

root ,	3
	3
/etc/passwd	3
/etc/shadow	3
/etc/hosts	3
/etc/(x)inetd.conf	4
/etc/syslog.conf	4
/etc/services	4
SUID, SGID, Sticky bit	4
,	5
world writable	5
/dev device	5
\$HOME/.rhosts, hosts.equiv	6
IP	6
hosts.lpd	7
UMASK	7
	8
	8
	8

Last update: 2022/01/11 08:21 https://atl.kr/dokuwiki/doku.php/%ED%8C%8C%EC%9D%BC_%EB%B0%8F_%EB%94%94%EB%A0%89%ED%84%B0%EB%A6%AC_%EA%B4%80%EB%A6%AC

root ,

/etc/profile, ~/.bash_profile PATH “.”, “::”

```
(          ) PATH=.:$PATH:$HOME/bin  
(          ) PATH=$PATH:$HOME/bin:.
```

가

```
#find / -nouser -print
```

/etc/passwd

/etc/passwd

```
#chmod 644 /etc/passwd  
#chown root /etc/passwd
```

/etc/shadow

/etc/shadow

```
#chmod 400 /etc/shadow  
#chown root /etc/shadow
```

/etc/hosts

/etc/hosts

```
#chmod 600 /etc/hosts  
#chown root /etc/hosts
```

/etc/(x)inetd.conf

/etc/xinetd.conf /etc/xinetd.d/

```
#chown root /etc/xinetd.conf
#chmod 600 /etc/xinetd.conf
```

※ /etc/xinetd.d/

/etc/syslog.conf

CentOS6

```
#chown root /etc/rsyslog.conf
#chmod 640 /etc/rsyslog.conf
```

/etc/services

```
#chown root /etc/services
#chmod 644 /etc/services
```

SUID, SGID, Sticky bit

Step 1)

```
#chmod -s <file_name>
```

Step 2)

```
#find / -xdev -user root -type f \( -perm -04000 -o -perm -02000 \) -exec
ls -al {} \;
```

Step 3)

Setuid

(가)

```
#!/usr/bin/chgrp <group_name> <setuid_file_name>
#!/usr/bin/chmod 4750 <setuid_file_name>
```

,

```
: .profile, .kshrc, .cshrc, .bashrc, .bash_profile, .login, .exrc,
.netrc
```

```
#ls -l .bash_profile
#chmod o-w .bash_profile
```

world writable

```
world writable : 가 ( :
rwxrwxrwx root root < >)
```

```
#find / -type f -perm -2 -exec ls -l {} \;
#chmod o-w <file name>
```

/dev

device

```
#find /dev -type f -exec ls -l {} \;
major, minor number 가 device
```

\$HOME/.rhosts, hosts.equiv

```
#ls -al /etc/hosts.equiv
#chown root /etc/hosts.equiv
#chmod 600 /etc/hosts.equiv
```

/etc/hosts.equiv \$HOME/.rhosts +

```
#cat /etc/hosts.equiv (or $HOME/.rhosts)
```

IP

Step 1) vi /etc/hosts.deny ()

Step 2) , (ALL Deny)

```
( )
( ) ALL:ALL
```

Step 3) vi /etc/hosts.allow ()

```
( )
( ) sshd : 192.168.0.148, 192.168.0.6
```

()

< TCP Wrapper 가 >

SYSTAT, FINGER, FTP, TELNET, RLOGIN, RSH, TALK, EXEC, TFTP, SSH

< TCP Wrapper >

/etc/hosts.deny -> IP /etc/hosts.allow ->
IP

-->

/etc/passwd

```
#chown <user_name> <user_home_directory>
#chmod o-w <user_home_directory>
```

/etc/passwd 가 , 가 (/) 가

```
Step 1) 가
#userdel <user_name>
Step 2) 가
#vi /etc/passwd
#test:x:501:501:::/bin/bash ( 가 / )
#test:x:501:501:~/home/test:/bin/bash ( / -> /home/test)
```

```
#ls -al [ ]
#find / -type f -name "*" ( )
#find / -type d -name "*" ( )
```

Step 1) -t Step 2) ,

From: <https://atl.kr/dokuwiki/> - AllThatLinux!

Permanent link: https://atl.kr/dokuwiki/doku.php/%ED%8C%8C%EC%9D%BC_%EB%B0%8F_%EB%94%94%EB%A0%89%ED%84%B0%EB%A6%AC_%EA%B4%80%EB%A6%AC

Last update: 2022/01/11 08:21

