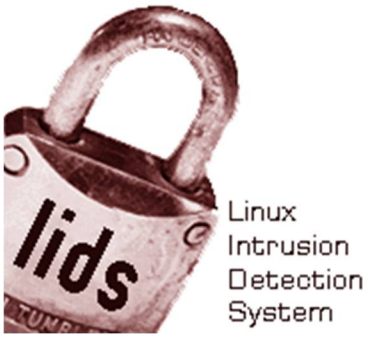


Linux Intrusion Detection System (LIDS)

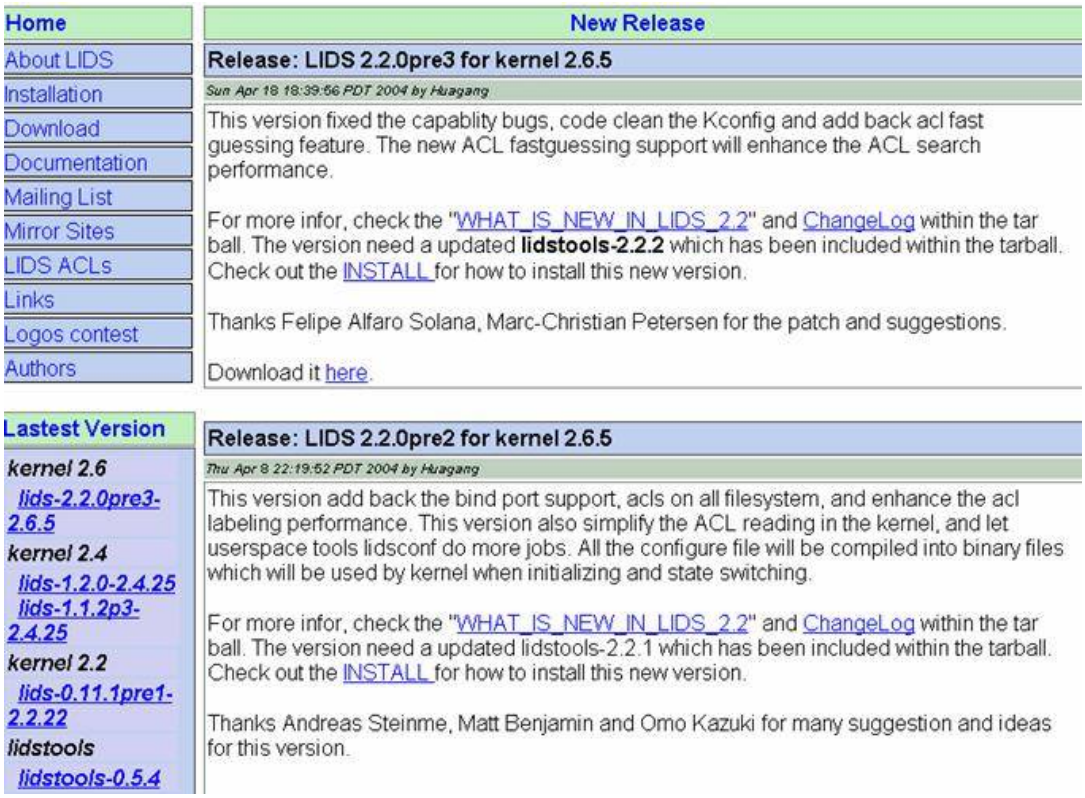
LIDS (Linux Intrusion Detection System) uygulamasını tanıtmadan önce IDS (Intrusion Detection System[İzinsiz giriş tespit sistemi]) kavramı üzerine kısa bir açıklama yapmakta yarar var. IDS, sistemde gerçekleştirilen uygunsuz davranışları, sistem kaynaklarını, sistem dışından gelen izinsiz giriş-saldırı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

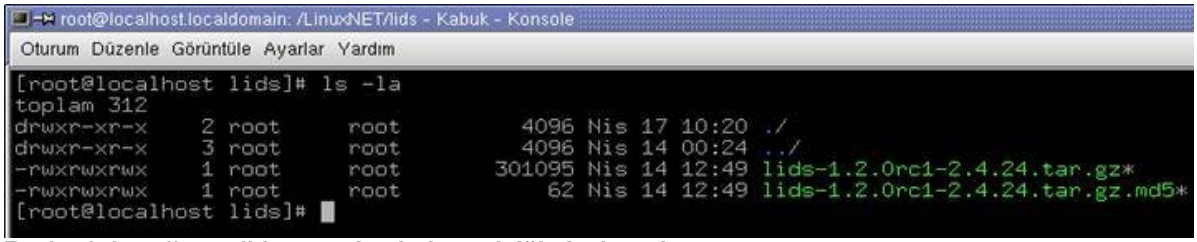


LIDS hakkındaki gerekli tüm döküman ve dosyaları bulabileceğiniz adres:
http://www.lids.org

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.

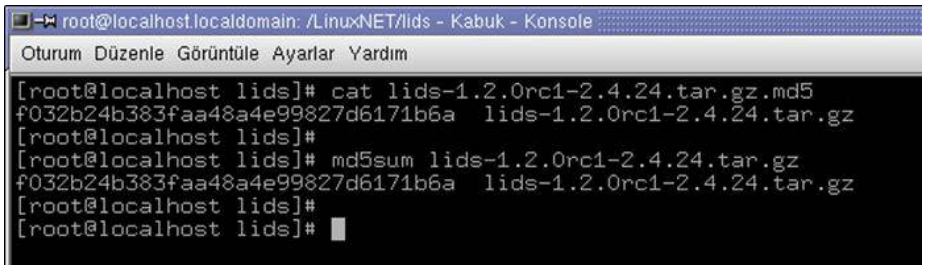
Kullandığım Linux(Kernel 2.4.24) için uygun LIDS uygulaması:
lids-1.2.0rc1-2.4.24.tar.gz

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



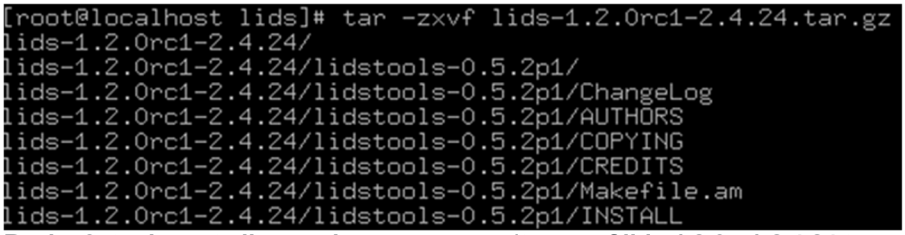
Resim 1: http://www.lids.org adresinden çektiğimiz dosyalar.
Buradaki .md5 uzantılı dosya uygulamanın md5 kontrolünü içermektedir.

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).



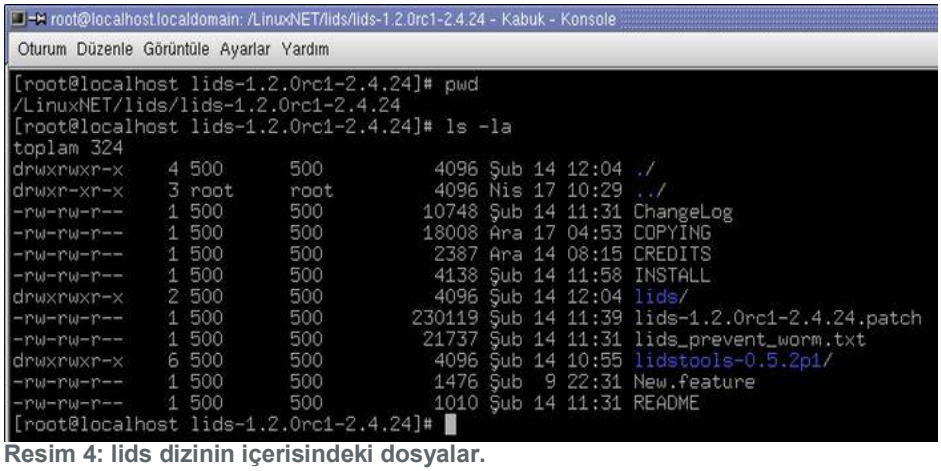
Resim 2: md5sum komutu ile dosyanın md5 kontrolünü yapıyoruz.

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



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

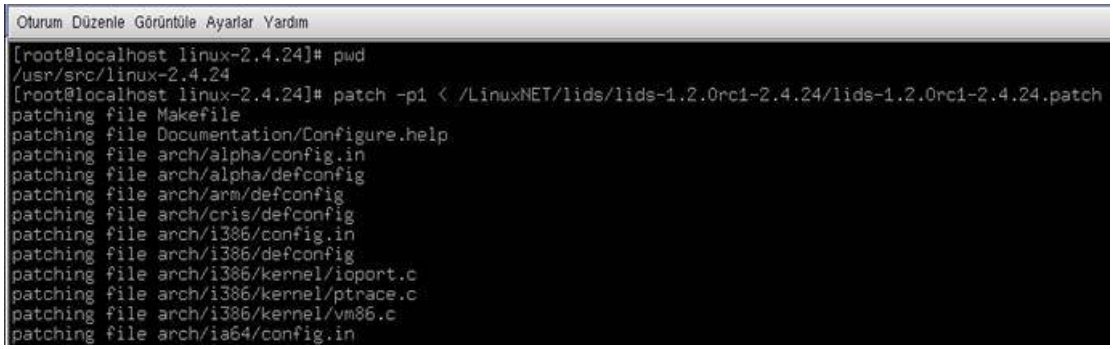
Dosyayı açtıktan sonra lids dizinine giriyoruz(Resim 4).
 # cd lids-1.2.0.rc1-2.4.24/



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

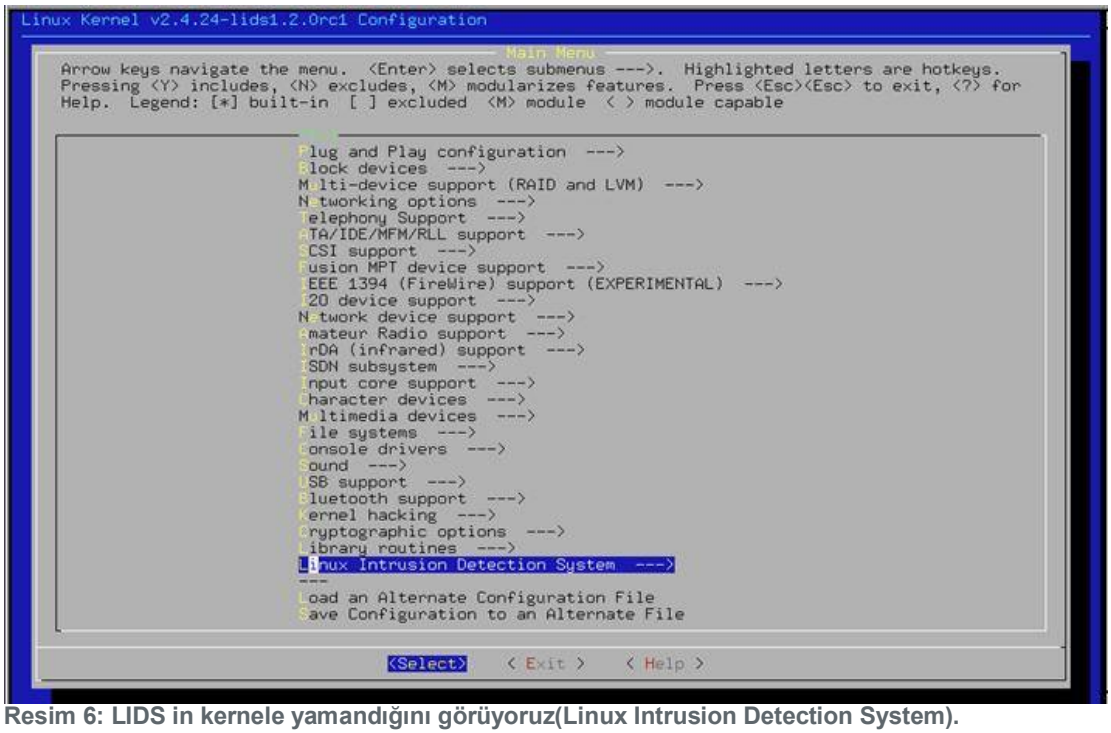
Şimdiki aşama lids dizini içerisinde bulunan *lids-1.2.0rc1-2.4.24.patch* isimli dosyayı kernelimize yamalayacağız(Resim 5). Bu işlemi yapabilmek için yukarıda belirttiğimiz gibi sisteminizdeki Linux işletim sisteminize uygun kernel kaynak kodlarına ihtiyaç vardır. Sisteminize uygun Kernel kodlarını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



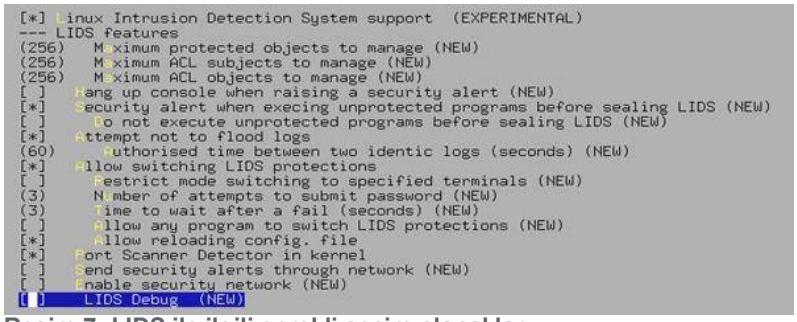
Resim 5: LIDSi kernele yamamak için kullandığımız komut *patch* komutudur.

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)



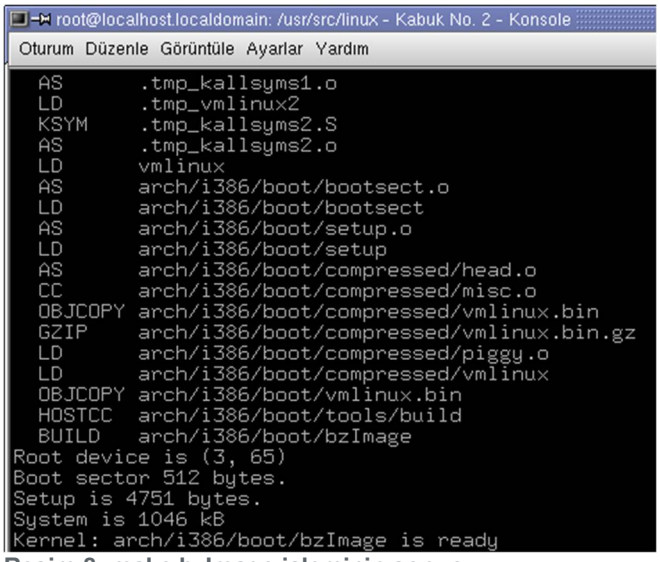
Resim 6: LIDS in kernele yamandığını görüyoruz(Linux Intrusion Detection System).

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

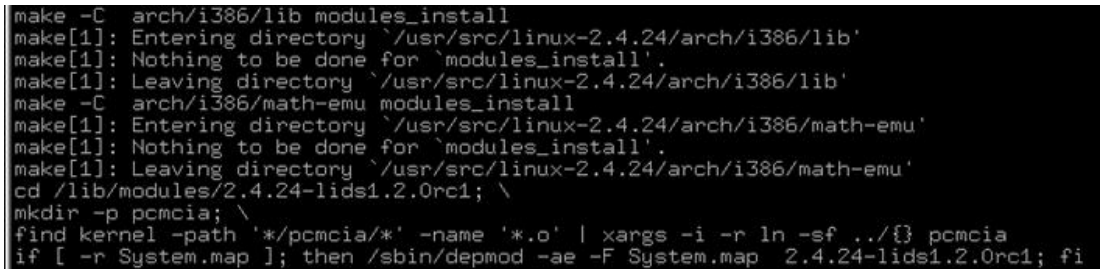


Resim 7: LIDS ile ilgili gerekli seçim olanakları.

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



Resim 8: make bzImage işleminin sonucu.



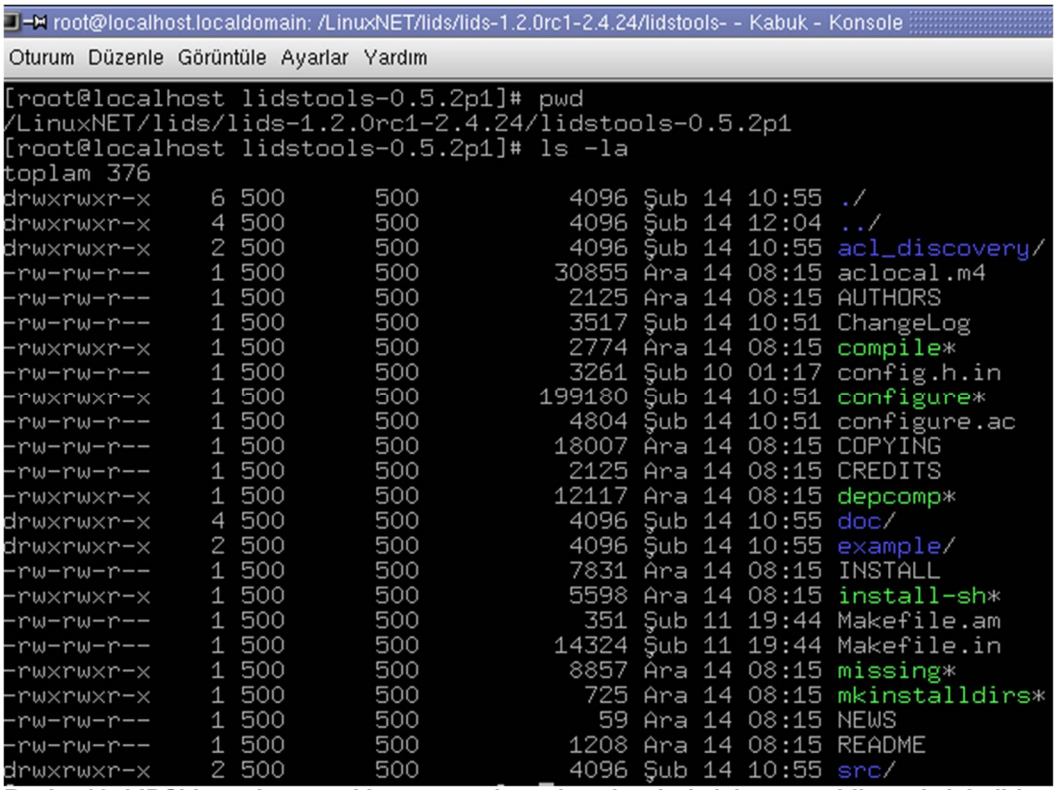
Resim 9: *make modules_install* sonrası

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

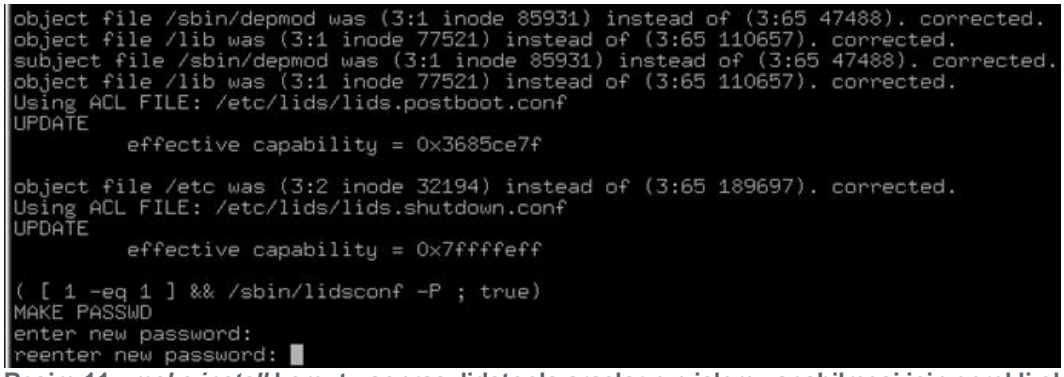
Örnek **lilo.conf** dosyası:

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 araçlarınıda 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)



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



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

LIDS kurulumu tamamlandıktan sonra(lidstools araçları da dahil) ***lidsadm –I*** (bu komutu baslangıç 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 oluştuğu 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 etmenizde 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
masajını görürsünüz. Eğer bazı aksaklıklar olursa bu komut ile gerekli uyarıları incelerseniz, 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>

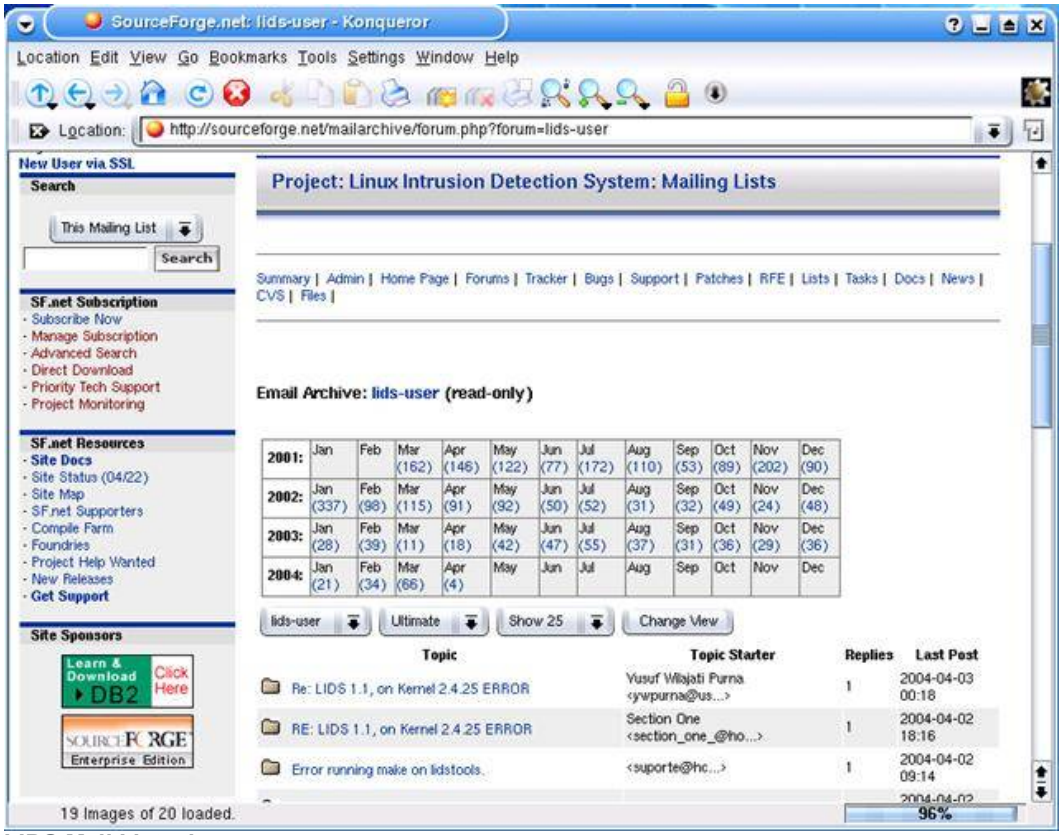
Usage: lidsconf -A [acl_type] [-s subject] -o object [-d] [-t from-to] [-i level] -j ACTION
lidsconf -D [acl_type] [-s file] [-o file]
lidsconf -Z [acl_type]
lidsconf -U
lidsconf -L [acl_type] [-e]
lidsconf -P
lidsconf -v
lidsconf -[h|H]

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 kuralar]
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
…
…



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[@]olympos.org