Universitas
Pembangunan Jaya

Pertemuan 5, 6, dan 7:

INF210: Komputer dan Masyarakat

KEAMANAN DAN KEJAHATAN KOMPUTER

Dosen: Wayan Suparta, PhD

Pendahuluan

- **Keamanan komputer** (***computer security***) atau dikenal juga dengan sebutan **cybersecurity** atau **IT security** adalah keamanan infromasi yang diaplikasikan kepada komputer dan jaringannya. K**eamanan komputer** bertujuan membantu user agar dapat mencegah penipuan atau mendeteksi adanya usaha penipuan di sebuah sistem yang berbasis informasi.

- Infrastruktur Jaringan komputer, seperti LAN dan Internet, memungkinkan untuk menyediakan informasi secara cepat, sekaligus membuka potensi adanya lubang keamanan *(security hol*e).

- Mengapa keamanan komputer dibutuhkan?

Security Methodology

Level 5

Security

Level 4

Informasi Security

Level 3

Network Security

Level 2

Database Security | Data Security | Computer Security | Device Security | Application Security

Level 1

Physical Security

Aspek-aspek dalam Keamanan Komputer

Perbedaan	Privacy	Integrity	Authentication	Availability	Acces control	Non repudiation
Definisi	Menjaga informasi dari orang yang tidak berhak mengakses	Informasi tidak boleh diubah tanpa seizin pemilik informasi	Menyatakan bahwa informasi benar"nasli, org yg mengakses benar" org yg dimaksud	Upaya pencegahan ditahannya informasi	Sistem yang di rancang utk memungkinkan wewenang membatasi pnguna utk mengakses	Aspek menjaga agar seorang tidak dapat menyangkal telah melakukan sebuah transaksi
Bentuk serangan	Usaha penyadapan	Adanya virus trojan, pemakai lain yang mengubah informasi tanpa izin	Data dapat dimanupulasi	Pemakai diirimi permintaan yg bertubi2	Masuk kedalam suatu sistem tanpa diketahui admin,	Usaha penipuan Carding
Contoh	Data data yang sifatnya pribadi harus dapat di proteksi dlm penggunaan dan penyebarannya	Email di intercept di tengah jalan, di ubah isinya kemudian diteruskan ke alamat yang di tuju	Data dikonfirmasi ulang dgn captcha (kode)	Tidak dapat membuka email atau kesulitan mengakses emailnya	Pembatasan orang yang dapat mengakses informasi dan user harus menggunakan password	Seorang mengirimkan email untuk memesan barang tidak dapat menyangkal bahwa dia telah mengirim email tersebut padahal dia tidak memesan barang apapun
Usaha	Dengan menggunakan Teknologi Kriptografi, jangan memberikan data akun kepada orang lain	Menginstall anti virus, jangan menyebarkan informasi kita ke orang lain	1. Adanya tools yg membuktikan keaslian dokumen. 2. 2. akses contrl	Kinerja sistem harus selalu memadai tanpa menghiraukan jumlah user atau proses yg harus dijalankan	Memberikan hak akses kepada orang orang terpercaya dengan id	Jangan asal menyuruh orang lain untuk menfoto copy kartu kredit atau identitas

Aspek-aspek dalam Keamanan Komputer

Perbedaan	Privacy	iIntegrity	Authentication	Availability	Acces control	Non repudiation
Definisi	Pencegahan agar suatu informasi tidah dapat diakses oleh orang yang tidak berhak	Informasi tidak boleh diubah tanpa seizin pemilik informasi	Metode untuk menyatakan bahwa informasi asli, atau orang yang mengakses	Upaya pencegahan diitahannya informasi yang berlebihan oleh yg tidak berhak	Mengacu pada sistem yang dapat mengkontrol, memantau dan membatasi pergerakan	Merupakan hal yang bersangkutan dengan si pengirim, agar sesorg tdk menyangkal telah melakukan transaksi
Bentuk serangan	Usaha pembajakan, penyadapan, pencurian informasi	Adanya virus, trojan horse, atau user lain yang mengubah tanpa izin	Pencurian informasi	DOS (Denial Of Service) & Mailbomb	Masuk kedalam suatu sistem tanpa diketahui admin, tanpa hak izin akses	Adanya akun palsu/ email yang sengaja memesan barang
Contoh	Mengubah status/identitas diri pada suatu akun data pribadi, pencurian pada kartu kredit	Email di intercept di tengah jalan, diubah isinya, kemudian di teruskan ke alamat yang di tuju	Terjadi pada saat login	Membanjiri email korban dengan data / kiriman email yg banyak	Login website Database	Seseorg yang mengirim email untuk memesan tdk dpt menyangkal bahwa sudah mengirim
Usaha	Menggunakan teknologi enkskripsi untuk meningkatkan privacy	Pemasangan antivirus, mengenkripsi data & digital signature.	Watermarking (teknik penyembunyian data atau informasipada suatu media	Email firewall & Tarpitting (mencegah spam)	-Menambahkan alat keamanan, seperti RFID, Voice -- kombinasi angka dan huruf sebagai password -- firewall	Melakukan mengkornfirmasi agar menggunakan identitas Asli/KTP

Model Serangan Keamanan

Menurut W. Stallings (1995) dalam *"Network and Internetwork Securit*y," , serangan *(attac*k) terdiri dari :

- ***Interruption*:** Perangkat sistem menjadi rusak atau tidak tersedia. Serangan ditujukan kepada ketersediaan *(availabilit*y) dari sistem. Contoh serangan adalah "denial of service attack".
- ***Interception*:** Pihak yang tidak berwenang berhasil mengakses asset atau informasi. Contoh dari serangan ini adalah penyadapan *(wiretappin*g).
- ***Modification*:** Pihak yang tidak berwenang berhasil mengubah (tamper) aset. Contoh dari serangan ini antara lain adalah mengubah isi dari website dengan pesan-pesan yang merugikan pemilik web site.
- ***Fabrication*:** Pihak yang tidak berwenang menyisipkan objek palsu ke dalam sistem. Contoh dari serangan jenis ini adalah memasukkan pesan-pesan palsu seperti e-mail palsu ke dalam jaringan komputer.

Jenis Ancaman Keamanan Komputer

Jenis Ancaman	Penjelasan
Virus	Program komputer yang dapat menggandakan atau menyalin dirinya sendiri, dapat merusak perangkat lunak komputer.
adware	Iklan produk atau penawaran layanan yang merupakan bagian dari sebuah situs atau aplikasi.
Backdoor trojan	Program TCPWrapper yang dimodifikasi oleh orang yang tidak bertanggung jawab
bluejacking	Kerjanya mirip spam pada e-mail komputer
Spyware	Program yang bertindak sebagai mata-mata untuk mengetahui kebiasaan pengguna komputer dan mengirimkan informasi tersebut ke pihak lain.
Dialers	Mengubah halaman web, yang dikenal sebagai istilah ***deface***
Browser hijackers	Mengetahui bagaimana session hijacking dapat dilakukan, sehingga sejauh mana kelemahan dari situs web dapat digunakan untuk melakukan komunikasi.

Bentuk Ancaman Jaringan

HACKER	CRACKER
- Orang yang secara diam-diam mempelajari sistem yang biasanya sukar dimengerti untuk kemudian mengelolanya dan men-share hasil ujicoba yang dilakukannya. - Hacker tidak merusak sistem	- Orang yang secara diam-diam mempelajari sistem dengan maksud jahat – Muncul karena sifat dasar manusia yang selalu ingin membangun (salah satunya merusak)

- Macam-macam Serangan
  - ❖ Intrusion
  - ❖ Intelligence
  - ❖ Land Attack
  - ❖ Logic Bomb
  - ❖ Operation System Fingerprinting
  - ❖ Smurf Attack
  - ❖ Scanning
  - ❖ Back door

Penyusup (*intruder*)

Karakteristik Penyusup :

1. [redacted] - tipe penyusup ini pada dasarnya tertarik menemukan jenis sistem dan data yang anda miliki.
2. [redacted] - tipe penyusup ini berusaha untuk merusak sistem anda, atau merubah web page anda, atau sebaliknya membuat waktu dan uang anda kembali pulih.
3. [redacted] - tipe penyusup ini berusaha menggunakan sistem anda untuk memperoleh popularitas dan ketenaran. Dia mungkin menggunakan sistem profil tinggi anda untuk mengiklankan kemampuannya.
4. [redacted] - tipe penyusup ini tertarik pada data yang anda miliki dalam sistem anda. Ia mungkin seseorang yang beranggapan bahwa anda memiliki sesuatu yang dapat menguntungkannya secara keuangan atau sebaliknya.

Istilah bagi penyusup :

1. [redacted]; tahu mengenai hacking tapi tidak mengetahui metode dan prosesnya.
2. [redacted]; mencoba script2 yang pernah di buat oleh aktivis hacking, tapi tidak paham bagaimana cara membuatnya.
3. [redacted]; paham sedikit metode hacking, dan sudah mulai berhasil menerobos sehingga berfalsafah ; HACK IS MY RELIGION.
4. [redacted]; hacker pemula, teknik hacking mulai dikuasai dengan baik, sering bereksperimen.
5. [redacted] aktivitas hacking sebagai profesi.
6. [redacted]; hacker yang membuat komunitas pembelajaran di antara mereka.
7. [redacted]; master of the master hacker, lebih mengarah ke penciptaan tools-tools yang powerfull yang salah satunya dapat menunjang aktivitas hacking, namun lebih jadi tools pemrograman system yang umum.

Penanganan: Mendeteksi Serangan

- **Anomaly Detection (Penyimpangan)**
  mengidentifikasi perilaku tak lazim yang terjadi dalm 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 yg memungkinkan terjadinya penyusupan
- **Aplikasi yang dipakai**
  - Aplikasi yg dipakai sudah diperikasa dan apakah sudah dapat dipercaya.
- **Manajemen**
  - Pengolahan suatu sistem yg baik menurut standard operating procedure (SOP)
- **Mempertahankan (Perlindungan)**
  - Pada era jaringan, perlu dikuatirkan tentang keamanan dari sistem komputer, baik komputer PC atau yang terkoneksi dengan jaringan, seperti (LAN).

5 Langkah keamanan komputer

- **Aset**

  Perlindungan aset merupakan hal yang penting dan merupakan langkah awal dari berbagai implementasi keamanan komputer.
- **Analisa Resiko**

  Identifikasi akan resiko yang mungkin terjadi, sebuah even yang potensial yang bisa mengakibatkan suatu sistem dirugikan.
- **Perlindungan**

  Pada era jaringan, perlu dikwatirkan tentang keamanan dari sistem komputer, baik PC atau yang terkoneksi dgn jaringan
- **Alat**

  Tool yg digunakan pada PC memiliki peran penting dalam hal keamanan karena tool yang digunakan harus benar-benar aman.
- **Prioritas**

  Perlindungan PC secara menyeluruh.

Exercise #1

https://new.edmodo.com/groups/kommas-29276205

Sebutkan lima cara untuk memproteksi keamanan komputer!

Silakan jawab dalam edmodo. Akses akun: **v28hwd**

Strategi & Teknik Keamanan Komputer

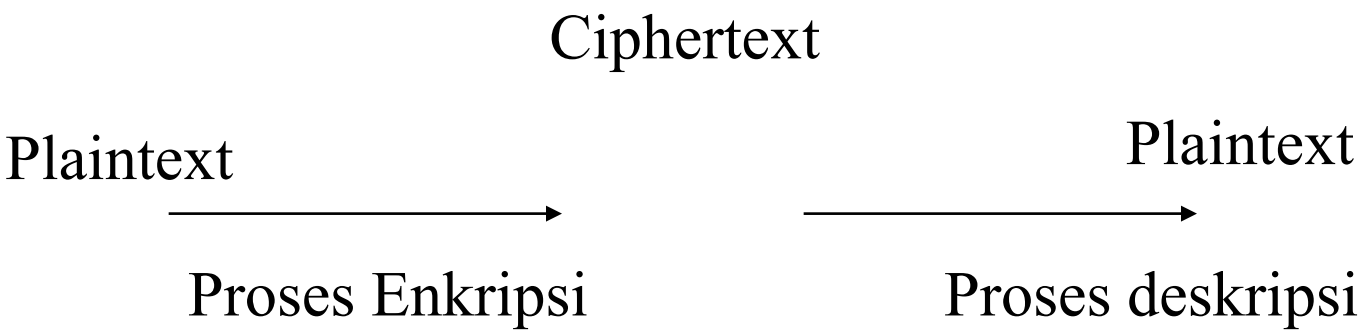
- *Keamanan fisik*
- Kunci komputer
- Keamanan bios
- Xlock dan Vlock
- Mendeteksi gangguan keamanan fisik
- Password

Enkripsi

- **Enkripsi** adalah sebuah proses yang melakukan perubahan sebuah kode yang bisa dimengerti menjadi sebuah kode yang tidak bisa dimengerti (tidak terbaca). Enkripsi dapat diartikan sebagai kode atau *chiper.*
- Metode enkripsi yang lebih umum adalah menggunakan sebuah algoritma dan sebuah kunci. Kunci harus diletakkan terpisah dari pesan yang terenkripsi dan dikirimkan secara rahasia. Teknik semacam ini disebut sebagai symmetric (single key) atau secret key cryptography.
- Enkripsi Modern:
  - Simetris Kriptografi
  - Asimetris Kriptografi
  - Enkripsi Public-Key
  - Fungsi *Hash* Satu Arah
  - PGP (Pretty Good Privacy)
  - Analisa Pemacahan Algoritma Kriptografi

  - Biometric
  - MD-5
  - Sertifikat Digital
  - Secure Socket Layer
  - Tanda Tangan Digital
- **Dekripsi** adalah proses dengan algoritma yang sama untuk mengembalikan informasi teracak menjadi bentuk aslinya.

Kriptografi, Enkripsi dan Dekripsi



Simetris Kriptografi adalah algoritma yang menggunakan kunci yang sama pada enkripsi dan deskripsinya.
Misalnya : Pesan x, chanel public, exo

DES (data enkripsi standar), 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.

Contoh: RSA (Rivest, Shamir, Adleman).

Enkripsi Public-Key

Salah satu kesulitan dari enkripsi konvensional adalah mendistribusikan kunci yang digunakan dalam keadaan aman. Ini dapat diatasi dengan sebuah kunci dengan nama enkripsi ***public key***. Teknik yang dapat dilakukan:

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 mengankripsikan pesannya dengan kunci public dari B.
d. Ketika B 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 dokumen atau pesan, sebagai identitas dari si pengirim 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 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 di dalam 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 dokumen, tanda tangan tersebut tidak bisa dipindahkan ke dokumen lainnya.
3. Keabsahan tandatangan digital itu dapat diperiksa oleh pihak menerima pesan, walaupun belum pernah bertemu.

Sertifikat Digital

Sertifikat digital adalah kunci publik dan informasi penting mengenai jati diri pemilik kunci publik seperti misalnya nama, alamat, pekerjaan, jabatan, perusahaan. Kunci publik adalah kunci yang dipublikasikan kepada semua orang. Contoh: 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. Kanal diautentikasi, server selalu diautentikasi dan di clien juga diautentikasi untuk menjaga keamanan data yang akan dikirim melalui jaringan komputer.
3. Kanal 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).

Biometric

Biometrik adalah 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.

Hand geometry

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

Eye Biometric

A. SISTEM RETINA BIOMETRIC

Merupakan sistem biometric yang memiliki teknologi yang canggih, dan keakuratan yang baik, serta proteksi 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 scanning yang cepat
- Keuntungan
  - Harga yang mahal
  - Jika kesahatan mata terganggu, sistem tidak bisa digunakan.

IP (Internet Protocol)

IP termasuk TCP/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.

Transmission Control Protocol (TCP)

TCP pada umumnya digunakan pada layanan 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 tidak menerima duplikat beberapa aplikasi data.

User Datagram Protocol (UDP)

Sebagai tambahan dari TCP terdapat satu protocol level transport lainnya 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. Hal tersebut 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 .

Paket filter router

Paket filter router menggunakan ketentuan 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 (Cth: 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 mengizinkan 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

- Kontruksi dari suatu firewall bukankah suatu pekerjaan yang mudah.
- Langkah-langkah untuk membangun suatu firewall adalah:
  - **Identifikasi topologi dan protocol**: indentifikasi topologi jaringan yang digunakan dan protocol. Hal tersebut merupakan langkah pertama untuk membangun suatu firewall. Itu hal utama bagi desainer suatu jaringan bila tidak mengetahuinya maka akan sulit memulai langkah selanjutnya.
  - **Pengembangan Policy (kebijakan)**: Kebijakan di sini tergantung keamanan apa yang akan dibuat, itu tergantung firewall yang akan dibuat.
  - **Memiliki Tool yang cukup**: Untuk membangun satu firewall dibutuhkan hardware dan software yang memadai.
  - **Menggunakan tool yang efektif** : maksudnya agar tidak ada pemborosan (efisiensi).
  - **Melakukan test konfigurasi**, walaupun suatu kebijakan telah dibuat , konfigurasi dari suatu firewall sangat berperan besar.

Exercise #2

https://new.edmodo.com/groups/kommas-29276205

Kerjakan dalam kelompok (1 kelompok = 2 orang) dan submit ke Edmodo

TUGAS DISKUSI

1. Langkah praktis membangun firewall.
2. Bagaimana membuat sebuah TCP/IP?
3. Bagaimana merealisasikan Open System Interconnection?
4. Cara pembuatan Internet Control Message Protocol (ICMP)
5. Berikan 5 contoh cara membuat protocol
6. Cara kerja internet protocol (IP)
7. Cara kerja sistem iris biometric
8. Cara membuat alamat TELNET
9. Cara membuat alamat FTP
10. Cara wifi memvariasikan IP address
11. Cara kerja system retina biometric
12. Cara kerja sidik jari sebagai alat keamanan komputer

13. Cara kerja sertifikasi digital
14. Cara kerja tanda tangan digital
15. Cara kerja Secure Socket Layer
16. Cara membuat fungsi hash
17. Cara kerja kriptografi
18. Cara kerja enkripsi
19. Terangkan proses deskripsi
20. Terangkan proses Pretty Good Privacy (PGP)
21. Terangkan cara membuat password
22. Terangkan cara kerja Xlock dan Vlock
23. Cara membuat username
24. Terangkan algoritma CAESAR CIPHER dari *plain text*