SUDOSH İLE KULLANICI DENETİMİ (AUDIT)

1. Denetim (audit) Gerekliliği

Gelişen teknoloji ile güvenlik çok büyük bir önem kazanmıştır. Dışarıya dönük güvenlik araçlarının kullanımı giderek artmıştır. Bu ilerlemelerle birlikte artık firmalar kendi kendilerini kontrol mekanizmaları geliştirmiştir. İç denetim mekanizması olarak da sayılabilecek audit kavramı ortaya çıkmıştır. Firmalar kendi sistem yöneticilerinin sistemde neler yaptıklarını bilmek istemekte ve güvenilir üçüncü kişilere kendi sistem yöneticilerini denetim yetkisi getirmektedir.

Sistem yöneticilerinin sistemlerde hangi komutları çalıştırdığını görmek ve birebir konsol simülasyonunu izlemek için **sudosh** basit ve kullanışlı bir araçtır.

2. Sudosh

SudoSH bir audit programıdır. Kullanıcıların konsolda yazdıklarını kaydeder ve gerekli görüldüğünde kayıtları almamızı sağlar.

sudosh projesi 2.0 sürümüyle birlikte eas adı altında duyurulmaya başlanmıştır. eas sürümü, sudosh a göre çok daha komplikedir. Ancak sudosh projesi basit ve kullanılabilirdir.

Sudosh 2004 yılından beri geliştirilmektedir. Open Software License V2 lisansına sahiptir.

3. Sudosh'ın Sisteme Kurulumu

Sudosh hemen hemen tüm Unix türevlerinde çalışmaktadır.

```
# wget http://sudosh.sourceforge.net/sudosh-1.8.2.tar.gz
# tar -zxvf sudosh-1.8.2.tar.gz
# cd sudosh-1.8.2
# ./configure
# make
# make install
```

Sudosh için bir log dizini oluşturmalısınız.

```
# mkdir /var/log/sudosh
# sudosh -i
```

Sudosh kurulumu bu şekilde tamamlanmaktadır.

4. Sudosh Yapılandırması

Sudosh'ı iki şekilde çalıştırabilirsiniz. Birincisi sudo komutu yardımı ile, ikincisi ise kullanıcıların öntanımlı kabuğu olarak sudosh'ı atayarak.

4.1. sudo kullanarak sudosh ın çalıştırılması

Öncelikli olarak sudo paketinin sisteminizde kurulu olması gerekir.

Eğer kurulum dizinini değiştirmediyseniz sudosh öntanımlı olarak /usr/local/bin/sudosh dizinine kurulacaktır.

/etc/sudoers dosyasına;

```
-- /etc/sudoers begin --
User_Alias      ADMINS=admin1,admin2,admin3
User_Alias      DBAS=dba1,dba2,dba3
Cmnd_Alias      SUDOSH=/usr/local/bin/sudosh

ADMINS          ALL=SUDOSH
DBAS            ALL=(oracle)/usr/local/bin/sudosh
-- /etc/sudoers end --
```

şeklinde bir konfigürasyon eklenebilir.

sudosh'ı sudo komutuyla kullanıp kayıt yapması sağlanabilir.

```
afsin@enderunix:~> sudo sudosh
Password:
starting session for afsin as root,/dev/tty3 (/bin/sh)
(root-1108345370)
linux:~ # echo $SHELL
/bin/sh
```

```
enderunix:~ # exit
exit
afsin@enderunix:~>
```

4.2 Kullanıcıların öntanımlı kabuğunu sudosh olarak atayarak

Kullanıcının öntanımlı kabuğunu sudosh olarak ayarlayarak kullanıcı sisteme giriş yapar yapmaz kayda geçilmesi sağlanır. Kullanıcı, sudosh kullanmak için ekstra bir komut kullanmaz ve sudosh kabuğunda olduğunun farkına varamaz.

Öncelikle sudosh'ın /etc/shells dosyasında tanımlı olması gerekir. Daha sonra /etc/password dosyasında kullanıcının kabuk değişkeni /usr/local/bin/sudosh olarak ayarlanmalıdır.

```
# cat /etc/passwd |grep afsin
afsin:x:1002:100:Afsin Taskiran:/home/afsin:/usr/local/bin/sudosh
```

4.3 Kayıtları Görmek

Sudosh-replay komutuyla sudosh kayıtlarını görebilirsiniz.

```
# sudosh-replay
Date                Duration From         To           ID
====                ======== ====         ==           ==
05/03/2006 13:01:27 1m4s      test           test           test-test-
1146650487-1v29bxMiJY822nI4
05/05/2006  09:30:40  26m         afsin        afsin        afsin-afsin-
1146810640-oxXbxrhASMUUtBKx

Usage: sudosh-replay ID [MULTIPLIER] [MAXWAIT]
See 'sudosh-replay -h' for more help.
Example: sudosh-replay afsin-afsin-1146810640-oxXbxrhASMUUtBKx 1 2
#
```

Oturumlardaki ekran çıktılarını görmek için aşağıdaki komutu kullanabilirsiniz.

```
enderunix:~#       sudosh-replay       test-test-1146650487-
1v29bxMiJY822nI4 0
afsin@enderunix:~> echo $SHELL
/bin/sh
afsin@enderunix:~> sudo su -
Password:
afsin@enderunix:~> whoami
```

```
test
afsin@enderunix:~>
afsin@enderunix:~>
afsin@enderunix:~>
afsin@enderunix:~> exit
logout
enderunix:~ #
```

KAYNAKLAR:

[1] man sudosh

İlk güncelleme: 05.05.2006
Son güncelleme: 05.05.2006

Afşin TAŞKIRAN
EnderUNIX Yazılım Geliştirme Takımı @ Türkiye
afsin ~ enderunix.org
www.enderunix.org/afsin