

# Hardening Linux Web Server in 60 Minutes

Oleh: whatsoever

Kadang kala, *SysAdmin* sering lupa pada beberapa hal yang seharusnya tidak terlupakan oleh mereka yang pada akhirnya membuat *system* mereka menjadi mudah untuk dikuasai oleh orang yang bermaksud jahat atau iseng. Ada beberapa *SysAdmin* yang memang ternyata khilaf dan ada beberapa juga memang tidak terlalu menguasai area nya dengan benar dan ada juga yang kurang pengalaman sehingga mereka (*SysAdmin*) menjadi membiarkan saja keamanan dari aset-aset penting mereka.

Apa yang akan dibahas di modul ini:

- Bagaimana cara melakukan instalasi linux menggunakan *RAID-1* yang berfungsi ganda sebagai duplikat dan juga sebagai alat untuk forensik elektronik.
- Menghentikan layanan yang tidak penting.
- Bagaimana cara mengkonfigurasi *Firewall* anda.
- Membatasi akses ke *file/data* penting, konfigurasi dan binari dan bahkan menghilangkan ke-“MAHA”-an *root*.
- Memodifikasi *PHP* untuk menggunakan *patch* dari pihak ketiga yang bertujuan untuk membuat situs dan aplikasi berbasis *web* anda menjadi lebih kebal terhadap serangan.
- Memanajemen *log* menggunakan aplikasi tambahan berbasis *web*.
- Bagaimana manajemen *server linux* anda menggunakan metode yang lebih baik.
- Bagaimana cara *recovery* dan bereaksi terhadap insiden keamanan yang terjadi.

Apa yang tidak akan dibahas di modul ini:

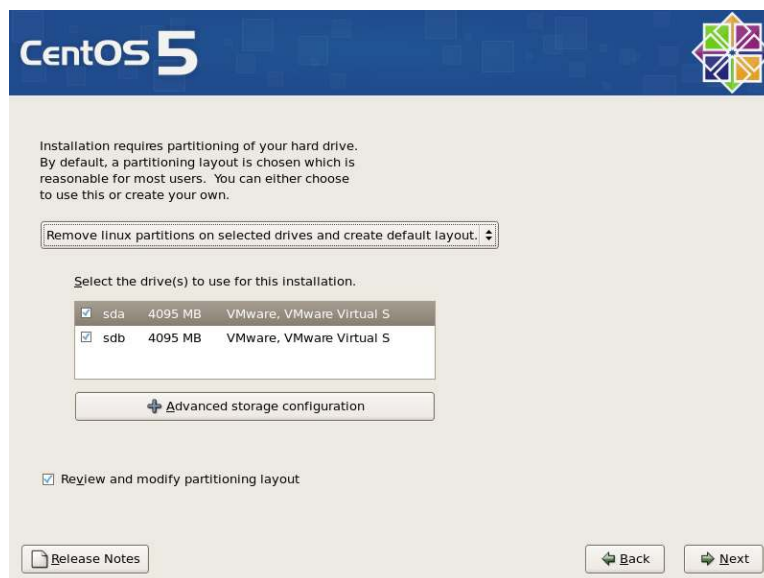
- Bagaimana cara memodifikasi kernel linux anda menggunakan Bastille atau GRSEC.
- Bagaimana cara melakukan instalasi HIDS atau NIDS.
- Bagaimana cara membuat situs anda ramai dikunjungi.

# Hardening Linux Web Server

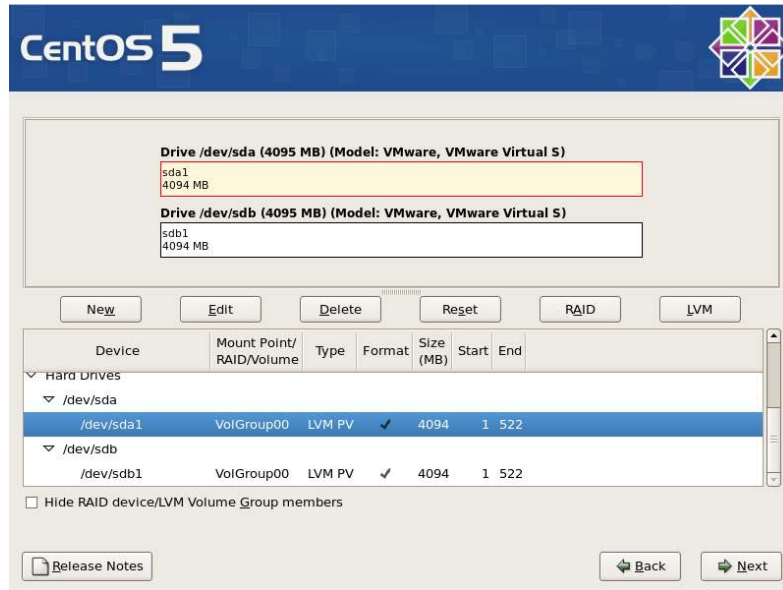
- Instalasi system operasi
  - Instalasi system operasi menggunakan RAID-1



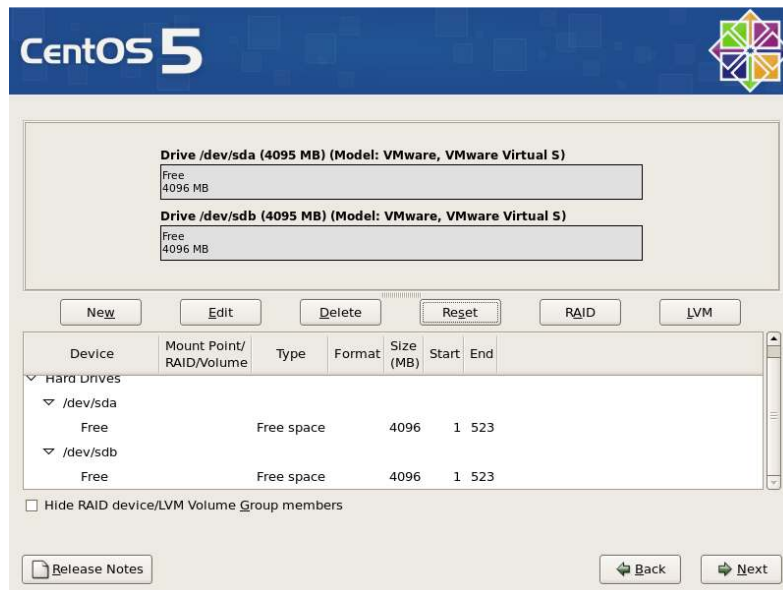
Pada menu *Boot*, tekan “Enter” tanpa memasukkan parameter lain.



Centangin semua *option* dan pilih “Remove Linux Partition on selected drives”, lalu klik “Next”.

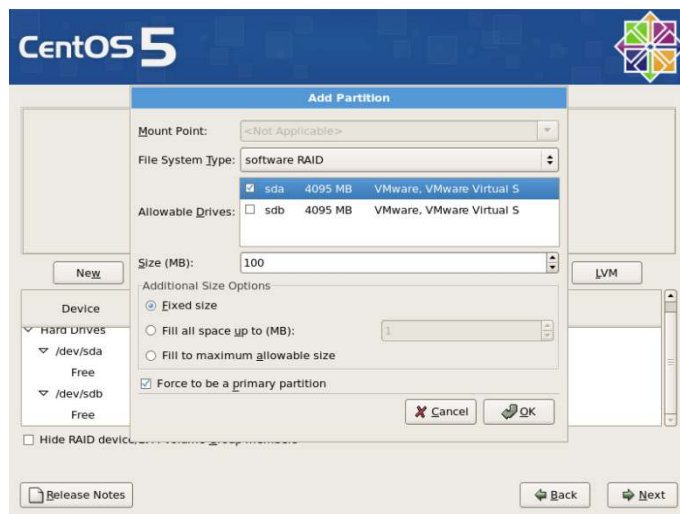
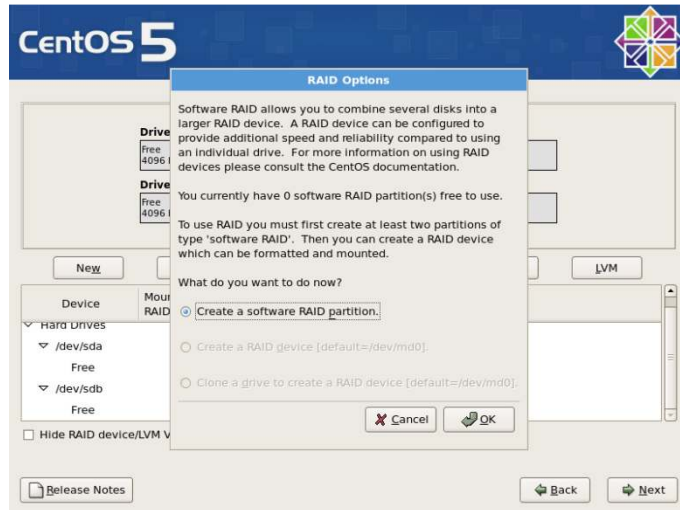


Pilih partisi yang akan di hilangkan dan hasil nya akan terlihat seperti gambar dibawah ini

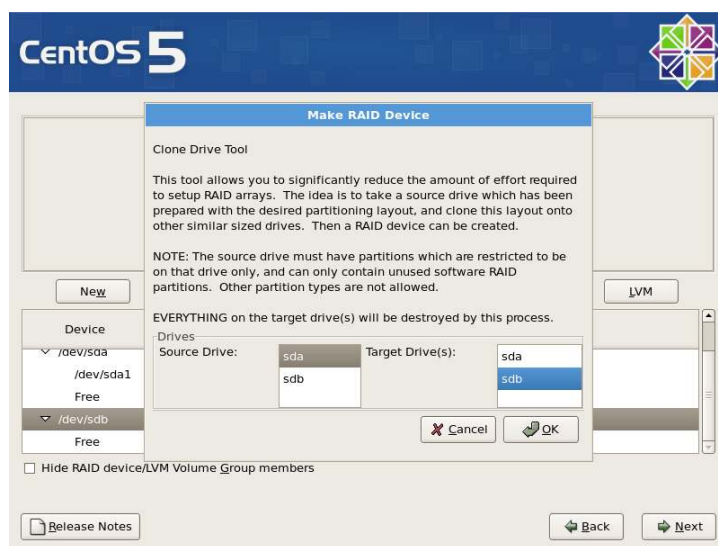
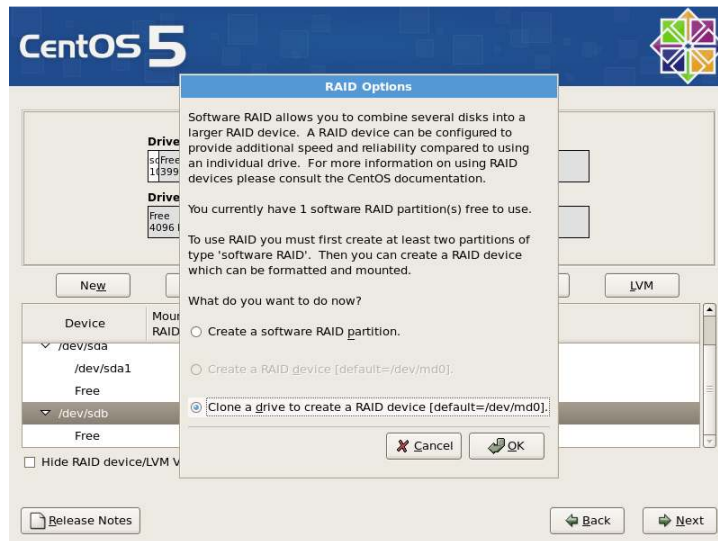


Setelah itu siapkan partisi nya untuk di buat *RAID-1*, dengan langkah sebagai berikut:

- Klik di *drive* "sda" yang partisi nya telah dihapus, kemudian klik "RAID".
- Lalu pilih "create a software raid partition" dan klik "OK"
- Centangin *option* "sda" dan pilih *file system type* "software RAID" jangan lupa centangin juga pilihan "force to be primary partition" lalu klik "OK".



- Setelah partisi nya telah terbentuk maka pilih *drive* "sdb" dan klik "RAID".
- Pilih *option* "Clone a drive", klik "OK" setelah itu pilih *source* "sda" dan target "sdb".



- Setelah klik “OK” maka anda harus memilih partisi “/dev/sda1” dan klik “RAID”
- Pilih *option* “Create a RAID device” dan klik “OK”.
- Setelah urusan partisi selesai maka kita akan dengan mudah masuk kedalam pemilihan besar kecil *slice* yang kita ingin kan nanti untuk *system linux*.
- Penulis hanya menggunakan 3 *slice*, yaitu “/boot” “swap” dan “/”.
- Setelah selesai dengan semua *RAID* kita lanjut ke pemilihan *package* yang akan di instalasi.

**CentOS 5**

### RAID Options

Software RAID allows you to combine several disks into a larger RAID device. A RAID device can be configured to provide additional speed and reliability compared to using an individual drive. For more information on using RAID devices please consult the CentOS documentation.

You currently have 2 software RAID partition(s) free to use.

What do you want to do now?

Create a software RAID partition.  
 Create a RAID device [default=/dev/md0].  
 Clone a drive to create a RAID device [default=/dev/md0].

Hide RAID device/LVM Volume Group members

**CentOS 5**

### Make RAID Device

Mount Point: /boot

File System Type: ext3

RAID Device: md0

RAID Level: RAID1

RAID Members:

<input checked="" type="checkbox"/>	sda1	102 MB
<input checked="" type="checkbox"/>	sdb1	102 MB

Number of spares: 0

Hide RAID device/LVM Volume Group members

**CentOS 5**

### Make RAID Device

Mount Point: <<Not Applicable>>

File System Type: swap

RAID Device: md1

RAID Level: RAID0


RAID Members:

<input checked="" type="checkbox"/>	sda2	518 MB
<input type="checkbox"/>	sda3	3475 MB
<input checked="" type="checkbox"/>	sdb2	518 MB

Number of spares: 0

Hide RAID device/LVM Volume Group members

**CentOS 5**



Make RAID Device

Drive  sda1 1517

Drive  sdb1 1517

Mount Point: <Not Applicable>

File System Type: swap

RAID Device: md1

RAID Level: RAID0

RAID Members:

- sda2 518 MB
- sda3 3475 MB
- sdb2 518 MB


Number of spares: 0

LVM

Device	Mo	RAI
Hard Drives		
/dev/sda		
/dev/sda1	/de	
/dev/sda2	/de	
/dev/sda3	/de	
/dev/sdb		
/dev/sdb1	/dev/m	software RAID

Hide RAID device/LVM Volume Group members

**CentOS 5**



Make RAID Device

Drive  sda1 1517

Drive  sdb1 1517

Mount Point: /

File System Type: ext3

RAID Device: md2

RAID Level: RAID0

RAID Members:

- sda3 3475 MB
- sdb3 3475 MB


Number of spares: 0

LVM

Device	Mo	RAI
Hard Drives		
/dev/sda		
/dev/sda1	/de	
/dev/sda2	/de	
/dev/sda3	/de	
/dev/sdb		
/dev/sdb1	/dev/m	software RAID

Hide RAID device/LVM Volume Group members

**CentOS 5**



The GRUB boot loader will be installed on /dev/md0.

No boot loader will be installed.

You can configure the boot loader to boot other operating systems. It will allow you to select an operating system to boot from the list. To add additional operating systems, which are not automatically detected, click 'Add.' To change the operating system booted by default, select 'Default' by the desired operating system.

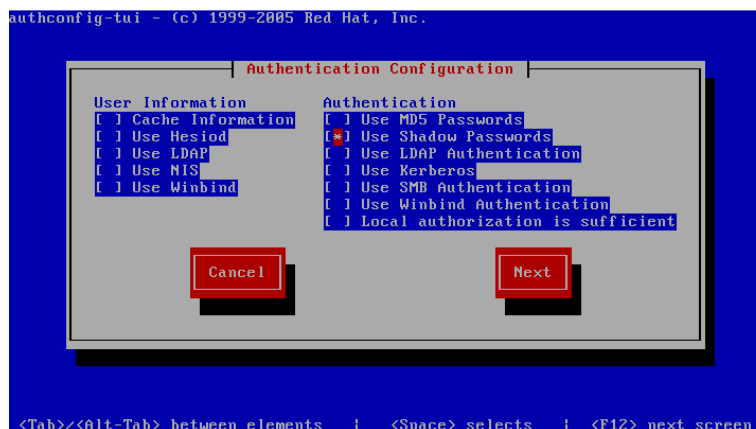
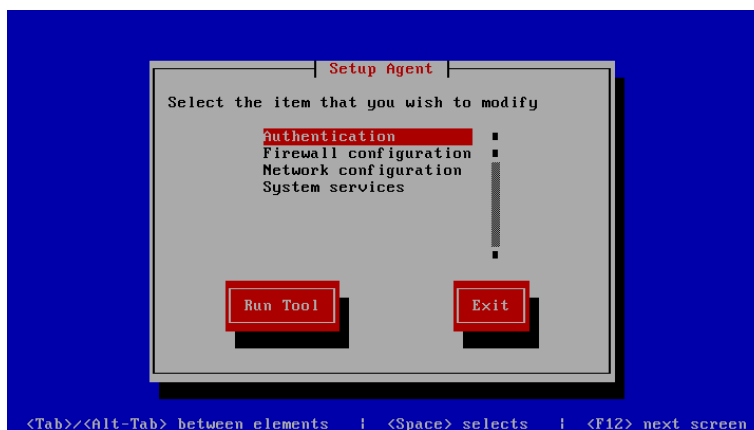
Default	Label	Device
<input checked="" type="checkbox"/>	CentOS	/dev/md2

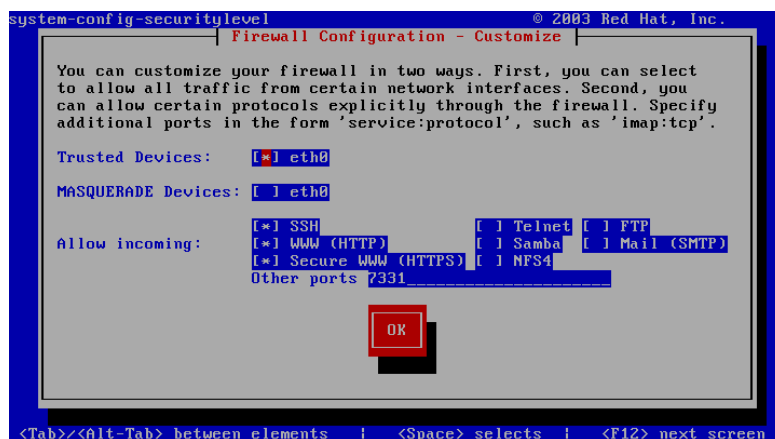
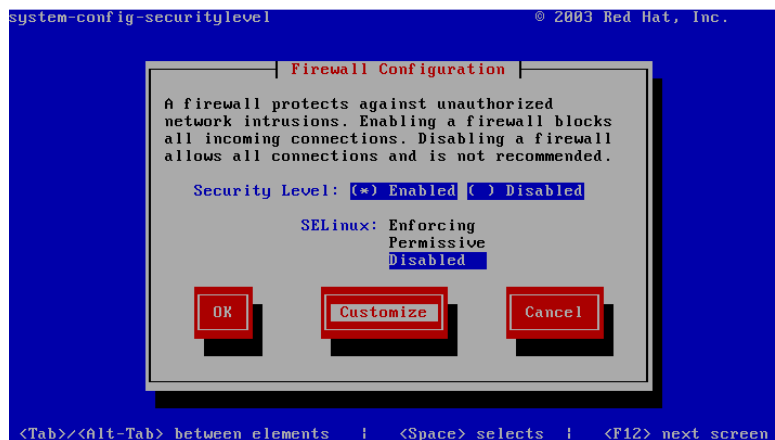
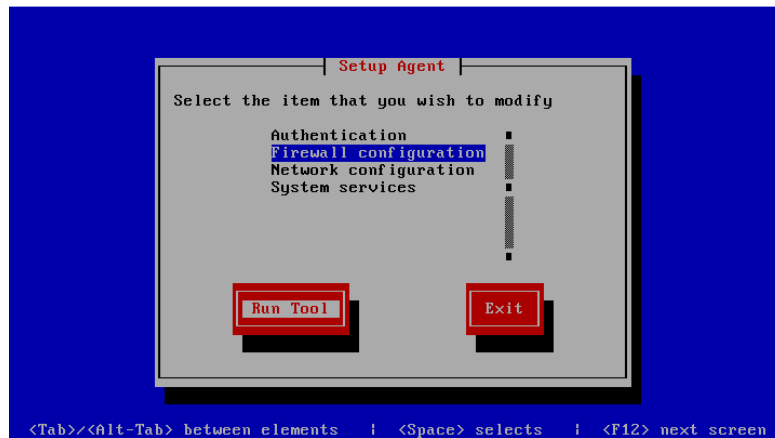
A boot loader password prevents users from changing options passed to the kernel. For greater system security, it is recommended that you set a password.

Use a boot loader password

Configure advanced boot loader options

- Instalasi Paket
  - Pilih instalasi minimum.
  - Hilangkan semua centang pada *option packages*.
- Konfigurasi awal
  - Setelah proses instalasi selesai, maka kita akan melakukan *restart/reboot*.
  - Menu yang akan kita temui berikutnya adalah konfigurasi awal system centos.
  - Pilih menu "Authentication" lalu pencet "Run Tool" lalu centangin "Use Shadow Password".
  - Berikutnya kita pilih menu "Firewall Configuration" dan centangin "Security Level: Enabled" dan "SELinux: Permissive" lalu pilih "Costumize".
  - Di menu "Costumize", centangin "trusted device: eth0", "Allow incoming: SSH, WWW, HTTPS" dan "Other Ports: Optional".





- Tuning & updating system

- Sampai pada tahap ini, kita akan me-non-aktifkan beberapa *services/daemon* yang tidak kita butuhkan untuk saat ini, *login* dengan “user: root” dan *password* yang telah anda isi sebelumnya pada proses *setup*.
- Jalankan perintah “*ntsysv*” dan pastikan hanya yang di tulis berikut yang aktif: *anacron*, *crond*, *iptables*, *irqbalance*, *kudzu*, *mcstrans*, *network*, *readahead\_early*, *restorecond*, *sshd*, *syslog*, *sysstat*, *yum-updatesd*.
- Edit file konfigurasi *repository yum* anda dengan menggunakan *text editor* kesukaan anda.
- Pastikan konfigurasi nya dengan benar:

```

-----
# CentOS-Base.repo for CentOS 5.2
# sample version by whatsoever
#

[base]
name=CentOS-$releasever - Base
baseurl=http://centos.cbn.net.id/5.2/os/$basearch/
gpgcheck=1
gpgkey=http://centos.cbn.net.id/RPM-GPG-KEY-CentOS-5

[updates]
name=CentOS-$releasever - Updates
baseurl=http://centos.cbn.net.id/5.2/updates/$basearch/
gpgcheck=1
gpgkey=http://centos.cbn.net.id/RPM-GPG-KEY-CentOS-5

[addons]
name=CentOS-$releasever - Addons
baseurl=http://centos.cbn.net.id/5.2/addons/$basearch/
gpgcheck=1
gpgkey=http://centos.cbn.net.id/RPM-GPG-KEY-CentOS-5

[extras]
name=CentOS-$releasever - Extras
baseurl=http://centos.cbn.net.id/5.2/extras/$basearch/
gpgcheck=1
gpgkey=http://centos.cbn.net.id/RPM-GPG-KEY-CentOS-5

[centosplus]
name=CentOS-$releasever - Plus
baseurl=http://centos.cbn.net.id/5.2/centosplus/$basearch/
gpgcheck=1
enabled=0
gpgkey=http://centos.cbn.net.id/RPM-GPG-KEY-CentOS-5

# -EOF-
-----

```

- Lalu jalankan perintah “yum -y upgrade”.
- Setelah semua upgrade system telah selesai, jalankan perintah:
 

```
“yum -y install wget bzip2 unzip zip fileutils gcc gcc-c++ ncurses-devel pam-devel libxml2-devel libxslt-devel m4 flex
byacc wget which install pcre pcre-devel binutils autoconf automake libtool zlib lsof man man-pages mlocate quota
rsync sysstat xinetd cron bzip2-devel ntp httpd php php-devel php-gd php-imap php-ldap php-mysql php-odbc php-
pear php-xml php-xmlrpc mysql mysql-server aspell-devel httpd-devel libjpeg-devel libpng-devel pcre-devel libc-
client-devel mysql-devel postgresql-devel unixODBC-devel net-snmp-devel gd-devel freetype-devel perl-DBI.i386”
```
- Jalankan perintah:
  - chkconfig --levels 235 httpd on; /etc/init.d/httpd start
  - chkconfig --levels 235 ntpd on; ntpdate 0.pool.ntp.org; /etc/init.d/ntp start
  - chkconfig --level 2345 mysql on; chown root:sys /etc/my.cnf
  - chmod 700 /etc/my.cnf\*; service mysqld start
  - adduser whatsoever
  - passwd whatsoever

- Edit file konfigurasi *sshd*:
  - `mv /etc/ssh/sshd_config /etc/ssh/sshd_config`
  - `vi /etc/ssh/ssd_config`

```
-----  
  
# sshd configuration  
# modded version by whatsoever  
  
Port 7331  
Protocol 2  
  
SyslogFacility AUTHPRIV  
LogLevel INFO  
  
LoginGraceTime 1m  
PermitRootLogin no  
StrictModes yes  
MaxAuthTries 2  
  
PasswordAuthentication yes  
ChallengeResponseAuthentication no  
GSSAPIAuthentication yes  
GSSAPICleanupCredentials yes  
  
UsePAM yes  
  
AcceptEnv LANG LC_CTYPE LC_NUMERIC LC_TIME LC_COLLATE LC_MONETARY LC_MESSAGES  
AcceptEnv LC_PAPER LC_NAME LC_ADDRESS LC_TELEPHONE LC_MEASUREMENT  
AcceptEnv LC_IDENTIFICATION LC_ALL  
  
X11Forwarding no  
PrintMotd yes  
PrintLastLog yes  
Compression delayed  
ShowPatchLevel no  
  
Banner /etc/sshbanner  
  
Subsystem sftp /usr/libexec/openssh/sftp-server  
# -EOF-
```

- ```
-----  
▪ vi /etc/sshbanner  
-----
```

```
PSP Custom Firmware 5.00 M33-3  
have a nice day.. :)  
-----
```

- Edit file konfigurasi *iptables*:
  - `mv /etc/sysconfig/iptables /etc/sysconfig/iptables.ORIG`
  - `vi /etc/sysconfig/iptables`

```
-----  
  
# iptables configuration  
# re-modded version by whatsoever  
*filter
```

```

:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -i eth0 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 443 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 7331 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 8000 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 10000 -j ACCEPT
# -----
# to use the NACL for SSHD
#-A RH-Firewall-1-INPUT -i eth0 -p tcp --dport 7331 -s aa.bb.xx.yy/24 -j ACCEPT
# -----
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
# -EOF-
-----

```

○ Edit file konfigurasi *kernel*:

- mv /etc/sysctl.conf /etc/sysctl.conf.ORIG
- vi /etc/sysctl.conf

```

-----

# Kernel sysctl configuration
# See sysctl(8) and sysctl.conf(5) for more details.
kernel.panic = 60
net.ipv4.ip_forward=0
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.lo.accept_source_route = 0
net.ipv4.conf.eth0.accept_source_route = 0
net.ipv4.conf.default.accept_source_route = 0
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
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.lo.accept_redirects = 0
net.ipv4.conf.eth0.accept_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.all.log_martians = 0
net.ipv4.conf.lo.log_martians = 0
net.ipv4.conf.eth0.log_martians = 0
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.lo.accept_source_route = 0
net.ipv4.conf.eth0.accept_source_route = 0
net.ipv4.conf.default.accept_source_route = 0
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

```

```

net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.lo.accept_redirects = 0
net.ipv4.conf.eth0.accept_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
kernel.sysrq = 0
net.ipv4.tcp_fin_timeout = 15
net.ipv4.tcp_keepalive_time = 1800
net.ipv4.tcp_window_scaling = 0
net.ipv4.tcp_sack = 0
net.ipv4.tcp_timestamps = 0
net.ipv4.tcp_syncookies = 1
net.ipv4.icmp_echo_ignore_broadcasts = 1
net.ipv4.icmp_ignore_bogus_error_responses = 1
net.ipv4.conf.all.log_martians = 1
net.ipv4.tcp_max_syn_backlog = 1024
net.ipv4.tcp_max_tw_buckets = 1440000
net.ipv4.ip_local_port_range = 16384 65536
net.ipv4.conf.all.arp_announce = 2
net.ipv4.conf.all.arp_ignore = 1
# -EOF-

```

- ```

-----

```
- chown root:root /etc/sysctl.conf
  - chmod 0600 /etc/sysctl.conf
  - /sbin/sysctl -p
  - /sbin/sysctl -w net.ipv4.route.flush=1
  - /etc/init.d/iptables restart
  - /etc/init.d/sshd restart

○ Edit host.conf:

- Vi /etc/host.conf

```

-----
order host, bind
nospoof on
-----

```

○ Testing the httpd:

- vi /var/www/html/info.php

```

-----
<?php
phpinfo();
?>
-----

```

- Lalu arahkan browser anda ke <http://ip-atau-domain-box-anda.net>
- Perhatikan bahwa tidak terdapat patch suhosin di PHP anda.

○ Patching the PHP with suhosin:

- cd /usr/local/src/
- wget [http://centos.cbn.net.id/5.2/updates/SRPMS/php-5.1.6-20.el5\\_2.1.src.rpm](http://centos.cbn.net.id/5.2/updates/SRPMS/php-5.1.6-20.el5_2.1.src.rpm)
- rpm -ivh php-5.1.6-12.el5.src.rpm
- biarkan saja kalo ada yang peringatan "*warning*".
- cd /usr/src/redhat/SOURCES
- wget [http://www.hardened-php.net/suhosin/\\_media/suhosin-patch-5.1.6-0.9.6.patch.gz](http://www.hardened-php.net/suhosin/_media/suhosin-patch-5.1.6-0.9.6.patch.gz)

- gunzip suhosin-patch-5.1.6-0.9.6.patch.gz
- mv suhosin-patch-5.1.6-0.9.6.patch php-5.1.6-suhosin.patch
- cd /usr/src/redhat/SPECS/
- vi php.spec

```
-----
[...]
Source51: php.ini
```

```
Patch0: php-5.1.6-suhosin.patch
Patch1: php-5.1.4-gnusrsrc.patch
Patch2: php-5.1.4-warnings.patch
Patch5: php-4.3.3-install.patch
Patch6: php-5.0.4-norpath.patch
Patch7: php-4.3.2-libtool15.patch
Patch13: php-5.0.2-phpize64.patch
# Patch14: php-5.1.6-ecalloc.patch
[...]
%setup -q
%patch0 -p1 -b .suhosin
%patch1 -p1 -b .gnusrsrc
%patch2 -p1 -b .warnings
%patch5 -p1 -b .install
%patch6 -p1 -b .norpath
%patch7 -p1 -b .libtool15
%patch13 -p1 -b .phpize64
# %patch14 -p1 -b .ecalloc
[...]
```

- rpmbuild -ba php.spec
- cd /usr/src/redhat/RPMS/i386
- rpm -Uvh --force php-\*
- cd /usr/src
- wget http://www.hardened-php.net/suhosin/\_media/suhosin-0.9.20.tgz
- tar xvfz suhosin-0.9.20.tgz
- cd suhosin-0.9.20
- phpize
- ./configure
- make
- make install
- vi /etc/php.d/suhosin.ini

```
-----
extension=suhosin.so
-----
```

- restart httpd "/etc/init.d/httpd restart"
- voila.. PHP anda telah di patch menggunakan suhosin.

- Instalasi Aplikasi Web

- Joomla

- mkdir /var/www/html/cms
- cd /var/www/html/cms
- wget http://joomlancode.org/gf/download/frsrelease/8897/32884/Joomla\_1.5.8-Stable-Full\_Package.zip
- unzip Joomla\_1.5.8-Stable-Full\_Package.zip
- chmod 777 /var/www/html/cms/\*

- jalankan browser anda dan tuju ke `http://localhost/cms`
- dan ikuti petunjuk instalasi joomla
- jangan lupa untuk melakukan `chmod` sesuai dengan parameter yang anda inginkan terhadap folder `"/var/www/html/cms"`.

- Hardening

- Instalasi APF (Advanced Policy Firewall)

- `cd /root/source/`
- `wget http://www.r-fx.ca/downloads/apf-current.tar.gz`
- `tar -zxvf apf-current.tar.gz`
- `cd apf-9*`
- `./install.sh`
- `rm -rf /root/source/apf-9*`
- `mv /etc/apf/conf.apf /etc/apf/conf.apf.ORIG`
- `vi /etc/apf/conf.apf`

```

-----
#!/bin/bash
#
# APF 9.6 [apf@r-fx.org]
# Copyright (C) 1999-2007, R-fx Networks <proj@r-fx.org>
# Copyright (C) 2007, Ryan MacDonald <ryan@r-fx.org>

DEVEL_MODE="0"
INSTALL_PATH="/etc/apf"

IFACE_IN="eth0"
IFACE_OUT="eth0"
IFACE_TRUSTED=""

SET_VERBOSE="1"
SET_FASTLOAD="0"
SET_VNET="0"
SET_ADDIFACE="0"
SET_MONOKERN="0"
SET_REFRESH="120"
SET_TRIM="500"
VF_ROUTE="1"
VF_CROND="1"
VF_LGATE=""

RAB="1"
RAB_SANITY="1"
RAB_PSCAN_LEVEL="3"
RAB_HITCOUNT="1"
RAB_TIMER="300"
RAB_TRIP="1"
RAB_LOG_HIT="1"
RAB_LOG_TRIP="0"

TCP_STOP="DROP"
UDP_STOP="DROP"
ALL_STOP="DROP"

```

PKT\_SANITY="1"  
PKT\_SANITY\_INV="0"  
PKT\_SANITY\_FUDP="1"  
PKT\_SANITY\_PZERO="1"  
PKT\_SANITY\_STUFFED="0"

TOS\_DEF="0"  
TOS\_DEF\_RANGE="512:65535"  
TOS\_0=""  
TOS\_2=""  
TOS\_4=""  
TOS\_8="21,20,80"  
TOS\_16="25,110,143"

TCR\_PASS="0"      TCR\_PORTS="33434:33534"  
ICMP\_LIM="10/s"  
RESV\_DNS="1"  
RESV\_DNS\_DROP="1"  
BLK\_P2P\_PORTS="1214,2323,4660\_4678,6257,6699,6346,6347,6881\_6889,6346,7778"  
BLK\_PORTS="135\_139,111,513,520,445,1433,1434,1234,1524,3127"  
BLK\_MCATNET="0"  
BLK\_PRVNET="0"  
BLK\_RESNET="1"  
BLK\_IDENT="1"

SYSCTL\_CONNTRACK="34576"  
SYSCTL\_TCP="1"  
SYSCTL\_SYN="1"  
SYSCTL\_ROUTE="0"  
SYSCTL\_LOGMARTIANS="0"  
SYSCTL\_ECN="0"  
SYSCTL\_SYNCOOKIES="1"  
SYSCTL\_OVERFLOW="0"

HELPER\_SSH="1"  
HELPER\_SSH\_PORT="7331"  
HELPER\_FTP="0"  
HELPER\_FTP\_PORT="21"  
HELPER\_FTP\_DATA="20"

IG\_TCP\_CPORTS="80,443,7331,8000,10000"  
IG\_UDP\_CPORTS=""  
IG\_ICMP\_TYPES="3,5,11,0,30,8"

**EGF="1"**  
**EG\_TCP\_CPORTS="80"**  
**EG\_UDP\_CPORTS="53"**  
**EG\_ICMP\_TYPES="all"**  
**EG\_TCP\_UID=""**  
**EG\_UDP\_UID=""**  
**EG\_DROP\_CMD="eggdrop psybnc bitchx BitchX init udp.pl"**

USE\_DS="1"  
DS\_URL="feeds.dshield.org/top10-2.txt"    # block.txt url (no \*/://)

```

DS_URL_PROT="http"           # protocol to use for wget
USE_DROP="1"
DROP_URL="www.spamhaus.org/drop/drop.lasso" # drop.lasso url (no */)
DROP_URL_PROT="http"        # protocol to use for wget

USE_ECNSHAME="1"
ECNSHAME_URL="r-fx.ca/downloads/ecnshame.lst" # url (no */)
ECNSHAME_URL_PROT="http"    # protocol to use for wget

USE_RD="1"
RD_URL="r-fx.ca/downloads/reserved.networks" # reserved.networks url
RD_URL_PROT="http"          # protocol to use for wget

USE_RGT="0"
GA_URL="yourhost.com/glob_allow.rules"      # glob_allow.rules url (no */)
GA_URL_PROT="http"                          # protocol for use with wget
GD_URL="yourhost.com/glob_deny.rules"       # glob_deny.rules url (no */)
GD_URL_PROT="http"                          # protocol for use with wget

LOG_DROP="1"
LOG_LEVEL="crit"
LOG_TARGET="LOG"
LOG_IA="1"

LOG_LGATE="0"
LOG_EXT="0"
LOG_RATE="100"
LOG_APF="/var/log/apf_log"

CNFINT="$INSTALL_PATH/internals/internals.conf"
. $CNFINT
# -EOF-
-----

```

- lalu jalankan perintah “/etc/init.d/apf restart”

#### ○ Instalasi LES (Linux Environment Security)

- cd /root/source/
- wget http://www.r-fx.ca/downloads/les-current.tar.gz
- tar -zxvf les-current.tar.gz
- cd les-0.\*
- ./install.sh
- cd ..
- rm -rf /root/source/les\*
- jalan perintah “les –help” atau “/usr/local/sbin/les –help”

#### ○ Instalasi LSM (Linux Socket Monitor)

- cd /root/source/
- wget http://www.r-fx.ca/downloads/lsm-current.tar.gz
- tar -zxvf lsm-current.tar.gz
- cd lsm-0.\*
- ./install.sh
- cd ..
- rm -rf /root/source/lsm-\*

- `vi /usr/local/lsm/conf.lsm`
  - ganti parameter `USER="root"` dengan email anda
- Instalasi Webmin \*optional\*
  - `cd /root/source/`
  - `wget http://transact.dl.sourceforge.net/sourceforge/webadmin/webmin-1.441-1.noarch.rpm`
  - `rpm -ivh webmin-1.441-1.noarch.rpm`
  - `rm -f webmin-1.441-1.noarch.rpm`
  - jalankan perintah `"/etc/init.d/webmin start"`
- Lain-lain
  - dstat
    - `mkdir /root/source/`
    - `cd /root/source/`
    - `wget http://dag.wieers.com/rpm/packages/dstat/dstat-0.6.7-1.el5.rf.noarch.rpm`
    - `rpm -ivh dstat-0.6.7-1.el5.rf.noarch.rpm`
    - jalankan perintah `"dstat -tcidylp -M topcpu --tcp --udp -f 5"`
    - parameter lain harap refer ke manual `"dstat"` (man dstat)
  - whowatch
    - `wget http://dag.wieers.com/rpm/packages/whowatch/whowatch-1.4-1.2.el5.rf.i386.rpm`
    - `rpm -ivh whowatch-1.4-1.2.el5.rf.i386.rpm`
    - jalankan perintah `"whowatch"`
    - parameter lain harap refer ke manual `"whowatch"` (man whowatch)
  - pktstat
    - `wget -c http://dag.wieers.com/rpm/packages/pktstat/pktstat-1.8.4-1.el5.rf.i386.rpm`
    - `rpm -ivh pktstat-1.8.4-1.el5.rf.i386.rpm`
    - jalankan perintah `"pktstat -cnTt -i eth0 -w 2"`
    - parameter lain harap refer ke manual `pktstat` (man pktstat)
  - iftop
    - `wget http://dag.wieers.com/rpm/packages/iftop/iftop-0.17-1.el5.rf.i386.rpm`
    - `rpm -ivh iftop-0.17-1.el5.rf.i386.rpm`
    - jalankan perintah `"iftop -nNpBP -i eth0"`
    - parameter lain harap refer ke manual `iftop` (man iftop)
  - tcptrack
    - `wget http://dag.wieers.com/rpm/packages/tcptrack/tcptrack-1.3.0-1.el5.rf.i386.rpm`
    - `rpm -ivh tcptrack-1.3.0-1.el5.rf.i386.rpm`
    - jalankan perintah `"tcptrack -i eth0"`
    - parameter lain harap refer ke manual `tcptrack` (man tcptrack)
  - splunk
    - `cd /root/source/`
    - `wget 'http://www.splunk.com/index.php/download_track?file=3.4.1/linux/splunk-3.4.1-45588.i386.rpm&ac=&wget=true&name=wget&typed=releases'`
    - `rpm -ivh splunk-3.4.1-45588.i386.rpm`
    - jalankan perintah `"/opt/splunk/bin/splunk start"`
    - *web console* dapat anda liat di `"http://server-anda.com:8000"`

- cleaning up
  - `cd /root/source/`
  - jalankan perintah "`rm -f *.rpm`".
- BONUS
  - How to **OWNING** a Tiger in 10 Minutes (maybe less).
    - reboot
    - pencet "command key" + "s" button. (single user mode)
    - tetap di "single user mode"
    - ketik "`fsck -fy`" lalu pencet "return"
    - jalanin command ini secara berurutan:
      - `mount -uw /`
      - `rm /private/var/db/.AppleSetupDone`
      - `exit`
    - reboot
    - congratz.. u manage to manipulate the box !!