

**UJIAN AKHIR SEMESTER  
KEAMANAN INFORMASI**

**Soal 1 dan soal 2**



**Di Susun Oleh**

**Ahmad Fajar Novianto**

**1310651116**

**JURUSAN TEKNIK INFORMATIKA  
FAKULTAS TEKNIK  
UNIVERSITAS MUHAMMADIYAH JEMBER  
2014/2015**

Salah satu bagian mendasar dalam Information System Security adalah Access Control. Menurut definisi dari CISSP (Certified Information System Security Profesional) Study Guide, Access Control didefinisikan sebagai suatu proses untuk mengatur / mengontrol siapa saja yang berhak mengakses suatu resource-resource tertentu yang terdapat di dalam sebuah sistem. Di dalam proses ini akan diidentifikasi siapa yang sedang melakukan request untuk mengakses suatu resource tertentu dan apakah orang tersebut memiliki hak akses (authorized) untuk mengakses resource tersebut.

Access control memproteksi data terhadap unauthorized access atau akses yang dilakukan oleh orang yang memang tidak memiliki hak akses terhadap resource tersebut. Akses di sini bisa berupa melihat data (view) ataupun melakukan perubahan terhadap suatu data (modify).

Dengan demikian Access Control mendukung terwujudnya

- ☐ Confidentiality Memastikan data hanya bisa dilihat oleh orang yang memiliki hak akses untuk melihat data tersebut atau dikenal dengan istilah No Unauthorized Read
- ☐ Integrity Memastikan data hanya bisa ditulis dan diubah oleh orang yang memiliki hak akses untuk melakukan penulisan ataupun pengubahan terhadap data tersebut atau dikenal dengan istilah No Unauthorized Write

Ketika membahas tentang Access Control, kita akan menemui dua entitas utama yang terlibat, yaitu

- ☐ Subject of the Access Control Yang menjadi subject di sini adalah entitas yang mengajukan request / permintaan untuk melakukan akses ke data.
- ☐ Object of the Access Control Yang menjadi object di sini adalah entitas yang mengandung atau mengatur data. Atau dengan kata lain object adalah resource yang tersedia di dalam suatu sistem

## CONTOH

### **Access Control**

Aspek ini berhubungan dengan cara pengaturan akses kepada informasi. Hal ini biasanya berhubungan dengan klasifikasi data (public, private, confidential, top secret) & user (guest, admin, top manager, dsb.), mekanisme authentication dan juga privacy. Access control seringkali dilakukan dengan menggunakan kombinasi userid/password atau dengan menggunakan mekanisme lain (seperti kartu, biometrics).

## ...SOAL 2

### ANTI VIRUS



#### 1.1 pengertian anti virus

**Antivirus** adalah sebuah jenis perangkat lunak yang digunakan untuk mengamankan, mendeteksi, dan menghapus virus komputer dari sistem komputer. **Antivirus** disebut juga **Virus Protection Software**. Aplikasi ini dapat menentukan apakah sebuah sistem komputer telah terinfeksi dengan sebuah virus atau tidak. Umumnya, perangkat lunak ini berjalan di latar belakang (background) dan melakukan pemindaian terhadap semua berkas yang diakses (dibuka, dimodifikasi, atau ketika disimpan). Antivirus - antivirus terbaru sekarang tidak hanya mendeteksi virus. Program antivirus sekarang juga telah dilengkapi dengan kemampuan untuk mendeteksi spyware, rootkits, dan malware - malware lainnya. Tidak hanya itu, antivirus sekarang dilengkapi firewall untuk melindungi komputer dari serangan hacker dan anti spam untuk mencegah masuknya email sampah dan/atau virus ke inbox pengguna.

#### 1.2 Cara kerja anti virus

**Pada umumnya, cara kerja antivirus adalah:**

- Pendeteksian dengan menggunakan basis data virus signature (*virus signature database*): Cara kerja antivirus ini merupakan pendekatan yang banyak digunakan oleh antivirus tradisional, yang mencari tanda-tanda dari keberadaan dari virus dengan menggunakan sebagian kecil dari kode virus yang telah dianalisis oleh vendor antivirus, dan telah dikatalogisasi sesuai dengan jenisnya, ukurannya, daya hancurnya dan beberapa kategori lainnya. Cara ini terbilang cepat dan dapat diandalkan untuk mendeteksi virus-virus yang telah dianalisis oleh vendor antivirus, tapi tidak dapat mendeteksi virus yang baru hingga basis data virus signature yang baru diinstalasikan ke dalam sistem. Basis data virus signature ini dapat diperoleh dari vendor antivirus dan umumnya dapat diperoleh secara gratis melalui download atau melalui berlangganan (*subscription*), dan/atau
- Pendeteksian dengan melihat cara bagaimana virus bekerja: Cara kerja antivirus seperti ini merupakan pendekatan yang baru yang dipinjam dari teknologi yang diterapkan dalam Intrusion Detection System (IDS). Cara ini sering disebut juga sebagai **Behavior-blocking detection**. Cara ini menggunakan policy (kebijakan) yang harus diterapkan untuk mendeteksi keberadaan sebuah virus. Jika ada kelakuan perangkat lunak yang "tidak wajar" menurut policy yang diterapkan, seperti halnya perangkat lunak yang mencoba untuk

mengakses address book untuk mengirimkan e-mail secara massal terhadap daftar e-mail yang berada di dalam address book tersebut (cara ini sering digunakan oleh virus untuk menularkan virus melalui e-mail), maka antivirus akan menghentikan proses yang dilakukan oleh perangkat lunak tersebut. Antivirus juga dapat mengisolasi kode-kode yang dicurigai sebagai virus hingga administrator menentukan apa yang akan dilakukan selanjutnya. Keuntungan dari cara ini adalah antivirus dapat mendeteksi adanya virus-virus baru yang belum dikenali oleh basis data virus signature. Kekurangannya, jelas karena antivirus memantau cara kerja perangkat lunak secara keseluruhan (bukan memantau berkas), maka seringkali antivirus membuat alarm palsu atau "*False Alarm*" (jika konfigurasi antivirus terlalu "keras"), atau bahkan mengizinkan virus untuk berkembangbiak di dalam sistem (jika konfigurasi antivirus terlalu "lunak"), terjadi false positive. Beberapa produsen menyebut teknik ini sebagai *heuristic scanning*. Teknologi Heuristic Scanning ini telah berkembang begitu jauh hingga sekarang. Beberapa antivirus mengecek sebuah file dengan definisi biasa. Jika lolos dari deteksi biasa, maka file tersebut dijalankan di sebuah lingkungan virtual. Semua perubahan yang dilakukan file bersifat seperti virus, maka pengguna akan diperingatkan.

### Cara Menginstal Anti Virus Avira

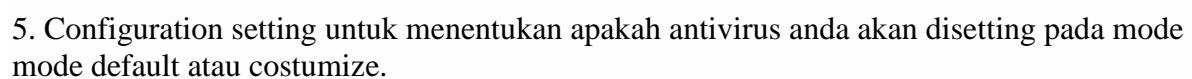
1. Klik 2x pada file aplikasi yang telah anda download untuk mengexecution/memulai instalasi.



2. Click "Continue" pada button untuk proses selanjutnya



3. Biarkan proses instalasi selesai dan akan muncul gambar seperti dibawah ini.



6. Anda akan ditawarkan Licence Agreement untuk melanjutkan proses instalasi atau membatalkannya. Centang I agree dan klik next untuk melanjutkan proses instalasi.



7. Instalasi akan memberitahukan bahwa antivirus yang anda install adalah versi gratis pribadi dan tidak dapat digunakan untuk kepentingan publik? Untuk melanjutkan klik next.



8. Pilih salah satu mode instalasi complete (keseluruhan) atau custom (sebagian/sesuai keinginan anda). Saya sarankan untuk memilih complete mode untuk lebih amannya. Dan agar semua sistem protek tertanam pada antivirus anda. Dan tekan next untuk melanjutkan instalasi.



9. Dalam step ini anda akan di suguhkan pilihan apakah anda akan memakai antivirus ini dengan Registrasi Valid Lisence ataukah menggunakan Free Lisence dengan setting dan konfigurasi standart Avira. Untuk Free Mode unchecked check box bawah sehingga Registration Window non aktif. Kemudian click next.



10. Selanjutnya system akan melakukan instalasi program tersebut, tunggu sampai proses instalasi complete. Selama proses instalasi tampilan akan tampak seperti gambar berikut:





11. Setelah instalasi selesai anda bisa langsung menggunakan antivirus tersebut, atau berlanjut ke advance setting untuk melakukan secure scanning. Klik OK untuk melanjutkan proses scanning.



Kelebihan :

Mampu mendeteksi virus-virus yang tidak bisa dideteksi antivirus lain

Terintegrasi dengan pendeteksi Rootkit

Kemudahan untuk mengaktifkan / non aktifkan antivirus.

Proses scan relatif cepat

Pemakaian resources memori yang kecil

Update Virus Definition yang relatif cepat

Ada fasilitas untuk mencari nama virus, dari daftar yang ada

Mampu menambah Scheduler scan atau update sebanyak mungkin.

Kelemahan :

Kadang salah mendeteksi aplikasi/file sebagai virus.



Customisasi scan hanya untuk drive, tidak bisa untuk folder.

Ukuran Update manual yang harus di download cukup besar, belum ada alternatif yg lebih kecil.

Membuka file karantina yang berisi ribuan akan sangat lama

Aplikasi tidak bisa di maximize