sudo cp /etc/ssh/sshd\_config /etc/ssh/sshd\_config\_BACKUP

sudo nano /etc/ssh/sshd\_config

sudo /etc/init.d/ssh reload

ssh -p 54321 [me@12.34.56.78](mailto:me@12.34.56.78)

sudo mv /etc/ssh/sshd\_config\_BACKUP /etc/ssh/sshd\_config

sudo /etc/init.d/ssh reload

export USER=someuser

groupadd sftpusers

useradd -d /home/$USER -G sftpusers -s /bin/false $USER

passwd $USER

mkdir -m 751 /home/chroot-sftp /home/chroot-sftp/{dev,home}

mkdir -m 770 /home/chroot-sftp/home/$USER

chown root:$USER /home/chroot-sftp/home/$USER

echo '$AddUnixListenSocket /home/chroot-sftp/dev/log

:programname, isequal, "internal-sftp" -/var/log/sftpusers.log

:programname, isequal, "internal-sftp" ~ ' > /etc/rsyslog.d/chroot-sftp.conf

service rsyslog restart

echo '/var/log/sftpusers.log {

weekly

missingok

rotate 52

compress

delaycompress

postrotate

invoke-rc.d rsyslog reload > /dev/null

endscript

}' > /etc/logrotate.d/chroot-sftp

mkdir -m 750 /home/$USER /home/$USER/.ssh

chown root:$USER /home/$USER /home/$USER/.ssh

nano /home/$USER/.ssh/authorized\_keys

nano /etc/ssh/sshd\_config

#Subsystem sftp /usr/lib/openssh/sftp-server

Subsystem sftp internal-sftp -l VERBOSE

Match group sftpusers

ChrootDirectory /home/chroot-sftp

ForceCommand internal-sftp -l VERBOSE

AllowTcpForwarding no

AllowAgentForwarding no

X11Forwarding no

/etc/init.d/ssh restart

sftp someuser@123.45.67.890

sftp -oPort=54321 someuser@123.45.67.890

export SHARE\_PATH=/example/path/to/wp-content/themes

chown -R :www-data $SHARE\_PATH && chmod -R g+s $SHARE\_PATH

mkdir /home/chroot-sftp/home/$USER/SHARE

mount --bind $SHARE\_PATH /home/chroot-sftp/home/$USER/SHARE

mkdir /home/chroot-sftp/home/$USER/SHARE/devTheme

chown $USER:www-data /home/chroot-sftp/home/$USER/SHARE/devTheme

export USER=someuser

umount /home/chroot-sftp/home/$USER/SHARE

userdel $USER && rm -R /home/chroot-sftp/home/$USER /home/$USER

sudo nano /etc/php5/apache2/php.ini

disable\_functions = "apache\_get\_modules, apache\_get\_version, apache\_getenv, apache\_note, apache\_setenv, disk\_free\_space, diskfreespace, exec, highlight\_file, ini\_restore, ini\_set, openlog, passthru, phpinfo, popen, proc\_open, proc\_nice, shell\_exec, show\_source, symlink, system"

<Directory /path/to/www/somesite.com-root>

**php\_admin\_value open\_basedir "/path/to/www/somesite-ROOT"**

</Directory>

php\_admin\_value open\_basedir "**/path/1:/path/2:/path/3**"

sudo aptitude install php5-suhosin

sudo -i  
aptitude install libapache2-mod-suphp

a2dismod php5

useradd -s /bin/false user

chown -R user:user /home/user

find /home/user/www -type d -exec chmod 755 {} \;

find /home/user/www -type f -exec chmod 644 {} \;

find /home/user/www -type f -name "\*.php" -exec chmod 600 {} \;

mysql > SELECT user, host, password FROM mysql.user;

mysql > DROP DATABASE test;

sudo -i

/sbin/iptables –L

bash: iptables: command not found

aptitude install -y iptables

iptables-save > /etc/iptables.up.rules

nano /etc/iptables.test.rules

\*filter  
# Loopback traffic rule  
-A INPUT -i lo -j ACCEPT  
-A INPUT ! -i lo -d 127.0.0.0/8 -j REJECT  
# Inbound & outbound traffic  
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT  
-A OUTPUT -j ACCEPT  
### Allow HTTP (port 80) & HTTPS (port 443) ###  
-A INPUT -p tcp --dport 80 -j ACCEPT  
-A INPUT -p tcp --dport 443 -j ACCEPT  
### Allow SSH ###  
-A INPUT -p tcp -m state --state NEW --dport 22 -j ACCEPT  
# Allow ping  
-A INPUT -p icmp -m icmp --icmp-type 8 -j ACCEPT  
# Firewall logging  
-A INPUT -m limit --limit 5/min -j LOG --log-prefix "iptables denied:" --log-level 7  
# Block all other inbound  
-A INPUT -j REJECT  
-A FORWARD -j REJECT  
COMMIT

### Allow HTTP (port 80) & HTTPS (port 443) ###  
-A INPUT -p tcp --dport 80 -j ACCEPT  
-A INPUT -p tcp --dport 443 -j ACCEPT

-A INPUT -p tcp --dport 25 -j ACCEPT

### Allow SSH ###  
-A INPUT -p tcp -m state --state NEW --dport 54321 -j ACCEPT

iptables-restore < /etc/iptables.test.rules  
iptables-save > /etc/iptables.up.rules

nano /etc/network/interfaces

pre-up iptables-restore < /etc/iptables.up.rules

exit

sudo –i

aptitude install libwww-perl

cd /usr/local/src

wget <http://www.configserver.com/free/csf.tgz>

tar xzf csf.tgz && cd csf

./install.sh

perl [/etc/csf/csftest.pl](file:///C:\etc\csf\csftest.pl)

nano /etc/csf/csf.conf

csf -f

MONOLITHIC\_KERNEL = "1"

csf -r

csf -h for the CSF manual

csf -a [IPADDRESS] to allow an IP

csf -d [IPADDRESS] to block an IP

csf -dr [IPADDRESS] to unblock an IP

csf -f to flush the rules, disabling the firewall

csf -s to start the firewall

csf -r to restart the firewall

csf -x to disable CSF

csf -e to enable CSF

csf -c to check for a CSF update

csf --mail [me@myblog.com](mailto:me@myblog.com)  
csf --m

sudo netstat -tap | grep LISTEN

sudo netstat -tapn | grep LISTEN

sudo netstat -tap > ~/services.lst

ps ax | grep cupsd

dpkg --list

dpkg --list | grep cups

sudo aptitude install sysv-rc-conf

sudo sysv-rc-conf

sudo aptitude install harden-servers

sudo iptables –L INPUT

sudo iptables –D INPUT 4

sudo iptables –D INPUT 4

sudo nano [/etc/hosts.deny](file:///C:\etc\hosts.deny)

sshd : all

sudo nano [/etc/hosts.allow](file:///C:\etc\hosts.allow)

sshd : 123.45.67.890

sudo nano /etc/sysctl.conf

#**accept\_source\_route** - Disable IP source routing.

net.ipv4.conf.all.accept\_source\_route=0  
net.ipv4.conf.default.accept\_source\_route=0  
net.ipv6.conf.all.accept\_source\_route=0  
net.ipv6.conf.default.accept\_source\_route=0

#**redirects** - Secure the routing table.

net.ipv4.conf.all.accept\_redirects=0  
net.ipv6.conf.all.accept\_redirects=0  
net.ipv4.conf.all.send\_redirects=0  
net.ipv6.conf.all.send\_redirects=0

#**rp\_filter** - Prevent IP spoofing.

net.ipv4.conf.all.rp\_filter=1  
net.ipv4.conf.lo.rp\_filter=1  
net.ipv4.conf.eth0.rp\_filter=1  
net.ipv4.conf.default.rp\_filter=1

#**log\_martians** - Log potential attacks.

net.ipv4.conf.all.log\_martians=1

#**ignore\_broadcasts** - Avoid DoS (Smurf) attack participation.

net.ipv4.icmp\_echo\_ignore\_broadcasts=1

#**tcp\_syncookies** - Prevent SYN flood DDoS attacks.

net.ipv4.tcp\_syncookies=1  
ipv4.tcp\_max\_syn\_backlog=1280

sysctl –f

sysctl -a