

FreeBSD Ağ Uygulamaları ve Güvenlik

Murat Balaban

EnderUNIX Çekirdek Takımı Üyesi

murat@enderunix.org

4BSD Networking

- 25 yıl
- En sağlam, uyumlu ve “tamam” TCP/IP yığıtı
- Neredeyse bütün UNIX’ler ve hatta Windows bu kodu kullanır

```
[mb@x-wing murat]$ strings FTP.EXE | grep Cal  
@(#) Copyright (c) 1983 The Regents of the University of California.  
[mb@x-wing murat]$
```

4.2 BSD (1983)	First widely available release of TCP/IP.
4.3 BSD (1986)	TCP performance improvements.
4.3 BSD Tahoe (1988)	Slow start, congestion avoidance.
4.3 BSD Reno (1990)	TCP header prediction, SLIP header compression, routing table changes.
4.4 BSD (1993)	Multicasting, long fat pipe modifications.

- FreeBSD/NetBSD/OpenBSD 4.4 BSD (Lite) tabanlıdır

4.4 BSD-Lite'a FreeBSD eklentileri

- mbuf kümelerinin yoğun kullanımıyla soket ve TCP performansı artırıldı
- Paket alımı “connection hashing” yöntemiyle hızlandırıldı
- 100BT ve FDDI desteği
- LBL'den multicast kodu
- Paket Filtreleme ve Firewall yeteneği



FreeBSD 5.3 Networking Yenilikleri

- Fine-grained locking, daha çok SMP performansı
- Netgraph
- KQUEUE
- PFIL_HOOKS
- NDIS Binary uyumluluğu



FreeBSD 5.3 Networking Yenilikleri

...devam

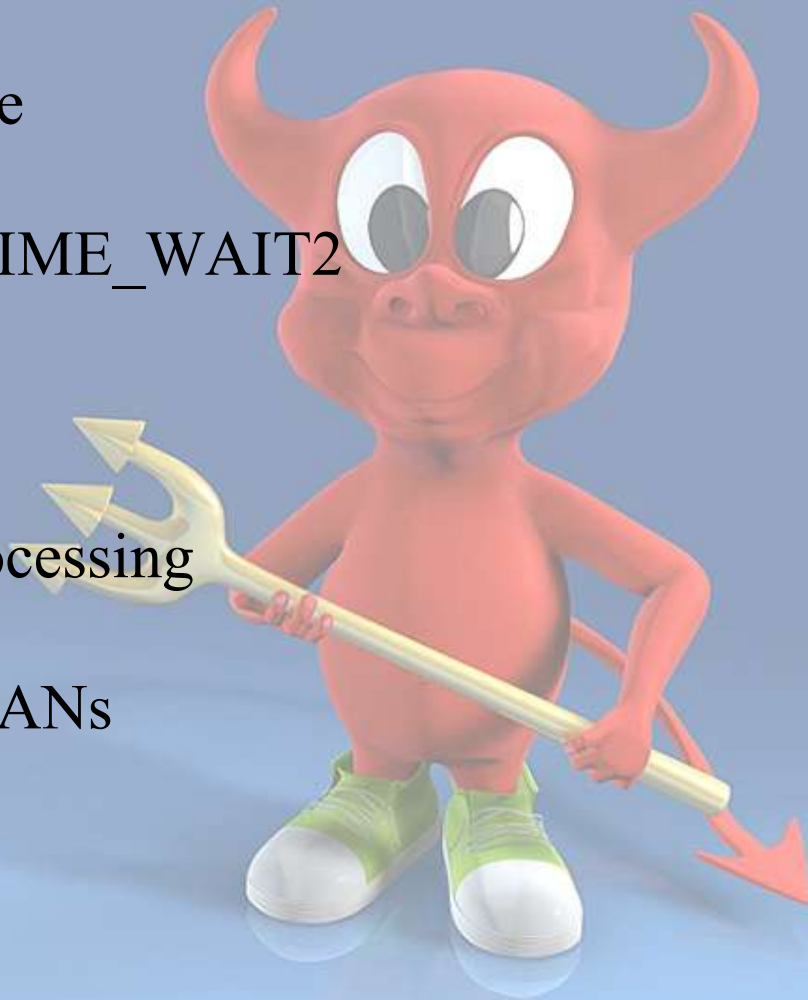
- POLLING
- IP Fastforward
- RFC3990 Increased Initial Congestion Window
- Inflight BW-delay limiter
- TCP SACK



FreeBSD 5.3 Networking Yenilikleri

...devam

- TCP Hostcache
- Compressed TIME_WAIT2
- Random IPID
- IP Options Processing
- Automatic VLANs



FreeBSD 5.3 Networking Yenilikleri

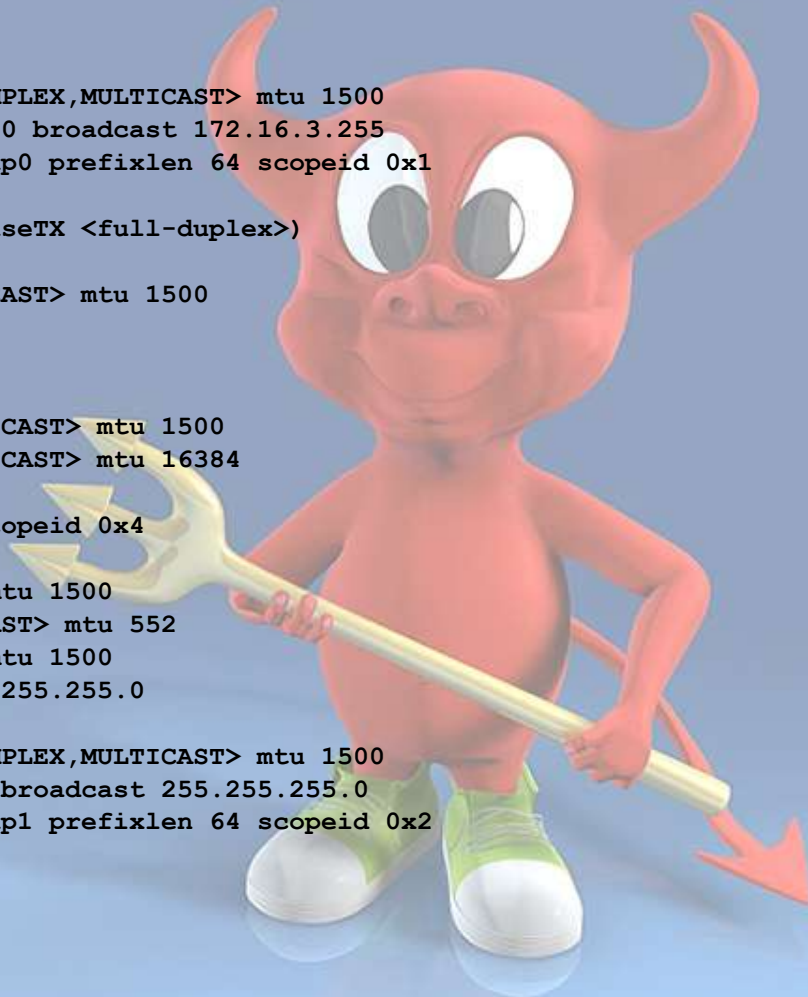
...devam

- Interface renaming
- Universal Memory Allocator
- PRCLONING
- Bluetooth netgraph module
- ATM netgraph module



FreeBSD 5.3 Networking Pratikleri: ifconfig

```
root@gediz:~# ifconfig
fxp0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    inet 172.16.0.2 netmask 0xfffffc00 broadcast 172.16.3.255
    inet6 fe80::290:27ff:fe2c:1310%fxp0 prefixlen 64 scopeid 0x1
    ether 00:90:27:2c:13:10
    media: Ethernet autoselect (100baseTX <full-duplex>)
    status: active
fxp1: flags=8802<BROADCAST,SIMPLEX,MULTICAST> mtu 1500
    ether 00:0b:cd:06:6d:71
    media: Ethernet autoselect (none)
    status: no carrier
lp0: flags=8810<POINTOPOINT,SIMPLEX,MULTICAST> mtu 1500
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
    inet6 ::1 prefixlen 128
    inet6 fe80::1%lo0 prefixlen 64 scopeid 0x4
    inet 127.0.0.1 netmask 0xff000000
ppp0: flags=8010<POINTOPOINT,MULTICAST> mtu 1500
sl0: flags=c010<POINTOPOINT,LINK2,MULTICAST> mtu 552
faith0: flags=8002<BROADCAST,MULTICAST> mtu 1500
root@gediz:~# ifconfig fxp1 10.0.0.1 255.255.255.0
root@gediz:~# ifconfig fxp1
fxp1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    inet 10.0.0.1 netmask 0xff000000 broadcast 255.255.255.0
    inet6 fe80::20b:cdff:fe06:6d71%fxp1 prefixlen 64 scopeid 0x2
    ether 00:0b:cd:06:6d:71
    media: Ethernet autoselect (none)
    status: no carrier
root@gediz:~#
```



FreeBSD 5.3 Networking Pratikleri:

netstat, arp

```
root@gediz:~# netstat -rn
Routing tables
```

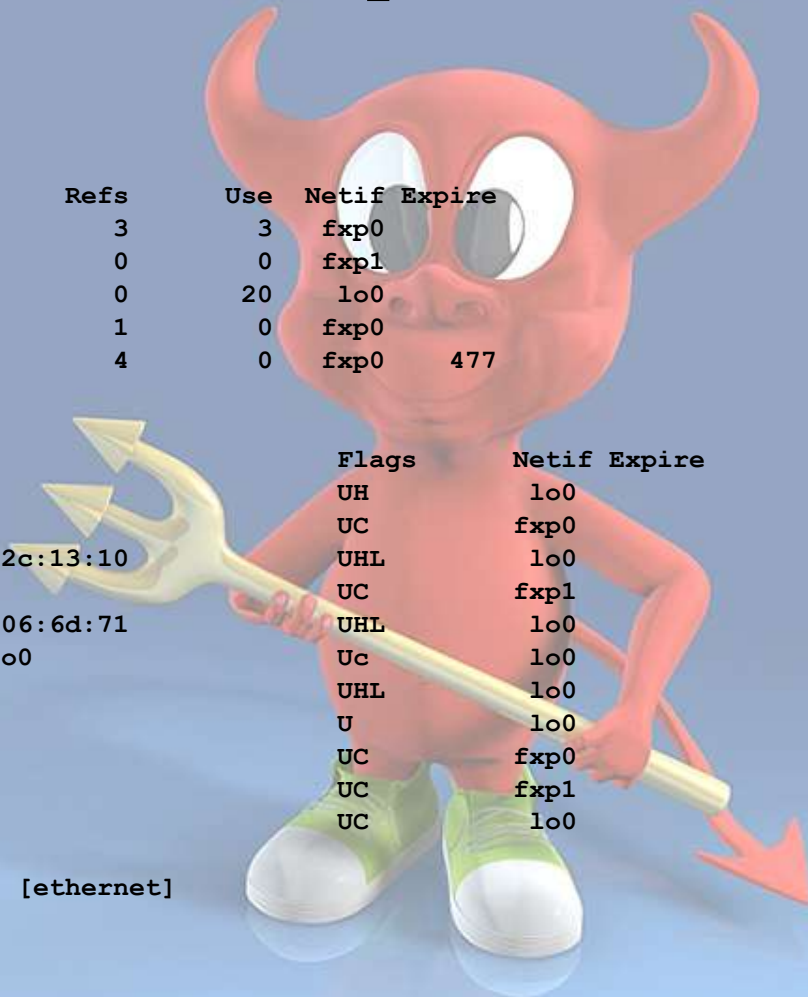
Internet:

Destination	Gateway	Flags	Refs	Use	Netif	Expire
default	172.16.0.1	UGSc	3	3	fxp0	
10	link#2	UC	0	0	fxp1	
127.0.0.1	127.0.0.1	UH	0	20	lo0	
172.16/22	link#1	UC	1	0	fxp0	
172.16.0.1	00:00:0c:07:ac:b8	UHLW	4	0	fxp0	477

Internet6:

Destination	Gateway	Flags	Netif	Expire
::1	::1	UH	lo0	
fe80::%fxp0/64	link#1	UC	fxp0	
fe80::290:27ff:fe2c:1310%fxp0	00:90:27:2c:13:10	UHL	lo0	
fe80::%fxp1/64	link#2	UC	fxp1	
fe80::20b:cdff:fe06:6d71%fxp1	00:0b:cd:06:6d:71	UHL	lo0	
fe80::%lo0/64	fe80::1%lo0	Uc	lo0	
fe80::1%lo0	link#4	UHL	lo0	
ff01::/32	::1	U	lo0	
ff02::%fxp0/32	link#1	UC	fxp0	
ff02::%fxp1/32	link#2	UC	fxp1	
ff02::%lo0/32	::1	UC	lo0	

```
root@gediz:~# arp -a
? (172.16.0.1) at 00:00:0c:07:ac:b8 on fxp0 [ethernet]
root@gediz:~#
```



FreeBSD 5.3 Networking Pratikleri: route

Default route:

```
root@gediz:~# route add default 172.16.0.1
add default: gateway 172.16.0.1
```

```
root@gediz:~# netstat -rn | grep defa
default          172.16.0.1      UGSc         3         0    fxp0
```

Net route:

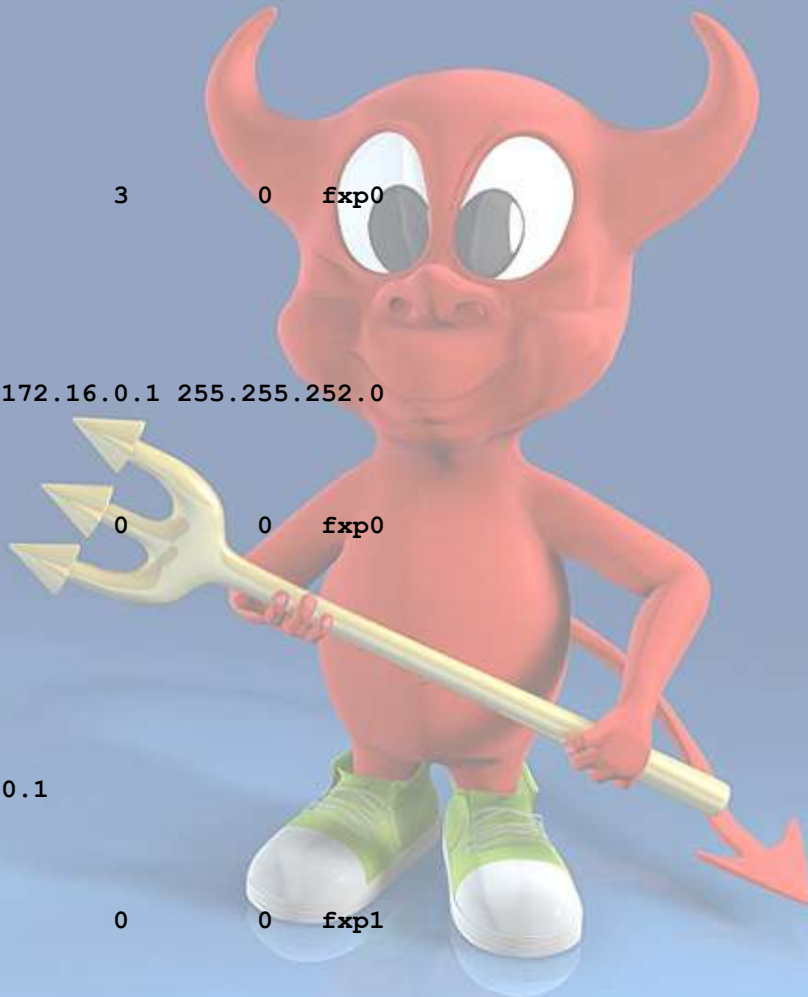
```
root@gediz:~# route add -net 100.100.100.0 172.16.0.1 255.255.252.0
add net 100.100.100.0: gateway 172.16.0.1
```

```
root@gediz:~# netstat -rn | grep "100.100"
100.100.100/22    172.28.0.1      UGSc         0         0    fxp0
```

Host route:

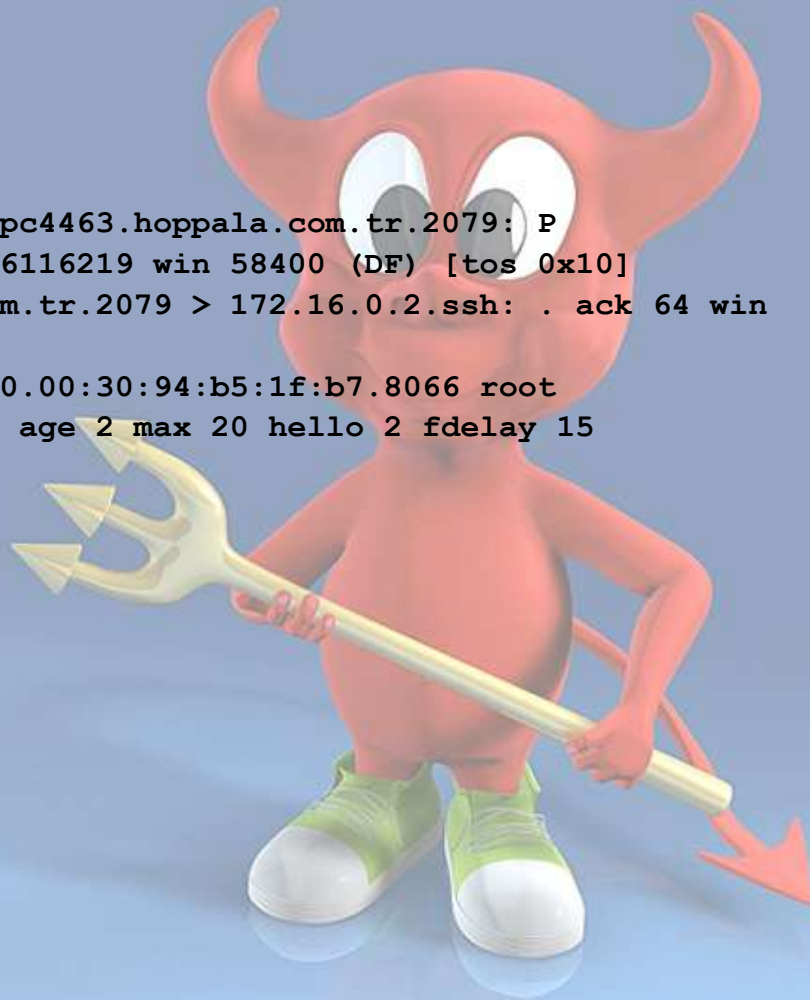
```
root@gediz:~# route add 111.111.11.11 10.0.0.1
add host 111.111.11.11: gateway 10.0.0.1
```

```
root@gediz:~# netstat -rn | grep "111.11"
111.111.11.11    10.0.0.1        UGHS         0         0    fxp1
```



FreeBSD 5.3 Networking Pratikleri: tcpdump

```
root@gediz:~# tcpdump -i fxp0
tcpdump: listening on fxp0
13:22:27.015220 172.16.0.2.ssh > pc4463.hoppala.com.tr.2079: P
3899699194:3899699258(64) ack 4136116219 win 58400 (DF) [tos 0x10]
13:22:27.191042 pc4463.hoppala.com.tr.2079 > 172.16.0.2.ssh: . ack 64 win
64799 (DF)
13:22:27.624981 802.1d config 8000.00:30:94:b5:1f:b7.8066 root
8000.00:05:9a:a5:e4:b7 pathcost 8 age 2 max 20 hello 2 fdelay 15
^C
15 packets received by filter
0 packets dropped by kernel
root@gediz:~#
```



FreeBSD 5.3 Networking Pratikleri:

/etc/rc.conf

```
----- /etc/rc.conf -----
ifconfig_fxp0="inet 172.16.0.2 netmask 255.255.252.0"
ifconfig_fxp0_alias0="inet 172.16.0.3 netmask 0xffffffff"
defaultrouter="172.16.0.1"
hostname="gediz.devel.enerunix.org"
----- /etc/rc.conf -----

root@gediz:~# sh /etc/netstart
Doing stage one network startup:
Doing initial network setup:.
fxp0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    inet6 fe80::290:27ff:fe2c:1310%fxp0 prefixlen 64 scopeid 0x1
    inet 172.16.0.2 netmask 0xfffffc00 broadcast 172.16.3.255
    ether 00:90:27:2c:13:10
    media: Ethernet autoselect (100baseTX <full-duplex>)
    status: active
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
    inet6 ::1 prefixlen 128
    inet6 fe80::1%lo0 prefixlen 64 scopeid 0x4
    inet 127.0.0.1 netmask 0xff000000
add net default: gateway 172.16.0.1
Additional routing options: TCP keepalive=YES.
Routing daemons:.
root@gediz:~#
```



FreeBSD 5.3 Networking Pratikleri: /stand/sysinstall arabirimi

/stand/sysinstall -> Configure -> Networking -> Interfaces -> fxp0

```
Host:                                Domain:
lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk  lqqqqqqqqqqqqqqqqqqqqqqqqqqqqk
xdiz.devel.enderunix.orgx          xevel.enderunix.orgx
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqj    mqqqqqqqqqqqqqqqqqqqqqqqqqqqj
IPv4 Gateway:                       Name server:
lqqqqqqqqqqqqqqqqqqqqqqqqqqqqk    lqqqqqqqqqqqqqqqqqqqqqqqqqqqqk
x172.16.0.1      x                  x172.16.100.100 x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqj    mqqqqqqqqqqqqqqqqqqqqqqqqqqqj
lqqqqq Configuration for Interface fxp1 qqqqqqqqq
x IPv4 Address:                     Netmask:
x lqqqqqqqqqqqqqqqqqqqqqqqqqqqqk  lqqqqqqqqqqqqqqqqqqqqqqqqqqqqk
x x172.16.0.2      x                x255.255.252.0 x
x mqqqqqqqqqqqqqqqqqqqqqqqqqqqqj  mqqqqqqqqqqqqqqqqqqqqqqqqqqqj
x Extra options to ifconfig:
x lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk
x x                                x
x mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
x
x      lqqqqqqk                    lqqqqqqqqqqqqk
x      x OK x                      x CANCEL x
x      mqqqqqqqj                   mqqqqqqqqqqqqj
x
```

FreeBSD 5.3 Networking Pratikleri:

PPP (Dialup Internet)

- **Seri modem**

COM1 -> /dev/ttys0 /dev/cuaa0

COM2 -> /dev/ttys1 /dev/cuaa1

- /

etc/ppp/ppp.conf

```
set device /dev/ttyS0
```

```
set speed 115200
```

```
set timeout 180
```

```
set phone 145
```

```
set authname kullaniciadi@ttnet
```

```
set authkey dialupsifre
```

```
set ifaddr 10.0.0.1/0 10.0.0.2/0 255.255.255.0 0.0.0.0
```

```
enable dns
```

```
add default HISADDR
```



FreeBSD 5.3 Networking Pratikleri:

PPP (ADSL) PpOE

default:

```
set log Phase Chat LCP IPCP CCP tun command  
ident user-ppp VERSION (built COMPILATIONDATE)
```

```
set device PpOE:x11:ppp  
set speed sync  
set mru 1492  
set mtu 1492  
set ctsrts off  
enable lqr  
set lqrperiod 5  
set redial 15 28800  
set reconnect 15 28800  
enable dns  
add default HISADDR
```

tttnet:

```
set cd 5  
set dial  
set login  
set timeout 0  
set authname kullaniciadi@tttnet  
set authkey 1234567  
set ifaddr 10.0.0.1/0 10.0.0.2/0 255.255.255.0 0.0.0.0
```



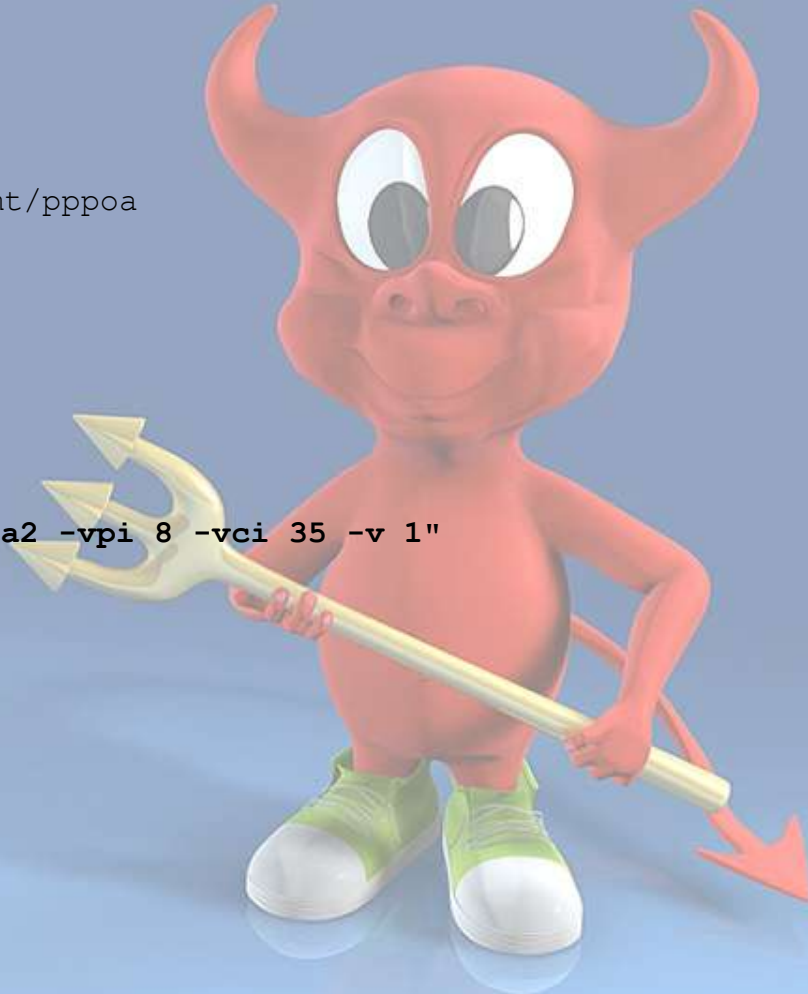
FreeBSD 5.3 Networking Pratikleri:

PPP (ADSL) PPOA

```
root@gediz ~# cd /usr/ports/net-mgmt/pppoa
root@gediz pppoa# make install
```

adsl:

```
set authname kullaniciadi@ttnet
set authkey sifre
set device !"/usr/local/sbin/pppoa2 -vpi 8 -vci 35 -v 1"
accept chap
set speed sync
set timeout 0
enable lqr
set lqrperiod 5
set redial 15 10000
set dial ""
add default HISADDR
enable dns
```



FreeBSD 5.3 Networking Pratikleri: Firewalling / NAT

```
root@gediz:~# sysctl -w net.inet.ip.forwarding=1
net.inet.ip.forwarding: 0 -> 1
root@gediz:~#
```

1. IPFW - NATD
Luigi Rizzo
3. IPFILTER
Darren Reed
6. PF - ALTQ
OpenBSD Project



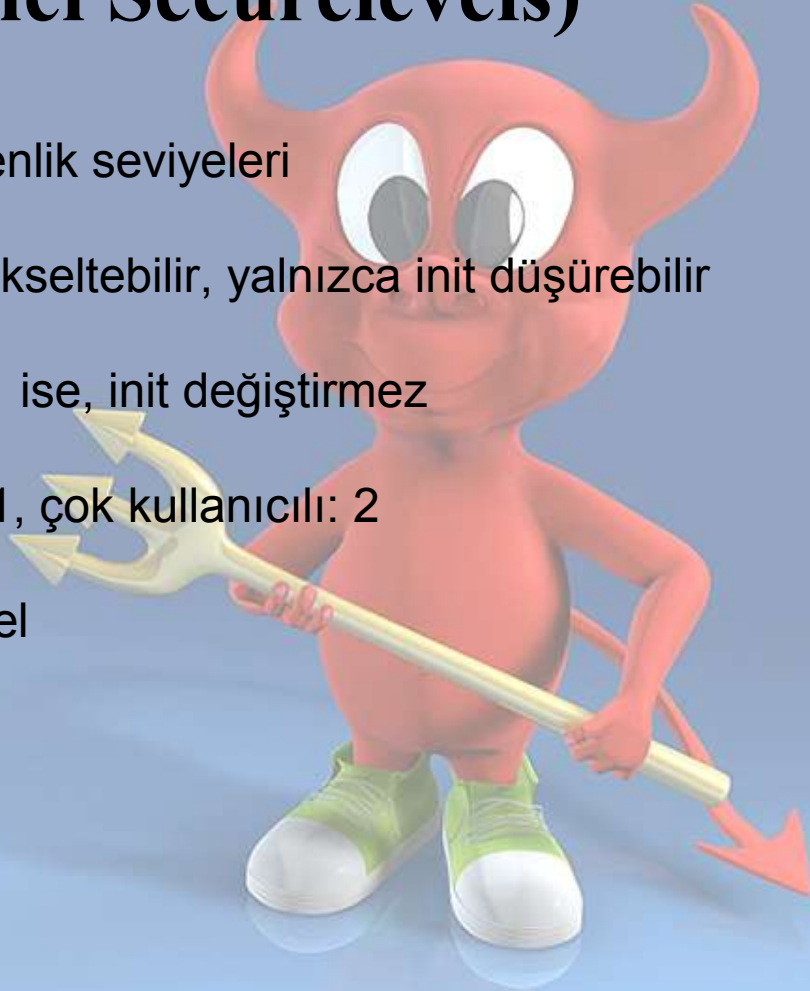
FreeBSD 5.3 Güvenlik

- The FreeBSD Security Officer
security-officer@freebsd.org
Jacques Vidrine nectar@freebsd.org
- The FreeBSD Security Team
Jacques Vidrine
Dag-Erling Smorgrav
Robert Watson
Warner Losh
- The FreeBSD Security List
security-announce@freebsd.org
- The FreeBSD Security Web
<http://www.freebsd.org/security/>



FreeBSD 5.3 Güvenlik Çekirdek Güvenlik Seviyeleri (Kernel Securelevels)

- -1 den 2'ye kadar güvenlik seviyeleri
- Her proses seviyeyi yükseltebilir, yalnızca init düşürebilir
- İlk güvenlik seviyesi -1 ise, init değiştirmez
- Değilse, tek kullanıcı: 1, çok kullanıcı: 2
- sysctl : kern.securelevel



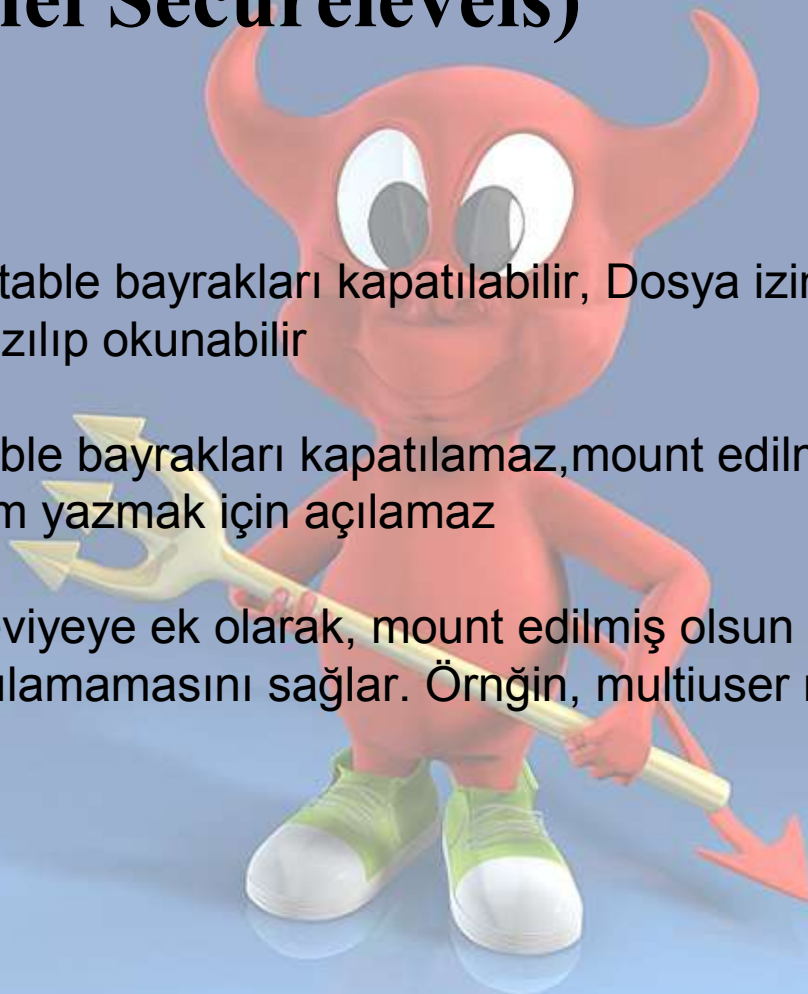
FreeBSD 5.3 Güvenlik Çekirdek Güvenlik Seviyeleri (Kernel Securelevels)

-1: En güvensiz seviye

0 : Güvensiz seviye: immutable bayrakları kapatılabilir, Dosya izinlerine bağlı olarak, bütün aygıtlar yazılıp okunabilir

1 : Güvenli seviye: immutable bayrakları kapatılamaz, mount edilmiş disk aygıtları /dev/mem ve /dev/kmem yazmak için açılmaz

2 : En güvenli seviye: 1. Seviyeye ek olarak, mount edilmiş olsun ya da olmasın, disklerin yazmak için açılmamasını sağlar. Örneğin, multiuser mode'da newfs çalışmaz.



FreeBSD 5.3 Güvenlik

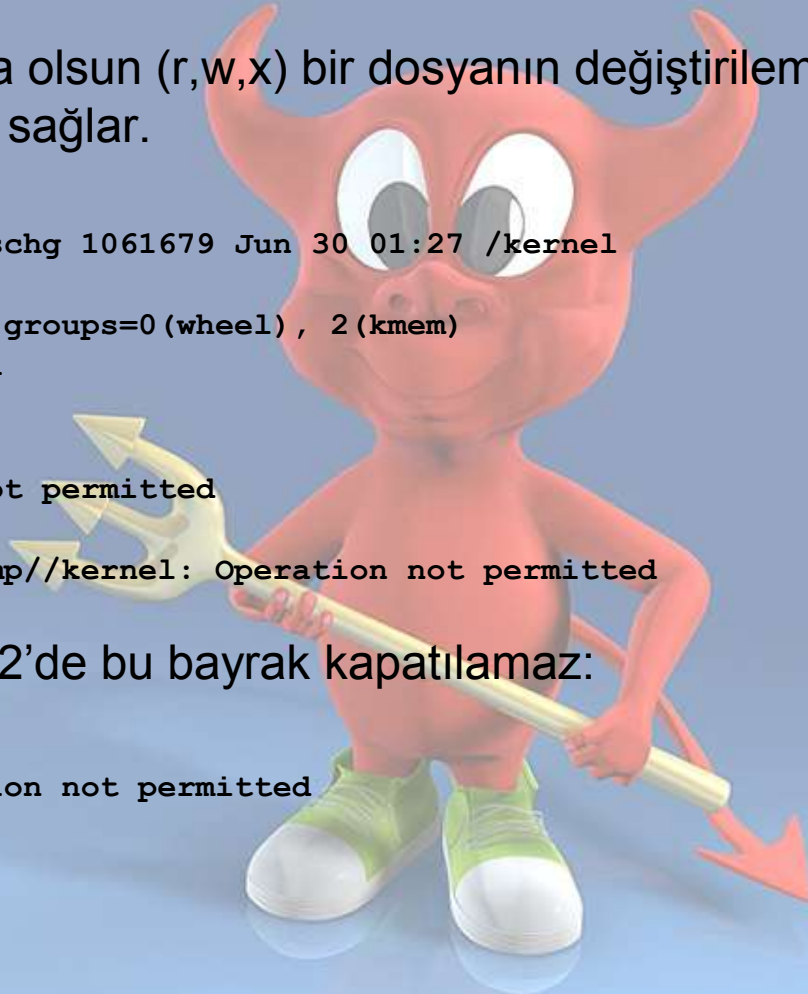
Değiştirilemez Bayrağı (Immutable Flag)

- Dosya izinleri ne olursa olsun (r,w,x) bir dosyanın değiştirilemez olarak belirlenmesine olanak sağlar.

```
# ls -lo /kernel
-r-xr-xr-x 1 root wheel schg 1061679 Jun 30 01:27 /kernel
# id
uid=0(root) gid=0(wheel) groups=0(wheel), 2(kmem)
# sysctl kern.securelevel
kern.securelevel: 2
# rm -rf /kernel
rm: /kernel: Operation not permitted
# mv /kernel /tmp/
mv: rename /kernel to /tmp//kernel: Operation not permitted
```

- Güvenlik seviyesi 1 ve 2'de bu bayrak kapatılamaz:

```
# chflags noschg /kernel
chflags: /kernel: Operation not permitted
```



FreeBSD 5.3 Güvenlik VPN, IPSec

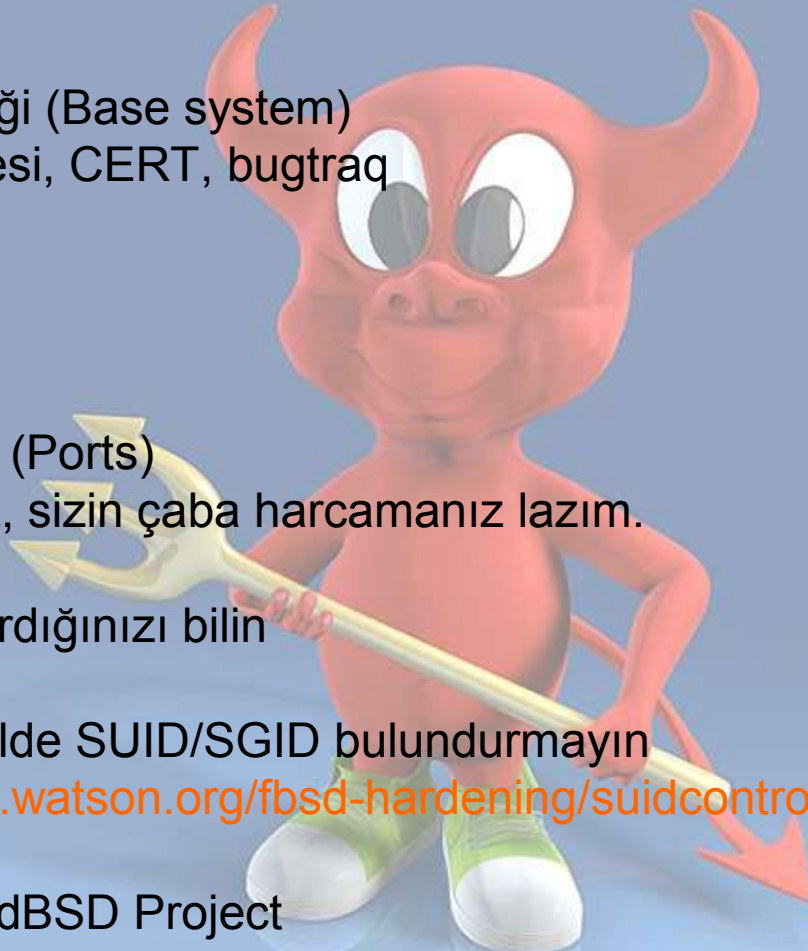
- GIF tüneli
gifconfig
- Dialup VPN
PPTP, mpd
- IPSec
isakmp, racoon



FreeBSD 5.3 Güvenlik

Sürekli güncel kalın

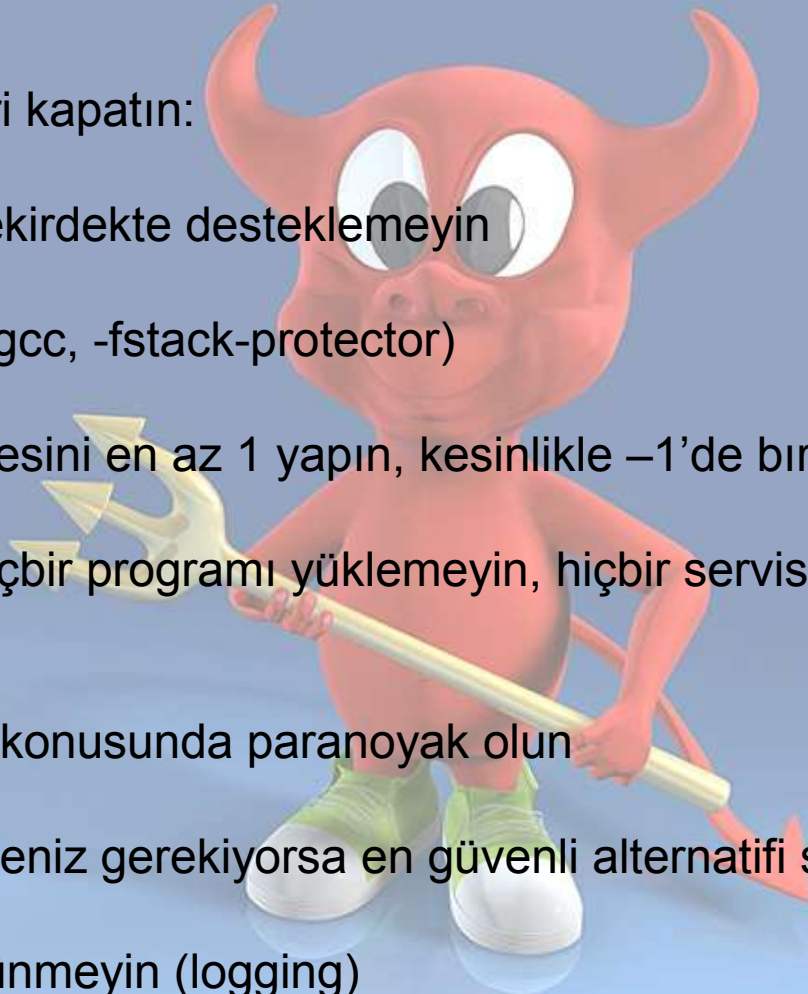
- Temel sistem güncelliği (Base system)
security-announce listesi, CERT, bugtraq
cvsup, make world
- Security Branch
- Port sistemi güncelliği (Ports)
FreeBSD takip etmez, sizin çaba harcamanız lazım.
- Sisteminizde ne çalıştırdığınızı bilin
- İhtiyacınız olmadığı halde SUID/SGID bulundurmayın
suidcontrol <http://www.watson.org/fbsd-hardening/suidcontrol.html>
- DARPA funded TrustedBSD Project
MACs, kernel tokens, POSIX 1.e standart security extensions



FreeBSD 5.3 Güvenlik

Bazı tavsiyeler

- options NO_LKM
İhtiyaç yoksa, LKM'leri kapatın:
- İhtiyaç yoksa BPF'i çekirdekte desteklemeyin
- Protector patch (yeni gcc, -fstack-protector)
- Sistem güvenlik seviyesini en az 1 yapın, kesinlikle -1'de bırakmayın
- İhtiyacınız olmayan hiçbir programı yüklemeyin, hiçbir servisi açmayın
inetd !!!
- Özellikle ağ servisleri konusunda paranoyak olun
- İlla bir ağ servisi vermeniz gerekiyorsa en güvenli alternatifi seçin
- Kayıt tutmaktan yüksünmeyin (logging)



FreeBSD 5.3 Güvenlik

Bazı tavsiyeler

- Blackhole
net.inet.tcp.blackhole=2
net.inet.udp.blackhole=1
- log_in_vain
sysctl -w net.inet.tcp.log_in_vain=1
sysctl -w net.inet.udp.log_in_vain=1
- RC.CONF:
icmp_log_redirect="YES"
icmp_drop_redirect="YES"
tcp_drop_synfin="YES" (options TCP_DROP_SYNFIN)



SORULAR???

