The following tips assume that the reader is starting with a default installation of Red Hat Enterprise Linux 5. This high-impact guidance can be applied quickly, but is by no means complete. For more complete guidance, please see our other publication, "Guide to the Secure Configuration of Red Hat Enterprise Linux 5," which can be found online at http://www.nsa.gov. These tips may or may not translate gracefully for other Linux distributions or modified installations of RHEL.

General Principles

- Encrypt all data transmitted over the network. Encrypting authentication information (such as passwords) is particularly important.
- Minimize the amount of software installed and running in order to minimize vulnerability.
- Use security-enhancing software and tools whenever available (e.g., SELinux and Iptables).
- Run each network service on a separate server whenever possible. This minimizes the risk that a compromise of one service could lead to a compromise of others.
- Maintain user accounts. Create a good password policy and enforce its use. Delete unused user accounts.
- Review system and application logs on a routine basis. Send logs to a dedicated log server. This prevents intruders from easily avoiding detection by modifying the local logs.
- Never log in directly as root, unless absolutely necessary. Administrators should use `sudo` to execute commands as root when required. The accounts capable of using sudo are specified in `/etc/sudoers`, which is edited with the `visudo` utility. By default, relevant logs are written to `/var/log/secure`.

Disk Partitions and Mounting

During initial installation, ensure that filesystems with user-writeable directories such as the following are mounted on separate partitions: `/home`, `/tmp`, `/var/tmp`.

During system configuration, change mount options in `/etc/fstab` to limit user access on appropriate filesystems. The `defaults` option is equal to `rw,suid,dev,exec,auto,nouser,async`. Using `noexec` instead prevents execution of binaries on a file system (though it will not prevent scripts from running). Using `nosuid` will prevent the setuid bit from having effect. The `nodev` option prevents use of device files on the filesystem.

Physical Security

Configure the BIOS to disable booting from CDs/DVDs, floppies, and external devices, and set a password to protect these settings.
Next, set a password for the GRUB bootloader. Generate a password hash using the command `/sbin/grub-md5-crypt`. Add the hash to the first line of `/etc/grub.conf` as follows:

```
password --md5 passwordhash
```

This prevents users from entering single user mode or changing settings at boot time.

Keep Software Up to Date

Either download updates manually through the Red Hat Network (http://rhn.redhat.com) or register each system with RHN to apply updates automatically. Security updates should be applied as soon as possible.

The default version of `yum-updatesd` does not function reliably. A better solution is to apply updates through a cron job. First, disable the service with:

```
/sbin/chkconfig yum-updatesd off
```

Second, create the file `yum.cron`, make it executable, place it in `/etc/cron.daily` or `/etc/cron.weekly`, and ensure that it reads as follows:

```
#!/bin/sh
/usr/bin/yum -R 120 -e 0 -d 0 -y update yum
/usr/bin/yum -R 10 -e 0 -d 0 -y update
```

Disable Unnecessary Services

To list the services configured to start at boot, run the following command:

```
/sbin/chkconfig --list
```

Find the column for the current run level to see which services are enabled. The default run level is 5. To disable a service, run the following command:

```
/sbin/chkconfig servicename off
```

Unless they are required, disable the following:

anacron	haldaemon	messagebus
apmd	hidd	microcode_ctl
autofs`	hplip*	pcscd
avahi-daemon*	isdn	readahead_early
bluetooth	kdump	readahead_later
cups*	kudzu	rhnsd*
firstboot	mcstrans	setroubleshoot
gpm	mdmonitor	xfs

Items marked with a * are network services. It is particularly important to disable these. Additionally, the following services can be safely disabled if NFS is not in use: `netfs`, `nfslock`, `portmap`, `rpcgssd`, and `rpcidmapd`. Some software relies on `haldaemon` and `messagebus`, so care should be taken when disabling them. Changes will take effect after a reboot.

Disable SUID and SGID Binaries

To find SUID and SGID files on the system, use the following command:

```
find / \( -perm -4000 -o -perm -2000 \) -print
```

The following files can have their SUID or SGID bits safely disabled (using `chmod -s filename`) unless required for the purpose listed in the second column:

File:	Required For:
/bin/ping6	IPv6
/sbin/mount.nfs	NFS
/sbin/mount.nfs4	NFS
/sbin/netreport	network control
/sbin/umount.nfs	NFS
/sbin/umount.nfs4	NFS
/usr/bin/chage	passwd
/usr/bin/chfn	account info
/usr/bin/chsh	account info
/usr/bin/crontab	cron
/usr/bin/lockfile	Procmail
/usr/bin/rcp	rsh
/usr/bin/rlogin	rsh
/usr/bin/rsh	rsh
/usr/bin/wall	console messaging
/usr/bin/write	console messaging
/usr/bin/Xorg	Xorg
/usr/kerberos/bin/ksu	Kerberos
/usr/libexec/openssh/ssh-keysign	SSH host-based authentication
/usr/lib/vte/gnome-pty-helper	Gnome, Xorg
/usr/sbin/ccreds_validate	Pam auth caching
/usr/sbin/suexec	Apache, CGI
/usr/sbin/userisdnctl	ISDN
/usr/sbin/usernetctl	network control

To see which RPM package each file belongs to, run `rpm -qf filename`. If the package is not necessary, remove it with `rpm -e packagename`. Precise control over the packages installed during initial system installation can be achieved using a Kickstart file.

Remove X Windows

A server will not typically need X Windows to provide its services, so remove it if possible:

```
yum groupremove "X Window System"
```

Installation of X Windows can also be completely prevented during initial system installation.

Configure and Use Iptables and TCP Wrapper

The Iptables firewall should be configured to allow only necessary network communications. For workstations, this may entail blocking all incoming communications, except for those related to connections the system initiated. If Iptables is currently running, view the current firewall policy with the following command:

```
/sbin/iptables -L
```

By default, the output should correspond to rules stored in the file `/etc/sysconfig/iptables`. Understand and edit these rules, removing any lines that allow unnecessary communications. To activate the updated rules, restart the service.

Also configure the TCP Wrapper library to protect network daemons that support its use by adding appropriate rules to `/etc/hosts.allow` and `/etc/hosts.deny`.

Configure and Use SELinux

The default SELinux policy, called `targeted`, provides protection against compromised or misconfigured system services. This policy should not interfere with normal system operation. Ensure that `/etc/selinux/config` includes the following lines:

```
SELINUX=enforcing
SELINUXTYPE=targeted
```

Stronger policies such as `strict` and `mls` can be used if appropriate. However, these require customization to operate successfully for many general-purpose usage scenarios.

Set Kernel Parameters

At boot, the system reads and applies a set of kernel parameters from `/etc/sysctl.conf`. Add the following lines to that file to prevent certain kinds of attacks:

```
net.ipv4.conf.all.rp_filter=1
net.ipv4.conf.all.accept_source_route=0
net.ipv4.icmp_echo_ignore_broadcasts=1
net.ipv4.icmp_ignore_bogus_error_messages=1
kernel.exec-shield=1
kernel.randomize_va_space=1
```

For more possible parameters, including settings for IPv6, please see our complete guide.

NTP

For most systems, the `ntpd` service introduces unnecessary overhead. Instead, call its update utility, `ntpdate`, directly through a cron job. Create the file `/etc/cron.d/ntpdate` with the following line:

```
15 * * * * root /usr/sbin/ntpdate server
```

Substitute an appropriate NTP server for *`server`*. Hosts on a network should synchronize their time from a local NTP server, and then only this local NTP server should acquire the time from an external, trusted source.

Configure or Disable SSH

SSH is often required, but if it is not, disable it:

```
/sbin/chkconfig sshd off
```

If SSH is required, ensure the SSH configuration file `/etc/ssh/sshd_config` includes the following lines:

```
PermitRootLogin no
Protocol 2
```

If possible, limit SSH access to a subset of users. Create a group called `sshusers` and only add the users that need remote access. Then, add the following line to `/etc/ssh/sshd_config`:

```
AllowGroups sshusers
```

Restart the service so that these changes take effect.

Disable IPv6

Unless your policy or network configuration requires it, disable IPv6. To do so, prevent the kernel module from loading by adding the following line to `/etc/modprobe.conf`:

```
install ipv6 /bin/true
```

Next, add or change the following lines in `/etc/sysconfig/network`:

```
NETWORKING_IPV6=no
IPV6INIT=no
```

Hardening Tips

For Default Installation of

Red Hat Enterprise Linux 5

Systems and Network Analysis Center
National Security Agency
9800 Savage Rd.
Ft. Meade, MD 20755
http://www.nsa.gov