

## Unix sistem girişlerinin takibi

Bugünkü yazıda, FreeBSD sisteminiz eğer henüz kullanıcı sonrasını okunup güncellenen, utmp, wtmp, ve lastlog dosyalarının bir göz atacağız. Bu dosyaların normal günlük (log) dosyaları gibi doğrudan ulaşılabilir bulunmadığı için, bunları okuyabilmemiz için gerekli olan programlar hakkında biraz bilgi vereceğiz. Son olarak makaleyi giriş (login) veterinerleri için kullanacağımız birkaç program hakkında konuşarak bitireceğiz. Makalede İngilizce terimlerin ne anlama geldiklerini kısaca açıklayıcı olarak bakımından belirterek başlayalım:

log = günlük

login = giriş

ev = home

terminal = bağlantı noktası

virtual terminal = sanal bağlantı noktası

Kelimeler ile başlıyoruz. İlk olarak /var/log/lastlog dosyasıyla başlayabiliriz. Herhangi bir kullanıcı sisteme girdiğinde giriş programı bu dosyayı okuyarak kullanıcının FreeBSD sisteminde ne zaman girdiğini belirler ve daha sonra yeni girişi tarihinin bir satır olarak kayıtlara geçirir. Bakalım "genesis" kullanıcısı FreeBSD sisteme girdiğinde ne oluyor:

```
login: genesis
```

```
Password:
```

```
Warning: your password expires on Tue Feb 6 14:50:29 2001
```

```
Last login: Sat Feb 3 15:56:53 from biko
```

```
Copyright (c) 1980, 1983, 1986, 1988, 1990, 1991, 1993, 1994
```

```
The Regents of the University of California. All rights reserved.
```

```
Welcome to FreeBSD 4.2!!!
```

```
You have new mail.
```

```
You cannot kill time without injuring eternity.
```

Bakalım buradan ne oluyor. Giriş programı genesis kullanıcıya girilen şifreyi kabul etti ve /etc/master.passwd dosyasındaki şifrelenmiş satırlarla karşılaştırdı. Ayrıca /etc/login.conf dosyasında okuyarak şifrenin uzunluğunu ve daha önce belirlediğimiz uzunluğa eşit olduğunu doğrularken şifrenin süresinin salı gününe sonlanacağını belirleyerek bize çıktı olarak gösterdi. Daha sonra var/log/lastlog dosyasını okuyarak kullanıcının ne zaman sisteme girdiğini bulup, (görünümlerini görebük kullanıcıya ait giriş bilgileri Cumartesi günü biko adındaki bir bilgisayardan çekilmiş) bu bilgiyi telif hakkı, günün mesajı, yenisalınane-posta uyarısı ve şubizimeski dostumuz fortune programı tarafından üretilen Henry David Thoreau'nun bir sözüyle birlikte bize çıktı olarak verdi.

Bumesajları giri ş sırasında geçmeniz mümkün. Geniş kullanıcılar ak, ev(home) dizininde .hushlogin adında bir dosya yaratıyorum:

```
cd
touch .hushlogin
```

Daha sonra sisteme dençi kipte kargirdi ğimde:

```
exit
```

```
login: genesis
Password:
```

Alimony is a system by which, when two people make a mistake, one of them keeps paying for it.  
-- Peggy Joyce

Şeklinde bir çiktı alıyorum. Dikkate dersanız genesis kullanıcısının büseferaldı ğitek mesaj, kullandı ğınız shell konfigürasyonun tarafında çalı şıp çalı şmayacağını belirleyebilece ğiniz fortune programının tarafında üretilen günün sözü oldu. Bugiri şise gere ğinden çoksessiz olmu şabenziyor zira nee-posta alı pılmadı ğımız nede şifremizin suresinin nezamandolacağı hakkında hiç bir bilgialmadık.

İkinci kayıt dosyamız w, who, ve users komutları ile okuyabilece ğimiz ve o anda sistemi kullanmakta olanki şiler hakkında bilgi içeren, /var/run/utmp dosyası. Gelin bu komutlara users komutu ile başlayarak bir gözatalım:

```
users
genesis test1 test2 test3
```

users komutu sisteme sadece benim oldu ğunu çok fazla detay olmadan görebilmeki için çok yararlıdır. Fakat hangileri terminalde hangikull anıcıların bulundu ğunu görmek isterseniz w komutunu kullanmanız gerekiyor.

```
w
```

```
5:01PM up 3:30, 7 users, load averages: 0.04, 0.06, 0.02
USER TTY FROM LOGIN@ IDLE WHAT
genesis v0 - 1:31PM 1 more
genesis v1 - 1:32PM - w
genesis v2 - 1:32PM 3:11 xinit /home/genesis/.x
genesis v3 - 1:46PM - pico utmp
test3 v4 - 4:51PM - -tcsh (tcsh)
test1 p0 biko 4:50PM 10 -tcsh (tcsh)
test2 p1 biko 4:51PM 1 -tcsh (tcsh)
```

Görünüşe göre FreeBSD sistemimde yedi adet aktif halde bulunan kullanıcı FreeBSD sistemime fi ziksel olarak ve ayrıca ilkdört bağlantı noktasında (v0-v3) başlı ğı gözükmekte. "test3" kullanıcısı da lokal olarak 5.(v4) sıradaba ğlı olarak gözükmekte. "test1" kullanıcısı "biko" ad ındakibilgisayardan ilka ğ

bağlantı noktası (p0) üzerinden bağlanarak gözükürken, "test2" kullanıcısı ise ikinci bağlantı noktasından (p1) yine "biko" adlı bilgisayarla bağlanmaktadır.

Burada gördüğümüz `IDLE` bölümü ise bağlanılan kullanıcının son zamanlarda yaptığı şey yazdığını, `WHAT` bölümü ise her bağlantı noktasında hangi programların çalıştığını göstermektedir. Tüm bağlantı noktalarında hangi programların çalıştırıldığını görebilmek için `d` parametresini kullanabiliriz:

```
w -d |more
```

```
5:10PM up 3:39, 7 users, load averages: 0.00, 0.00, 0.00
USER TTY FROM LOGIN@ IDLE WHAT
219 -csh (csh)
1085 _su (csh)
1107 man w
1108 sh -c /usr/bin/zcat /usr/share/man/cat1/w.1.gz | more
1110 more
genesis v0 - 1:31PM 10 more
220 -csh (csh)
1138 w -d
genesis v1 - 1:32PM - w -d
221 -csh (csh)
396 /bin/sh /usr/X11R6/bin/startx
401 xinit /home/genesis/.xinitrc --
403 xfce
408 /usr/local/lib/netscape-linux/navigator-linux-4.76.bin
409 (dns helper) (navigator-linux-)
genesis v2 - 1:32PM 3:20 xinit /home/genesis/.x
222 -csh (csh)
977 pico utmp
genesis v3 - 1:46PM - pico utmp
1074 -tcsh (tcsh)
test3 v4 - 4:51PM 9 -tcsh (tcsh)
1061 -tcsh (tcsh)
test1 p0 biko 4:50PM 19 -tcsh (tcsh)
1066 -tcsh (tcsh)
test2 p1 biko 4:51PM 7 -tcsh (tcsh)
```

Bu komutu dikkatederseniz normal bir kullanıcı olarak kullanıldım. Siz de sisteminizde bu komutu süper kullanıcı olarak kullanmanız gerek kalmadıkça kullanabilirsiniz. Komutu süper kullanıcı olarak kullanmanın tek farkı sadece kendi programlarınızda geldiği şifrelerin kullanılmakta oldukları programlara müdahale etme şansını size vermesi olacaktır. `whois` komutu `w` komutunun verdiği çıktıya çok yakın bir çıktı vermektedir:

```
who
```

```
genesis    ttyv0    Feb  3 13:31
genesis    ttyv1    Feb  3 13:32
genesis    ttyv2    Feb  3 13:32
genesis    ttyv3    Feb  3 13:46
test3      ttyv4    Feb  3 16:51
test1      ttyp0    Feb  3 16:50    (biko)
test2      ttyp1    Feb  3 16:51    (biko)
```

Eğer `who` komutunu `am` parametresi ile kullanırsanızda geniş sonuçlar alabilirsiniz:

```
who am i
genisis      ttyv1    Feb 13:32
```

Görünüşe göre `genisis` kullanıcısi ikinci sanalbağlantı noktası (virtual terminal) üzerinde bağlı bulunmakta.

Bunun yanında `who` komutunun `var/run/utmp` dosyası yerine `/var/log/wtmp` dosyasını okumasına glayabilirsiniz.

```
who /var/log/wtmp

genisis      ttyv0    Feb 3 13:25
shutdown    ~        Feb 3 13:30
             ttyv0    Feb 3 13:30
reboot      ~        Feb 3 13:31
genisis     ttyv0    Feb 3 13:31
genisis     ttyv1    Feb 3 13:32
genisis     ttyv2    Feb 3 13:32
genisis     ttyv0    Feb 3 13:34    (biko)
genisis     ttyv3    Feb 3 13:46
genisis     ttyv1    Feb 3 15:04    (biko)
genisis     ttyv4    Feb 3 15:04
             ttyv0    Feb 3 15:31
genisis     ttyv0    Feb 3 15:56    (biko)
             ttyv0    Feb 3 16:00
genisis     ttyv0    Feb 3 16:00    (biko)
             ttyv0    Feb 3 16:23
genisis     ttyv0    Feb 3 16:23    (biko)
             ttyv0    Feb 3 16:23
genisis     ttyv0    Feb 3 16:23    (biko)
             ttyv4    Feb 3 16:32
genisis     ttyv4    Feb 3 16:32
             ttyv4    Feb 3 16:32
genisis     ttyv4    Feb 3 16:32
             ttyv0    Feb 3 16:45
             ttyv1    Feb 3 16:45
test1       ttyv0    Feb 3 16:50    (biko)
test2       ttyv1    Feb 3 16:51    (biko)
             ttyv4    Feb 3 16:51
test3       ttyv4    Feb 3 16:51
             ttyv4    Feb 3 17:36
shutdown    ~        Feb 3 20:39
             ttyv3    Feb 3 20:39
             ttyv1    Feb 3 20:39
             ttyv0    Feb 3 20:39
             ttyv2    Feb 3 20:39
reboot      ~        Feb 3 20:40
genisis     ttyv0    Feb 3 20:40
genisis     ttyv1    Feb 3 20:40
genisis     ttyv2    Feb 3 20:40
genisis     ttyv3    Feb 3 20:43
genisis     ttyv4    Feb 4 08:25
```

Çıktımsisteminyenidenba şlatılmasıvekapatılmasıhakkındakibilgilerideiç erdiğine dikkatedin.SizinFreeBSDsisteminizde,kullanıcıla rınnekadarsıklıklasistemegirip çıktıklarınaba ğlıolaraklistedahauzunolabilir.E ğerçıkıtınızçokuzuniseenson10giri şı aşığidakikomutilegörebilirsiniz:

```
who /var/log/wtmp | tail
```

/var/log/wtmpdosyasıhergiri ş,çıkı ş,güncellemeġünü,sistemkapanmasıvesistem yenidenba şlatılmasıileilgilibilgilerinkaydınıtutmakta.Bu dosyadakibilgilereise last ve ackomutlarınıkullanarakula şabilirsiniz.Hadigelinyukarıdakiçıkıtyı last komutundanaldı ğımızçıkıtlekarsıla ştırılm:

```
last
genisis ttyv4 Sun Feb 4 08:25 still logged in
genisis ttyv3 Sat Feb 3 20:43 still logged in
genisis ttyv2 Sat Feb 3 20:40 still logged in
genisis ttyv1 Sat Feb 3 20:40 still logged in
genisis ttyv0 Sat Feb 3 20:40 still logged in
reboot ~ Sat Feb 3 20:40
shutdown ~ Sat Feb 3 20:39
test3 ttyv4 Sat Feb 3 16:51 - 17:36 (00:44)
test2 ttyv1 biko Sat Feb 3 16:51 - shutdown (03:48)
test1 ttyv0 biko Sat Feb 3 16:50 - shutdown (03:48)
genisis ttyv4 Sat Feb 3 16:32 - 16:51 (00:18)
genisis ttyv4 Sat Feb 3 16:32 - 16:32 (00:00)
genisis ttyv0 biko Sat Feb 3 16:23 - 16:45 (00:21)
genisis ttyv0 biko Sat Feb 3 16:23 - 16:23 (00:00)
genisis ttyv0 biko Sat Feb 3 16:00 - 16:23 (00:22)
genisis ttyv0 biko Sat Feb 3 15:56 - 16:00 (00:03)
genisis ttyv4 Sat Feb 3 15:04 - 16:32 (01:27)
genisis ttyv1 biko Sat Feb 3 15:04 - 16:45 (01:41)
genisis ttyv3 Sat Feb 3 13:46 - shutdown (06:52)
genisis ttyv0 biko Sat Feb 3 13:34 - 15:31 (01:57)
genisis ttyv2 Sat Feb 3 13:32 - shutdown (07:06)
genisis ttyv1 Sat Feb 3 13:32 - shutdown (07:06)
genisis ttyv0 Sat Feb 3 13:31 - shutdown (07:07)
reboot ~ Sat Feb 3 13:31
shutdown ~ Sat Feb 3 13:30
genisis ttyv0 Sat Feb 3 13:25 - shutdown (00:04)
reboot ~ Sat Feb 3 13:25
wtmp begins Sat Feb 3 13:25:04 2001
```

Dikkatederseniz.Ensongiri şlersondavegüncelgiri şlerenbastaolmaküzeresıratam ters şekilde.Bunagöree ğerçıkıtyısadecel0satıraindirgemekisterseniz headkomutuile sondakide ğilenbastakigiri şlerigörebilirsiniz:

```
last | head
```

Sonüçbolumhangikullanıcısystemenezamansiste megiripnezamançıkıtyı ğını,ne kadarsurekaldı ğınıveçıkı şnedenininyenidenba şlatmaveyasisteminkapanmasını olduġunugöstermesiaçısındanönemlidir.

last komutu ayrıca reboot gibide geniş parametrelerle kullanılabilir.

```
last reboot
reboot      ~           Sat Feb  3 20:40
reboot      ~           Sat Feb  3 13:31
reboot      ~           Sat Feb  3 13:25
wtmp begins Sat Feb  3 13:25:04 2001
```

Bu parametre FreeBSD sistemimizin kapanış veyeniden başlatma tarihleri hakkında bize güzel bir özetsunmakta.

ac programı ise /var/log/wtmp dosyasında bulunabilir. Şeyi çıkartıp toplayarak fazla bağlantı zamanı olan kullanıcıları bulmak için kullanılır. Eğer ac'yı parametrelemeden kullanırsanız /var/log/wtmp dosyasında bulunan tüm bağlantı toplamını çıktı olarak alırsınız.

```
ac
      total    165.04
```

Günlük olarak toplam bağlantı zamanını görmek isterseniz:

```
ac -d
Feb  3 total    124.42
Feb  4 total    41.52
```

Her kullanıcı için /var/log/wtmp tutulmuş toplam bağlantı zamanlarını görmek için ise:

```
ac -p
      test1      4.12
      test2      4.11
      test3      0.75
      genesis    156.06
      total      165.04
```

Özetlemek gerekirse: w, who, ve users, /var/run/utmp dosyasındaki; last ve ac ise /var/log/wtmp içindeki bilgileri görmek için kullanılıyor.

Bugünkü makalede bahsetmek istediğim diğer şey ise kullanılmayan bağlantı noktalarının kilitletmesi hakkında. Normalde kullanıcı oturumunu kapatmadan önce birkaç dakika için bağlantı noktasından ayrılabilir. Bazen ise kullanıcı oturumunu kapatmadan önce birkaç dakikalığına bağlantı noktasından ayrılabilir. Sistem iniş yapılıncaya kadar bilgileriniz o arada ulaşılmaz hale gelebilir. Sistem iniş yapılıncaya kadar bilgileriniz o arada ulaşılmaz hale gelebilir. Sistem iniş yapılıncaya kadar bilgileriniz o arada ulaşılmaz hale gelebilir. FreeBSD sisteminiz lock kadında bir program ile gelmekte. Eğer sadece lock komutu verirseniz tekrar terminale girebilmek için şifrenizi girmeniz gerekecektir.

```
lock
Key:
Again:
lock: /dev/tty0 biko timeout in 15 minutes
time now is Sun Feb  4 11:48:34 EST 2001
Key:
```

Yukarıdakiörne ğebakarsanızba ğlantınoktasının15dakikaveyakullanıcıgelip şifresini gelipgirenekadarkilitlihaldetutulaca ğınıgörürsünüz.E ğer lockkomutunuher verdiĝinizdeayrıbir şifregirmekistemiyorsanız lock -pkullanarakba ğlantınoktasını açmakiçinkullanaca ğınız şifreingiri ş şifrenizolmasınısa ğlayabilirsiniz.Kilitlenmişbir baĝlantınoktasıancak şifreingirilmesi,zamanasimisuresiningeçmesinin beklenip baĝlantınoktasınıkendikendinikapatmasınısa ğlanmasıveyasüperkullanıcınınbu programı şlemnumarasınabir kill sinyaliğöndererek kapatmasıilegerçekte şir.

Bununyanındaportkoleksiyonumuziçindekullanabil eceĝimiz vlockadındadabir programbulunmakta. İnterneteba ğlıvesüperkullanıcıhesabındaiken:

```
cd /usr/ports/security/vlock
make install clean
```

Komutlarileprogramıkurabilirsiniz.programıkull anmakiçinise:

```
vlock
This TTY is now locked.
Please enter the password to unlock.
genesis's Password:
```

Buprogramın şifreolaraksadecekullanıcı şifrelerinikullandı ğıdikkatinizi çekecektir.Süperkullanıcıisesadece rootkomutuvebunuizleyen şifresiileterminali açabilmektedir.

```
genesis's Password: (type in the word "root")
root's Password:
```

vlockprogramıayrıcaFreeBSDsistemizdekitümba ğlantınoktalarına ğgiri şlerini engellemeden,tekbirkomutlakitleyebilmektedir. Eĝer vlock -akomutunuverirsem ekranımdasuçkıtıyalırım:

```
The entire console display is now completely locked.
You will not be able to switch to another virtual console.
Please enter the password to unlock.
genesis's password
```

BuekrandaALTfonksiyontu şlarıımve"genesis"veyasüperkullanıcı şifresinibilmeyen vefizikselolarakFreeBSDsistemimegelipgiri ş yapmayaçalı şantümkullanıcılara kapatılmışdurumdadır.BuözellikFreeBSDsistemisinunucuola rakkullananki şileriçin çokyararlıolacaktır.Zira vlock -atümba ğlantınoktalarınıkapatırkena ğgiri şlerine tamamenizinvermektedir.

ÖzgürÖzdemircili

<http://www.enderunix.org>

<http://news.enderunix.org>

<http://haber.enderunix.org>

Sorularınızıçin: [dionypheles@gmx.net](mailto:dionypheles@gmx.net)

## **Kaynaklar**

*DruLavigne* in“MonitoringUnixLogins”adlıyazısındançevrilmiştir.

Yazar`insayfasına <http://www.oreilynet.com/pub/au/73>,orijinalmetneise [http://www.onlamp.com/pub/a/bsd/2001/02/14/FreeBSD\\_Basics.html](http://www.onlamp.com/pub/a/bsd/2001/02/14/FreeBSD_Basics.html) adresinden ulaşabilirsiniz.