

Jail Nedir?

Java ile haşırneşir olanlarınız sandbox gaveling konseptine yabancı olmamalı. Bu konuda bilgisi olmayanlar için, herkese kendi içinde çalışabilmek için bir yer sağlar diyebiliriz. Bir kişiye ait sandbox diğer bir kişi tarafından kullanılamaz ve hatta hiçbirşey paylaşılamaz. FreeBSD`de *jail`ler* kısaca bunu sağlamak için kullanılır. Her işlemi kendi içinde tutarlar ve diğer işlemlere karışmasını engellerler. Jail kendine ait bir ip numarasına ihtiyaç duyar ki buda adres sıkıntısı olanlar için biraz sorun yaratabilir. Eğer böyle bir sıkıntısı olan kişiler aşağıda tartışacağımız *chroot* komutunu kullanabilirler. Jail kadar güvenli olmasa da yine de hiç bir güvenlik kullanılmamasından iyidir.

Bu ne bakımdan işimize yarayacak? Örneğin ftp sunucusu ve internet çıkışı olan bir şirket düşünün. Sunucu için yeni bir hata keşfediliyor ve cracker arkadaşımız ftp servisi sayesinde root erişimi sağlıyor. Bu sunucudaki ftp servisi eğer bir sandbox veya jail içinde çalıştırılıyorsa cracker bu makinadaki, içinde özel bilgilerinde olduğu herşeye ulaşabilir. Fakat eğer FTP sunucusu jail içinde çalıştırılırsa cracker ancak ftp dosyalarına ulaşabilecek.

Tabiki bu tamamen risksiz degil. Eğer secure level 0`da çalışıyorsanız cracker yalın disk aygıtına erişip oradan bilgileri okuyabilir. Çözüm tabiki çok basit- jail kullanmanızı gerektirecek kadar önemli bilgi içeren bir makinada gerekli secure level`ların kullanılması. Bu cracker`ın yalın disk aygıtlarına ulaşip okumasını engelleyecektir.

Jail konfigürasyonu

Jail konfigürasyonu gerçekten çok kolay.

İlk olarak system konfigürasyonunuzun jail kullanmaya uygun olduğundan emin olalım. Her jail kendi ip adresine sahip olmalı ve servisler ancak belli adresleri dinleyerek gelen isteklere cevap veriyor olmalı. Örneğin, eğer bilgisayar adresleriniz `199.232.41.26` (ana) ve `199.232.41.27` (jail) ise, `/etc/rc.conf` dosyasına `inetd_flags="-wW -a 199.232.41.26"` parametresini ekleyerek `inetd daemon`unun` sadece `199.232.41.26` ip adresini dinlemesi için ayarlamalısınız. Eğer bunu yapmazsanız alınan ip numarası yüzünden karışıklıklar çıkacaktır.

Bazı daemon`lar için bu kolay olan birşey değil - `sendmail` ve `rpcbind` bunun iki örneği olarak verilebilir. Eğer sisteminizde bu servisleri çalıştırıyorsanız, jail içine alıp orada servis vermelerini sağlamayı düşünebilirsiniz. Bütün jail içinde çalışmayan servisleri tek adres dinlemek üzere ayarladıktan sonra makinanızı yeniden başlatın. Bu herşeyi düzenleyerek herhangi bir karışıklığı önleyecektir.

Herşeyi ayarladıktan sonra `/usr/jail/ftp` gibi jail'I içinde barındıracak bir klasör oluşturun. Daha sonra `/usr/src` klasörüne girip şunları yazın:

```
# make world DESTDIR=/usr/jail/ftp
# cd etc
# make distribution DESTDIR=/usr/jail/ftp
# cd /usr/jail/ftp/dev
# sh
# MAKEDEV jail
# cd ..
# ln -sf /dev/null kernel
```

Bu komutlar jail'I oluşturup gerekli programların çalışmasını sağlayacaktır. Bu işlem gerçekte `perl`, `gcc`, ve `sendmail` gibi servisin gerektiğinden çok daha fazla programı yükleyecektir. Fakat aklınızda tutmanız gereken şey işlem bozulana kadar ihtiyacınız olmayan servislerin burdan kaldırılmasının işlem çalışana kadar gerekli programların yüklenmesinden daha kolay olduğudur.

Bunun yanında daha kolay bir konfigürasyon arayüzü oluşturması açısından `/stand/sysinstall` klasörünü `/usr/jail/ftp/stand` içine kopyabilirsiniz. Birazdan bunu nasıl kullanacağımızı anlatacaz.

Sistem yeniden başlatılmış olarak şimdi jail çalışma ortamını ayarlamaya hazırız. İlk olarak servisi başlatalım:

```
# jail /usr/jail/ftp jail.hostname.com 199.232.41.27 /bin/sh
```

Bu komut sizi jail çalışma ortamında çalışan komut satırına götürecektir. Buradan `/stand/sysinstall` (/ bu düzeyde sistemin değil jail'in ana klasörünü belirtmektedir) komutunu çalıştırabilirsiniz.

Root şifresinin değiştirilmesi(system root şifresi ile aynı şifreyi kullanmayın!), kullanıcı hesaplarının eklenmesi, ve `/etc/resolv.conf` dosyasının değiştirilmesi gibi yapılması gereken birkaç konfigürasyon daha var. Yapmanız gereken konfigürasyon için `man 8 jail` komutunu kullanarak yazanları uygulayınız. Unutmayın ki sisteme girmeniz gerekecek bunun için de jail içerisinde SSH sunucusunu çalıştırmayı unutmayın.

Jail çalışma ortamını konfigre ettikten sonra komut satırından çıktığımızda jail kapanacaktır.

Jail'I çalıştırmaya çok yakınız. İlk olarak ip adresini ayarlayın. Örneğin :

```
ifconfig fxp0 inet alias 199.232.41.27 255.255.255.255
```

Bunu `/etc/rc.conf` içinden ayarlayarak boot sırasında uygulanmasını sağlayabilirsiniz.

Şimdi jail'ı başlatalım. Bunu iki komutla yapıyoruz:

```
# mount -t procfs proc /usr/jail/ftp/proc
# jail /usr/jail/ftp jail.hostname.com 199.232.41.27 /bin/sh /etc/rc
```

Birkaç uyarı mesajı göreceksiniz ve artık jail içinde çalışan bütün servisleri görebilirsiniz. Eğer SSH çalıştırıyorsanız, jail ortamına sanki başka bir bilgisayara bağlanıyormuş gibi bağlanabilirsiniz.

`halt` gibi normal kapatma komutları jail içinde çalışmaz. Kapatmak için ilk önce sisteme girin ve jail ortamında root olun. Daha sonra jail içinden `kill -TERM -1` veya `kill t -KILL -1` ile servisi kapatabilirsiniz.

Şu anda FTP ve DNS servisleri veren sunucuları rahatlıkla jail içinden çalıştırabilirsiniz. Bitirmeden önce son bir not daha:

`security.jail.set_hostname_allowed` (veya 5.0 öncesi sistemlerde `jail.set_hostname_allowed`) `sysctl` değişkeni jail içinden `system` isminin değiştirilip değiştirilmeyeceğine karar verir. Bu kurulum sonunda açık olarak gelir. Eğer kapatmak isterseniz `/usr/jail/ftp/etc/sysctl.conf` içinde `security.jail.set_hostname_allowed=1` parametresini `security.jail.set_hostname_allowed=0` olarak ayarlamanız yeterli olacaktır. Bunun FreeBSD-4.x makinelerde `jail.set_hostname_allowed=0` olduğunu unutmayın!

Sonuç

Bu yazıda jail kavramının nasıl hayata uygulandığını gördünüz. İster bir sistemden birkaç servis çalışıyor, ister genel servis sağlayıcı olarak çalışın, jail'leri sisteminizde kullanmanız size geceleri rahat bir uyku çekmenizde yardımcı olacaktır.

Ozgur Ozdemircili

<http://www.siberhayat.com>

Siberhayat.com - siber yasamlarimizin bir yansimasi –

Sorulariniz icin: ozgur@siberhayat.com