Syahrul Imardi, MT

#3

PENGANTAR MK KPL

KEAMANAN KOMPUTER

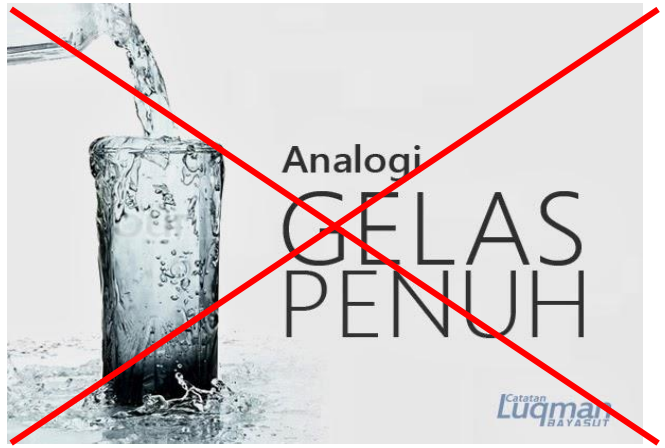
STMIK
Amik Riau

MATAKULIAH
KEAMANAN PERANGKAT LUNAK

SYAHRUL IMARDI, M.T

Pertemuan 3 : KEAMANAN KOMPUTER

TIPE-TIPE PROSES TRANSFORMASI ILMU



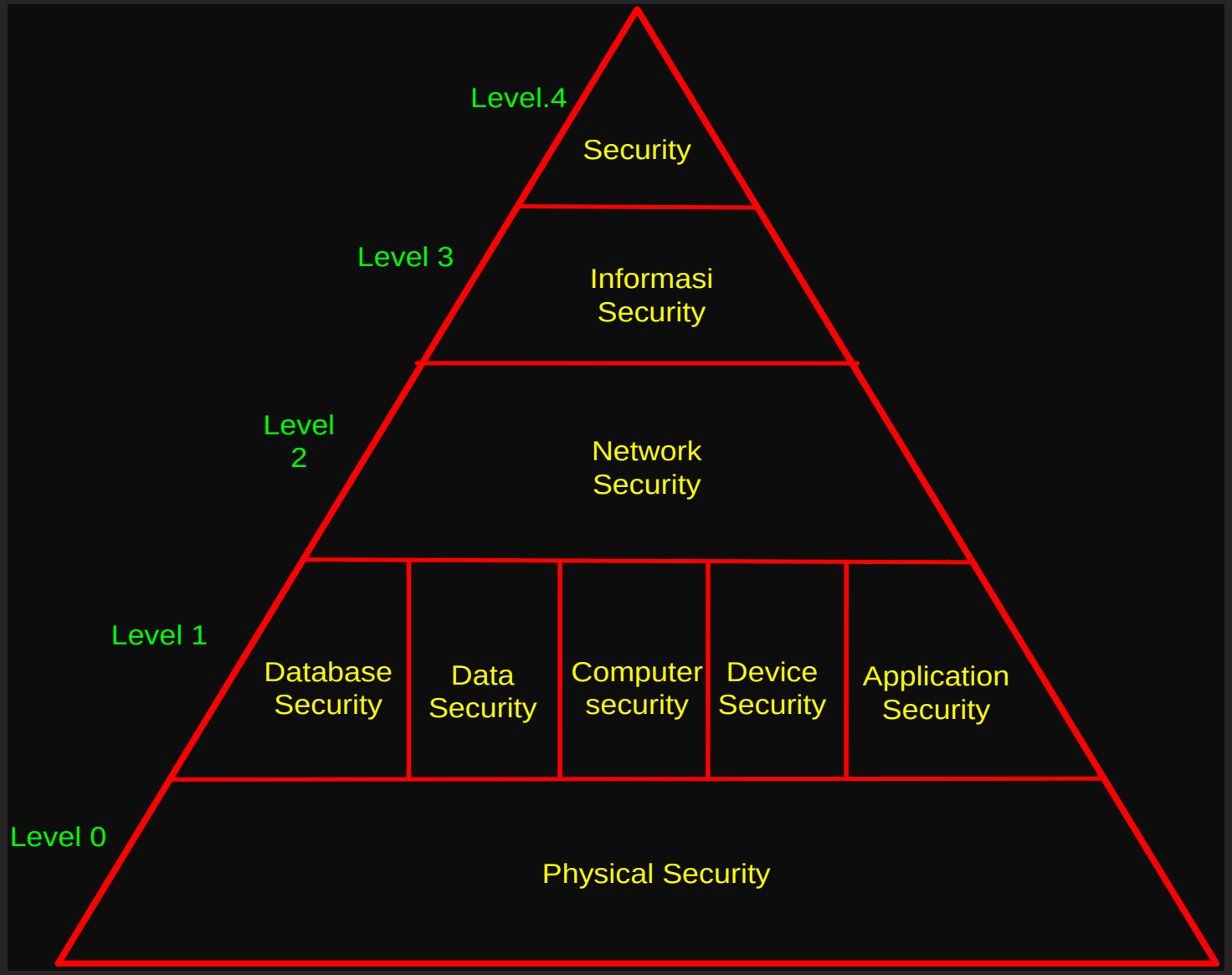
Aspek2 keamanan komputer

- Authentication
  - Agar penerima informasi dapat memastikan keaslian pesan dari orang yang diminta.
- Integrity
  - Keaslian pesan yang dikirim melalui sebuah jaringan, dan dapat dipastikan bahwa informasi yang dikirim tidak dimodifikasi
- Nonrepudiation
  - Merupakan hal yang bersangkutan dengan sipengirim, sipengirim tidak dapat mengelak bahwa dialah yang mengirim pesan/informasi itu
- Authority
  - Informasi yang ada pada sistem jaringan tidak dapat dimodifikasi oleh pihak yang tidak berhak akses
- Confithentiality
  - Usaha untuk menjaga informasi dari orang yang tidak berhak akses
- Privacy
  - pribadi
- Availability
  - ketersediaan informasi ketika dibutuhkan
- Access control
  - Pengaturan (user ID)

Aspek2 Ancaman komputer

- Interruption
  - Informasi yang ada dirusak dihapus ketika dibutuhkan data sudah tidak ada lg
- Interception
  - Informasi yang ada disadap/ orang yang tidak berhak akses kekomputer dimana informasi tersebut disimpan.
- Modifikasi
  - Merupakan ancaman terhadap integritas, orang yang tidak berhak berhasil menyadap lalulintas informasi yang sedang dikirim
- Febrication
  - Memalsukan

Security Methodology



Mendeteksi serangan

- **Anomaly Detection (Penyimpangan)**

  Mengidentifikasi perilaku tak lazim yang terjadi dalam Host atau Network.
- **Misuse Detection**

  Detektor melakukan analisis terhadap aktivitas sistem, mencari event atau set event yang cocok dengan pola Perilaku yang dikenali sebagai serangan.
- **Network Monitoring**

  (sistem pemantau jaringan) untuk mengatahui adanya lubang keamanan Biasanya dipakai (SNMP)
- **Intrusion Detection System (IDS)**

  Penghambat atas semua serangan yg akan menggangu sebuah jarigan.

Mencegah serangan

- Desain Sistem
  - Desain sistem yg baik tidak meninggalkan lobang2 yang memungkinkan terjadinya penyusupan
- Aplikasi yang dipakai
  - Aplikasi yg dipakai sudah diperiksa dan apakah sudah dapat dipercaya.
- Manajemen
  - Pengolahan suatu sistem yg baik menurut standard operating procedure (SOP)

Mempertahankan (Perlindungan)

Pada era jaringan, perlu dikwatirkan tentang keamanan dari sistem komputer, baik komputer PC atau yang terkoneksi dengan jaringan, seperti LAN

5 Langkah keamanan komputer.

- Aset
  - Perlindungan aset merupakan hal yg penting dan merupakan langkah awal dari berbagai implementasi keamanan komputer.
- Analisa Resiko
  - Identifikasi akan resiko yg mungkin terjadi, sebuah even yg potensial yg bisa mengakibatkan suatu sistem dirugikan.
- Perlindungan
  - Pada era jaringan, perlu dikwatirkan tentang keamanan dari system komp, baik PC atau yg terkoneksi dgn jaringan
- Alat
  - Tool yg digunakan pd PC memiliki peran penting dlm hal Keamanan krn tool yg digunakan harus benar2 aman.
- Prioritas
  - Perlindungan PC secara menyeluruh

- Strategi & Teknik Keamanan Komputer
- Keamanan fisik
- Kunci komputer
- Keamanan bios
- Xlock dan Vlock
- Mendeteksi gangguan keamanan fisik
- Password

Kejahatan Komputer

- Tugas!

1.Macam – macam serangan pada komputer

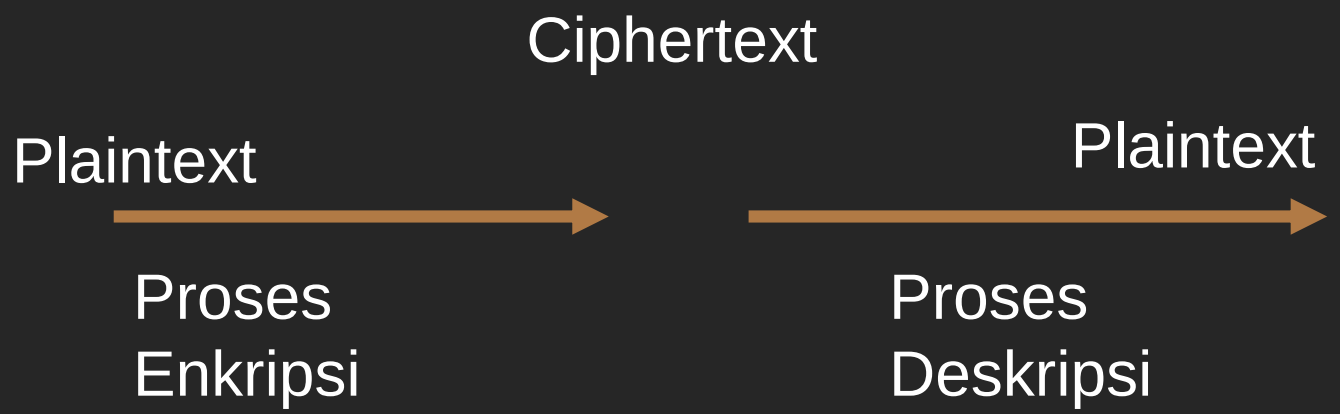
2. Sejarah Perkembangan Virus

Macam-macam Serangan

- Intrusion
- Intelligence
- Land Attack
- Logic Bomb
- Operation System Fingerprinting
- Smurf Attack
- Scanning
- Back door

Dasar Keamanan Komputer

- Kriptografi, Enkripsi dan Dekripsi



Enkripsi Modern

Enkripsi modern berbeda degan enkripsi konversional karena enkripsi modern sudah menggunakan komputer dalam pengoperasiannya. Berfungsi mengamankan data, baik yang ditrasfer melalui jaringan komputer maupun tidak.

Enkripsi Modern

- Simetris Kriptografi
- Asimetris Kriptografi
- Enkripsi Public-Key
- Fungsi *Hash* Satu Arah
- MD-5
- Tanda Tangan Digital
- Sertifikat Digital
- Secure Socket Layer
- PGP (Pretty Good Privacy)
- Biometric
- Analisa Pemacahan Algoritma Kriptografi

Simetris Kriptografi

Simetris Kriptografi adalah algoritma yang menggunakan kunci yang sama pada enkripsi dan deskripsinya.

Ex : Pesan x, chanel public, e xo

DES (data enkripsi standar) NIST⟶

Terbagi menjadi 3 kelompok

1. Pemrosesan kunci
2. Enkripsi data 64 bit
3. Deskripsi data 64 bit

Asimetris Kriptografi

Kunci asimetris adalah pasangan kunci kriptografi yang salah satunya digunakan untuk proses enkripsi dan yang satunya lagi untuk deskripsi. Semua orang yang Mendapatkan kunci publik dapat mengenkripsikan suatu pesan,sedangkan hanya satu orang saja yang memiliki rahasia tertentu.

Ex : RSA (Rivest, Shamir, Adleman)

Enkripsi Public-Key

Salah satu kesulitan dari enkripsi konvensional adalah mendistribusikan kunci yang digunakan dalam keadaan aman. untuk mengatasi kelemahan tersebut dengan suatu model enkripsi tampa memerlukan sebuah kunci untuk didistribusikan metode ini dikenal dengan nama enkripsi public key.

Untuk enkripsi konvensional, kunci yang digunakan pada proses enkripsi dan deskripsi adalah sama

Teknik yang dapat dilakukan Public-key

a. Masing-masing sistem dalam network akan menciptakan sepasang kunci yang digunakan enkripsi dan deskripsi pada informasi yang diterima.
b. Masing-masing sistem akan menerbitkan kunci enkripsinya (public key) dengan memasang dalam register umum atau file sedangkan pasangannya tetap dijaga sebagai kunci pribadi.
c. Jika A ingin mengirimpesan ke B, maka A akan mengankrpsikan pesannya dengan kunci public dari B.
d. Ketika Bm menerima pesan dari A, maka B akan menggunakan kunci privatenya untuk mendekripsi pesan dari A.

Fungsi Hash Satu Arah

a. Sidik jari (fingerprint). Membuat sidik jari dari suatu dokuman atau pesan, sebagai indentitas dari sipengirim pesan.
b. Fungsi kompresi. Kompresi besarnya dapat bervariasi sehingga dinamakan satu arah.
c. Messages digest. Merupakan inti sari dari suatu dokumen dan merupakan satu ringkasan dokumen yang dapat dipahami maknanya.

MD-5

Merupakan fungsi hash yang sering
digunakan untuk mengamankan suatu
jaringan komputer dan internet yang sengaja
dirancang dengan tujuan sebagai berikut :

1. Keamanan: Hal ini tidak isa dielakkan bila suatu sistem algoritma tidak bisa dipecahkan
2. Kecepatan: software yang digunakan memiliki kecepaten yang tinggi karena berdasarkan pada sekumpulan manipulasi.
3. Simple: tanpa menggunakan struktur data yang kompleks.

Tanda Tangan Digital

Tanda tangan digital merupakan tanda tangan yang dilakukan memakai alat elektronik yang berfungsi sama dengan tanda tangan manual. Tanda tangan digital merupakan kumpulan bit yang bisa melakukan fungsi elektronik yang memakai fungsi hash satu arah.

Sifat tandatangan digital:

1. Authentication: jaminan dari suatu pesan yang belum dimodifikasi didalam pengiriman, juga merupakan kunci yang membuktikan keaslian untuk kunci public, pemakai atau identifikasi sumber yang boleh memverifikasi hak untuk mengirim pesan.
2. Cuma berlaku untuk sekali pengirim dokuman, tandantangan tersebut tidak bisa di pindahkan kedokumen lainnya.
3. Keabsahan tandatangan digital itu dapat diperiksa oleh pihak menerima pesan, walaupun belum pnh bertemu.

Sertifikat Digital

Sertifikat digital adalah kunci pulik dan informasi penting mengenai jati diri pemilik kunci publik seperti misalnya nama, alamat, pekerjaan, jabatan, perusahaan.

Kunci publik adalah kunci yang dipublikasika kepada semua orang.

Ex: jika akan mengirim e-mail kepada seseorang kita harus mengetahui kunci publiknya

Secure Socket Layer

SLL dikembangkan oleh Netscape Communication Corp pada tahun 1994. SLL dapat melindungi transmisi HTTP dengan menambahkan lapisan enkripsi pengamanan

Keamanan yang diberikan SLL:

1. Menjadikan saluran (kanal) sebagai saluran (kanal) privat. Artinya data yang dikirim internet ke tempat tujuan akan terjamin keamanannya.
2. Kanel diautentikasi, server selalu diautentikasi dan di clien juga diautentikasi untuk menjaga keamanan data yang akan dikirim melalui jaringan komputer.
3. Kanel yang andal, dimana setiap data yang disadap dan dimodifikasi saat data dikirim oleh pihak yang tidak bertanggung jawab dapat diketahui oleh pihak yang sedang berkirim data (dideteksi) dengan menggunakan message integrity (authentication).

Tugas !

1. Situs yang memberikan jaminan Privasi
2. Situs Tip-tip Keamanan (security)

DiprintSC

Biometric

Biometrik adalah pengenalan identifikasi menggunakan fisik manusia. Ciri-ciri tersebut digunakan untuk membedakan suatu pola dengan pola yang lainya. Ciri yang bagus adalah ciri yang memiliki daya pembeda yang tinggi sehingga pengelompokan pola berdasarkan ciri yang dimiliki dapat dilakukan dilakukan dengan akurat.

Fingerprint (sidik jari)

Sidik jari dapat digunakan sebagai sarana Keamanan komputer karena memiliki ciri-ciri yang unik, setiap manusia memilikinya, dan selalu ada perbedaan antara satu dengan yang lainnya.

Pada dasarnya tubuh manusia Bisa dijadikan sebagai indentitas, seperti wajah, tangan, suara, mata, gaya berjalan, telinga dan lain sebagainya.

Keuntungan dan kerugian fingerprint

- Keuntungan
  - Teknologi yang canggih
  - Dimiliki semua orang
  - Ketelitian yang tinggi
  - Stabilitas jangka panjang
  - Kemampuan menampung berbagai fiture
  - Biaya yang secara komparatif rendah
- Kerugian
  - Kemampuan tidak bisa dipakai oleh banyak pemakai (orang cacat jari)
  - Dipengaruhi oleh kondisi kulit
  - Sensor mudah kotor

Hand geometry

Sistem biometric hand geometry bisa digunakan untuk keperluan autentikasi karena dimiliki oleh semua manusia (kecuali cacat tangan) dan unik.

- Keuntungan
  - Teknologi yang canggih
  - Tidak mengganggu
  - Penerimaan pemakai yang tinggi
- Kerugian
  - Ketelitian yang rendah
  - Mahal
  - Sukar digunakan untuk beberapa pamakai (anak2 rendah sedi)
  - Hilang jari atau tangan, sistem tidak bisa digunakan.

Eye Biometric

A. SISTEM RETINA BIOMETRIC

Merupakan sistem biometric yang memiliki teknologi yang canggih, dan keakuratan yang baik, sertaproteksi yang kuat karena ada di dalam bola mata.

- Keuntungan
  - Teknologi yang canggih
  - Potensi ketelitian yang tinggi
  - Stabilitas jangka panjang
  - Fitur terlindung
  - Perbedaan yang tinggi (ras, suku, dan bangsa)
- Kerugian
  - Susah digunakan
  - Faktor kesehatan
  - Harga yang mahal

B. SISTEM IRIS BIOMETRIC

Merupakan suatu sistem biometric yang memiliki teknologi yang canggih, keakuratan yang baik, dan proteksi yang kuat.

- Keuntungan
  - Teknologi yang canggih
  - Potensi ketelitian yang tinggi
  - Proses scannng yang cepat
- Keuntungan
  - Harga yang mahal
  - Jika kesahatan mata terganggu, sistem tidak bisa digunakan.

Lapisan Keamanan Jaringan

Komunikasi TCP/IP dapat mengamankan suatu jaringan dengan bantuan dari kriptografi dirancang untuk tujuan yang berbeda dalam pengamanan data dan komunikasi, baik stanlone computer maupun komputer yang terhubung dengan jaringan komputer, seperti LAN,WAN, Internet, salah satu cara pengamanan data dan komunikasi dalam jaringan meliputi secure socket layer (SSL), transport layer security (TLS) yang berfungsi mengamankan lalu lintas.

Protocol Jaringan

- IP (Internet Protocol)

  IP pada umumnya bertindak sebagai ground untuk Internet, IP menyediakan dua layanan interface kelayanan yang lebih tinggi.

  - *Send* digunakan untuk meminta pentrasmisian suatu unit data
  - *Deliver* digunakan oleh IP untuk menotifikasikan user akan kedatangan unit data.

Ex

- Send
  {
    Alamat sumber
    Alamat tujuan
    Protocol
    Tipe indikator layanan
    Identifikasi
    Penanda fragmentasi
    Waktu
    Panjang Data
    Pilihan data
  }

Deliver
{
  Alamat sumber
  Alamat tujuan
  Protocol
  Tipe indikator layanan

  Panjang data
  Pilihan data
}

Transmission Control Protocol (TCP)

TCP pada umumnya digunakan pada lanyanan internet

TCP merupakan reliabel yang memberikan tiga aplikasi layer:

1. Tujuan menerima aplikasi data jika data lain telah dikirim
2. Tujuan menerima semua aplikasi data
3. Tujuan tidakmenerima duplikat beberapa aplikasi data.

TCP

TCP akan melakukan KILL untuk suatu koneksi yang melanggar aturan dari salah satu aplikasi data diatas.

Ex :

- jika pertengahan paket TCP hilang atau rusak pada waktu pengiriman paket maka paket tersebut tidak akan diterima. jika pengiriman diulangai kembali dan tetap ada data yang hilang atau rusak,maka koneksi akan diputus secara otomatis.

User Datagram Protocol (UDP)

Sebagai tambahan dari TCP terdapat satu perotocol level trasport lainya yang umum digunakan sebagai bagian dari suite protocol TCP/IP yang disebut dengan UDP.

Pada dasarnya UDP adalah suatu layanan protocol yang kurang bisa diandalkan karena kurang bisa memberikan perlindungan dalam pengiriman dan duplikasi data.

Internet Control Message Protocol (ICMP)

ICMP adalah protocol pada TCP/IP yang bertugas mengirimkan pesan-pesan kesalahan dan kondisi lain dan memerlukan perhatian khusus. Haltersebut dapat dilakukan dengan mengevaluasi pesan yang dihasilkan oleh ICMP.

Jenis pesan ICMP ada dua

1. ICMP error message
2. ICMP query message

IP Security (IPsec)

Arsitektur keamanan IP yang dikenal dengan IP security (IPsec) menjadi standarisasi keamanan komputer. IPsec didesain untuk melindungi komunikasi dengan cara menggunakan TCP/IP.

Firewall

Firewall adalah alat yang digunakan untuk mencegah orang luar memperoleh akses ke suatu jaringan. Firewall merupakan suatu kombinasi dari perangkat lunak dan perangkat keras. Firewall biasanya menerapkan pengeluaran rencana atau perintah untuk menyortir alamat yang tak dikehendaki dan diinginkan

Cara kerja firewall

Firewall bekerja dengan mengamati paket IP yang melewatinya. Berdasarkan komfigurasi dari firewall, akses dapat diatur berdasarkan IP address, port, dan arah informasi.

- Untuk memahami firewalls bekerja kita perlu mengetahui pengalamatan IP. Statis & dinamis

- IP alamat statis adalah alamat yang permanen, yang merupakan alamat dari suatu mesin yang selalu dihubungkan keinternet.
- IP address dinamis adalah alamat IP yang selalu berubah-ubah yang berfungsi sebagai koneksi ke jaringan.

Karakteristik firewall

- Segala lalulintas jaringan, baik dari dalam ataupun dari luar harus melalui firewall. Hal tersebut menghalangangi semua akses dalam bentuk apapun kecuali firewall.
- Kebijakan keamanan hanya akan memberikan ijin untuk memasuki server atau jaringan komputer yang memenuhi syarat tertentu.
- Firewall sendiri bebas terhadap penetrasi, yang menandakan bahwa suatu sistem dapat dipercaya dan menjamin keamanan dari sistem operasi.

Tipefirewall

Ada beberapa macam perbedaan dari firewall, masing-masing tipe memiliki keuntungan dan kerugian, secara umum, tipe dari firewall ada 3 macam.

- Paket filter router
- Application level gateway
- Circuit level gateway

Paket filter router

Paket filter router menggunakan ketantuan untuk paket IP, mana yang boleh masuk dan mana yang harus ditolak.

Informasi yang disaring dari suatu paket yang melewati jaringan, diantarannya:

- Sumber IP address: alamat asli dari IP paket (Ex : 192,186.1.2)
- Tujuan IP address: alamat IP yang akan menerima IP paket (Ex : 192,186.1.3)
- Tujuan dan sumber transport-level address merupakan level trasport dari port number (seperti TCP dan UDP)
- IP protocol, yang berfungsi sebagai transpot protocol
- Interface: untuk router dengan tiga atau lebih port, dari interface router mana paket datang atau bertujuan.

Application level gateway

- Application level gateway juga dikenal dengan application-proxy firewall. Pada tipe ini user harus melakukan kontak dengan gateway yang menggunakan aplikasi TCP/IP, sepert TELNET atau FTP
- Aplikasi komponen proxy
  - telnet
  - FTP
  - rlogin
  - Sendmail
  - HTTP
  - The x window system

Circuit level gateway

- Circuit level gateway merupakan sistem proxy server yang secara statis menggambarkan jaringan lalulintas yang akan disampaikan. Circuit proxy selalu mengijzinkan paket yang berisi port number number yang diizinkan oleh aturan policy (kebijakan). Circuit level geteway berjalan pada level jaringan level OSI (**Open System Interconnection)**

Membangun firewall

- Kontriksi dari suatu firewall bukankah suatu pekerjaan yang mudah.
- Langkah-langkah untuk membangun suatu firewall adalah:
  - Identifikasi topologi dan protocol : indetifikasi topologi jaringan yang digunkan dan protocol.Hal tersebut merupakan langkah pertama untuk membangun suatu firewall. Itu hal yang utama bagi desainer suatu jaringan bila tidak mengetahuinya maka akan sulit memulai langkah selanjutnya.
  - Pengembangan Policy(kebijakan):Kebijakan disini tergantung keamanan apa yang akan dibuat , itu tergantung firewall yang akan dibuat .\
  - Memiliki Tool yang cukup :Untuk membangun sutu firewall dibutuhkan hardware dan software yang memadai.
  - Menggunakan tool yang efektif :maksudnya agar tidak ada pemborosan. Jika satu dirasa cukup untuk apa ditambah dengan yang lain.
  - Melakukan test konfigurasi.walaupun suatu kebijakan telah dibuat , konfigurasi dari suatu fire wall sangat berperan besar.

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?