

FreeBSD guvenligi

Hepimizin zaman gectikce farkina vardigi gerceklerden biri de su anda her turlu isimizi halledebilecegimiz ve hayatimizin bir parcasi olan internet`in guvenli olmadigidir.Bu guvensizligi ortadan kaldirmak icin gelistirilen guvenlik duvarlarini hepimiz kullanmaktayiz.FreeBSD sistemiz ise baska hicbir urune gerek birakmadan iki tur guvenlik duvari mekanizmasini icinde barindirarak gelmektedir: : `ipfw` ve `ipfilter`. Daha da iyisi yillardan beri yazilmis olan dokumanlar bunlarin konfigrasyonlarini en iyi sekilde aciklamakta ve sizin kendi guvenlik duvari mekanizmanizi olusturmaniza buyuk yardim saglamaktadir.Iste bu dokumanlardan birer ornek:

```
man ipfw
```

[FreeBSD Handbook: Section 10.7 -- Firewalls
Setting Up a Dual-Homed Host using IPFW and NATD](#)

```
man ipf
```

[IPFilter and PF resources](#)

Saglam guvenlik her zaman “Derinde guvenlik” demektir. Yani bir guvenlik mekanizmasi herhangi bir sekilde gecilirse veya calismayi durdurursa arka planda calisan ikinci bir yedek mekanizmanin bulunmasidir.Sistemlerinizde guvenlik duvari bulunsa bile onemli noktalardan biri de kullanilmayan servislerin durdurulmasidir. Normalde desktop olarak kullandiginiz bir sistemde cok az sayida calisan servise ihtiyaciniz olacaktır.

Sisteminizde disaridan gelen isteklere cevap verecek olan servisleri gormek icin su komutu kullanabilirsiniz:

```
sockstat -4
```

Her sistemin ciktisi calistirdiginiz servislere gore degisecektir.

Normalde 6000 (X Window Sunucusu) port`unu gormek dogaldir. Eger gormuyorsanız x-window`unuzu baslatip `sockstat -4` komutunu tekrar deneyin.Son yillarda x-window servisi icin bircok acik bulundugu icin bu servisi kapatmaniz yararınıza olacaktır. Meraklanmayin! Bu port`u kapatirsanız hala local olarak sisteminizde X-window`u kullanabileceksiniz.

Bu port`u kapatmanin birkac yolu bulunmakta.En kolay yolu ise `/usr/X11R6/bin/startx` dosyasina girip `serverargs` satirinda degisiklik yapmaktir. Bu satiri asagidaki gibi degistirin:

```
serverargs="-nolisten tcp"
```

Degisiklikleri kaydettikten sonra normal kullanıcı olarak X`i baslattiginizda artik `sockstat -4` ciktinizda 6000. port kapali gorunecektir.

Eger 6000. port`u acik birakmanin ne tur sorunlara yol actigi hakkında bilgi edinmek isterseniz [Crash Course in X Window Security](#) sayfasina goz atabilirsiniz.

6000. port`u kapattigimiza gore diger acik port`larimize bakabiliriz.Normal olarak incelememiz gerek olan e-posta servisleri ile ilgili 2 port daha bulunmakta: 25 (smtp) ve 587 (submission).Posta alip gonderebilmek icin 587. port`a ihtiyaciniz yoktur. Bunu /etc/mail/sendmail.cf. icinde :

```
O DaemonPortOptions=Port=587, Name=MSA, M=E
```

Satirini bulup onune bir # isareti koyarak kapatabilirsiniz.Bundan sonra tell sendmail`in degisiklikleri uygulamasini icin su komutu vermelisiniz:

```
killall -HUP sendmail
```

-HUP komutu sendmail`i durdurmayacak sadece /etc/mail/sendmail.cf`a degisiklikleri uygulamasini soyleyecektir.Simdi sockstat -4 komutu verdiginizde 587.port`un artik acik olmadigini goreceksiniz.

Peki ya 25.port Bu port`un acik olmasini isteyebilir veya istemeyebilirsiniz. Bu tamamen sizin posta gondermek icin hangi posta istemcisini kullandiginiz ile ilgilidir.Bu port`u kapatmak icin su komutu /etc/rc.conf dosyaniza ekleyin:

```
sendmail_enable="NO"
```

Bu komut sendmail`in sadece local systeme servis vermesini saglayacaktır.Eger posta istemcinizin yazilim ile birlikte gelen ve kendi kullandigi bir SMTP servisi var ise /etc/rc.conf dosyaniza ekleyeceginiz asagidaki komut ile sendmail servisini tamamen durdurabilirsiniz:

```
sendmail_enable="NONE"
```

Eger "sockstat" ciktinizda 111. port (portmap) acik gorunuyorsa, yine /etc/rc.conf dosyaniza asagidaki parametreleri ekleyerek su satirlari kapatabilirsiniz:

```
nfs_server_enable="NO"  
nfs_client_enable="NO"  
portmap_enable="NO"
```

Portmap sadece NFS calistiriyorsanız gerekli olacagından masaustu istemcilerin bu servise ihtiyaclari olmayacaktır.Guvenlik acisindan pek cok sorunu bulunan bu servisi kapatmanız yerinde bir karar olacaktır.

syslog (port 514) ciktinizda yer alan diger servislerden olacaktır.Tamamen kapatmanız sizing gunluk tutulan mesajlari almanizi engelleyeceginden bunu sadece local sistemde calistirmek guvenlik sorununuzu, servisi acik birakarak ortadan kaldiracaktır:

```
syslogd_enable="YES"  
syslogd_flags="-ss"
```

Bu iki `ss` uzaktaki sistemlerden bilgi alınmasını engelleyecek ve local sistemde hala aktif halde olmasını sağlayacaktır.

Bir sonraki asamada `inetd_enable` parametresinin `etc/rc.conf` dosyasında aktif olmasından (`inetd_enable="YES"`) emin olmaktır.

Eğer IP adresinizi ISP'nizin DHCP sunucusundan alıyorsanız `dhclient` (port 68) servisini açık bırakmalısınız eğer kapatırsanız IP adresi alamayacak ve dolayısıyla internet bağlantınızı sağlayamayacaksınız demektir.

Eğer `sockstat` çıktınızda bunun dışında açık bir port görürseniz `man rc.conf` komutu ile bu açık olan portların kapatılma yöntemlerini görebilirsiniz. Eğer burada da bulamazsanız bu büyük bir ihtimalle yüklediğiniz yazılımlar ile beraber gelen bir başlangıç script'i dir. Bu scriptleri görmek için aşağıdaki komutu kullanabilirsiniz:

```
cd /usr/local/etc/rc.d
```

Çoğu yazılım yüklenme sırasında kendini ".sample" sonu ile `rc.d` klasörüne atmaktadır. Bu sona sahip script'ler başlangıç sırasında dikate alınmayacaktır. Bu klasörde bulunan ".sh" sonlu dosyalar başlangıçta çalıştırılan dosyalar olduğundan bunların çalışmasını engellemek için .sh uzantısını .sample olarak değiştirmeniz yeterli olacaktır. Buna örnek olarak eğer sistemimde `snmpd` çalışıyorsa ve bu servisin başlangıçta çalışmasını istediğiniz şekilde engelleyebilirim:

```
cd /usr/local/etc/rc.d  
mv snmpd.sh snmpd.sh.sample  
killall snmpd
```

Bunun yanında sizi "işletim sistemi tanımlama" saldırılarından koruması için `/etc/rc.conf` dosyanıza ilk önce kernel'inizi `options TCP_DROP_SYNFIN` parametresini ekledikten ve kernel'inizi yeniden derledikten sonra bu parametreyi ekleyebilirsiniz:

```
tcp_drop_synfin="YES"
```

Sistemimize DOS saldırısı için kullanılacak ICMP redirect'i engellemek için eklenebilecek (daha fazla bilgi için [ARP and ICMP redirection games article](#). Sayfasına göz atabilirsiniz) diğer iki parametre ise şunlardır:

```
icmp_drop_redirect="YES"  
icmp_log_redirect="YES"
```

`icmp_log_redirect` opsiyonunu kullanırken dikkat etmeniz gereken nokta her icmp redirect durumunu log dosyasına eklediği için Dos saldırısı durumunda `/var/log` dosyanızın dolmasına yol açacaktır.

Guvenlik duvarinizi hazirlarken su parametreyi de kullanmaniz tum kapali port`lara gelen saldirilari da gorebilmenizi saglayacaktır:

```
log_in_vain="YES"
```

Diger bir parametre ise

```
accounting_enable="YES"
```

dir.Bu system dosyalarinizi duzenlemeye yardimci olacaktir. Bu konuda daha fazla bilgi icin `man sa` ve `man lastcomm` yardim dosyalarına bakabilirsiniz.

Son olarak fazla yer kaplamamasi acisindan devamlı islem yaptigimiz gecici dosya klasorumuzun her acilista temizlenmesini saglayacak olan su parametreyi kullanabiliriz:

```
clear_tmp_enable="YES"
```

Simdi isterseniz `/etc/rc.conf` dosyasini birakip sistemimizin guvenligi icin baska neler yapabilecegimize bakalim.Ben kisisel olarak kullanıcı sifrelerinin sifrelenmesinde kullanılan mekanizmayı, Blowfish algoritmasına degistirmeyi, daha hizli ve daha guvenli olmasını acisindan uygun gormekteyim.Bu konuda daha fazla bilgi icin [comparison of algorithms](#) sayfasina basvurabilirsiniz.

Eger bu tur seylere merakiniz var ise tavsiye edilecebilecek ikinci kaynak Blowfish`in programcisi tarafından hazirlanan [Cryptogram newsletter](#) `dir.

Blofish hash`lerini degistirmek icin `/etc/login.conf` dopsyasında `passwd_format` satirini asagidaki gibi degistirin:

```
:passwd_format=blf:\
```

Bundan sonra degisiklikleri kaydedip veritabanini tekrar yapilandirmak icjn:

```
cap_mkdb /etc/login.conf
```

komutunu kullanabiliriz. Daha sonra kullanicilarinizin sifrelerini tekrar degistirmeniz gerekecektir. Boylece her kullanıcı kendisine yeni algoritma ile sifrelenmiş bir sifre alabilecektir. Bunu su sekilde yapabilirsiniz:

```
passwd username
```

Bunu bitirdikten sonra `more /etc/master.passwd` komutunu verip tum sifrelere bir goz atin. Yeni alinan sifrelerin yeni algoritma kullandigi icin `$2` ile basladigini goreceksiniz.

```
more /etc/master.passwd
```

Son olarak `adduser` komutunun her kullanıcı eklendiğinde bu algoritmayı kullanmasını sağlamak için `/etc/auth.conf` dosyasında bulunan `crypt_default` satırını şu şekilde düzenlemeniz gerekecektir:

```
crypt_default=blf
```

Sisteminize girdiğinizde karşınıza gelen login ekranı öncesinde gözüken FreeBSD copyright bilgisini ve yararlı bilgileri farketmissinizdir. İste sistemize giren kişileri karşılayacak bu mesajları değiştirme yolu `motd` dosyasından geçmektedir.

İsteginize göre `etc/motd` dosyasını değiştirebilir bir atasozu veya bir söylem yerleştirebilirken buraya sisteminize giren kişilerin izinsiz olarak sistemi kullanmaları sonucunda başlarına ne gibi dertler acabileceğinizi belirten ufak bir notta ekleyebilirsiniz.

FreeBSD copyright dosyasını kaldıralım:

```
touch /etc/COPYRIGHT
```

Şimdi ise komut satırınızda yazılı olan parametreleri değiştirelim. Bunun için `/etc/gettytab` dosyası içinde

```
:cb:ce:ck:lc
```

İle başlayan satırı bulalım. `r\n\ \r\n\r\nr\n:n:` arasında bulunan parametreleri değiştirelim. Örneğin benim giriş ekranım şu şekilde görünmekte:

```
Uplink'e hoşgeldiniz.Nasil yardımcı olabilirim?  
login:
```

FreeBSD `motd` dosyanızı her acilista güncelleyip tekrar aynı bilgileri geriye yüklemeye çalışacağından bunu önlemek için şu parametreyi `/etc/rc.conf` içine ekleyebilirsiniz:

```
update_motd="NO"
```

Sizin dışınızda kimsenin sisteminize superkullanıcı (root) olarak girmesine gerek olmayacağından bunu da kısıtlamak mantıklı olacaktır. `/etc/ttys` içinde `tttyv0` ve `tttyv8` olmayacağından arasında bulunan tüm `secure` sözcüklerini `insecure` olarak değiştirmeniz fiziksel olarak bilgisayarınız karşısında bulunmadan hiçbir yerden root kullanıcı ile girmesine izin verilmeyecektir. Girmeye çalıştığınızda alacağınız mesaj "Login incorrect" olacaktır.

Eğer masaüstünüzde standart olarak gelen 9 terminalden daha az veya daha çok terminal kullanmak isterseniz `/etc/ttys` içinde bulunan `ttys` değerlerini "on" veya "off" şeklinde ayarlayarak kullanabilirsiniz. Bunun yanında `tttyv8` değerinin "off" olarak ayarlı olduğuna dikkat edin. Bu parametreyi "on" olarak ayarlarsanız X window acilista otomatik olarak başlatabilirsiniz.

Son olarak bakacagimiz yer ise hangi kullanicilarin, nereden sisteme girmelerine izin verdigimizi belirtebilecegimiz bir dosya olan `/etc/login.access` dosyasi.

Eger sistemimizi fiziksel olarak onunde bulunmak disinda her türlü dis baglantiiya kapatmak isterseniz asagidaki parametre onundeki `#` isaretini:

```
#-:wheel:ALL EXCEPT LOCAL .win.tue.nl
```

Ve `.win.tue.nl` parametresini kaldırarak asagidaki sekilde gorunmesini saglayin:

```
 -:wheel:ALL EXCEPT LOCAL
```

Eger sadece belli bir ip adresi olan bir sistemden sisteminize girmek istiyorsanız `.win.tue.nl` parametresini uzaktaki sisteminizin ip adresi veya ismi ile degistirin. Eger birkac yerden baglanmak isterseniz aralarinda birer bosluk birakarak bunlari ekleyebilirsiniz.

Eger sisteminize giris yapan bir veya iki kisi bulunuyorsa diger tum girisleri su sekilde onleyebilirsiniz:

```
 -:ALL EXCEPT kullanıcı1 kullanıcı2:ttv0 ttv1 ttv2 ttv3 ttv4
```

Buradaki `kullanici1` `kullanici2` isimlerini kendi kullanıcı isimleriniz ile degistirmeyi unutmayin!

Alternatif olarak kullanicilarinizi bir grup altinda toplayip o gruba izin verme sansiniz da bulunmakta. Bu ornek `ozgur`, `omer`, ve `ozkan` adinda uc kullaniciyi sisteminize ekleyecek ve bunlari da `ender` isimli grup altinda toplayacaktır. Bunun icin ilk olarak `/etc/group` dosyasina su parametreyi ekleyelim:

```
ender:*:100:ozgur,omer,ozkan
```

Kendi gurubunuzu eklediginizde dikkat edeceginiz nokta GID (bu ornek icin 100) baska bir grup icin kullanilmadigina emin olmaktir.

Daha sonra `etc/login.access` kismini asagidaki sekilde degistirin:

```
 -:ALL EXCEPT ender:ttv0 ttv1 ttv2 ttv3 ttv4 ttv5
```

Bu guruba kayitli tum kullanicilar ile giris yapmayi denedikten sonra baska bir kullaniciyi deneyiniz. "Permission denied" hatasi aliyorsanız sisteminizde yaptiginiz degisiklikler tam olarak calisiyor anlamina gelecektir

Iyi sanslar!

Ozgur Ozdemircili
ozgur@enderunix.org
<http://www.enderunix.org>
<http://www.enderunix.org/ozgur/blog>

KAYNAKLAR

[Dru Lavigne](#)`nin “Securing FreeBSD” yazisindan derlenmistir.Orjinal metne http://www.onlamp.com/pub/a/bsd/2003/07/24/FreeBSD_Basics.html adresinden ulasabilirsiniz.