Lab 9: How to build your own rpm

Objective: To help students to learn

- How to build a rpm
- Port scan detection
- Understand how syslog works.

Preparation: *beehive* and *log server* will be used.

[1] Install rpmbuild on your machine:

```
[root@beehive ~root]# yum –y install rpm-build
```

[2] Install gcc compiler:

```
[root@beehive ~root]# yum grouplist
[root@beehive ~root]# yum –y groupinstall "Development Tools"
```

[2] Setup rpm build tree:

```
[root@beehive ~root]# su – ken
[ken@beehive ~]$ mkdir -p rpm/tmp
[ken@beehive ~]$ cp –rvf /usr/src/redhat/* rpm
[ken@beehive ~]$ tree
rpm
|-- BUILD
|-- RPMS
|   |-- athlon
|   |-- i386
|   |-- i486
|   |-- i586
|   |-- i686
|   `-- noarch
|-- SOURCES
|   `-- scanlogd-2.2.6.tar.gz
|-- SPECS
|   `-- scanlogd.spec
|-- SRPMS
`-- tmp
```

[3] Set rpmmacros:

```
[ken@beehive ~]$ rpm –eval %_topdir
/usr/src/redhat

[ken@beehive ~]$ echo "%_topdir $HOME/rpm" > ~/.rpmmacros
[ken@beehive ~]$ rpm –eval %_topdir
/home/ken/rpm
```

[1] Download src.rpm: (Example: http://vault.centos.org/5.7/os/SRPMS/setup-2.5.58-7.el5.src.rpm)

```
[ken@loghost~]$ wget http:// vault.centos.org/5.7/os/SRPMS/setup-2.5.58-7.el5.src.rpm
```

[2] Install src.rpm:

```
[ken@beehive ~]$ rpm –ivh setup-2.5.58-7.el5.src.rpm
```

[3] Build rpm:

```
[ken@beehive ~]$ rpmbuild –ba SPECS/setupspec
```

Build rpm from tarball:

[1] Download tarball: (Example: http://www.cse.csusb.edu/ken/download/scanlogd/scanlogd-2.2.tar.gz)

```
[ken@beehive ~]$ cd SOURCES
[ken@beehive SOURCES]$ wget http://www.cse.csusb.edu/ken/download/scanlogd/scanlogd-2.2.tar.gz
```

[2] Create startup script:

```
[ken@beehive SOURCES]$ vi scanlogd.init
```

```
#!/bin/bash
# scanlogd     This bash script start scanlogd
# Author:      Ken Han
#
# chkconfig:   2345 08 92
#
# description:  scanlogd startup script

# source function library
. /etc/rc.d/init.d/functions
test -x /usr/sbin/atd || exit 0

RETVAL=0
SCANLOG_HOME=/usr/sbin
SCANLOG_OWNER=scanlogd
if [ ! -f $SCANLOG_HOME/scanlogd ]
then
        echo "Scanlogd startup: cannot start"
        exit
fi
prog="scanlogd"

start() {
    # Start the scalogd:
    # The following command assumes that the scanlogd login will not prompt the user for any values

    # Check if scanlogd is already running
    if [ ! -f /var/lock/subsys/scanlogd ]; then
      echo -n $"Starting $prog: "
      daemon /usr/sbin/scanlogd
      RETVAL=$?
```

```
          [ $RETVAL -eq 0 ] && touch /var/lock/subsys/scanlogd
           echo
        fi
        return $RETVAL
}


stop() {
        echo -n $"Stopping $prog: "
        killproc /usr/sbin/scanlogd
        RETVAL=$?
        [ $RETVAL -eq 0 ] && rm -f /var/lock/subsys/scanlogd
        echo
        return $RETVAL
}


restart() {
        stop
        start
}

case "$1" in
  start)
        start
        ;;
  stop)
        stop
        ;;
  status)
        status scanlogd
        RETVAL=$?
        echo "------------------------------------------------------------------------------"
        tail /var/log/alert
        echo "------------------------------------------------------------------------------"
        ;;
  restart)
        restart
        ;;
  *)
        echo $"Usage: $0 {start | stop | status | restart}"
        exit 1
esac

exit $?
exit $RETVAL
```

[3] Create scanlogd.spec file:

```
[ken@beehive SOURCES]$ cd ../SPECS
[ken@beehive SPECS]$ cd ../SPECS
[ken@beehive SPECS]$ vi scanlogd.spec
```

```
Summary: Tools for detecting ports scanning.
Name: scanlogd
Version: 2.2
Release: 1.5
#Source: http://www.openwall.com/scanlogd/%{name}-%{version}.tar.gz
Source: %{name}-%{version}.tar.gz
Source1: scanlogd.init
Group: System Environment/Base
URL: http://www.openwall.com/
BuildRoot: %{_tmppath}/%{name}-buildroot
License: GPL
BuildPrereq: /usr/bin/perl
Requires: kernel >= 2.4.0
Requires(post,postun): chkconfig

%description
The scanlogd utility detects the network port scanning activities.
If you need to detect port scan, you should install this package.

%prep
rm -rf %{buildroot}

%setup -q

# Put it to a reasonable place
#perl -pi -e "s,/usr/local,%{prefix},g" * */*

%build
OPT="linux"
make $OPT

%install
mkdir -p $RPM_BUILD_ROOT/usr/sbin
mkdir -p $RPM_BUILD_ROOT%{_mandir}/man8
mkdir -p $RPM_BUILD_ROOT/etc/rc.d/init.d

install -m700 scanlogd $RPM_BUILD_ROOT/usr/sbin
install -m600 scanlogd.8.gz $RPM_BUILD_ROOT%{_mandir}/man8
install -c -m755 %{SOURCE1} $RPM_BUILD_ROOT/etc/rc.d/init.d/scanlogd

%clean
rm -rf $RPM_BUILD_ROOT $RPM_BUILD_DIR/%{name}-%{version}

%post
/sbin/chkconfig --add scanlogd
perl -e 'print "\n# Save scanlog messages to alert file\n";' >> /etc/syslog.conf
```

```
#kern.*                                 /dev/console

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none          /var/log/messages

# The authpriv file has restricted access.
authpriv.*                              /var/log/secure
# Log all the mail messages in one place.
mail.*                                  -/var/log/maillog
# Log cron stuff
cron.*                                  /var/log/cron
# Everybody gets emergency messages
*.emerg                                 *
# Save news errors of level crit and higher in a special file.
uucp,news.crit                                  /var/log/spooler
# Save boot messages also to boot.log
local7.*                                /var/log/boot.log
# Save scanlog messages to alert file
daemon.alert                            /var/log/alert
```

[8] Setup syslog Server:

Stop syslog service:

```
[root@logsver ~root]# service syslog stop
```

Edit /etc/sysconfig/syslog

```
[root@ logsver ~root]# vi  /etc/sysconfig/syslog
```

Replace the line

SYSLOGD_OPTIONS=”-m 0”

with

SYSLOGD_OPTIONS=”-rm 0”

Re-start the syslog service:

```
[root@ logsver ~root]# service syslog restart
```

Check the log:

```
[root@ logsver ~root]# tail /var/log/messages
```

You will find:

syslogd 1.4.1: restart (remote reception).

Add a Firewall Rule for accepting remote syslog reception:

```
[root@ logsver ~root]# iptables -L
[root@ logsver ~root]# iptables -I RH-Firewall-1-INPUT -p udp -i eth0 -s 192.168.1.0/24  - -dport 514 –j ACCEPT
[root@ logsver ~root]# iptables-save > /etc/sysconfig/iptables
[root@ logsver ~root]# service iptables restart
[root@ logsver ~root]# iptables -L
```

```
perl -e 'print "daemon.alert \t\t\t\t\t\t  /var/log/alert\n";' >> /etc/syslog.conf
perl -e 'system("useradd -c scanlogd -d\/ -s \/sbin\/nologin scanlogd")';
perl -e 'system("touch /var/log/alert;chmod 500 /var/log/alert")';
perl -e 'system("service syslog restart")';

%preun
if [ "$1" = 0 ]; then
        /sbin/chkconfig --del scanlogd
fi

%files
/usr/sbin/scanlogd
/usr/share/man/man8/scanlogd.8.gz
/etc/rc.d/init.d/scanlogd
%defattr(-,root,root,0755)
%config /etc/rc.d/init.d/scanlogd

%changelog
```

[4] Build rpm:

```
[ken@beehive SPECS]$ rpmbuild   –ba   scanlogd.spec
[ken@beehive SPECS]$ cd
[ken@beehive ~]$ tree  rpm
```

[5] Install your own rpm:

```
[ken@beehive  ~]$ su –
[root@beehive  ~root]# chkconfig  –list | grep  scanlogd
[root@beehive ~root]# cp  /home/ken/rpm/BUILD/scanlogd*.rpm   .
[root@beehive ~root]# rpm  –Uvh scanlogd*.rpm
[root@beehive ~root]# chkconfig  –list | grep  scanlogd
[root@beehive ~root]# service  scanlogd  start
```

[6] Port Scan your machine:

```
[root@ns ~root]# yum –y  install  nmap
[root@ns ~root]# tail  /var/log/alert
[root@ns ~root]# nmap  beehive
```

On beehive:

```
[root@beehive ~root]# tail  /var/log/alert
```

On logserver:

```
[root@logsver ~root]# tail  /var/log/alert
```

[7] How syslogd works

```
[root@beehive ~root]# vi /etc/syslog.conf
# Log all kernel messages to the console.
# Logging much else clutters up the screen.
```

Configure the syslog Clients:

```
[root@beehive ~root]# vi /etc/syslog.conf
```

Add following line:

```
*.* @192.168.1.0/24
```

Re-start the syslog service:

```
[root@beehive ~root]# service syslog restart
```

Add a Firewall Rule for accepting remote syslog reception:

```
[root@beehive ~root]# iptables -L
[root@beehive ~root]# iptables -I OUTPUT -p udp -s 139.182.148.150 -d 139.182.148.151 --dport 514 -j ACCEPT
[root@beehive ~root]# iptables-save > /etc/sysconfig/iptables
[root@beehive ~root]# service iptables restart
[root@beehive ~root]# iptables -L
```

Check the log from syslog Server:

```
[root@logsver ~root]# tail -f /var/log/messages  (CTRL + C to escape)

[root@logsver ~root]# tail -f /var/log/secure (CTRL + C to escape)
```

Lab 9 Report:

[1] What the run levels are?

[2] Use "*man*" command to find out "*chkconfig*" command and answer the following:

1. **How to check run levels using *chkconfig* command?**
2. **How to add *scanlogd* to run level 345 using *chkconfig* command?**
3. **How to turn off *scanlogd* from run level 345 using *chkconfig* command?**
4. **How to turn on *scanlogd* from run level 345 using *chkconfig* command?**
5. **How to remove *scanlogd* from run level 345 using *chkconfig* command?**

[3] What are the differences between rpm installation and tar ball installations?

[4] Download fail2ban from
Using following command: superb-west.dl.sourceforge.net
wget http://superb-west.dl.sourceforge.net/sourceforge/fail2ban/fail2ban-0.8.1.tar.bz2

[5] Build your own fail2ban rpm using above lab.

[6] How forward local log to remote log server?