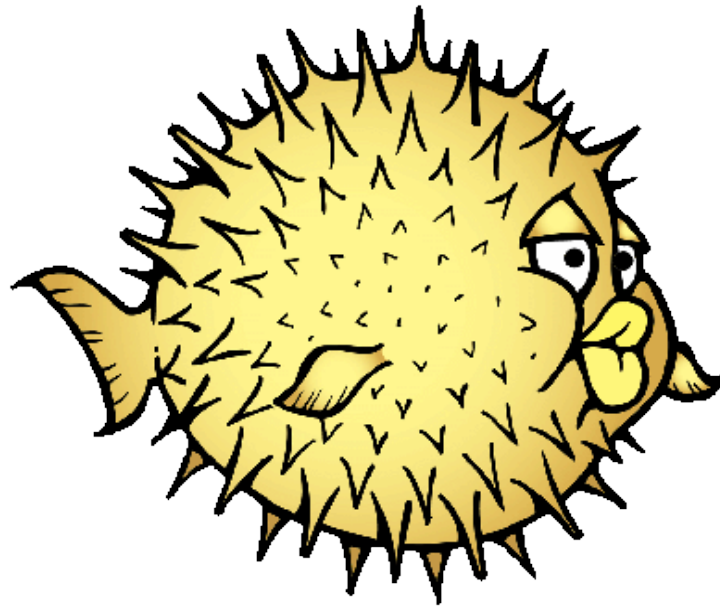


**OpenBSD**



***Open*BSD**

**Introducción a OpenBSD  
- secure by default -**

Autor: Hernán Costante – [hdc \[at\] openbsd.org](mailto:hdc@openbsd.org)



**OpenBSD**

**Que es OpenBSD?**

OpenBSD???

Pero de qué me estas  
hablando querido?



**OpenBSD**

## Que es OpenBSD?

- ★ Sistema Operativo tipo BSD
- ★ Multiplataforma (intel, amd, arm, sparc, digital, sgi, motorola, mac, hp, zaurus y landisk entre otros)
- ★ Basado en NetBSD
- ★ Foco en la seguridad y la criptografía
- ★ Emulación de binarios de SVR4 (Solaris), FreeBSD, SunOS, HPUX, BSD/OS y GNU/Linux
- ★ Los man están muy completos



**OpenBSD**

## Que es OpenBSD?

- ★ Instalación minimalista (así se logró que sólo tuviera 2 bugs remotos en mas de 10 años!)
- ★ Seguridad de código proactiva (se somete el código a constantes auditorías)
- ★ Sus principales usos (o los más conocidos) son como firewall (usando PF) y como terminador de túneles VPN (IPSec nativo en el kernel)

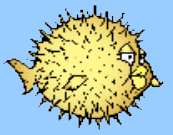


**OpenBSD**

# Que es OpenBSD?

- ★ El núcleo del proyecto se radica en Canada, así que no tiene restricciones de criptografía
- ★ Las nuevas versiones se liberan los 1ros de Mayo y los 1ros de Noviembre (cada 6 meses)
- ★ Versión actual 4.2
- ★ Su mascota se llama Puffy y es un pez globo (Pufferfish)... (y multifacético)





**OpenBSD**

**Un Poco de Historia**

# Sobre OpenBSD



**OpenBSD**

## Un Poco de Historia

- ★ En 1994, Theo de Raadt, debido a diferencias filosóficas con los otros fundadores de NetBSD, decidió fundar su propio sistema operativo. Basado en la seguridad, objetivo principal pero no el único.  
Así, en 1995 funda OpenBSD y el 1ro de Julio de 1996 lanza el primer release...  
OpenBSD 1.2



**OpenBSD**

## Un Poco de Historia

- ★ Según relevamientos realizados en Septiembre de 2001 OpenBSD es el 2do sistema operativo BSD más utilizado luego de FreeBSD (jo! por encima de NetBSD!)
- ★ Desde 2001 se comienza una limpieza de licenciamiento, dejando casi solamente código con licencia BSD, las herramientas con otras licencias son re desarrolladas con licencia BSD



**OpenBSD**

## Un Poco de Historia

- ★ En Junio de 2002 Mark Dawn de Internet Security Systems encuentra el primer bug remoto en la instalación por defecto en OpenSSH
- ★ El 13 de Marzo de 2007 el personal de Core Security Technologies (los cuales se basan en OpenBSD para algunos de sus productos de seguridad) encuentra el segundo bug remoto en la instalación por defecto en IPv6



**OpenBSD**

## Un Poco de Historia

- ★ El 25 de Julio de 2007 se anuncia “OpenBSD Foundation”, asociación sin fines de lucro con el fin de solucionar los problemas con las donaciones (hasta el momento se realizaban a nombre de Theo)



**OpenBSD**

**Instalación**

Ahora sí, que  
comience la acción



**OpenBSD**

## Instalación

- ★ Instalación por consola (modo texto)
- ★ Muy compleja a simple vista
- ★ En un par de instalaciones todo se vuelve mas fácil y sencillo
- ★ No tiene boot manager, así que si se quiere compartir el equipo con otro sistema operativo se debe utilizar el boot manager de ese (ej. Grub)



**OpenBSD**

## Instalación

- ★ La instalación se puede realizar de las siguiente formas:
  - Comprando los medios oficiales e instalarlos de esos CDs o descargando la ISO
  - Descargando los ISO e instalarlo por Internet o por red (ftp o http)
  - Armandos nuestra propia ISO con los archivos del sitio



**OpenBSD**

# Instalación

- ★ Instalación de ejemplo, usando CD y en un equipo dedicado (sin compartir con otros sistemas operativos)



**OpenBSD**

# Instalación

Luego de bootear y reconocer los dispositivos de nuestro equipo, empieza la parte que requiere interacción con el ser humano (vivo) mas cercano, en nuestro caso seleccionamos la opcion "i":

```
rootdev=0x1100 rrootdev=0x2f00 rawdev=0x2f02  
erase ^?, werase ^W, kill ^U, intr ^C, status ^T  
(I)nstall, (U)pgrade or (S)hell? i
```

Luego seleccionamos la terminal (no es necesario cambiarlo):

```
Specify terminal type: [vt220] <enter>
```

Ahora el idioma del teclado (enter o "es"):

```
kbd(8) mapping? ('L' for list) [none] <enter>
```

Seguimos con la instalación??? y si, sino para que llegamos a este punto?:

```
Proceed with install? [no] y
```



**OpenBSD**

# Instalación

Nos detecta los discos (en este caso wd0 ya que es IDE) y nos pregunta en cual queremos instalar OpenBSD, mmm que difícil es la elección.... me parece que lo mejor va a ser instalarlo en wd0:

```
Available disks are: wd0.
```

```
Which one is the root disk? (or done) [wd0] <enter>
```

Ya que vamos a usar sólo OpenBSD para este equipo, ponemos "yes", esto nos escribirá el mbr para que pueda bootear:

```
Do you want to use *all* of wd0 for OpenBSD? [no] yes
```



**OpenBSD**

# Instalación

Bien, ahora hay que armar las particiones (vamos a crear 1 sola para todo y otra para swap), pero primero borramos la partición creada por defecto:

```
> d a
```

Creamos 2 particiones, una para / (root) y otra para el swap (a y b respectivamente):

```
> a a
```

```
offset: [3069360] <enter>  
size: [36030960] 7g  
Rounding to nearest cylinder: 307440  
FS type: [4.2BSD] <enter>  
mount point: [none] /
```

```
> a b
```

```
offset: [3376800] <enter>  
size: [35723520] 1g  
Rounding to nearest cylinder: 614880  
FS type: [swap] <enter>
```



**OpenBSD**

# Instalación

Grabamos los cambios y salimos:

```
> w  
> q
```

Nos pregunta si queremos borrar todo el contenido de las particiones, así que le ponemos que sí:

```
The next step *DESTROYS* all existing data on these  
partitions!  
Are you really sure that you're ready to proceed? [no] y
```

Ahora vamos a configurar algunas cositas de nuestro futuro equipo:

```
Enter system hostname (short form, e.g. 'foo'): pufffy  
Configure the network? [yes] <enter>  
Available interfaces are: fxp0  
Which one do you wish to initialize?(or 'done') [fxp0] <enter>  
Symbolic (host) name for fxp0? [pufffy] <enter>  
The default media for fxp0 is  
      media: Ethernet autoselect (100baseTX full-duplex)  
Do you want to change the default media? [no] <enter>  
IPv4 address for fxp0? (or 'dhcp') 192.168.0.10  
Netmask? [255.255.255.0] <enter>
```



**OpenBSD**

# Instalación

## Seguimos con la configuración...

```
IPv6 address for fxp0? (or 'rtsol' or 'none') [none] <enter>
DNS domain name? (e.g. 'bar.com') [my.domain] test.local
DNS nameserver? (IP address or 'none') [none] 192.168.0.2
Use the nameserver now? [yes] <enter>
Default IPv4 route? (IP address, 'dhcp' or 'none') 192.168.0.1
Edit hosts with ed? [no] <enter>
Do you want to do any manual network configuration? [no] <enter>
Password for root account? (will not echo) pAssWOrd
Password for root account? (again) pAssWOrd
```

## Ahora elejimos donde estan los paquetes que vamos a instalar:

```
Location of sets? (cd disk ftp http or 'done') [cd] <enter>
Available CD-ROMs are: cd0.
Which one contains the install media? (or 'done') [cd0] <enter>
Pathname to the sets? (or 'done') [4.1/i386] <enter>
```



**OpenBSD**

# Instalación

Elegimos los paquetes ahora:

```
Select sets by entering a set name, a file name pattern or 'all'.  
De-select sets by prepending a '-' to the set name, file name  
pattern or 'all'. Selected sets are labeled '[x]'.
```

```
[X] bsd  
[X] bsd.rd  
[ ] bsd.mp  
[X] base40.tgz  
[X] etc40.tgz  
[X] misc40.tgz  
[X] comp40.tgz  
[X] man40.tgz  
[X] game40.tgz  
[ ] xbase40.tgz  
[ ] xetc40.tgz  
[ ] xshare40.tgz  
[ ] xfont40.tgz  
[ ] xserv40.tgz
```

```
Set name? (or 'done') [bsd.mp] all
```

Terminamos la selección y continuamos la instalación:

```
Set name? (or 'done') [done] <enter>
```

```
Ready to install sets? [yes] <enter>
```



**OpenBSD**

# Instalación

Luego de instalados los paquetes no queremos instalar mas nada:

```
Location of sets? (cd disk ftp http or 'done') [done] <enter>
```

Seleccionamos las ultimas opciones...

```
Start sshd(8) by default? [yes] <enter>
```

```
Start ntpd(8) by default? [no] yes
```

```
Do you expect to run the X Window System? [no] yes
```

```
Change the default console to com0? [no] <enter>
```

```
What timezone are you in? ('?' for list) [Canada/Mountain]
```

```
America/Buenos_Aires
```

Y por último reiniciamos el equipo:

```
# reboot
```

**Listooooo!!!!!!!!!!!!**

**Ya instalamos OpenBSD... al final no era taaaan difcil :P**



**OpenBSD**

**Diferencias con Linux**

# El Juego de las diferencias



**OpenBSD**

## Diferencias con Linux

- ★ Estilo BSD puro
- ★ Iniciación de demonios vía scripts (/etc/rc)
- ★ Como muchos desarrolladores de aplicaciones no tienen en cuenta a OpenBSD, este utiliza un sistema de árbol de portes y paquetes precompilados por los desarrolladores de OpenBSD. Estos resuleven dependencias y son fáciles de administrar y mantener. El orden es: Paquete > Port > fuente externo



**OpenBSD**

## Diferencias con Linux

- ★ Kernel y binarios se mantienen actualizados por CVS
- ★ Sale un nuevo release cada 6 meses
- ★ Software no BSD no viene en la instalación por defecto (se pueden instalar aparte)



**OpenBSD**

## Diferencias con Linux

- ★ El kernel es /bsd el "base" y /bsd.mp el "multiprocesador"
- ★ Los nombres de disco son:
  - /dev/wd(x) (ide)
  - /dev/sd(x) (scsi)
- ★ No soporta filesystems con journaling (ReiserFS, IMB JFS, SGI XFS, etc). Si soporta Ext3 (lo reconoce como Ext2)



**OpenBSD**

## Diferencias con Linux

- ★ Trae PF para filtrado de paquetes, NAT, Masquerading, etc.
- ★ Configuración de las interfaces de red en `/etc/hostname.(nombre_de_inteface)`
- ★ Nombre de host en `/etc/myname`
- ★ Default Gateway en `/etc/mygate`
- ★ Shell por defecto "ksh" (pero se puede instalar bash)



**OpenBSD**

## Diferencias con Linux

- ★ Los nombres de las interfaces son por fabricante y no por tipo (ej Ralink: ral[n])
- ★ La instalación se realiza sobre un slice, el cual contiene todas las particiones
- ★ El filesystem por defecto es Fast File System (FFS), que no tiene journaling (no lo necesita)



**OpenBSD**

## Instalación de Aplicaciones

Igual a los demas  
sin nada que envidiar



**OpenBSD**

## Instalación de Aplicaciones

- ★ Podemos instalar las aplicaciones de 3 formas diferentes:
  - Paquetes precompilados (packages)
  - Ports
  - Código fuente externo



**OpenBSD**

## Instalación de Aplicaciones

### Paquetes Precompilados (packages)

★ Para instalar:

```
# pkg_add [paquete]
```

★ Para desinstalar:

```
# pkg_delete [paquete]
```

★ Para obtener información:

```
# pkg_info                (los instalados)
```

```
# pkg_info [paquete]    (info del pkt)
```



**OpenBSD**

## Instalación de Aplicaciones

### Ports

- ★ Se debe descargar el archivo `ports.tar.gz` y desempaquetarlo.
- ★ Se depositan en `/usr/ports`
- ★ Para buscar un port se ejecuta en `/usr/ports`:

```
# make search key=[string]
```

- ★ Para instalar un port se ejecuta en la carpeta del port (ej. `/usr/port/www/opera`):

```
# make install clean
```

y para desinstalar:

```
# make uninstall clean
```



**OpenBSD**

## Instalación de Aplicaciones

### Código fuente

- ★ Como se compila normalmente un fuente
- ★ Se debe tener cuidado con la compatibilidad para OpenBSD, generalmente es necesario tocar el código.



**OpenBSD**

## Instalación de Aplicaciones

### Algunas aplicaciones disponibles

- ★ Base de Datos:  
MySQL, SQLite, PostgreSQL, etc.
- ★ X11:  
KDE, Gnome, XFCE, Fluxbox, Enlightenment...
- ★ Web:  
Apache, Squid, Bind, PHP, etc.
- ★ Mail:  
Sendmail, Qmail, Postfix, Squirrel, etc.
- ★ Otros:  
Firefox, Opera, Thunderbird, OpenOffice, XMMS, etc.



**OpenBSD**

**Actualización**

be current...  
be happy



**OpenBSD**

## Actualización

Que es lo que se actualiza????

- ★ Kernel y archivos del sistema (los sources)  
en la primera actualización descarga cerca de 600mb
- ★ Ports  
en la primera actualización descarga cerca de 100mb
- ★ X11  
en la primera actualización descarga cerca de 400mb



**OpenBSD**

## Actualización

Por ejemplo, para actualizar por cvsup:  
Que es lo que se necesita????

- ★ Estar online  
(conectado a Internet, basta con http)
- ★ Tener instalado cvsup
- ★ Archivos de configuración de actualización de cvsup



**OpenBSD**

# Actualización

## Ejemplo de archivo de cvsup: "cvsup-file-src"

```
# Defaults that apply to all the collections
*default release=cvs
*default delete use-rel-suffix
*default umask=002
*default host=anoncvs3.usa.openbsd.org
*default base=/usr
*default prefix=/usr
*default tag=OPENBSD_4_1

# If your network link is a T1 or faster, comment out the
following line.
*default compress

#OpenBSD-ports
#OpenBSD-all
OpenBSD-src
#OpenBSD-www
#OpenBSD-x11
#OpenBSD-xf4
#OpenBSD-xenocara
```

Luego se ejecuta:

```
# cvsup -g -L 2 cvsup-file-src
```



**OpenBSD**

## Actualización

Luego de actualizar por cvsup que hacemos??

- ★ Src: se debe hacer un rebuild del kernel y los archivos de sistema actualizados
- ★ Ports: Actualizar cada port viejo
- ★ X11: hacer un rebuild de X

El proceso completo lo podemos ver en:  
- [wiki.openbsd.org](http://wiki.openbsd.org)



**OpenBSD**

## Packet Filter

- Disculpe señor  
paquete, a donde se  
dirige? -



**OpenBSD**

## Packet Filter

### Señoras y señores, con ustedes... **The OpenBSD Packet Filter**

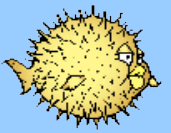
- ★ Filtrado de paquetes (pass o block)
- ★ Redirección de paquetes (rdr)
- ★ NAT
- ★ BINAT
- ★ Proxy de ftp y handshake
- ★ Normalización de paquetes (scrub)
- ★ Antispoof



**OpenBSD**

## Packet Filter

- ★ Queueing (QoS)
- ★ Traffic Shaping
- ★ Etiquetado de paquetes
- ★ Logging de paquetes (tcpdump)
- ★ AuthPF (establece reglas según autenticación)



**OpenBSD**

## Packet Filter

- ★ CARP (cluster)
- ★ PFSync (sincronización de estado)
- ★ Interface Web (aplicación externa)



Seguridad

“Porque la seguridad importa”





**OpenBSD**

# Seguridad

- ★ Security levels (kernel)
- ★ Kernel flags (files and folders)
- ★ Otros



**OpenBSD**

# Seguridad

## Security Levels

- ★ Permite elevar o disminuir el nivel de seguridad, puede tener los valores:  
-1, 0, 1 y 2
- ★ El valor en por defecto es 1, salvo en el primer booteo que es 0.
- ★ Se modifican en el archivo `/etc/rc.securelevel`



**OpenBSD**

# Seguridad

## Security Levels

- ★ -1: sin la seguridad nominal del kernel y funciones especiales de seguridad
- ★ 0: con funciones básicas de seguridad en el kernel
- ★ 1: no se puede escribir en /dev/mem y /dev/kmem, raw devices como "RO", los flags schg y sappnd no se pueden sacar, no se pueden cargar o descargar los módulos del kernel online
- ★ 2: level 1 + system clock limitado, pfctl no puede cambiar reglas o nat, no se pueden modificar los valores del sysctl  
DDB kernel debugger



**OpenBSD**

# Seguridad

## Kernel Flags

- ★ Se setean como permisos sobre files o carpetas (con un security level 1 o -)
- ★ sappnd: lo puede poner o sacar root, solo se puede agregar info (no sacar o editar), no se puede sacar en sec level 1 (ideal logs)
- ★ schg: lo puede poner o sacar root, no se pueden eliminar mover o reemplazar, no se puede sacar en sec level 1
- ★ uappnd: lo puede poner o sacar root u otro usuario, solo se puede agregar info



**OpenBSD**

# Seguridad

## Otros

- ★ Auditoria de código permanente
- ★ Protecciones de memoria
- ★ Separación de privilegios
- ★ Revocación de privilegios
- ★ chroot/jail
- ★ Propolice
- ★ Otros...



**OpenBSD**

**OpenBSDeros.org**

**.: OpenBSDeros :.**

<http://www.openbsderos.org>

**Comunidad de  
Usuarios de OpenBSD**



**OpenBSD**

**OpenBSDeros.org**

- ★ Foro, log, wiki, galeria y otras secciones
- ★ Artículos tecnicos
- ★ Noticias y novedades de OpenBSD
- ★ Y mas!!!



**OpenBSD**

# Preguntas



Preguntas???