Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Keeping Red Hat Linux Systems Secure with up2date

In this paper I will give an in depth overview of the software update mechanisms used by the Red Hat Network from Red Hat Inc. After giving an introduction to this technology, I will then elaborate on its software update utility, up2date. Program setup, and numerous ways of running up2date will then be examined. Red Hat Network's benefits and limitations will be outlined. Four methodologies will also be outlined which can be used more easily to keep current large implementations of Red Hat Linux. I will include detaile...

Copyright SANS Institute
Author Retains Full Rights

AD
CounterTack
CounterTack Active Forensics for In-Progress Attacks
GET THE WHITE PAPER NOW >>>

Keeping Red Hat Linux Systems Secure with *up2date*

John Mravunac

GSEC Practical Assignment Version 1.4b, Option 1

8th July, 2003

© SANS Institute 2003, Author retains full rights

Abstract

In this paper I will give an in depth overview of the software update mechanisms used by the Red Hat Network from Red Hat Inc. After giving an introduction to this technology, I will then elaborate on its software update utility, up2date. Program setup, and numerous ways of running up2date will then be examined. Red Hat Network's benefits and limitations will be outlined. Four methodologies will also be outlined which can be used more easily to keep current large implementations of Red Hat Linux. I will include detailed update process flows and communication diagrams for each of the different update architectures.

The purpose of this paper is to inform system administrators who are responsible for Linux systems, of the importance of keeping their systems up to date. The ease with which system security can be achieved will also be examined. As with other operating systems, Linux systems that are not kept up to date with software patches can become insecure, and vulnerable to attack.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Introduction

In today's world of ever increasing technological growth, keeping computer systems current with the latest security errata, has become more important than ever. Linux is being adopted on a wide scale, because it is generally considered to be a secure operating system. However, as with all software systems, bugs can lead to exploitable vulnerabilities rendering the system insecure. Linux vendors have attempted to address this issue in a similar manner to Microsoft, with it's Software Update Services (SUS) utility. Examples of Linux software update utilities include the Red Hat Network (RHN) from RedHat, APT from Debian, and YasT2 from SuSE.

The only constant is change when it comes to the world of computer security. New bugs in software are constantly being found which create vulnerabilities within computer systems, and new exploits are constantly being written to take advantage of these. Part of a security administrator's job is to stay current with developments in software flaws, that may allow crackers to obtain unauthorised access to the network they are responsible to protect. Failing to keep software up to date which allows an attacker to gain highly confidential information can be disastrous to a company's future. Corporate espionage is not a new concept, but these days has taken on a new form by way of electronic information theft, and is growing in popularity.

> "Fortune 1,000 companies lost more than $45 billion last year from trade theft, according to a survey by the American Society for Industrial Security and Price Waterhouse Coopers. Other estimates put the figure closer to $100 billion."[1]

Web page defacement is another popular method of generating "fear, uncertainty and doubt"[2] in the quality of services a competitor may have.

Security is an issue that is playing a large role in today's decision making processes in regards to which operating systems to use in running businesses. Using systems considered to be more secure from the outset should hopefully help administrators keep the system more easily secure. This is one of the reasons why the Linux operating system has grown in popularity in the last few years. As companies have been testing this relatively young operating system and receiving positive results, other companies have been quick to adopt it also.

Linux since it began its development a little over 10 years ago, and has proved itself to be a stable operating system which has been adopted by many large organisations. Two of the major reasons why companies have been embracing the operating system are:

(i) it is considered secure, and
(ii) the total cost of ownership is lower than rival systems.

Currently there are approximately 133 Linux distributions being actively developed,

---

[1] The Associated Press. "High-Tech Spy vs. Spy". July 1, 2000
URL: http://abcnews.go.com/sections/tech/DailyNews/transmetaspy000701.html

[2] Irwin, Roger. "What Is FUD?" 1998.
URL: http://www.geocities.com/SiliconValley/Hills/9267/fuddef.html

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

of which the Red Hat Linux distribution has the largest market share. Having been founded in 1994, Red Hat has since formed partnerships with many large integration companies such as IBM and Sun, which will continue to increase the distribution's popularity. With more and more companies developing applications which work on the Linux platform, this is going to see the use of Linux spread even further. The server market has been an area that has seen Linux implemented most widely, for services such as mail, web and DNS. These critical systems are usually accessible directly from the Internet, a dangerous area to place a company critical machine. Therefore utmost care needs to be taken in ensuring the system is secure.

Even though a Linux operating system may be secure on the day of installation, it will not stay that way indefinitely. Sooner or later a bug in one of the many software components of a server operating system will be found. We have recently seen bugs appear in common software components such as OpenSSH, OpenSSL, and Bind. All of these are usually accessible from the Internet, and therefore if left unpatched, provide a significant threat to the machine they are run on. Fortunately when using Open Source software, administrators can take advantage of the Open Source community's fast bug patching. Along with the community of programmers, the Linux distribution vendors need to keep their distribution specific binary packages up to date with all the relevant patches. In order to be able to apply these patches, the administrator first needs to be aware that they exist. Staying current with security issues can be achieved in a number of ways, the most common and perhaps quickest way is to be subscribed to a security alert mailing list, such as the CERT® Advisory Mailing List.[3] There are also other mailing lists such as BugTraq[4], and distribution specific lists, which can be useful. Patches should be installed as soon as possible in order to get the machines back to a secure state.

In order to make the process simpler of keeping these Linux systems up to date, and therefore secure, a number of the major Linux software vendors have produced mechanisms that apply software patches to machines running their operating systems. Red Hat have produced an update mechanism called up2date which has been developed in order to make the job a relatively simple task. This is an important feature, as the job of looking after company servers may not always rest in the capable hands of an experienced administrator, depending on the size of the business. Many administrators may decide that it is sufficient to keep only the publicly accessible machines updated, but reports show that 70 - 80% of attacks originate within the company network.[5] These tools should allow for Red Hat Linux machines, both inside and outside the company network, to be easily kept up to date.

In order to be confident that updates will be maintained regularly, there needs to be a

---

[3] CERT® Advisory Mailing List
URL: http://www.cert.org

[4] BugTraq SecurityFocus Mailing List
URL: www.securityfocus.com

[5] Dempsey, Shelley. "Fraud: Here come the cyber-crime busters."
Business Review Weekly. Feb 2001
URL: http://brw.com.au/Stories/20010216/8897.aspx

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

clearly defined role assigned to one person. Doing so prevents confusion among the system administrators as they know who is responsible, and it therefore allows them to take control when other people are not around. Otherwise you run the risk of confusing administrators that another has already performed the updates, meanwhile the system(s) are left vulnerable.

To use binary packages or not to?

One of the debates which is often raised in the discussion concerning software updates, is whether it is advantageous to use precompiled binary packages, or to build the software from source code. There are benefits to be found in both methods. Using binary packages provided by the distribution, definitely makes the job much easier, especially when updating many packages on multiple systems. These packages have already been tested in order to work with other packages included in the distribution, which is important in maintaining the systems stability. On the other hand. one very good reason for building your own packages, is having the ability to create a leaner package, without unnecessary features compiled within it. Although with many of the Red Hat update mechanisms, listed below, you are able to specify which local packages to install. This allows you to download a source package (eg. Package-x.xx.src.rpm), build the binary package as lean as is required, and install it just as easily as a distribution package on all machines.

Other important benefits of using distribution supplied packages are:

(i) they support dependency checking which saves a lot of time in not having to perform multiple downloads, or having to visit numerous web sites in search of files.

(ii) Download is from a trusted source, so there is more confidence in the integrity of the installed software.

up2date

Red Hat Linux consists of many RPM (RPM Package Manager) Packages. These packages are comprised of various software applications and utilities. This is the utility developed by Red Hat for determining which system RPM packages need to be updated, via the Red Hat Network and installing/updating them. It works with standard Red Hat Linux systems, as well as Red Hat Enterprise Linux systems, and can be used for maintaining software on single home systems, as well as large corporate networks. *up2date*, in conjunction with the Red Hat Network, allows administrators to manage any number of servers and workstations securely and remotely from a central location, via an SSL-enabled Web browser. Speed is crucial when fixing security related problems, and from my experience Red Hat has usually been one of the first distributions to provide patches. Red Hat offers additional services such as Proxy and Satellite Servers which will be described in depth later, as well a Monitoring Module for a fee. One of the benefits Red Hat Linux derives from the structure of Linux is that ALL system updates may be downloaded and applied in the one process. There are no reboots necessary to complete the update (apart from kernel updates), and updates don't generally produce the requirement of additional new updates to be applied, as is the case with Microsoft operating

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

systems. Another point to make about the Red Hat package update system, is that the process is always a pull operation from the clients, rather than a push operation from the up2date server, which makes the procedure far more robust and reliable.

The Red Hat Network is capable of sending notifications via email to system administrators when new updates have been made available. Receiving notifications can save time in not having to do daily or weekly checks for new packages. The Red Hat Network website below (see Diagram 1), shows you which systems have out of date software.

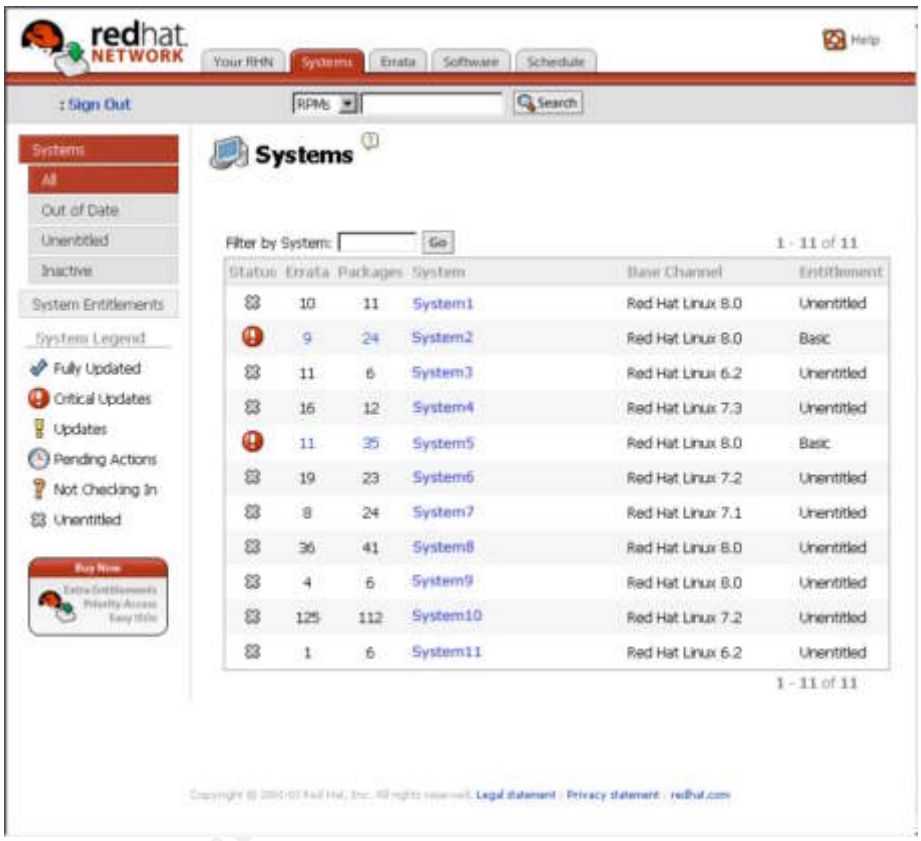

Diagram 1.

Software components:

up2date - the update agent that performs the package actions.
rhnsd - a daemon process which periodically polls the Red Hat Network to see if there are any queued actions available, and runs them. This daemon is necessary if you want to schedule updates or other actions through the Web interface.
rhn_check - checks the Red Hat Network for queued actions, and performs them.
rhn.redhat.com - the Red Hat Network website
rhnreg_ks - a program that allows systems to be registered to the RHN non-interactively (eg. during a kickstart installation)

The update agent has a quite a few configuration options, some of them being: installing packages once they are downloaded; downloading source RPMs along with binary RPMs; and, the option of upgrading packages where the default configuration file(s) have been modified.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Benefits

- All transactions are encrypted
- The site uses digital signatures
- All electronic communications with the Red Hat Network are signed using GPG
- Command line tool, GUI or daemon for remote updates
- Notification via email
- Rollbacks are possible
- SSL enabled Web site
- Dependency checking to ensure stability
- Trusted source for updates (Red Hat)

Limitations

- Each system needs to be registered on the Red Hat Network, which can be costly (later we will see a way around this)
- Only supports RedHat versions 6.2 and higher + RHE Linux
- Fee based system (although payment does give you access to the operating system ISOs, priority downloads, and priority notifications)

How up2date works

1. The update agent (up2date) on the client communicates with the RHN servers using XMLRPC and provides the system's 'System ID'.
2. The RHN server provides the client system with an authentication token, a list of channels the system is subscribed to (Red Hat 7.1, 7.2, 7.3, 8.0 and others), and the date the list of updates for the channel were updated.
3. The update agent downloads the latest update list if not already downloaded. The update list is a simple XML file containing a listing of all the available packages for the channel including some properties such as version and size.
4. The update agent decides which of the available RPM packages are relevant to this system.
5. The relevant RPM headers which have not already been downloaded are downloaded.
6. Checks are run on the RPM headers to determine any conflicts or whether any package dependencies are required.
7. The update agent downloads all required RPMs.
8. The update agent installs all downloaded RPMs.
9. The RHN servers are notified of the installed packages and your System Profile is updated.

Setup

Understanding the importance of staying current with software, RedHat has included the up2date package by default in all of the preset installation groups available during installation. This makes it a simple task of performing the following steps in order to update your system software:

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

1. Start Red Hat Network Registration Client

The up2date agent can be run via the command line by typing 'up2date' or via a GUI console which can be started by selecting the 'Red Hat Network' program from the desktop start menu. up2date requires the system to have Internet access, whether this access is direct, or via a proxy.

The first time up2date is run on a system any necessary changes to the configuration need to be made and saved before continuing. Some of the more common options to change would be the proxy settings, and the pkgSkipList. The pkgSkipList allows you to specify which packages will not be automatically updated if a new version is available, and usually specifies any kernel packages.

If you have not already manually imported the Red Hat, Inc. public key you will now be required to do so. This can be achieved by running the command:

```
rpm --import /usr/share/rhn/RPM-GPG-KEY
```

This is necessary to be able to verify the integrity of the downloaded packages, as each package has been digitally signed by Red Hat.

Note: the up2date agent requires you to either be logged in as the root user, or at least know the root user's password.

2. Register a User Account

To begin the registration process you will need to rerun the update agent program. Once the information screens (which highlight the benefits of using the Red Hat Network, and display the Privacy Statement) have been passed, you will be required to register a user account. Seeing as this is the first system you are registering with the RHN, you will need to choose a new unique username and password. Choose a password that is difficult to guess as this will be used to authenticate you via the Web interface. First time users are prompted with an additional information screen where you are able to supply optional information such as Name, Address, Contact details, and whether you would like to subscribe to the Red Hat e-Newsletter.

3. Register a System Profile

A unique System Profile is necessary for each computer system registered, and consists of hardware and software information about the system. The System Profile information is used by the Red Hat Network to determine what software update notifications you receive. You will be required to specify a Profile name for the current system, the hostname is used by default. You have the option of providing RHN with the hardware information about your system, such as RedHat version, CPU speed and IP address. If you do not wish to include the hardware and network information in your system profile, deselect 'Include the following information about hardware and network'.

In order to create a software profile the RHN registration will now list all the RPM packages found in your RPM database. These are the packages for which you will

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

receive notifications, and you can customise the list here. By default all installed packages are included in the list. This RPM list can be modified later via the RHN Web interface.

4. Finish Registration

To complete and confirm the system registration select 'Next' on the 'Send Profile Information to Red Hat Network' screen. This will send the system's profile information to the RHN, and place a digital certificate on your machine (/etc/sysconfig/rhn/systemid). This is a certificate that identifies your system to the RHN, and a file you may wish to backup.

Registration is now complete.

5. Entitle your system

Now that your system is registered it is necessary to entitle this system via the SSL enabled RHN web site, in order to obtain updates. To entitle your system, go to https://rhn.redhat.com[6] and login using the same username and password you just provided during the RHN registration. Selecting 'Systems' on the top menu bar will load a page displaying all of your registered systems, along with their errata status. Selecting 'System Entitlements' from the left navigation bar will load a page displaying the registered systems, along with an “Entitlement” selection drop down menu. As every registered system receives a free “Demo” subscription you should already see 'Demo' selected, otherwise you would select 'Demo' and click 'Update Entitlements'.

6. Run up2date

There are three ways to apply updates:

(i) run the command *up2date* from the command line

Running up2date from the command line is probably the most efficient and most flexible way to update your system. up2date can take many arguments as options, the most common in daily use being *-l* (or *--list*) to list the packages available for retrieval (see Diagram 2), and -u (or *--update*) to update the system with all of the relevant packages. The update argument will not update any packages on the file skip list, this would require the additional *-f* (or *--force*) option to be specified. Updating your system is a simple matter of running:

```
up2date -u
```

which will result in output similar to Diagram 3.

[6] Red Hat Network Home Page
URL: http://rhn.redhat.com

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

```
[root@mach1 root]# up2date -l

Fetching package list for channel: redhat-linux-i386-8.0...
########################################

Fetching Obsoletes list for channel: redhat-linux-i386-8.0...
########################################

Fetching rpm headers...
######################################
Name                                     Version        Rel
-----------------------------------------------------------
XFree86                                  4.2.1          21
XFree86-100dpi-fonts                     4.2.1          21
XFree86-75dpi-fonts                      4.2.1          21
XFree86-Mesa-libGL                       4.2.1          21
XFree86-Mesa-libGLU                      4.2.1          21
XFree86-Xnest                            4.2.1          21
XFree86-base-fonts                       4.2.1          21
XFree86-devel                            4.2.1          21
XFree86-font-utils                       4.2.1          21
XFree86-libs                             4.2.1          21
XFree86-tools                            4.2.1          21
XFree86-truetype-fonts                   4.2.1          21
XFree86-twm                              4.2.1          21
XFree86-xauth                            4.2.1          21
XFree86-xdm                              4.2.1          21
XFree86-xfs                              4.2.1          21
bash                                     2.05b          5.1
gnome-panel                              2.0.6          9.2
redhat-config-date                       1.5.15         1
unzip                                    5.50           12

The following Packages were marked to be skipped by your configuration:

Name                                     Version        Rel  Reason
-------------------------------------------------------------------------------
kernel                                   2.4.20         18.8 Pkg name/pattern
kernel-source                            2.4.20         18.8 Pkg name/pattern
```

Diagram 2.

```
[root@localhost root]# up2date -u

Fetching package list for channel: redhat-linux-i386-8.0...
########################################

Fetching Obsoletes list for channel: redhat-linux-i386-8.0...
########################################

Fetching rpm headers...

Testing package set / solving RPM inter-dependencies...
########################################
bash-2.05b-5.1.i386.rpm:    ########################## Done.
Preparing              ########################################### [100%]

Installing...
   1:bash                   ########################################### [100%]
```

Diagram 3.

If a package name is supplied as an option to the update agent on the command

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

line, the package will either be installed with the required dependencies, or updated to the most recent version along with it's associated packages.

(ii) run up2date via a GUI interface

If *up2date* is run on a system running a graphical desktop, or from the command line without any options, up2date's GUI interface will appear. Updating your system with this interface is a fairly straight forward process. Once the Channel to check for updates has been selected, the Update Agent will build a list of updated RPMS installed on your system. This list will be displayed in two parts, the packages flagged to be skipped, and the rest of the available package updates. The packages you wish to update should have their check box selected, and the package skip list may be overridden here also. If you are unsure whether or not to update a particular package, the GUI interface allows you to view the advisory for the selected package. The advisory outlines what the package does, and why the update has been made available. Once all packages have been selected, the Update Agent will test for conflicts and package dependencies (which will also be downloaded and installed). When the installation of the updates is complete you will be presented with a listing of all the packages that were just installed.

Updating your system is a simple matter of selecting check boxes and navigating through the Update Agent's screens with the 'Forward' button.

(iii) schedule updates via the RHN Web site

Software updates, new installations, removals and system reboots, can all be scheduled via the RHN website. Scheduling system reboots can be quite handy when having to administer remote systems, although it may be preferable to perform the task manually via SSH, in order to confirm that the system has started up successfully sooner. Management of multiple machines around the globe is made easy with this centralised management and reporting system. Signing onto the site provides you with a number of navigation bars and menus from which you can choose to modify the software installed on your registered systems, or check on the status of scheduled jobs. Clicking on the 'Systems' tab will display a list of all registered systems, along with their upgradeable packages, and relevant errata. If a system is “unentitled“, then clicking on 'System Entitlements' in the left menu will allow you to entitle the system using the 'Entitlement' drop down, and the 'Update Entitlements' button.

Scheduling the installation of software updates is performed by selecting a registered system from the 'Systems' page, and either clicking 'update now' beside 'Critical updates available' in red text, or by selecting 'Errata' from this systems navigation bar. The latter allows a subset of updates to be applied, whereas the first option assumes you wish to install all available updates. Completing the schedule setup is a matter of either just confirming you want to have the updates applied, or selecting which packages to update, and then confirming. See Diagram 4 for successful update output.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

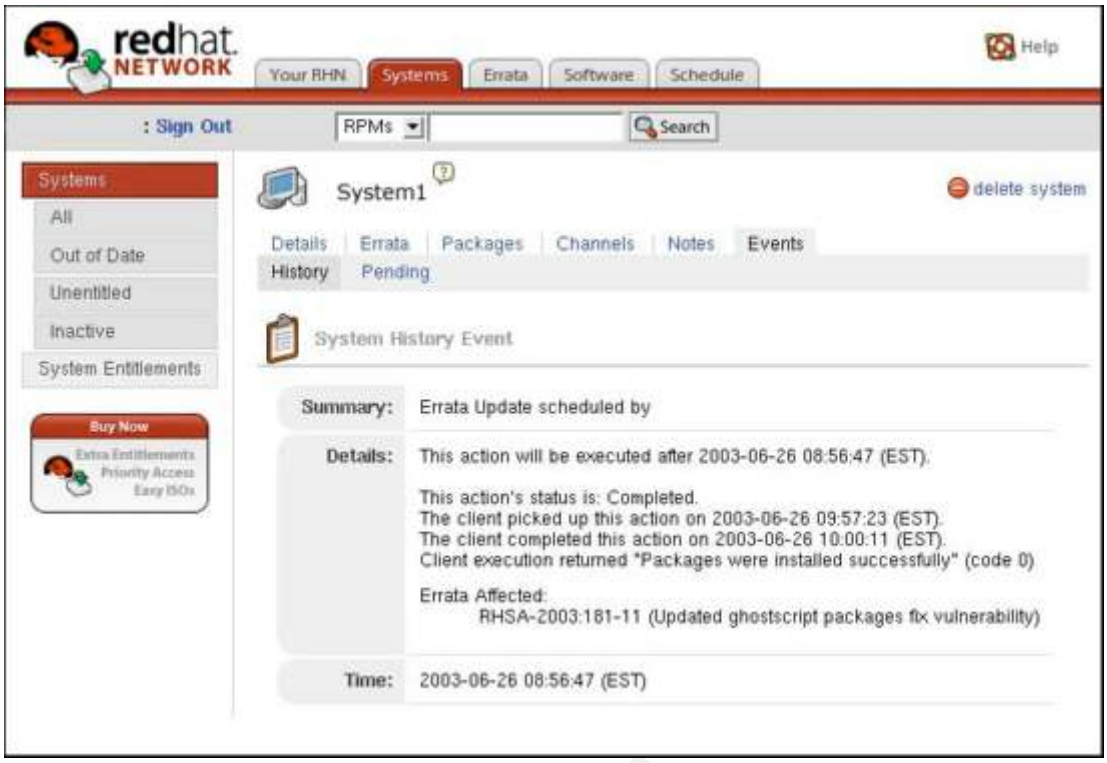

Diagram 4.

The RHN scheduling system works by setting up the jobs needed to be run by each System Profile on the RHN server. Each of the registered systems has a Red Hat Network Daemon (rhnsd) installed and running, which periodically (120 minutes is the default - this is set in the file /etc/sysconfig/rhn/rhnsd) connects to the RHN and checks for updates and notifications. The Red Hat Network Daemon will run an external program rhn_check to perform the task of connecting to the RHN servers, and retrieve any actions that may be queued. The rhn_check reads the system's digital server ID from /etc/sysconfig/rhn/systemid, and uses this to identify the machine to the RHN. Once authenticated, rhn_check begins sequentially processing the requested actions, reporting successes and failures back to the RHN.

Note: if the Red Hat Network Daemon configuration file is modified, then the daemon must be restarted (as root) by issuing the command:

```
service rhnsd restart
```

The minimum time interval allowed between checks is 60 mins, anything less will default back to 120 mins.

Multiple System Updates

When a larger number of machines need to be kept up to date, the task becomes an even larger time restraint, and the manual procedures outlined above may not be suitable. There are a number of ways around this, and it is a matter of finding the solution which is most advantageous to follow. Below four methods have been outlined in order to keep a large number of machines current.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Option 1

Automatic application of errata - All systems registered with the RHN have the option of automatically downloading and installing relevant updates, with no user intervention (see Diagram 5). This option is activated by logging onto the RHN website and navigating to the properties page of each system. The 'Auto Errata Update:' property needs to be modified to 'Yes'. Diagram 6 shows the communication flows for this update method.

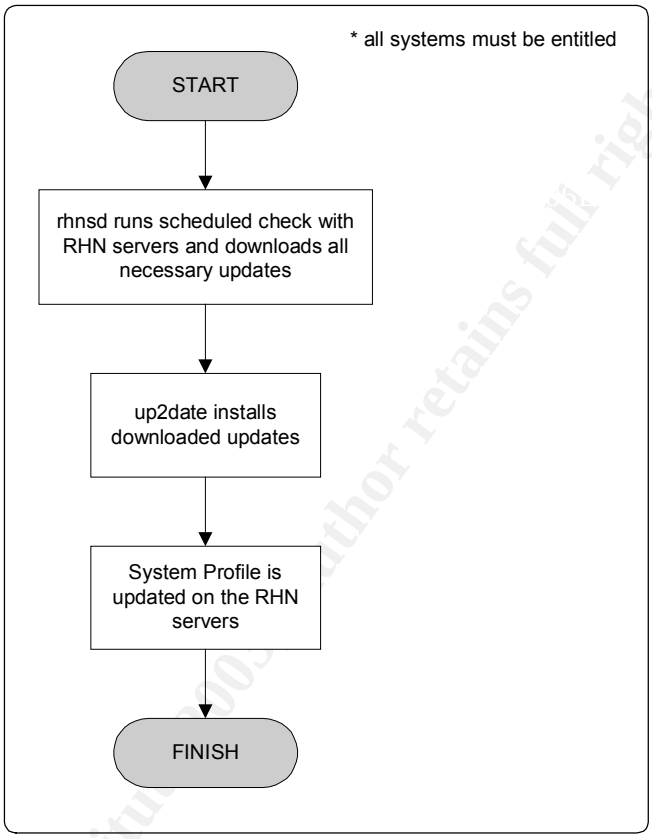

Diagram 5.

Although this option may sound like a good idea, it is not a recommended method of keeping your production systems current. All packages including the SkipList packages will be applied as soon as they are available, which could result in system failures due to package and environment conflicts. Also worth noting, any kernel updates require a reboot, which may not be performed if administrators are unaware of the update being applied.

A drawback with this method is that all machines on your network need to have either HTTP or HTTPS access to the Internet.

Total cost of update method : US$60 per client per year

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

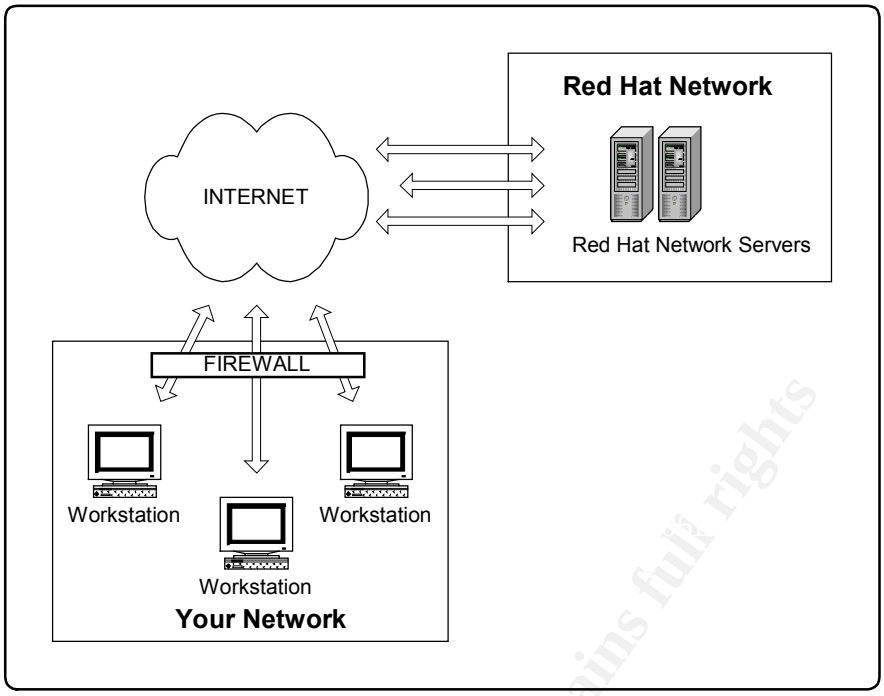

Diagram 6.

Option 2

Red Hat Network Enterprise (RHEN) - Subscribing to this service brings with it additional features which simplify the job of managing a network of RedHat Linux systems. The additional features include Package Profile Comparison, Search Systems, System Grouping, Multiple Administrators, System Set Manager and Massive Scalability. Our focus is on the 'System Set Manager' feature which allows you to apply actions to sets of systems, rather than to single systems. This feature alone would save an enormous amount of time when trying to keep the software on these systems current. 'Multiple Administrators' would increase the time saving benefits by allowing a number of administrators to look after the status of their set of systems, whether this is geographically (their office), or workload-focused (type of service the system supplies eg. web serving, workstations). As can be seen in Diagram 7, the updates are initiated by the administrator and downloaded directly from Red Hat's servers. The communication flow is similar to Diagram 5.

A drawback with this method is that all machines on your network need to have either HTTP or HTTPS access to the Internet.

Total cost of update method : US$96 per client per year

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

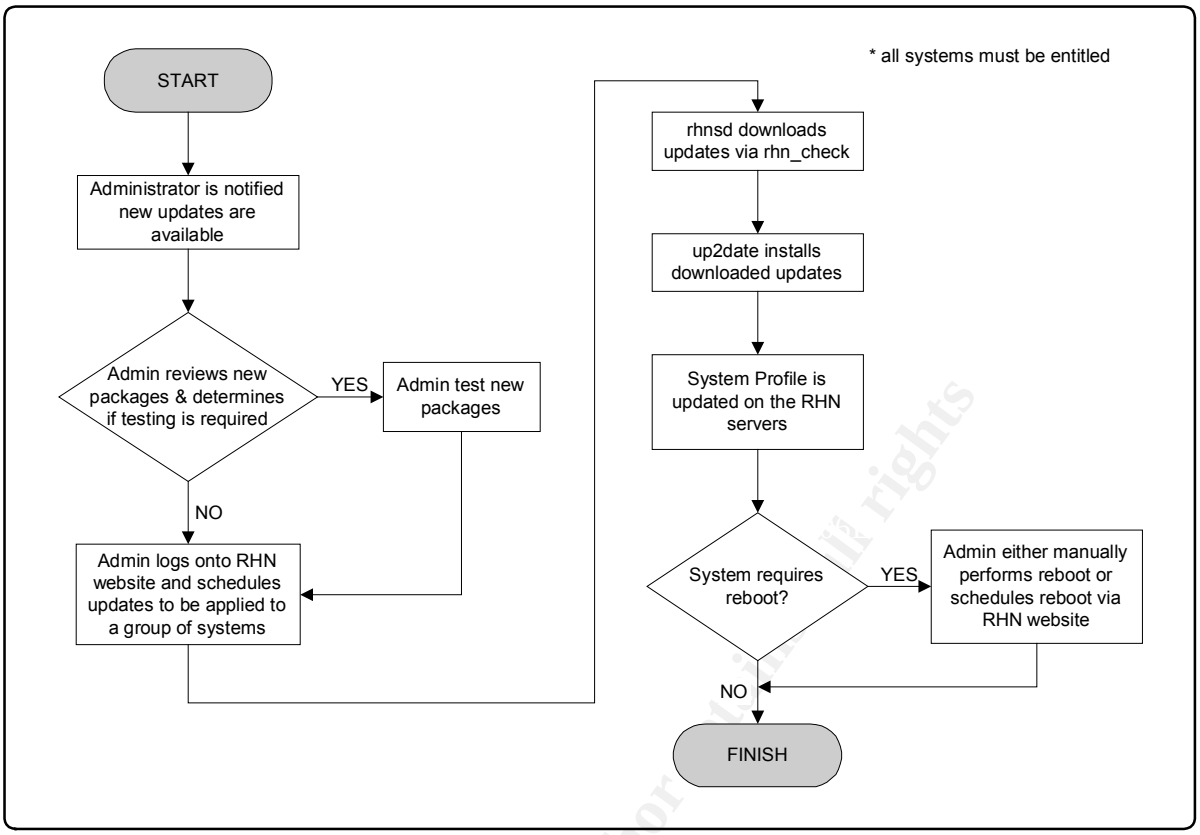

Diagram 7.

Option 3

Red Hat Proxy Servers - This is an add on service to the Red Hat Network Enterprise which by means of a different architecture model allows extra flexibility in managing a large number of systems. Rather than connecting directly to the RHN servers themselves, the systems on your network rely on the Proxy Server to perform this task for them, as well as caching the downloaded content (see Diagram 9). Subscription to this service provides an enormous reduction in bandwidth utilisation, and increases the speed with which systems obtain their updates. This is due to the Proxy Server having to download the updates only once and distribute them to local clients from there.

Custom and third party errata can also be applied seamlessly using the Proxy Server module by creating custom software channel. This functionality provides an extremely easy method of rolling out additional software to any or all the systems on your network.

Total cost of update method : Approx. US$12000 per server + US$96 per client per year

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

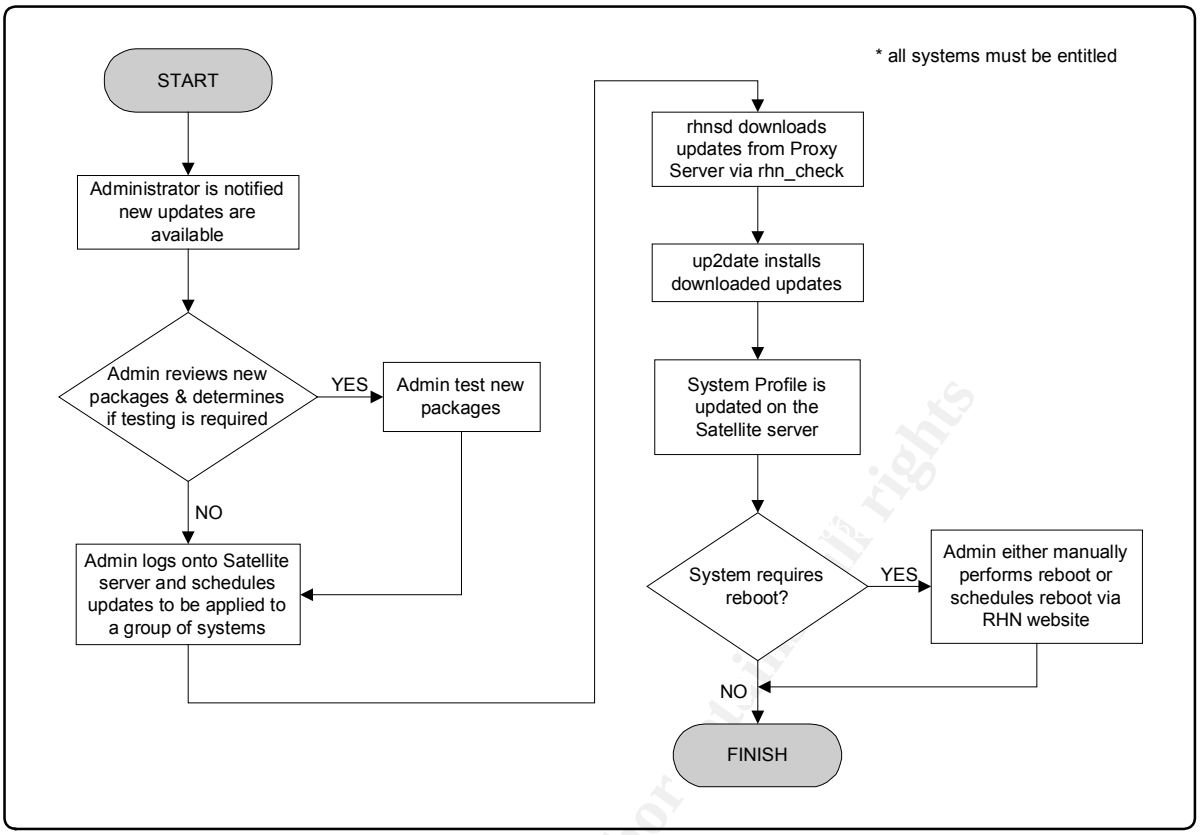

Diagram 8.

Red Hat Satellite Servers - These servers allow all the functionality of the Red Hat Network Enterprise services to be implemented within the network. The Satellite server performs the role of the RHN server, authenticating and authorising systems connecting to it, and distributing any necessary updates (see Diagram 8). There are a number of benefits from having this server within the corporate network. System updates may be performed without the need for Internet connectivity or having to rely on the RHN servers being available (see Diagram 9). So apart from the extra redundancy this solution provides, it also increases the security of the update system, by running everything within your firewall(s) which drastically reduces bandwidth costs.

Having the entire RHEN platform running on your servers adds the flexibility of being able to create customised channels with which to update systems. It also allows you to create your own notification policies, errata messages and package solutions. Packaging updates into groups has the benefit of saving time when updating similar types of systems, but can also be very useful when deployments need to be staged. The Satellite Server can be updated either over the Internet or via update discs supplied by Red Hat. The major downside of this method is the cost because the functionality does provide easy software updates even for very large organisations.

Total cost of update method : Approx. US$24000 per server + US$96 per client per year

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

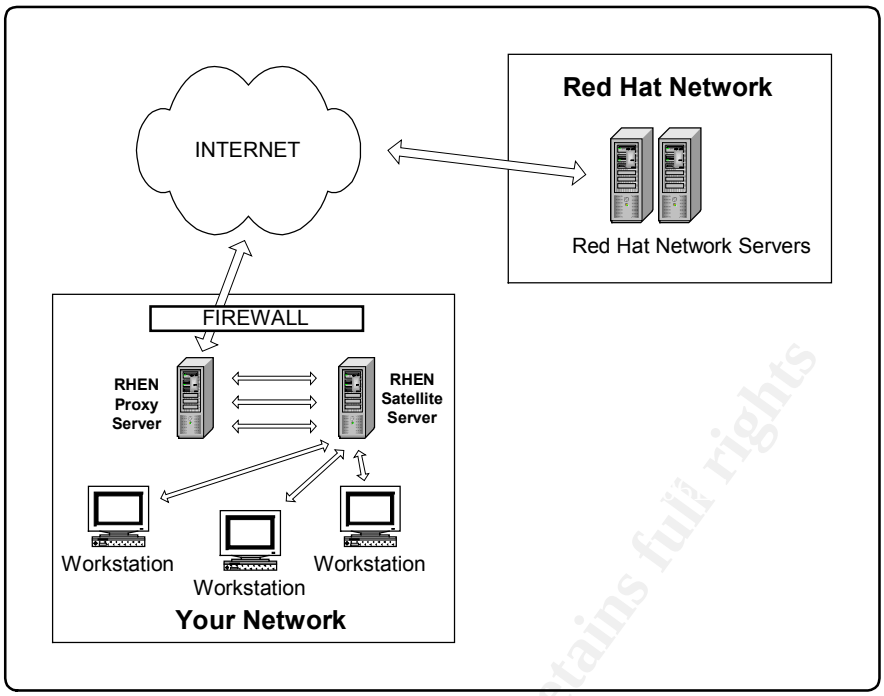

Diagram 9.

Option 4

Not-RedHat up2date server - This option requires the setup and use of a third party open source application, which mimics the main functionality of Red Hat's Satellite Server Software Delivery Module. The application is called NRH-up2date and can be downloaded free of charge. The major benefits with this option are the same as those mentioned in 'Option 3', but with the added cost advantage. Also worth noting is that by using NRH-up2date none of the systems obtaining updates need to be registered with the RHN, further adding to its list of advantages. Systems are able to register and obtain a unique System ID from the NRH-up2date server, list and download available updates for their version of Red Hat Linux (RHL). The server is able to serve updates for multiple RHL versions, and will soon allow custom channels to be set up. This solution is capable of all the security features Red Hat offers, but in addition offers the option of locking down which User IDs are able to register new systems, and can implement checksum checking of existing System IDs. NRH-up2date also includes the use of an access authentication token which is handed out on successful login and does not allow downloads of packages without one.

This is still a fairly young project so may contain some glitches, but in my experience has worked really well. The latest release version is 1.2.2, and new versions are common, as the project is being actively developed. Support is available in the form of a user forum where people appear to be quite helpful and prompt with their suggestions. There are new features in development currently, one of which is the ability to create custom channels, and another being the client systems tacking functionality, which is very useful to system administrators. Once these additional features are added to what NRH-up2date can already perform, there will be very little

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

difference between it and Red Hat's own service.

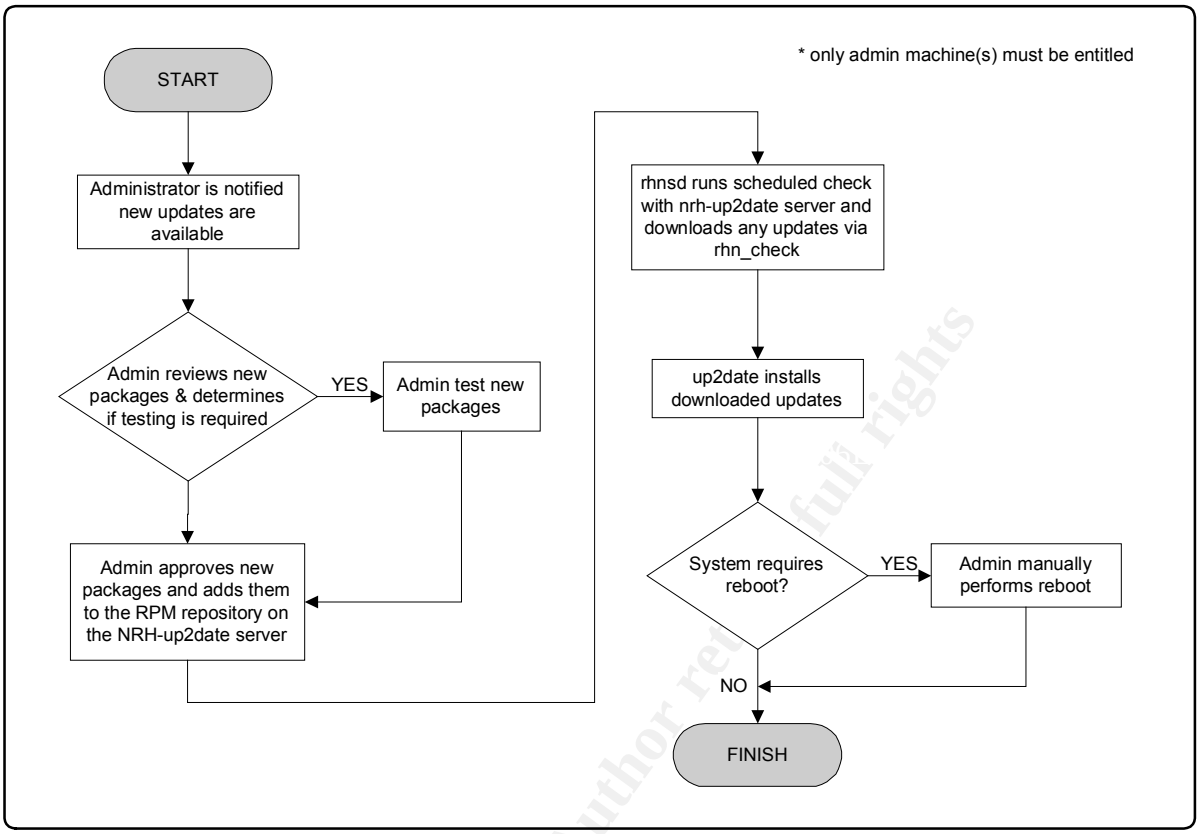

Diagram 10.

Referring to Diagram 10 above, an effective method of maintaining a larger deployment of Red Hat Linux machines would be to download and test the latest updates on a set of systems with identical setups to production machines. Once the updates have been proven on the test servers and workstations, the update RPMs can be added to the repository on the NRH-up2date server(s) from which the production systems will automatically receive them (see Diagram 11). In order for the production systems to automatically download and apply the available updates, a cron job (a scheduled job run by a cron daemon) run as the root user will need to be configured. This would serve the same effect as the 'auto errata' property on the RHN web site.

Total cost of update method: US$60 per server per year + NIL per client

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

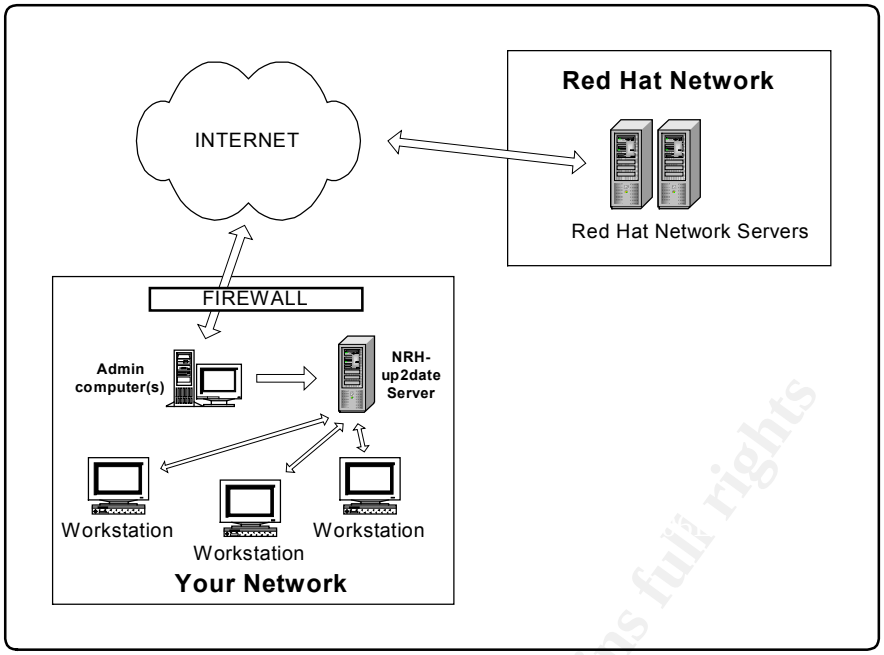

Diagram 11.

NRH-up2date is not the only active project aiming to develop an alternative to Red Hat's costly Red Hat Network. Another example is called CURRENT[7], and currently provides a similar amount of functionality as NRH-up2date. The project developers have taken a slightly different approach, in that they have coded mainly in Python, rather than perl, with some python, and are aiming towards having a SQL backend database. Future developments will include client management, and will hopefully be a total replacement to what Red Hat has to offer.

Conclusion

Linux, and in particular Red Hat Linux, is making inroads into many organisations all around the world. This is due in part to its stability and cost effectiveness, but also because of its relatively better security. Although even with its superior network and system security, it is only effective when kept up to date. Fortunately the Linux vendors, as well as the developer community are aware of the importance of staying secure, and are prompt in releasing any necessary updates. To ensure that these updates are applied to as many systems as possible, a number of software update mechanisms have been released. up2date is just one useful utility which can be employed to keep a system secure via its ability to check for, download, and install updates. The update mechanisms described above have been successfully tested and do work in keeping systems secure to exploit attacks, whilst at the same time requiring very little ongoing administration. There are pros and cons to each update methodology, and each should be explored to determine the most advantageous solution. Each method will work to keep your system up to date, and therefore stay secure with Red Hat Linux operating systems.

[7] CURRENT
URL: http://current.tigris.org

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

REFERENCES

Bauer, Mick. "Staying Current without Going Insane"
Linux Journal. July 2002 (Issue 99): 38-43

Bodnar, Ladislav. "Linux Distributions – Facts and Figures". 5 July, 2003.
URL: http://www.distrowatch.com/stats.php?1

Egan, Dave (Ed.) Red Hat Certified Engineer Study Guide
California: Osborne/McGraw-Hill, 2000

Dempsey, Shelley. "Fraud: Here come the cyber-crime busters."
Business Review Weekly. Feb 2001
URL: http://brw.com.au/Stories/20010216/8897.aspx

Irwin, Roger. "What Is FUD?" 1998.
URL: http://www.geocities.com/SiliconValley/Hills/9267/fuddef.html

Kramarov, Alex. "NRH-up2date". 7 April, 2003.
URL: http://nrh-up2date.com/cvs/docs/INSTALL

Red Hat Inc."Understanding the differences between Red Hat Enterprise Network and Red Hat Network". 2003.
URL: http://www.redhat.com/software/whichnetwork/

Red Hat Inc. "Red Hat Network Enterprise - User Reference Guide 2.1". 2003.
URL: http://www.redhat.com/docs/manuals/RHNetwork/ref-guide/enterprise/

Red Hat Network Basic:
URL: http://www.redhat.com/docs/manuals/RHNetwork/ref-guide/

The Associated Press. "High-Tech Spy vs. Spy". July 1, 2000
URL: http://abcnews.go.com/sections/tech/DailyNews/transmetaspy000701.html

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

RESOURCES:

BugTraq SecurityFocus Mailing List
URL: www.securityfocus.com

CERT® Advisory Mailing List
URL: http://www.cert.org

CURRENT
URL: http://current.tigris.org

Red Hat Network Home Page
URL: http://rhn.redhat.com

RPM update utitity - rhupdate
URL: http://www.jjminer.org/rhupdate/

up2date Manual Pages
`man up2date`

© SANS Institute 2003, Author retains full rights

Last Updated: May 26th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**