UYGULAMALARINIZI HAPSEDİN
CAMMP

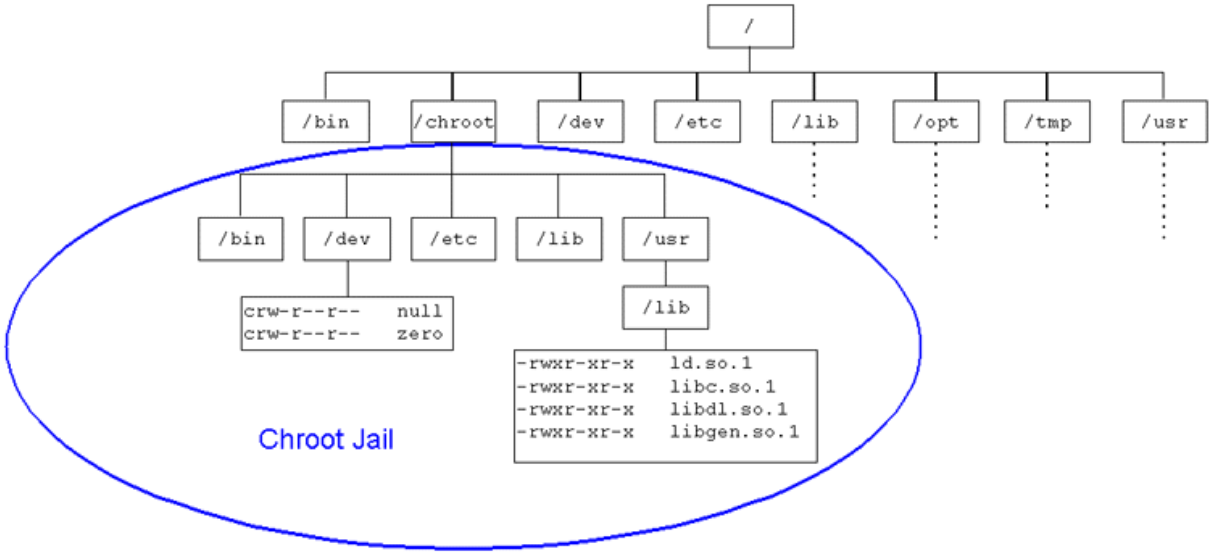
Chroot **A**pache **M**ysql **M**odSecurity **P**hp

gokhan@enderunix.org, Gökhan Alkan

1. Giriş

Chroot, sunucu servisleri ve uygulamalar için yeni bir kök (/) dizini tanımlar. Kısaca çalıştırılacak olan servis ya da uygulama için gerekli kütüphaneler, yapılandırma dosyaları, sürücü dosyaları (device file) bu servis için belirlenen kök dizinde bulunan ilgili yollara (path) kopyalanır ve sunucu yazılımları belirlenen kök dizini altında çalıştırılır.

Aşağıdaki şekilde (Şekil 1 Chroot Kullanımı İle Yeni **Dosya Sistemi Hiyerarşisi**) chroot kullanımı ile dosya sistemine erişim gösterilmiştir.



Şekil 1 Chroot Kullanımı İle Yeni Dosya Sistemi Hiyerarşisi

Şekil 1'de görüldüğü gibi sunucu servis yazılımının ve uygulamaların işletim sistemi kaynaklarına erişimi kısıtlanmış sadece gerekli ve belirtilen kaynaklara erişimine izin verilmektedir.

2. Motivasyon

Apache, php ve mysql yazılımlarının birlikte kullanıldığı düşünüldüğünde, uygulamadan veya servislerden kaynaklanan bir açıklıktan ötürü saldırgan hapishane dışındaki işletim sistemi kaynaklarına erişim sağlayamayacaktır. Katmanlı güvenlik anlayışı çerçevesinde sunucu servis yazılımlarının chroot ortamında çalıştırılması gerekmektedir.

Katmanlı güvenlik anlayışı ve chroot ortamında sunucu yazılımlarının ve uygulamaların çalıştırılmasının önemini anlamanın en keskin yolu, olaya saldırgan gözü ile bakmaktır. Bu önemi, eğitim amaçlı geliştirilmiş "basic php shell" uygulaması ile kullanılarak yapılabilecekler ile anlayabilirsiniz

http://code.google.com/p/cammp/wiki/CAMMPShowsOff

3. Çözüm

Buraya kadar teoride her şey yolunda gitti. Peki ya bu sunucu yazılımlarını ve uygulamaları ayrı ayrı chroot ortamında çalıştırmak için ne yapmak gerekli? Uygulamalarınızı chroot ortamı altında çalıştırmak için uzun ve çetrefilli yollardan geçmeniz gerekmektedir. Gerekli dizinler ve dosyalar oluşturulmalı, gerekli dosyalar chroot ortamı altında bulunan ilgili dizinlere kopyalanmalı, kullanıcı/grup ikilisi oluşturulmalı vs vs. Ki bu adımların gerçekleştirilmesi sırasında her şeyin yolunda gitmeyeceği de hesaba katılırsa, sunucu servis yazılımlarını ve uygulamaları chroot ortamı altında çalıştırmak bazen oldukça can sıkıcı bir durum alabilmektedir. Ayrıca kurulumun tamamlanmasının ardından izinler ile ilgili sıkılaştırmaların gerçekleştirilmesi de cabası.

İşte CAMMP bütün bu işlemleri sizin için kolaylaştıracak bir araç. Chroot Apache Mysql Modsecurity Php sunucu servis ve yazılımların baş harflerinden oluşan CAMMP bütün bu işlemleri sizin için kolayca ve kısa sürede gerçekleştiriyor. Şu an için RHEL Linux sistemlerde test edilen CAMMP yakın zamanda diğer Unix/Linux dağıtımları içinde destek verecektir.