

## Süreç Hesaplaması

Son Güncelleme Pazartesi, 17 Kasım 2008

Sistem yöneticilerinin hangi kullanıcıların hangi komutu ne zaman çalıştırdığını görmesi gerekli güvenlik açısından önemlidir, çünkü saldırılar her zaman dıþardan gelmez. Sisteme yapılan saldırıların sonuçlarının tespit etmek için sistemde olan kullanıcıların çalıştırdığı zararlı programları için Süreç hesaplaması ile sistemde yapılan işlemleri detaylı olarak kayıttan tutmak gerekir. Redhat sistemlerde aşağıdaki komutları vererek süreç denetimi çalıştır hale getirilir. Aşağıdaki gibi `ac` komutunu herhangi bir parametre vermeden kullanırsanız, komutu çalıştıran kullanıcının sistemde geçirdiği zamanı saat olarak ekrana basar. Sisteme giren bütün kullanıcıların sistemde geçirdiği süreyi öğrenmek içinse `ap` komutunu kullanırız. Kullanıcı adı, çalıştırılan komut ve bu komutların hangi terminalde çalıştırıldığını görmek için `lastcomm` kullanıcı ismi komutu kullanılır. Özetli olarak kayıttan bulunan bütün komutları ve bu komutların kaç sefer çalıştırıldığını `ls` komutu ile kayıtların kullanıcı başına İstatistikleri çıkarılır. Bu komutları karşılaştırdığınızda sisteminizde olmaması gereken hareketleri görebilir ve ona göre önlemler alabilirsiniz.