

Menganalisis Log Firewall dengan Memanfaatkan MySQL

Mengamati file log merupakan hal yang wajib dikuasai oleh seorang sysadmin. Kebanyakan file log yang ada di Linux hanya berbentuk file teks biasa. Kali ini penulis akan menjelaskan teknik mengubah file log *firewall* dari file teks biasa ke dalam database MySQL.

Salah satu tugas rutin yang biasa dikerjakan oleh seorang sysadmin adalah mengamati file log suatu aplikasi server. Dari file log yang ada ini, seorang sysadmin dapat dengan mudah mengetahui segala aktivitas yang berhubungan dengan kejadian yang terjadi di system. Misalnya, catatan *logging user* yang *login* atau *logout* dari suatu situs web. Selain itu, file log juga berfungsi untuk monitoring keamanan. Contohnya adalah file-file log yang dihasilkan oleh program-program pemonitor keamanan. Dengan menggunakan event log syslog di Linux, kita dapat mengetahui aktifitas yang sudah terjadi, mencari penyebab suatu masalah (*debugging*), dan mengamati apakah ada hal-hal yang ganjil (monitoring keamanan).

Sayangnya, file teks yang dihasilkan oleh syslog tidak cukup mudah untuk dianalisis. Tanpa menggunakan syslog, log firewall Anda kemungkinan besar tersebar di berbagai file log yang terdapat dalam suatu system.

Pada artikel kali ini, penulis akan menjelaskan cara mengubah firewall log dari file syslog yang berbentuk file teks ke dalam database MySQL. Saat membuat artikel ini, penulis menjalankannya di Fedora Core 4, dan seharusnya hal ini dapat Anda terapkan juga dengan mudah pada distro yang lainnya.

1. Periksa Setting Kernel

Bagi Anda yang menggunakan default kernel yang terdapat di Fedora Core 4, dapat melewati langkah ini. Kernel yang terdapat pada distro-distro saat ini, tidak perlu disetting lagi. Tetapi bagi yang menggu-

nakan modifikasi kernel sendiri, yakinkan kalau kernel di system Linux Anda sudah di compile dengan pilihan CONFIG_NETFILTER, CONFIG_IP_NF_IPTABLES, CONFIG_IP_NF_FILTER, dan CONFIG_IP_NF_TARGET_ULOG. Kebanyakan aplikasi-aplikasi firewall juga membutuhkan pilihan CONFIG_IP_NF_CONTRACK, CONFIG_IP_NF_FTP, dan CONFIG_IP_NF_IRC. Pastikan juga kalau iptables juga sudah di-compile dengan mendukung ulog.

2. Install MySQL

Bagi yang sudah menginstalasikan aplikasi MySQL di systemnya, dapat melewati langkah ini. Bagi yang belum menginstall MySQL, install terlebih dahulu paket-paket MySQL di sistem Fedora Anda dengan menggunakan aplikasi Add/Remove Applications atau dengan menggunakan perintah RPM. Berikut ini hasil dari rpm mysql yang telah terinstal di sistem.

```
# rpm -qa | grep mysql
mysql-server-4.1.11-2
mysql-bench-4.1.11-2
mysql-4.1.11-2
mysql-devel-4.1.11-2
php-mysql-5.0.4-10
libdbi-dbd-mysql-0.7.1-3
mysqlclient10-3.23.58-6
```

Setelah MySQL terinstalasi dengan baik, jalankan service MySQL dan set *password* untuk user root yang ada di MySQL.

```
# /etc/init.d/mysql start
# mysqladmin -u root password
'passwordanda'
```

Note : (ubah 'passwordanda' dengan password pilihan Anda)

3. Inisialisasi Database

Langkah berikut yang akan kita lakukan adalah membuat database ulogdb sebagai tempat untuk menaruh semua catatan log yang dihasilkan oleh syslog. Selain itu, database ini nantinya akan digunakan juga oleh Nulog untuk mempermudah analisis data log yang sudah masuk kedalam database ulogdb. Untuk mempersingkat waktu, buka teks editor kesayangan Anda, lalu ketikkan baris SQL di bawah ini, kemudian simpan dengan nama file ulogd.sql.

```
.....
.....
-- Untuk Listing ulogd.sql
-- selengkapnya, dapat Anda
-- temukan dalam CD Majalah
-- InfoLINUX edisi ini
.....
.....
--
-- Table structure for table
'udp_ports'
--
CREATE TABLE udp_ports (
  udp_dport smallint(5) unsigned
  NOT NULL default '0',
  first_time int(10) unsigned
  default NULL,
  last_time int(10) unsigned
  default NULL,
  count int(10) default NULL,
  PRIMARY KEY (udp_dport),
  KEY last_time (last_time)
) TYPE=MyISAM;
```

```

root@server1:/lib/iptables
File Edit View Terminal Tabs Help
--FWXCF-XF-X 1 root root 2992 Mar 18 2005 libipt_realn.so
--FWXCF-XF-X 1 root root 6496 Mar 18 2005 libipt_recent.so
--FWXCF-XF-X 1 root root 3284 Mar 18 2005 libipt_REDIRECT.so
--FWXCF-XF-X 1 root root 4580 Mar 18 2005 libipt_REJECT.so
--FWXCF-XF-X 1 root root 5628 Mar 18 2005 libipt_rpc.so
--FWXCF-XF-X 1 root root 3776 Mar 18 2005 libipt_SAME.so
--FWXCF-XF-X 1 root root 8668 Mar 18 2005 libipt_sctp.so
--FWXCF-XF-X 1 root root 4240 Mar 18 2005 libipt_SNAT.so
--FWXCF-XF-X 1 root root 1864 Mar 18 2005 libipt_standard.so
--FWXCF-XF-X 1 root root 3440 Mar 18 2005 libipt_state.so
--FWXCF-XF-X 1 root root 1904 Mar 18 2005 libipt_TARPIT.so
--FWXCF-XF-X 1 root root 9344 Mar 18 2005 libipt_tcpmss.so
--FWXCF-XF-X 1 root root 2912 Mar 18 2005 libipt_TCPMSS.so
--FWXCF-XF-X 1 root root 6956 Mar 18 2005 libipt_tcp.so
--FWXCF-XF-X 1 root root 3700 Mar 18 2005 libipt_tos.so
--FWXCF-XF-X 1 root root 3412 Mar 18 2005 libipt_TOS.so
--FWXCF-XF-X 1 root root 1796 Mar 18 2005 libipt_TRACE.so
--FWXCF-XF-X 1 root root 3516 Mar 18 2005 libipt_ttl.so
--FWXCF-XF-X 1 root root 3564 Mar 18 2005 libipt_TTL.so
--FWXCF-XF-X 1 root root 4636 Mar 18 2005 libipt_udp.so
--FWXCF-XF-X 1 root root 4480 Mar 18 2005 libipt_ULOG.so
--FWXCF-XF-X 1 root root 1792 Mar 18 2005 libipt_unclean.so
[root@server1 iptables]# pwd
/lib/iptables
[root@server1 iptables]#
    
```

```

root@server1:~
File Edit View Terminal Tabs Help
[root@server1 ~]# mysql -u root -p
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 15 to server version: 4.1.11

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> create database ulogdb;
Query OK, 1 row affected (0.12 sec)

mysql> use ulogdb;
Database changed
mysql> source /tmp/ulogd.sql;
Query OK, 0 rows affected (0.18 sec)

Query OK, 0 rows affected (0.00 sec)

Query OK, 0 rows affected (0.00 sec)

Query OK, 0 rows affected (0.18 sec)
    
```

Periksa apakah Iptables Anda sudah mendukung penggunaan ulog.

Buat database ulogdb sebagai tempat menyimpan file log di MySQL.

```

--
-- Table structure for table
'ulog'
--
CREATE TABLE ulog (
  id int(10) unsigned NOT NULL
  auto_increment,
  raw_mac varchar(80) default
  NULL,
  oob_time_sec int(10) unsigned
  default NULL,
  oob_time_usec int(10) unsigned
  default NULL,
  oob_prefix varchar(32) default
  NULL,
  oob_mark int(10) unsigned
  default NULL,
  oob_in varchar(32) default
  NULL,
  oob_out varchar(32) default
  NULL,
  ip_saddr int(10) unsigned
  default NULL,
  ip_daddr int(10) unsigned
  default NULL,
  ip_protocol tinyint(3)
  unsigned default NULL,
  ip_tos tinyint(3) unsigned
  default NULL,
  ip_ttl tinyint(3) unsigned
  default NULL,
  ip_totlen smallint(5) unsigned
  default NULL,
  ip_ihl tinyint(3) unsigned
  default NULL,
  ip_csum smallint(5) unsigned
  default NULL,
    
```

```

  ip_id smallint(5) unsigned
  default NULL,
  ip_fragoff smallint(5)
  unsigned default NULL,
  tcp_sport smallint(5) unsigned
  default NULL,
  tcp_dport smallint(5) unsigned
  default NULL,
  tcp_seq int(10) unsigned
  default NULL,
  tcp_ackseq int(10) unsigned
  default NULL,
  tcp_window smallint(5)
  unsigned default NULL,
  tcp_urg tinyint(4) default
  NULL,
  tcp_urgp smallint(5) unsigned
  default NULL,
  tcp_ack tinyint(4) default
  NULL,
  tcp_psh tinyint(4) default
  NULL,
  tcp_rst tinyint(4) default
  NULL,
  tcp_syn tinyint(4) default
  NULL,
  tcp_fin tinyint(4) default
  NULL,
  udp_sport smallint(5) unsigned
  default NULL,
  udp_dport smallint(5) unsigned
  default NULL,
  udp_len smallint(5) unsigned
  default NULL,
  icmp_type tinyint(3) unsigned
  default NULL,
  icmp_code tinyint(3) unsigned
    
```

```

  default NULL,
  icmp_echoid smallint(5)
  unsigned default NULL,
  icmp_echoseq smallint(5)
  unsigned default NULL,
  icmp_gateway int(10) unsigned
  default NULL,
  icmp_fragmtu smallint(5)
  unsigned default NULL,
  pwsniff_user varchar(30)
  default NULL,
  pwsniff_pass varchar(30)
  default NULL,
  ahesp_spi int(10) unsigned
  default NULL,
  timestamp timestamp(14) NOT
  NULL,
  UNIQUE KEY id (id),
  KEY index_id (id),
  KEY timestamp (timestamp),
  KEY ip_saddr (ip_saddr),
  KEY udp_dport (udp_dport),
  KEY tcp_dport (tcp_dport),
  KEY oob_time_sec (oob_time_
  sec),
  state smallint(6) unsigned
  default NULL,
  end_timestamp datetime default
  NULL,
  start_timestamp datetime
  default NULL,
  username varchar(30) default
  NULL,
  user_id smallint(5) unsigned
  default NULL,
  client_os varchar(128) default
  NULL,
    
```

```
client_app varchar(128)
default NULL
) TYPE=MyISAM;
```

Setelah selesai, copykan file ulogd.sql ke direktori /tmp, dan lakukan proses dump file ulogd.sql tersebut ke database ulogdb. Untuk melakukan hal tersebut, lakukan langkah-langkah di bawah ini:

```
# cp ulogd.sql /tmp
```

Login sebagai user root yang ada dalam database MySQL.

```
# mysql -u root -p
```

Masukkan password user root MySQL Anda. Setelah masuk ke dalam database MySQL, ketikkan baris perintah berikut untuk membuat database ulogdb yang nantinya akan berfungsi untuk menerima log firewall dari ulog.

```
create database ulogdb;
use ulogdb;
source /tmp/ulogd.sql;
grant select,insert,update,drop,
delete,create temporary tables
on ulogdb.* to ulog@localhost
identified by 'ulogpass';
flush privileges;
quit;
```

Penjelasan dari perintah sql di atas adalah sebagai berikut:

- Kita membuat sebuah database bernama ulogdb sebagai host file log-nya.
- Perintah source /tmp/ulogd.sql, menyeni-

apkan database untuk nulog-php, yang akan digunakan sebagai tempat untuk menaruh informasi ke tabel MySQL yang dihasilkan oleh ulog.

- Perintah grant pada baris SQL di atas, akan menciptakan user "ulog" (dengan password "ulogpass"), yang memiliki hak akses read/write ke database ulogdb. Anda dapat mengubah password "ulog-pass", ke password lain yang sesuai dengan keinginan Anda.

4. Instal dan konfigurasi ulogd

Langkah berikut yang harus Anda lakukan adalah menginstallasikan aplikasi logging daemon ulogd. Untuk pengguna Fedora Core 4, instalasikan saja file RPM ulogd dan ulogd-mysql yang terdapat dalam CD majalah InfoLINUX edisi ini.

```
# rpm -ivh ulogd-1.23-2.fc4.
i386.rpm
# rpm -ivh ulogd-mysql-1.23-2.
fc4.i386.rpm
```

Setelah ulogd terinstalasi dengan baik di sistem Anda, selanjutnya adalah mengonfigurasi ulogd. Edit file /etc/ulogd.conf, dan isikan pada bagian parameter MySQL, sesuai dengan yang terdapat di sistem Anda. Pada bagian plugin, hapus tanda pagar pada bagian.

```
#plugin="/usr/lib/ulogd/ulogd_
MYSQL.so"
```

```
plugin="/usr/lib/ulogd/ulogd_
MYSQL.so"
```

Selanjutnya edit juga pada bagian MYSQL, sesuai dengan parameter yang ada di MySQL Anda. Sebagai contoh, dalam MySQL di komputer penulis menggunakan user ulog yang mempunyai password ulog-pass, dengan host adalah localhost, dan nama database MySQL yang akan digunakan menerima log firewall dari ulog adalah ulogdb.

Maka di bagian MYSQL dalam file /etc/ulogd.conf, penulis mengisikan sebagai berikut:

```
[MYSQL]
table="ulog"
pass="ulogpass"
user="ulog"
db="ulogdb"
host="localhost"
```

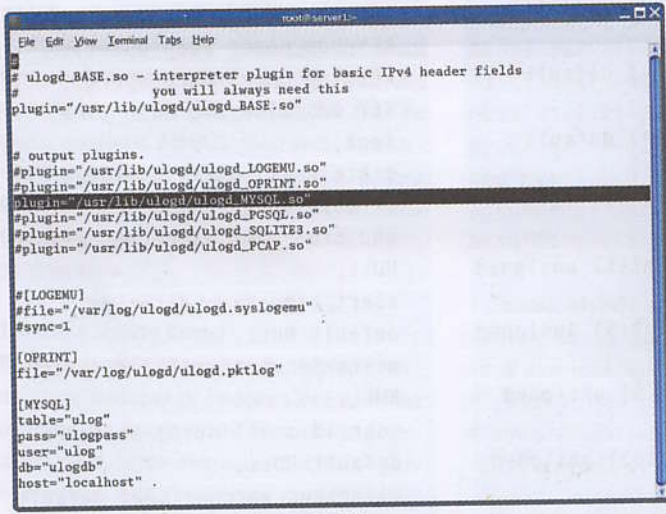
Berikan juga comment out pada beberapa baris di file ulogd.conf, untuk menjaga agar file log tidak di letakkan ke dalam file teks lagi.

```
#plugin="/usr/lib/ulogd/ulogd_
LOGEMU.so"

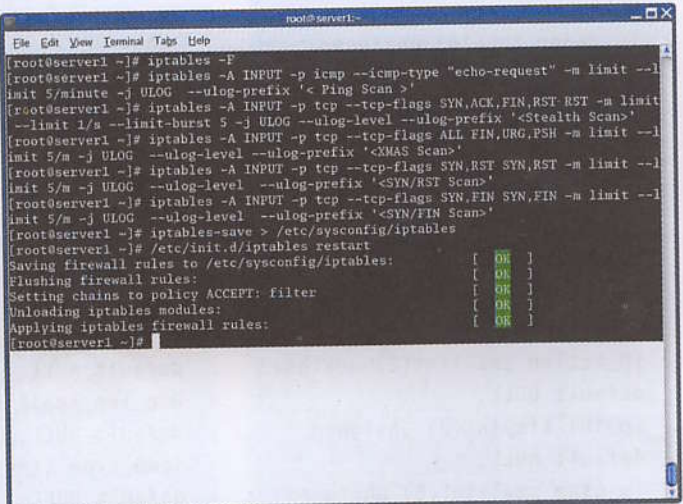
#[LOGEMU]
#file="/var/log/ulogd/ulogd.
syslogemu"
#sync=1
```

Untuk konfigurasi file ulog.conf secara lengkap, bisa Anda peroleh di dalam CD majalah InfoLINUX edisi ini.

Setelah ulog.conf sudah dikonfigurasi dengan baik, lakukan restart daemon ulogd



Edit ulogd.conf untuk mengaktifkan plugins ulog for MySQL.



Buat beberapa rule iptables untuk me-redirect proses iptables ke ulog.

Tampilan aplikasi Nulog yang memudahkan kita menganalisis catatan ulog yang terjadi.

- Untuk melihat apakah keseluruhan rule iptables tersebut sudah masuk atau belum, ketikkan perintah iptables -L untuk melihatnya.

```
[root@server1 sysconfig]#
iptables -L
Chain FORWARD (policy ACCEPT)
target prot opt source
destination
```

```
Chain INPUT (policy ACCEPT)
target prot opt source
destination
```

```
ULOG icmp -- anywhere
anywhere icmp
echo-request limit: avg 5/
min burst 5 ULOG copy_range
0 nlogroup 1 prefix `<Ping
Scan>' queue_threshold 1
```

```
ULOG tcp -- anywhere
anywhere tcp flags:
FIN,SYN,RST,ACK/RST limit: avg
1/sec burst 5 ULOG copy_range
0 nlogroup 1 prefix `<Stealth
Scan>' queue_threshold 1
```

```
ULOG tcp -- anywhere
anywhere tcp flags:
FIN,SYN,RST,PSH,ACK,URG/
FIN,PSH,URG limit: avg 5/
min burst 5 ULOG copy_range
0 nlogroup 1 prefix `<XMAS
Scan>' queue_threshold 1
```

```
ULOG tcp -- anywhere
anywhere tcp flags:
SYN,RST/SYN,RST limit: avg
5/min burst 5 ULOG copy_range
0 nlogroup 1 prefix `<SYN/RST
```

```
Scan>' queue_threshold 1
ULOG tcp -- anywhere
anywhere tcp flags:
FIN,SYN/FIN,SYN limit: avg
5/min burst 5 ULOG copy_range
0 nlogroup 1 prefix `<SYN/FIN
Scan>' queue_threshold 1
```

```
Chain OUTPUT (policy ACCEPT)
target prot opt source
destination
```

- Selanjutnya, simpan rule iptables tersebut ke dalam file /etc/sysconfig/iptables dengan menggunakan perintah iptables-save.
- Selanjutnya, restart service iptables Anda.

```
# iptables-save > /etc/
sysconfig/iptables
```

```
# /etc/sysconfig/iptables
restart
```

Catatan: Selain dengan mengetikkan perintah iptables secara manual, Anda dapat juga mempermudah pembuatan rule iptables dengan menggunakan aplikasi antar muka untuk iptables, seperti shorewall, firehol, maupun firestarter.

6. Testing

Setelah Anda melakukan semua langkah diatas, saatnya mengetes apakah log dari iptables sudah berhasil kita masukkan ke dalam database MySQL. Caranya adalah sebagai berikut. Anggap saja komputer yang kita setting ini adalah komputer1 (192.168.2.1).

Dari komputer2 (192.168.2.2), kita melakukan ping dan port scanner ke komputer1.

```
# ping 192.168.2.1
```

Lihat hasil logging iptablesnya di tabel ulog yang ada di database ulogdb.

```
# mysql -u ulog -h localhost -p
ulogdb
```

Setelah masuk ke MySQL, lihat apakah sudah ada data dari ulog didalam tabel ulog. Dari MySQL konsol, coba Anda lakukan perintah select.

```
mysql> select *from ulog;
```

Jika sudah terdapat data di dalam tabel tersebut, berarti Anda telah berhasil melakukan konfigurasi ini dengan baik. Lihat dibagian field oob_prefix, di situ akan tertulis kalau kegiatan ping yang Anda lakukan tadi termasuk ke dalam <Ping Scan>.

Coba lagi dengan melakukan usaha port scanning dari komputer2 ke komputer1.

```
# nmap -v 192.168.2.1
```

Coba lihat lagi di dalam tabel ulog, apakah catatan file log usaha port scanning yang baru saja Anda lakukan sudah masuk didalam tabel tersebut atau belum. Jika sudah masuk, Anda akan melihat di bagian field oob_prefix pada record tersebut, akan tertulis kalau kegiatan port scanning yang Anda lakukan termasuk ke dalam <Stealth Scan>.

7. Menganalisis Log Menggunakan Nulog

Setelah data file log yang dihasilkan oleh syslog telah tersimpan dengan baik ke dalam database MySQL, langkah selanjutnya yang akan penulis jelaskan adalah mengonfigurasi Nulog untuk mempermudah analisis file log. Nulog adalah sebuah aplikasi yang dibuat dengan bahasa PHP, yang berfungsi sebagai antarmuka untuk menganalisis file log firewall. Dengan menggunakan Nulog, Anda dapat dengan mudah melihat segala aktifitas log yang sudah terekam dalam suatu database (seperti MySQL misalnya), yang ditampilkan secara real time dalam tampilan yang *user friendly*. Untuk dapat menggunakan Nulog, ikuti penjelasan di bawah ini:

- Extract file source Nulog yang ada di CD majalah *InfoLINUX* edisi ini, ke direktori

root Web Server Anda. Secara default, document root Apache di Fedora Core 4 berada di direktori `/var/www/html`. Untuk itu, extract file `nulog-1.1.3.tar.gz` yang ada di CD ke direktori tersebut.

```
# tar -xvzf nulog-1.1.3.tar.gz -C /var/www/html
```

- Ubah nama folder-nya menjadi `nulog`, dan ubah hak kepemilikannya menjadi user root.

```
# cd /var/www/html
# mv nulog-1.1.3 nulog
# chown root.root nulog -Rf
```

- Selanjutnya ubah beberapa parameter yang ada di file `config.inc` yang terdapat dalam direktori `include`, agar dapat terkoneksi ke database `uologdb`.

```
# vi /var/www/html/nulog/include/config.inc
```


- Sesuaikan beberapa parameter yang terdapat dalam file tersebut, sesuai dengan

konfigurasi database `uologdb` yang telah kita buat.

```
.....
# database Host
$db_host="localhost";
# database name
$db_uolog="uologdb";
# database user
$db_user="uolog";
# database password
$db_pwd="uologpass";
.....
.....
```

- Simpan file tersebut setelah selesai dikonfigurasi. Selanjutnya buka browser, jalankan service Apache, lalu ketikkan `http://localhost/nulog`, untuk melihat segala aktifitas security yang telah terekam di database `uologdb`. Setelah tampilan `Nulog` terbuka, Anda dapat dengan mudah menganalisa segala hal yang berkaitan dengan keamanan di sistem Anda. Dari keterangan yang ditampilkan oleh

`Nulog`, Anda dapat menjaga sistem Anda dari kegiatan port scanning, Denial of Service, dan hal lainnya yang dilakukan oleh pihak luar yang mungkin berencana untuk menjebol celah keamanan yang terdapat di sistem Anda

Demikian "Tutorial" yang dapat penulis jelaskan kali ini. Dengan menggunakan file log yang diubah ke bentuk database, Anda dapat dengan mudah menggunakan utility lain yang dapat mempermudah analisis file log. Meskipun semua aktivitas yang berhubungan dengan *security* sudah dapat dilihat dengan jelas, tetap diperlukan pemantauan yang berkala untuk dapat menangani kegiatan mencurigakan yang dilakukan oleh pihak luar. Karena seberapa pun canggihnya suatu sistem, tetap memerlukan peran manusia untuk dapat mengontrolnya. Semoga artikel singkat ini dapat membantu Anda untuk mempermudah menganalisis keamanan yang ada di sistem Anda. Sampai jumpa! 
Supriyanto (supriyanto@infolinix.co.id)

Pazia

acer

National Hacking

COMPETITION 2006

NO. 1 di Indonesia & di dunia kompetisi **CAPTURE THE FLAG**
menggunakan **100** ACER Aspire Notebook yang dibawa ke **9** kota besar di Indonesia

Hadiah ACER Aspire Notebook 3620 series untuk 9 kota dan ACER Aspire Notebook 5670 series, Training Ethical Hacking & Countermeasures di Informatics Professional Development Centre, Piala Bergilir plus nonion F-1 ke Sepang, Malaysia. Pendaftaran Rp 50.000,- termasuk snack dan sertifikat Informasi lebih lanjut ke: ceobogor.net, <http://ceo-bogor.net> atau HP +628159331153

Kompetisi Hacking atau yang dikenal dengan nama CAPTURE THE FLAG yang diselenggarakan oleh Pazia - Acer merupakan event nasional pertama di Indonesia yang diharapkan akan menghasilkan ahli-ahli komputer Indonesia, dan dapat membuat teknologi informasi di negeri ini menjadi lebih maju.

Disediakan tempat untuk 200 peserta di setiap kota, dengan dilengkapi oleh 100 ACER Aspire Notebook yang siap dipakai untuk mencari data dalam jaringan internal dengan team pemandu dibawah Dani Firman Syah.

Juri dan pengarah kompetisi: Rusmanto (Pemred Infolinux) dan Michael S. Sunggardi (praktisi komputer), kompetisi nasional ini berhadiah ACER Aspire Notebook 3620 series untuk di setiap kota, dan pada grand final yang akan diselenggarakan di Jakarta berhadiah ACER Aspire Notebook 5670 series, Piala Bergilir dan kesempatan menonton balap F1 tanggal 19 Maret 2006 di Sepang Malaysia.

Semarang : Universitas AKJ, 18 Februari 2006

* MIP Computer - Nita/Gabuti - 024-70115618, 70136868

Jogja

Universitas Kristen Duta Wacana, 21 Februari 2006

* Wirabiana Komputer - Rita/Kristina - 0274-522077

Medan

STMIK Mikroskill, 24 Februari 2006

* Focus - Juliana - 061-7330800

Padang

Universitas Negeri Padang, 27 Februari 2006

* Venes Jaya - Cici/hong/butei - 0751-32310, 23893

Bandung : Universitas Maranatha, 02 Maret 2006

* Prima - Nita - 022-2016221

Surabaya

High Tech Mdl, 04 Maret 2006

* Apkomindo JaIm - Andi/David - 031-5018842

Denpasar

Universitas Udayana, 06 Maret 2006

* Balsoft - Mirah/Juniashih - 0361-418050

Makassar : MTC Karebosi, 09 Maret 2006

* Flash Computer - Rita/Lia - 0411-857888, 5053667

Jakarta : Mega Bazar, 11 Maret 2006

* Pazia Pilar Merrycom - 021-62313117

JACC M2M, 14 Maret 2006

* Sekretariat JACC - Eko - 021-6000325; 30005135

Semarang, Jogja, Medan, Padang, Bandung, Surabaya, Denpasar, Makassar, Jakarta

PC Mill

CHIP

Computer

PCplus

NEOTEK

LINUX

Intel

Kingston

CISCO SYSTEMS

intel

Jacc