

ssh root

```
root ssh
. root su
```

```
$ sudo vim /etc/ssh/sshd_config
PermitRootLogin no
```

ftp

```
ftp
sql
```

```
vsftp
```

```
$ sudo vim /etc/vsftpd.conf
chroot_local_user=YES
```

```
chroot_list_file
```

ssh

```
가 . ftp 가
/home 가 ..
```

```
$ chmod 701 /home
$ chmod 701 /
```

root

```
gcc gcc+ df ps
가
```

```
$ chmod 100 /usr/bin/gcc /usr/bin/g++
$ chattr +i /usr/bin/gcc /usr/bin/g++
```

가 +i , , 가

```
$ chmod 100 /bin/ps
$ chattr +i /bin/ps
```

. c c++ 가 가

su

su

```
$ vim /etc/group
wheel:x:10:root,manager
```

wheel:x:10:root , su 가
manager su
su

```
$ chown root.wheel /bin/su
$ chmod 4750 /bin/su
$ chattr +i /bin/su
```

su root wheel

ping

ping ping 가

```
$ vi /etc/sysctl.conf
net.ipv4.icmp_echo_ignore_all=1
```

net.ipv4.icmp_echo_ignore_all=1 ping

```
$ /sbin/sysctl -w net.ipv4.icmp_echo_ignore_all=0
```

ping 0 1

SYN Flooding

Dos

tcp_syscookies 1

```
$ vi /etc/sysctl.conf
net.ipv4.tcp_syscookies=1
```

. KLDP

Setuid

Setuid

passwd 가 root 가

```
$ ls -al /usr/bin/passwd
-rwsr-xr-x 1 root root 22984 1 7 2007 /usr/bin/passwd
```

rwsr rwxr rwsr . setuid가

setuid(0) c

Setuid 가 . setuid

find setuid가

```
$ find / -user root -perm -4000 -print
/usr/kerberos/bin/ksu
/usr/lib/nspluginwrapper/plugin-config
/usr/libexec/openssh/ssh-keysign
/usr/sbin/userhelper
/usr/sbin/usernetctl
/usr/sbin/suexec
/usr/sbin/ccreds_validate
/usr/bin/chfn
/usr/bin/rcp
/usr/bin/newgrp
/usr/bin/rlogin
/usr/bin/sudoedit
/usr/bin/at
/usr/bin/rsh
/usr/bin/chsh
/usr/bin/chage
/usr/bin/gpasswd
```

```
/usr/bin/crontab
/usr/bin/staprun
/usr/bin/sudo
/usr/bin/passwd
/usr/bin/Xorg
/lib/dbus-1/dbus-daemon-launch-helper
/sbin/umount.nfs4
/sbin/pam_timestamp_check
/sbin/mount.ecryptfs_private
/sbin/mount.nfs
/sbin/unix_chkpwd
/sbin/mount.nfs4
/sbin/umount.nfs
/bin/su
/bin/ping6
/bin/umount
/bin/mount
/bin/ping

$ find / -user root -perm -2000 -print
/sbin/netreport
/usr/bin/wall
/usr/bin/crontab
/usr/bin/ssh-agent
/usr/bin/write
/usr/bin/lockfile
/usr/bin/screen
/usr/local/firewall
/usr/libexec/utempter/utempter
/usr/sbin/sendmail.sendmail
/usr/sbin/lockdev
```

```
          setuid          ping          root
                setuid          .
```

```
$ chmod 100 /bin/ping
```

```
/usr/bin/change
/usr/bin/wall
/usr/bin/chfn
/usr/bin/at
/bin/mount
/bin/unmount
/usr/bin/crontab
/usr/bin/newgrp
/usr/bin/write
/usr/sbin/usernetctl
/bin/ping
```

/bin/traceroute

가 가 .

...

ftp ssh . lastlog ssh
root .bash_history

•

From:

<http://www.obg.co.kr/doku/> - **OBG WiKi**

Permanent link:

<http://www.obg.co.kr/doku/doku.php?id=linux:security>

Last update: **2020/11/29 14:09**

