Securing Red Hat Linux for the non-Unix Computer Officer

Bob Dowling
University Computing Service

Overview of talk

- Start with a virgin system
- I'll be using Red Hat Linux 9
  - More modern versions more security-aware
- Turn off unwanted services
  - Once per system
- Updating packages
  - Regularly

Turning off unwanted services

- Every break-in needs an “in”
- Need to know what services are required
- Network services especially important
- Need to know how to turn them off (or on)
- GUI: redhat-config-services

What services are needed?

- Need to know what we need
- Need a tight specification of the system
  - From an academic?!!
- The “Vaguely Defined Workstation”:
  - X11 — Graphics
  - NTP — Timekeeping
  - SSH — Secure access (for you, at least!)
  - NFS — Client-side remote file access
Network services to leave on

- Basic networking
  - network
  - portmap
- NFS client
  - netfs
  - nfslock
- Time-keeping
  - ntpd
- Windowing system
  - sgi_fam
  - xinetd
- Secure access
  - sshd

Network services to turn off

- Turn off every other network service
  - You just need to recognise network services
- All network services depend on network
- Some depend on portmap and xinetd
- These three are already on

Networking summary

- Turn off unwanted services
- GUI: redhat-config-services
- Reboot after making the changes
- But wait until software upgraded too
Software upgrades
- A break-in requires something to be broken
- Keep our network services up-to-date
- Keep all our software up-to-date!
- Want to recognise real Red Hat packages
- Need to be an NFS client
  - Accessing the Unix Support NFS server

Recognising Red Hat packages
- Red Hat sign their packages
- We need a key to recognise the signature
  - /usr/share/doc/rpm-4.2/RPM-GPG-KEY
- Only need do this once

# rpm --import /usr/share/doc/rpm-4.2/RPM-GPG-KEY

Unix Support NFS Server
- nfs-uxsup.csx.cam.ac.uk
- /linux/redhat
- Need to “mount” it locally
- mkdir /mnt/redhat
- Add a line to /etc/fstab:
  nfs-uxsup.csx.cam.ac.uk:/linux/redhat /mnt/redhat nfs ro,nosuid 0 0
- mount /mnt/redhat

NFS Server Contents
# mount /mnt/redhat
# cd /mnt/redhat
# ls 5.2 7.0 7.2 8.0 beta contrib enterprise rawhide
# ls 6.2 7.1 7.3 9 code current local_extras updates
# ls 9/en/os/1386 autorun EULA images README RELEASE-NOTES SRPMS
# ls updates/9/en/os athlon 1386 1386 1686 noarch SRPMS
Updates

- Red Hat updates software after release
  - Newer versions of entire packages
  - Not just *ad hoc* patches
- There are automated procedures
  - Red Hat Network, rpm-apt
  - cost, loss of control
- Manual upgrading is still the best

An assisting package

- Want to avoid “dependency hell”
- Want assistance resolving dependencies
- Packaged dependency database

```bash
# cd /mnt/redhat/9/en/os/i386/RedHat/RPMS
# ls rpmdb-*
rpmdb-redhat-9-0.20030313.i386.rpm
# rpm --install rpmdb-*
```

Configuring `rpmdb-redhat`

- Need to configure it for our systems
  - `/etc/rpm/macros.solve`
- Need to tell it where the main packages are
  - `/mnt/redhat/9/en/os/i386/RedHat/RPMS`

```
# The path to the dependency universe packages.
# This should be a path to the packages contained
# in the solve database.
%_solve_pkgsdir /mnt/redhat/9/en/os/i386/RedHat/RPMS/
```

Updates directory

- Directory of upgrades
- `/mnt/redhat/updates/9/en/os/`
- Three possible subdirectories:
  - i686 — kernel, C library
  - i386 — almost everything
  - noarch — architecture-independent packages
Updates procedure

- `rpm --freshen`
  - Only updates packages already installed
- Need to cover three subdirectories
- Must update kernel and C library first
  - Reboot before proceeding
- Update everything else second
  - Reboot

Kernel and C library updates

- Do we need to update at all?
- Update with the i686 versions
- Often dependencies in i386 and noarch
- Occasional dependencies in main release
  - Dependency database will help you here
- Reboot afterwards

Kernel & C library update needed?

```
# cd /mnt/redhat/updates/9/en/os
# ls i686
  glibc-2.3.2-27.9.i686.rpm   nptl-devel-2.3.2-27.9.i686.rpm
  kernel-2.4.20-9.i686.rpm   openssl-0.9.7a-5.i686.rpm
  kernel-smp-2.4.20-9.i686.rpm
# rpm --query kernel glibc
  kernel-2.4.20-8
  glibc-2.3.2-11.9
```

Kernel & C library update example

```
# rpm --freshen i686/{glibc,kernel}/*.i686.rpm
  error: Failed dependencies:
    glibc-common = 2.3.2-27.9 is needed by glibc-2.3.2-27.9
# rpm --freshen i686/{glibc,kernel}/*.i686.rpm i386/glibc-common-2.3.2-27.9.i386.rpm
# cd
# reboot
```
Applications update example

```bash
# mount /mnt/redhat
# cd /mnt/redhat/updates/9/en/os
# rpm --freshen {noarch,i386,i686}/*.rpm
warning: package openssl = 0.9.7a-5 was already added,
replacing with openssl <= 0.9.7a-5
# reboot
```

Order of architectures matters
- Later listed packages “win”

Updating summary: Once
- Load GPG key
- Create /mnt/redhat directory
- Update /etc/fstab file
- Load & configure rpmdb-redhat package

Updating summary: Routine
- Mount /mnt/redhat
- Kernel and glibc updates available?
- Update kernel and glibc packages
- Reboot
- Update everything
- Reboot
Conclusion

- Security is not so hard
- Decide what the system is for (hard)
- Turn off unnecessary services (easy)
  - `redhat-config-services`
- Keep packages up to date (boring)
  - Set up once
  - Update routinely (weekly?)
  - `rpm --freshen`