

finger 3

Anonymous FTP 4

r 5

cron 6

Dos 7

NFS 7

NFS 8

automountd 9

RPC 9

NIS, NIS+ 10

tftp, talk 11

Sendmail 12

Sendmail 12

Sendmail 13

DNS 14

DNS Zone Transfer 14

..... 15

..... 16

..... 17

..... 18

..... 19

..... 19

..... 20

ssh 21

ftp 21

ftp shell 22

Ftpusers 22

Ftpusers 23

at 25

SNMP 26

SNMP 26

..... 27

NFS 28

expn, vrfy 28

Apache 29

finger

Finger() 가 가 가 가

※ Finger(): who 가
finger

rhel inetd

```
#cat /etc/inetd.conf
#finger stream tcp nowait bin /usr/lbin/fingered
```

fingerd

Step 1) /etc/inetd.conf finger # ()

```
( ) finger stream tcp nowait bin /usr/lbin/fingered fingerd
( ) #finger stream tcp nowait bin /usr/lbin/fingered fingerd
```

Step 2) inetd

```
#ps -ef | grep inetd
root 141 1 0 15:03:22 ? 0:01 /usr/sbin/inetd -s
#kill -HUP [PID]
```

rhel xinetd

```
#ls -all /etc/xinetd.d/* | egrep "echo finger"
```

finger 가

Step 1) vi /etc/xinetd.d/finger Step 2) (Disable
= yes)

```
service finger
{
```

```
socket_type = stream
wait = no
user = nobody
server = /usr/sbin/in.fingerd
disable = yes
}
```

Step 3) xinetd

```
#service xinetd restart
```

Anonymous FTP

	FTP	FTP	
Anonymous FTP(FTP)	anonymous	가
	가 local exploit		

FTP

/etc/passwd ftp anonymous

```
#userdel ftp
```

ProFTP

conf/proftpd.conf anonymous User, Useralias
(proftpd.conf)

```
<Anonymous ~ftp> <- Anonymous
# User ftp <- anonymous
Group ftp
# UserAlias anonymous ftp <-
</Anonymous>
```

vsFTP

vsFTP (/etc/vsftpd/vsftpd.conf , /etc/vsftpd.conf)

anonymous_enable=NO

<https://access.redhat.com/solutions/2048173>

r

r-command 가 NET Backup

rsh, rlogin, rexec r command 가

rsh, rlogin, rexec (shell, login, exec)

```
#ls -all /etc/xinetd.d/* | egrep "rsh|rlogin|rexec" | egrep -v "grep|klogin|kshell|kexec"
```

Step 1) vi /etc/xinetd.d/ rlogin, rsh, rexec

Step 2) (Disable = yes) • /etc/xinetd.d/rlogin • /etc/xinetd.d/rsh • /etc/xinetd.d/rexec

```
service rlogin
{
  socket_type = stream
  wait = no
  user = nobody
  log_on_success += USERID
  log_on_failure += USERID
  server = /usr/sbin/in.fingerd
  disable = yes
}
```

Step 3) xinetd

```
#service xinetd restart
```

r-command (\$HOME/.rhosts, hosts.equiv) Step 1) r command
- .rhosts, hosts.equiv hostname(IP)
* IP IP - .rhosts, hosts.equiv 600 -
TCP_Wrapper IP 가
rlogin, rshell, rexec backup, (/etc/hosts.equiv .rhosts
-

)

<https://access.redhat.com/solutions/7321>

cron

cron

root

crontab

,

```

cron      /etc/crontab ←
  /etc/cron.daily ←
/etc/cron.monthly ←
/etc/cron.hourly ←
/etc/cron.weekly ←
/etc/cron.allow ← crontab
/etc/cron.deny ← crontab

```

Step 1) crontab SUID가 SUID (crontab OS) ※ crontab

```

# ls -l /usr/bin/crontab
# chmod 750 /usr/bin/crontab

```

Step 2) cron

```

# chown root <cron >
# chmod 640 <cron >

```

■ crontab Step 1) /etc/cron.d/cron.allow
/etc/cron.d/cron.deny

```

#chown root /etc/cron.d/cron.allow
#chmod 640 /etc/cron.d/cron.allow
#chown root /etc/cron.d/cron.deny
#chmod 640 /etc/cron.d/cron.deny

```

Step 2) /etc/cron.d/cron.allow /etc/cron.d/cron.deny

```

# cat /etc/cron.allow (crontab )
# cat /etc/cron.deny (crontabl )

```


Step 1) NFS

```
#systemctl stop nfs
#systemctl disable nfs
#kill -9 [PID]
```

Step 2)

```
1.
#ls -al /etc/rc.d/rc*.d/* | grep nfs
2.
#mv /etc/rc.d/rc2.d/S60nfs /etc/rc.d/rc2.d/_S60nfs
```

NFS

가

가

가

가 NFS
, everyone

NFS

/etc/exports

Step 1) /etc/exports

가

가

```
( ) #/stand host1( IP ) host2
```

Step 2)

nobody

```
# vi /etc/export
# /stand host1 (root_squash)
```

() "insecure"

Step 3. NFS

```
#/etc/exportfs -u
#/etc/exportfs -a
```

automountd

가 automountd
가 RPC(Remote Procedure Call)

root , 가

automountd

```

automountd
#ps -ef | grep automount(or autofsd)
root 1131 1 0 jun 15 ? 32:11 /usr/sbin/automountd
Step 1) automountd
#kill -9 [PID]
Step 2)
1.
#ls -al /etc/rc.d/rc*.d/* | grep automount(or autofsd)
2.
#mv /etc/rc.d/rc2.d/S28automountd /etc/rc.d/rc2.d/_S28automountd

```

RPC

(, Dos,) RPC

(Buffer Overflow), Dos, RPC

가 root

RPC : rpc.cmsd, rpc.ttdbserverd, sadmind, rusersd, walld, sprayd, rstatd, rpc.nisd, rexd, rpc.pcnfsd, rpc.statd, rpc.yppupdated, rpc.rquotad, kcms_server, cachefsd

LINUX (inetd) Step 1) /etc/inetd.conf # ()

```

( ) rpc.cmsd/2-4 dgram rpc/udp wait root /usr/dt/bin/rpc.cmsd rpc.cmsd
( ) #rpc.cmsd/2-4 dgram rpc/udp wait root /usr/dt/bin/rpc.cmsd rpc.cmsd

```

Step 2) inetd

```

#ps -ef | grep inetd
root 141 1 0 15:03:22 ? 0:01 /usr/sbin/inetd -s
#kill -HUP 141

```

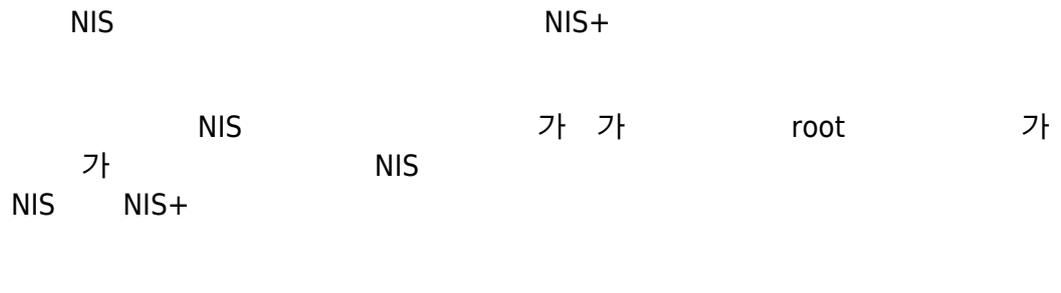
LINUX (xinetd) Step 1) vi /etc/xinetd.d/ RPC
Step 2) (Disable = yes)

```
service finger
{
  disable = yes
  socket_type = stream
  wait = no
  -
}
```

Step 3) xinetd

```
#service xinetd restart
```

NIS, NIS+



```
#ps -ef | egrep "ypserv|ypbind|ypxfrd|rpc.yppasswdd |rpc.yupdated"
root 3809 3721 0 08:44:40 ? 0:00 /usr/lib/nis/ypserv
```

Step 1) NFS

```
#kill -9 [PID]
```

Step 2) , 1.

```
#ls -al /etc/rc.d/rc*.d/* | egrep
"ypserv|ypbind|ypxfrd|rpc.yppasswdd|rpc.yupdated"
```

2.

```
#mv /etc/rc.d/rc2.d/S73ypbind /etc/rc.d/rc2.d/_S73ypbind
```

tftp, talk

가

Linux [inetd]

```
#cat /etc/inetd.conf | grep "tftp|talk|ntalk"  
tftp dgram udp6 SRC nobody /usr/sbin/tftpd tftpd -n
```

Step 1) vi `"/etc/inetd.conf"`

```
#vi /etc/inetd.conf
```

Step 2) tftp, talk, ntalk

```
#tftp dgram udp6 SRC nobody /usr/sbin/tftpd tftpd -n  
#talk dgram udp wait root /usr/sbin/talkd talkd  
#ntalk dgram udp wait root /usr/sbin/talkd talkd
```

Step 3) inetd

```
#kill -HUP [inetd pid]
```

Linux [xinetd] tftp, talk, ntalk

```
#vi /etc/xinetd.d/tftp  
#vi /etc/xinetd.d/talk  
#vi /etc/xinetd.d/ntalk
```

Step 1) vi `/etc/xinetd.d/` tftp, talk, ntalk

Step 2) (Disable = yes) `/etc/xinetd.d/tftp` `/etc/xinetd.d/talk`
`/etc/xinetd.d/ntalk`

```
service tftp
{
    socket_type = dgram
    protocol = udp
    wait = yes
    user = root
    server = /usr/sbin/in.tftpd
    server_args = -s /tftpboot
    disable = yes
}
```

Step 3) xinetd

```
#service xinetd restart
```

Sendmail

Sendmail
Sendmail

Sendmail (Buffer Overflow)
가

1. Sendmail

```
#ps -ef | grep sendmail
```

2. Sendmail

```
#telnet localhost 25
```

Sendmail , <http://www.sendmail.org/> , OS

SMTP , 가
Dos

SMTP

```
#ps -ef | grep sendmail | grep -v "grep"
#cat /etc/mail/sendmail.cf | grep "R\$*" | grep "Relaying denied"
R$* $#error $@ 5.7.1 $: "550 Relaying denied"
```

Step 1) vi /etc/mail/sendmail.cf /etc/sendmail.cf

Step 2)

```
( ) #R$* $#error $@ 5.7.1 $: "550 Relaying denied"
( ) R$* $#error $@ 5.7.1 $: "550 Relaying denied"
```

Step 3) IP, domain, Email Address sendmail ()

```
#cat /etc/mail/access
)
localhost.localdomain RELAY
localhost RELAY
127.0.0.1 RELAY
spam.com REJECT
```

Step 4) DB

```
#makemap hash /etc/mail/access.db < /etc/mail/access
```

Sendmail



```
#ps -ef | grep sendmail | grep -v "grep"
#grep -v '^ *#' /etc/mail/sendmail.cf | grep PrivacyOptions
```

Step 1) vi /etc/mail/sendmail.cf

가 Zone Transfer Zone , ,

DNS /etc/named.conf allow-transfer xfrnets

```
#ps -ef | grep named | grep -v "grep"
#cat /etc/named.conf | grep 'allow-transfer'
#cat /etc/named.boot | grep "xfrnets"
```

< DNS > ■ BIND8 DNS (named.conf)

```
Options {
  allow-transfer ( IP);
};
```

■ BIND4.9 DNS (named.conf)

```
Options
xfrnets IP
```

< DNS > DNS (DNS SID)

```
#ps -ef | grep named
root 3809 3721 0 08:44:40 ? 0:00 /usr/sbin/in.named
```

DNS

```
#kill -9 [PID]
```

WEB

가

Indexes

```
#vi /[Apache_home]/conf/httpd.conf
Options Indexes FollowSymLinks
```

“Indexes”

Step 1) vi `/[Apache_home]/conf/httpd.conf`

```
#vi /[Apache_home]/conf/httpd.conf
```

Step 2) Options Indexes () Option
Indexes

```
<Directory />
  Options Indexes FollowSymLinks
  AllowOverride None
  Order allow, deny
  Allow from all
</Directory>
```

() Option Indexes -Indexes

```
<Directory />
  Options Indexes ( -Indexes)
  AllowOverride None
  Order allow, deny
  Allow from all
</Directory>
```

Apache root

root 가 ,
root 가 가 root

Apache (User Group)

```
#vi /[Apache_home]/conf/httpd.conf
User [root가 ]
Group [root가 ]
```

Step 1) User & Group 가 User & Group root가
 User [root가] Group [root가]

Step 2) Apache

가
 가 가 가
 AllowOverride Authconfig

```
#vi /[Apache_home]/conf/httpd.conf
AllowOverride None
```

AllowOverride None

Step 1) vi /[Apache_home]/conf/httpd.conf

```
#vi /[Apache_home]/conf/httpd.conf
```

Step 2) AllowOverride AuthConfig

```
( ) AllowOverride 'None'
<Directory "/usr/local/apache2/htdocs">
  AllowOverride None
  Allow from all
</Directory>

( ) AllowOverride 'AuthConfig'
<Directory "/usr/local/apache2/htdocs">
  AllowOverride AuthConfig
  Allow from all
</Directory>
```

Step 3) .htaccess ()

```
AuthName " "
AuthType Basic
```

```
AuthUserFile /usr/local/apache/test/.auth
Require valid-user
```

```
AuthName ( ) AuthType (Basic
, Digest) AuthUserFile ( )
( ) Require , AuthGroupFile
```

Step 4)

```
htpasswd -c /usr/local/apache/test/.auth test
New password:
Re-type new password:
Adding password for user test
[root@localhost apache]#
```

Step 5)

Apache

Apache

Apache htdocs

```
#ls -ld /[Apache_home]/htdocs/manual
#ls -ld /[Apache_home]/manual
```

가

Step 1) #ls

```
#rm -rf /[Apache_home]/htdocs/manual
#rm -rf /[Apache_home]/manual
```

Step 2) #ls

```
#ls -ld /[Apache_home]/htdocs/manual
#ls -ld /[Apache_home]/manual
```

Step 3) 가

가

```

                , aliases
                (DocumentRoot) root (/)
                root 가
Options FollowSymLinks

```

```

#vi /[Apache_home]/conf/httpd.conf
Options Indexes FollowSymLinks

```

Step 1) vi /[Apache_home]/conf/httpd.conf

```

#vi /[Apache_home]/conf/httpd.conf

```

Step 2) Options FollowSymLinks

```

( ) Options FollowSymLinks
<Directory />
  Options Indexes FollowSymLinks
  AllowOverride None
  Order allow, deny
  Allow from all
</Directory>

( ) Options FollowSymLinks -FollowSymLinks
<Directory />
  Options FollowSymLinks -FollowSymLinks
  AllowOverride None
  Order allow, deny
  Allow from all
</Directory>

```

가

가 가

LimitRequestBody

```
#vi /[Apache_home]/conf/httpd.conf
LimitRequestBody 5000000
( 5M )
```

Step 1) vi /[Apache_home]/conf/httpd.conf

```
#vi /[Apache_home]/conf/httpd.conf
```

Step 2) LimitRequestBody

```
)
<Directory />
LimitRequestBody 5000000 ( " / " 5M :byte)
</Directory>
```

가 가

OS , 가 가

가 가

DocumentRoot

```
#vi /[Apache_home]/conf/httpd.conf
DocumentRoot "/usr/local/apache/htdocs"
DocumentRoot "/usr/local/apache2/htdocs"
DocumentRoot "/var/www/html"
```

DocumentRoot가

Step 1) vi /[Apache_home]/conf/httpd.conf

```
#vi /[Apache_home]/conf/httpd.conf
```

Step 2) DocumentRoot /usr/local/apache/htdocs,
/usr/local/apache2/htdocs, /var/www/html 가

```
DocumentRoot " "
```

ssh

SSH /
Telnet, FTP /
가

Step 1) SSH

```
#service sshd start
#service ssh start
#systemctl start sshd
```

Step 2) SSH 가 OS SSH

ftp

FTP 가
FTP 가 (,)

```
ftp
#ps -ef | grep ftp
vsftpd ProFTP (vsftpd, proftpd SID )
#ps -ef | egrep "vsftpd|proftpd"
root 3809 3721 0 08:44:40 ? 0:00 /usr/sbin/vsftpd
```

“ftp”

vsftpd ProFTP

```
# service vsftpd(proftp) stop
#/etc/rc.d/init.d/vsftpd(proftp) stop      kill -9 [PID]
```

ftp shell

```
FTP ftp
      (Shell) , ftp
      가
ftp /bin/false
```

```
#cat /etc/passwd
ftp:x:500:100:Anonymous FTP
USER:/var/ftp:/sbin/bash
```

passwd /bin/false가

Step 1) vi /etc/passwd

Step 2) ftp /bin/false

```
( ) ftp:x:500:100:Anonymous FTP USER:/var/ftp:/sbin/bash
( ) ftp:x:500:100:Anonymous FTP USER:/var/ftp:/bin/false
```

Step 3) Step 2 usermod

```
# usermod -s /bin/false [ ID] 가
```

Ftpusers

```
가 ftp ftpusers
ftpusers 가 , FTP
가
```

ftusers

```
#ls -al /etc/ftusers
#ls -al /etc/ftpd/ftusers
rw-r----- root <ftusers >
```

“ftusers” 가 root가 640 가

FTP ftusers FTP /etc/ftusers , /etc/ftpd/ftusers ProFTP
 /etc/ftusers , /etc/ftpd/ftusers vsFTP /etc/vsftpd/ftusers,
 /etc/vsftpd/user_list , /etc/vsftpd.ftusers, /etc/vsftpd.user_list

Step 1) /etc/ftusers

```
#ls -l /etc/ftusers
```

Step 2) /etc/ftusers (root, 640)

```
#chown root /etc/ftusers
#chmod 640 /etc/ftusers
```

※ vsFTP FTP (1) vsftpd.conf userlist_enable=YES
 : vsftpd.ftusers, vsftpd.user_list ftpusers, user_list
 (ftusers, user_list) (2) vsftpd.conf
 userlist_enable=NO , : vsftpd.ftusers ftpusers
 (ftusers)

Ftusers

root FTP root
 FTP 가 가
 ftp root 가

```
#cat /etc/ftusers
#cat /etc/ftpd/ftusers
#root ( ) , root
```

ProFTP

```
#cat /etc/proftpd.conf
```

RootLogin on

vsFTP

```
#cat /etc/vsftp/ftpusers
#cat /etc/vsftp/user_list

#cat /etc/vsftpd.ftpusers
#cat /etc/vsftpd.user_list
#root (      )      , root
```

root FTP 가

< FTP root > Step 1) vi ftpusers
(/etc/ftpusers /etc/ftpd/ftpusers)

```
#vi /etc/ftpusers /etc/ftpd/ftpusers
```

Step 2) ftpusers root 가 ,

```
(      ) #root      , root
(      ) root
```

< ProFTP ROOT >

Step 1) vi proftpd (/etc/proftpd.conf)

```
#vi /etc/proftpd.conf
```

Step 2) proftpd (/etc/proftpd.conf) RootLogin off

```
(      ) RootLogin on
(      ) RootLogin off
```

Step 3) ProFTP

< vsFTP ROOT > Step 1) vi ftpusers
(/etc/vsftp/ftpusers , /etc/vsftpd.ftpusers)

```
#vi /etc/vsftp/ftpusers
```

Step 2) ftpusers root 가 ,

```
( ) #root , root
( ) root
```

Step 3) vsFTP

※ vsFTP FTP (1) vsftpd.conf userlist_enable=YES
: vsftpd.ftpusers, vsftpd.user_list ftpusers, user_list (ftpusers, user_list
) (2) vsftpd.conf userlist_enable=NO , :
vsftpd.ftpusers ftpusers (ftpusers)

at

at
root at ,
/etc/at.allow ← at /etc/at.deny ← at
“cron”

Step 1) at (at OS) * at SUID가
SUID

```
# ls -l /usr/bin/at
# chmod 4750 /usr/bin/at
```

Step 2) cron

```
# chown root <at >
# chmod 640 <at >
```

■ at Step 1) /etc/cron.d/at.allow
/etc/cron.d/at.deny

```
#chown root /etc/cron.d/at.allow
#chmod 640 /etc/cron.d/at.allow
#chown root /etc/cron.d/at.deny
#chmod 640 /etc/cron.d/at.deny
```

Step 2) /etc/cron.d/at.allow /etc/cron.d/at.deny

```
# cat /etc/at.allow (at )
# cat /etc/at.deny (at )
```

SNMP

SNMP

가

SNMP

SNMP

Step 1) ps -ef | grep snmp

```
#ps -ef | grep snmp
root 2028 1 0 Nov 24 ? 0:00 /usr/sbin/snmpdm
```

Step 2) snmp

```
#service snmpd stop
```

SNMP

SNMP Community String Public, Private Community String 가

Community String Default public, private 가 ,
String Dos 가 ,

```
#vi /etc/snmp/snmpd.conf
com2sec notConfigUser default public
```

public , private

Step 1) vi SNMP

```
#vi /etc/snmp/snmpd.conf
```

Step 2) Community String ()

```
( ) com2sec notConfigUser default public
( ) com2sec notConfigUser default < >
```

Step 3)

```
# service snmpd restart
```

가 ,
가 OS OS
OS

Step 1) : vi /etc/motd

```
#vi /etc/motd
```

Step 2) Telnet : vi /etc/issue.net

```
#vi /etc/issue.net
```

Step 3) FTP : vi /etc/vsftpd/vsftpd.conf

```
#vi /etc/vsftpd/vsftpd.conf
ftpd_banner=" "
```

Step 4) SMTP : vi /etc/mail/sendmail.cf

```
#vi /etc/mail/sendmail.cf
0 Smtg GreetingMessage=" "
```

Step 5) DNS : vi /etc/named.conf

```
#vi /etc/named.conf
```

NFS

	가		NFS
NFS		가	가

```
#ls -al /etc/exports
rw-r--r-- root <nfs >
```

“NFS” 가 root가 644 가

/etc/exports (root, 644)

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

expn, vrfy

SMTP expn, vrfy

VRFY, EXPN ,

noexpn, novrfy

```
#vi /etc/mail/sendmail.cf
0 PrivacyOptions= (noexpn, novrfy goaway )
```

※ goaway : authwarnings, noexpn, novrfy, noverb, needmailhelo, needexpnhelo, needvrfyhelo, nobodyreturn

< > Step 1) vi /etc/mail/sendmail.cf

```
#vi /etc/mail/sendmail.cf
```

Step 2) /etc/mail/sendmail.cf noexpn, novrfy 가

```
( ) 0 PrivacyOptions=authwarnings
( ) 0 PrivacyOptions=authwarnings, noexpn, novrfy goaway
```

Step 3) SMTP

< > Step 1)

```
#ps -ef | grep sendmail
root 441 1 0 Sep19 ? 00:00:00 sendmail: accepting connections
#kill -9 [PID]
```

Step 2) SMTP 가 OS 1.

```
#ls -al /etc/rc*.d/* | grep sendmail
```

2.

```
#mv /etc/rc2.d/S88sendmail /etc/rc2.d/_S88sendmail
```

Apache

가 HTTP , OS

가

ServerTokens, ServerSignature

```
# vi /[Apache_Home]/conf/httpd.conf
ServerTokens Prod
ServerSignature off
```

httpd.conf ServerTokens, ServerSignature 가

Step 1) vi `/[Apache_home]/conf/httpd.conf`

```
#vi /[Apache_home]/conf/httpd.conf
```

Step 2) `ServerTokens Prod` `ServerSignature Off`
Off ()

```
<Directory />
  Options Indexes FollowSymlinks
  ServerTokens Prod
  ServerSignature Off
-
-
</Directory>
```

ServerTokens

Prod		Apache
Min		Apache/2.2.3
OS	+	Apache/2.2.3 (CentOS) ()
Full		Apache/2.2.3 (CentOS) DAV/2 PHP/5.16

From: <https://at1.kr/dokuwiki/> - AllThatLinux!

Permanent link: https://at1.kr/dokuwiki/doku.php/%EC%84%9C%EB%B9%84%EC%8A%A4_%EA%B4%80%EB%A6%AC

Last update: 2022/01/18 00:59

