OS : CentOS 5.x
작성일 : 2009년 2월
작성자 : http://www.100dedi.net
문서 버전  Ver 1.2


# 리눅스 보안 지침 및 최적화

부 서 명 :  기술지원팀
작 성 자 :  박 성 우
검 수 자 :  전 선 표
작 성 일 자 : 2009년 2월

# 목 차

## [1] OS 설치 및 패키지 업데이트

### 1. 리눅스 설치

1) 개요

리눅스를 설치할 때 시스템을 어떤 용도로  사용할 것인가에 따라 파티션구성 및 패키지 선택이 달라질 수 있다. 서버는 여러 사용자에게 서비스를 제공하는 것을 목적으로 함으로써 X-windows 나 컴파일러, 게임 등 불필요한 패키지는 설치하지 않도록 한다.

2) Partitioning

2-1) 파티셔닝 목적

# 디스크공간 고갈 유형의 DoS 공격에 대한 방어
# SUID 프로그램 에 대한 보호
# 백업과 업그레이드 관리 용이
# 빠른 부팅
# 각 파일시스템에 대한 마운트 방법 제어가능
# 하드링크를 통한 해킹방지
=> 현재는 시스템 및 데이터를 복원하고자 할때 소요되는 시간 및 비용에 비하여 백업된 데이터를 이용한 시스템 재설치 및 복원이 효율적으로 판단되어 파티션을 나누지 않는것이 추세이다. 이로인하여 백업의 중요성이 강하게 부각되고 있다.

2-2) 설치 패키지 선택

Custom mode 로 최소설치 또는 Server Mode 로 설치

### 2. OS 설치 후 기본설정

1) 시스템 정보 확인

last, pstree, ifconfig, netstat -anp, df -h, cat /proc/cpuinfo, cat /proc/meminfo, uname -a 등의 명령으로 OS설치후의 시스템의 기본정보를 체크한다.

2) 시스템 및 CMOS 시간동기화

아래의 명령처럼 외부의 time 서버를 기준으로 시스템 및 하드웨어의 시간을 조정한다.
Cron에 등록하여 하루 또는 일주일에 한번은 시간동기화를 실행한다.

```
# rdate -s time.bora.net && clock -r && clock -w
```

3) 초기 실행데몬 선택

ntsysv or setup 명령을 통하여 시스템 운영에 불필요한 데몬을 중지시킨다.
초기 시스템은 iptables, network, sshd, syslog 만 실행하도록 한다.

4) 불필요한 패키지 제거

시스템에 설치되어 있는 피키지 리스트는 /root/install.log 에 기록되어 있다. 뿐만아니라 yum을 이용한 package update 시에도 그 기록이 install.log에 남게된다.
아래 보기와 같이 기본적으로 이용하지 않는 패키지는 제거한다.

# 기본적으로 이용하지 않는 패키지 (yum remove 명령어 이용)
eject, kernel-pcmcia-cs, raidtools, setserial, statserial, rsh, redhat-config-mouse
gpm-devel, gpm, nfs-utils, yp-tools ypbind, isdn4k-utils, fam-devel, anacron, irda-utils,
:: yum remove “제거를원하는패키지명”

5)fstab 수정 ( tmp device 등에는 일반 사용자가 SUID 바이너리를 실행하거나 디바이스 파일을 생성하게 하면 안된다. 또한 프로그램 실행권한까지 제거하는것이 좋다. )

**파티션을 나눌때는 시스템 파티션과 DATA 파티션을 구분하여 설정하는것이 좋다.**

ex) 시스템 파티션 : / , /tmp　　ex) DATA 파티션 : /home, /usr/local

```
[root@localhost smile_tech]# vi /etc/fstab
LABEL=/                 /                       ext3    defaults        1 1
LABEL=/home             /home                   ext3    defaults        1 1
LABEL=/usr/local        /usr/local              ext3    defaults        1 1
```

```
devpts                  /dev/pts                devpts  gid=5,mode=620  0 0
tmpfs                   /dev/shm                tmpfs   defaults,noexec,nosuid,nodev    0 0
proc                    /proc                   proc    defaults        0 0
sysfs                   /sys                    sysfs   defaults        0 0
LABEL=SWAP-hdc2         swap                    swap    defaults        0 0
```

**=> 파티션을 나눌때는 절대적인 법칙은 없다. 서버의 용도에 맞도록 파티션을 나누는것이 올바르며 파티션 분할이 시스템 보안의 기초임을 유념하는것이 좋다.**

### 3. 최신패키지로 업데이트

불필요한 패키지 제거후 최신버전으로 업데이트한다.

업데이트 방법중 yum ( Yellow dog Updater, Modified)을 통한 방법을 예로든다.

# Yum Update

1) Download

wget http://linux.duke.edu/projects/yum/download/2.0/yum-2.0.7-1.noarch.rpm

wget ftp://ftp.kreonet.net/pub/Linux/redhat/linux/9/en/os/i386/RedHat/RPMS/libxml2-python-2.5.4-1.i386.rpm

2) 설치

rpm -Uvh libxml2-python-2.5.4-1.i386.rpm

rpm -Uvh yum-2.0.7-1.noarch.rpm

3) 설정

3-1) cat /etc/yum.conf

```
[main]
  cachedir=/var/cache/yum
  keepcache=1
  debuglevel=2
  logfile=/var/log/yum.log
  pkgpolicy=newest
  distroverpkg=redhat-release
  tolerant=1
  exactarch=1
  obsoletes=1
  gpgcheck=1
  plugins=1
  metadata_expire=1800

  # PUT YOUR REPOS HERE OR IN separate files named file.repo
  # in /etc/yum.repos.d
```

3-2) cat /etc/yum.repos.d/CentOS-Base.repo

```
[base]
  name=CentOS-$releasever - Base
  mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=os
  #baseurl=http://mirror.centos.org/centos/$releasever/os/$basearch/
  gpgcheck=1
  gpgkey=http://mirror.centos.org/centos/RPM-GPG-KEY-CentOS-5

  #released updates
  [updates]
  name=CentOS-$releasever - Updates
  mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=updates
  #baseurl=http://mirror.centos.org/centos/$releasever/updates/$basearch/
  gpgcheck=1
  gpgkey=http://mirror.centos.org/centos/RPM-GPG-KEY-CentOS-5
```

```
#packages used/produced in the build but not released
[addons]
name=CentOS-$releasever - Addons
mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=addons
#baseurl=http://mirror.centos.org/centos/$releasever/addons/$basearch/
gpgcheck=1
gpgkey=http://mirror.centos.org/centos/RPM-GPG-KEY-CentOS-5

#additional packages that may be useful
[extras]
name=CentOS-$releasever - Extras
mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=extras
#baseurl=http://mirror.centos.org/centos/$releasever/extras/$basearch/
gpgcheck=1
gpgkey=http://mirror.centos.org/centos/RPM-GPG-KEY-CentOS-5

#additional packages that extend functionality of existing packages
[centosplus]
name=CentOS-$releasever - Plus
mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=centosplus
#baseurl=http://mirror.centos.org/centos/$releasever/centosplus/$basearch/
gpgcheck=1
enabled=0
gpgkey=http://mirror.centos.org/centos/RPM-GPG-KEY-CentOS-5
```

4) 업데이트 실행 및 검토

#] yum -c /etc/yum.conf update

#] rpm -qa > /root/update.log ( 현채 update 된 rpm package 들의 정보 저장 )

5) grub.conf 설정

업데이트 후 아래와 같이 grub.conf 파일에서 root 파티션 위치를 LABEL명 대신 파티션명으로 수정하는것이 추후 관리에 용이하다.

# /etc/grub.conf

```
Default=0                       ## title Number 이며, 0 부터 순서대로 카운팅 된다.
timeout=5
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
title CentOS (2.6.18-92.1.22.el5)                          ## title number 0
    root (hd0,0)
    kernel /vmlinuz-2.6.18-92.1.22.el5 ro root=/dev/sda3
    initrd /initrd-2.6.18-92.1.22.el5.img
title CentOS (2.6.18-92.1.18.el5)                          ## title number 1
    root (hd0,0)
    kernel /vmlinuz-2.6.18-92.1.18.el5 ro root=/dev/sda3
    initrd /initrd-2.6.18-92.1.18.el5.img
title CentOS (2.6.18-92.1.13.el5)                          ## title number 2
    root (hd0,0)
    kernel /vmlinuz-2.6.18-92.1.13.el5 ro root=/dev/sda3
    initrd /initrd-2.6.18-92.1.13.el5.img
title CentOS (2.6.22.19)                                   ## title number 3
    root (hd0,0)
    kernel /vmlinuz-2.6.22.19 ro root=/dev/sda3
    initrd /initrd-2.6.22.19.img
```

6) HDD 속도체크
아래 보기와 같이 커널업데이트후 하드디스크 속도를 체크한다.
ATA HDD 인 경우 읽기 속도는 50MB/sec, SATA 는 60MB/sec 정도이면 정상이다.
# UDMA 사용여부 체크 ( SATA 방식의 HDD 는 적용되지 않음 )

```
[root@ ~]# hdparm /dev/hda

/dev/hda:
 multcount    = 16 (on)
 IO_support   =  0 (default 16-bit)
 unmaskirq    =  0 (off)
 using_dma    =  1 (on)
 keepsettings =  0 (off)
 readonly     =  0 (off)
 readahead    = 256 (on)
 geometry     = 16383/255/63, sectors = 81920000, start = 0
```

# SATA HDD 의 경우

```
[root@~]# hdparm /dev/sda

/dev/sda:
 IO_support   =  0 (default 16-bit)
 readonly     =  0 (off)
 readahead    = 256 (on)
 geometry     = 9729/255/63, sectors = 156301488, start = 0
```

# HDD 속도 검사
buffer 에서의 속도가 60MB 정도가 일반적이며 속도가 현저히 떨어질경우 HDD 교체를 해야한다.
단, HDD 속도검사는 single Mode 에서 가장 안정적으로 측정가능하며, 서비스중인 상태에서는
정확한 측정값을 얻기가 힘들다.

```
/dev/sda:
 Timing cached reads:   3304 MB in  2.00 seconds = 1653.14 MB/sec
 Timing buffered disk reads:  172 MB in  3.01 seconds =  57.23 MB/sec
```

# history 파일에 날짜및 시간 설정 => /etc/profile 파일에 다음내용 설정

```
HISTTIMEFORMAT=" %Y-%M-%D_%H:M:%SW"
export HISTTIMEFORMAT
```

위 내용 기록 후 다음 실행
`# source /etc/profile`
**→ OS 설치 및 기본설정이 완료된 후 커널을 항상 최신버전으로 유지하는것이 중요하다.**

## [2] 시스템 기본 보안 및 최적화 설정

### 1. 콘솔 로그인 데몬수 조정
콘솔상에서 로긴 가능한 데몬수를 1개로 수정

```
# vi /etc/inittab

# Run gettys in standard runlevels
1:2345:respawn:/sbin/mingetty tty1
#2:2345:respawn:/sbin/mingetty tty2  => 주석
#3:2345:respawn:/sbin/mingetty tty3  => 주석
#4:2345:respawn:/sbin/mingetty tty4  => 주석
#5:2345:respawn:/sbin/mingetty tty5  => 주석
#6:2345:respawn:/sbin/mingetty tty6  => 주석
```

변경 후 바로 적용을 원하는 경우 " init q " 입력

## 2. 일반 사용자의 root 로긴 제한

# 다음 설정과 같이 wheel 그룹에 속한 유저만이 root 로 로그인이 가능하도록 한다.

```
# 계정생성
일반계정 생성시에 초기 그룹에 users 를 할당한다.
root로 로긴 가능하게 할 계정은 아래와 같이 wheel 그룹에 추가한다.
# useradd -g100 -G10 admin

# cat /etc/group
 wheel:x:10:root,admin      => wheel그룹에 admin 계정이 등록 되었다.

# chmod 4750 /bin/su
/bin/su'의 모드를 4750(rwsr-x---)으로 변경하였습니다
# ls -al /bin/su
-rwsr-x--- 1 root wheel 24120  5월 25  2008 /bin/su
```

## 3. sshd 환경설정

# ssh로 서버 접근시 root 계정으로 바로 로그인하는 것을 허용하지 않는다.

```
#] cat /etc/ssh/sshd_config

## ssh 접속포트를 변경하고자 할 경우 다음 내용을 수정 후 방화벽에서 해당 포트를 함께 open한다.
Port 22       # 포트를 변경하여 사용한다.
## AllowUsers 설정을 하면 AllowUsers 에 등록되지 않은 계정은 ssh 접속을  하지 못한다.
## 여러개의 계정을 등록 원하는 경우 스페이스로 구분한다.
## ex) AllowUsers admin test1 test2
AllowUsers admin        # admin 계정만 로그인 가능

## ssh 접속시 root 계정으로 Direct 접속을 차단함으로써 2중인증의 효과와 함께 root 계정의
비밀번호를 보호한다.
PermitRootLogin no      # root 계정으로 직접 접속 금지
```

## 4. 불필요한 계정 및 그룹 삭제

# /etc/passwd 와 /etc/shadow 에 등록되어 있는 미사용 계정이나 그룹을 제거한다.
Adm, news, gopher, sync, shutdown, halt, operator, games, ftp, rpc, rpcuser, nfsnobody, nscd
등이 대표적으로 사용하지 않는 계정들이다.
Lp 계정은 printer를 사용하지 않는경우 제거한다.

# 비밀번호 보안설정
/etc/login.defs 를 활용하여 최소 길이와 최소 사용기간, 최대 사용기간을 설정한다.

```
PASS_MAX_DAYS   99999
PASS_MIN_DAYS   0
PASS_MIN_LEN    5
PASS_WARN_AGE   7
```

## ## 서버 운용에 유용한 명령어들..

## 5. SUID와 SGID 파일 및 디렉토리, 파일 퍼미션 조정

가장 기본적인 크래킹기법이 되는것이 SUID, SGID 파일을 이용한 권한 획득 법이다.
따라서 SUID, SGID 파일에 대한 철저한 관리가 필요하다.
아래와 같이 OS 최초 setting 단계의 suid, sgid 파일의 리스트를 관리하는것이 한 방법이다.

```
#] Find / -type f -perm +6000 -exec ls -alF {} W; > /root/suid-before.txt
```

이후 주기적으로 점검하여 비교한다.

```
#] find / -type f -perm +6000 -exec ls -alF {} W; > /root/suid_after.txt
#] diff /root/suid-before.txt /root/suid_after.txt   => 아무 결과가 출력되지 않으면 정상
```

```
# 기본 파일들의 퍼미션 수정또한 필요하다.
 echo “chmod 500 /proc” >> /etc/rc.d/rc.local
```

**6. 파일 및 디렉토리 보안**

```
 6-1) 무소속 파일 찾아 소유권 부여
 : 무소속 파일은 언제든 크래커에 노출될 수 있으므로 반드시 권한을 부여한다.
 #] find / -user -o -nogroup
 #] find W( -nouser -o -nogroup W)W -exec chown root.root {} W;

 6-2) /dev 에 device 파일 외의 것이 있는지 확인
 * /dev 또는 .udev 디렉토리는 시스템에 존재하는 장치에 대한 정보를 유지하는 DB
 * /dev 디렉토리에는 sysfs에 등록된 장치외에는 생성되지 않도록 신경써야 한다.
 #] find /dev -type f -exec ls -al {} W;
 6-3) .foward 파일 생성여부 점검
 #] find / -name ‘.foward’ -exec cat {} W; -print

 6-4) 원격접속 허용파일 생성여부 점검
 #] find / -name .rhosts -exec cat {} W; -print

 6-5) 숨김 파일 혹은 비정상 파일 존재여부 점검
 #] find / -name “..” -print -xdev
 #] find / -name “.*” -print -xdev | cat -v
 #] find / -name “.*” W-exec ls -alF {} W;
```

**7. 커널 변수 조정**

```
# 커널 변수 조정은 큰 효과를 보기는 어렵다. 그러나 시스템상에서 기본적으로 보안설정은 한다는
  의미에서 설정을 하는것이 좋으며, 간략하게 내용을 숙지하는것이 시스템관리에 도움이 된다.

# /etc/sysctl.conf 에 설정된 내용을 적용시킨다.
sysctl -p

# 현재 적용된 ( 적용가능한 ) 설정을 sysctl-before.txt 파일로 저장한다.
sysctl -a > sysctl-before.txt

# vi /etc/sysctl.conf ( default 설정 내용과 다른 부분만 적용 )
```

```
# /etc/sysctl.conf 에 추가한다.
# /etc/sysctl.conf 를 적용시킬땐 sysctl -p 명령을 실행한다.(default : /etc/sysctl.conf)
# 변수 하나만 변경시엔 sysctl -w net.ipv4.ip_forward=0 이런 식으로..

# icmp redirects를 허용하지 않는다.
net.ipv4.conf.eth0.accept_redirects=0
net.ipv4.conf.lo.accept_redirects=0
net.ipv4.conf.default.accept_redirects=0
net.ipv4.conf.all.accept_redirects=0
# icmp redirects를 보내지 않는다.
net.ipv4.conf.eth0.send_redirects = 0
net.ipv4.conf.lo.send_redirects = 0
net.ipv4.conf.default.send_redirects = 0
net.ipv4.conf.all.send_redirects = 0

# 게이트웨이로부터의 redirect를 허용하지 않음으로써 스푸핑을 막기 위해 설정한다.
net.ipv4.conf.eth0.secure_redirects=0
net.ipv4.conf.lo.secure_redirects=0
net.ipv4.conf.default.secure_redirects=0
```

```
net.ipv4.conf.all.secure_redirects=0
# 스푸핑을 막기 위해 source route 패킷을 허용하지 않는다.
net.ipv4.conf.eth0.accept_source_route=0
net.ipv4.conf.lo.accept_source_route=0
net.ipv4.conf.default.accept_source_route=0
net.ipv4.conf.all.accept_source_route=0

# 자신의 네트워크가 스푸핑된 공격지의 소스로 쓰이는 것을 차단한다.
net.ipv4.conf.eth0.rp_filter=2
net.ipv4.conf.lo.rp_filter=2
net.ipv4.conf.default.rp_filter=2
net.ipv4.conf.all.rp_filter=2

# 스푸핑된 패킷이나 소스라우팅, Redirect 패킷에 대해 로그파일에 정보를 남긴다.
net.ipv4.conf.eth0.log_martians=1
net.ipv4.conf.lo.log_martians=1
net.ipv4.conf.default.log_martians=1
net.ipv4.conf.all.log_martians=1

# syncookies가 작동할 때 SYN Flooding 공격이 있으면 messages 파일에 아래와 같은 내용이 출력된다.
net.ipv4.tcp_syncookies = 1

# 일정한 시간과 IP별로 보내고 받는 SYN 재시도 횟수를 3회로 제한한다.
net.ipv4.tcp_syn_retries = 3

# 연결을 종료시 소요되는 시간을 줄여준다(기본 설정값: 60).
net.ipv4.tcp_fin_timeout=20
################### END ###################
```

```
# 설정 변경값을 적용시킨다.
sysctl -p /etc/sysctl.conf

# 변경후 적용된 sysctl 값을 sysctl-after.txt 파일에 저장한다.
sysctl -a > sysctl-after.txt

# 변경전 값(sysctl-before)과 변경후 값(sysctl-after)을 비교하여 차이를 sysctl-last에 저장
diff sysctl-before sysctl-after > sysctl-last
```

### 8. iptables 설치

```
# 최신 커널버전 확인
[root@smile_tech saint]# finger @finger.kernel.org
```

```
# 현재 커널 버전 확인
[root@smile_tech saint]# uname -a
Linux smile_tech 2.6.18-92.1.22.el5 #1 SMP Tue Dec 16 12:03:43 EST 2008 i686 athlon i386
GNU/Linux

# 최신 커널버전 확인
The latest stable version of the Linux kernel is:          2.6.28.3
The latest prepatch for the stable Linux kernel tree is:   2.6.29-rc3
The latest snapshot for the stable Linux kernel tree is:   2.6.29-rc3-git7
The latest 2.4 version of the Linux kernel is:             2.4.37
The latest 2.2 version of the Linux kernel is:             2.2.26
The latest prepatch for the 2.2 Linux kernel tree is:      2.2.27-rc2
The latest -mm patch to the stable Linux kernels is:       2.6.28-rc2-mm1
```

```
# iptables 의 string 패치는 커널 2.6 버전이상에서는 default 로 포함되어 설치된다.
  따라서 2.6 이하의 커널버전을 이용하는 경우 2.6이상의 최신 커널로 업데이트만 실행하여도
  string 패치를 추가적으로 적용할 필요가 없다.
```

# iptables source 컴파일

```
cd /usr/src/
[root@smile_tech src]# wget http://www.netfilter.org/files/iptables-1.3.1.tar.bz2
[root@smile_tech src]# rpm -e lokkit
[root@smile_tech src]# rpm -e iptables

[root@smile_tech src]# cd /usr/src/iptables
[root@smile_tech iptables]# make
[root@smile_tech iptables]# find /* > /root/iptables1
[root@smile_tech iptables]# make install
[root@smile_tech iptables]# make install-devel
[root@smile_tech iptables]# find /* > /root/iptables2

# iptables source 컴파일 전/후 비교
[root@smile_tech iptables]# diff /root/iptables1 /root/iptables2 > /root/iptables-install
```

# connlimit 및 Geoip 패치

```
# Source 다운로드
  Kernel 2.6.23 버전에는 default 로 connlimit은 설정이 되어 있다.

최신 커널   => ftp://ftp.kernel.org/pub/linux/kernel/v2.6/linux-2.6.28.tar.gz
patch       => ftp://ftp.netfilter.org/pub/patch-o-matic-ng/snapshot/patch-o-matic-
ng-20090302.tar.bz2
iptables    => ftp://ftp.netfilter.org/pub/iptables/iptables-1.4.2-rc1.tar.bz2
patch match => http://bjerkeset.com/patches/geoip-match-2.6.22.patch.gz

# geoip patch 풀기
[root@localhost ~]# gunzip geoip-match-2.6.22.patch.gz
[root@localhost ~]# ln -s /usr/src/linux-2.6.16.27 /usr/src/linux
[root@localhost ~]# ln -s /usr/src/iptables-1.3.5 /usr/src/iptables


# Iptablse Source 설치
[root@localhost ~]# cd /usr/src/iptables
[root@localhost iptables]# ./configure
[root@localhost iptables]# make && make install;


# Geoip patch
[root@localhost iptables]# cd /usr/src/patch-o-matic-ng-200xxxxx
[root@localhost patch-o-matic-ng-20090302]# IPTABLES_DIR=/usr/src/iptables KERNEL_DIR=/usr/src/
linux ./runme --download ./patchlets

[root@localhost patch-o-matic-ng-20090302]# IPTABLES_DIR=/usr/src/iptables KERNEL_DIR=/usr/src/
linux ./runme geoip
Do you want to apply this patch [N/y/t/f/a/r/b/w/q/?] y

[root@localhost patch-o-matic-ng-20090302]# IPTABLES_DIR=/usr/src/iptables KERNEL_DIR=/usr/src/
linux ./runme connlimit
Do you want to apply this patch [N/y/t/f/a/r/b/w/q/?] y
```

Excellent! Source trees are ready for compilation.

#geoip patch 적용
]# cd /usr/src/linux/net/ipv4/netfilter/
]# cp /usr/src/geoip-match-2.6.22.patch /usr/src/linux/net/ipv4/netfilter/
patch -p1 < geoip-match.patch --> 위 명령 실행시 패치 할 원본 파일을 묻게되며 원본 파일은 ipt_geoip.c를 입력해야 하며 커널 2.6.22는 ipt_geoip.c를 패치해 주어야 make에서 오류가 발생하지 않음

Networking -> Networking support -> Networking options -> Network packet filtering ( replases ipchains ) ->
Core Netfilter Configuration

# 커널 컴파일 --> 커널 컴파일 관련 모든 명령은 커널소스 디렉토리 내에서 실행해야함

  make memuconfig 아래 항목에서 geoip 및 connlimit선택, connlimit의 경우 해당 Netfilter Configuration 하위 메뉴에
  있는 모든 메뉴를 선택해 주어야 make상에서 오류가 발생하지 않음 -> Device Drivers -> Networking support -> Networking support -> Networking options -> Network packet filtering (replaces ipchains) -> IP: Netfilter Configuration -> [*] geoip match support

# make --> 커널 버전 변동없이 geoip만 추가 할 경우는 아래의 순서로 컴파일을 진행함

    make oldconfig
    make modules
    make modules_install
# make modules

# make modules_install

# make install

# 국가 DB 최신 정보로 업데이트

geoip 모듈은 /var/geoip 경로의 DB파일 참조함
- CSV 파일 변환 wget http://people.netfilter.org/peejix/geoip/tools/csv2bin-20041103.tar.gz tar zxfp csv2bin-20041103.tar.gz cd csv2bin make

- 국가별 DB 다운로드 wget http://www.maxmind.com/download/geoip/database/GeoIPCountryCSV.zip unzip GeoIPCountryCSV.zip ./csv2bin ../GeoIPCountryWhois.csv mkdir /var/geoip cp geoipdb.bin /var/geoip/ cp geoipdb.idx /var/geoip/

cp /usr/src/iptables/iptables /sbin -> iptables 소스파일의 iptables를 /sbin으로 복사

# IPTABLES geoip 룰 적용 = 예제)
  - 일본과 미국에서의 웹 접속을 차단하고 다른 곳에서의 접속은 허용할 때
  iptables -A INPUT -p tcp --dport 80 -m geoip --src-cc JP,US -j DROP
  iptables -A INPUT -p tcp --dport 80 -j ACCEPT

  - 한국에서의 ftp만 허용하고 나머지 국가에서의 접속은 차단하고자 할 때
  iptables -A INPUT -p tcp --dport 21 -m geoip --src-cc KR -j ACCEPT
  iptables -A INPUT -p tcp --dport 21 -j DROP
  또는 iptables -A INPUT -p tcp --dport 21 -m geoip ! --src-cc KR -j DROP

# iptables 정책설정

```
# 웹서버 포트 지정
WebPort=80
iptables=/usr/local/sbin/iptables
# Setting default filter policy ( 기본정책 )
$iptables -P INPUT DROP
$iptables -P OUTPUT DROP
$iptables -P FORWARD DROP

# Allow unlimited traffic on loopback
$iptables -A INPUT -i lo -j ACCEPT
$iptables -A OUTPUT -o lo -j ACCEPT
$iptables -A INPUT -i lo -s 127.0.0.1 -d 127.0.0.1 -j ACCEPT

# Invalid Packet drop       # Invalid IPs 공인IP가 아니거나 미리 예약된 IP들
$iptables -A INPUT -m state -state INVALID -j DROP
$iptables -A INPUT -s 10.0.0.0/8 -j DROP
$iptables -A INPUT -s 172.16.0.0/12 -j DROP
$iptables -A INPUT -s 192.168.0.0/16 -j DROP
$iptables -A INPUT -s 255.255.255.255/32 -j DROP
$iptables -A INPUT -s 127.0.0.0/8 -j DROP
$iptables -A INPUT -s 240.0.0.0/5 -j DROP
$iptables -A INPUT -s 0.0.0.0/8 -j DROP
$iptables -A INPUT -s 169.254.0.0/16 -j DROP
$iptables -A INPUT -s 172.16.0.0/12 -j DROP
$iptables -A INPUT -s 192.0.2.0/24 -j DROP
$iptables -A INPUT -s 192.168.0.0/16 -j DROP
$iptables -A INPUT -s 224.0.0.0/4 -j DROP
$iptables -A INPUT -s 240.0.0.0/5 -j DROP
$iptables -A INPUT -s 248.0.0.0/5 -j DROP
$iptables -A INPUT -s 255.255.255.255/32 -j DROP

# SYN Flooding Protect ( 공격이 심한경우 limit-burst 값을 하향 조정)
$iptables -A INPUT -p tcp -syn -m limit -limit 1/s -limit-burst 20 -j ACCEPT
$iptables -A INPUT -p tcp -syn -j DROP
# DNS ( 외부 네임서버 이용시)
$iptables -A OUTPUT -p udp -dport 53 -j ACCEPT
$iptables -A INPUT -p udp -sport 53 -j ACCEPT
$iptables -A OUTPUT -p tcp -dport 53 -j ACCEPT
$iptables -A INPUT -p tcp -sport 53 -m state -state ESTABLISHED,RELATED -j ACCEPT

# Allow incoming ssh
$iptables -A INPUT -p tcp -dport 22 -j ACCEPT
$iptables -A INPUT -p tcp -sport 22 -j ACCEPT
$iptables -A OUTPUT -p tcp -sport 22 -j ACCEPT
$iptables -A OUTPUT -p tcp -dport 22 -j ACCEPT

# Allow incoming http
$iptables -A INPUT -p tcp -dport 80 -m recent -update -seconds 1 -hitcount 30 -name HTTP -j
DROP
$iptables -A INPUT -p tcp -dport 80 -j ACCEPT
$iptables -A INPUT -p tcp -sport 80 -j ACCEPT
$iptables -A OUTPUT -p tcp -sport 80 -j ACCEPT
$iptables -A OUTPUT -p tcp -dport 80 -j ACCEPT
```

```
# Allow MySQL
$iptables -A INPUT -p tcp -dport 3306 -j ACCEPT
$iptables -A INPUT -p tcp -sport 3306 -j ACCEPT
$iptables -A OUTPUT -p tcp -sport 3306 -j ACCEPT
$iptables -A OUTPUT -p tcp -dport 3306 -j ACCEPT

# for AUTH
$iptables -A INPUT -p tcp -dport 113 -m state -state NEW,ESTABLISHED -j ACCEPT

# time / rdate
$iptables -A OUTPUT -p tcp -dport 37 -j ACCEPT
$iptables -A INPUT -p tcp -sport 37 -j ACCEPT
$iptables -A OUTPUT -p udp -dport 37 -j ACCEPT
$iptables -A INPUT -p udp -sport 37 -j ACCEPT

## MAIL(SMTP)
$iptables -A INPUT -p tcp -s 0.0.0.0/0 -d 100.100.100.100 --dport 25 -j ACCEPT
$iptables -A OUTPUT -p tcp -s 100.100.100.100 -d 0.0.0.0/0 --dport 25 -j ACCEPT

## 특정 IP (102.102.102.102)에서 ssh와 ftp만 접근 허용 ##
$iptables -A INPUT -p tcp -s 102.102.102.102 -d 100.100.100.100 --dport 22 -j ACCEPT
$iptables -A OUTPUT -p tcp -s 100.100.100.100 -d 102.102.102.102 --sport 22 -j ACCEPT
$iptables -A INPUT -p tcp -s 102.102.102.102 -d 100.100.100.100 --dport 21 -j ACCEPT
$iptables -A OUTPUT -p tcp -s 100.100.100.100 -d 102.102.102.102 --sport 21 -j ACCEPT
$iptables -A INPUT -p udp -s 102.102.102.102 -d 100.100.100.100 --dport 20 -j ACCEPT
$iptables -A OUTPUT -p udp -s 100.100.100.100 -d 102.102.102.102 --sport 20 -j ACCEPT
$iptables -A INPUT -p tcp -s 102.102.102.102 -d 100.100.100.100 --dport 20 -j ACCEPT
$iptables -A OUTPUT -p tcp -s 100.100.100.100 -d 102.102.102.102 --sport 20 -j ACCEPT
### 특정 IP 에서 접근 허용 끝 ###
```

## [3] 홈페이지 보안관리

### 1. 관리자페이지 접근통제

1-1) 문제점

웹서비스의 사용자나 데이터, 컨텐츠를 손쉽게 관리하기 위한 목적으로 다양한 기능과 권한을 갖고 있는 홈페이지의 관리자페이지는 일반적으로 추측하기 쉬운 URL ( /admin, /manager )을 사용하고 있어 ID/PW 에 대한 크랙 또는 접근 허가 정책의 미설정으로 웹관리자의 권한이 노출되어 홈페이지의 변조뿐만아니라 웹서버의 권한까지 노출되는 위험에 있다.

1-2) 조치방법

관리자 로그인페이지는 유추하기 어려운 디렉토리명이나 파일명을 사용한다.
별도의 IP 레벨로 접근권한을 설정. ( htaccess ) 웹인터페이스는 SSL과 같은 암호화를 적용.

1-3) apache 설정

httpd.conf 파일의 Directory 섹션의 AllowOverride 지시자에서 AuthConfig, Limit 추가하여 .htaccess 를 통하여 사용자게정, 패스워드를 등록한 사용자만 접그 및 특정 IP에서만 접근 가능하도록 설정한다.

#] vi /usr/local/apache/conf/httpd.conf

```
# 특정 페이지의 인증설정
<Directory /home/www/관리페이지>
AllowOverride FileInfo AuthConfig Limit
Order deny,allow
Deny from all
</Directory>
AccessFileName .htaccess
<Files ~ "^Wht">
```

```
Order allow,deny
Deny from all
</Files>

# 특정 디렉토리 리스팅 제한  : 해당 디렉토리의 indexes 옵션을 제거
<Directory /home>
    Options indexes
    AllowOverride indexes
    IndexOptions FancyIndexing VersionSort FoldersFirst NameWidth=*
    #Order deny,allow
    Order allow,deny
    Allow from all
</Directory>
```

1-4) apache htaccess 설정
관리자 페이지등의 비공개용 페이지의 경우 접속제한을 설정하여 외부침입에 대응해야 한다.

```
# 1-3)에서의 apache 설정이 완료되면 해당페이지 (관리자 페이지 등)의 디렉토리에서 access설정을
  한다.
# cat /home/www/관리자페이지/.htaccess
  AuthName "Manager Page"
  AuthType Basic
  AuthUserFile /home/www/관리자페이지/.htpasswd
  AuthGroupFile /dev/null
  require valid-user
  Order deny,allow
  Deny from all
  Allow from 10.10.10.10
```

```
# 위와같이 설정 후 htpasswd 파일 생성
#] ~apacheDIR/bini/htpasswd -c /home/www/관리자페이지/.htpasswd 관리계정명
      New password: *******
      Re-type new password: ******
      Adding password for user 관리계정명
```

1-5) apache scritp 실행방지
파일업로드폴더에 .htaccess 파일을 만들고 아래와 같이 설정하여 업로드된 Server Side Script가 실행되지 않도록 설정하며, FileMatch 지시자를 이용하여 해당파일에 대해서 직접 URL 호출을 금지시킨다.

```
$ cat .htaccess
<FileMatch "W.(php|inc|lib)">
Order allow,deny
Deny from all
<FileMatch>
AddType text/html .html .htm .php .php3 .php4 .phtml .phps .inc .cgi .pl .shtml .jsp
```

## 2. 주요 Application 취약점

제로보드, 테크노트, 그누보드 : 각 게시판의 개발사이트에서 최신버전으로 패치
- 제로보드 : http://www.zeroboard.com/
- 테크노트 : http://technote.co.kr/php/technote1/home.php
- 그누보드 : http://sir.co.kr/

## 3. Mass Injection 및 웹 취약점

개발단계에서의 수정 및 보완이 불가능하다면 웹 방화벽을 이용하도록 한다.
공개 웹방화벽 전용 홈페이지 : http://www.krcert.or.kr/firewall/index.htm

[4] 응용프로그램 보안

1. bind

# /etc/named.conf 수정

```
# recursion 을 허용할 ip로  recursion 필요 없는경우 no 로 설정
# Recursion : 간략히 설명하면 Recursion 이 허용되면 서버상에 설정된 도메인 뿐만 아니라 누구든지
  해당 서버를 네임서버로 설정하여 질의가 가능하게 된다.

123.123.123.123 및 123.123.123.0/24 대역으로 제한한 예입니다.
Options {
            allow-recursion {123.123.123.123; 123.123.123.0/24; };
        };

recursion 을 허용할 필요가 없다면 다음과 같은 설정으로 차단합니다.
options {
           allow-recursion {none;};
        };
또는,
options {
          recursion no;
        };

# Transfer 전송을 허용할 IP 주소나 대역을 기록한다.
# Transfer 는 2차 네임서버를 구동하는 경우 적용 ( 네임서버 1대 작동하는 경우 no 로 설정)
일반적으로 Zone Transfer는 1차네임서버와 2차네임서버간의 동일한 Zone 정보를 유지하기 위해서 이루어지기 때
문에 2차네임서버에서만 Zone Transfer를 할 수 있도록 설정해야 한다. 만약, 허가되지 않은 사용자에
게 영역전송을 허
용할 경우 DNS 서버의 중요한 정보가 유출되며, 공격자는 전송받은 Zone 정보를 이용하여 호스트 정
보, 네트워크 구성
형태 등의 많은 정보를 파악할 수 있게 된다.

 options {
         allow-transfer {127.0.0.1; local-ipaddress;
         }

# version
# Bind 의 버전은 외부에 노출되면 해당 버전에 대한 취약점을 이용하여 공격에 이용될 수 있음.
  version  " xxxxxx  "
```

2. ftp

# vsftpd.conf 파일에서 다음 사항은 최소한 설정되어야 한다.

```
Anonymous_enable=NO                # anonymous 접근 거부
chroot_local_user=YES              # 로그인후 자신의 계정의 파일만 열람 가능
```

3. php

```
# 보안상의 이유로 서버단에서는 url_fopen 을 비 활성화 한다.
# 단 부득이하게 fopen( "http://..... ) 라는 값을 사용하여야 하는경우 세션 단계에서 url_fopen을
# 허용하도록 한다.
allow_url_fopen = Off

# 세션 단계에서 url_fopen 허용
# error 발생하는 페이지의 최 상단에 다음 구문 삽입
# [? ini_set( "allow_url_fopen" ,  "1" ); ?]

# 페이지 에러를 표시하지 않는다 ( 소스구문 노출을 방지한다. )
```

```
display_errors = Off
# 단, 개발단계에서의 에러확인이 필요한 경우 On 으로 설정하여 test 한다.

# register_globals 를 On 으로 하면 변수가 get, post, session 변수인지 체크하지 않아도 됩니다.
# 쓰기에 따라서 보안적인 부분에 문제가 생길 수 있습니다.
register_globals = Off
```

4. mail

# /etc/mail/sendmail.mc 설정 ( 설정 변경 후 make -C /etc/mail 을 이용한다. )

```
# 다음 사항 주석을 제거하여 인증을 거치지 않은 계정은 메일 발송이 되지 않도록 변경
TRUST_AUTH_MECH(`EXTERNAL DIGEST-MD5 CRAM-MD5 LOGIN PLAIN')dnl
define(`confAUTH_MECHANISMS', `DIGEST-MD5 CRAM-MD5 LOGIN PLAIN')dnl

## --> cyrus-sasl/lib-sasl auth 인증을 사용하는설정


# Addr 부분을 127.0.0.1 에서 0.0.0.0으로 바꿈 ( 127.0.0.1 로 설정되어 있을경우 외부 Relay

# 허용되지 않는다.

DAEMON_OPTIONS(`Port=smtp,Addr=0.0.0.0, Name=MTA')dnl
## --> localhost로 설정시 외부에서 메일발송이 불가능(아웃룩/외부메일설정등)
```

# /etc/mail/access 설정 ( Relay 설정 )

```
# RELAY / DROP / REJECT 설정   ( RELAY 앞의 공백은 tab 키를 이용 )
localhost.localdomain  RELAY
localhost RELAY
127.0.0.1 RELAY

# hacker.com 도메인 메일 거부하는 경우
hacker.com REJECT

# RELAY 설정 후 open Relay 상태 확인

# 외부의 서버에서 relay 체크할 서버의 25번 포트로 접속한다.
telnet 222.222.222.222 25
220 test.com ESMTP Sendmail 8.13.8/8.13.8; ........
ehlo test.com
250-test.com Hello xxxxxxxxx [333.333.333.333], pleased to meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-8BITMIME
250-SIZE
250-DSN
250-ETRN
250-AUTH LOGIN PLAIN
250-DELIVERBY
250 HELP
MAIL FROM: test@test.com
250 2.1.0 test@test.com... Sender ok
RCPT TO: test@test.com
550 5.7.1 test@test.com... Relaying denied. Proper authentication required.
QUIT
=>  Relay Denied !!
## 중요 !!
```

```
Relay test 중에 아래와 같은 메세지가 나오는 경우가 있다.
550 5.7.1 tset@test.com... Relaying denied. IP name lookup failed [xxx.xxx.xxx.xxx]
이 경우 메일을 발송하는 곳의 Reverse IP 가 lookup 되지않아 발송이 되지 않은 것으로
Reverse IP가 질의되는경우 Spam Relay 로 악용될 수 있다.
Sendmail.cf 파일에서 다음 내용을 주석처리한다면 이러한 위험도 예방할 수 있다.

#R<FAIL>        $#error $@ 5.7.1 $: "550 Relaying denied. IP name lookup failed "
$&{client_name}
```

# SPF 레코드 등록 및 Reverse Domain 등록

```
# Reverse Domain 등록 확인
# Reverse Lookup 이 되지 않을경우 해외쪽에서 Spam 으로 간주되는 경우가 많다.
# Reverse 란 도메인 질의의 반대되는 개념으로 IP 를 질의 하였을때 해당 도메인과 매칭을 한다.
 [root@thiswell named]# nslookup
 > 222.222.222.222
 Server:         220.90.215.11
 Address:        220.90.215.11#53

 222.222.222.222.in-addr.arpa      name = test.com.

# spf 레코드 등록 확인
# SPF 기술은 메일 헤더에서, 발송한 서버의 IP 와 From: 헤더의 메일 주소의 도메인에 등록된 TXT
  레코드 값을 비교하여 매치가 되는지 여부를 확인 해 보내는 이의 메일 주소를 속이지 하지
  못하도록 하는 방법이다.

 [root@thiswell named]# nslookup
 > set type=txt
 > test.com

 Non-authoritative answer:
 test.com    text = 'v=spf1 ip4:222.222.222.222 ~all'

   Authoritative answers can be found from:
   test.com    nameserver = ns.test.com.test.com.
```

# SPF 관련 참조 문서 ( 스마일 서브 홈페이지 “서버관리강좌” 란 )
http://www.1000dedi.net/hosting/gnuboard4/bbs/board.php?bo_table=serverLecture&wr_id=757

# 개 정 내 용 #