cepat, sekaligus membuka potensi adanya lubang keamanan (security hole)

INSTITUT TEKNOLOGI PLN Your Future Starts Today!

2

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

Dikti MONKS MERDEKA BELAJAR Kampus Merdeka

## Penyebab Meningkatnya Kejahatan Komputer

- Aplikasi bisnis berbasis TI dan jaringan komputer meningkat : online banking, e-commerce, Electronic data Interchange (EDI).
- Desentralisasi Server.
- Transisi dari single vendor ke multi vendor.
- Meningkatnya kemampuan pemakai (user)
- Semakin kompleksnya sistem yang digunakan, semakin besarnya source code program yang digunakan.
- Berhubungan dengan jaringan / internet.

INSTITUT TEKNOLOGI PLN Your Future Starts Today!

3

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

Dikti MONKS MERDEKA BELAJAR Kampus Merdeka

## Klasifikasi kejahatan Komputer :

```

graph LR
    A[LEVEL ANNOYING] --> B[LEVEL DANGEROUS]
  
```

INSTITUT TEKNOLOGI PLN Your Future Starts Today!

4

INTERNASIONAL, MODERN, MANDIRI, UNGGUL

Dikti MONFS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

### Klasifikasi kejahatan Komputer :

- Menurut David Ilove [Jhon D. Howard, "An Analysis Of Security Incidents On The Internet 1989-1995" PhD thesis, Engineering and Public policy, carnegia Mellon University, 1997] berdasarkan lubang keamanan, keamanan dapat di klasifikasikan menjadi empat yaitu:

INSTITUT TEKNOLOGI PLN Your Future

5

INTERNASIONAL, MODERN, MANDIRI, UNGGUL

Dikti MONFS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

### Klasifikasi kejahatan Komputer :

- Keamanan yang bersifat fisik (Physical security), termasuk akses orang ke gedung, peralatan, dan media yang digunakan. Contoh:
  - ✓ Wiretapping atau hal-hal yang berhubungan dengan akses ke kabel atau komputer yang digunakan juga dapat dimasukkan kedalam kelas ini.
  - ✓ 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)
  - ✓ Syn Flood Attack, dimana sistem (host) yang dituju dibanjiri oleh permintaan sehingga dia menjadi ter-lalu sibuk dan bahkan dapat berakibat macetnya sistem (hang)

INSTITUT TEKNOLOGI PLN Your Future

6

INTERNASIONAL, MODERN, MANDIRI, UNGGUL

Dikti MONFS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

### CONTOH DoS

INSTITUT TEKNOLOGI PLN Your Future

7

INTERNASIONAL, MODERN, MANDIRI, UNGGUL

Dikti MONFS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

### Beberapa klasifikasi serangan DoS:

- Land Attack**  
Land attack merupakan serangan kepada sistem dengan menggunakan program yang bernama "land". Program land menyerang server yang dituju dengan mengirimkan packet palsu yang seolah-olah berasal dari server yang dituju. Dengan kata lain, source dan destination dari packet dibuat seakan-akan berasal dari server yang dituju. Akibatnya server yang diserang menjadi bingung.
- Loteria**  
Program loteria merupakan "perbaikan" dari program land, dimana port yang digunakan berubah-ubah sehingga menyulitkan bagi pengamanan.
- Ping Broadcast (Smurf)**  
Salah satu mekanisme serangan yang baru-baru ini mulai banyak digunakan adalah menggunakan ping ke alamat broadcast, ini yang sering disebut dengan smurf. Seluruh komputer (device) yang berada di alamat broadcast tersebut akan menjawab. Jika sebuah sistem memiliki banyak komputer (device) dan ping broadcast ini dilakukan terus menerus, jaringan dapat dipenuhi oleh respon-respon dari device-device tersebut. Akibatnya jaringan menjadi lambat.
- Ping of Death (PoD)**  
Ping of death sebenarnya adalah eksploitasi program ping dengan memberikan packet yang ukurannya besar ke sistem yang dituju. Beberapa sistem UNIX ternyata menjadi hang ketika diserang dengan cara ini. Program ping umum terdapat di berbagai operating system, meskipun umumnya program ping tersebut mengirimkan packet dengan ukuran kecil (tertentu) dan tidak memiliki fasilitas untuk mengubah besarnya packet. Salah satu implementasi program ping yang dapat digunakan untuk mengubah ukuran packet adalah program ping yang ada di sistem Windows 95.

INSTITUT TEKNOLOGI PLN Your Future

8

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

Dikti MONS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

## Klasifikasi Kejahatan Komputer

- Keamanan yang berhubungan dengan orang (personal)
  - ✓ Identifikasi user (username dan password)
  - ✓ Profil resiko dari orang yang mempunyai akses (Pemakai dan pengelola)
- Keamanan dari data dan media serta teknik komunikasi
- Keamanan dalam operasi:
  - ✓ Adanya prosedur yang digunakan untuk mengatur dan mengelola sistem keamanan, dan juga termasuk prosedur setelah serangan (post attack recovery)

INSTITUT TEKNOLOGI PLN Your Future Starts Today!

9

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

Dikti MONS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

## ISTILAH LAIN DARI PENYERANG

- HACKER => **Peretas** (Inggris: **hacker**) adalah orang yang mempelajari, menganalisis, memodifikasi, menerobos masuk ke dalam komputer dan jaringan komputer, baik untuk keuntungan atau dimotivasi oleh tantangan.
- CRACKER => seseorang yang masuk secara ilegal ke dalam system komputer. Istilahnya cracker ini merupakan para *hacker* yang menggambarkan kegiatan yang merusak dan bukan hacker pada pengertian sesungguhnya. *Hacker* dan *Cracker* mempunyai proses yang sama tapi motivasi dan tujuan yang berbeda.
- CARDER => kelompok orang yang melakukan tindakan kejahatan dengan melakukan manipulasi nomor kartu kredit orang lain dan menggunakannya untuk kepentingan pribadi.

INSTITUT TEKNOLOGI PLN Your Future Starts Today!

10

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

Dikti MONS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

## Karakteristik Penyusup

- The Curious (Si ingin Tahu)
  - ✦ Tertarik menemukan jenis dan data yang anda miliki.
- The Malicious (Si Perusak)
  - ✦ Berusaha merusak sistem, atau merubah web page, atau sebaliknya membuat waktu dan uang anda kembali pulih.
- The High-Profile (Si Profil Tinggi)
  - ✦ Berusaha menggunakan sistem, untuk memperoleh popularitas dan ketenaran. Dan juga mungkin menggunakan sistem profil tinggi anda untuk mengiklankan kemampuannya
- The Competition (Si Pesaing)
  - ✦ Penyusup ini tertarik pada data yang anda miliki dalam sistem anda, ia mungkin seseorang yang beranggapan bahwa anda memiliki sesuatu yang dapat menguntungkan secara keuangan atau sebaliknya

INSTITUT TEKNOLOGI PLN Your Future Starts Today!

11

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

Dikti MONS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

## Istilah bagi penyusup

- Mundane ; tahu mengenai hacking tapi tidak mengetahui metode dan prosesnya.
- lamer (script kiddies) ; mencoba script2 yang pernah di buat oleh aktivis hacking, tapi tidak paham bagaimana cara membuatnya.
- wannabe ; paham sedikit metode hacking, dan sudah mulai berhasil menerobos sehingga berfalsafah ; HACK IS MY RELIGION.
- larva (newbie) ; hacker pemula, teknik hacking mulai dikuasai dengan baik, sering bereksperimen.
- hacker ; aktivitas hacking sebagai profesi.
- wizard ; hacker yang membuat komunitas pembelajaran di antara mereka.
- guru ; master of the master hacker, lebih mengarah ke penciptaan tools-tools yang powerful yang salah satunya dapat menunjang aktivitas hacking, namun lebih jadi tools pemrograman system yang umum.

INSTITUT TEKNOLOGI PLN Your Future Starts Today!

12

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

Dikti MONFS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

## Memahami Hacker Bekerja

- Secara umum hacker bekerja melalui beberapa tahapan :
  1. Tahap Mencari tahu system komputer sasaran.
  2. Tahap Penyusupan.
  3. Tahap Penjelajahan.
  4. Tahap Keluar dan menghilangkan Jejak.

INSTITUT TEKNOLOGI PLN Your Future Starts Today!

13

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

Dikti MONFS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

## CARA KERJA PENYUSUP

- Melacak sinyal dari jarak jauh menggunakan kartu jaringan wireless menggunakan receiver tambahan di luar ruangan.
- Menjadi unknown tak dikenal menggunakan firewall bawaan dari produk Microsoft atau peranti lain seperti ZoneAlarm dari Zone Lab untuk melindungi komputernya dari alat pemindai balik IDS (Intrusion Detection System).
- Mendapatkan IP Address, aim entrance point, dan server DHCP (Dynamic Host Configuration Protocol) menggunakan aplikasi seperti NetStumbler atau module wireless customer lainnya.
- Mengeksploitasi kelemahan – kelemahan jaringan wireless dengan cara yang tidak jauh beda dengan yang dilakukan oleh penyusup jaringan pada umumnya. Biasanya Attacker mengincar dengan kesalahan-kesalahan umum, misalnya : default IP, default password, dll
- Dengan bantuan alat custom analyzer, penyusup melakukan spot gelombang udara, mengambil contoh information yang ada di dalamnya, dan mencari MAC Address dan IP Address yang current yang bisa dihubungi.
- Mencuri information penting dari lalu lintas promote untuk memetakan jaringan target.

INSTITUT TEKNOLOGI PLN Your Future Starts Today!

14

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

Dikti MONFS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

## Dalam internetworking beberapa jenis gangguan dikenal dengan istilah:

1. Hacking, berupa pengrusakan pada infrastruktur jaringan yang sudah ada, misalnya pengrusakan pada sistem dari suatu server.
2. Phishing, berupa pemalsuan terhadap data resmi dilakukan untuk hal yang berkaitan dengan pemanfaatannya.
3. Deface, perubahan terhadap tampilan suatu website secara illegal.
4. Carding, pencurian data terhadap identitas perbankan seseorang, misalnya pencurian nomor kartu kredit, digunakan untuk memanfaatkan saldo yang terdapat pada rekening tersebut untuk keperluan belanja online.
5. Serta masih banyak istilah pada sistem keamanan jaringan yang berkaitan dengan penyalahgunaan maupun pengrusakan sistem yang sudah ada.

INSTITUT TEKNOLOGI PLN Your Future Starts Today!

15

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

Dikti MONFS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

## Aspek Keamanan Komputer

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

INSTITUT TEKNOLOGI PLN Your Future Starts Today!

16

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

Dikti MONS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

## Aspek Keamanan Komputer

### 2. Integrity

- Defenisi : Informasi tidak boleh diubah tanpa seijin pemilik informasi.
- Contoh : e-mail di Intercept ditengah jalan, diubah isinya, kemudian diteruskan ke alamat yang dituju.
- 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.

INSTITUT TEKNOLOGI PLN Your Future

17

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

Dikti MONS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

## Aspek Keamanan Komputer

### 4. Availability

- Defenisi : Berhubungan dengan ketersediaan informasi ketika dibutuhkan.
- Contoh hambatan :
  - "deniel of service attack" (Dos attack), dimana server dikirim permintaan (biasanya palsu) yang bertubi-tubi atau permintaan yang diluar perkiraan sehingga tidak dapat melayani permintaan lain atau bahkan sampai down, hang, crash.
  - Mailbom, dimana seorang pemakai dikirim e-mail bertubi-tubi (katakan ribuan email) dengan ukuran yang besar sehingga sang pemakai tidak dapat membuka e-mailnya atau kesulitan mengakses e-mailnya.

INSTITUT TEKNOLOGI PLN Your Future

18

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

Dikti MONS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

## Aspek Keamanan Komputer

### 5. Acces Control.

- Defenisi : Cara pengaturan akses kepada informasi. Berhubungan dengan masalah authentication dan juga privacy.
- Metode : Menggunakan kombinasi userid/password atau dengan menggunakan mekanisme lain.

### 6. Non-repudation.

- Defenisi : Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi. Dukungan bagi electronic commerce.

INSTITUT TEKNOLOGI PLN Your Future

19


INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

Dikti MONS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

## BENTUK-BENTUK DASAR SERANGAN :

Menurut W. Stallings, "Network and Internetwork Security," Prentice Hall, 1995. serangan (attack) terdiri dari :

- 1. Interruption** : Suatu aset sistem dihancurkan, sehingga tidak lagi tersedia atau tidak dapat digunakan. Serangan ditujukan kepada ketersediaan (availability) dari sistem. Contoh serangan adalah "Denial of service attack".



- 2. Interception** : Pengaksesan aset informasi oleh orang yang tidak berhak. Penyerangan terhadap layanan confidentiality. Contoh dari serangan ini adalah penyadapan (wiretapping) pencurian data pengguna kartu kredit

INSTITUT TEKNOLOGI PLN Your Future

20


INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

Dikti MONS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

### BENTUK-BENTUK DASAR SERANGAN :

Menurut W. Stallings, "Network and Internetwork Security," Prentice Hall, 1995. serangan (*attack*) terdiri dari :

- 2. Interception** : Pengaksesan asset informasi oleh orang yang tidak berhak. Penyerangan terhadap layanan confidentiality. Contoh dari serangan ini adalah penyadapan (wiretapping) pencurian data pengguna kartu kredit.



Source Interceptor Destination

INSTITUT TEKNOLOGI PLN Your Future

21


INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

Dikti MONS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

### BENTUK-BENTUK DASAR SERANGAN :

Menurut W. Stallings, "Network and Internetwork Security," Prentice Hall, 1995. serangan (*attack*) terdiri dari :

- 3. Modification** : Pihak yang tidak berwenang tidak saja berhasil mengakses, akan tetapi dapat juga mengubah (tamper) aset. Contoh dari serangan ini antara lain adalah mengubah isi dari website dengan pesan –pesan yang merugikan pemilik website.



Source Interceptor Destination

INSTITUT TEKNOLOGI PLN Your Future

22

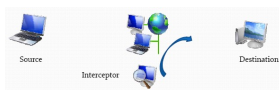
INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

Dikti MONS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

### BENTUK-BENTUK DASAR SERANGAN :

Menurut W. Stallings, "Network and Internetwork Security," Prentice Hall, 1995. serangan (*attack*) terdiri dari :

- 4. Fabrication** : Pihak yang tidak berwenang menyisip objek palsu ke dalam sistem. Contoh dari serangan jenis ini adalah memasukkan pesan-pesan palsu seperti e-mail palsu kedalam jaringan komputer.



Source Interceptor Destination

INSTITUT TEKNOLOGI PLN Your Future

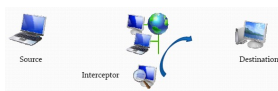
23

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

Dikti MONS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

### BENTUK-BENTUK DASAR SERANGAN :

- ☐ **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>) dicracked sehingga content situs tersebut berubah
  - Tahun 2001, Nasabah klikbca.com disadap identitas accountnya oleh seseorang yang membuat situs mirip (uri dan tampilannya) dengan klikbca yang asli
  - 10 Maret 1997 Seorang hacker dari Massachusetts berhasil pematikan 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>



Source Interceptor Destination

INSTITUT TEKNOLOGI PLN Your Future

24

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

**Dikti MONS MERDEKA BELAJAR Kampus Merdeka**

**INSTITUT TEKNOLOGI PLN**

## Pelanggaran Keamanan Komputer

Tahun	Khusus
1996	U.S Federal Computer Incident Response Capability (FedCIRC) melaporkan bahwa lebih dari 2500 "insiden" di sistem komputer atau jaringan komputer yang disebabkan oleh gagalnya sistem keamanan atau adanya usaha untuk membobol sistem keamanan.
1996	FBI National Computer Crimes Squad, Washington D.C., memperkirakan kejahatan komputer yang terdeteksi kurang dari 15% dan hanya 10% dari angka itu yang dilaporkan.
1997	Penelitian Deloitte Touch Tohmatsu menunjukkan bahwa dari 300 perusahaan di Australia, 37% (dua diantara lima) pernah mengalami masalah keamanan sistem komputernya.
1996	Ingris, NCC Information Security Breaches Survey menunjukkan bahwa kejahatan komputer menaik 200% dari tahun 1995 ke 1995 kerugian rata-rata US \$30.000 /insiden.
1998	FBI Melaporkan bahwa kasus persidangan yang berhubungan dengan kejahatan komputer meroket 950% dari tahun 1996 ke tahun 1997, dengan penangkapan dari 4 ke 42, dan terbukti di pengadilan naik 88% dari 16 ke 30 kasus.

INSTITUT TEKNOLOGI PLN **Your Future** Starts Today!

25

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

**Dikti MONS MERDEKA BELAJAR Kampus Merdeka**

**INSTITUT TEKNOLOGI PLN**

## Pelanggaran Keamanan Komputer

Tahun	Khusus
1988	Keamanan sistem mail sendmail di eksploitasi oleh Robert Tapan Morris sehingga melumpuhkan sistem internet. Diperkirakan biaya yang digunakan untuk memperbaiki dan hal-hal lain yang hilang digunakan untuk memperbaiki dan hal-hal lain yang hilang adalah sekitar \$100 juta. Ditahun 1990 morris dihukum dan hanya didenda \$10.000
10 Maret 1997	Seorang hacker dari Massachusetts berhasil mematikan telekomunikasi sebuah airport local sehingga mematikan komunikasi kontrol tower dan menghalau pesawat yang hendak mendarat. Dia juga mengacaukan sistem telepon di rutland massachusetts
1990	Kevin Poulsen mengambil alih sistem komputer telekomunikasi di Los Angeles untuk memenangkan kuis di sebuah radio local.
1995	Kevin Mitnick, mencuri 20.000 nomor kartu kredit, menyalin sistem operasi DEC secara ilegal dan mengambil alih hubungan telepon di New York dan California.
1995	Vladimir Levin membobol bank-bank di kawasan Wallstreet mengambil uang sebesar \$10 juta.
2000	Fabian Clone menjebol situs aetna.co.id dan jakarta mail dan membuat direktori atas namanya berisi peringatan terhadap administrator distus tersebut.

INSTITUT TEKNOLOGI PLN **Your Future** Starts Today!

26

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

**Dikti MONS MERDEKA BELAJAR Kampus Merdeka**

**INSTITUT TEKNOLOGI PLN**

## 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](#)

INSTITUT TEKNOLOGI PLN **Your Future** Starts Today!

27

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

**Dikti MONS MERDEKA BELAJAR Kampus Merdeka**

**INSTITUT TEKNOLOGI PLN**

## 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

INSTITUT TEKNOLOGI PLN **Your Future** Starts Today!

28

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

Dikti MONFS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

## 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

INSTITUT TEKNOLOGI PLN Your Future Starts Today!

29

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

Dikti MONFS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

## Security hole pada OS dan servis

❑ Ancaman

- [Buffer over flow yang menyebabkan local/remote exploit](#)
- [Salah konfigurasi](#)
- [Instalasi default yang mudah dieexploit](#)
- Dan lain-lain

INSTITUT TEKNOLOGI PLN Your Future Starts Today!

30

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

Dikti MONFS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

## Buffer overflow (1)

❑ Mengapa bisa terjadi buffer over flow?

- Program yang begitu kompleks, sehingga programmer sendiri tidak mengetahui kelemahan programnya
- Relies on external data to control pada program

```

void sample_function(void)
{
    char buffer[10];
    printf("Happy Happy!\n");
    return;
}

int main()
{
    sample_function();
    printf("Hello World!\n");
}
  
```

Figure 7.2  
Sample code with function call.

INSTITUT TEKNOLOGI PLN Your Future Starts Today!

31

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

Dikti MONFS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

## Buffer overflow (2)

❑ 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!

INSTITUT TEKNOLOGI PLN Your Future Starts Today!

32



INTERNASIONAL, MODERN, MANDIRI, UNGGUL

Dikti MONBS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

## 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

INSTITUT TEKNOLOGI PLN Your Future Starts Today!

33

INTERNASIONAL, MODERN, MANDIRI, UNGGUL

Dikti MONBS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

## Instalasi 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

INSTITUT TEKNOLOGI PLN Your Future Starts Today!

34

INTERNASIONAL, MODERN, MANDIRI, UNGGUL

Dikti MONBS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

## Ancaman serangan melalui jaringan

- ❑ **Ancaman**
  - [Sniffing \(penyadapan\)](#)
  - [Spoofing \(pemalsuan\)](#)
  - [Session hijacking \(pembajakan\)](#)
  - DOS attack
  - Spamming
  - Hacking
  - Malicious Software (Malware)
  - Snooping
  - Pharming
  - Defacing
  - Phishing
  - Jamming

INSTITUT TEKNOLOGI PLN Your Future Starts Today!

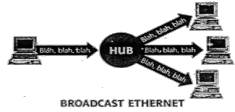
35

INTERNASIONAL, MODERN, MANDIRI, UNGGUL

Dikti MONBS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

## 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

INSTITUT TEKNOLOGI PLN Your Future Starts Today!

36

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

Dikti MONFS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

## 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

INSTITUT TEKNOLOGI PLN Your Future Share Your Future

37

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

Dikti MONFS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

## Session Hijacking (Pembajakan)

- Bagaimana Session Hijacking terjadi?
  - Sniff
  - Prediksi *sequence number*
  - Spoof IP/MAC address
- Pencegahan
  - Cegah sniffing
  - Cegah spoofing

INSTITUT TEKNOLOGI PLN Your Future Share Your Future

38

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

Dikti MONFS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

## 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

INSTITUT TEKNOLOGI PLN Your Future Share Your Future

39

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

Dikti MONFS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

## DOS attack(2)

- Ancaman mematikan servis secara local
  - Membunuh proses pada servis
  - Mengubah konfigurasi servis
  - Mengcrashkan servis
  - Dan lain-lain
- Pencegahan
  - Patch terbaru
  - Pengaturan *privilege* user dengan tepat
  - Deteksi perubahan dengan program *integrity-checking*

INSTITUT TEKNOLOGI PLN Your Future Share Your Future

40

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

Dikti MONBS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

## 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

INSTITUT TEKNOLOGI PLN Your Future Starts Today!

41

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

Dikti MONBS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

## 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

INSTITUT TEKNOLOGI PLN Your Future Starts Today!

42

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

Dikti MONBS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

## DOS attack(5)

- Ancaman menguras resource secara *remote*
  - Teknik Syn flood
  - Teknik Smurf attack
  - Teknik DDOS (Distributed DOS)
  - Dan lain-lain

INSTITUT TEKNOLOGI PLN Your Future Starts Today!

43

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

Dikti MONBS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

## 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

INSTITUT TEKNOLOGI PLN Your Future Starts Today!

44

INTERNASIONAL, MODERN, MANDIRI, UNGGUL

Dikti MONFS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

## 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)

INSTITUT TEKNOLOGI PLN Your Future

45

INTERNASIONAL, MODERN, MANDIRI, UNGGUL

Dikti MONFS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

## 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

INSTITUT TEKNOLOGI PLN Your Future

46

INTERNASIONAL, MODERN, MANDIRI, UNGGUL

Dikti MONFS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

## 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

INSTITUT TEKNOLOGI PLN Your Future

47

INTERNASIONAL, MODERN, MANDIRI, UNGGUL

Dikti MONFS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

## Jenis Attack(1)

- **Spamming** adalah kegiatan mengirim email palsu dengan memanfaatkan server email yang memiliki "smtp open relay" atau spamming bisa juga diartikan dengan pengiriman informasi atau iklan suatu produk yang tidak pada tempatnya dan hal ini sangat mengganggu bagi yang dikirim.
- **Hacking** adalah kegiatan menerobos program komputer milik orang/pihak lain. Hacker adalah orang yang gemar ngoprek komputer, memiliki keahlian membuat dan membaca program tertentu, dan terobsesi mengamati keamanan (security)-nya. "Hacker" memiliki wajah ganda; ada yang budiman ada yang pencolong. "Hacker" budiman memberi tahu kepada programmer yang komputernya diterobos, akan adanya kelemahan-kelemahan pada program yang dibuat sehingga bisa "bocor" agar segera diperbaiki. Sedangkan, hacker pencolong, menerobos program orang lain untuk merusak dan mencuri datanya.
- **Malware (Malicious Software)** adalah aplikasi komputer yang khusus dibuat dengan tujuan mencari kelemahan dan celah dari software. Malware terdiri dari pemrograman (kode, script, konten aktif, dan perangkat lunak lain) yang dirancang untuk mengganggu atau meniadakan software dengan tujuan untuk mengumpulkan informasi yang mengarah pada hilangnya privasi/eksploitasi/mendapatkan akses tidak sah ke sumberdaya sistem.
- **Snooping** adalah suatu pemantauan elektronik terhadap jaringan digital untuk mengetahui password atau data lainnya. Ada beragam teknik snooping atau juga dikenal sebagai eavesdropping, yakni: shoulder surfing (pengamatan langsung terhadap display monitor seseorang untuk memperoleh akses), dumpster diving (mengakses untuk memperoleh password dan data lainnya), digital sniffing (pengamatan elektronik terhadap jaringan untuk mengungkap password atau data lainnya).

INSTITUT TEKNOLOGI PLN Your Future

48

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

Dikti MONBS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

## Jenis attack(2)

- **Pharming** adalah situs palsu di internet, merupakan suatu metode untuk mengarahkan komputer pengguna dari situs yang mereka percaya kepada sebuah situs yang mirip. Pengguna sendiri secara sederhana tidak mengetahui kalau dia sudah berada dalam perangkap, karena alamat situsnya masih sama dengan yang sebenarnya.
- **Defacing** adalah kegiatan mengubah halaman situs/website pihak lain, seperti yang terjadi pada situs Merkominfo dan Partai Golkar, BI dan situs KPU saat pemilu 2004 lalu. Tindakan deface ada yang semata-mata iseng, untuk kebolehan, pamer kemampuan membuat program, tapi ada juga yang jahat, untuk mencuri data dan dijual kepada pihak lain.
- **Phishing** adalah kegiatan memancing pemakai komputer di internet (user) agar mau memberikan informasi data diri pemakai (username) dan kata sandinya (password) pada suatu website yang sudah di-deface. Phishing biasanya diarahkan kepada pengguna online banking, isian data pemakai dan password yang vital yang telah dikirim akhirnya akan menjadi milik penjahat tersebut dan digunakan untuk belanja dengan kartu kredit atau yang rekening milik korban.
- **Jamming** adalah aksi untuk mengacaukan sinyal di suatu tempat. Dengan teknik ini sinyal bisa di-ground-kan, sehingga sinyal tidak bisa ditangkap sama sekali. Jamming akan lebih berbahaya apabila dilakukan oleh orang yang tidak bertanggung jawab (misal: teroris), yang dengan aksinya mengakibatkan jaringan di suatu kota lumpuh (dalam rangka melancarkan aksi terornya).

INSTITUT TEKNOLOGI PLN Your Future Starts Today!

49

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

Dikti MONBS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

## Ancaman via aplikasi berbasis web (1)

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

INSTITUT TEKNOLOGI PLN Your Future Starts Today!

50

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

Dikti MONBS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

## 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

INSTITUT TEKNOLOGI PLN Your Future Starts Today!

51

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

Dikti MONBS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

## 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

INSTITUT TEKNOLOGI PLN Your Future Starts Today!

52

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

**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

INSTITUT TEKNOLOGI PLN *Your Future* Starts Today!

53

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

**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

INSTITUT TEKNOLOGI PLN *Your Future* Starts Today!

54

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

**Virus, worm**

- ❑ **Ancaman**
  - Kerusakan, kehilangan data
  - Menguras resource sistem (memory, processor, 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

INSTITUT TEKNOLOGI PLN *Your Future* Starts Today!

55

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

**Lapisan Keamanan**

1. Lapisan Fisik:
  - ✓ Membatasi akses fisik ke mesin:
    - ✓ Akses masuk ke ruangan komputer
    - ✓ Penguncian komputer secara hardware
    - ✓ Keamanan BIOS
    - ✓ Keamanan Bootloader
  - ✓ Backup Data :
    - ✓ Pemilihan piranti back-up
    - ✓ Penjadwalan Backup
  - ✓ Mendeteksi gangguan Fisik :
    - ✓ Log File : Log pendek atau tidak lengkap, log yang berisikan waktu yang aneh, log permissi atau kepemilikan yang tidak tepat, catatan pelayanan reboot atau restart, log yang hilang, masukan su atau logiri dari tempat janggal.
    - ✓ Mengontrol akses sumber daya.

INSTITUT TEKNOLOGI PLN *Your Future* Starts Today!

56

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

Dikti MONFS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

## Lapisan Keamanan

### 2. Keamanan Lokal :

- ✓ Berkaitan dengan user dan hak-haknya:
  - ✓ Berikan mereka fasilitas minimal yang diperlukan.
  - ✓ Hati-hati terhadap saat / dari mana mereka login, atau tempat seharusnya mereka login.
  - ✓ Pastikan dan hapus rekening mereka ketika mereka tidak lagi membutuhkan akses.

INSTITUT TEKNOLOGI PLN Your Future

57

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

Dikti MONFS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

## Lapisan Keamanan

### 3. Keamanan Root

- ✓ Hanya menjadi root dalam melakukan tugas tunggal tertentu.
- ✓ Batasi jalur perintah bagi pemakai root.
- ✓ Jangan menggunakan perangkat utilitas rlogin/rshrexec.

### 4. Keamanan File dan system file

- ✓ Directory home user tidak boleh mengakses perintah mengubah sistem, seperti partisi, perubahan device dan lain-lain.
- ✓ Lakukan setting limit system
- ✓ Atur akses dan permission file
- ✓ Selalu cek program-program yang tidak dikenal.

INSTITUT TEKNOLOGI PLN Your Future

58

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

Dikti MONFS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

## Lapisan Keamanan

### 5. Keamanan Password dan Enkripsi:

- ✓ Hati-hati terhadap brute force attack dengan membuat password yang baik
- ✓ Selalu mengenkripsi file yang diperlukan
- ✓ Lakukan pengamanan pada level tampilan, seperti screen saver.

### 6. Keamanan Kernel :

- ✓ Selalu Update kernel system operasi
- ✓ Ikut review bugs dan kekurangan-kekurangan pada system operasi

### 7. Keamanan Jaringan :

- ✓ Waspada! paket sniffer yang sering menyadap port ethernet
- ✓ Lakukan prosedur untuk mengecek integritas data
- ✓ Verifikasi informasi DNS
- ✓ Lindungi Network File Sistem
- ✓ Gunakan Firewall untuk barrier antar jaringan privat dengan jaringan eksternal.

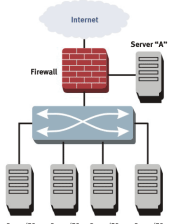
INSTITUT TEKNOLOGI PLN Your Future

59

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

Dikti MONFS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

## FIREWALL



JENIS-JENIS FIREWALL

1. Packet Filtering Gateway
2. Application Layer Gateway
3. Circuit Level Gateway
4. Statefull Multilayer Inspection Firewall

INSTITUT TEKNOLOGI PLN Your Future

60

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

Dikti MONFS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

## Packet Filtering Gateway

Packet filtering gateway dapat diartikan sebagai firewall yang bertugas melakukan filterisasi terhadap paket-paket yang datang dari luar jaringan yang dilindunginya.

Application Layer
Transport Layer
Internet Layer
Network Layer
Physical Layer

Gambar : Lapisan untuk Proses Packet Filtering Gateway

INSTITUT TEKNOLOGI PLN Your Future

61

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

Dikti MONFS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

## Application Layer Gateway

- Model firewall ini juga dapat disebut Proxy Firewall. Mekanismenya tidak hanya berdasarkan sumber, tujuan dan atribut paket, tapi bisa mencapai isi ( *content* ) paket tersebut.

Gambar Web server dengan Firewall

INSTITUT TEKNOLOGI PLN Your Future

62

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

Dikti MONFS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

Bila kita melihat dari sisi layer TCP/IP, firewall jenis ini akan melakukan filterisasi pada layer aplikasi ( *Application Layer* ).

Application Layer
Transport Layer
Internet Layer
Network Layer
Physical Layer

Gambar Proxy Firewall dilihat pada Model TCP/IP

INSTITUT TEKNOLOGI PLN Your Future

63

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

Dikti MONFS MERDEKA BELAJAR Kampus Merdeka INSTITUT TEKNOLOGI PLN

## Circuit Level Gateway

- Model firewall ini bekerja pada bagian Lapisan transport dari model referensi TCP/IP. Firewall ini akan melakukan pengawasan terhadap awal hubungan TCP yang biasa disebut sebagai TCP Handshaking, yaitu proses untuk menentukan apakah sesi hubungan tersebut diperbolehkan atau tidak. Bentuknya hampir sama dengan *Application Layer Gateway* , hanya saja bagian yang difilter terdapat ada lapisan yang berbeda, yaitu berada pada layer Transport.

Application Layer
Transport Layer
Internet Layer
Network Layer
Physical Layer

Gambar Circuit Level Gateway dilihat pada Model TCP/IP

INSTITUT TEKNOLOGI PLN Your Future

64

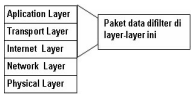


INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

**Dikti MONFS MERDEKA BELAJAR Kampus Merdeka** INSTITUT TEKNOLOGI PLN

## Statefull Multilayer Inspection Firewall

- Model firewall ini merupakan penggabungan dari ketiga firewall sebelumnya. Firewall jenis ini akan bekerja pada lapisan Aplikasi, Transport dan Internet.
- Dengan penggabungan ketiga model firewall yaitu *Packet Filtering Gateway*, *Application Layer Gateway* dan *Circuit Level Gateway*, mungkin dapat dikatakan firewall jenis ini merupakan firewall yang ,memberikan fitur terbanyak dan memeberikan tingkat keamanan yang paling tinggi.



Gambar Statefull Multilayer Inspection Firewall dilihat pada Model TCP/IP

INSTITUT TEKNOLOGI PLN **Your Future** Source: StudiJal

65

INTERNASIONAL, MODEREN, MANDIRI, UNGGUL

**Dikti MONFS MERDEKA BELAJAR Kampus Merdeka** INSTITUT TEKNOLOGI PLN

## Macam-macam Port Pada Jaringan

- 20 – FTP-DATA. "Active" koneksi FTP menggunakan dua port: 21 adalah port kontrol, dan 20 adalah tempat data yang masuk. FTP pasif tidak menggunakan port 20 sama sekali.
- 21 – Port server FTP yang digunakan oleh File Transfer Protocol. Ketika seseorang mengakses FTP server, maka ftp client secara default akan melakukan koneksi melalui port 21.
- 22 – SSH (Secure Shell). Port ini ini adalah port standar untuk SSH, biasanya diubah oleh pengelola server untuk alasan keamanan.
- 25 – SMTP, Simple Mail Transfer Protocol, atau port server mail, merupakan port standar yang digunakan dalam komunikasi pengiriman email antara sesama SMTP Server.
- 80 – WWW atau HTTP port server web. Port yang paling umum digunakan di Internet. jadi ketika user mengetikkan alamat IP atau hostname di web broeser maka web browser akan melihat IP tsb pada port 80
- 81, Web Server Alternatif  
ketika port 80 diblok maka port 81 akan digunakan sebagai port alternatif hosting website

INSTITUT TEKNOLOGI PLN **Your Future** Source: StudiJal

66