OpenBSD ve PF Kullanımı

Huzeyfe ÖNAL
huzeyfe@enderunix.org

Sunum Planı

- BSD'ler?
- Özelde OpenBSD...
- OpenBSD Kullanımı
- OpenBSD Ağ ayarları
- Paket Yönetim Sistemi
- Packet Filter(PF) ve Kullanımı

BSD Ailesi

- Bsd Nedir?
- Günümüzdeki durumu
- Günümüzdeki *BSD Çeşitleri
- Lisans politikası
- Kullanım Alanları

FreeBSD

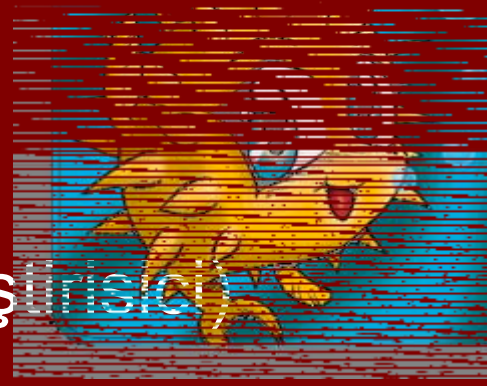
- FreeBSD 4.4BSD-Lite tabanlı
- Tarihçesi
- En yaygın kullanılan BSD sürümü
  -Dökümantasyonu bol
- “The power to serve “ sloganına uygun
- Geniş Mimari desteği
- Kolay ve Esnek kullanım

NetBSD

- OpenBSD'nin atası sayılabilir
- Sağlam bir ekip
- Temiz kod
- Diğer *BSD ler ile kod paylaşımı
- Olabildiğince fazla mimari hedefi

  Tost makinenizde bile çalışabilir ☺
- acorn32 ,algor, alpha,amd64, amiga, amigappc, arc, arm32 , atari, mvme68k, mvmeppc, netwinder, news68k, newsmips, next68k, ofppc, pc532, playstation2, pmax, pmppc, prep, sandpoint, sbmips, sgimips, shark, sparc ....

OpenBSD



- **Theo de Raadt** (eski bir NetBSD geliştiricisi)
- Güvenlik amaçlı bir proje
- Özgür, açık, standartlara uyumlu
- BSD Lisansı ile sorunsuz kod dağıtımı
- Sorunlara farklı yaklaşım

  “a” kodunda bir sorun varsa tüm kodu bu sorun için tara...
- Devamlı kod kontrolü
- Güvenlik altyapısının geliştirimi için yeni araştırma ve sonuçlarını paylaşma

OpenBSD....

- Sistem yapısı Linux'dan farklı
  OpenBSD!="kernel"
- 15 mimari için sorunsuz destek
- Sürüm zamanları belirli
- Aktif ve genişleyen bir topluluk
- Gelişmiş paket yönetim sistemi
- SMP desteği(şimdilik i386 & amd64 için)
- Temiz kod, temiz dökümantasyon
  -Man sayfaları, FAQ., e-posta listeleri

OpenBSD sürümleri.

- Release: Orjinal CD ile birlikte dağıtılan sürüm.
- Stable: Release + çeşitli güvenlik ve performans eklentileri.
- Current: Geliştiricilerin üzerinde çalıştığı sürüm. Bir sonraki sürümün temeli
- Geriye yönelik destek...

  -3.6 çıkınca 3.4 bitiyor

Kurulumda Dikkat Edilecek hususlar

- Sunucu kurulumu
- Deneme/masaüstü kurulumu
- Donanım uyumluluğu

  -http://openbsd.org/plat.html mimariye uygun donanım listesi
- Kurulum Yöntemi

  ftp, http, cdrom, fat/ext2 partition üzerinden, NFS*
- Dağıtım seti seçimi

Dağıtım setleri

- Kurmak istediğiniz bileşenleri seçmek için kullanılır
- **Bsd**: Sistemin çekirdeği, bu paket olmadan sisteminiz boot etmeyecektir ->Gerekli

  bsd.mp SMP desteği için.
- **baseXX.tgz**: OpenBSD nin çekirdek programlarını oluşturur, /bin, /sbin, /usr/bin, and /usr/sbin dizinleri. ->gerekli
- **etcXX.tgz** /etc/ dizini ve içerisindeki çeşitli dosyaları içerir /var/log dizini ve /root dizini gibi sistemin çalışmasını sağlayan önemli dizin ve dosyalar ->Gerekli
- **manXX.tgz** : baseXX.tgz ve etcXX.tgz paketi ile birlikte gelen paketlere ait man sayfaları
- **compXX.tgz**:Çeşitli derleyici araçlar ve bunlara ait man sayfaları

Dağıtım setleri

- **miscXX.tgz**: Daha çok masaüstü sistem için gerekli paketleri içeren bir dağıtım paketidir.
- **xbaseXX.tgz** : X sisteminin çalışması için gereken başlıklar, kütüphaneler, programları
- **xservXX.tgz** : X için gerekli ekran kartı sürücülerini barındırır

- **xshareXX.tgz**: X sistemi hakkında çeşitli bilgilendirmelerin bulunduğu paket seti.
- Seçmek için **+dağıtım_seti**, ya da **–dağıtım_seti** kullanılabilir
- Kurulum için gerekli olmayan paketler sonradan da kurulabilir

Kurulum Sonrası Genel Ayarlar

- man afterboot(8)
- Yetkisiz Kullanıcı ekleme

  - adduser(8)
- Uzaktan erişimi kısıtlamak

  kullanıcıyı wheel grubuna dahil etme

  sshd_config
- Root yetki eksiltme

  -sudo kullanımı

#rm * copluk ☺

Kurulum Sonrası Genel Ayarlar...

- Kullanılacak Klavye düzenini ayarlamak

#kbd -l |grep "tr"

us.swapctrlcaps
jp.swapctrlcaps
fr.swapctrlcaps
be.swapctrlcaps
us.swapctrlcaps.dvorak
us.swapctrlcaps.iopener
tr
tr.nodead

kbd tr
keyboard mapping set to tr

OpenBSD Ağ Ayarları

- Ağ arabirimi tanınmış mı?

  #dmesg

fxp0 at pci0 dev 10 function 0 "Intel 82557" rev 0x0c: irq 5, address 00:02:b3:2b:10:f7 inphy0 at fxp0 phy 1: i82555 10/100 media interface, rev. 4

- Ağ bilgilerini atama
- Aktif hale getirme
- Değişiklik yapma

Ethernet arabirimi

- Markaya göre isim.
- Eth0, eth1 değil, rl0 fxp0, fxp1

#ifconfig rl0 ...

#ifconfig –a

- Kayıtların kalıcı olması için /etc/hostname.arabirim_Adı

Örnek;

fxp için /etc/hostname.fxp0 dosyası

rl0 için /etc/hostname.rl0

Ethernet Arabirimi

- Hostname.arabirim dosya formatı

  inet ipaddress netmask broadcastaddress options

- DHCP'den Ip aldırmak

  #echo dhcp >/etc/hostname.fxp0

  #dhclient arabirim_adı

- Ethernet kartına alias tanımlamak

  #ifconfig rl0 inet alias 192.168.0.39 netmask 255.255.255.255

#ifconfig –A

- Aynı ağda alias eklenirse netmask /32 olmalı
- Aliasları silmek

#ifconfig rl0 delete

Ethernet arabirimi...

fxp1 :
flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500 media: Ethernet autoselect (10baseT) status: **active** inet6 fe80::202:b3ff:fe63:e3ec%fxp1 prefixlen 64 scopeid 0x2 inet 6.3.4.127 netmask 0xfffff800 broadcast 68.43.111.255

- Değişiklikleri aktif hale getirmek

#reboot

#sh /etc/netstart

Ağ yapılandırması...

- Geçici yönlendirme tanımlama
  #route add –net 192.168.1.0 netmask ...
  #route del –net ...
- Kalıcı yönlendirme tanımlama
- Varsayılan çıkış kapısı
  #echo 10.10.10.1 > /etc/mygate
- kalıcı olması için /etc/mygate
- IP Forwarding

#net.inet.ip.forwarding=1 # 1=Permit forwarding (routing) of packets

#net.inet6.ip6.forwarding=1

sysctl net.inet.ip.forwarding=1 net.inet.ip.forwarding: 0 -> 1

Kalıcı yönlendirme tanımlama

- Özel bir dosya yok
- /etc/routes oluşturulur

  [-net | -host] hedef geçityolu

  şeklinde tanımlar girilir.
- /etc/netstart ‘a ek bölüm girilerek kolaylık sağlanır

```
if [ -f /sbin/route ]; then if [ -f /etc/routes ]; then cat
 /etc/routes | while read line do /sbin/route add $line done
 fi else echo "$0: /sbin/route does not exist" exit 1 fi
```

Ağ Ayarları

- Yönlendirme tablosunu okuma

 # netstat -rn -f inet

Routing tables

Internet:

Destination	Gateway	Flags	Refs	Use	Mtu	Interface
default	22.1.1.8	UGS	1	146039	-	em0
10.99.99/24	link#2	UC	1	0	-	em1
127.0.0.1	127.0.0.1	UH	0	5899	33224	lo0
224/4	127.0.0.1	URS	0	0	33224	lo0

#route show

Bilgisayar ismi ve dns sunucu tanımlama

- /etc/myname
- /etc/resolv.conf

-Nameserver

nameserver 10.10.10.10

-Domain

domain enderunix.org

- /etc/hosts

ip adresi hostismi_uzun host ismi

10.10.10.1 people.enderunix.org people

- /etc/host.conf

order hosts,bind ...

OpenBSD Sistem yapılandırma Dosyaları(/etc)

- */etc/changelist*
- */etc/daily*
- */etc/fstab*
- */etc/ftpchroot*
- */etc/ftpusers*
- */etc/master.passwd*
- */etc/mk.conf*
- */etc/syslog.conf*

/etc/...

- /etc/pf.conf
- /etc/rc.conf
- /etc/netstart
- /etc/man.conf
- /etc/shells
- /etc/ssh/
- /etc/ssl/
- /etc/sysctl.conf
- .....

Paket Yönetim Sistemi

- Klasik kaynak koddan kurulum
  ./configure&&make&&make install
- Hazır derlenmiş paketler
- pkg_add(1)
- pkg_create(1)
- pkg_delete(1)
- pkg_info(1)
- ftp, http, disk üzerinden kurulum

Paket yönetim sistemi

- Port ağacı?
- Port sistemi kurulumu
- ftp ftp://ftp.openbsd.org/pub/OpenBSD/3.6/ports.tar.gz

  # cp ports.tar.gz /usr

  # cd /usr;

  #tar xzf ports.tar.gz
- Port ağacında arama
- make search key=“nmap"

Paket yönetim sistemi

- Porttan paket kurulumu

#cd /usr/ports/net/mtr

#make install

- Kurulum seçenekleri için

$ make show=FLAVORS

no_x11

$ env FLAVOR="no_x11" make

Packet Filter(PF)

- IPF'in Lisans sorunu ve yeni bir arayış
- OpenBSD 3 ile birlikte PF(packet filter)
- Anlaşılabilir kural dizgesi
- Esnek paket filtreleme
- Layer 2 paket filtreleme
- NAT(snat/dnat/binat)işlemleri
- Trafik kontrolü
- Yük dengeleme

PF

- Açılışta aktif hale getirmek

  /etc/rc.conf

  pf=YES
- Tüm yapılandırma için tek dosya

  /etc/pf.conf
- Pfctl ile anlık kontrol

  pfctl –e

  pfctl –d

  pfctl –s nat
- Kural tablosunu yükleme

  pfctl –f /etc/pf.conf

/etc/pf.conf

- Belirli bir düzende olmalı

  Makrolar

  Tablolar

  Seçenekler

  Trafik normalleştirme

  Bandwith kontrolü

  NAT

  RDR

  Paket filtreleme
- Sıralamada hata olursa kurallar yüklenmez

Kural yazımı

- Son uyan kazanır!
  -quick önemli...
- Pass in log on rl0 proto tcp from any to 12.12.13.14 port 23 keep state
- ! İle tersleme yapılabilir
- Tablolar, listeler kullanılabilir
- Öntanımlı olarak heryerden heryere geçiş var...

Makrolar

- Programlama dillerindeki değişkenler gibi esnek kural yazımı sağlar

```
dis_ag="fxp0"
dmz_ic="rl0"
guvenli_ag="192.168.0.0/24"
block in log on $dis_ag from $dmz_ic
```

- Benzer özellikleri liste halinde kullanabilme

```
guv_port="{21,22,80}"
yasak_port="{445 137 139}"
```

Tablolar

- Listelere benzer
- Listelerden oldukça performanslı
- Anlık kayıt eklenip silinebilir

table <spam_yap> {1.2.3.4, 4.5.6.7 }
Table <rfc1918> {10.0.0.0/8, 176.16.0.0/12, 192.168.0.0/16 }
Table <ban_ip> file “/etc/banned.list”
Table <res> file “/etc/res1” file ”/etc/res2”
#cat /etc/banned.list
1.2.3.4
5.6.7.8
9.10.11.12
Yahoo.com

block in log on $dis_Ag from <spam_yap>

Paket Filtreleme

- Pass
- Block

block drop in all

block return-rst in all /tcp-rst, icmp port unreachable

pass in on fxp0 proto tcp from any to 100.100.100.3 port 22

- Değişken Ip adresleri için arabirim tanımlanabilir.

Block in log on $ext_if

nat

sysctl net.inet.ip.forwarding=1

- Nat on dis_if from ic_ag to any -> dis_if
- Nat on dis_if from 10.1.2.0/24 to any -> 100.101.102.103
- DHCP den ip aliyorsa

nat on fxp0 from 192.168.1.0/24 to any -> (fxp0)

!!Filtrelemenin tersine ilk uyan kazanır...

- Hariç bırakma

no nat on fxp0 proto tcp from 192.168.1.0/24 to any

RDR

- **rdr on** *dis_if* **proto** protokol **from** kaynak-*ip* **to** *public-ip* **port** *public- port* -> hedef-ip **port** içerdeki-*port*
- rdr on fxp0 proto tcp from any to 29.69.18.18 port 2000 -> 192.168.1.20 8 port 22
- RDR kuralları nat kurallarından sonra gelmeli
- rdr on fxp0 proto tcp from any to 29.69.18.18 port 1024:65535 -> 192.168.1.200 port 1024

Pf...

- Yük dengeleme
- Bandwith ayarlaması
- Log takibi

  -pflogd
- Log izleme

/var/log/pflog

#tcpdump -n -t -r /var/log/pflog

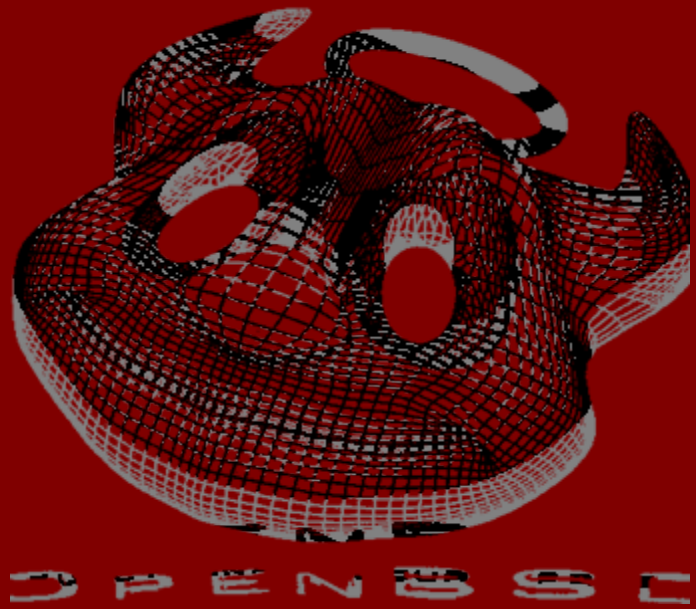
Anlık izleme

#tcpdump –i pflog0

#pftop

Kaynaklar

- http://www.openbsd.org
- http://www.undeadly.org
- http://www.bsdnews.com
- http://www.google.com/bsd
- http://www.enderunix.org
- http://www.huzeyfe.net/openbsd



Sorular

?