Ege Üniversitesi
Network Güvenlik Grubu

LİNUX SİSTEM GÜVENLİĞİ RAPORU 2003

Bornova/ İZMİR, 2003

Bu Sürüm (Linux Sistem Güvenliği Raporu 2003 -v1.0)Hakkında

Hazırlayanlar:
Nazmiye Çınar, Mehmet Bıçak, 2003.
Ege Üniversitesi Network Yönetim Grubu'nda staj çalışması olarak hazırlandı.

Danışman:
Enis Karaaslan, Ege Üniversitesi Network Yönetim Grubu

Teşekkürler:
Dökümanın kontrolünde, düzeltmeler ve eklemelerinde yaptıkları katkılardan dolayı Ar. Gör. Mehmet Ersan Topaloğlu, Enis Akar, Sedat Kulduk'a teşekkürler.

İletişim:
Döküman hakkında yorum, düzeltme döndürmek; dökümana bilgi-bölüm eklemek için bizimle lütfen irtibata geçiniz. ***Email:*** security@nyg.ege.edu.tr

Ege Üniversitesi Network Güvenlik Grubu

İÇİNDEKİLER

1GİRİŞ

Oluşturulan bu dokümanın amacı Linux sisteminizi daha güvenli hale getirecek bilgiler sağlamaktır. Linux dünyadaki geliştiricilerin de yardımıyla Linus Torvalds tarafından yaratılan Unix türevi kaynak kodu açık, herkesin yararlanabileceği ücretsiz bir .işletim sistemidir.

Linux, kişisel bilgisayarlarda bir işletim sistemi olarak kullanılabileceği gibi, ağ üzerinde servis veren sunucular(server) olarak da hizmet verebilmektedir. Ağ (network), paylaşım amacıyla iki ya da daha fazla cihazın bir araya getirilmesiyle oluşturulan bir yapıdır. Bir ağla amaçlananlar bilgiye erişim, iletişim, kaynak paylaşımı, ölçeklenebilirlik, yüksek güvenilirlik, harcanacak paradan tasaruf olmaktadır.

İlk zamanlarda bilgisayar güvenliği denildiğinde akla gelen bilgisayarın fiziksel güvenliğiydi. Ancak ağ ve internet üzerinden iletişim yaygınlaştıkça ve daha önemli fonksiyonlar üstlendikçe ağ güvenliği kritik önem taşımaya başlamıştır.

Tedbir almadan bilgisayarlar sanal iletişimin bir parçası haline getirildiğinde, meraklı insanların veya hacker'ların paylaşımına sunulmuş olmaktadır. Bu kişiler kötü amaçlı ise bu tür bir nüfuz; veri kaybına, daha kotü durumlarda para,zaman ve prestij kaybına sebep olabilmektedir.

Unix/Linux sistemleri doğası ve yapısı gereği güvenli işletim sistemleri olarak bilinmektedir. Daha doğrusu Linux sistemler çeşitli basamaklar sonunda daha kolay bir şekilde güvenli hale getirilebilmektedir. Bu dokümanda Linux sistemlerin nasıl daha güvenli hale getirilebileceği konusunda okuyucuya yardımcı olunmaya çalışılacaktır.

2 FİZİKSEL GÜVENLİK

Fiziksel güvenlik önlemleri, doğal afetlerin, fiziksel hırsızlığın, art niyetli kişilerin, böceklerin verebileceği zararları engellemeye çalışır. Eğer bir laboratuvardaysanız veya bir şirkette çalışıyorsanız fiziksel güvenlik ayrı bir önem taşır. Bazı işyerlerinde bilgisayarların fiziksel saldırıya açık halde bırakılması kovulma sebebi olabilir. Linux'u fiziksel saldırılara karşı güvenli hale getirmek için yapılabilecekler aşağıda açıklanmıştır.

2.1BİOS GÜVENLİĞİ

Linux yükleyicileri(Linux loader), sistemin nasıl açılacağını anlamak için Bios'a ulaşır. (Bios, donanımınızı yönlendiren ve ayarlarını yapan en alt düzey yazılımdır.) Bios default olarak önce A sonra C yerine önce C'den daha sonra A'dan boot edecek şekilde ayarlamalıdır. Disketten boot etme ihtiyacı duyulduğunda bu düzenleme değiştirilebilir. Ancak daha sonra yine eski haline getirilmelidir.

Saldırganlar, Bios'a erişip bios ayarlarını değiştirerek yeniden sistemin disketten başlatılmasını engellemek için Bios'un değiştirilmesi engellenmelidir. Bu durumu Bios açılırken şifre sorgulanması yaparak engelleyebiliriz. Aslında bu da okadar da güvenlik sağlamaz. Çünkü saldırgan biosu söküp taktığında bios sıfırlanacaktır ve şifre sorgulaması ortadan kalkacaktır. Ancak şifre sorgulaması, caydırıcılık açısından önemlidir.(biosun sökülüp takolması zaman alacak ve saldırgan muhtemelen iz bırakacaktır)

2.2SİSTEM YÜKLEYİCİ GÜVENLİĞİ(lilo güvenliği)

Lilo(**li**nux **lo**ader), linuxlar için sistem yükleyicisidir. Bazı linux dağıtımlarında, saldırgan lilo promptuna aşağıdaki komutu yazdıktan sonra root olarak sisteme ulaşabilir. Bu komutlar linux'u tek kullanıcı moduna (single-user mode) dönüştürür.

```
LILO: linux single
LILO: linux 1
```

Aşağıdaki işlemler yapılarak bu olay engellenebilir.

1. Boot scriptini değiştirerek, kabuk(shell) açılırken sulogin programının çalıştırılarak şifre sorgulanmasının yapılması sağlanmalıdır.
2. `/etc/lilo.conf` değiştirilerek Lilo şifrelenmesi sağlanmalıdır. Bunuyapmak için

```
PASSWORD=<password>
    RESTRICTED
```

satırları lilo.conf a eklenmelidir.

2.3BİLGİSAYAR KİLİTLERİ

Yukarıda yaptığımız herşey bilgisayarın harddiskinin veya kendisinin çalınması durumunda hiçbir işe yaramayacaktır. Bu nedenle bilgisayarların çalınmasına karşı çeşitli önlemlerin(kilitler..vb.) alınması gerekir.

3 SİSTEM GÜVENLİĞİ

Unix/Linux sistemleri daha güvenli hale getirme konusunda bu başlık altında sistemi oluşturan temel alt sistemlerin güvenliği ele alınacaktır. Bu sistemler;

- Kullancı güvenliği
- Dosya sistemi güvenliği ve dosya izinleri
- Şifre seçimi ve şifre dosyalarının güvenliği
- Servis güvenliği
- Çekirdek güvenliği
- Paket yönetim sistemleri
- Dosya kayıt güvenliği

olarak adlandırılabilir.

3.1KULLANICI GÜVENLİĞİ

Linux sistemleri güvenli hale getirmede düşünülmesi gereken ilk etap ağ içerisindeki yerel kullanıcılara karşı önlem almaktır. Saldırganların ilk isteyeceği şey root hesabına ulaşmak olacaktır çünkü root daha geniş haklara sahiptir ve de şüphesiz yerel kullanıcılar buna en yakın kişiler. O halde;

- Kullanıcılara yeni hesap açarken onlara gerekli olan kadar, minimum imtiyaz hakkı verilmeli.

- Ne zaman login, log-off olduklarını belirleyen kayıtlar mutlaka tutulmalı.

- Aktif olmayan hesaplar silinmeli(Bunu log dosyalarını kontrol ederek görebilirsiniz).

Ayrıca root hesabı adına da dikkat edilmesi gereken bazı hususlar vardır;

- Root olarak giriş izni çok fazla kullanıcıya verilmemelidir. Her kullanıcının root un ulaşabileceği bir çok veriye ulaşmasına gerek yoktur. Aksi taktirde sistem kontrolü oldukça zorlaşır.

- Root olarak rlogin/rsh/rexec (r-utilities) kullanılmamalı. Kesinlikle .rhosts dosyası yaratılmamalıdır.

3.2DOSYA SİSTEMİ GÜVENLİĞİ

Bilindiği üzere Linux çok kullanıcılı(multi-user) işletim sistemidir ve bu da kullanıcıların hesap güvenliğinin sağlanmasını gerektirir. Bunun için Linux ta dosya izin sistemi(file permission system) geliştirilmiştir.Dosya güvenliği için aşağıdakiler yapılmalıdır [2], [3], [7].

- Her kullanıcı home directory iznini 700 yapmalı ve de dosya ilk oluşturulurken 077 izniyle oluşturmalıdır(creation mask).

- Set User-ID (setuid) / Set Group-ID (setgid): Setuid veya setgid bitiyle oluşturulan her dosya grubunun ya da sahibinin izinleri altında herhangi biri tarafından çalıştırılabilir. Bunu bir düşünürsek herhangi biri root un sahip olduğu setuid dosyasını çalıştırdığı süre içerisinde root haklarına sahip olur. O halde bu bitleri sahip olması gerekmeyen programlardan kaldırmak, en son versiyon SUID/SGID programlarını yüklemek ve bunlara ek olarak /etc/fstab partition ı default değil de nosuid olmasını sağlamak alınabilecek önemli tedbirlerdir. Bu konuda dikkatli olunmalı çünkü root/SUID programlar sistemlerde saldırganlar tarafından kullanılan en yaygın açıklardan biridir.

Setuid/setgid programlar aşağıdaki komutla bulunabilir ve chmodla değiştirilebilir:

/* /usr/bin/find / -user root -perm -4000 -o -perm -2000 */

```
root# find / -type f -perm +6000 -ls
59520 30 -rwsr-xr-x 1 root root 30560 Apr 15 1999 /usr/bin/chage
59560 16 -r-sr-sr-x 1 root lp 15816 Jan 6 2000 /usr/bin/lpq

root# chmod -s /usr/bin/chage /usr/bin/lpq
root# ls -l /usr/bin/lpq /usr/bin/chage
-rwxr-xr-x 1 root root 30560 Apr 15 1999 /usr/bin/chage
-r-xr-xr-x 1 root lp 15816 Jan 6 2000 /usr/bin/lpq
```

- Herhangi bir sahibi olmayan ya da bir gruba ait olmayan dosyaları belirlemek gerekir. Bu tip dosyalar bir saldırganın sisteme girdiğinin işareti olabilir. Sahipsiz dosyalar şu şekilde belirlenebilir;

```
root# find / -nouser –o –nogroup
```

- Eğer NFS(Network FileSystem) sunucusu kullanılıyorsa /etc/exports şekillendirirken mümkün olduğu kadar erişim kısıtlanmalıdır. Root a write izni verilmemeli, sadece read izni verilmelidir.

- cahttr komutunu (immutable bit) kullanarak dosyaların silinmesi ,değiştirilmesi kontrol edilebilir. Hemen aşağıda kullanıma bir örnek verilmiştir;

```
#chattr +i /bin/login    (login dosyasında artık değişiklik
yapılamaz)
#chattr +a /bin/messages   (messages dosyası artık silinemez)
```

Önemli sistem dosyaları ve erişim hakları EK-1'de olduğu gibi düzenlenebilir. [2]

3.3 ŞİFRE(PASSWORD) GÜVENLİĞİ

Günümüzde kullanılan en önemli güvenlik özelliklerinden biri de şifrelerdir. Kullanıcıların, saldırgan tarafından tahmin edilmesi güç, kendisi tarafından

hatırlamasının kolay ve güvenli şifreler belirlemeleri gerekmektedir. Sistemde /etc/login.defs konfigürasyon dosyasından kullanıcı şifrelerinin karakter yapısı güvenli bir biçimde ayarlanmalıdır. Ayrıca passwd programlarımız güncel ve şifre seçimlerimizi uygun bir şekilde denetleyen programlar olmalıdır. İyi şifreler aşağıdaki özelliklere sahiptir;

- Büyük ve küçük harf içerirler
- Noktalama işaretleri ve rakamlar içerirler
- Bazı kontrol karakterleri ve/veya boşluklar içerirler
- Kolaylıkla hatırlanabilirler ve bu nedenle bir yere not edilme ihtiyacı duymazlar
- En az sekiz karakter uzunluğundadırlar.
- Kolay ve hızlı yazılırlar ve böylece etraftan bakan birisi ne yazdığını anlayamaz.

Linux sistemleri şifreleri DES (Data Encryption Standard) algoritmasıyla şifreler ve /etc/passwd dosyasında bazen de /etc/shadow dosyasında saklarlar. Bu tek yönlü bir algoritmadır. Böylece geri şifreleme söz konusu olmaz ve de şifreniz deşifre edilmez. Sisteme girildiğinde şifreniz dosyadakiyle karsılaştırılıp kontrol edilir.

Ancak saldırganlar boş durmayıp , sürekli açık aramaktadırlar. Eğer şifreler "kötü" seçildiyse "Crack" ve "John the Ripper" gibi programlar kullanarak kolayca deşifre edebilirler. Genelde bu tip programlar olabilecek bütün şifreleri deneyerek amaçlarına ulaşırlar. Ancak sistem yöneticileri ya da kullanıcılar bu programları kendi yararlarına kullanabilir. Kendi ağınızda kullanıcılarınızın şifrelerinin ne kadar güvenli olduğunu test etmek bu programlarla oldukça kolaylaşır. Bu arada kullanılmayan hesapları /usr/bin/passwd –l komutuyla kullanılmaz hale getirmek de alınabilecek önlemlerden biridir.

3.4GEREKSİZ SERVİSLERİN KAPATILMASI

Herhangi bir saldırıdan korunmanın en etkili yolu gereksiz servisleri ve programları kaldırmaktır. Herhangi bir ağa bağlanmadan önce hangi servislerin gerekli olduğuna karar vermeli ve gereksiz programlar kaldırılmalıdır. Peki gereksiz servisleri kaldırmak niçin bu kadar önemlidir? Çünkü var olan her servis, dışarıdan bizim bilgisayarımıza saldırmak isteyen kişiler için potansiyel bir açıktır ve bu açık kullanılarak dışarıdan bizim bilgisayarımıza bağlanılabilir.

Servisleri kapatmanın birkaç yolu vardır. Şimdi bunlara kısaca değinelim.[2]

- /etc/inetd.conf dosyasına bakarak inetd tarafından hangi servislerin sunulduğunu görmek mümkündür. Bu servislerden gereksiz olanların başına # işareti konularak bu servis pasif hale getirilebilir.Bu durumda iken bir SIGHUP komutu gönderilerek inetd.conf dosyasını update edilebilir. Bu aşağıdaki gibi yapılabilir:

  1)`root> chmod 600 /etc/inetd.conf` komutuyla sadece root'un bu dosyayı okuyabilmesi ve yazabilmesi sağlanır.

  2)Gerekli değişiklikler yapıldıktan sonra ftp, telnet, shell, login, exec, talk, ntalk, imap, pop-2, pop-3, finger gibi servisleri pasif hale getirilebilir (kullanmadığımız sürece).

3)`root>killall -HUP inetd` komutuyla inetd ye sinyal gönderilebilir.

4)`chattr +i /etc/inetd.conf` komutunu kullanarak birilerinin inetd.conf dosyasını değiştirmesi engellenebilir.

- /etc/rc*.d ve /etc/rc.d/rc* başlangıç dizinlerini kontrol eder ve herhangi bir sunucunun çalıştırılıp çalıştırılmadığını gösterir. Gereksiz servisler isimleri değiştirilerek veya /sbin/chconfig –del komutu kullanılarak etkisiz hale getirilebilir.

3.5ÇEKİRDEK (KERNEL) GÜVENLİĞİ

Unix işletim sistemleri 4 ana parçadan bir diğer deyişle katmandan oluşur. En dıştaki katman bilgisayara ne yapması gerektiğini söylediğimiz komut katmanıdır. Daha sonra dosya sistem katmanı gelir ki bu da bilgisayarın hard disklerindeki bilgileri organize etmek adına olan işleri yapar. Shell katmanı kullanıcı ile bilgisayar arasındaki iletişimi sağlayan katmandır. Ve son olarak ise en içteki çekirdek gelir. Çekirdek bilgisayarın çalışmasını sağlayan en temel, öz işletim sistemidir. İşlemciye ve de donanıma en yakın kısımdır. Bilgisayar çalıştırıldığında yüklenen çalıştırılabilir (executable) bir dosyadır. Çekirdek yüklendikten sonra sistem programlarıyla sistem donanımı arasındaki, bilgisayarla bağlantılı çeşitli aletlerin yönetimi, hafıza, işlemler ve bilgi iletişimi gibi işleri kontrol eder.

Görüldüğü üzere çekirdek bu kadar temel bir yapı olduğundan güvenliğinin sağlanması da oldukça büyük önem teşkil ediyor. Güvenlik sağlamak amacıyla çeşitli çekirdek şekillendirme opsiyonları /proc pseudo-filesystem altında bulunur. /proc/sys direkt olarak güvenlikle ilgili dosyalar içerir. Red Hat Linux lardaki /etc/sysctl.conf dosyası birkaç default özellikleri taşımaktadır, /sbin/sysctl programı ise bu değişkenleri kontrol etmek için kullanılmaktadır. Bu seçenekleri şekillendirmek için /bin/echo da kullanılabilir. Örnekleri aşağıda görmek mümkündür [1], [2].

2.0 çekirdekler için yapılabilecek birkaç şey;

- IP yönlendirme (CONFIG_IP_FORWARD) : Eğer bu opsiyon açık olursa Linux kutusu bir yönlendirici haline gelir. Şu komut kullanılarak bu opsiyon açılabilir;

```
root#  echo 1 > /proc/sys/net/ipv4/ip_forward
```

Veya şu komutla da kapatılabilir;

```
root#  echo 0 > /proc/sys/net/ipv4/ip_forward
```

- IP syn cookies (CONFIG_SYN_COOKIES) : SYN saldırısı makinedeki tüm kaynakları tüketen bir servis reddi saldırısıdır. Bu seçeneğin açık olması gerekir. Bu işlem şu komutla yapılabilir;

```
root# echo echo 1 > /proc/sys/net/ipv4/tcp_syncookies
```

- IP ateşduvarı (CONFIG_IP_FIREWALL) : Makine eğer bir ateş duvarı olarak yapılandırılacaksa veya maskeleme yapılacaksa bu seçenek açılmalıdır.

2.2 çekirdekler için yapılabilecek birkaç şey;

- Bu seçeneklerin çoğu yukarıdaki seçeneklerle aynı ancak birkaç değişiklik mevcut. En önemlisi ise IP ateşduvarı kodu.2.0 daki ipfwadm programı yerine burada ipchains programı kullanılıyor. Ek olarak bu çekirdeklerde CONFIG_FILTER seçeneğine hayır demek birçok kullanıcı için güvenli olacaktır.

Daha fazla seçenek özellikleri ve ayrıntılı bilgi için www.linuxsecurity.com/docs adresindeki kernel güvenliği ile ilgili dokümanları incelemek faydalı olacaktır.

3.6PAKET YÖNETİM SİSTEMLERİ

Paket yönetim sistemleri tüm dosya türlerini (programlar, veriler, belgeler, yapılandırma dosyaları, vb.) özel olarak biçimlendirilmiş, paket adı verilen tek bir dosyada saklarlar. Paket içindeki tüm dosyalar yüklenecek yazılıma aittir ve yüklenen paketler veri tabanında tutulur. Paket yüklenmeden önce paketin sisteme hangi dosyaları ekleyeceğini, ne gibi değişiklikler yapacağını ve de kullanıcıya neler sağlayacağını görmek mümkün olur. Bu programlar, program kurma, kaldırma, güncelleştirme ve tekrar derleme gibi işlevler için kullanılır.

Rpm, RedHat ve türevleri, Dpkg ise Debian ve türevleri için paket yöneticiliği yapan programlardır. Bu programların yukarıda saydığımız özellikleri sistem güvenliğini sağlamada ayrı bir yarar sağlar.[10], [18]

Şimdi bazı önemli komutlara göz atalım.[2]

- #rpm -e <paket ismi>

```
#dpkg -r <paket ismi>
```

komutları paketi kaldırmak için kullanılır.

- #rpm –Uvh <paket ismi.rpm>

```
#dpkg -i        <paket  ismi.deb>
```

komutları yeni paket kurmak için kullanlır.

- #rpm –qvl <paket ismi.rpm>

```
#dpkg -c    <paket ismi.deb>
```

komuları paketin tüm içeriğini görmek için kullanılır.

- #rpm –qvia

```
#dpkg -l
```

komutları kurulmuş paketler hakkında bilgi verir.

- #rpm –Va
  ```
  #debsums -a
  ```

  komutları paketin karakteristik özelliklerini doğrulamak için kullanılır.(basic integrity check)

- #rpm –qf <dosya ismi(absolute-path olarak)>
  ```
  #dpkg -S <dosya ismi(absolute-path olarak)>
  ```

  komutları dosyanın hangi pakete ait olduğunu gösterir.

3.7DOSYA KAYIT GÜVENLİĞİ

Syslogd, sistemle ilgili çeşitli işlevlerin(system processes), klogd ise çekirdek(kernel) ile ilgili çeşitli işlevlerin kaydını tutar. Kayıt alınan dosyalara örnek olarak sistemde dolaşan e-maillerin kayıtlı tutulduğu dosya, apache web sunucusunun kayıtlarının bulunduğu dosya ve güvenlik kayıtlarının bulunduğu dosyayı vermek mümkündür. Syslog genellikle sistemdeki potensiyel problemlerin göstericisi olarak kullanılır. [11]

Güvenlik açısından dikkat etmemiz gereken kurallar vardır. Bunlar:[2]

- /etc/syslog.conf dosyasının default değerleri iyi ayarlanmalıdır. Böylece daha kolay ve iyi analiz yapmak mümkün olur.
  ```
  #şifre onaylama(authentication) girişimini gösterme
    auth.* ; authpriv.*          /var/log/authlog
  #çekirdek mesajlarını göster
    kern.*                       /var/log/kernlog

   #uyarı ve hata mesajlarını göster
    *.warn ;  *.err              /var/log/syslog
  ```
- log dizinine ve syslog dosyalarına erişim kısıtlanmalıdır.Bunu yapmak için:
  ```
  chmod 751  /var/log/etc/logrotate.d
  chmod 640  /etc/syslog.conf/etc/logrotate.conf
  chmod 640  /var/log/*log
  ```

  komutları kullanılmalıdır.

3.8Yama (Patch) Yüklenmesi

Saldırganlar her geçen gün yepyeni sistem açıklarını tespit etmekte ve yenileri için çalışmaktadırlar. Bu sebeple savunma ve güvenlik önlemleri de artmaktadır. Bunlardan biri de yama(Patch) dediğimiz kullanılan programların yenilenmiş versiyonlarının yüklenmesidir. Örneğin; Red Hat Linux ta AutoRPM, Debian da apt-get yenilenme olan paketleri yüklemede ve kurmada kullanılan programlardır.

3.9Yedekleme

Bazen çeşitli nedenlerden dolayı önemli verilerin kaybı olabilir. Bu kayıpları önemli dizinleri yedeklerini alarak telafi etmek mümkün olabilir. Kolaylık sağlaması açısından yedeği alınması gereken önemli dizinlerin altında gereksiz programlar(internette kopyası olabilecek veriler), resimler olmamalıdır.Yedek aldığımız dizinlerle yedek dizinimizin ayrı bölmelerde olması, bölmelerden herhangi birindeki bozulma karşısında diğer bölmedeki kopyasını kaybetmemiş oluruz. Öncelikle /etc ve /root'u en başta yedeklemekte fayda vardır eğer bunlar dışında diğer önemli dosyalarımız da varsa bunları da ekleyip [19] daki scriptle yedeklerini almak mümkün olacaktır.

3.10Web Kaynaklarını Takip Etmek

Her geçen gün, Linux ve diğer sistemlere yönelik çeşitli saldırılar ve bu saldırılara karşı savunma yöntemleri ortaya çıkmaktadır. Bu tür bilgiler sistem yöneticisi tarafından takip edilmelidir. Kullanılabilecek web kaynakları için EK-2'ye göz atabilirsiniz. Bu siteler 2003 Temmuz ayında derlenmiştir, her geçen gün yenilerinin eklendiği veya var olanların kapanabileceği göz önünde tutulmalıdır.

4SUNULAN SERVİSLERİN GÜVENLİĞİ

Sistemlere yapılan önemli saldırıların bir nedeni de sunulan servislerdeki çeşitli açıklardır. Bu servislerden ele alınacak olanlar şunlardır;

- Web güvenliği
- DNS güvenliği
- Telnet/SSH

4.1WEB GÜVENLİĞİ

Apache şu an dünyada bulunan en popüler web sunucu yazılımıdır. Apache de işler önceden hazır olan modüller sayesinde yapılır. Ayrıca ücretsiz ve kaynak kodu açıktır. Yani istenilen modül yoksa kullanıcı kendi modülünü geliştirebilir. Apache'yi download etmek için (www.apache.org/dist/) sitesine göz atılabilir .

Apache'nin config dosyası /etc/httpd dosyasıdır. Bu dosyanın oluşumunda birçok seçenek vardır. Bunlardan biri de kullanıcılara verilecek olan haklardır. Teknik olarak güvenliği sağlamak için yapılabilecek en iyi şey kullanıcılara minimum hakkın verilmesidir. Kullanıcıya güvenli bir şifre sağlanmalı ve sisteme minimum erişim hakkı verilmelidir.[11]

Dokümanlara ulaşmayı sınırlaması için kullanıcılara bir şifre ve kullanıcı ismi verilerek her isteyenin istediği dokümana ulaşması engellenebilir. Böylece dokümana ulaşım kontrol altına alınmış olur. Öncelikle kullanıcılar için bir database oluşturulması gerekecektir.Yeni kullanıcılar eklemek ve varolanlarda değişiklik yapmak için htpasswd programına ihtiyaç duyulacaktır. Eğer bu dosya daha önce derlenmemişse;

```
make htpasswd
```

komutu çalıştırılmalıdır.

Eğer mehmet_nazmiye kullanıcı isimli birisi database'e girilecekse;

```
htpasswd -cm  etc/httpd/conf/private_users mehmet_nazmiye
```

komutu kullanılabilir.Daha sonra şifre istenecek ve ekleme işi tamamlanacaktır. Güvenlik nedeniyle oluşturulan şifre dosyasının root'un altında olmamasına dikkat edilmelidir. Çünkü bu dosyanın buradan download edilmesine sebep olabilir.

Listen ip-adres: port_number komutuyla web sunucusunun(server) hangi adres ve porttaki isteklere yanıt vereceği belirlenebilir. Örneğin, Apache'nin sadece yerel isteklere cevap vermesi için /etc/httpd/conf/httpd.conf dosyasında değişiklik yaparak aşağıdaki komutu okuması sağlanabilir :[2]

```
Listen 127.0.0.1:80
```

Default olarak tüm dosya sistemine erişimi engellemek için aşağıdaki komutlar kullanılmalıdır.[2]

```
<Directory />
Options None
AllowOwerride None
Order deny,allow
Deny from all
```

```
<Directory />
```

/etc/httpd/conf/access.conf dosyası içerisindeki sınırlı sayıda adresi kullanarak server erişiminin kontrolü sağlanabilir.Bunu gerçekleştirmek için aşağıdaki komutlar kullanılır.[2]

```
<Directory /home /httpd /html>
#default olarak tüm erişimleri kapat
Order deny,allow
#yerel makineden erişimi sağla
Allow from 127.0.0.1
#tüm yerel ağdan erişimi sağla
Allow from 192.168.1
#sadece uzaktaki bir bilgisayardan erişimi sağla
Allow from 192.168.5.3
</Directory>
```

/etc/httpd/conf/access.conf dosyasındaki bir bilgiye erişim yapılacağı zaman şifre sorgulamasının yapılması için :[2]

```
<Directory /home/httpd/html/protected>
Order deny,allow
Deny from all
Allow from 192.168.1.11
AuthName "Private information"
AuthType Basic
AuthUserFile etc/httpd/conf/private-users
AuthGroupFile  etc/httpd/conf/private-groups
Require group <group-name(grupismi)>
</Directory>
```

komutları kullanılmalıdır.

4.2DNS GÜVENLİĞİ

DNS, host isimlerini(www.mehmet_nazmiye.com) ip adresine(152.302.1.1) çeviren sistemdir. DNS(Domain name server), dünyanın çeşitli yerlerindeki sunucuların oluşturduğu ağdır(network) da diyebiliriz. Tüm bilgiler sadece bir database'de saklanmaz. Bilgiler dünyaya yayılmış olan sunuculara dağıtılmıştır.

DNS'lerin güvenliği yeterince sağlanmazsa, izni olmayan bazı kişiler DNS database'ine girebilir ve bunu kötü amaçlar için kullanabilir. Mesela, www.xbank.com adresini girdiğiniz zaman size farklı bir ip adresi vererek yanlış yere yönlendirebilir ve bu arada siz şifrenizi girerken şifrenizi alarak kötü amaçlar için kullanabilir.Görüldüğü gibi DNS güvenliğinin sağlanmaması çok ciddi sorunlara sebep olabilir.

Şimdi DNS güvenliğinin sağlanmasında dikkat edilecek birkaç hususdan bahsedelim.[2]

- Yerel sunuculardaki(slave server) zone(bir kısım database) bilgilerinin güncellenmesi sadece ana sunucu(master server) tarafından yapılmalıdır. Böyle yapılmaması izni olmayan kişilerin host isimlerine ve ip numaralarına ulaşmasına sebep olabilir.

- Bind'in versiyonunun belirlenmesi engellenmelidir. Bind versiyonunun belirlenmesi saldırganın o versiyondaki açıkları kullanmasını sağlayabilir ve saldırgan kolayca sisteme girebilir.
- Bind'ı normal bir kullanıcı çalıştıracak şekilde şekillendirmek gerekir. Bind başladıktan sonra kolayca kendi yapması gerekenin dışında bazı uygulamaları gerçekleştirebilir ve root yerine normal bir kullanıcı olarak çalışabilir.
- Erişim kontrol listesini kullanarak kullanıcıları farklı güvenilirlik gruplarına ayırmak gerekir.

4.3Telnet / SSH

SSH, telnetin, güvenli veri akışı sağlayan halidir. Telnet , veri iletimini açık metin olarak yapar. Açık metin parolalar saldırılara karşı savunmasızdır. SSH, veri iletimini(bağlantı kurulurken ve kurulduktan sonra) şifreli olarak gerçekleştirir.Varolan en iyi ücretsiz güvenlik sağlayıcıları arasında gösterilir.

Şimdi de onun kurulumunda nelere dikkat edilmesi gerektiğine bakalım.[2]

1)SSH paketleri yüklenmeli.
2)SSH, publickey şifrelemesini kullanır. Publickey(hem host hem de uzaktaki sistem tarafından bilinir) ve privatekey(sadece host tarafından bilinir) oluşumu sağlanmalı.
3)Publickey uzaktaki sisteme gönderilmeli(kopyalanmalı).
4)Uzaktaki sisteme login olunmalı.

Daha fazla bilgi için www.linuxsecurity.com ve http://www.linux-mag.com/2001-11/bind9_01.html adreslerini ziyaret edebilirsiniz.

5VİRÜSLER VE İLGİLİ TEHLİKELER

Şu anda kötü amaçlar için yazılmış birçok program vardır. Bunları iki gruba ayırmak mümkündür. Bunlar, host programa ihtiyaç duyanlar ve bağımsız olanlardır. Bunlardan ilki bazı programların arkasına saklanırlar ve sisteme zarar verirler. Trapdoors, truva atları, bombalar ve virüsler örnek olarak verilebilir.Bağımsız olanlar ise herhangi bir programa bağlı kalmadan çalıştırılabilirler. Örnek olarak, bakteriler ve solucanlar verilebilir. [14]

5.1HOST PROGRAMLARA İHTİYAÇ DUYAN TEHLİKELER:

Tehlike olarak aşağıdakileri saymak mümkündür:

- TRAP DOORS: Trap doors lar program içinde saklanırlar. Trap door'un varlığından haberdar olan biri genel güvenlik önlemlerine takılmadan erişim hakkı kazanabilir. Linux ve diğer işletim sistemlerinin trap doorlara karşı önlem alması çok zordur. Trap door'u tespit etmek ve saldırıyı engellemek için programların gelişimi çok iyi takip edilmelidir. [14]
- TRUVA ATLARI(TROJAN HORSES): Truva atları faydalı bir program gibi gözükür. Bunlar bazı gizli kodlar içerir. Bu programlar çalıştırıldığı zaman sisteme zarar verecek işler yürütürler. Truva atları, sisteme dolaylı olarak da zarar verebilirler. Örneğin erişilemeyen bir dosyanın izinlerini Truva atları kullanarak kaldırabilir ve o dosyalara ulaşılabilir. Saptanması çok zor olan bir diğer truva atı da derleyicilerin(compiler) çalıştığı zaman yeni bilgileri bazı yerlere aktarmalarıdır. Eğer sistem login(giriş) dosyasına yeni bir kullanıcı hesabı açılabilir ve daha kötüsü bu kullanıcı haftalarca tespit edilemeyebilir. Truva atları bilgilerin yok edilmesine de neden olabilir. Bunlar faydalı bir işlev yapıyorlarmış gibi görünürken, aynı zamanda da dosyaları silebilirler. Bu nedenle asla bilinmeyen, kaynak kodu belli olmayan ikili(binary) dosya root olarak çalıştırılmamalıdır [14]. Sonuç olarak, Linux'ta Truva atlarına sık sık rastlanır ve bunlar sistem için çok zararlı olabilirler.
- BOMBALAR: Bombalar, herhangi bir programın içerisine bazı kişiler tarafından yerleştirilir ve bazı şartların sağlanması durumunda patlayarak sisteme zarar verirler. Bu şartlara örnek olarak haftanın özel bir günü, bilgisayar kullanan kişi verilebilir. Bombalar, tüm dosyaları ve bilgileri silebilir, sistemi göçertebilir veya başka şekilde zarar verebilirler. Bazı satıcılar, müşteriye sistemi kurarken ödeme tarihinde patlayacak şekilde bomba ayarlayabilirler ve ödeme günü geldiğinde para ödenmediği takdirde bu bombalarla karşılaşmak mümkün olur. [14]
- VİRÜSLER: Virüs inaktif halde bulunan diğer programları etkileyen bir programdır ve derlendiği takdirde zarar verici olur, onun dışında potansiyel risk durumunda, ancak zararsız bir şekilde bulunur. En basit haliyle virüs, bir uygulamayı yada programı başlatırken fazladan çalıştırılacak kod parçasıdır. Bu zaman içerisinde derlenebilir(executable) kod kısmını diğer dosyalara kopyalayarak yayılır, hedef dosyaları tarayarak amacına ulaşır ve genellikle asıl programı değiştirmeden programdan ayrılır. Çok çeşitli virüs tipleri vardır.Şimdi kısaca bunlara değinelim.

  Boot virüsleri derlenebilir kod parçalarını disk sektörlerine yerleştirirler ve bilgisayar başlatılırken bu virüsler de otomatik olarak çalışmaya başlarlar.

Yüklenmeyi bitiren virüs ardından makinenin normal bir şekilde başlıyormuş gibi görünmesini sağlamak için çeşitli önlemler alır. Dosya virüsleri program dosyaları içine yerleşirler ve virüslü program çalıştığında onlar da çalışırlar. Hemen arkasından orijinal program çalıştırılır ve de oluşan anormalliğin kullanıcının dikkatinden kaçması sağlanır. Bunlar dışında makro virüsler, script virüsler ve de işletim sisteminin özelliklerinden yararlanan companion virüsleri de sayabiliriz.[15]

Yaygın bir fikir var ki bu da virüslerin Linux işletim sistemi altında etkin olamayacağıdır. Ancak bu pek doğru değil, Linux da derlenebilen ELF dosyalarına ulaşan bir virüs kolaylıkla etkili olabilir ama bir yandan Linux altında bir virüsün yayılmak için yararlı bir yer bulamayacağı da ayrı bir gerçektir.Yazma haklarına sahip olan kullanıcının dosyayı nerede çalıştırdığına bağlı olarak sadece bozuk bir uygulama dosyalara yayılabilir. Deneyimli bir sistem yöneticisi sadece gerçekten ayrıcalık gerektiren zamanlarda root olarak bağlanacaktır ve normal bir kullanıcı da bu tarz bozuk dosyaları çalıştırdığında virüs yalnızca o kullanıcıya ait dosyalarda etkin olabilecektir. Linux altındaki virüsler yukarıda da bahsettiğimiz gibi sistem dizinlerindeki ELF dosyalarını bozarlar. Örneğin; Linux.Jac.8759 virüsü çalıştırıldığında, bulunduğu dizinlerdeki çalıştırılabilir dosyalara yazabilme izni olup olmadığını kontrol eder ve bulduğu dosyalara sinmeye çalışır.

Tabiiki başa gelecek kötü durumlardan kaçınmak için "AntiVir" http://www.hbedv.com/, "Shopes" http://www.sophos.com/, "InterScan VirüsWall" http://www.antivirus.com/products/isvw/. gibi anti-virus programlarıda kullanılabilir.

Sonuç olarak düşünülenin aksine Linux sistemler de virüslerden zarar görebilirler. Bu sebeple kullanıcılar güvenli bir sistem için yazılımları mümkün olan en kısa sürede güncellemek, sadece gerekli ağ servislerini kullanmak, uygulamaları güvenilir sitelerden indirmeye çalışmak, indirilen paketlerin PGP yada MD5 yeterliliğinin olmasına dikkat etmek durumundadır.

5.2HOST PROGRAMA İHTİYAÇ DUYMAYAN TEHLİKELER

Tehlike olarak aşağıdakileri saymak mümkündür:

- SOLUCANLAR: Network solucan programları network bağlantıları aracılığıyla bilgisayardan bilgisayara atlarlar. Sistem içerisinde aktif duruma geldikten sonra solucanlar virüs veya bakteri gibi davranabilir veya truva atlarını aktif hale getirerek sisteme zarar verebilir. Solucanlar, elektronik mail veya uzaktan login olup, komutları kullanarak kendisini kopyalayabilir. Sisteme bulaştıktan sonra solucanlar virüslerle aynı işi yaparlar. Bunlar ayrıca hangi sistemlerin enfekte olup hangi sistemlerin olmadığını anlayabilirler. Sisteme bulaştıktan sonra virüslerle ve solucanlarla başa çıkmak güçtür. Bu nedenle de sistemi daha güvenli hale getirerek onların sisteme bulaşma ihtimalini en aza indirmek gerekir. [14]

- BAKTERİLER: Bakteriler direk olrak dosyalara veya sistemlere zarar vermezler. Bunların yaptığı tek şey sürekli olarak kendilerini kopyalamalarıdır. Bakteriler sürekli olarak ürerler ve sistemin CPU'sunu, hafızasını(memory) ve disk alanını(disk-space) işgal ederek bilgisayarın kullanıcıya vakit ve yer ayırmasını engeller. [14]

6ARAÇLARLA KONTROL

Unix/Linux işletim sistemlerini daha güvenli hale getirmek için çok sayıda ücretsiz yazılım aracı bulunmaktadır. Bu dökümanda başlıca ele alacağımız araçlar şunlardır:

- PAM
- TCP Wrapper
- Bastille-Linux
- SNORT
- Firewall/filter
- Tripwire
- Nmap

6.1PAM *(Pluggable Authentication Modules)*

PAM (Pluggable Authentication Modules) kullanarak, kullanıcıların servis bazlı erişimi denetlenebilir. Her şey, servislerin yapılandırım dosyalarının bulunduğu ve genelde /etc/pam.d olan dizinden denetlenmektedir. Ftp, login, xdm vs gibi birçok servis pam ile denetlenebilir. Dolayısıyla, sistem yöneticisi kimin neye hakkı olması gerektiğini denetleme imkanına sahip olmaktadır [16]. http://www.kernel.org/pub/linux/libs/pam/ adresinden bu modül elde edilebilir. Detaylı bilgi için bakınız [17].

6.2TCP ÖRTÜCÜLER(TCP WRAPPERS)

TCPWrapper, hemen hemen her Unix işletim sisteminde vardır. Bu program aracılığıyla sistemde kurulu servislere olan erişim bilgisayar bazında denetlenebilmektedir. TCPWrapper iki farklı şekilde yapılandırılabilir: ya servisleri taşıyarak yada /etc/inetd.conf dosyasını değiştirerek [16].

TCPWrapper, /etc/inetd.conf dosyasındaki servislerin erişimini kontrol eder. Eğer elimizde X diye bir servis varsa ve biz bunu örtmek istiyorsak aşağıdaki komut yazılmalıdır.

```
ftp stream tcp nowait root /usr/sbin/tcpd  X  -l -L -i -o
```

Erişim kontrolünde iki ana dosya kullanılmaktadır [16]:
/etc/hosts.allow : Erişmesine izin verilen bilgisayarlar
/etc/hosts.deny : Erişmesine izin verilmeyen bilgisayarlar

Tcp örtücüler, servislerin erişimini kısıtlamayı sağlar. Tcp örtücüler başarısız olan bağlantı girişimlerini de takip eder ve kaydeder. Böylece bir saldırı olduğunda fark edilebilmektedir. Herhangi bir bilgisayar, makinadaki bir servise erişmeye çalışırsa önce /etc/hosts.allow listesine bakılır. Eğer bu listeye göre bu bilgisayara izin veriliyorsa bilgisayar servise ulaşır. Listede yoksa daha sonra /etc/hosts.deny listesine bakılır ve eğer listede bulunuyorsa bilgisayar servise ulaşamaz. Eğer her iki durum da gerçekleşmezse bilgisayar yine servise ulaşır.[2]

`/etc/hosts.allow` dosyasına sadece makinaya erişimine izin verilen bilgisayarlar eklenmelidir. Default olarak tüm servislerin kullanımının engellenmesi önerilmektedir. Bunu gerçekleştirmek için /etc/hosts.deny dosyasına da *ALL: ALL* satırı eklenmelidir.

TCPWrapper diğer araçlar ile birlikte de çalışabilmektedir. TCPWrapper ftp://ftp.porcupine.org/pub/security adresinden elde etmek mümkündür [16].

6.3Bastille-Linux

Bastille-Linux Linux/UNIX işletim sistemlerini güçlendirmek için kullanılan bir PERL programıdır. Program çalıştırıldığında çeşitli sorular sorulmakta ve verilen cevaplara göre sisteminizde ayarlamalar yapılmaktadır. Her sorunun ayrıntılı açıklamaları verilmektedir. Yapılan değişiklikler geri alınabilmekte, yeni yapılandırım ile işe başlanılabilmekte, yapılanlar görülebilmektedir. Ayrıca, ateşduvarı yapılandırılması yapmak da mümkündür. Şu anda Red Hat, Debian, Mandrake, SuSE and TurboLinux Linux dağırımlarını ve HP-UX ve Mac OS X işletim sistemlerini desteklemektedir. Döküman hazırlanırken Bastille-Linux'un sürüm numarası 2.0.4 olarak ilan edilmişti. Bu yazılım http://www.bastille-linux.org adresinden elde edilebilir. [16],[6]

6.4Snort

Snort, bir ağda oluşan trafiği incelemeye ve belli kriterlere göre paketleri ayıklamaya yarayan ağ izleme ve görüntüleme yazılımıdır. Snort sayesinde pasif olarak paketleri incelerken, aynı zamanda karşı işletim sistemi hakkında bilgi edinme imkanı bulunmaktadır. Yazılım birden fazla çıktı biçimi desteklemektedir. En yaygın çıktı biçimi olarak TCPDUMP biçimi kullanılmaktadır. Snort yazılımının kütük dosyaları için MySql sunucu desteği de bulunmaktadır. Bir çok firmanın ağ trafiği kontrolü için kullandığı ağ saldırı tespit sistemidir. Snort 3 moda sahiptir:

- Koklayıcı(Sniffer) Modu: Ağ trafiğini izleyen çalışma şeklidir. Bu modda çalıştırmak için aşağıdaki komutlar kullanılmalıdır:
  "./snort –v" Bu komut sadece TCP/IP paket başlıklarını gösterir.
  Sadece paket başlıkları (TCP/UDP/ICMP ve IP) ve veri akışını görmek için:
  "./snort –vd" komutu verilmelidir.
  Ağ trafiğiyle ilgili daha ayrıntılı bilgi görmek için
  ./snort -vde ya da ./snort -d -v -e komutları kullanılabilir.
- Paket Kaydedici(Logging) Modu: Kayıt işlemlerini kütük dosyası şeklinde yapan çalışma şeklidir. Bu modda çalıştırmak için aşağıdaki komutlar kullanılmalıdır:
  "./snort -dev -l ./log" komutu ile ağdaki hareketleri önceden belirlenmiş bir dizine(LOG) kaydeder.
  ./snort -dev -l ./log -h 192.168.1.0/24 komutu komut satırı belirtilen ip adresine kütük dosyasını kaydeder.
  ./snort -l ./log -b komutu ile kütük dosyasını ikili dosya olarak tcp döküm formatında kaydeder.
  ./snort -dv -r packet.log komutu ile binary olarak kaydedilen kütük dosyasını okur.
  ./snort -dvr packet.log icmp komutu sadece icmp paketlerini göstermek için kullanılır.
- Ağ Saldırı Tespit Sistemi(Network Instruction Detection) Modu: Saldırı ve ağdaki hareketlere karşı akıllı tepkiler verir. Snort'u bu şekilde çalıştırmak için:
  "./snort -dev -l ./log -h 192.168.1.0/24 -c snort.conf" yazılır.
  Burada ***snort.conf*** kural dosyasıdır. Eğer hedef dizini yoksa ***/var/log/snort*** dizininin altına kayıt işlemi yapılır.

"./snort -d -h 192.168.1.0/24 -l ./log -c snort.conf "
Bu komut satırı en temel özellikleriyle Snort yazılımını çalıştırır.

Snort yazılımı ücretsiz olarak dağıtımı yapılan bir yazılımdır. Snort yazılımını http://www.snort.org adresinden indirmek mümkündür. Snort'un Unix ve Windows platformlarında çalışan sürümleri bulunmaktadır. Snort'un belirli durumlar için girilen parametreler ve komutlar aşağıdaki gibidir:

- Kütük dosyalarını ilksel olarak kaydetmek ve syslog'a alarm yollamak için:
  ./snort -c snort.conf -l ./log -s -h 192.168.1.0/24
- Kütük dosyalarını /var/log/snort altına hızlı alarm olarak yollamak için:
  ./snort -c snort.conf -s -h 192.168.1.0/24
- Kütük dosyalarını ikili olarak kaydedip Windows istasyonlarına alarm olarak yollamak için:
  ./snort -c snort.conf -b -M WORKSTATIONS
- Bu komutların yanında Snort yazılımını arka planda çalıştırmak için "-D", IP adreslerini gizlemek için "-O" parametreleri komut satırına eklenmelidir.

6.5FIREWALL/FILTER

Diğer bir güvenlik önlemi ise bilgisayarlardaki firewall(güvenlik duvarı) dır. Firewall ağı internetten korumak için geliştirilmiştir. En basit hali bir Linux makinesidir. Bir Ethernet kartı ile internete, diğer Ethernet kartı ile de ağa bağlıdır. Internetten akan ya da internete giden verilerin filtrelenme işlemini yapar böylece ağ içinde servisleri denetleme konusuna daha az özen gösterilir. Firewall kurma aşamasında ipchains adlı bir program kullanılır. Örneğin su komut;

```
#ipchains -l input -p TCP -s  192.168.1.11 telnet -j DENY -l
```

belirtilen ip numarasından gelen telnet portuna ulaşımı engelleyecektir. Ayrıca yine ipchains kullanarak 6000:60003 arası portlara(X portları) ulaşımı dışardan kapatmak yararlı olacaktır;

```
#ipchains -A input -i eth0 -p tcp -y --destination-port
6000:6003 -j DENY
```

IP Tables/Netfilter ise, yine Linux ortamında kullanabilen ipchains programının bir üst versiyonu olan güvenlik duvarıdır. Paket filtreleme, NAT gibi uygulamların gereçekleştirilmesini sağlar. Detaylı bilgi ve gerekli ek yazılımlar http://www.netfilter.org/ vede yakında http://security.ege.edu.tr adreslerinden temin edilebilir.

6.6TRIPWIRE

Eğer sisteme bir saldırı varsa bunu ortaya çıkarmak da güvenlik önlemlerinin bir parçasıdır. İşte bunu yapan Tripwire, kaynak kodu ve Linux binary kodu ücretsiz olan

bir yazılımdır. Bu program sistemde bulunan tüm dosyaların imzalarını tespit eder ve veri tabanına kaydeder. Sistemde herhangi bir değişiklik olduğu düşünülürse programı çalıştırarak bunlar hakkında rapor üretmesini sağlanabilir ve Tripwire bu raporu saklar ve isterseniz size e-mail olarak da gönderebilir. Veri tabanını güncelleyerek ikinci bir rapor üretmesi istendiğinde en son değişiklikleri görmeniz mümkün olur. Bu programı /root dizini altına kurmaya dikkat etmelidir [13].

6.7Nmap

Nmap ağı gözden geçirerek güvenlik denetimini sağlar. IP paketlerini kullanır ve uzaktaki sistemin hangi işletim sistemini kullandığını, hangi portları açıkolduğunu, firewall/filter tiplerini ve hatta servisi kullananın kullanıcı adını belirleyebilir [5].

Nmap, hackerlar tarafından kullanıldığı gibi, sistem yöneticileri tarafından da kendi ağ güvenliklerini test etmek amacıyla da kullanılabilir.

7SONUÇ

Sonuç olarak; Unix/Linux sistemler doğası ve yapısı gereği güvenli işletim sistemleri olarak bilinmektedir. Daha doğrusu Linux sistemler çeşitli basamaklar sonunda daha rahat bir biçimde güvenli hale getirilebilir. Bu dokümanda Linux sistemlerin nasıl daha güvenli hale getirilebileceği konusunda okuyucuya yardımcı olunmaya çalışılmıştır.

Öncelikle dökümanda da belirtildiği gibi bilgisayarın fiziksel güvenliğinden başlayarak, dosya sistemi, çeşitli servisler, şifre ve çekirdek güvenliğini sağlamak, dışarıdan gelebilecek olan çeşitli virüs tehlikelerine karşı önlem almak, ayrıca en son yamaları yüklemek ve yedekleme yapmak suretiyle daha güvenli bir sisteme sahip olunabilmektedir. Snort kurarak ağ denetimini, Tripwire kullanarak sistem dosya denetimi sağlanabilir ve de Nmap yükleyerek sistem açıklarını bulup gerekli önlemleri alarak sistem güçlendirilebilmektedir. Ayrıca güvenlikle ilgili çesitli mail gruplarına, forumlara üye olunarak bir çok programda her geçen gün yenileri ortaya çıkarılan güvenlik açıklarından haberdar olunabilmekte, bunları önlemek için alınması gereken tedbirler ve de en son yamalara ulaşılabimektedir.

Sürekli gelişen ve ilerleyen bilgisayar teknolojisi düşünüldüğünde yeni keşfedilen sistem zayıflıkları ve alınabilecek önlemleri yakından takip etmek ise Linux sistem güvenliğini sağlama konusunda yapılabilecek en önemli işlerden biridir.

8KAYNAKÇA

1 . Genel güvenlik konseptleri
http://www.securityfocus.com/

2. Linux sistemlerin güvenliği ile ilgili çeşitli dokümanlar
http://www.linuxsecurity.com/docs

3. Saldırganlar, güvenlik açıkları ve alınabilecek önlemlerle ilgili makaleler
http://neworder.box.sk/subject.php?subject=Articles%20-%3E%20Security

4. Linux / Çekirdek(kernel) ve özellikleri
http://www.purists.org/linux

5. nmap port tarayıcısı
http://www.nmap.org

6. Bastille Linux Sistem güçlendirme projesi
http://www.bastille-linux.org

7. Genel güvenlikle ilgili makaleler
http://devel.gazi.edu.tr

8. Genel güvenlikle ilgili makaleler
http://www.dayioglu.net

9. Genel güvenlikle ilgili makaleler
http://www.dikey8.com

10. RPM paket yönetimi
http://www.rpm.org

11. Apache web sunucusu yönetimi
http://apacheweek.com

12. Linux güvenliği ile ilgili makaleler
http://kemalgok.virtualave.net

13. Tripwire dosya denetleme programı
http://www.tripwire.org

14. Network Security Essentials, William Stallings

15. Linux'la ilgili Türkçe dokümanlar
http://www.turkcelinux.com/article.php?32.0

16. Serbest yazılım araçları ile karmaşık ağların güvenliğini sağlamak
http://linux.atlink.it/linuxfocus/Turkce/July2002/article245.shtml

17. Pluggable Authentication Modules (PAM)
http://www.kernel.org/pub/linux/libs/pam/pre/doc/current-draft.txt

18.Paket yönetim sistemleri- RPM
http://www.geleceklinux.com/belgeler/rpm_paketleri.php

19.Yedekleme ve önemi
http://ilkerf.tripod.com/teknik/yedekleme.htm

9EKLER

9.1EK-1: ÖNEMLİ SİSTEM DOSYALARI VE ERİŞİM HAKLARI

Önemli sistem dosyaları ve erişim hakları aşağıda olduğu gibi düzenlenebilir[2]:

Dosya/dizin	Açıklama	Erişim hakkı
/var/loglog	dosyalarını içeren dizin	751
/var/log/messages	sistem mesajları	644
/etc/crontab	sistem crontab dosyası	600
/etc/syslog.conf	syslog sunucusu şekillendirme dosyası	640
/etc/logrotate.conf	sistem log dosyalarının dönüşünü sağlar	640
/var/log/wtmp	şu an kim login durumda olduğunu gösterir	660
/var/log/lastlog	en son kimin login olduğunu göster	640
/etcftpusers	Ftp olamayan kullanıcıların listesi	600
/etc/passwd	kullanıcı hesaplarını listele	644
/etc/shadow	şifreli hesapların şifresini gösterir	600
/etc/pam.d	PAM şekillendirme dosyaları	750
/etc/hosts.allow	erişim control dosyası	600
/etc/hosts.deny	erişim control dosyası	600
/etc/lilo.conf	boot yükleyicisi şekillendirme dosyası	600
/etc/securetty	root loginini sağlayan TTY arabirimi	600
/etc/shutdown.allow	ctrl-alt-del'ye izin verilen kullnıcılar	400
/etc/security	sistem erişimi güvenlik dosyalar	700
/etc/rc.d/init.d	RedHat sistemler erişim control dosyası	750
/etc/init.d	Debian sistemler erişim control dosyası	750
/etc/sysconfig	RedHat için sistem ve network config dosyaları	751
/etc /inetd.conf	internet süpersunucu şekillendirme dosyası	600
/etc/cron.allow	cron kullnmaya yetkisi olan kullanıcılar	400
/etc/cron.deny	cron kullnmaya yetkisi olmayan kullanıcılar	400
/etc/ssh	ssh şekillendirme dosyası	750
/etc/sysctl.conf	RDH lar için ayarlanabilir kernel seçeneklerini içeren dosya	400

9.2EK-2: Web Kaynakları – Güvenlik Siteleri

http://www.securityfocus.com
:Genel güvenlik konseptleri

http://www.linuxsecurity.com
:Linux sistemlerin güvenliği ile ilgili çeşitli dokümanlar

http://www.securityportal.com
:sisteminizde deneyebileceğiniz exploitleri burdan bulabilirsiniz.

www.linuxtoday.com
:Linux ve güvenliği ile ilgili son haberleri burdan alabilirsiniz.

http://www.apacheweek.com
:Apache web sunucusu yönetimi

http://www.cert.org
:Internet güvenliği, sistem açıkları, güvenlik uyarıları, network araştırmaları ilgili bilgiler, güvenlik uyarı listesi: http://www.cert.org/contact_cert/certmaillist.html

www.ciac.org:
Windows, Linux güvenlik açıkları, son yamalar ve çeşitli sistem güvenlik dokümanlari

http://www.olympos.org
Türkçe Güvenlik Sitesi, duyurular, dökümantasyon, forum

http://security.ege.edu.tr
:Güvenlik konusunda Ege Üniversitesi Network Güvenlik Grubu'nun çalışmalarını ve Türkçe Güvenlik Dökümantasyon Projesine bu adresten ulaşabilirsiniz.

http://www.tripwire.org
: Tripwire dosya denetleme programı

http://www.bastille-linux.org
:Bastille Linux Sistem güçlendirme projesi

www.whitehats.com
: Saldırılar, savunma yöntemleri ile ilgili bilgiler, dökümantasyon, forum.

www.intrusion.com
:saldırı tespit sistemleri ile ilgili bilgiler

http://oslab.snu.ac.kr/~djshin/linux/mail-list/
:Linux' la ilgili çeşitli haber gruplarına burdan ulaşılabilir.

http://www.linuxsecurity.com/general/mailinglists.html
Linux Güvenlik Listeleri