Chapter 21
Security

Firewall (1)

- Using ipfw

1. **Add these options in kernel configuration file and recompile the kernel**

```
options     IPFIREWALL
options     IPFIREWALL_VERBOSE
options     IPFIREWALL_FORWARD
options     IPFIREWALL_DEFAULT_TO_ACCEPT
```

2. **Edit /etc/rc.conf to start firewall**
   - % man rc.conf and search firewall keyword

```
# firewall
firewall_enable="YES"
firewall_script="etc/firewalls/rules"
firewall_quiet="YES"
```

Firewall (2)

3. **Edit ipfw command script that you specify in rc.conf**
   - Ex: /etc/firewall/rules

– **ipfw command**
   - % sudo ipfw list (show current firewall rules)
   - % sudo ipfw flush (delete all firewall rules)

   - % ipfw add {pass|deny} {udp|tcp|all} from where to where

Firewall (3)

> Example (Head part)

```
#!/bin/sh

fwcmd="/sbin/ipfw -q"
myip="140.113.235.4"
${fwcmd} -f flush

${fwcmd} add pass all from ${myip} to any

# Allow TCP through if setup succeeded
${fwcmd} add pass tcp from any to any established
${fwcmd} add deny log all from any to any frag
echo -n "Established "

# Allow icmp (ping only)
${fwcmd} add pass icmp from any to any icmptypes 0,3,8,11
```

Firewall (4)

> Example (service part)

```
# Allow SMB
${fwcmd} add pass tcp from 140.113.235.0/24 to ${myip} 137-139 setup

# Allow HTTP/HTTPS
${fwcmd} add pass tcp from any to ${myip} 80 setup
${fwcmd} add pass tcp from any to ${myip} 443 setup
echo -n "HTTP/HTTPS "

# SSH access control
${fwcmd} add pass tcp from any to any 22 setup
echo -n "SSH "

# open any system port that your system provide
```

Firewall (5)

> Example (Tail part)

```
# Default to deny
${fwcmd} add 65500 reset log tcp from any to any
${fwcmd} add 65501 reject udp from any to any
${fwcmd} add 65502 reject log icmp from any to any
${fwcmd} add 65534 deny log all from any to any
```

Firewall (6)

- Manual reset firewall rules
  - **Edit the script and**
  - **% sudo sh /etc/firewall/rules**
- When you install new service and wondering why it can not use…
  - **% sudo ipfw flush**
  - **Delete all firewall rules to remove problems caused by firewall**

Firewall (7)

- Debug your system via log file
  - /var/log/security

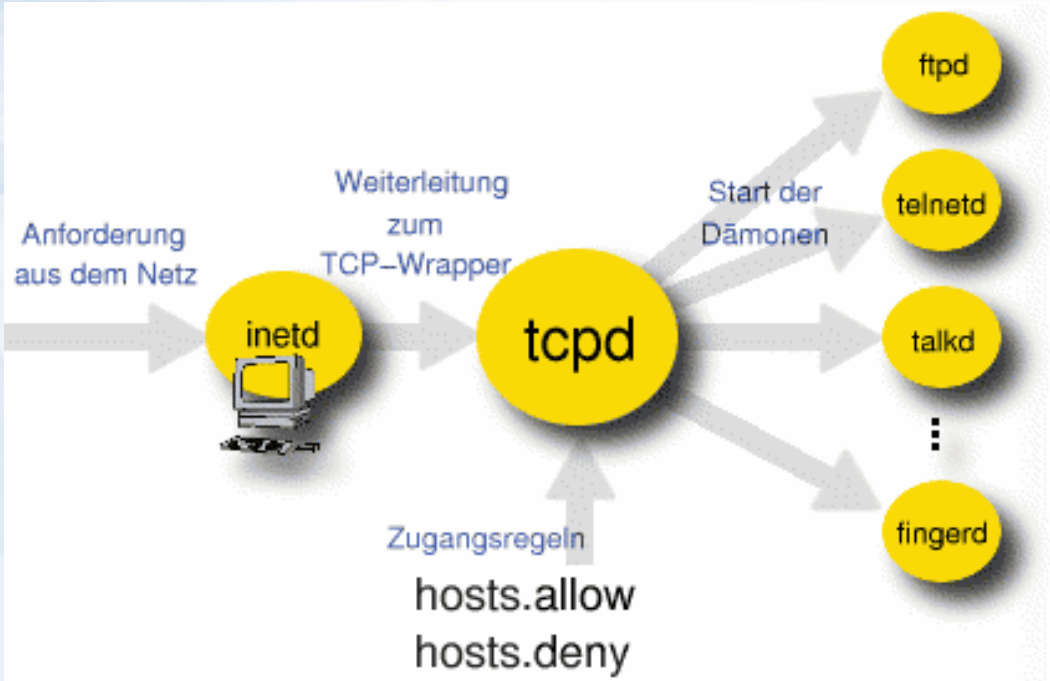
```
Dec 25 11:25:36 tybsd last message repeated 2 times
Dec 25 11:45:06 tybsd kernel: ipfw: 65500 Reset TCP 211.48.52.58:1997 140.113.235.4:5554 in via fxp0
Dec 25 11:45:07 tybsd kernel: ipfw: 65500 Reset TCP 211.48.52.58:1997 140.113.235.4:5554 in via fxp0
Dec 25 11:45:07 tybsd kernel: ipfw: 65500 Reset TCP 211.48.52.58:4062 140.113.235.4:1023 in via fxp0
Dec 25 11:45:08 tybsd kernel: ipfw: 65500 Reset TCP 211.48.52.58:4062 140.113.235.4:1023 in via fxp0
Dec 25 11:45:09 tybsd kernel: ipfw: 65500 Reset TCP 211.48.52.58:4246 140.113.235.4:9898 in via fxp0
Dec 25 12:05:44 tybsd kernel: ipfw: 65500 Reset TCP 204.100.126.30:2188 140.113.235.4:445 in via fxp0
Dec 25 12:05:45 tybsd last message repeated 2 times
```

/etc/hosts.equiv and ~/.rhosts

- Trusted remote host and user name DB
  - **Allow user to login (via rlogin) and copy files (rcp) between machines without passwords**
  - **Format:**
    - Simple: hostname [username]
    - Complex: [+-][hostname|@netgroup]
      [[+-][username|@netgorup]]
  - **Example**
    - bar.com foo (trust user "foo" from host "bar.com")
    - +@adm_csie_cc (trust all hosts from amd_csie_cc group)
    - +@adm_csie_cc -@tytsai
- Not to use this

/etc/hosts.allow (1)

- TCP Wrapper
  - **Provide support for every server daemon under its control**



/etc/hosts.allow (2)

- To see what daemons are controlled by inetd, see /etc/inetd.conf

```
#ftp    stream  tcp nowait  root    /usr/libexec/ftpd   ftpd -l
#ftp    stream  tcp6    nowait  root    /usr/libexec/ftpd   ftpd -l
#telnet stream  tcp nowait  root    /usr/libexec/telnetd    telnetd
#telnet stream  tcp6    nowait  root    /usr/libexec/telnetd    telnetd
shell   stream  tcp nowait  root    /usr/libexec/rshd   rshd
#shell  stream  tcp6    nowait  root    /usr/libexec/rshd   rshd
login   stream  tcp nowait  root    /usr/libexec/rlogind    rlogind
#login  stream  tcp6    nowait  root    /usr/libexec/rlogind    rlogind
```

- TCP wrapper should not be considered a replacement of a good firewall. Instead, it should be used in conjunction with a firewall or other security tools

/etc/hosts.allow (3)

- To use TCP wrapper
  1. **inetd daemon must start up with "-Ww" option (default)**
     - **Or edit /etc/rc.conf**

```
inetd_enable="YES"
inetd_flags="-wW"
```

  2. **Edit /etc/hosts.allow**
     - Format:
       daemon:address:action

       - daemon is the daemon name which inetd started
       - address can be hostname, IPv4 addr, IPv6 addr
       - action can be "allow" or "deny"

       - Keyword "ALL" can be used in daemon and address fields to means everything

/etc/hosts.allow (4)

- **First rule match semantic**
  - Meaning that the configuration file is scanned in ascending order for a matching rule
  - When a match is found, the rule is applied and the search process will stop

> example

```
ALL :     localhost, loghost @adm_cc_csie : allow
ptelnetd pftpd sshd: @sun_cc_csie, @bsd_cc_csie, @linux_cc_csie : allow
ptelnetd pftpd sshd: cflee, ycchang, zeiss, liao, tybsd : allow
identd :  ALL : allow
portmap :  140.113.17. ALL : allow
sendmail : ALL : allow
rpc.rstatd : @all_cc_csie 140.113.17.203: allow
rpc.rusersd : @all_cc_csie 140.113.17.203: allow
ALL : ALL : deny
```

/etc/hosts.allow (5)

> Advance configuration

- **External commands (twist option)**
  - twist will be called to execute a shell command or script

```
# The rest of the daemons are protected.
telnet : ALL \
         : severity auth.info \
         : twist /bin/echo "You are not welcome to use %d from %h."
```

- **External commands (spawn option)**
  - spawn is like twist, but it will not send a reply back to the client

```
# We do not allow connections from example.com:
ALL : .example.com \
      : spawn (/bin/echo %a from %h attempted to access %d >> \
      /var/log/connections.log) \
      : deny
```

/etc/hosts.allow (6)

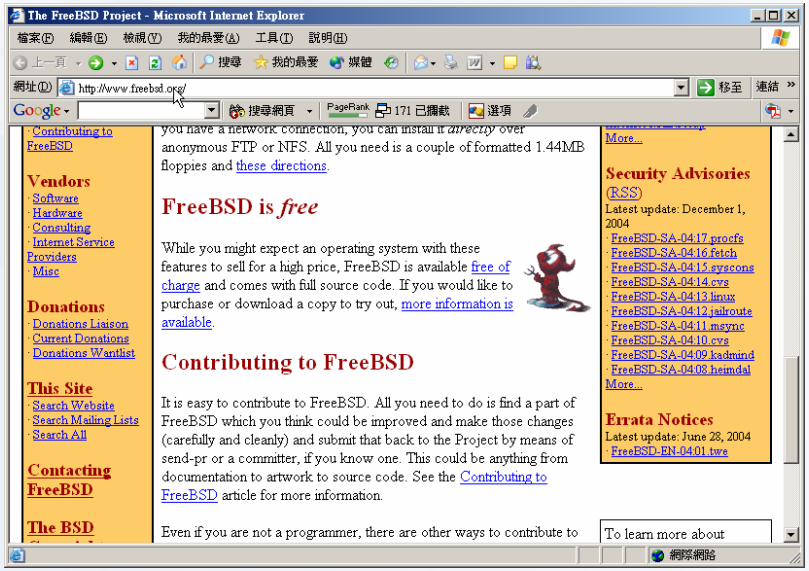
- **Wildcard (PARANOID option)**
  - Match any connection that is made from an IP address that differs from its hostname

```
# Block possibly spoofed requests to sendmail:
sendmail : PARANOID : deny
```

> See man 5 hosts_access

FreeBSD Security Advisories (1)

- Advisory
  - **Security information**
- Where to find it
  - **freebsd-security-notifications Mailing list**
    - http://lists.freebsd.org/mailman/listinfo/freebsd-security-notifications
  - **Web page (Security Advisories Channel)**
    - http://www.freebsd.org



FreeBSD Security Advisories (2)

> Advisory content

- **core**
  - core OS
- **contrib**
  - Software for FreeBSD project
- **Ports**
  - Add on software
- **Solution**
  - Workaround
  - Solution

```
=============================================================================
FreeBSD-SA-XX:XX.UTIL                                   Security Advisory
                                                        The FreeBSD Project

Topic:          denial of service due to some problem❶

Category:       core❷
Module:         sys❸
Announced:      2003-09-23❹
Credits:        Person@EMAIL-ADDRESS❺
Affects:        All releases of FreeBSD❻
                FreeBSD 4-STABLE prior to the correction date
Corrected:      2003-09-23 16:42:59 UTC (RELENG_4, 4.9-PRERELEASE)
                2003-09-23 20:08:42 UTC (RELENG_5_1, 5.1-RELEASE-p6)
                2003-09-23 20:07:06 UTC (RELENG_5_0, 5.0-RELEASE-p15)
                2003-09-23 16:44:58 UTC (RELENG_4_8, 4.8-RELEASE-p8)
                2003-09-23 16:47:34 UTC (RELENG_4_7, 4.7-RELEASE-p18)
                2003-09-23 16:49:46 UTC (RELENG_4_6, 4.6-RELEASE-p21)
                2003-09-23 16:51:24 UTC (RELENG_4_5, 4.5-RELEASE-p33)
                2003-09-23 16:52:45 UTC (RELENG_4_4, 4.4-RELEASE-p43)
                2003-09-23 16:54:39 UTC (RELENG_4_3, 4.3-RELEASE-p39)❼
FreeBSD only:   NO❽

For general information regarding FreeBSD Security Advisories,
including descriptions of the fields above, security branches, and the
following sections, please visit
http://www.FreeBSD.org/security/.

I.   Background❾

II.  Problem Description❿

III. Impact(11)

IV.  Workaround(12)

V.   Solution(13)

VI.  Correction details(14)

VII. References(15)
```

FreeBSD Security Advisories (3)

- Example
  - **proc filesystem advisory**

```
=============================================================================
FreeBSD-SA-04:17.procfs                                     Security Advisory
                                                          The FreeBSD Project

Topic:          Kernel memory disclosure in procfs and linprocfs

Category:       core
Module:         sys
Announced:      2004-12-01
Credits:        Bryan Fulton, Ted Unangst, and the SWAT analysis tool
                Coverity, Inc.
Affects:        All FreeBSD releases
Corrected:      2004-12-01 21:33:35 UTC (RELENG_5, 5.3-STABLE)
                2004-12-01 21:34:23 UTC (RELENG_5_3, 5.3-RELEASE-p2)
                2004-12-01 21:34:43 UTC (RELENG_5_2, 5.2.1-RELEASE-p13)
                2004-12-01 21:33:57 UTC (RELENG_4, 4.10-STABLE)
                2004-12-01 21:35:10 UTC (RELENG_4_10, 4.10-RELEASE-p5)
                2004-12-01 21:35:57 UTC (RELENG_4_8, 4.8-RELEASE-p27)
CVE Name:       CAN-2004-1066
```

FreeBSD Security Advisories (4)

> Example

– **workaround**

```
IV.  Workaround

Unmount the procfs and linprocfs file systems if they are mounted.
Execute the following command as root:

  umount -A -t procfs,linprocfs

Also, remove or comment out any lines in fstab(5) that reference
`procfs' or `linprocfs', so that they will not be re-mounted at next
reboot.
```

FreeBSD Security Advisories (5)

> Example

– **solution**

```
V.   Solution

Perform one of the following:

1) Upgrade your vulnerable system to 4-STABLE or 5-STABLE, or to the
RELENG_5_3, RELENG_5_2, RELENG_4_10, or RELENG_4_8 security branch dated
after the correction date.

2) To patch your present system:

The following patches have been verified to apply to FreeBSD 4.8, 4.10,
5.2, and 5.3 systems.

a) Download the relevant patch from the location below, and verify the
detached PGP signature using your PGP utility.

[FreeBSD 4.x]
# fetch ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-04:17/procfs4.patch
# fetch ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-04:17/procfs4.patch.asc

[FreeBSD 5.x]
# fetch ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-04:17/procfs5.patch
# fetch ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-04:17/procfs5.patch.asc

b) Apply the patch.

# cd /usr/src
# patch < /path/to/patch

c) Recompile your kernel as described in
<URL:http://www.freebsd.org/handbook/kernelconfig.html> and reboot the
system.
```