

# Mengamankan Server Linux dengan LIDS

## Bagian 1 dari 2 Artikel

Di satu sisi, banyak *hacker* yang selalu mencari tahu kelemahan sistem untuk diperbaiki. Di sisi lain, banyak *hacker* yang berusaha mencari tahu dan mengembangkan berbagai cara untuk melindungi sistem dari serangan-serangan yang sangat tidak diinginkan. Berikut ini kita membahas salah satu karya *hacker*, LIDS.

Ketika kali pertama mendengar nama LIDS (Linux Intrusion Detection System) yang langsung terbayang di benak saya adalah sebuah aplikasi yang berfungsi sebagai sistem pendeteksi penyusup pada *network* semacam SNORT. Namun saya keliru besar, karena ternyata yang dimaksud itu adalah NIDS (*Network Intrusion Detection System*). LIDS adalah sebuah patch dan tool admin untuk mengoptimalkan fungsi keamanan pada kernel Linux. LIDS merupakan sebuah implementasi dari referensi monitor pada kernel. LIDS juga merupakan sebuah *Mandatory Access control* pada kernel.

### Mengapa menggunakan LIDS?

Mungkin pertanyaan ini akan kerap kali muncul. Mengapa menggunakan LIDS, sementara banyak security patch yang dibuat oleh berbagai pihak? Jawabannya cukup sederhana, "Sesuai dengan kebutuhan", atau lebih cocok dengan istilah "*Use the right tools for the right jobs*". Masing-masing patch yang dikeluarkan tentunya memiliki kelebihan tersendiri, dan itu semua kembali kepada anda, patch mana yang paling cocok untuk keperluan Anda.

Namun yang perlu diperhatikan adalah beberapa permasalahan yang ada pada sistem operasi Linux secara umum, yaitu:

- File system tidak memiliki proteksi atau pengamanan.
- Proses yang berjalan tidak memiliki proteksi atau pengamanan.

- Administrasi terhadap system tidak terlindungi.
- Super User (root) memiliki kekuasaan penuh yang dapat melanggar hak.
- Model dari *Access Control List* (DAC) pada Linux belum lah cukup.

Begitulah beberapa permasalahan umum yang terdapat pada sistem operasi Linux. Tapi isu yang paling besar dari permasalahan di atas adalah account "Maha Dewa" root. Permasalahan ini pun mungkin terdapat pula pada system \*NIX lainnya. Jika sebuah proses atau user memiliki privileges root, maka tidak ada sedikit pun alasan yang dapat mencegah proses atau user tersebut untuk menghancurkan sistem. Tidak heran jika account atau *privileges root* sangat diminati oleh para *intruder*. Hal ini sangat membuat mereka yang bertugas sebagai sysadmin harus menderita sakit kepala, pusing tujuh keliling. Permasalahan inilah yang ingin ditangani oleh LIDS dengan mengimplementasikan Access Control Lists (ACLs) untuk mencegah mereka yang ingin merusak sistem, meski mereka memiliki privileges root sekali pun. Dengan ACLs, LIDS ini mampu melakukan proteksi terhadap file dan proses.

### Fitur-fitur pada LIDS

Fitur yang ditawarkan oleh LIDS cukup banyak dan cukup untuk melindungi mesin Linux anda dari tangan-tangan jahil para *intruder*. Fitur-fitur tersebut adalah:

- Perlindungan atau proteksi terhadap file

dan direktori dari apa pun termasuk root pun tidak dapat melakukan perubahan dari file atau direktori yang diproteksi. Bahkan sebuah file pun dapat disembunyikan (*hidden*).

- Perlindungan atau proteksi terhadap proses dari apa saja, termasuk root, tidak dapat mematikan proses yang diproteksi. Bahkan sebuah proses dapat disembunyikan (*hidden*).
- Access Control Lists yang lebih baik.
- Dapat menggunakan dan menambahkan kapabilitas untuk mengontrol seluruh sistem.
- Peringatan terhadap keamanan langsung dari kernel.
- Pendeteksi port scanner pada kernel.
- Mendukung framework LSM (Linux Security Model) pada kernel 2.5.x dan 2.6.x.
- Pembatasan (*restriction*) terhadap akses proses jaringan.

### Kekurangan LIDS

Jika sebuah sistem memiliki kelebihan tentu ia juga akan memiliki kekurangan, demikian juga dengan LIDS. Beberapa kekurangan LIDS yang saya amati di antaranya:

- Setiap file dan proses yang berada pada system linux harus memiliki ACLs, hal ini tentu akan cukup merepotkan. Namun, hal ini dapat dimaklumi karena keamanan berbanding terbalik dengan kenyamanan.
- Kesalahan dalam mendefinisikan ACLs akan mengunci sistem, sehingga kita tidak dapat berbuat apapun.

- Setiap file harus memiliki ACLs yang jelas, tak terkecuali untuk file yang berisi scripting. Untuk hal ini ACLs juga harus diturunkan terhadap file lain yang akan dipanggil oleh skrip tersebut.
- LIDS belum mampu untuk mendeteksi keanehan-keanehan atau penyerangan pada level aplikasi, contohnya seperti penyerangan terhadap web melalui protokol http, sql injection.

## Implementasi LIDS

Di atas telah dibahas mengenai kelebihan, kekurangan serta fitur-fitur yang ditawarkan oleh LIDS, namun bagaimana implementasinya pada dunia nyata? Bagaimana LIDS dapat membantu Anda mengamankan mesin Linux anda? Berikut implementasi LIDS dalam dunia nyata untuk mengamankan mesin Linux Anda.

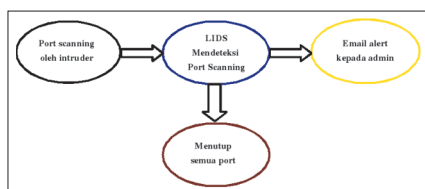
Berikut ini beberapa metode penyerangan secara *remote* (jarak jauh) yang umum dilakukan oleh para intruder, dan bagaimana LIDS mencegahnya:

### 1. Intruder melakukan port scanning

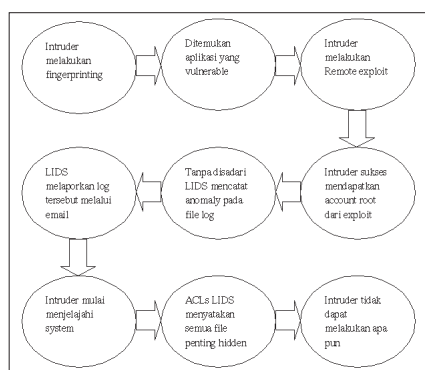
Gambar 1 menunjukkan proses port scanning dan dua tindakan LIDS, yaitu memberi tahu ke system administrator dan menutup semua port.

### 2. Remote exploit untuk mendapatkan privilege root

Gambar 2 menunjukkan proses intruder berusaha mengakses root dan cara LIDS mencegahnya.



Gambar 1. Proses port scanning.



Gambar 2. Akses privilege root dan cara mengatasinya.

### 3. Remote exploit untuk melakukan port binding/connect back

Gambar 3 menjelaskan proses intruder mengakses root, menjelajahi sistem dan membuat back door, serta tindakan LIDS mengatasi remote exploit ini.

### 4. Exploit lokal terhadap sebuah daemon yang berjalan

Gambar 4 menunjukkan salah satu dari metode penyerangan secara lokal yang umum dilakukan oleh para intruder, dan bagaimana LIDS mencegahnya.

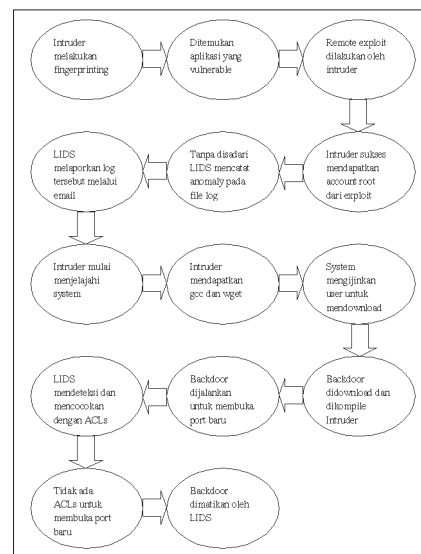
Cerita di atas hanya sebagian kecil dari berbagai teknik yang dilakukan oleh para intruder untuk mendapatkan akses root terhadap sistem, serta bagaimana LIDS mempersulit intruder dalam mendapatkan akses terhadap root atau bahkan akses penuh terhadap sistem. Masih banyak teknik yang digunakan oleh para intruder untuk menguasai sistem, di sini lah LIDS bertugas untuk mempersulit mereka agar tidak menguasai bahkan merusak sistem. Namun, sekali pun Anda menggunakan patch pengamanan berlapis tujuh sekelas LIDS, tapi jika Anda malas mengikuti perkembangan dan memperbarui sistem Anda, semua ini akan sia-sia.

## Prasyarat instalasi LIDS

Dalam tulisan ini penulis berasumsi bahwa pembaca telah memiliki pengetahuan dasar tentang kernel serta cara melakukan kompilasi kernel. Distribusi Linux yang digunakan pada tulisan ini adalah Red Hat Linux 9.0, terinstalasi lengkap dengan paket *development*.

Kebutuhan awal:

1. Kernel versi 2.4.29 dapat diambil dari situs resmi kernel <http://www.kernel.org> atau mirror terdekat <http://kambing.vlsm.org/kernel-linux>.
2. LIDS versi 1.2.2 untuk kernel 2.4.29 bernama `linux-2.4.29-lids1.2.2-ow1.diff.bz2`, dapat diambil dari <http://www.lids.org> atau <http://irvan.or.id/download.php>.
3. LIDS Tool versi 0.5.6 dapat diambil dari <http://lids.planetmirror.com/download/lidstools/lidstools-0.5.6.tar.gz>, atau dari mirror terdekat <http://irvan.or.id/download.php>.
4. Paket *development* pada linux seperti gcc, gnumake, ncurses, dan lain-lain.



Gambar 3. Remote exploit dan port binding.

## Tahapan instalasi dan konfigurasi LIDS

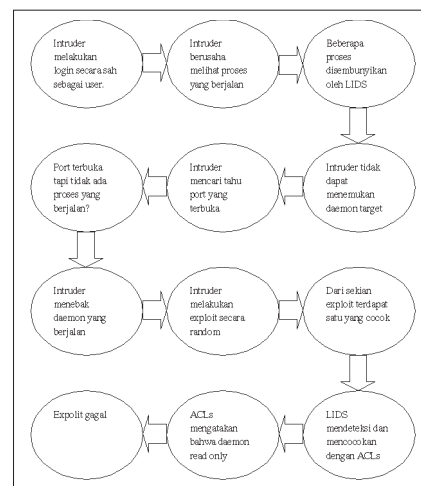
Kini kita akan masuk kepada tahapan instalasi dan konfigurasi LIDS untuk melindungi mesin dari tangan intruder, dengan paket-paket yang telah dikumpulkan. Tahapan ini dibagi lagi menjadi beberapa langkah, yaitu:

- Patching dan kompilasi kernel Linux dengan LIDS.
- Instalasi lidstool.
- Konfigurasi ACLs pada LIDS.

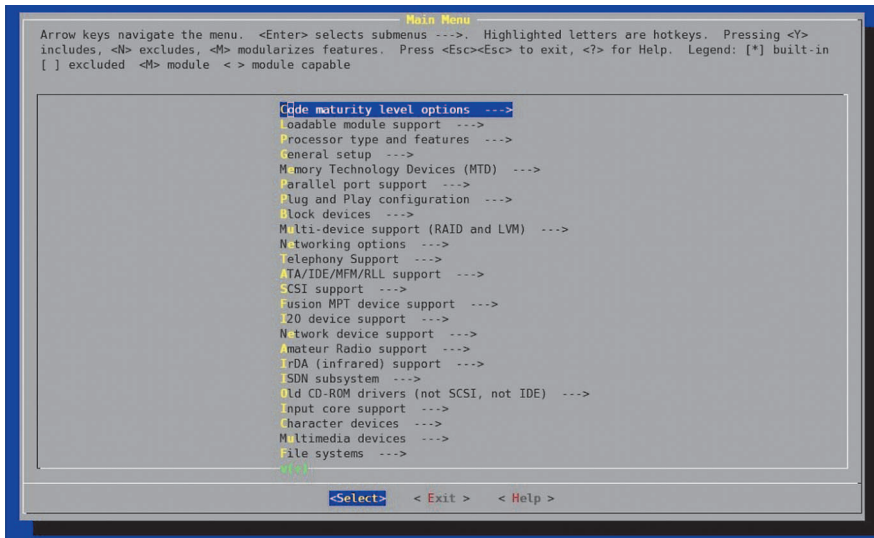
Mari kita mulai tahapan-tahapan tersebut.

### 1. Patching dan kompilasi kernel Linux dengan LIDS

Pertama-tama agar semua paket tersusun rapih, buat direktori yang bernama `lids` di



Gambar 4. Penyerangan lokal.



Gambar 5. Konfigurasi kernel dengan make menuconfig.

bawah direktori /var/tmp.

```
# mkdir -p /var/tmp/lids
```

Lalu salin semua paket yang dibutuhkan ke dalam direktori /var/tmp/lids kemudian pindah ke direktori /usr/src.

```
# cd /usr/src
```

Ekstrak paket kernel linux-2.4.29.tar.bz2.

```
# tar -jxvf /var/tmp/lids/linux-2.4.29.tar.bz2
```

Buat symbolic link /usr/src/linux yang mengarah ke /usr/src/linux-2.4.29.

```
# ln -s linux-2.4.29 linux
```

Salin dan ekstrak linux-2.4.29-lids1.2.2-owl.diff.bz2.

```
# cp /var/tmp/lids/linux-2.4.29-lids1.2.2-owl.diff.bz2
```

```
# bunzip2 linux-2.4.29-lids1.2.2-owl.diff.bz2
```

Patch kernel Linux dengan LIDS.

```
# cd linux
```

```
# patch -p1 < ../linux-2.4.29-lids1.2.2-owl.diff
```

Konfigurasi kernel.

```
# make mrproper
```

```
# make menuconfig
```

Dari perintah make menuconfig akan menghasilkan tampilan konfigurasi seperti gambar 5.

Pada menu pertama terdapat pilihan

Code maturity level options. Masuk pada menu tersebut dan aktifkan pilihan Prompt for incomplete driver. Hal ini sangat dianjurkan pada HOWTO dari situs yang bersangkutan sebelum kita mengaktifkan LIDS.

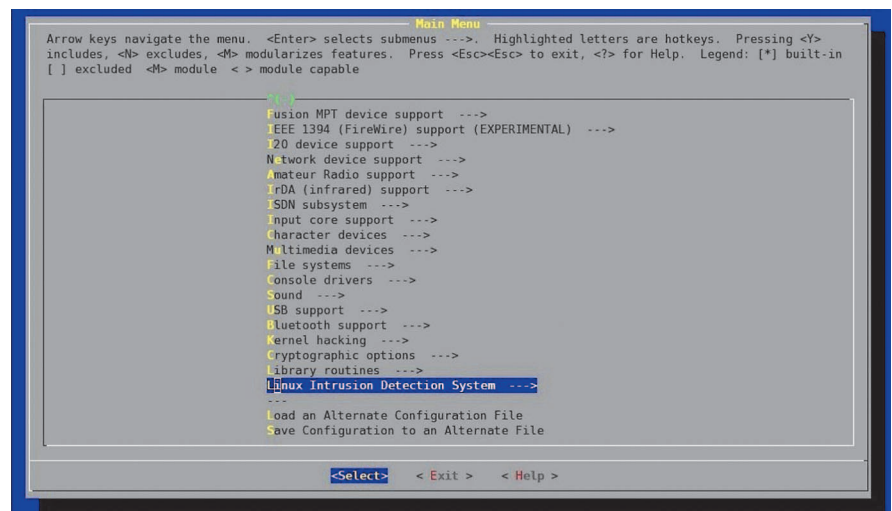
Ketika kernel telah di-patch, maka akan tampil satu menu yaitu menu Linux Intrusion Detection System.

Untuk dapat menggunakan LIDS seperti yang ditunjukkan pada HOWTO dari situs yang terkait, Anda harus mengaktifkan beberapa pilihan pada menu Linux Intrusion Detection System. Untuk kebutuhan awal hanya dengan konfigurasi dasar, sudah sangat cukup untuk melindungi system anda dari tangan-tangan intruder.

Masuk ke menu Linux Intrusion Detection System dan aktifkan pilihan yang ada

seperti berikut:

[*]	Linux Intrusion Detection System support (EXPERIMENTAL)
---	LIDS features
(512)	Maximum protected objects to manage
(512)	Maximum ACL subjects to manage
(512)	Maximum ACL objects to manage
[ ]	Hang up console when raising a security alert
[*]	Security alert when execing unprotected programs before sealing LIDS
[ ]	Do not execute unprotected programs before sealing LIDS
[*]	Attempt not to flood logs
(60)	Authorised time between two identic logs (seconds)
[*]	Allow switching LIDS protections/features
[*]	Allow switching LIDS/LIDS_GLOBAL
[*]	Implicitly protect LIDS admin passwd
[ ]	Restrict mode switching to specified terminals
(3)	Number of attempts to submit password
(3)	Time to wait after a fail (seconds)
[ ]	Allow any program to switch LIDS protections
[*]	Allow reloading config.



Gambar 6. Menuconfig LIDS.

```

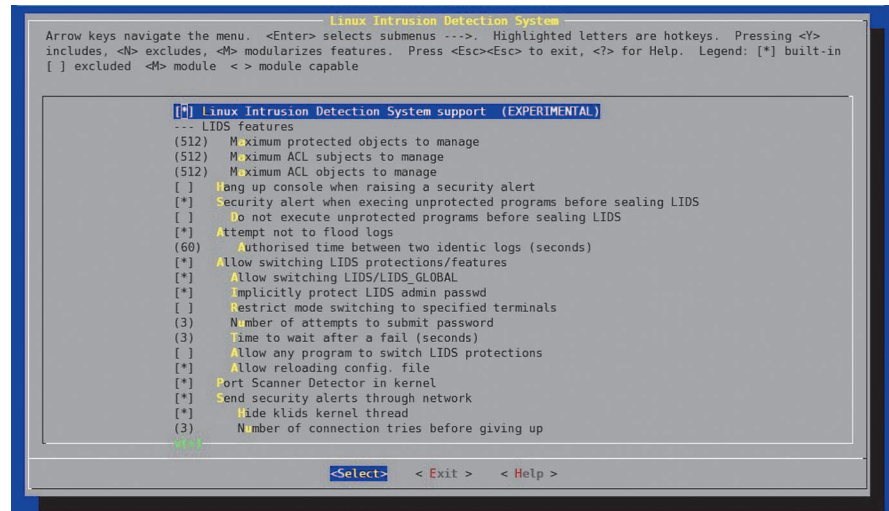
file
[*] Port Scanner Detector in
kernel
[*] Send security alerts
through network
[*] Hide klids kernel thread
(3) Number of connection tries
before giving up
[*] Attempt not to flood logs
(60) Authorised time between
two identic logs (seconds)
[*] Allow switching LIDS
protections/features
[*] Allow switching LIDS/
LIDS_GLOBAL
[*] Implicitly protect LIDS
admin passwd
[ ] Restrict mode switching
to specified terminals
(3) Number of attempts to
submit password
(3) Time to wait after a
fail (seconds)
[ ] Allow any program to
switch LIDS protections
[*] Allow reloading config.
file
[*] Port Scanner Detector in
kernel
[*] Send security alerts
through network
[*] Hide klids kernel thread
(3) Number of connection
tries before giving up
(30) Sleep time after a
failed connection
(16) Message queue size
[*] Enable security network
[*] Enable NETFILTER MARK
[*] Enable Trusted Path
Execution (TPE) mode feature
[ ] Enable Trusted Domain
Enforcement (TDE) feature
[ ] Enable CAP_LIDS_SANDBOX_
EFF_SET
[ ] LIDS Debug

```

Keluar dan simpan konfigurasi tersebut serta lakukan kompilasi kernel Linux.

```
# make dep clean module module_
install bzImage
```

Salin kernel dan System.map yang baru ke direktori /boot.



Gambar 7. Menuconfig LIDS lebih detail.

```
# cp /usr/src/linux/arch/i386/
boot/bzImage /boot/vmlinuz-
2.4.29
# cp /usr/src/linux/System.map
/boot/System.map-2.4.29
```

Edit file konfigurasi boot loader Anda, sesuaikan partisi harddisk Anda. Untuk lilo, pada /etc/lilo.conf tambahkan baris kernel baru sebagai berikut:

```

image=/boot/vmlinuz-2.4.27
    label=linux
    read-only
    root=/dev/hda5

```

Simpan konfigurasi tersebut lalu keluar dari editor dan ketik:

```
# lilo
```

Untuk grub, tambahkan baris berikut pada /etc/grub.conf (jika tidak ada grub.conf, edit file /boot/grub/menu.lst):

```

title Red Hat Linux, LIDS Kernel
    root (hd0,4)
    kernel /boot/vmlinuz-2.4.29
    root=/dev/hda5 ro

```

Sekali lagi, sesuaikan posisi partisi root dalam yang ditunjuk Lilo atau Grub di atas dengan posisi root yang ada di partisi hard-disk Anda.

## 2. Instalasi lidstools

Selanjutnya kita akan melakukan instalasi paket lidstools. Lidstools adalah paket yang berisi tools administrasi LIDS digunakan

untuk membuat ACLs. Berikut langkah-langkah dalam menginstal lidstools.

Pindah direktori ke /usr/src dan ekstrak paket source lidstools.

```
# cd /usr/src
# tar -zxvf /var/tmp/lids/
lidstools-0.5.6.tar.gz
```

Pindah ke direktori source code lidstools.

```
# cd lidstools-0.5.6
```

Konfigurasi, compile dan instal lidstools dengan langkah berikut:

```
# ./configure KERNEL_DIR=/usr/
src/linux
# make
# make install
```

Isikan password jika ditanyakan. Selanjutnya edit file /etc/lids/lids.ini, dan ubah paramater ACL\_DISCOVERY=0 menjadi ACL\_DISCOVERY=1. Hal ini dimaksudkan untuk membantu anda dalam membuat ACLs. Selanjutnya simpan konfigurasi dan restart mesin anda dengan kernel yang baru.

Jika tidak menemui kendala pada langkah pertama dan kedua, Anda akan berada pada shell dengan kernel yang baru. Langkah berikutnya adalah langkah yang sangat penting, yaitu mengonfigurasi ACLs LIDS pada sistem. Bagian yang akan dibahas pada edisi berikut itulah yang menentukan dalam melindungi sistem Anda.

**Irvan** (irv@irvan.or.id)