sudo -i  
echo 'deb <http://ubuntu.cr0.org/repo/> kernel-security/' >> /etc/apt/sources.list

echo 'deb <http://debian.cr0.org/repo/> kernel-security/' >> [/etc/apt/sources.list](file:///C:\Users\olly\etc\apt\sources.list)

wget <http://kernelsec.cr0.org/kernel-security.asc> && apt-key add kernel-security.asc

aptitude install linux-image-grsec

sudo -i

cd /usr/local/src

aptitude install -y wget patch kernel-package initramfs-tools libncurses5-dev

export KERNEL\_SERIES="2.6"

export KERNEL\_VERSION="2.6.32.15"

export GRSEC\_VERSION="2.2.0-2.6.32.15-201006271253"

export GRADM\_VERSION="2.2.0-201006192157"

wget <http://www.kernel.org/pub/linux/kernel/v$KERNEL_SERIES/linux-$KERNEL_VERSION.tar.bz2>  
wget <http://www.kernel.org/pub/linux/kernel/v$KERNEL_SERIES/linux-$KERNEL_VERSION.tar.bz2.sign>  
gpg --keyserver wwwkeys.pgp.net --recv-keys 0x517D0F0E  
gpg --verify linux-$KERNEL\_VERSION.tar.bz2.sign linux-$KERNEL\_VERSION.tar.bz2

wget <http://grsecurity.net/stable/grsecurity-$GRSEC_VERSION.patch>  
wget <http://grsecurity.net/stable/grsecurity-$GRSEC_VERSION.patch.sig>  
wget <http://grsecurity.net/spender-gpg-key.asc>  
gpg --import spender-gpg-key.asc  
gpg --verify grsecurity-$GRSEC\_VERSION.patch.sig  
wget <http://grsecurity.net/stable/gradm-$GRADM_VERSION.tar.gz>  
wget <http://grsecurity.net/stable/gradm-$GRADM_VERSION.tar.gz.sig>  
gpg --verify gradm-$GRADM\_VERSION.tar.gz.sig

tar xjf linux-$KERNEL\_VERSION.tar.bz2  
patch -p0 < grsecurity-$GRSEC\_VERSION.patch  
cd linux-$KERNEL\_VERSION

gunzip -c /proc/config.gz > .config && make oldconfig

nano .config

CONFIG\_PARAVIRT\_GUEST=y   
CONFIG\_XEN=y   
CONFIG\_PARAVIRT=y   
CONFIG\_PARAVIRT\_CLOCK=y   
CONFIG\_XEN\_BLKDEV\_FRONTEND=y   
CONFIG\_XEN\_NETDEV\_FRONTEND=y   
CONFIG\_HVC\_XEN=y   
CONFIG\_XEN\_BALLOON=y   
CONFIG\_XEN\_SCRUB\_PAGES=y

make menuconfig

echo 1 > /proc/sys/kernel/grsecurity/grsec\_lock

make-kpkg clean   
make-kpkg --initrd kernel\_image kernel\_headers

dpkg -i ../\*.deb

aptitude -y install grub   
update-grub -y

cat [/etc/fstab](file:///C:\Users\olly\etc\fstab)

sed -i '/^# kopt/ c\# kopt=root=**/dev/xvda** ro' /boot/grub/menu.lst

sed -i '/^# groot/ c\# groot=(**hd0**)' /boot/grub/menu.lst

sed -i '/^# indomU/ c\# indomU=false' /boot/grub/menu.lst

update-grub -y

shutdown -r now

uname -r

sudo -i  
cd /usr/local/src  
wget <http://www.grsecurity.net/~paxguy1/paxtest-0.9.7-pre5.tar.gz>  
tar xzvf paxtest-0.9.7-pre5.tar.gz  
cd paxtest-0.9.7-pre5  
make generic

[./paxtest](file:///C:\Users\olly\notes\wpSecNew\Hardening_the_Linux_Kernel\paxtest) kiddie  
[./paxtest](file:///C:\Users\olly\notes\wpSecNew\Hardening_the_Linux_Kernel\paxtest) blackhat

nano README

aptitude install -y flex bison

export GRADM\_VERSION="2.2.0-201006192157"  
cd /usr/local/src  
tar xzf gradm-$GRADM\_VERSION.tar.gz  
cd gradm2

make  
make install

make nopam  
make install

man gradm

aptitude install build-essential

sudo –i

cd /usr/local/src

wget http://www.ossec.net/files/ossec-hids-2.5.1.tar.gz

tar xzvf ossec-hids-2.5.1.tar.gz

cd ossec-hids-2.5.1

./install.sh

<global>

<white\_list>127.0.0.1</white\_list>

<white\_list>1.2.3.0/24</white\_list> #this is CIDR notation

<white\_list>109.82.107.65</white\_list>

</global>

/var/ossec/bin/ossec-control [start/stop/restart]

exit

cd /path/to/WordPress/wp-content/plugins

wget http://www.ossec.net/files/other/wpsyslog2.tar.gz

tar xzvf wpsyslog2.tar.gz && rm wpsyslog2.tar.gz

chown www-data:www-data -R wpsyslog2

sudo aptitude install –y chkrootkit rkhunter

sudo chkrootkit

sudo rkhunter -c

echo "

#!/bin/bash

chkrootkit | mail -s 'chkrootkit Scan - **HOSTNAME**' **YOU@SOMESITE.com**

" > /etc/cron.daily/chkrootkit.sh \

&& chmod 700 /etc/cron.daily/chkrootkit.sh

echo "

#!/bin/sh

(

rkhunter --versioncheck

rkhunter --update

rkhunter --cronjob --report-warnings-only

) | mail -s 'rkhunter Scan - **HOSTNAME**' **YOU@SOMESITE.com**

" > /etc/cron.daily/rkhunter.sh \

&& chmod 700 /etc/cron.daily/rkhunter.sh

sudo aptitude install libapache2-mod-evasive

sudo a2enmod mod-evasive

sudo –i

aptitude install apache2-prefork-dev build-essential git-core libapr1-dev libaprutil1-dev libopenssl-ruby rake ruby rubygems ruby1.8-dev snort-mysql

gem install prawn

gem install mysql

gem install passenger

gem install -v=2.3.2 rails

ln -s /var/lib/gems/1.8/bin/pass\* /usr/bin

export WEBPATH="/your/web-root/path"

cd ~ && mkdir $WEBPATH/snorby

git clone git://github.com/mephux/Snorby.git

mv Snorby/\* $WEBPATH/snorby

nano /etc/apache2/sites-available/snorby

<VirtualHost \*:80>

ServerName **snorby.somesite.com**

DocumentRoot **/your/web-root/path**/snorby/public

<Directory **/your/web-root/path**/snorby/public>

AllowOverride all

Options -MultiViews

</Directory>

</VirtualHost>

mysql -u root -p

create database snortDB;

grant all privileges on snortDB.\* to snortUSER@localhost identified by "snortPASS";

flush privileges;

quit

cd /usr/share/doc/snort-mysql/

zcat create\_mysql.gz | mysql -u snortUSER -h localhost -p snortDB

nano /etc/snort/snort.conf

And run a search, that's CTRL-W, for this #commented line:

# output database: log, mysql, user=root password=test dbname=db host=localhost

Uncomment it by losing the # and change the values so it looks something like this:

output database: log, mysql, user=**snortUSER** password=**snortPASS** dbname=**snortDB** host=localhost

mv $WEBPATH/snorby/config/database.yml.example $WEBPATH/snorby/config/database.yml

mv $WEBPATH/snorby/config/email.yml.example $WEBPATH/snorby/config/email.yml

nano $WEBPATH/snorby/config/database.yml

nano $WEBPATH/snorby/config/email.yml

passenger-install-apache2-module

nano /etc/apache2/apache2.conf

cd $WEBPATH/snorby

rake snorby:setup RAILS\_ENV=production

rake snorby:reset RAILS\_ENV=production

rm /etc/snort/db-pending-config

a2ensite snorby

/etc/init.d/snort start && apache2ctl restart

exit

nmap -sT [your server's IP]

sudo mysql -u snorbyUSER -psnorbyPASS -e"use snorbyDB; SELECT \* FROM event INNER JOIN signature ON event.signature=signature.sig\_id ORDER BY event.timestamp;"

sudo -i

aptitude install libapache-mod-security

a2enmod mod-security

cd /usr/local/src  
wget http://sourceforge.net/projects/mod-security/files/modsecurity-crs/0-CURRENT/modsecurity-crs\_2.1.2.tar.gz

tar zxf modsecurity-crs\_2.1.2.tar.gz

cd modsecurity-crs\_2.1.2 && ls –la

mkdir /etc/apache2/modsecurity

cp \*.example /etc/apache2/modsecurity/ modsecurity\_crs\_10\_config.conf

cp -R base\_rules/\* /etc/apache2/modsecurity

echo "<IfModule security2\_module>  
Include modsecurity/\*.conf  
</IfModule>" >> /etc/apache2/httpd.conf

nano /etc/apache2/modsecurity/modsecurity\_crs\_10\_config.conf

SecRuleEngine DetectionOnly

SecAuditEngine RelevantOnly  
SecAuditLog /var/log/apache2/audit\_log  
SecDebugLog /var/log/apache2/modsec\_debug\_log  
SecDebugLogLevel 1

apache2ctl restart

exit

nano /var/log/apache2/audit\_log