



Linux
Intrusion
Detection
System

Linux Intrusion Detection System (LIDS)

LIDS (Linux Intrusion Detection System) uygulamasını tanıtmadan önce IDS (Intrusion Detection System [İzinsiz giriş tespit sistemi]) kavramı üzerine kısa bir açıklama yapmakta yarar var. IDS, sistemde gerçekleştirilen uygunsuz davranışları, sistem kaynaklarını, sistem dışından gelen izinsiz giriş-saldırı izlerini denetler.

Sistemde gerçekleştirdiğimiz iyi önlemlere rağmen Internet tabanlı saldırılara maruz kalmak büyük sorunlar teşkil etmektedir (Virüs/DoS/DDoS atakları, izinsiz kullanıcı girişi sonucu meydana gelen sorunlar vb.).

Sisteme karşı uygunsuz davranışta bulunan saldırganı tespit etmenin en iyi yollardan biri izinsiz giriş tespit sistemi kullanmaktır. Bu tür uygulamalar ağı (Network) veya sistem kaynaklarının yetkisiz kullanımını takip eder. Genellikle izinsiz giriş tespit sistemleri olağan dışı davranışları algılayabilmeleri için kendisine belirtilen kurallar çerçevesinde tanımlama yapar.

LIDS(Linux Intrusion Detection System) Nedir?

LIDS, sistemdeki önemli dosyaları koruyan ve tanımlanan kurallar çerçevesinde süreçleri (process) izleyen bir uygulamadır. Kendisine bir kural tanımlanır ve o kurala göre dosya/dizinleri korur. Örneğin, kendisine eklenen kurallara göre belirlenen süreçler kullanıcıların gözünden saklanabilir. Böylece **ps** komutunun sonucunda bu süreç, gözlerden saklandığı için ortaya çıkmayacaktır. LIDS bu tür işlemleri yapabilmesi için yazılımla birlikte sunulan kernel yama dosyasını kernele (çekirdek) yamamak gerekmektedir. Kural tanımlama (ekleme/çıkarma) işlemi yazılımın lidstools isimli araçları ile yapılabilmektedir.



Home	New Release
About LIDS	Release: LIDS 2.2.0pre3 for kernel 2.6.5
Installation	Sun Apr 18 18:39:56 PDT 2004 by Huangang
Download	This version fixed the capability bugs, code clean the Kconfig and add back acl fast guessing feature. The new ACL fastguessing support will enhance the ACL search performance.
Documentation	For more infor, check the " WHAT IS NEW IN LIDS 2.2 " and ChangeLog within the tar ball. The version need a updated lidstools-2.2.2 which has been included within the tarball. Check out the INSTALL for how to install this new version.
Mailing List	Thanks Felipe Alfaro Solana, Marc-Christian Petersen for the patch and suggestions.
Mirror Sites	Download it here .
LIDS ACLs	
Links	
Logos contest	
Authors	

Lastest Version	Release: LIDS 2.2.0pre2 for kernel 2.6.5
kernel 2.6 lids-2.2.0pre3-2.6.5	Thu Apr 8 22:19:52 PDT 2004 by Huangang
kernel 2.4 lids-1.2.0-2.4.25 lids-1.1.2p3-2.4.25	This version add back the bind port support, acs on all filesystem, and enhance the acl labeling performance. This version also simplify the ACL reading in the kernel, and let userspace tools lidsconf do more jobs. All the configure file will be compiled into binary files which will be used by kernel when initializing and state switching.
kernel 2.2 lids-0.11.1pre1-2.2.22	For more infor, check the " WHAT IS NEW IN LIDS 2.2 " and ChangeLog within the tar ball. The version need a updated lidstools-2.2.1 which has been included within the tarball. Check out the INSTALL for how to install this new version.
lidstools lidstools-0.5.4	Thanks Andreas Steinme, Matt Benjamin and Omo Kazuki for many suggestion and ideas for this version.

LIDS hakkındaki gerekli tüm doküman ve dosyaları bulabileceğiniz adres:
<http://www.lids.org>

Kurulum:

LIDS yazılımını <http://www.lids.org> adresinden yükleyebilirsiniz.

Kurulum için gerekenler:

- Sisteminizde kurulu olan Linux'a ait kernel kodları [<http://www.kernel.org>]

- Kernel ile aynı versiyona sahip LIDS uygulaması [<http://www.lids.org>]

Bu yazıda anlatılan işlemler Linux 2.4.24 kernel versiyonu üzerinde gerçekleştirildi. Çeşitli kernel sürümlerine ait LIDSin farklı versiyonları vardır.

Kullandığımız Linux(Kernel 2.4.24) için uygun LIDS uygulaması:
lids-1.2.0rc1-2.4.24.tar.gz

LIDS sürümleri, Kernel v2.x serisini desteklemektedir. Sistemimizdeki kernele uygun yama(patch) dosyasını[www.lids.org] adresinden yüklüyoruz(Resim 1).

```
root@localhost.localdomain: /LinuxNET/lids - Kabuk - Konsole
Oturum Düzenle Görüntüle Ayarlar Yardım

[root@localhost lids]# ls -la
toplam 312
drwxr-xr-x  2 root    root      4096 Nis 17 10:20 ./
drwxr-xr-x  3 root    root      4096 Nis 14 00:24 ../
-rwxrwxrwx  1 root    root     301095 Nis 14 12:49 lids-1.2.0rc1-2.4.24.tar.gz*
-rwxrwxrwx  1 root    root        62 Nis 14 12:49 lids-1.2.0rc1-2.4.24.tar.gz.md5*
```

Resim 1: <http://www.lids.org> adresinden çektiğimiz dosyalar.
Buradaki .md5 uzantılı dosya uygulamanın md5 kontrolünü içermektedir.

Uygulamamızın MD5 kontrolünü yaparak çektiğimiz dosyanın doğruluğunu test ettik. MD5 kontrolleri LIDSin web sitesinde uygulamalarla birlikte sunulmaktadır. MD5 kontrol içeriği sitede uzantısı .md5 olan dosyalardır(Resim 2).

```
root@localhost.localdomain: /LinuxNET/lids - Kabuk - Konsole
Oturum Düzenle Görüntüle Ayarlar Yardım

[root@localhost lids]# cat lids-1.2.0rc1-2.4.24.tar.gz.md5
f032b24b383faa48a4e99827d6171b6a lids-1.2.0rc1-2.4.24.tar.gz
[root@localhost lids]#
[root@localhost lids]# md5sum lids-1.2.0rc1-2.4.24.tar.gz
f032b24b383faa48a4e99827d6171b6a lids-1.2.0rc1-2.4.24.tar.gz
[root@localhost lids]#
[root@localhost lids]#
```

Resim 2: md5sum komutu ile dosyanın md5 kontrolünü yapıyoruz.

Bu kontrollerden sonra yazılımı açalım. Yazılımı açmak için kullandığımız komut **tar** komutudur(Resim 3).

```
[root@localhost lids]# tar -zxvf lids-1.2.0rc1-2.4.24.tar.gz
lids-1.2.0rc1-2.4.24/
lids-1.2.0rc1-2.4.24/lidstools-0.5.2p1/
lids-1.2.0rc1-2.4.24/lidstools-0.5.2p1/ChangeLog
lids-1.2.0rc1-2.4.24/lidstools-0.5.2p1/AUTHORS
lids-1.2.0rc1-2.4.24/lidstools-0.5.2p1/COPYING
lids-1.2.0rc1-2.4.24/lidstools-0.5.2p1/CREDITS
lids-1.2.0rc1-2.4.24/lidstools-0.5.2p1/Makefile.am
lids-1.2.0rc1-2.4.24/lidstools-0.5.2p1/INSTALL
```

Resim 3: tar komutu ile uygulamayı açıyoruz(tar -zxvf lids-1.2.0rc1-2.4.24.tar.gz).

Dosyayı açtıktan sonra lids dizinine giriyoruz(Resim 4).
cd lids-1.2.0.rc1-2.4.24/

```
root@localhost.localdomain: /LinuxNET/lids/lids-1.2.0rc1-2.4.24 - Kabuk - Konsole
Oturum Düzenle Görüntüle Ayarlar Yardım

[root@localhost lids-1.2.0rc1-2.4.24]# pwd
/LinuxNET/lids/lids-1.2.0rc1-2.4.24
[root@localhost lids-1.2.0rc1-2.4.24]# ls -la
toplam 324
drwxrwxr-x  4 500    500      4096 Şub 14 12:04 ./
drwxr-xr-x  3 root    root      4096 Nis 17 10:29 ../
-rw-rw-r--  1 500    500     10748 Şub 14 11:31 ChangeLog
-rw-rw-r--  1 500    500     18008 Ara 17 04:53 COPYING
-rw-rw-r--  1 500    500     2387  Ara 14 08:15 CREDITS
-rw-rw-r--  1 500    500     4138  Şub 14 11:58 INSTALL
drwxrwxr-x  2 500    500     4096  Şub 14 12:04 lids/
-rw-rw-r--  1 500    500    230119 Şub 14 11:39 lids-1.2.0rc1-2.4.24.patch
-rw-rw-r--  1 500    500    21737  Şub 14 11:31 lids_prevent_worm.txt
drwxrwxr-x  6 500    500     4096  Şub 14 10:55 lidstools-0.5.2p1/
-rw-rw-r--  1 500    500     1476  Şub  9 22:31 New.feature
-rw-rw-r--  1 500    500     1010  Şub 14 11:31 README
[root@localhost lids-1.2.0rc1-2.4.24]#
```

Resim 4: lids dizinin içerisindeki dosyalar.
Uzantısı .patch olan dosyayı kernelimize ekleyip, kerneli yeniden derleyeceğiz.

Şimdiki aşama lids dizini içerisinde bulunan *lids-1.2.0rc1-2.4.24.patch* isimli dosyayı kernelimize yamalayacağız(Resim 5). Bu işlemi yapabilmek için yukarıda belirttiğimiz gibi sisteminizdeki Linux işletim sisteminize uygun kernel kaynak kodlarına ihtiyaç vardır. Sisteminize uygun Kernel kodlarını [<http://www.kernel.org>] adresinden bulabilirsiniz.

Kernel kodlarını /usr/src/ dizini altına açın.

cd /usr/src/linux-2.4.24

patch -p1 < /lids_dizini/lids-1.2.0rc1-2.4.24.patch

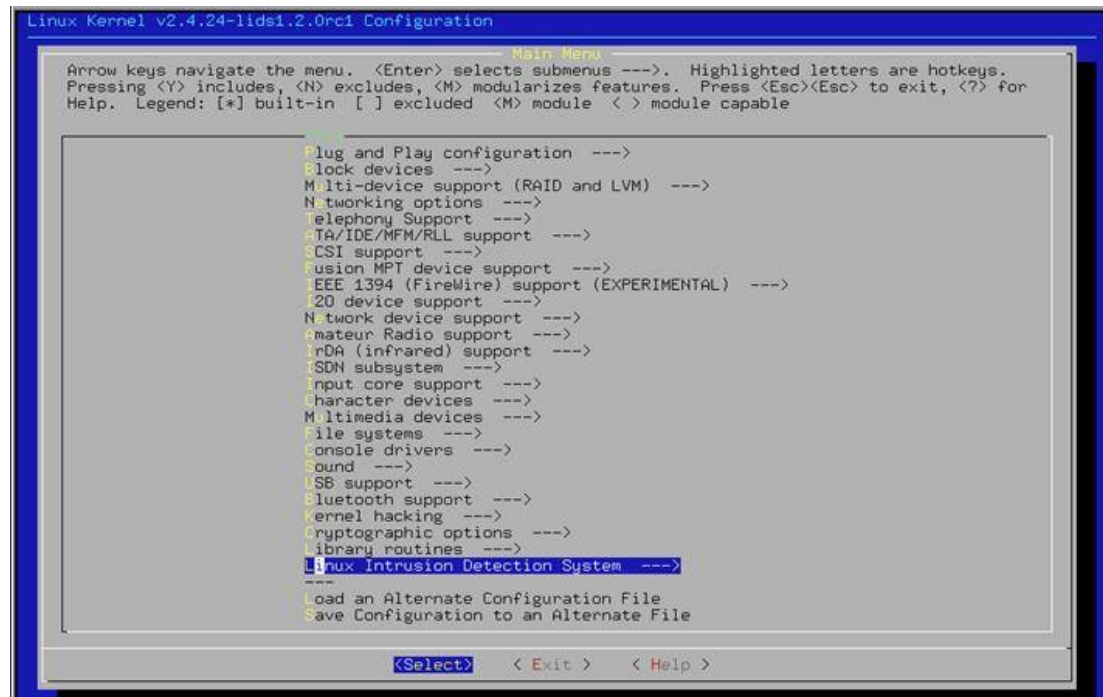
Böylece LIDSi kernele entegre ederek lidtools araçlarının bir parçası olan **lidsadm** adlı uygulamanın tüm işlemlerini kernel seviyesinde yapmasına olanak sağlar.

```
Oturum Düzenle Görüntüle Ayarlar Yardım
[root@localhost linux-2.4.24]# pwd
/usr/src/linux-2.4.24
[root@localhost linux-2.4.24]# patch -p1 < /LinuxNET/lids/lids-1.2.0rc1-2.4.24/lids-1.2.0rc1-2.4.24.patch
patching file Makefile
patching file Documentation/Configure.help
patching file arch/alpha/config.in
patching file arch/alpha/defconfig
patching file arch/arm/defconfig
patching file arch/cris/defconfig
patching file arch/i386/config.in
patching file arch/i386/defconfig
patching file arch/i386/kernel/ioport.c
patching file arch/i386/kernel/ptrace.c
patching file arch/i386/kernel/vm86.c
patching file arch/ia64/config.in
```

Resim 5: LIDSi kernele yamamak için kullandığımız komut **patch** komutudur.

LIDSi sorunsuz kernele yamadıktan sonra kerneli yeniden derleyeceğiz. Kerneli yapılandırırken **make menuconfig** / **make xconfig** / **make config** komutlarından birini kullanabilirsiniz.

[root@localhost /usr/src/linux]# make menuconfig (Resim 6)



Resim 6: LIDS in kernele yamandığını görüyoruz(Linux Intrusion Detection System).

Artık LIDS ile ilgili gerekli işlemleri seçebiliriz(Resim 7).

```
[*] Linux Intrusion Detection System support (EXPERIMENTAL)
--- LIDS features
(256) Maximum protected objects to manage (NEW)
(256) Maximum ACL subjects to manage (NEW)
(256) Maximum ACL objects to manage (NEW)
[ ] Hang up console when raising a security alert (NEW)
[*] Security alert when execing unprotected programs before sealing LIDS (NEW)
[ ] Do not execute unprotected programs before sealing LIDS (NEW)
[*] Attempt not to flood logs
(60) Authorised time between two identic logs (seconds) (NEW)
[*] Allow switching LIDS protections
[ ] Restrict mode switching to specified terminals (NEW)
(3) Number of attempts to submit password (NEW)
(3) Time to wait after a fail (seconds) (NEW)
[ ] Allow any program to switch LIDS protections (NEW)
[*] Allow reloading config. file
[*] Port Scanner Detector in kernel
[ ] Send security alerts through network (NEW)
[ ] Enable security network (NEW)
[ ] LIDS Debug (NEW)
```

Resim 7: LIDS ile ilgili gerekli seçim olanakları.

Sistemimiz için gerekli yapılandırmayı seçtikten sonra kerneli derleyebiliriz.

```
# make dep
# make bzImage (Resim 8)
# make modules
# make modules_install (Resim 9)
# cp arch/i386/boot/bzImage /boot/vmlinuz-2.4.lids
# cp System.map /boot/System.map
```



```
root@localhost.localdomain: /usr/src/linux - Kabuk No. 2 - Konsole
Oturum Düzenle Görüntüle Ayarlar Yardım

AS      .tmp_kallsyms1.o
LD      .tmp_vmlinux2
KSYM    .tmp_kallsyms2.S
AS      .tmp_kallsyms2.o
LD      vmlinux
AS      arch/i386/boot/bootsect.o
LD      arch/i386/boot/bootsect
AS      arch/i386/boot/setup.o
LD      arch/i386/boot/setup
AS      arch/i386/boot/compressed/head.o
CC      arch/i386/boot/compressed/misc.o
OBJCOPY arch/i386/boot/compressed/vmlinux.bin
GZIP    arch/i386/boot/compressed/vmlinux.bin.gz
LD      arch/i386/boot/compressed/piggy.o
LD      arch/i386/boot/compressed/vmlinux
OBJCOPY arch/i386/boot/vmlinux.bin
HOSTCC  arch/i386/boot/tools/build
BUILD   arch/i386/boot/bzImage
Root device is (3, 65)
Boot sector 512 bytes.
Setup is 4751 bytes.
System is 1046 kB
Kernel: arch/i386/boot/bzImage is ready
```

Resim 8: make bzImage işleminin sonucu.

```
make -C arch/i386/lib modules_install
make[1]: Entering directory `/usr/src/linux-2.4.24/arch/i386/lib'
make[1]: Nothing to be done for `modules_install'.
make[1]: Leaving directory `/usr/src/linux-2.4.24/arch/i386/lib'
make -C arch/i386/math-emu modules_install
make[1]: Entering directory `/usr/src/linux-2.4.24/arch/i386/math-emu'
make[1]: Nothing to be done for `modules_install'.
make[1]: Leaving directory `/usr/src/linux-2.4.24/arch/i386/math-emu'
cd /lib/modules/2.4.24-lids1.2.0rc1; \
mkdir -p pcmcia; \
find kernel -path '*/pcmcia/*' -name '*.o' | xargs -i -r ln -sf ../../{} pcmcia
if [ -r System.map ]; then /sbin/depmod -ae -F System.map 2.4.24-lids1.2.0rc1; fi
```

Resim 9: make modules_install sonrası

Derleme işlemi sona erdikten sonra açılış yöneticisini düzenlemeyi unutmayın(lilo/grup).

Örnek lilo.conf dosyası:

```
boot=/dev/hda
map=/boot/map
default=linux
keytable=/boot/tr_q-latin5.klt
prompt
nowarn
timeout=30
image=/boot/vmlinuz-2.4.lids
label=linux-lids
root=/dev/hdb1
read-only
image=/boot/vmlinuz
label=linux
root=/dev/hdb1
initrd=/boot/initrd.img
append="devfs=mount hdc=ide-scsi"
read-only
```

Artık LIDS için lidstool araçlarının da derleyebiliriz.

#cd <lids_dizini>/lidstools-0.5.2p1 (Resim 10)

[root@localhost lidstools-0.5.2p1]# ./configure KERNEL_DIR=/usr/src/linux-2.4.24/

[root@localhost lidstools-0.5.2p1]# make

[root@localhost lidstools-0.5.2p1]# make install (Resim 11)

```
root@localhost.localdomain: /LinuxNET/lids/lids-1.2.0rc1-2.4.24/lidstools- - Kabuk - Konsole
Oturum Düzenle Görüntüle Ayarlar Yardım
[root@localhost lidstools-0.5.2p1]# pwd
/LinuxNET/lids/lids-1.2.0rc1-2.4.24/lidstools-0.5.2p1
[root@localhost lidstools-0.5.2p1]# ls -la
toplam 376
drwxrwxr-x 6 500 500 4096 Şub 14 10:55 ./
drwxrwxr-x 4 500 500 4096 Şub 14 12:04 ../
drwxrwxr-x 2 500 500 4096 Şub 14 10:55 acl_discovery/
-rw-rw-r-- 1 500 500 30855 Ara 14 08:15 aclocal.m4
-rw-rw-r-- 1 500 500 2125 Ara 14 08:15 AUTHORS
-rw-rw-r-- 1 500 500 3517 Şub 14 10:51 ChangeLog
-rwxrwxr-x 1 500 500 2774 Ara 14 08:15 compile*
-rw-rw-r-- 1 500 500 3261 Şub 10 01:17 config.h.in
-rwxrwxr-x 1 500 500 199180 Şub 14 10:51 configure*
-rw-rw-r-- 1 500 500 4804 Şub 14 10:51 configure.ac
-rw-rw-r-- 1 500 500 18007 Ara 14 08:15 COPYING
-rw-rw-r-- 1 500 500 2125 Ara 14 08:15 CREDITS
-rwxrwxr-x 1 500 500 12117 Ara 14 08:15 depcomp*
drwxrwxr-x 4 500 500 4096 Şub 14 10:55 doc/
drwxrwxr-x 2 500 500 4096 Şub 14 10:55 example/
-rw-rw-r-- 1 500 500 7831 Ara 14 08:15 INSTALL
-rwxrwxr-x 1 500 500 5598 Ara 14 08:15 install-sh*
-rw-rw-r-- 1 500 500 351 Şub 11 19:44 Makefile.am
-rw-rw-r-- 1 500 500 14324 Şub 11 19:44 Makefile.in
-rwxrwxr-x 1 500 500 8857 Ara 14 08:15 missing*
-rwxrwxr-x 1 500 500 725 Ara 14 08:15 mkinstalldirs*
-rw-rw-r-- 1 500 500 59 Ara 14 08:15 NEWS
-rw-rw-r-- 1 500 500 1208 Ara 14 08:15 README
drwxrwxr-x 2 500 500 4096 Şub 14 10:55 src/
```

Resim 10: LIDSi kernele yamadıktan sonra kernel seviyesinde işlem yapabilmemiz için lidstools araçlarını(lidsadm/lidsconf) derlememiz gerekir.

```
object file /sbin/depmod was (3:1 inode 85931) instead of (3:65 47488). corrected.
object file /lib was (3:1 inode 77521) instead of (3:65 110657). corrected.
subject file /sbin/depmod was (3:1 inode 85931) instead of (3:65 47488). corrected.
object file /lib was (3:1 inode 77521) instead of (3:65 110657). corrected.
Using ACL FILE: /etc/lids/lids.postboot.conf
UPDATE
    effective capability = 0x3685ce7f

object file /etc was (3:2 inode 32194) instead of (3:65 189697). corrected.
Using ACL FILE: /etc/lids/lids.shutdown.conf
UPDATE
    effective capability = 0x7ffffeff

( [ 1 -eq 1 ] && /sbin/lidsconf -P ; true)
MAKE PASSWD
enter new password:
reenter new password:
```

Resim 11: *make install* komutu sonrası lidstools araçlarının işlem yapılabilmesi için gerekli olan şifre oluşturulur.

LIDS kurulumu tamamlandıktan sonra(lidstools araçları da dahil) ***lidsadm -I*** (bu komutu başlangıç betiklerine yazıp sistemi yeniden başlattığımızda lids otomatik olarak devreye girer) komutunu yazdıktan sonra sisteme kurallar tanımlayabiliriz. Yeni bir kural tanımlarken(ACL) öncelikle LIDSi pasif hale getirin.

Bu işlem için gereken komut:

lidsadm -S -- -LIDS

LIDSi pasif hale getirdikten sonra sisteme kurallar ekleyebiliriz.

Kural eklemek için kullanılan komut: ***lidsconf***

Kural yada kurallar belirttikten sonra belirttiğimiz kuralları kernele tanımlıyoruz:

lidsadm -S -- +RELOAD_CONF

Tanımladığımız kuralların kernel tarafından uygulanması için LIDSi aktif hale getiriyoruz.

lidsadm -S -- +LIDS

lidstools sisteme kurulduktan sonra oluşturulan ***/etc/lids*** dizininde bulunan ***.cap*** dosyalarını düzenleyerek kernelinize yetenek ekleyip çıkartabilirsiniz(boot işlemi sırasında ve sonrasında geçerli olacak).

Örneğin: Sistemde normal kullanıcıya root yetkisi veren bir dosyamız olduğunu varsayalım(nasıl olduğu meçhul);

```
[honeypot@localhost TEST]$ ls -la
suid-rwsr-sr-x 1 root root 11537 Nis 22 11:03 suid*
[honeypot@localhost TEST]$ id
uid=501(honeypot) gid=501(honeypot) gruplar=501(honeypot)
[honeypot@localhost TEST]$ ./suid
sh-2.05b# id
uid=0(root) gid=0(root)
```

/etc/lids dizininde bulunan ***.cap*** dosyalarında ***CAP_SETUID*** parametresinde ***-(eksi)*** işaretinin bulunmasına dikkat edelim. ***-(eksi)*** işareti bu özelliği iptal et, ***+(arti)*** işareti ise özelliği ekle anlamındadır.

.cap dosyalarında -7:CAP_SETUID olduğunda sistemde SETUID özelliğini kapattık. Düzeltmelerden sonra suid programının normal kullanıcıya root yetkisini vermediğini göreceğiz.

```
[root@localhost honeypot]# lidsadm -S -- -LIDS
```

SWITCH enter password:

```
[root@localhost honeypot]# lidsadm -S -- +RELOAD_CONF
```

SWITCH enter password:-> CAP_SETUID is now forbidden

```
[root@localhost honeypot]# lidsadm -S -- +LIDS
```

SWITCH enter password:

```
[honeypot@localhost TEST]$ ./suid
```

sh-2.05b\$

LIDS hakkındaki, özellikle *lidsadm* ve *lidsconf* komutlarının kullanımı ile ilgili bilgileri www.lids.org adresindeki doküman bölümünden okumanızı tavsiye ederiz. Eğer sisteminizde ağ servisleri kullanıyorsanız LIDSin bu servislere göre yapılandırılması ile ilgili bilgileri web sitesinden takip etmeniz ve lids forum bölümünü dikkatle incelemenizde yarar var. Aksi halde hatalarla karşılaşmak çok kolay.

Eğer LIDS doğru şekilde yapılandırılmışsa sisteminizi boot ettikten sonra

#dmesg komutuyla uyarılarda

Linux Intrusion Detection System 1.1.2 started

mesajını görürsünüz. Eğer bazı aksaklıklar olursa bu komut ile gerekli uyarıları incerseniz, sorunun kaynağını bulabilirsiniz.

dmeg komutuna ait örnek bir çıktı:

LIDS: lidsconf (dev 98:0 inode 44877) pid 478 ppid 424 uid/gid (0/0) on (vc/0) : access hidden file /etc/shadow

LIDS: lidsconf (dev 98:0 inode 44877) pid 478 ppid 424 uid/gid (0/0) on (vc/0) : access hidden file /etc/shadow - logging disabled for (60)s

LIDS: lidsadm (dev 98:0 inode 44876) pid 521 ppid 424 uid/gid (0/0) on (vc/0) : Give incorrect password (try #1) with caps=0x7590c1ff and flags=0x15

LIDS: Configuration file reloaded

LIDS: lidsadm (dev 98:0 inode 44876) pid 652 ppid 424 uid/gid (0/0) on (vc/0) : Changed: lids_cap_val=0x7590c1ff lids_flags=0x0

LIDS: lidsadm (dev 98:0 inode 44876) pid 653 ppid 424 uid/gid (0/0) on (vc/0) : LIDS switched to 1

LIDS: lidsadm (dev 98:0 inode 44876) pid 653 ppid 424 uid/gid (0/0) on (vc/0) : Changed: lids_cap_val=0x7590c1ff lids_flags=0x1

LIDS: lidsadm (dev 98:0 inode 44876) pid 654 ppid 424 uid/gid (0/0) on (vc/0) : LIDS locally switched to 1

LIDS: lidsadm (dev 98:0 inode 44876) pid 654 ppid 424 uid/gid (0/0) on (vc/0) : Changed: lids_cap_val=0x7590c1ff lids_flags=0x5

LIDSin bir parçası olan *lidsadm* komutu, kernelde nelerin izin verilip verilmediğinin yanında LIDSi durdurup yeniden başlatma olanağı verir.

```
[root@uml1 root]# lidsadm -h
```

lidsadm version 0.5.1 for LIDS project

Huagang Xie <xie[at]lids.org>

Philippe Biondi <pbi[at]cartel-info.fr>

Usage: lidsadm -[S|I] -- [+|-][LIDS_FLAG] [...]

lidsadm -V

lidsadm -h

Commands:

-S To submit a password to switch some protections

-I To switch some protections without submitting password (sealing time)

-V To view current LIDS state (caps/flags)

-v To show the version

-h To list this help

```
[root@uml1 root]# lidsadm -V [LIDSin verdiği izinler ve durumu]
```

VIEW

CAP_CHOWN 1

CAP_DAC_OVERRIDE 1

CAP_DAC_READ_SEARCH 1

CAP_FOWNER 1

CAP_FSETID 1

CAP_KILL 1

CAP_SETGID 1

CAP_SETUID 1

CAP_SETPCAP 1

CAP_LINUX_IMMUTABLE 0

CAP_NET_BIND_SERVICE 0

CAP_NET_BROADCAST 0

```
CAP_NET_ADMIN 0
CAP_NET_RAW 0
CAP_IPC_LOCK 1
CAP_IPC_OWNER 1
CAP_SYS_MODULE 0
CAP_SYS_RAWIO 0
CAP_SYS_CHROOT 0
CAP_SYS_PTRACE 0
CAP_SYS_PACCT 1
CAP_SYS_ADMIN 0
CAP_SYS_BOOT 0
CAP_SYS_NICE 1
CAP_SYS_RESOURCE 1
CAP_SYS_TIME 0
CAP_SYS_TTY_CONFIG 1
CAP_MKNOD 0
CAP_LEASE 1
CAP_HIDDEN 1
CAP_KILL_PROTECTED 1
CAP_PROTECTED 0
LIDS 1
LIDS_GLOBAL 1
RELOAD_CONF 0
POSTBOOT 0
SHUTDOWN 0
ACL_DISCOVERY 0
```

LIDSin diğer bir uygulama parçası olan *lidsconf* ile sistemdeki yetkiler sınırlandırılır. Böylece uygulamaların ne yapması gerektiği belirli kurallar çerçevesinde tanımlanır. Yanlış tanımlama sonucunda sistemdeki herhangi bir uygulama/uygulamalar çalışmaz yada ağ servislerin iptal olma olasılığı vardır. Lidsconf ile tanımlanan kurallar */etc/lids/lids.conf* dosyasına eklenir.

[root@uml1 root]# lidsconf -h

```
lidsconf version 0.5.1 for the LIDS project
Huagang Xie <xie@lids.org>
Philippe Biondi <philippe.biondi@webmotion.net>
```

```
Usage: lidsconf -A [acl_type] [-s subject] -o object [-d] [-t from-to] [-i level] -j ACTION
lidsconf -D [acl_type] [-s file] [-o file]
lidsconf -Z [acl_type]
lidsconf -U
lidsconf -L [acl_type] [-e]
lidsconf -P
lidsconf -v
lidsconf -[h|H]
```

Commands:

```
-A,--add To add an entry
-D,--delete To delete an entry
-Z,--zero To delete all entries
-U,--update To update dev/inode numbers
-L,--list To list all entries
-P,--passwd To encrypt a password with RipeMD-160
-v,--version To show the version
-h,--help To list this help
-H,--morehelp To list this help with CAP/SOCKET name
```

[root@uml1 root]# lidsconf -L [Tanımlanan kurallar]

```
Using ACL FILE: /etc/lids/lids.conf
LIST
```

```
effective capability = 0x7590c1ff
Subject ACCESS inherit time Object
```

```
-----
Any file READONLY: 0 0000-0000 /bin 0
Any file READONLY: 0 0000-0000 /lib 0
Any file READONLY: 0 0000-0000 /sbin 0
Any file READONLY: 0 0000-0000 /usr/bin 0
Any file READONLY: 0 0000-0000 /usr/sbin 0
Any file READONLY: 0 0000-0000 /usr/lib 0
Any file READONLY: 0 0000-0000 /boot 0
Any file READONLY: 0 0000-0000 /etc/rc.d 0
Any file READONLY: 0 0000-0000 /sbin/init 0
Any file READONLY: 0 0000-0000 /etc/rc.d/rc 0
/etc/rc.d/rc GRANT: 1 0000-0000 CAP_SYS_ADMIN 0
```

/etc/rc.d/rc GRANT: 1 0000-0000 CAP_NET_ADMIN 0
Any file READONLY: 0 0000-0000 /sbin/insmod 0

...
...

SourceForge.net: lids-user - Konqueror

Location Edit View Go Bookmarks Tools Settings Window Help

Location: http://sourceforge.net/mailarchive/forum.php?forum=lids-user

New User via SSL

Search

This Mailing List

Search

SF.net Subscription

- Subscribe Now
- Manage Subscription
- Advanced Search
- Direct Download
- Priority Tech Support
- Project Monitoring

SF.net Resources

- Site Docs
- Site Status (04/22)
- Site Map
- SF.net Supporters
- Compile Farm
- Foundries
- Project Help Wanted
- New Releases
- Get Support

Site Sponsors

Learn & Download DB2 Click Here

SourceForge Enterprise Edition

19 Images of 20 loaded.

Project: Linux Intrusion Detection System: Mailing Lists

Summary | Admin | Home Page | Forums | Tracker | Bugs | Support | Patches | RFE | Lists | Tasks | Docs | News | CVS | Files

Email Archive: lids-user (read-only)

	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
2001:												
2002:												
2003:												
2004:												

lids-user Ultimate Show 25 Change View

Topic	Topic Starter	Replies	Last Post
Re: LIDS 1.1, on Kernel 2.4.25 ERROR	Yusuf Wajati Purna <ywpurna@us...>	1	2004-04-03 00:18
RE: LIDS 1.1, on Kernel 2.4.25 ERROR	Section One <section_one_@ho...>	1	2004-04-02 18:16
Error running make on lidsutils	<suporte@hc...>	1	2004-04-02 09:14

2004-04-02 96%

LIDS Mail Listesi:

<http://sourceforge.net/mailarchive/forum.php?forum=lids-user>

Konu ile ilgili adresler:

<http://www.lids.org/document.html>

<http://www.lids.org/download.html>

<http://www.mandrakesecure.net/en/docs/lids.php>

<http://www.securityfocus.com/infocus/1496>

Tacettin Karadeniz
tacettink[.]@olympus.org