Mencegah Virus Tanpa Anti-Virus untuk Win XP, Win2K & Win2K3

Fandi Gunawan
fandigunawan@gmail.com
http://fandigunawan.wordpress.com

Makin maraknya (baca:hebatnya) virus-virus lokal yang terkadang terlambat dikenali anti-virus telah menjadi momok bagi pengguna sistem operasi Windows. Windows masih merupakan sistem operasi yang menguasai pasaran desktop, baik yang digunakan secara legal maupun ilegal. Masuknya virus-virus lokal lebih diperparah dengan kurang *update*-nya anti-virus dan kurangnya pengetahuan tentang *core* (baca:dasar) Windows itu sendiri. Namun bisakah kita meminimalisir peluang terinfeksinya komputer kita dengan virus-virus ini tanpa menggunakan anti-virus? Jawabannya akan dibahas di artikel ini.

Sebagai tambahan cerita penulis, sendiri telah mencoba cara ini untuk menjegal beberapa virus dan berakhir sukses. Sekitar belasan virus lokal maupun non lokal diinfeksikan secara sengaja maupun tidak sengaja pada komputer sendiri dan hasilnya Windows tetap berfungsi secara normal ataupun memimalisir ekses negatif virus-virus tersebut.

Sebenarnya apakah virus itu sendiri berbahaya? Menurut penulis, virus tidaklah berbahaya kalau tidak membius sistem yang “hidup”. Hal ini pernah penulis pelajari ketika masih SMA dengan materi mengenai virus (bukan virus komputer namun virus biologis). Dan hal ini juga berlaku pula untuk virus komputer. Virus sebenarnya menjadi berbahaya ketika:

1. Menginfeksi komputer dan menjadikannya agen untuk menyebarkan dirinya
2. Menginfeksi data-data dan menyebabkan virus tersebut menyebar melalui data yang terinfeksi
3. Mengubah pengaturan komputer sehingga mengganggu kerja kita

ataupun dilakukan penulis virus (virus writer) untuk mempersulit pembasmian virus tersebut
4. Merusak piranti keras maupun piranti lunak yang kita gunakan sehingga perlu diganti/diperbaiki

Virus sendiri selama ini banyak menginfeksi karena kita menggunkan akun yang mempunyai hak administrator (kuasa penuh) sehingga bila kita terinfeksi maka sistem secara otomatis secara keseluruhan akan terinfeksi. Hal ini akan berbeda bila kita punya sesuatu yang terbatas yang bilamana komputer kita terinfeksi virus tidak punyak kuasa/hak untuk merubah/menginfeksi sistem.

Ilustrasinya adalah sebagai berikut:
1. Akun dengan hak administrator bila terinfeksi maka ia (sengaja atau tidak sengaja) dapat dimanfaatkan oleh virus-virus ini untuk menginfeksikan dirinya ke sistem maupun data-data karena ia punya hak penuh untuk mengubah sistem dan data-data
2. Akun dengan hak terbatas ketika terinfeksi maka akses terbatas diberlakukan oleh operating system. Semisal virus tersebut hendak menginfeksi file-file kritis Windows, maka akses ke file-file tersebut akan ditolak. Hal ini juga berlaku ketika virus tersebut hendak mengganti pengaturan Windows yang dapat mengganggu kinerja Windows, maka akesnya akan ditolak. Hal ini dikarenakan Windows sendiri sebenarnya telah membatasi akses ke pengaturan maupun akses untuk merubah file-file yang sangat penting di Windows.

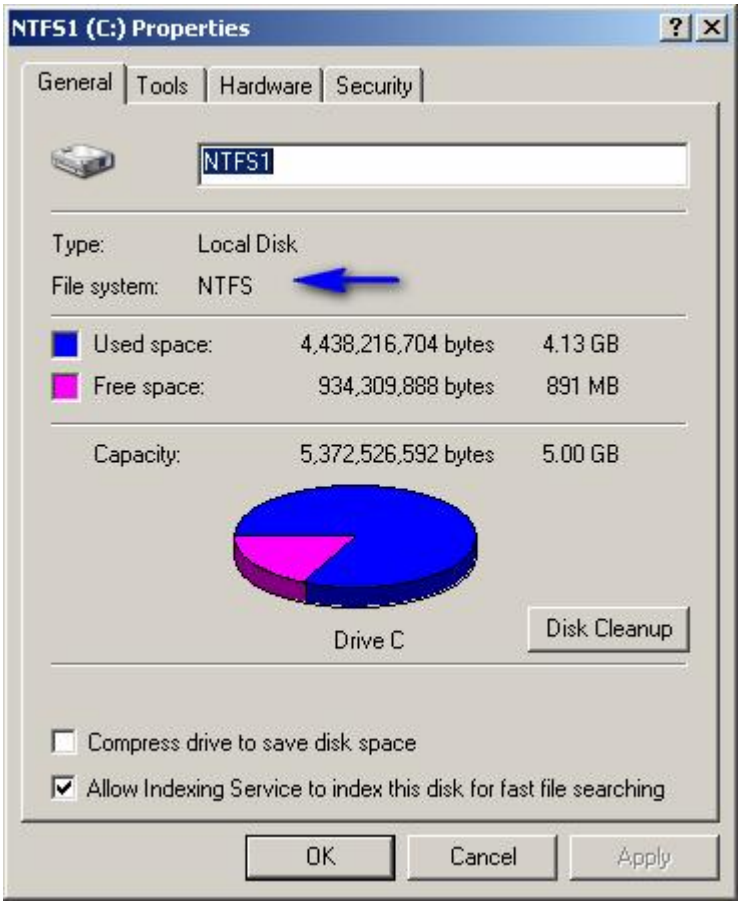
Cukup dengan dasar-dasar mengenai virus kita akan coba praktekkan secara langsung.

Pertama bila kita menggunakan sistem operasi, pastikan bahwa operating sistem tersebut terus-menerus di*update*/gunakan rilis terbaru. Disini penulis menggunakan Windows XP sp 2 yang sistem dasarnya cukup mirip dengan dua operating system lainnya yaitu Windows 2000 dan Windows 2003.

Kedua untuk Windows XP, 2K dan 2K3 pastikan Anda menggunakan NTFS sebagai filesystem-nya karena kita dapat memetik beberapa keuntungan:

1. Fitur kepemilikan (ownership) yang paling penting dikasus ini
2. Penjurnalan
3. Kompresi
4. Enkripsi
5. Lain-lain yang penulis sendiri kurang mengerti (maklum gak seberapa mendalami *file-system*)

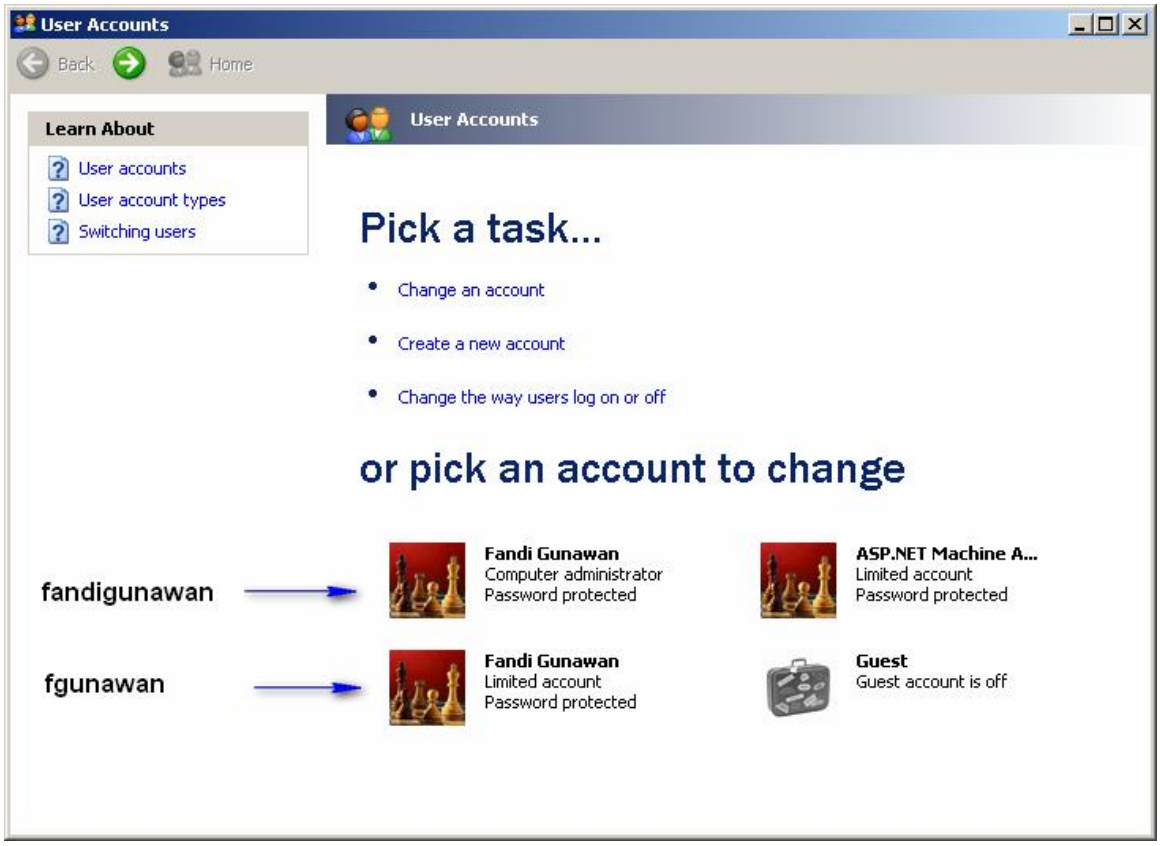
Berikut cara untuk mengetahui apakah Anda telah menggunakan NTFS
Klik kanan salah satu *drive* dan pilih *properties*



Disini penulis telah membuat dua akun : **fandigunawan** (administrator) dan **fgunawan** (limited account).

PERHATIAN KERAS : Perhatikan perbedaan antara penggunaan nama **fandigunawan** dan **fgunawan** pada contoh di artikel ini.

Anda dapat membuat sendiri dengan pergi ke Control Panel lalu ke User Account. Berikut tampilannya :



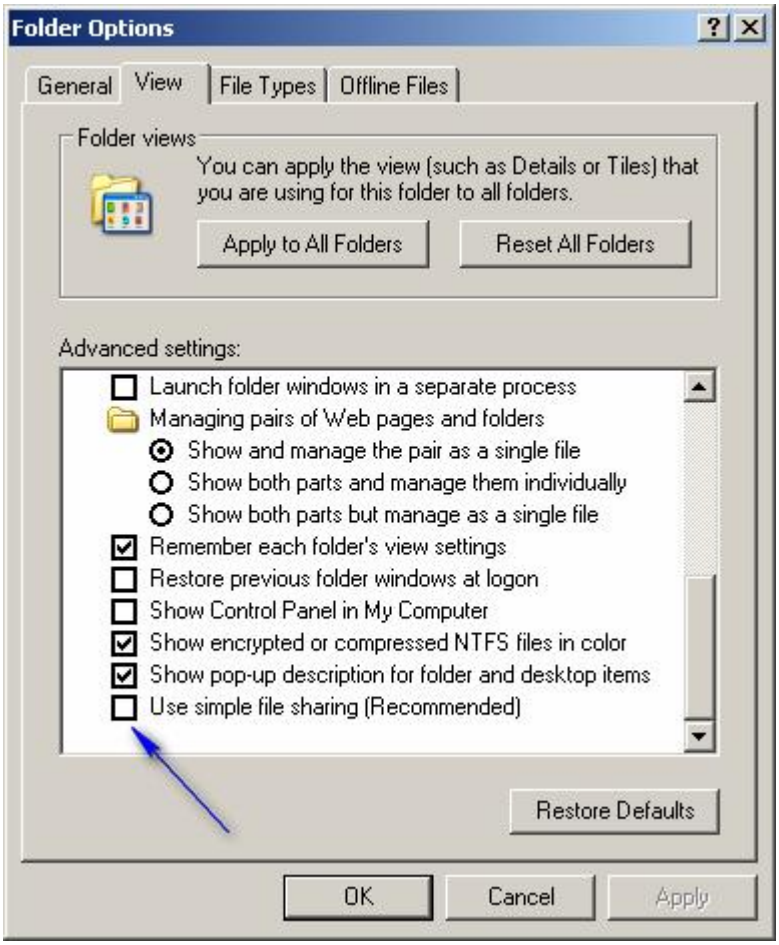
Perhatikan dengan seksama perbedaan tipe akun **fandigunawan** dan **fgunawan**.

Sebagai informasi tambahan di Windows terdapat group dan user.
User yang punya kekuasaan terbatas (*limited account*) masuk ke group **Users**
Administrator akan dimasukkan group **Administrators**.

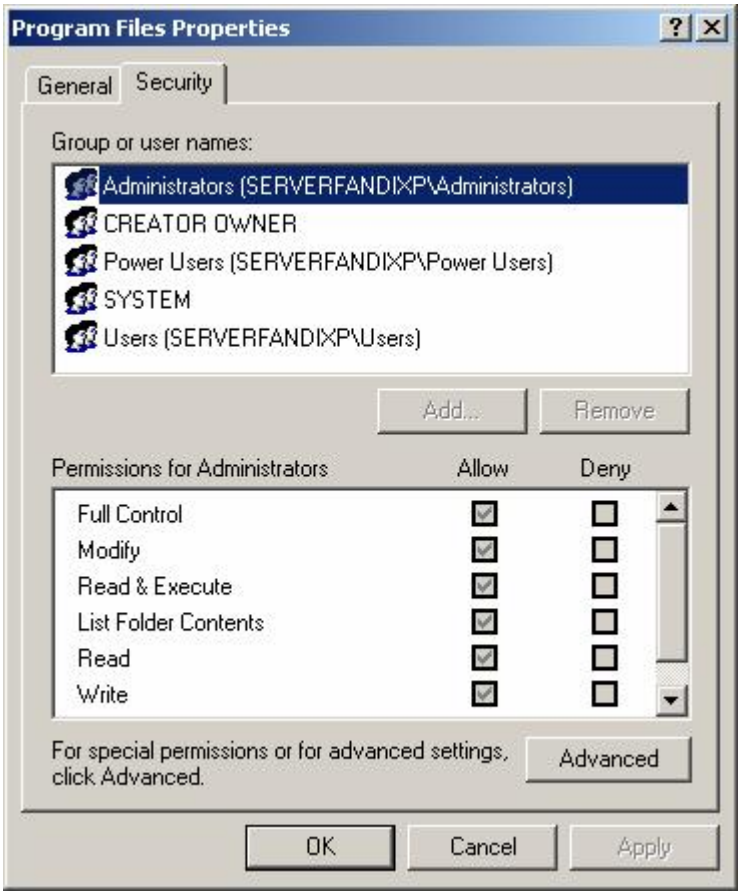
Hal inilah yang akan kita manfaatkan.

Ketiga, untuk mempermudah kita mengatur Windows kita perlu set beberapa hal:

1. Pergi ke *Windows Explorer – Tools – Folder Options* di tab *View* hilangkan tanda cek di pilihan *Use simple file sharing (recommended)*



Efek yang terjadi adalah tiap kali kita klik kanan file, drive ataupun folder akan muncul hal sebagai berikut:



Yang mana kita dapat mengubah akses ke file, drive ataupun folder tertentu.
Yup, persiapan cukup. Sekarang kita akan belajar cara kerjanya.

Secara default Windows sebenarnya telah diberikan fitur-fitur keamanan yang cukup memadai (meski cukup banyak tambal sulam).
Fasilitas yang ada tersbut misalnya adalah :

1. Kepemilikan di file-systemnya
2. DEP (Data Execution Prevention)
3. Firewall
4. Proteksi terhadap file-file penting Windows

Sekarang pakailah akun dengan hak akses terbatas (limited account) dalam contoh ini penulis menggunakan akun **fgunawan**. Jangan gunakan akun administrator kalau tidak terpakasa, misalnya untuk instalasi driver maupun merubah pengaturan Windows.

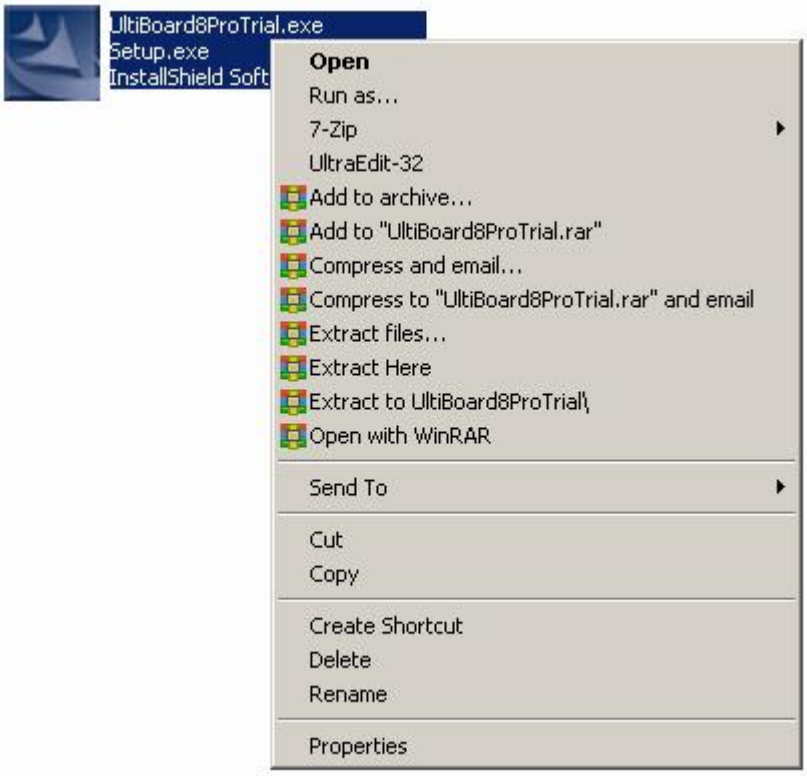
Sekarang kita harus terbiasa dengan beberapa hal yang penulis sendiri rasa sangat penting :

1. Fitur *runas* yang berguna untuk menjalankan program dengan hak akun lain

Runas merupakan fitur Windows usntuk mengeksekusi suatu file executable atau yang lain dengan hak akun lain.
Berikut ilustrasi ketika penulis hendak menginstal program. Ketika kita eksekusi setup.exe biasanya Windows akan menanyakan password secara otomatis dan akan muncul :

Nah masukkan user name yang punya kuasa administrator dan passwordnya kemudian OK. Jika benar maka program instalasi akan berjalan mulus.

Sebagai contoh ketika kita mau instalasi aplikasi yang bila pada kesempatan ini tidak berbentuk setup.exe maka gunakan :
Klik kanan file tersebut dan klik di run as ...



Nah Anda tinggal memasukkan password akun yang punya kuasa administrator dan jalankan instalasi seperti biasa.

Apa yang terjadi kalau kita eksekusi biasa?

a. File-file yang dikopikan oleh installer tersebut yang masuk ke direktori penting Windows seperti :
    i. Program Files

ii. Windows
Akan ditolak aksesnya (access denied)

b. Akses ke registry akan sangat dibatasi (tergantung pada *previledge* yang ada pada akun yang dipakai)
c. Pesan error dari installer sendiri

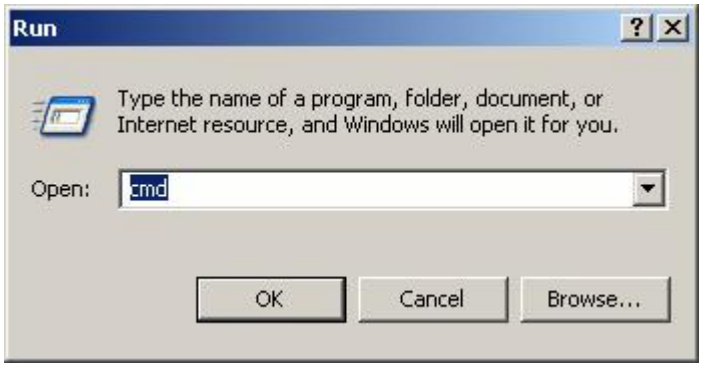
Nah dengan pengetahuan ini sebenarnya virus yang menyerang direktori-direktori penting Windows dan registry dapat ditangkal, jadi bisa buat menangkal mayoritas virus-virus yang ada dipasaran.

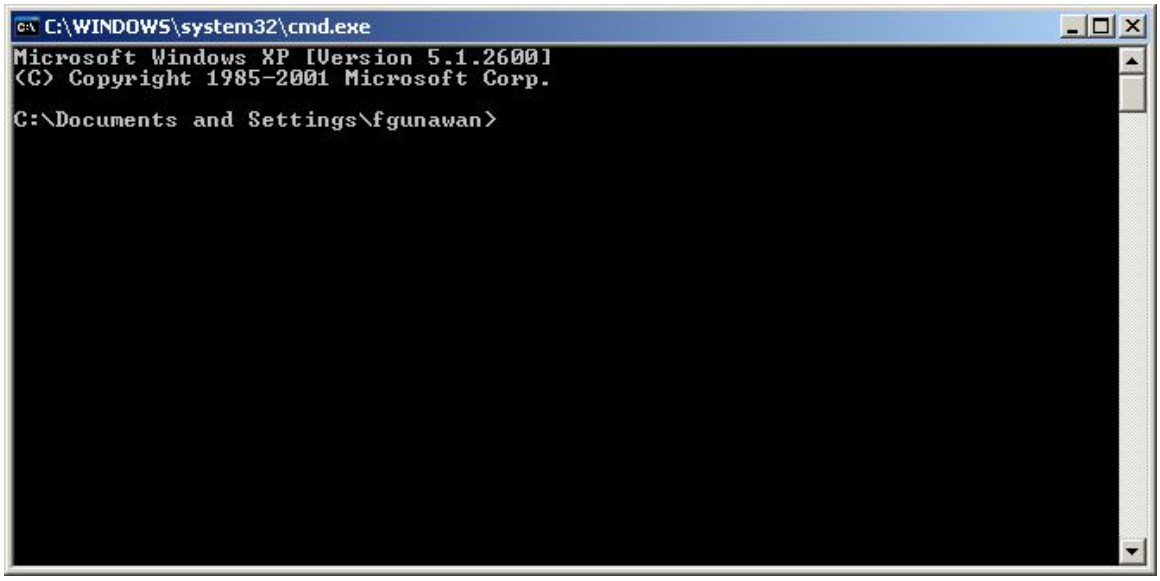
2. Larangan – larangan yang biasanya tidak kita temui
   Pada setting ini terkadang kita perlu sedikit ribet dengan seringnya melakukan klik kanan -> run as ... karena kita butuh akses yang punya previledge lebih tinggi (misalnya admin).
3. Terbiasa dengan setting baru yang kita aplikasikan
   Kita harus terbiasa dengan setting yang baru diaplikasikan ini.

Beberapa aplikasi yang membutuhkan previledge administrator :

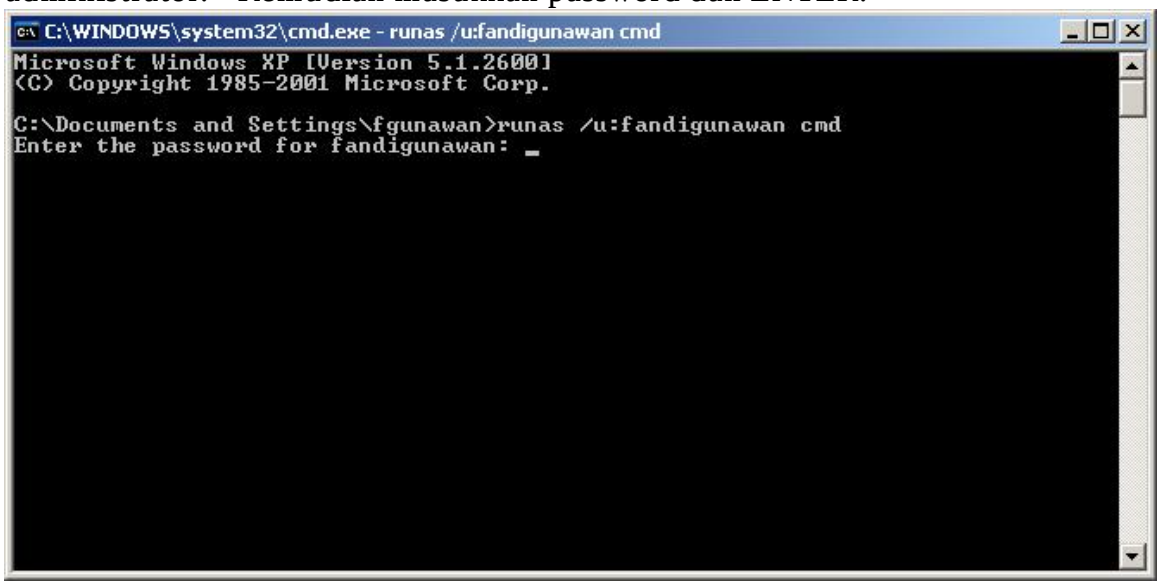
1. Msconfig (untuk mengganti setting waktu start-up)
2. Appwiz.cpl (alias Add and Remove Application)
3. Services.msc (setting on/off service di Windows)
4. Sysdm.cpl (alias System Properties)
5. Dan lain-lain

Dapat diakses dengan cara :
Ke Run->Ketik CMD

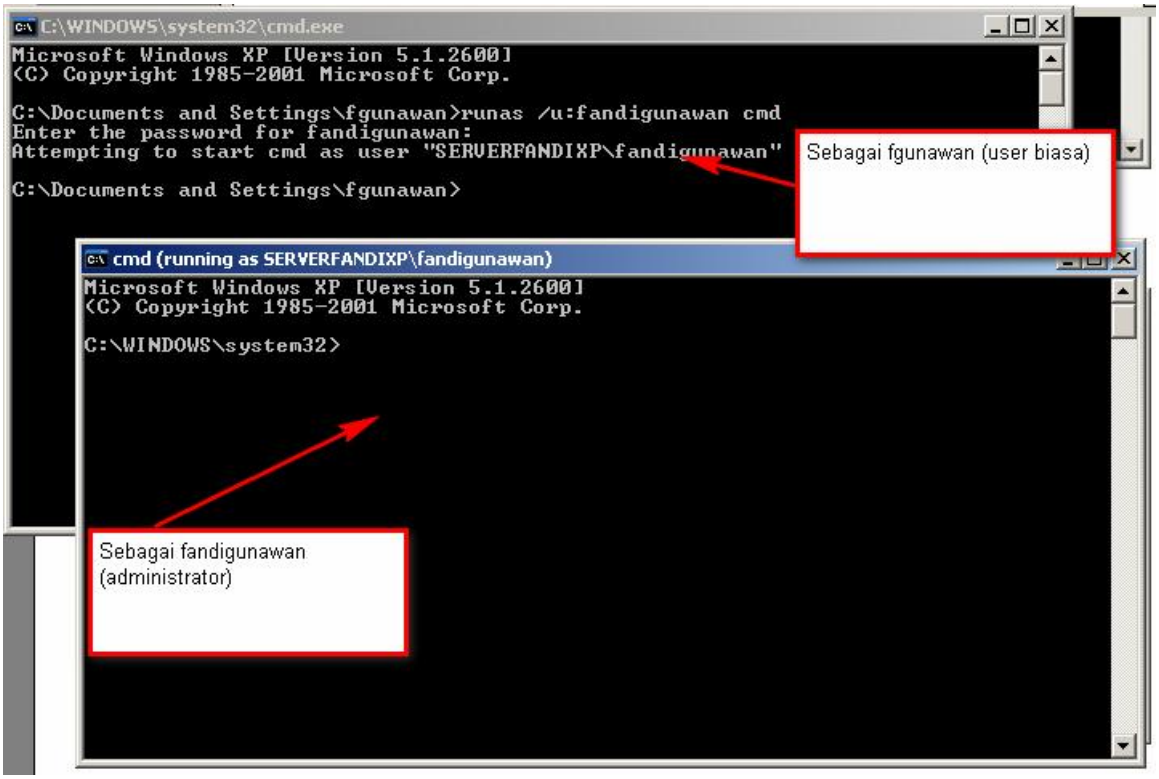




Ketik perintah : *runas /u:nama_user cmd* yang pada kasus penulis *runas /u:fandigunawan cmd* ingat fandigunawan mempunyai previledge administrator. Kemudian masukkan password dan ENTER.

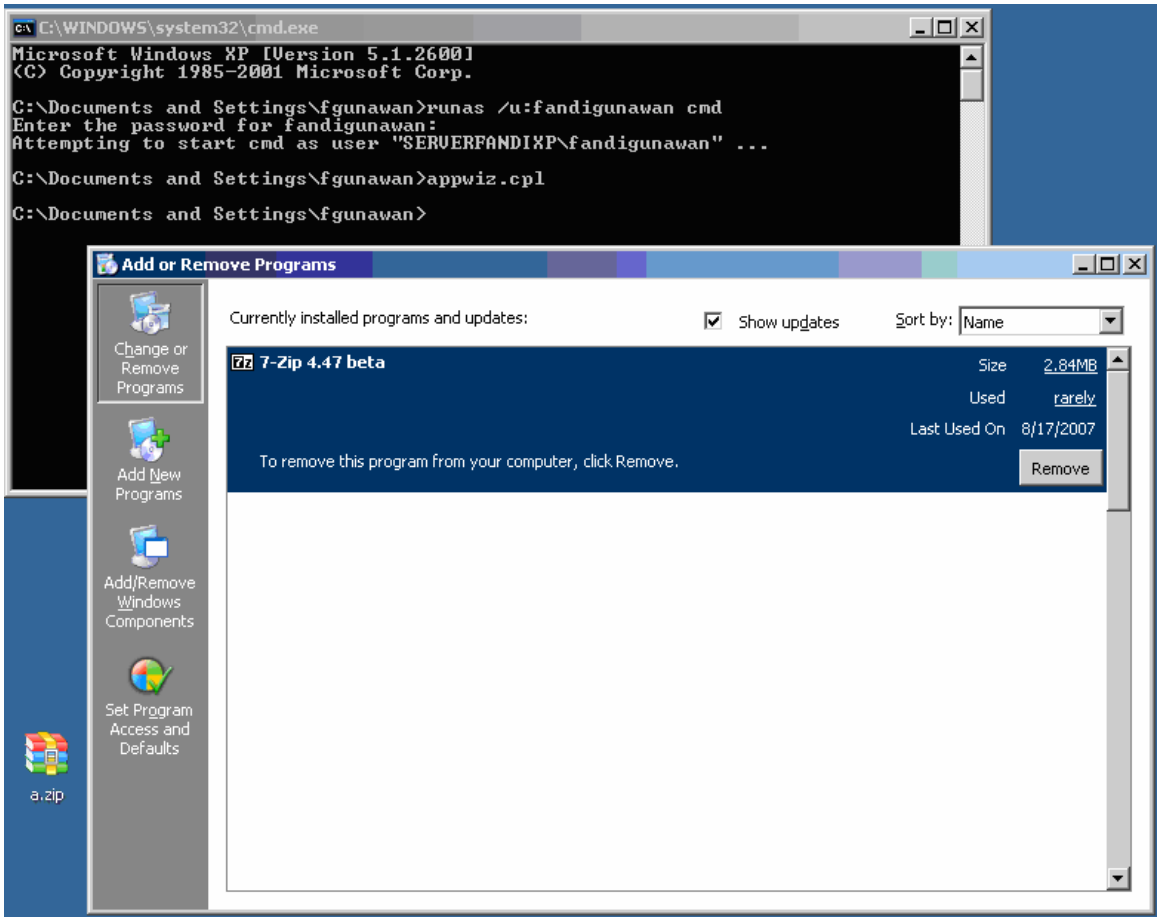


Jika benar maka akan muncul:



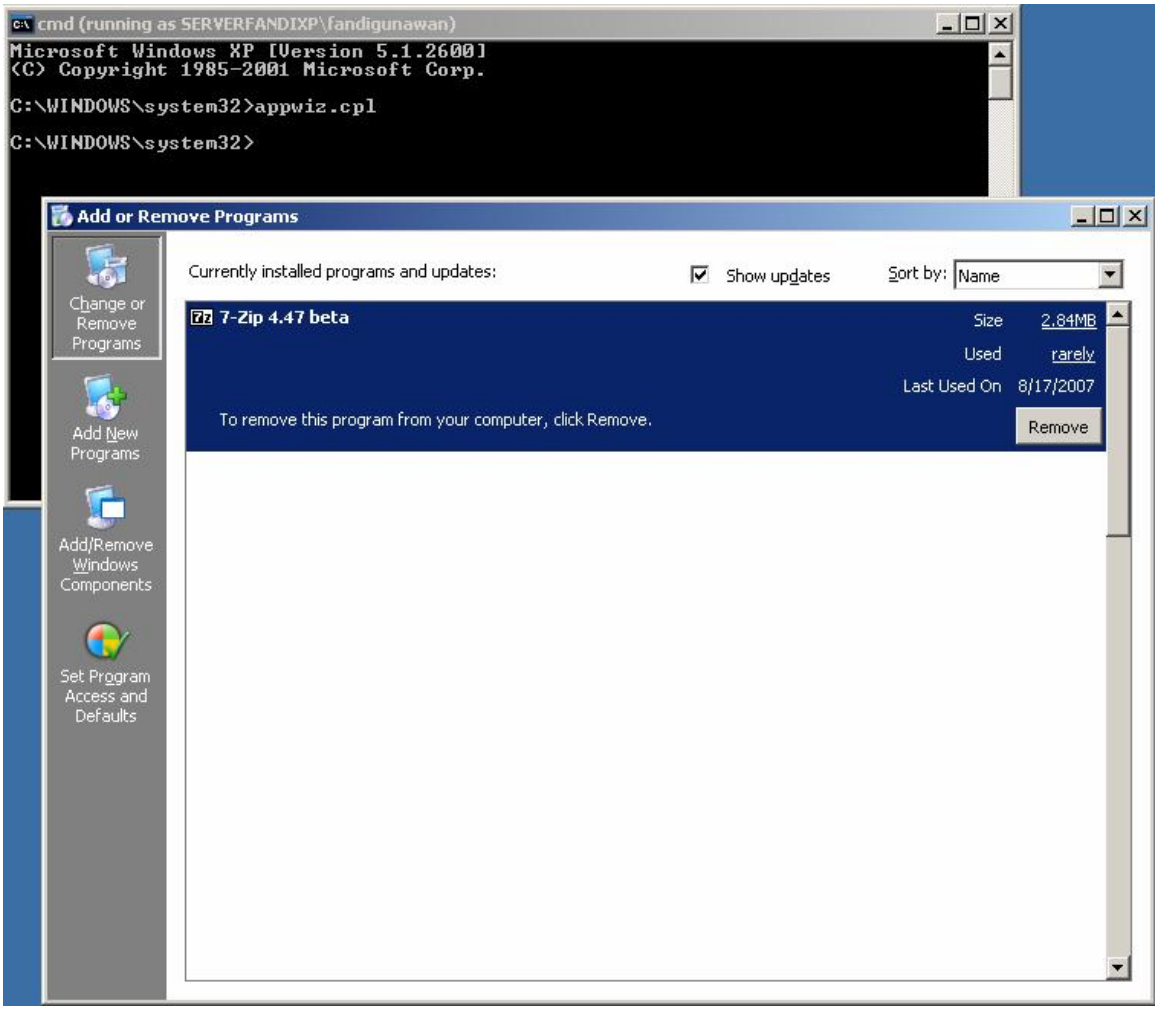
Nah ketik aja perintah diatas di cmd yang ada caption : cmd (Running as SERVERFANDIXP/fandigunawan)

Sekarang kita coba panggil appwiz.cpl dengan akun fgunawan (user biasa)



Namun di sini kita tidak bisa melakukan perubahan apapun (baik memodifikasi atau membuang aplikasi).

Kita coba pakai akun **fandigunawan** (administrator)



Nah apa beda dari 2 gambar diatas ? Kalau yang menggunakan akun **fgunawan** (user biasa) kita tidak bisa melakukan apapun, sedang dengan akun **fandigunawan** (administrator) kita bisa melakukan perubahan apapun.

Meski cara ini ampuh, tetap gunakan sabuk pengaman (Anti Virus) yang terus diupdate. Metode ini digunakan untuk mencegah masuknya virus-virus lokal yang belum terdeteksi Anti Virus.

Untuk saran dan kritik dapat dilayangkan ke e-mail penulis yang tertera dibawah ini.
fandigunawan@gmail.com?subject=IKC_cegah_virus

BIOGRAFI PENULIS

Fandi Gunawan. Menamatkan SMU di SMUN 2 Kediri tahun 2004. Kini sedang menyelesaikan kuliah S1 Electrical Engineering di President University. Sekarang sedang aktif dalam membangun komunitas berbasis opensource. Sedang dalam usaha keras untuk membangun usaha untuk mengintegrasikan dunia elektronika dan komputer yaitu Kaktus Aja! Gemar mempelajari tentang security, interfacing piranti keras, hardware programming, processor design (SPARC, 8051, PIC, MIPS dan ARM), OS design dan hardware cryptography. Bahasa pemrograman yang pernah dipakai : Pascal, MIPS assembly, 8051 Assembly Language, C for 8051, C for PIC and C for Computer, C#, VHDL dan Java. Berkecimpung dalam dunia OS yang melingkupi :
FreeDOS, MSDOS, Linux (pelbagai distro), FreeBSD, OpenBSD, NetBSD dan Windows (pelbagai versi)

URL : http://fandigunawan.wordpress.com (blog awak)
URL : http://kaktusaja.co.cc (Kaktus Aja!)
URL : http://eepu.wordpress.com (EESA of PU)
URL : http://coredotnet.co.cc (Core.NET of PU)

E-Mail : fandigunawan@gmail.com