# Linux Sunucuları için Güvenlik İpuçları

Korhan Gürler, Burç Yıldırım

{kg,by}@dikey8.com

# Planlama

- Sistemin vereceği hizmetin belirlenmesi
  - Kullanılacak yazılımın seçilmesi
    - İşletim Sisteminin ve yazılımların temini
    - İşletim Sistemi ve yazılımların yamalarının temini
  - Disk bölümlendirilmesinin ve dosya sisteminin planlanması
  - Kullanıcı planlanması
- Yapılan işlemlerin dökümantasyonu

# Fiziksel Güvenlik – I

- Fiziksel güvenlik önlemleri, kazaların, fiziksel hırsızlığın, doğal afetlerin, art niyetli kişilerin, sosyal patlama olaylarının, haşeratların, evcil hayvanların sisteme verebileceği zararları engellemeyi amaçlar.
  - Donanımın yeri ve fiziksel erişim olanakları
    - Kilitler ve diğer önlemler
  - Ağ yapısı
    - Tek hata noktası, elektronik dinleme, hata toleransı

# Fiziksel Güvenlik - II

- Kesintisiz Güç Kaynağı
- BIOS/RAM/EEPROM ve konsol parolaları ile sisteme fiziksel erişimin sınırlandırılması
- Tüm donanımın etiketlenmesi

# Kurulum – I

- Planlanan bölümlendirmenin uygulanması
  - `/` `/dev/hda2`
  - `/usr` `/dev/hda3`
  - `/var` `/dev/hdb2`
  - `/tmp` `/dev/hda4`
  - `/home` `/dev/hdc2`
- İşletim Sisteminin kurulumunda minimal yaklaşım uygulanmalı, gereksiz hiçbir yazılım kurulmamalıdır

# Kurulum – II

- İşletim Sistemine ve kurulan yazılımlara yamaların uygulanması
- Çekirdek için ek güvenlik sağlayan yamalar uygulanmalı
- İhtiyaç olmayan tüm parametreler çekirdekten çıkartılmalı
  - Geliştirilmekte olan ve bitmemiş seçenekler
  - Diğer işletim sistemleri için emulasyon
  - Kullanılmayan iletişim protokolleri
  - Kaynak yönlendirmeli paketler

# Kurulum – III

- Kullanıcı onaylama için PAM (pluggable application modules) kullanılmalı
  - PAM birçok alanda sınırlandırma imkanı sağlar
    - core, fsize (tek bir dosya büyüklüğü), işlemci zamanı gibi sınırlandırmalar mümkün
    - Bu tür ayarlarla sistemin veriminin artırılabilir

# Ayarlar – I

- BIOS
  - Disket sürücününü iptal edilmesi
  - Açılış sırasının düzenlenmesi
- Boot loader ayarları
  - Açılışta parola koruması
  - Ayar dosyasının sadece süper kullanıcı tarafından okunabilir/yazılabilir olması
  - Açılışta kullanıcının müdahalesine izin vermemesi

# Ayarlar – II

- Tek kullanıcı modu için parola koruması
- `/etc/profile.d` dizini ve Kabuk giriş ayarları (csh.login,sh.login)
  - Sistem parametrelerini tanımlar, mutlaka gözden geçirilmeli ve gereksiz her türlü parametre kaldırılmalı
- `/etc/rc.d` dizini
  - Sistemin açılış sırasında yüklediği sürücüler ve açtığı servisler
- `/etc/skel` dizini
  - Yeni bir kullanıcı tanımlandığında kullanıcı dizinine eklenen dosyalar
- `/etc/issue /etc/issue.net /etc/motd`
  - Yasal bildirimlerle sisteme giriş yapan kullanıcılar uyarılmalı

# Ayarlar – III

- `/etc/login.defs`
  - Kullanıcı sisteme giriş yaptığında ayar kontrollerinin yapıldığı dosya
    - Fail_delay  hatalı kullanıcı adı/parola sonrasında beklenecek süre
    - Faillog_enable  hatalı kullanıcı adı/parola kayıtları
- `/etc/securetty`
  - Süper kullanıcının giriş yapma haklarının olduğu terminalleri belirler

# Ayarlar – IV

- `/etc/sudoers`
  - Süper kullanıcı haklarıyla hangi kullanıcıların hangi yazılımları çalıştırma hakkı olduğunu tanımlar
- `/etc/inetd.conf`
  - *inetd* servisi, gelen ağ bağlantılarında hangi programın çalıştırılacağını belirler
  - Kullanılmayacak olan bazı servisler buradan kapatılabilir
    - *finger, auth, ftp, telnet* vs...

# Ayarlar – V

- `/etc/inittab`
  - Çeşitli çalışma seviyelerinde neler yapılacağını
  - Tuş kombinasyonlarında (ctrl+alt+del) sistemin nasıl davranacağını belirler
  - `ca::ctrlaltdel:/sbin/shutdown -t5 -r now`

# Parola Güvenliği – I

- `/etc/passwd`
  - Kullanıcı bilgilerinin tutulduğu dosya
  - `root:x:0:0::/root:/bin/bash`
- `/etc/shadow`
  - Kullanıcı parolalarının şifrelenmiş olarak tutulduğu dosya
  - `root:$1$T261Nxxq$Xc12E0XaYD3X9fPN.T.H01:12011:0:::::`

# Parola Güvenliği – II

- Kullanıcıların “sağlam” parola seçmeleri sağlanmalı
  - Yardımcı programlar ile yapılabilir
    - Cracklib vb...

```
Changing password for korhan
Enter the new password (minimum of 5, maximum of 127 characters)
Please use a combination of upper and lower case letters and numbers.
New password:
Bad password: too short.
Warning: weak password (enter it again to use it anyway).
New password:
```

  - Kullanıcıların periyodik aralıklarla parolalarının değiştirilmesi sağlanmalı
    - Bu parola geçerlilik süresi ayarlanarak yapılabilir

# Dosya Sistemi Güvenliği – I

- Önemli dizinler farklı dosya sistemlerinde olmalıdır
  - Kota konulabilir
  - Sadece okunabilir şekilde bağlanabilir
  - Dolan bir dosya sistemi diğerini etkilemez
- Yapılandırma dosyalarının hakları kontrol edilmeli
- Sistemde SUID/SGID hiç bir program bulunmamalı
  - `find / -perm +2000`
  - `find / -perm +4000`
- Dosyalar düzenli olarak bütünlük koruma programları ile kontrol edilmeli

# Dosya Sistemi Güvenliği – II

- /etc/fstab

```
/          /dev/hda2   ext3  nosuid,rw          1 1
/usr       /dev/hda3   ext2  nosuid,noexec,ro   1 1
/var       /dev/hdb2   ext2  defaults           1 2
/tmp       /dev/hda4   ext2  defaults           1 2
/home      /dev/hdc2   ext3  grpquota           1 2
```

# FTP servisi

- `/etc/ftpusers`
  - Sisteme FTP erişim izni verilmeyen kullanıcı adlarını tutar
- `/etc/ftphosts`
  - Belirli kullanıcıların, belirli adreslerden sisteme giriş yapmasını engelleyen/izin veren dosyadır
  - `allow [kullanıcı_adı] [host] [host]`
  - `allow  korhan      dikey8.com`
  - `deny   burc        dikey8.com`
- FTP protokolünde bilgiler düz metin olarak gider gelir
- *root* olarak FTP yapmak sakıncalıdır
- Mümkünse yerine daha güvenli olan *sftp* hizmeti kullanılmalıdır

# SMTP servisi

- “Relay” e kapatılmalı
  - sendmail için, `/etc/mail` dosyası
    - `localhost RELAY`
    - `dikey8.com RELAY`
- EXPN ve VRFY komutları iptal edilmeli

# SSH servisi

- *telnet* yerine kullanılabilen, bağlantılarını şifreli olarak yapan bir uzaktan kabuk erişim protokolü ve protokol ile iletişim kuran yazılım seti
- `/etc/ssh/sshd_config`
  - Hangi kullanıcıların SSH ile bağlanabileceği belirtilmeli
    - `AllowUsers korhan burc`

# chroot

- Herhangi bir hizmet veya yazılım için kök dizini ayarlarının yapılmasını sağlar
  - Bu kök dizin dışındaki herşey sistemde mevcut değilmişcesine işlev sağlar
  - Eğer bir hizmet veya yazılımdaki zayıflık yoluyla sisteme erişim sağlanırsa erişim hizmetin kök dizini içinde kalacaktır.
- Verilen tüm hizmetler mümkün ölçülerde “chroot” edilmelidir

# Kayıt Tutma

- Kayıt üretecek her yazılım ve hizmet mümkün olduğu kadar fazla kayıt üretmeli
- Kayıt dosyalarının bütünlüğü sağlanmalı
  - Kayıtlar uzaktaki başka bir makina da tutulabilir (syslog-ng)
- Kayıt üreten sistemler arasında zaman senkronizasyonu sağlanmalı

# Yedekleme

- Ürettiğiniz ve yerine koymakta zorlanacağınız herşeyin yedeğini almalısınız.
  - Sunduğunuz hizmetlerin içerik yedekleri
- Sistem ayarlarının yedeklerini almanız bir hata telafisini hızlandıracaktır
- `/proc /mnt /tmp` gibi dizinlerin yedeklenmesine genelde gerek yoktur.

# Yedekleme – II

- Yedekleme tekniği geri dönülmek istenilen zaman geri dönmeye izin vermelidir.
  - Diğer yedeklerin üstüne alınan yedekleme mantığı geri dönüşe izin vermemektedir.
  - Belli zamanlarda tam yedekleme almak, daha sık olarak artan yedekleme yapmak uygun bir çözümdür
  - Yedeklerin fiziksel olarak güvenli bir ortamda sağlanması

# Referanslar

- Openwall Projesi
  - http://www.openwall.com/
- Linux Dökümantasyon Projesi
  - http://www.tldp.org/

# Soru – Cevap

# Teşekkürler

Teşekkürler...