

- **Sistem Güvenliği**
 - **Kolay Tahmin Edilebilecek Şifre Kullanmayın ve Kullandırmayın**
 - **Sistem Güvenliği ile İlgili Haberleri İzleyin**
 - **Olabildiğinizde Güvenli İletişim Yapan Yazılımlar Kullanın**
 - **Güvenlikle İlgili Yamaları İzleyin ve Uygulayın**
 - **Gereksiz Yazılım Yüklemeyin**
 - **Gereksiz Servisler Çalışmasın**
 - **Gereksiz Portlar Açık Olmasın**
 - **Bilgisayarınızdaki Tüm Servisler Dünyaya Açık Olmasın**
 - **Log Dosyalarınıza Bakın**
 - **Sisteminizi Yedekleyin**

Sistem Güvenliği

İnternet'in yaygınlaşmasıyla "bilgisayar sistem güvenliği" de önemli sorunlar listesinde önce üst sıralara; sonunda da en üste tırmandı. LINUX, sistem güvenliği açısından en şanslı işletim sistemidir, çünkü kodu herkese açıktır. Bu iddia çok kişi tarafından ciddiye alınmamakla birlikte son yıllarda yaşanan deneyimler iddiayı doğrulamıştır.

Kapalı kodlu bir işletim sisteminde bir güvenlik açığı bulunduğunda, düzeltme yamaları ya da yeni sürümün geliştirilmesi, duyurulması ve yayınlanması zaman almaktadır. Bu sürenin ayları bulabildiği görülmüştür. Oysa, benzeri bir durum LINUX işletim sisteminde ortaya çıktığında, yamalar veya yeni sürümler birkaç saat içinde dünyaya yayılmaya başlamaktadır.

Sisteminizin güvenliği için salt işletim sistemine güvenmek çok büyük hatadır. "LINUX işletim sistemi altında virüs olmaz", "LINUX güvenlidir, kim-

se kıramaz” gibi inanışlar tamamen yersizdir. Bal gibi virüs de bulaşır; sisteminiz de kırılır...

Sistem yöneticilerinin en önemli görevlerinden birisi de sistemin güvenliği ile ilgili çalışmaları disiplinli bir şekilde yapmaktır.

Kolay Tahmin Edilebilecek Şifre Kullanmayın ve Kullandırmayın

Adı üstünde; “şifre”... Eğer yapışkanlı sarı bir kağıda yazıp ekranın köşesine yapıştıracaksanız ya da şifre diye adınızı veya “abc123”, “qwerty” gibi bir dizi kullanacaksanız hiç şifre kullanmayın daha iyi.

Şifreleri kesinlikle e-postayla göndermeyin. Şifreleriniz kolay hatırlayabileceğiniz kadar anlamlı ama tahmin edilemeyecek veya sözlüklerde bulunamayacak kadar anlamsız olsun. En iyisi atasözü, şarkı adı gibi cümlelerin baş harflerinden ve noktalama işaretlerinden oluşan şifrelerdir. “**Hehmi!**” gibi... (Hayatta en hakiki mürşit ilimdir!).

Sistem Güvenliği ile İlgili Haberleri İzleyin

En başta, kendinize en az bir LINUX güvenlik sitesi bulmalısınız. Bu site(ler)deki haberlere hiç değilse iki-üç günde bir göz atmalısınız. Yeni ortaya çıkan bir güvenlik açığı varsa hemen mümkün olduğunca ayrıntılarını öğrenip, sisteminizde önerilen kontrolleri yapıp gerekli güncellemeleri uygulamalısınız. Google’da “linux, güvenlik, security” gibi sözcüklerle yapacağınız bir arama sizi istemediğiniz kadar çok kaynağa yöneltecektir. <http://security.metu.edu.tr/belge.php> ve <http://www.linuxsecurity.com> genellikle her türlü gereksiniminizi karşılayacak kaynaklar içermektedir.

Olabildiğince Güvenli İletişim Yapan Yazılımlar Kullanın

Ethernet ağlarını dinlemek (sniff etmek de denir) çok kolay olduğu için, ne kadar iyi şifre seçip kullansanız da güvende olamazsınız. Bu hat dinleme sorununa bir çözüm olarak TCP/IP protokolüne **SSL** (*Secure Socket Layer*) özelliği eklenmiştir. SSL kullanan protokoller, her bağlantıda sunucu ile istemciyi bir kriptolama sistemi üzerinde anlaştırıp, ağ arabirime bastıkları tüm paketlerin bu sisteme göre kriptolanmasını sağlarlar. Genellikle RSA

(Rivest, Shamir, Adleman) adı verilen teknikle kriptolanan bu paketleri çözmek olanaksız değilse de pratik zaman sınırları içinde çözülemezler.

Bilgisayarınıza “telnet” kullanarak erişmeyin; onun yerine “ssh” kullanın. Ssh, tüm terminal haberleşmesinin kriptolu yapılmasını sağlayacaktır.

Güvenlikle İlgili Yamaları İzleyin ve Uygulayın

Tüm LINUX dağıtım kuruluşları gibi Mandrake de zaman zaman güvenlik yamaları yayınlamaktadır. Her hafta en az bir kere “Mandrake Control Center” altındaki “Software Manager” ile güvenlik yamalarını sorgulayıp, gerekli gördüklerinizi; hatta hepsini uygulayın. Her olasılığa karşı bu işleri sisteminizin yoğun kullanılmadığı zamanlarda; örneğin Cuma günleri akşam saatlerinde yapın. *“Cuma akşamları yama aramakla uğraşamam; arkadaşlarla eğlenmeye gideceğiz”* diyenlerdenseniz siz sistem yönetici olamazsınız; en azından “iyi” bir sistem yöneticisi olamazsınız. Sistem yöneticileri gezmezler, eğlenmezler (daha doğrusu sistemlerinin başında daha mutludurlar); herkes gibi geceleri uyumazlar; normal yemek yemezler; organizmaları kahveden protein, karbonhidrat gibi yaşamsal maddeleri soğurma yeteneğini geliştirmiştir.

Gereksiz Yazılım Yüklemeyin

Kesinlikle gerekli olmayan yazılımları sisteminize yüklemeyin; hele sisteminiz önemli servis(ler) veriyorsa... Kaynağı belli olmayan yazılımlardan uzak durun.

Gereksiz Servisler Çalışmasın

Sisteminizde kullanmayacağınız servisleri kapatın. Örneğin sisteminizden bir web sunucusu olarak yararlanmayacaksanız, **httpd** çalışmasın; hem boş yere bellek harcar hem de gereksiz risk almış olursunuz. Sisteminizin açılışı sırasında başlatılacak servisleri “Mandrake Control Center - System” altındaki “DrakXServices” yazılımıyla görsel olarak seçebilirsiniz.

Kim Korkar LINUX'tan?

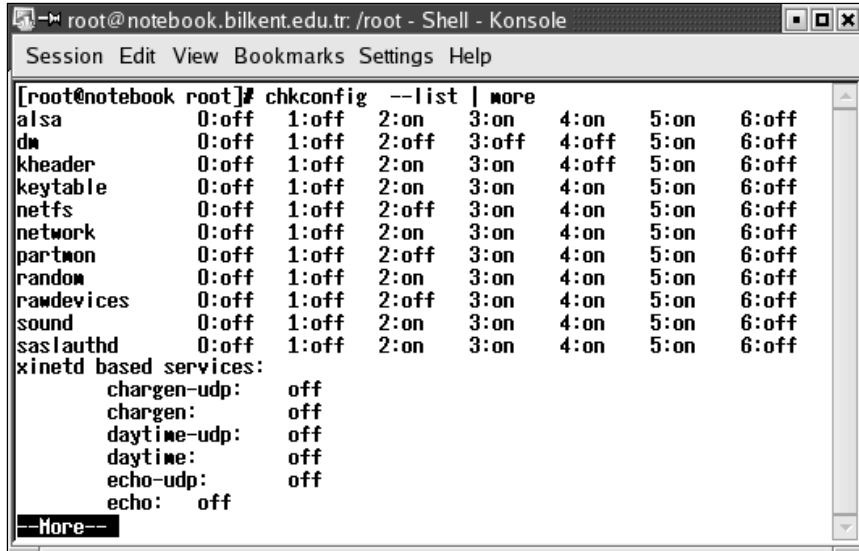
Bu işleri konsoldan yapmayı yeğlerseniz

chkconfig

komutunu kullanabilirsiniz.

chkconfig --list

komutuyla, **chkconfig** size sisteminizde çalışan servisleri, her çalışma düzeyi için (run level) ayrı ayrı belirtecektir.



```
[root@notebook root]# chkconfig --list | more
alsasrc 0:off 1:off 2:on 3:on 4:on 5:on 6:off
dm 0:off 1:off 2:off 3:off 4:off 5:on 6:off
kheader 0:off 1:off 2:on 3:on 4:off 5:on 6:off
keytable 0:off 1:off 2:on 3:on 4:on 5:on 6:off
netfs 0:off 1:off 2:off 3:on 4:on 5:on 6:off
network 0:off 1:off 2:on 3:on 4:on 5:on 6:off
partwon 0:off 1:off 2:off 3:on 4:on 5:on 6:off
random 0:off 1:off 2:on 3:on 4:on 5:on 6:off
rawdevices 0:off 1:off 2:off 3:on 4:on 5:on 6:off
sound 0:off 1:off 2:on 3:on 4:on 5:on 6:off
sslsauthd 0:off 1:off 2:on 3:on 4:on 5:on 6:off
xinetd based services:
  chargen-udp: off
  chargen: off
  daytime-udp: off
  daytime: off
  echo-udp: off
  echo: off
--More--
```

Örneğin

mysqld 0:off 1:off 2:on 3:on 4:on 5:on 6:off

satırı **mysqld** veritabanı sunucusunun 0,1 ve 6 çalışma düzeylerinde çalışmayacağını, ama 2, 3, 4 ve 5. düzeylerde çalışır durumda olacağını (olduğunu) gösterir.

Meraklısına...



Daha önce dördüncü LINUX çalışma düzeyinin kullanılmadığını söylemiş-tik. Hangi çalışma düzeyinde hangi yazılımların çalıştırılacağı **/etc/init-tab** dosyasından denetlenir. Eğer kendi gereksinimleriniz için özel bir dü-zey tanımlamak ve bu düzeyde birtakım yazılımları çalıştırmak isterseniz **/etc/inittab** dosyasında gerekli değişiklikleri yaparak kendi sisteminize özgü dördüncü düzey tanımınızı yapabilirsiniz.

Çalışma düzeylerini şöyle bir hatırlatmak gerekirse...

0	Kapanış düzeyi. Bu düzeyde pek çalışan program bulamazsınız...
1	Tek kullanıcı düzeyi. Sistem, gerek ağ üzerinden gerekse konsolundan birden fazla kullanıcıya hizmet vermez.
2	Çok kullanıcı düzeyi ama ağ üzerinden dizin/dosya paylaşımına izin verilmez (NFS yoktur).
3	Sistemin tam kapasite ile çalıştığı çok kullanıcı düzeyidir
4	Pek kullanılmaz
5	XFree86 pencere sisteminin çalıştığı düzeydir
6	"Reboot" düzeyidir. Yani, sistemi kapatan yazılımların çalıştığı düzeydir.

Sisteminizde **mysql** servisine gereksiniminiz yoksa

chkconfig mysql off

komutuyla servisin bir dahaki açılışta ve sonrasında başlatılmasını önleyebi-lirsiniz.

mysql veritabanı sunucusunu kullanmaya başladığınızda, açılışlarda kendi-liğinden başlaması için

chkconfig mysql on

komutunu kullanabilirsiniz.



chkconfig komutuyla birtakım servislerin otomatik olarak başlatılmasını sağladığınızda (--add seçeneği) ya da engellediğinizde (--del seçeneği), komutunuzun etkisi ancak sistemin bir dahaki açılışında görülür.

Yaptığınız değişikliğin etkisini hemen görmek istediğinizde; örneğin mysql'in hem hemen durdurulmasını hem de bir dahaki açılışta çalışmamasını sağlamak için

```
/etc/rc.d/init.d/mysql stop  
chkconfig mysql off
```

komutlarını kullanmalısınız.

chkconfig komutunun aslında tek yaptığı iş, **/etc/rc.d/init.d** dizinindeki açılış denetim komut dizelerini (*script*) düzenlemektir.

Gereksiz Portlar Açık Olmasın

Bildiğiniz gibi (daha doğrusu bilmeniz gerektiği gibi) TCP/IP iletişiminin temelinde “port” kavramı yatar. İnternet hatları üzerinden bilgisayarınıza ulaşan veri paketlerinin hangi yazılım tarafından karşılanacağını paketin içindeki port bilgisi belirler. Örneğin, 23 numaralı port genellikle “telnet” servisi ile ilgilidir. Yani, sisteminize varış port numarası (destination port) 23 olan bir veri paketi ulaştığında, bu paket “telnet” sunucu yazılımına, yani **in.telnetd** yazılımına iletilir.

Hangi port numarasını hangi yazılımın karşılayacağına ilişkin tanımları **/etc/services** dosyasında bulabilirsiniz.

```

root@notebook.bilkent.edu.tr: /root - Shell - Konsole
Session Edit View Bookmarks Settings Help
[root@notebook root]# more /etc/services
# /etc/services:
# service-name port/protocol [aliases ...] [# comment]

tcpmux      1/tcp                # TCP port service multi
plexer
tcpmux      1/udp                # TCP port service multi
plexer
rje         5/tcp                # Remote Job Entry
rje         5/udp                # Remote Job Entry
ftp         21/tcp               fsp fspd
ftp         21/udp
ssh         22/tcp                # SSH Remote Login Proto
col
ssh         22/udp                # SSH Remote Login Proto
col
telnet      23/tcp
telnet      23/udp
# 24 - private mail system
smtp        25/tcp               mail
smtp        25/udp               mail
time        37/tcp               timserver
time        37/udp               timserver
--More-- (6%)

```

TCP ve UDP portlarının ne demek olduğunu bilmiyorsanız en kısa zamanda TCP/IP temellerini öğrenmeniz gerekir. Açıkçası, TCP/IP bilmeden sistem yöneticisi olma şansınız pek yok! TCP/IP öğrenmek için Murat Yıldırımoğlu'nun Pusula Yayıncılık tarafından yayınlanan *TCP/IP* isimli kitabından (ISBN: 975-7092-25-8) yararlanabilirsiniz.

Bilgisayarınızdaki Tüm Servisler Dünyaya Açık Olmasın

İnternet üzerinde yer alan bilgisayarlar üzerindeki TCP/IP trafiğini denetim altına almak için kullanılan yazılımlara “Ateş duvarı, Firewall” denir. Bu yazılımların temel görevi sisteme giren ve sistemden çıkan tüm ağ paketlerini inceleyip, paketleri sistem yöneticisinin direktifleri doğrultusunda işlemektir. Örneğin, bir ateş duvarı yazılımı, **192.168.13.*** gibi adreslerden gelen telnet paketlerine izin verip bunun dışındaki IP bloklarından gelen tüm telnet paketlerini reddedebilir.

Sisteminizi dışarıya karşı korumak için LINUX’da pek çok araç vardır. Bu araçlardan en yaygın olanı “**iptables**” adıyla bilinen filtre yazılımıdır.

TCP Wrapper, temel olarak bilgisayarınıza hangi bilgisayarların, hangi servislerle erişebileceğini ya da erişemeyeceğini belirlemenizi sağlar. TCP Wrapper, yalnızca sisteminize giren paketleri denetlemek için işe yarar; sisteminizden çıkan paketler bu yazılımla denetlenemez.

TCP Wrapper, **/etc/hosts.allow** (sisteme erişmesine izin verilecek bilgisayarlar) ve **/etc/hosts.deny** (sisteme erişmesine izin verilmeyecek bilgisayarlar) dosyalarıyla denetlenir. Bu dosyalar **vi** ile düzenlenebilecek basit dosyalardır. Dosyalarda yapacağınız değişiklikler hemen etkili olur; yani, herhangi bir yazılımı; hele hele işletim sistemini yeniden başlatmanız gerekmez.

TCP Wrapper'ın denetim mantığı şöyledir:

1. Sisteminize bir TCP/IP paketi geldiğinde, port numarasına bakılarak hangi yazılıma iletileceğine karar verilir.
2. Paket eğer **/etc/services** dosyasında tanımlı bir servise gönderilecekse, önce **/etc/hosts.allow** dosyası taranarak paketin özelliklerine uygun bir tanım olup olmadığına bakılır. Örneğin gelen bir telnet paketiye ve **/etc/hosts.allow** dosyasında "**in.telnetd: 139.179.14.: ALLOW**" gibi bir satır varsa ("139.179.14. ile başlayan bir IP adresinden gelmek kaydıyla, tüm telnet paketlerini kabul et" anlamında), paket kabul edilir.
3. **/etc/hosts.allow** dosyasında, gelen pakete uygun bir satır bulunamazsa, benzeri bir tarama **/etc/hosts.deny** dosyasında tekrarlanır. Bu dosyada, sisteminize erişmesini istemediğiniz bilgisayarlar tanımlıdır.
4. Eğer bu dosyada da gelen pakete uygun bir kural kalıbı bulunamazsa, paketin içeri girmesine izin verilir.

hosts.allow ve **hosts.deny** dosyalarında yer alabilecek kalıp tanım satırlarının genel formatı:

servis: IP alan tanımı

şeklinindedir. Örneğin **/etc/hosts.allow** dosyasında yer alan

in.telnet.d: 139.179. ALLOW

gibi bir satır, IP adresi "139.179." ile başlayan bilgisayarlardan gelen telnet paketlerini kabul edecektir.

/etc/hosts.deny dosyasında yer alabilecek

in.telnet.d: 192.168.100.12 DENY

gibi bir satır, IP adresi 192.168.100.12 olan bilgisayardan gelecek telnet servisi isteklerine olumsuz yanıt verilmesini sağlayacaktır.

Genellikle, sağlamcı bir politika izlemek amacıyla **/etc/hosts.deny** dosyasında tek satır olur:

ALL: ALL:

Yani, “nereden gelirse gelsin, hiçbir **xinetd** servisi isteğini kabul etme!” Sisteme erişmesine izin verilecek bilgisayarlar da **/etc/hosts.allow** dosyasında belirtilir.

Her iki dosyada da “#” ile başlayan satırlar açıklama satırlarıdır.

hosts.deny ve **hosts.allow** dosyalarına tipik birer örnek vermek gerekirse:

/etc/hosts.deny	/etc/hosts.allow
ALL: ALL:	in.telnetd: 139.179.14. ALLOW ALL: 139.179.14.41 ALLOW ALL: 139.179.23. EXCEPT 139.179.23.45



TCP Wrapper ile yalnızca **xinetd** üzerinden verilen servisleri denetleyebilirsiniz. O yüzden **hosts.allow** ve **hosts.deny** dosyalarıyla sisteminizin trafiği üzerinde tam denetim sağlayamazsınız. Örneğin bu araçla bilgisayarınıza yönelik web trafiğini (http, 80. port üzerinden gelen trafik) denetleyemezsiniz çünkü http, xinetd'nin denetlediği bir servis değildir. Benzeri şekilde ftp sunucusu olarak pro-ftpd çalıştırıyorsanız (-ki, standart kurulumda böyle olacaktır), gene erişim denetimini TCP Wrapper ile yapamazsınız.

Sisteminize yönelik ve sisteminizden kaynaklanan trafiği tam olarak denetim altına almak için "**iptables**" veya "**ipchains**" ateş duvarı yazılımını kullanmalısınız. Son yıllarda "**iptables**" daha popüler bir yazılım olarak öne çıkmaktadır.

Eğer sisteminizde esnek bir trafik denetim sistemi kurmak istiyorsanız "**shorewall**" paketini kurmanızı öneririz. **shorewall**, **iptables** üzerine kurulmuş bir filtreleme sisteminin denetim yazılımıdır. "**shorewall**"u kurmak için Mandrake Control Center yazılımından "Security" seçimini yapıp "DrakFirewall" programını başlatınız. "shorewall" yazılımının ayarları en kolay, web tabanlı bir sistem yönetim aracı olan "webmin" ile yapılır.

Log Dosyalarınıza Bakın

LINUX işletim sisteminin seyir defteri olan log dosyalarına sık sık göz atmanız önemlidir. Özellikle de **/var/log/security** dosyası...

Log dosyaları genellikle çok sayıda ve karmaşık satırlardan oluşur. "**more xyz.log**" gibi komutlarla listelenip gözle kontrol edilmeleri zordur. Webmin servisinin "System – System Logs" seçimiyle daha kolay izlenebilecek log listeleri alabilirsiniz.

Sisteminizi Yedekleyin

Başkalarına ait bilgisayarlara girmek nedense çok sayıda hasta ruhlu insan için bir tutkudur. Bu tip insanlar, bir bilgisayarın güvenliğini kırmayı başardıklarında bu zaferlerini kutlamak isterler; bu yüzden de sistemleri tamamen çökertmek yerine "başarı"larını belgeleyen bir işaret bırakmayı yeğlerler. Sisteminize girildiğini hissettiğinizde yapabileceğiniz en akıllıca şey diskleri formatlayıp işletim sistemini baştan yüklemek olacaktır. Bu işin kolay bölü-

müdür; öte yandan iyimser bir bakış açısıyla da sürüm güncellemek için iyi bir fırsattır. Ancak; iş daha önce yapılmış ayarları, yüklenmiş uygulama programlarını, tanımlanmış kullanıcıları, onların kişisel dosyalarını yerine koymaya gelince işiniz zor olacaktır. Disiplinli ve dikkatli bir şekilde yedeklenmiş bir sistemde bu dosya/dizinleri yerine koymak zaman alsa bile kolayca yapılabilir. Napolyon sistem yöneticisi olsaydı, eminiz ki “*para, para, para*” yerine “*yedek, yedek, yedek*” derdi.

BUNLARI BİLİYOR MUYDUNUZ?

Kaç İşlemci?

UNIX ve türevi işletim sistemlerini oluşturan yazılımların en önemli özellikleri, her birinin "kendi işini, ama yalnızca kendi işini çok iyi ve hızlı yapan", esnek ama gereksiz işlevleri olmayan, "küçük" programcıklar olmalarıdır. Bu yazılımlar; anlamlı olabildiği her durumda birer "filtre" olarak yazılmıştır. "Filtre" olarak kullanılabilen programlar girdilerini STDIN'den alan, bu girdileri işleyip çıktılarını da "STDOUT" a gönderen programlardır. Bu sayede, bu programları "pipe" (|) ve "yönlendirme" (< , >) işlemleri ile peşpeşe ya da birlikte çalıştırılarak gereksinimlere göre anlamlı işler yapabilen zincirler oluşturulabilir.

UNIX'in çok önemli bir başka tasarım ilkesi de; olabildiğince, tüm verilerin, ayar/seçenek değerlerinin basit metin dosyalarında saklanması ve işlenmesidir.