Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

Installing and Securing Red Hat Linux 8.0 on a IBM Thinkpad

Michael Sparks, GSEC, CISSP

THIS PRACTICAL IS DEDICATED TO MY LATE FRIEND AND CO-WORKER KEN "KENNY B" BARTLETT, GCUX, CISSP. HE TAUGHT ME WHAT A TRUE UNIX GURU WAS ALL ABOUT. TAKEN BEFORE HIS TIME – GSG WILL ALWAYS REMEMBER HIM.

TABLE OF CONTENTS

Abstract

With the recent release of Red Hat Linux 8.0[1] (RH 8.0), and newly acquired Systems, Administration, and Network Security (SANS[2]) "Securing UNIX Systems"[3] training, I felt inspired to write this GIAC Certified UNIX Security Administrator (GCUX) practical assignment on "Installing and Securing Red Hat Linux 8.0 on an IBM ThinkPad". For the remainder of the document, I have written various third person type settings to keep the format as generic as possible, all the while, delivering my personal interpretation and experience of security controls and safeguards that should be added to any Linux system when it is introduced into a business environment. The objective is to deliver a secure portable Linux workstation to a small fictitious business office where would-be employees on a basic Local Area Network (LAN)[4] will be able to perform computer related business functions as mandated by their day-to-day responsibilities. For the sake of clarity, imagine that these employees work for an agency called "Windy Town Bookkeepers (WTB)." The employees of WTB work out of a cubicle, when performing primary duties, but must have the ability to move to various conference rooms when other departments require their expertise; hence the need for a laptop instead of a regular desktop computer. From an installation perspective, the assumption is that the person following this "step-by-step" installation is a moderately experienced UNIX or Linux system administrator.

"As a disclaimer, this would-be firm in no way represents any true-life business, company, corporation, or bookkeeping organization, either past, present, or future, no persons living or deceased, in as far as the author is aware of, at the time of this writing. As well, it in no way represents the views of the author's current employer or states or implies an association or sponsorship by Red Hat® Linux® other than allowed by page 9 of Red Hat's Trademark Guidelines,[5] which allows this use under an educational affiliation with SANS. Also, that all the material within is delivered in an "as is" state, meaning that given the authors current knowledge and skill level; this practical strives to deliver the author's best methods known for securing a Red Hat 8.0 work station. It is, in no way meant to replace the ever-demanding need to stay current with security hot fixes, release notes, continuous security diligence, or any appropriate paraphernalia required to protect the business and its end user, etc. With that being said, the build of our future employees' laptops will be performed with the thought that funds were somewhat limited, hence the IBM model 600 which was chosen for the system, and that the system, once delivered, will be required to share and store information that at times could be sensitive in nature, thus requiring copious security.

---

[1] http://www.linuxplanet.com/linuxplanet/reports/4460/1/

[2] http://www.sans.org

[3] http://www.giac.org/subject_certs.php#GCUX

[4] http://www.pcwebopaedia.com/TERM/l/local_area_network_LAN.html

[5] http://www.redhat.com/about/corporate/trademark/guidelines/?page=9

Security 101

Before starting this project, the topic of security in general needs to be addressed. A multitude of physical controls, security hot fixes, systems to monitor for intrusion, and a myriad of other techno-geek tools or software can be put in place in a network to protect your end user's laptop. However, all this will fail if you do not start with some kind of security structure and knowledge base of why you need to put all these things there in the first place. To be secure, the WTB executive and security staffs must have an outline of a clear environmental and informational security plan to march too. In this plan, it is good to know the who, what, when, where, why, and how of the march. All the five W's will be addressed with a document that the executive staff has created to help the executives, their staff, the employees, or any legally bound third parties of WTB understand acceptable use and unacceptable use. This document is titled Windy Town Security Policies and should be referred to any time a question arises as to what is or is not expected from an organizational security perspective. The following is a sketch of possible policy outline with brief descriptions of what each area covers:

Policy (Which way should I go George?)
Document Title: Windy Town Security Policies

Objective: To provide WTB with a clearly defined policy that establishes what is expected from an employee concerning acceptable use, compliance, security, and general usage of all WTB assets. This includes, but may not be limited to, environmental, intellectual, informational, third party, and physical assets along with any interaction that occurs because of employment with WTB.

Scope: This policy applies to all WTB' employees and any persons that agree to be bound through a legal binding agreement to this WTB' policy.

> Note: Policies, Procedures, and Processes should be clearly defined. As a measure to increase your compliance in each of these areas, policy should identify what is and is not expected of any person who is bound by these entities that may be a subset of the overall policy.

Good security should be an overall program and not an automated technological tool that can be employed to protect your company (although our security program may use automated tools as one layer of "Defense in Depth" – See Defense in Depth defined under the Infrastructure Design section). The following areas, with descriptions, will probably serve as a good baseline at a general policy to help protect the owners, management, employees, and third party groups that may be involved with the WTB Company:

- Acceptable Use - This is your primary statement that will identify what is expected in general from any person that is vetted[6] with this policy. Generally, there are three to four primary areas of concern that should have brief summaries of what is or is not

---

[6] Having been trained and tested/approved for the subject matter.

expected. The following are the authors recommendation, however, each company is different and it is suggested that you involve a legal consultant to validate what is required of your company:

- o Business and General – This describes what normal business you would expect from policy aware personnel.
- o Human Resource (HR) – Covers any requirements from a company and legal aspect concerning human relations.
- o Legal – Laws change all the time and this must be encompassed in any policy creation, modification, or removal.

- Compliance – Define what is or is not required and recommended along with clearly defined results of non-compliance.
- Security Awareness – The people that read this policy and are trained about security will be your greatest assets. Don't just feed them security; teach them how to incorporate security into their regular habits, both at work and away from work, and keep them up to date with security issues and how employees can handle these issues when faced with them. When incidents like mass-mailing viruses occur or a disgruntled client threatens violence against one of your employees, this awareness will help make your response team's life much easier, along with shorter recovery and less costs to your company if the people know how they should respond to such issues.
- Access Control – Securely speaking, any access should be determined on a "need to have" basis. This helps compartmentalize your company and if controls are mitigated in one area, it will most likely not pose a risk or exposure to all areas.
- Threats – Threats for this document are defined as a combination of a threat (usually a person or entity that has the capability to affect your company like a hacker or a tornado), a tool, such as malicious code, and likelihood, which causes you security problems or incidents. Items that might fall into this bucket are hackers, viruses, acts of God, catastrophes, etc.
- System Use – Describes what the system is intended to perform or accomplish, what controls are required, and who is responsible for the controls at each level. You may break this up into areas such as personal computers (PCs), controlled access areas (physical and intellectual), and network. These policies, procedures, behavior restrictions, etc. must address the needs of your company. From a security perspective, not only does it map out what is expected, but when normal functions deviate it will help alert the user that something is not functioning correctly which may be the sign of malicious or unauthorized activity.
- Classified Information – This area should define how any asset is classified, whether it is intellectual or physical, according to potential impact to the company. This sensitivity has a label attached to it, such as non-classified, confidential, or secret and the consequence associated with this label. An example of non-classified material, if shared, has no direct impact on the company's profit margin where unauthorized disclosure of information classified as Secret may incur legal or monetary ramifications. Here is where a process for authentication, encryption, and decryption of data should be identified. Authentication can be thought of as

7

something you know, something you have, or something you are. Two-factor authentication might be a password and a Secure ID pin number.[7]

- System Administration – Identify how administration is performed, when, and by whom, so there is no mistake on who can introduce changes to your areas. This may be divided into physical and intellectual areas depending on the size of your company.
- Incident Response – This will most likely include processes, procedures, and a team that comes to the needs of the company if there are any security issues or incidents. Depending on the size of your company, this team may include regular employees, a specialized computer or physical security response team, and a third party company that specializes in security incident response. Some portions of this response may include or be handled by government or state agencies
- Availability – In order to have a stable company, you have to identify what components are necessary to maintain business continuity or recover from a disaster in order to keep the business running. Backups, duplicate equipment, redundant servers, and alternative systems or recovery sites are terms that should be researched in order to keep your company assets available when you need them.
- Physical Security – Locked cabinets, building access, and any physical measures that are required for life safety or security should be addressed in this section of the policy.
- Exceptions – Business and security are a balancing act and sometimes there needs to be the ability to allow changes if the business expects to reap profits. These exceptions and how to go about receiving approval for them should be identified here. Generally, exceptions should be determined relative to their overall risk to the company and should have the appropriate level of authority approve them and establish some type of accountability if things go wrong because of an exception.
- Policy Change Process – With all rules that are identified, there must be a way to remove, modify, add, or increase the strength of any policies that exist. This is the area that should define how that takes place.

Policies are important and should be customized appropriately for your company, so take what is relative from the previous example and add, change, or remove what fits your needs. Remember, it is a good idea to have legal counsel on the final policy and make sure that whoever must follow this document reads and signs a copy for your and their protection.

If you need further help in this area, there are several examples and books that can be found on the Internet or you can purchase a comprehensive set of Information Security Policies by Charles Cresson Wood (http://www.netiq.com/order/publications.asp).

---

[7] http://www.rsasecurity.com/products/securid/index.html

Why Do We Need Security? (We're not in Kansas any more!)

When bookkeepers graduate from Business College, they generally don't say to themselves "boy I better go get a book on how to protect against hackers or viruses", so any security education that is required must come to them when they are hired on to work for your company. This section is a collection of security terms, definitions, and a short summary that will help the workers to understand why your WTB employees need to be educated about security.

Security Defined - Security is best defined as the measures required to protect WTB and their assets from illegal, inappropriate, unauthorized, malicious, or any unwanted behavior or alteration that attempts to disrupt normal business areas related to Confidentiality, Integrity, and Availability.

Confidentiality – At times customers, laws, and businesses must guard information or assets from unauthorized disclosure. This unauthorized disclosure of any information or sensitive material, whether it is intellectual or physical can be seen as a confidentiality breach. An example might be a pre-patent document or a customer's social security number that is published to the Internet without permission.

Integrity – Integrity can be thought of, as what you see is what you believe you should get. If a document is sent via email or a customer ledger is stored on a hard drive, you would expect it to be the same exact information that was put there in the first place. If it is not, the integrity is said to be tainted or unreliable.

Availability – Whatever is needed to perform a job function or to keep a business running must be available when it is needed. In security, this is addressed using the term Availability.

Risk – Risk for this paper is defined as the multiple of Threat x Vulnerability x Consequence. As risk cannot generally be removed, altogether while maintaining acceptable business operations that return profits, our security mindset will be to manage risk to an acceptable level. The risk values in this environment are determined through a qualitative and quantitative process and are identified as low, moderate, or high. For WTB management, low risk is the only acceptable risk that should exist in their business environment.

Threat – Examples are hackers, disgruntled employees or customers, self-propagating Malware[8], natural disasters such as tornados, etc.

Vulnerability – An unrealized weakness in a software system or program, defensive mechanism, or a control that allows unexpected or unauthorized action to occur.

Consequence – The impact incurred, perceived or otherwise, that affects normal business expectations. This could be as simple as loss of credibility to a company or as horrendous

---

[8] Malicious Software

9

as the demise of a company due to a constant hacker attack on your network where business was unable to return to a normal state.

Exploit – Generally software or a method that takes advantage of a vulnerability.

Low Risk – This is where generally acceptable principles or controls have been applied and the business can maintain operations that are expected to return acceptable profits.

Moderate Risk – This is where identified vulnerabilities exist and minimal measures or controls may or may not be in place, thus allowing the potential for exploitation to exist. The likelihood that exploitation will occur is relative to multiple factors that must be theorized when risk is assessed.

High Risk – This is unacceptable in all cases. This is where risk, likelihood of exploitation, and human life safety are in critically dangerous positions and should not be tolerated. High risk must be reduced as quickly as possible without creating other equal levels of risk. In software, this may be a vulnerability that allows privilege escalation to administrator or 'root' level access. In physical issues, this may be an open tile in a data center floor that is not roped off and circled with orange cones to identify a dangerous situation.

Likelihood - Confidence that an event or incident may or may not take place. This confidence can be assigned levels just like risk of low, moderate, or high. E.g., "There was a high likelihood of the tornado touching our building."

Security is a holistic program that is required when dealing with technology, business, people, and any other entities during our current climate. There is not a day that goes by where you do not hear of hackers or terrorism affecting some segment of the world. This fact coupled with legal and moral ethics; require awareness, knowledge, action and diligence to help protect personnel, assets, and business interactions from potential threats. Security, which can include environmental safety, should never be seen as a burden, but a responsibility and an obligation that is perceived as common value addition to any successful business.

System Description

During our project, we will be using an IBM ThinkPad 600 (TP600). It is not one of the newer laptops that IBM makes and if you have a larger budget, here is some high-end laptop or desktop models that IBM offers:

http://www-132.ibm.com/webapp/wcs/stores/servlet/CategoryDisplay?categoryId=2035724&storeId=1&catalogId=-840&langId=-1&ca=sbcthinkpad&me=W&met=inli&re=SBC

http://www-132.ibm.com/webapp/wcs/stores/servlet/CategoryDisplay?categoryId=2048974&storeId=1&catalogId=-840&langId=-1&ca=sbcnetvista&me=W&met=inli&re=SBC or

10

Please feel free to pick the system of your choice, as long as it is covered by Red Hat's compatibility list.[9]

Here is a table of the hardware specifications that will be used during the installation:

Hardware Selection for Finished System	
Manufacturer	IBM
System	ThinkPad 600
Type	2645
Architecture	AT Bus
System Clock	33 MHz
CPU Model	Pentium II
CPU Speed	300 MHz
Memory	128 Megabytes
Network Interface Card (NIC)	Intel® PRO/100 CardBus II
Hard Drive	IBM-DADA-25120 5.1GB
CDROM and Floppy Drives	The CDROM is installed in the chassis's bay and there is an externally attached floppy drive. Both are IBM products designed for the TP600. The floppy drive will be required to create a rescue disk.

For the complete IBM Technical Reference guides, for the ThinkPad 600, visit
ftp://ftp.pc.ibm.com/pub/pccbbs/mobiles/600tech.pdf

Red Hat Requirements

Now that we know the system description of where Red Hat Linux 8.0 will land, I want to take this time to brief you on some requirements laid out by Red Hat in order to be successful in the installation and hardening[10] of our future system.

---

[9] http://hardware.redhat.com

[10] http://dcb.sun.com/practices/profiles/solaris_security.jsp *Definition:* OS hardening is a process for reducing the vulnerability of a system by correcting or minimizing known OS security issues. Sun, 2001

If you purchase the original equipment manufacture compact disk (OEM CD) set, on the bottom of the box are the following requirements:

Hardware Compatibility
Red Hat Linux supports most modern PC hardware. Please check the Hardware Compatibility List at http://hardware.redhat.com I have included a screenshot (see figure 1.1) of the advanced search engine that you can use for other hardware compatibility checks as IBM's laptop is compatible, otherwise I could not have written this document☺

Minimum and Recommended Hardware Requirements	
CPU: Minimum:	Pentium Class
Recommended for text-mode:	200 Megahertz Pentium-class or better
Recommended for graphical:	400 Megahertz Pentium II or better
Hard Disk Space: *	
Personal Desktop:	1.5GB
Workstation:	2.0GB
Server:	1.3GB
Custom Minimum Installation: *Additional space will be required for file storage.	400MB

12

Memory:	
Minimum for text-mode:	64MB
Minimum for graphical:	128MB
Recommended for graphical:	192MB

There is also a sample list of compatible hardware components on the bottom of the OEM box; however, I felt this was too much information and thought it would be a lot easier to include an Individual Hardware Component Checklist template to streamline your compatibility validation. I have given the list its own pages (see figure 1) so you can print it and fill it in manually or copy and paste the software version into an editor or word processor of your choice for easy electronic population.

13

Individual Hardware Components and Their Details (Template)	
CPU:	
Intel:	*Fill in according to your system*
AMD:	*Fill in according to your system*
Duron:	*Fill in according to your system*
Other:	*Fill in according to your system*
Hard Disk Space*:	
Your System:	400MB or greater
*Additional space will be required for file storage.	
Memory:	
Minimum for text-mode:	64MB or greater
Minimum for graphical:	128MB or greater
Recommended for graphical:	128MB or greater
Video Cards:	
3DFX:	*Fill in according to your system*
ATI:	*Fill in according to your system*
Intel:	*Fill in according to your system*
Other:	*Fill in according to your system*
SCSI Controllers:	
Adaptec:	*Fill in according to your system*
AMI:	*Fill in according to your system*
Dell:	*Fill in according to your system*

Other:	*Fill in according to your system*
IDE Controllers:	
ATA:	*Fill in according to your system*
AMD:	*Fill in according to your system*
Intel:	*Fill in according to your system*
Other:	*Fill in according to your system*
Network Cards:	
3COM:	*Fill in according to your system*
Adaptec:	*Fill in according to your system*
Intel:	*Fill in according to your system*
Other:	*Fill in according to your system*
Modem or ISDN:	
Hayes:	*Fill in according to your system*
Other:	*Fill in according to your system*
Sound Card:	*Fill in according to your system*
Creative Labs:	
Other:	*Fill in according to your system*
Miscellaneous:	*Fill in according to your system*

Figure 1 Individual Hardware Component Checklist

15

Once you have populated your individual hardware component checklist, pay a visit to the Red Hat website to understand whether your system will be compatible. I have included a footnote for the RH website link[11] and a screen shot of the Advanced Search fields (See Figure 2) that you should see once you connect to the link. Although this specific system was not in their general hardware lists, the hardware compatibility list will be of great help to determine if Red Hat supports your specific hardware, if different from this laptop model. In my case, it was decided to take a chance in the compatibility department; especially since it is the only system available in order to complete this document. Not to worry; if it had failed in the dry run installation, the writing of this step-by-step guide would not have been completed.
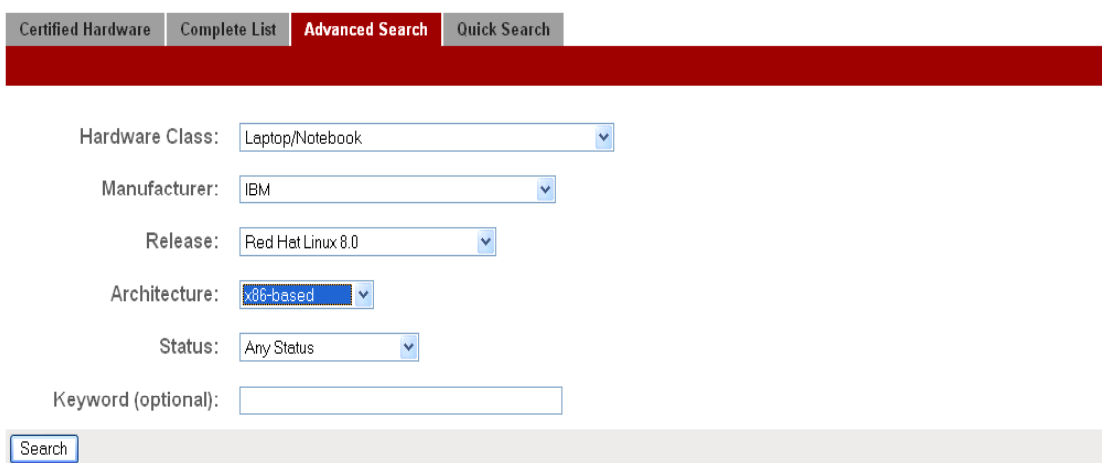
Figure 2 Red Hat Hardware Compatibility Advanced Search Screenshot

Laptop Role

As stated previously in the Abstract section, the objective is to deliver a secure portable Linux workstation to a small fictitious business office where would-be employees on a basic Local Area Network (LAN) will be able to perform computer related business functions as mandated by their day-to-day responsibilities. The next two sections describe what is expected of the bookkeeper who will be using the laptop and the software that will be installed in order to satisfy these requirements.

Employee Roles and Responsibilities

Our WTB will be required to fulfill and perform the following requirements in their day-to-day responsibilities:

- Able to work with sensitive and confidential material
- Be Information technology security aware

---

[11] http://hardware.redhat.com

16

- Also to utilize and manage standard bookkeeping software and computers, such as:
  - PC Computers, preferably on a IBM ThinkPad 600 with a Linux operating system
  - MyBooks – http://www.appgen.com/products/mybooks_instructions.html - a Linux-based bookkeeping program
  - OpenOffice.org Suite – http://www.openoffice.org/
    - Calc – Spreadsheet application
    - Draw – A graphic drawing program
    - Impress – A presentation program
    - Math – A function and formula creation program
    - Writer – A word processing program
    - Project Management – A project planning program
  - Standard computer email, calendaring, internet, and web proficiency
- Able to communicate appropriately with the WTB Board of Directors & officers, attorneys, accountants, and other various outside professionals
  - Support accounting oriented functions for the Executive & Accounting Directors
  - Filing and maintenance of ledgers and accounting files
  - Security Policy adherence
  - Record, type and distribute minutes of quarterly board meetings; assist in creation of formatted newsletters
  - Order and maintain office supplies
  - Answer phones and respond to email
  - Prepare year-end tax reporting information for accountants
  - Filing and file maintenance of all accounting documents (deposits, paid invoices, bank statements, investment statements, payroll journals, payroll taxes, interim and permanent financial, budget and audit reports)

Laptop Basic Software

Our IBM laptop once built, will require certain software to be able to accomplish the big list of roles and responsibilities of our WTB, so here are the names and details of the software that will be installed and used once the system is built and secured:

- MyBooks – http://www.appgen.com/products/mybooks_instructions.html
  - A financial management software program
  - Current Cost: $99.99
  - Client and Server installations are available, in this project it was determined that the single server download would suffice.
- OpenOffice.org Suite 1.0 – http://www.openoffice.org/ This is an open source software package that comes with the Red Hat installation disks
  - Calc – Spreadsheet application
  - Draw – A graphic drawing program
  - Impress – A presentation program
  - Math – A function and formula creation program

17

- o Writer – A word processing program
- o Project Management – A project planning program
- Ximian[12] Evolution 1.08 Email and Calendaring program

- Mozilla[13] 1.01 Internet Browser

- Tripwire[14] 2.3.1-14 for Linux. This is a file integrity checker that we will use to make sure our files do not change without being initiated by the appropriate administrator.

- RAV AntiVirus Desktop for Linux v8[15] an antivirus program designed for Linux.

- GnuPG version 1.0.7-6 a secure communication tool[16]. Its strengths are the ability to sign documents or email for non-repudiation as well as encrypt and decrypt data. For further information on this technology, please refer to GnuPG in the Appendix.

- Snort RPM or Red Hat Package Manager (RPM) version 1.9.1-1 a host intrusion detection system from http://www.snort.org.

---

[12] http://www.ximian.com/

[13] http://www.mozilla.org

[14] http://www.tripwire.org/

[15] http://www.ravantivirus.com/index.php

[16] http://www.gnupg.org/gph/en/manual.html#CONCEPTS

Infrastructure Design
The infrastructure where we will be landing our workstation is a design that was developed with a "Defense in Depth" approach. In order for our workstation to have a chance of being protected, we need it to land on a secure network. Basically, "Defense in Depth" designs are a layered approach to security. Each layer of security incorporates measures or controls that are an addition to the previous security measures or controls such that the failure of one of these controls does not constitute the failure of all controls. This method is discussed and exemplified in several information security books, which have been included in the "References" section of this practical. To get a grasp of our approach, Figure 3 shows the basic infrastructure design, which can be expanded to include other servers and systems as needed. The design is used with the premise that all network traffic is handled in a way that delivers maximum use with minimal exposure through compartmentalization.
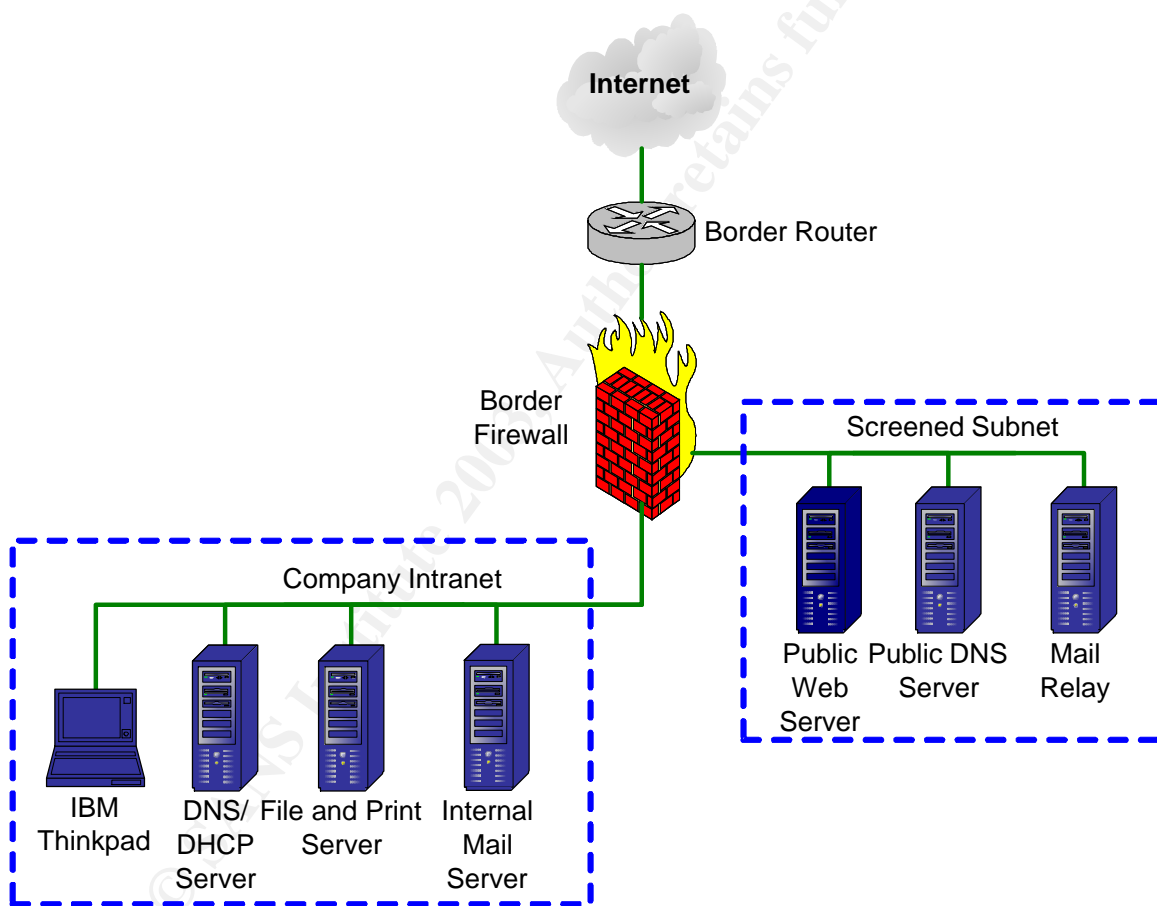

Figure 3 Basic Infrastructure Design

19

Risk Analysis

Risk analysis can be done using two primary methods. One is quantitative and the other is qualitative. Quantitative risk analysis assigns a value to all assets (people, information, legal documents, personal data, buildings, etc., sometimes referred to as a company's "Crown Jewels") and uses the asset value with threat strength and vulnerability values to determine overall risk. This is a very difficult way to analyze risk and generally not used as it is costly and time-consuming. Qualitative risk analysis relies on a trained individual, third party, or committee to be familiar with the company to gather information about assets and analyze this data to determine a company's risk. Qualitative is very dependent on the person or group's expertise relative to the environment being assessed. In this project, risk analysis will use a combination of these two methods coupled with an Overall Risk formula and scenario/asset analysis that delivers an overall risk score that is equated to a specific total risk term. Those terms are Low, Moderate, or High (remember the discussion back in Security 101?).

Any security measures or controls that are introduced will be done so with the knowledge that the initial overall risk analysis of the TP600 is either a Moderate or a High level and must be adjusted to a Low level. Overall, Low risk is acceptable to WTB management.

So, how is this done? Overall risk will be determined with qualitative decisions, related to a scenario that identifies point levels associated with Threats, Vulnerabilities, and consequences. Hidden in the qualitative side are deep discussions of things like, do we have that component installed or is that worm relevant to our build? These points are then plugged into a mathematical formula that is the multiple of threats (1-3 possible points, 1 being the lowest chance of threat and 3 being the highest chance of threat) x vulnerabilities (1-3 possible points) x consequences (1-3 possible points). If decimals are used when calculating the variables and overall risk, normal rounding of answers should take place. To evaluate the final score, the following ranges apply to the overall risk totals:

Total	Overall Risk
0 – 8	**Low**
9 – 17	**Moderate**
18 – 27	**High**

Let's try this method against a would-be scenario, and then we will apply it to our out-of-the-box RH8.0 build and determine if further controls are warranted as we proceed through the build process. Scenario: A security alert is issued when a hacker has created an exploit that attacks RH Linux 8.0 and has released this exploit into the wild. Our systems run on Linux, so the perception is that there is a High risk that we may be exploited. Nevertheless, to make sure, let us write up this scenario using our formula:

Threat – An identified hacker has created a worm to take advantage of a Sendmail vulnerability in RH8.0 – High **(3)**

Vulnerability – WTB has RH8.0 and the correct version of Sendmail, although some countermeasures are in place that prevents most introductions of viruses or worms into our environment – Moderate **(2)**

Consequence – WTB stands to lose availability and sensitive data if the worm successfully exploits any internal systems **(3)**

Overall Risk = Threat x Vulnerability x Consequence = 3 x 2 x 3 = 18 = High

Now let's try this process on the system as it is delivered out of the Red Hat box.

Scenario: We have just purchased Red Hat Linux 8.0, which has been out for a period of time, and are concerned about vulnerabilities, threats or chances of malicious software attacks that disclose sensitive data (Confidentiality), evil doers that might block our Internet access (Availability), or unanticipated accidents such as writing over a patented bookkeeping formula (Integrity) that could cause WTB serious financial impact. Now we have the scenario, let us determine the individual values as we did in the first scenario.

Threat – Hackers have created exploits that are capable of attacking several packages on Red Hat 8.0 – High **(3)**

Vulnerability – WTB' initial RH8.0 installation is susceptible to any of these exploits as there have been no security patches applied yet. However, some countermeasures at or near our border firewall prevent known attacks, viruses, or worms from entering into our environment. This is accomplished with a Network Intrusion Detection device – Moderate **(2)**

Consequence – WTB stands to lose availability and sensitive data if the worm successfully exploits any internal systems **(3)**

Overall Risk = Threat x Vulnerability x Consequence = 3 x 2 x 3 = 18 = High

Well, that's not good. The overall risk of RH8.0 out of the box is high and according to our policy and management, we need to place controls or countermeasures on the system to reduce our overall values to an acceptable Low. The following components will be added to reduce our overall risk to a Low Level and keep it there:

- Perform the installation on a secure isolated network,

- Install current Red Hat 8.0 security alert, bug fixes, and dependency errata,[18]

---

[18] http://www.redhat.com/apps/support/errata/

21

- Remove unneeded services and packages,

- Install and activate tools that will verify file integrity, allow for non-repudiation[19] inbound and outbound data transfer encryption and decryption,

- Set the system security controls, such as host firewalls to a level that denies all but necessary data transmission to our WTB future laptop,

- Establish regular security patch update process,

- Establish system and user backups, and

- Scan the system for vulnerabilities and identify a regular vulnerability assessment process to maintain an overall acceptable level of risk.

With these measures in place and a policy that covers the human factor of security, our administrators are quite certain that we will have a reasonably proactive and reactive plan to address most security incidents or risks. Now on to the installation!

---

[19] Non-repudiation is the process of identifying that any data transmission is from the actual person who sent the data originally and nobody is impersonating them.

Step-by-Step Guide

Now, to follow habit 3 of Stephen Covey, let's "Put First Things First"[20]

Acquire Trustworthy Installation Media (Is it safe?)
You will need a trustworthy version of the Red Hat Linux 8.0 installation CDROMs (Compact Disk (CD) Read Only Memory distribution medium).

Retail Purchase (The safest)
Personally, I felt the best way to acquire a secure installation package was to go down to my local computer store and buy it right off the shelf. I was raised with the thought that it is safer to go to the source then take chances with product vendor wannabes. You can also get it online from a company like Amazon[21] for approximately $30. It will take about 5-9 business days if you order online to receive a set of original equipment manufacture (OEM) CDs.

Download the Files You Need (Trust, but verify)
However, if you're strapped for funds, you can download it from the Red Hat website
 http://www.redhat.com/apps/download/ and there is no direct cost to you. This link is subject to change, especially, if you are reading this and a Red Hat version greater than 8.0 exists or just plain disappeared when you read this document. Please take the time to follow the directions as laid out by Red Hat[22]. In addition, as a hint, it is a lot easier if you download the ISO files and burn them to a CD for the Intel platform build. Support from the vendor is not free, although if you purchased the OEM disks, you will receive 30 days Web-based installation support and 30 days Red Hat Network Basic Service. For the free download, you are allowed one entitlement (speaking of changes, this is now known as demo use, it changed while I was writing this paper) and can receive access to this demo entitlement by creating an account at https://rhn.redhat.com. This account can help you in keeping current on patch updates using an automated patch update program called "up2date" (this program has its pros and cons), a must in security.

> Note: Whether you download your Red Hat media or use the OEM CDs for the system installation, a separate secure computer with a CD burner and a high-speed broadband connection is required (I used a DSL Line and was able to download what I needed in a reasonable time). This secure computer will act as a data integrity verification center (more of this in the next section on verifying files) for any files that are to be used in the secure build process, e.g. security and bug fixes that have been identified post OS creation. The entire build is best performed from a physically and logically isolated network. An alternative to having a CD burner would be to have compatible peripherals such as tape drives on your trusted download server and the workstation that you intend to build.

---

[20] Covey, Stephen R. 7 Habits of Highly Effective People. New York: Simon & Schuster, 1990

[21] http://www.amazon.com/exec/obidos/tg/detail/-/B00006LS9B/103-3872044-0595011

[22] http://www.redhat.com/download/howto_download.html

Download Errata (Nothings perfect!)

Like any of today's software, program code can be millions of lines and with time-to-market being the key driver for most companies. If the expectation is to reap any profits, there are bound to be some issues that are identified after the release of this software.

Red Hat, just like most major companies offers a way to check to see if issues have been identified and a couple of ways to fix these issues. The first is their Errata page, https://rhn.redhat.com/errata/rh8-errata.html, where we will download the current Security and Bugfixes to try and make the laptop secure against these known problems. With your secure server, download all the current Security and Bugfixes and burn them to a CD that will be used later in the Step-by-Step process. Use the information in the next section called Verify the Downloaded Files Integrity, to verify the MD5 sums. As added protection, the RPM installation will also make sure that the files are correct via an RPM key validation process, which will be covered later in this paper.

Here is a view of the headings you should see on the Errata site:

Red Hat Linux 8.0 (Psyche)
security alerts, bugfixes, enhancements

24

Verify the Downloaded Files Integrity (Who knows what Evil lurks)

You never know where evil doers will strike next and even with a great group like Red Hat, the possibility exists that their security could be circumvented and a Trojan[23] placed in their OS software. Therefore, if you cannot get the OEM disks due to a shortage of funds, you're just pinching pennies, or you're trying to enhance your security, you will want to verify that the files you download are the files that Red Hat intended for you to use and not those of a wily hacker. The trick to performing this verification is via two commands, "gpg" *and* "md5sum[24]". The "gpg" command is for verifying signed and encrypted files (it also has other capabilities like encryption and decryption) and the "md5sum" command is for checking a message digest of a specific file in order to verify integrity. You can find out information that is more detailed in your manual page, the Gnu[25] Privacy Guard (GPG) website[26], or the Red Hat installation documentation[27]. If you look up the "md5sum" command in the online manual (man) pages, the command is described as a command that "computes and checks MD5 message digest values.

Figure 4 is a screen shot of five "psyche" ISO files and one file titled MD5SUM at Red Hat's File Transfer Protocol (FTP) site[28]: These are the files that once verified; you will burn to a set of CDs in order to install Red Hat Linux 8.0 on your IBM laptop.

---
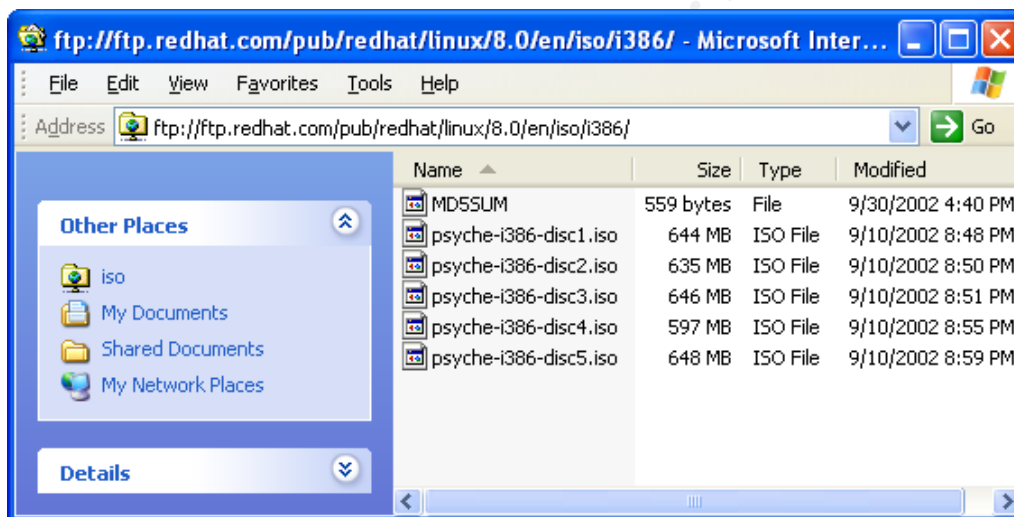
[23] Dan Edwards. Trojan. 1995 http://kldp.org/~eunjea/jargon/?idx=Trojan-horse

[24] Md5sum use - http://www.scrounge.org/linux/md5sums.html

[25] http://www.gnu.org/

[26] http://www.gnupg.org/

[27] http://www.redhat.com/docs/manuals/linux/

[28] ftp://ftp.redhat.com/pub/redhat/linux/8.0/en/iso/i386/ or http://www.redhat.com/download/mirror.html if the FTP site is experiencing high volume requests and unavailable.

25

Figure 4 Screen Shot of ISO files

This MD5SUM file is a text file that has all the "md5sum" values for the "psyche" ISO files signed with a Gnu[29] Privacy Guard (GPG) key. In order to verify the signature of this file or RPM package, you must have acquired, installed, and verified the fingerprint[30] of the signer's public key from a source such as the Red Hat site[31]. In this case, the signer, if legitimate, is Red Hat.

Note: Required actions, commands, which are case sensitive, or screen output are colored medium blue or are surrounded by a screen-simulated background. For ease of use, the command line prompts, e.g. [user@hostname user]$ or ['root'@hostname 'root']# are in **dark blue** and have been abbreviated as $ and #, respectively. The # identifies that you are logged in as a user with 'root' privileges and the $ is for a less-privileged user. Any variables, such as file names, are *italicized*, and the process of pressing the enter key to initiate the command, if required, is assumed to take place after you have finished typing in the complete command or is identified by the text <enter> following the command line symbols $ or #.

Creating a GPG Keys (You Need Protection)
The next set of commands will be used to import the Red Hat and RPM public GPG keys to your secure server's keyring and set up GPG on your Laptop. GPG is a tool for verifying the integrity of files and email along with the ability to encrypt or decrypt information of another GPG user you have shared public keys with. The use of GPG will increase security and reduce risk since you will be able to verify that files you use haven't changed, verify signatures of incoming GPG signed documents, create authentic documents that can be verified when you sign them with GPG, and encrypt or decrypt local or shared sensitive information. Of course, you will need to import public keys of trusted entities in order for this to work. The following is the process to create a GPG key pair[32] if you have never created one on Linux (perform this with your user account):

$ gpg - -gen-key

Output will talk about No Warranty (don't worry, most of the Linux world use it!) and output the following:

gpg: /'root'/.gnupg: directory created
gpg: /'root'/.gnupg/options: new options file created
gpg: you have to start GnuPG again, so it can read the new options file

Re-enter the key generation command.

---

[29] http://www.gnu.org/

[30] pgp.mit.edu

[31] http://www.redhat.com/solutions/security/news/publickey/

[32] Key pair – A public and private key used to perform asymmetric cryptography functions. Cryptography defined:
http://www.rsasecurity.com/rsalabs/faq/1-2.html

$ gpg - -gen-key

You will see the following screen (If you see an "insecure memory!" error, don't worry as this is because a regular user cannot lock memory. Re-enter the previous command if it fails, otherwise, just continue):

```
gpg (GnuPG) 1.0.7; Copyright (C) 2002 Free Software Foundation, Inc.
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions. See the file COPYING for details.

Please select what kind of key you want:
   (1) DSA and ElGamal (default)
   (2) DSA (sign only)
   (4) ElGamal (sign and encrypt)
   (5) RSA (sign only)
Your selection?
```

$ <enter>

Next, choose your key size; the default of 1024 should be fine:

Your selection? <enter>

Next, you will be asked, "Key is valid for? (0). This is acceptable; this selection tells the system that you do not intend to change your key. If you do, you will have to update this information with anyone you have shared your public key with in the past, but for now just select the default of (0).

Key is valid for? (0) <enter>

Next, you will see, choose "y" to validate your choice:

Key does not expire at all
Is this correct (y/n)? y

Next, you will be required to input the information you would like associated with your public key, fill this in accordingly:

Real name: Your name

Email address: my_red_hat_email@mydomain.com

Comment: Red Hat Newbie

After you enter your comment, your information will be displayed for final review.   If everything is fine, enter the letter "O" for okay and continue.

27

You selected this USER-ID:
    "Your name (Red Hat Newbie) <my_red_hat_email@mydomain.com>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O

You will be prompted for a Passphrase, this is like a password for your GPG keys, so choose it wisely and make it hard to guess for the bad person but something you will remember and not need to write down. Just like your regular password, it should contain alphanumeric and special characters to reduce the chance that it could be intercepted and cracked.

You need a Passphrase to protect your secret key.

Enter passphrase: FollowY0r$tr@ngPazzwdMeThodHere

Repeat passphrase: FollowY0r$tr@ngPazzwdMeThodHere

You will see the following screen where you will want to move your mouse around the screen to help the program generate random numbers that help create the prime for your keys. If you would like to read more about creating primes, see the documentation on cryptography supplied by RSA at:
http://www.rsasecurity.com/solutions/developers/whitepapers/IntroToCrypto.pdf.

We need to generate a lot of random bytes. It is a good idea to perform some other action (type on the keyboard, move the mouse, utilize the disks) during the prime generation; this gives the random number generator a better chance to gain enough entropy.

+++++.+++++.++++++++....++++++++++..+++++.+++++.+++++++.++++++++++.+++++++++++++++++++
+++++++++++++++++++........................++++

When done you will see output like below (your results will be different as the information here has been manipulated for example and keep the bad guys away from the authors private key) ☺:

gpg: /home/userdir/.gnupg/trustdb.gpg: trustdb created
public and secret key created and signed.
key marked as ultimately trusted.

pub 1024D/8A907747 2003-03-18 Your Name (Red Hat Newbie)
<my_red_hat_email@mydomain.com>
**   Key fingerprint = B48C 1100 F2E4 401F 8487 F3C1 F199 8B92 7754s**
sub 1024j/B2B4A623 2003-3-18

Remember this work should be taking place on a system that is already secured and has a CDROM burner that will be used to transport the ISO's and Security Errata to your new

© SANS Institute 2003,   As part of GIAC practical repository.   Author retains full rights.

laptop that will be built off the network. Also, if you downloaded the public keys from a site other than the Red Hat site, substitute the path where the GPG public keys currently reside. This information is also in the Red Hat documentation for referral[33]:

Importing Public Keys (I know You, You Know Me!)
In order to make Gnu Privacy work, you will have to import and export public keys if you expect to use the tool to its fullest. For this project, the Red Hat public key is needed to verify integrity of files that are acquired from Red Hat for updates, so this next section is dedicated to helping import these keys as needed.

Let's begin with the Red Hat RPM GPG public key.

As the 'root' user, use these commands to import the RPM GPG public key, which can be used to verify the integrity of RPMs. However if you use the RPM install command this will automatically happen:

Insert Red Hat 8.0 installation Disk 1 of 3.

mount /dev/cdrom

rpm - -import /mnt/cdrom/*RPM-GPG-KEY*

Enter this command to import a text file (mount the appropriate device that has the key text file store on it, in this case a floppy drive was used) that contains a verified Red Hat GPG public key[34]:

mount /dev/fd0

gpg - -import /mnt/floppy/*redhatgpgpublic.txt*

Enter the following command to list all public GnuPG keys installed.

gpg - -list-keys

You should see the following output:

/'root'/.gnupg/pubring.gpg
----
pub 1024D/DB42A60E 199-09-23 Red Hat Inc. <security@redhat.com>
sub 2048g/961630A2 199-09-23

Enter this command to verify the signer of the MD5SUM text file:

---

[33] http://www.redhat.com/docs/manuals/linux/

[34] http://www.redhat.com/solutions/security/news/publickey/#key and
http://www.redhat.com/solutions/security/news/publickey/key for verification directions.

gpg - -verify *MD5SUM*

Enter this command to verify the signer of an RPM package:

rpm - -checksig –v *<filename>.rpm*

You should receive output that verifies the file as a "Good signature from "Red Hat, Inc security@redhat.com"" and a Fingerprint: of: CA20 8686 2BD6 9DFC 65F6 ECC4 2191 80CD DB42 A60E which should match the Fingerprint located at the MIT website that was previously footnoted or "OK" for all components of the RPM. If not, there is a problem and you should download your data from a more reliable site and repeat the verification process. There are many more commands that can be used with GnuPG and a trip to the website that houses their handbook is a must, if you expect to use the tool to its fullest - http://www.gnupg.org/gph/en/manual.html#AEN335

The now verified MD5SUM text file looks like this when opened with the VI editor[35] (the characters highlighted in blue are the message digest characters that must match the MD5 digest output from our "md5sum" command that was run against the psyche files):

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

d7b16b081c20708dc0dd7d41793a4177  psyche-i386-disc1.iso
2df17bc02cb1b3316930ed4f7601ad9e   psyche-i386-disc2.iso
305d6ff5b5850fa316276710a148b0a3    psyche-i386-disc3.iso
0a77d7a3bc8c4e87508c46a2670242eb psyche-i386-disc4.iso
8dbcf16f0072ee47db49b08921a41ba5   psyche-i386-disc5.iso
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.0.6 (GNU/Linux)
Comment: For info see http://www.gnupg.org

iD8DBQE9mH6DIZGAzdtCpg4RAkKnAJ9FoKBr0tTIakp9XEn+3+jEWkES2QCfbVBo
OFisZU8vsf6HHUpUivNv39I=
=J1G1
-----END PGP SIGNATURE-----
```

To determine the integrity of the psyche files, the "md5sum" command checks the file by feeding the ISO, or a file that you wish to verify, into an algorithm that then creates 128-bit "fingerprint" or "message digest."[36] If the output matches the value in your signed MD5SUM file, your file is more than likely the original file intended for your secure use.

Enter following command to receive a message digest output for the install ISO file labeled psyche-i386-disc1.iso:

md5sum *psyche-i386-disc1.iso*

After a few seconds, you should see the following output:

---

[35] A crash course in using the VI editor - http://startlinux.co.nz/articles/article_74.php

[36] The MD5 Message-Digest Algorithm, http://www.ietf.org/rfc/rfc1321.txt, April 1992

d7b16b081c20708dc0dd7d41793a4177   psyche-i386-disc1.iso

Repeat this process for the other four psyche files to verify their integrity via the message digest. Once verified, you are ready to burn these to five CDs and use them for the install.

Again, if the output does not match, your files are Memorex (in other words – they are fake!) and you should seek a new reliable source for your ISO downloads that will be used to install Linux.

Verify Downloaded Errata (Caveat emptor)
Now that you have installed your public keys, you can verify your previously downloaded Errata. On the secure server, run the following commands:

 # rpm --checksig -v *.rpm > /home/userdir/OK.out

grep –v OK OK.out|more

This will show all file names and any signature verification failures. If all RPMs are correctly signed, you will only receive a list of the RPMs that you expect to run the freshen command against.   If there are any unacceptable RPMs, it will display an error and you should disregard that file and download a new safe version.

Install Off the Network (Paranoia is good!)
It literally takes seconds to minutes for a system to be compromised when connecting to a network that has Internet access and unrealized malicious activity. In fact, during this installation it is highly recommended that you have a specific isolated network designed to assemble, build, and test your systems prior to delivering the end product to any WTB. Ideally, the area will be in an access-controlled room or lab. This will help maintain the integrity of your build from start to finish and protect against premature connection to your final destination network. If you intend to use the Kickstart capability of Linux, make sure you take appropriate steps to harden any systems that are involved in this type of process[37]. Experience has shown that even in a controlled environment, traffic is not limited to one person and, if you are performing an unattended or scripted install, an 81/2" by 11" piece of paper that reads "Build in Progress – Do Not touch and your contact information" helps prevent time lost due to uninformed lab partners. For installations that require a greater level of protection, it is recommended that, you secure your environment according to recognized organization guidelines like those offered at the National Institute of Standards and Technology (NIST) Computer Security Division (CSD)[38] or British Standards Institute (BSi).[39] There is a charge by some affiliations for their documentation, so if you are limited in

---

[37] http://www.redhat.com/docs/manuals/linux/RHL-8.0-Manual/custom-guide/ch-kickstart2.html

[38] http://csrc.nist.gov/index.html

[39] http://emea.bsi-global.com/InformationSecurity/Overview/index.xalter

31

funds start with NIST or the SANS Reading Room.[40] Again, note that we are striving to build a system for bookkeepers. The expectations are that an extra level of diligence is required to protect material that is sometimes sensitive in nature. Therefore, from time to time, you will see that this guide goes the extra mile to address the infamous security triad of Confidentiality, Integrity, and Availability (CIA), not to be confused with the Culinary Institute of America[41] or any other agency that might be trying to protect important recipes. ☺

Release Notes (Last minute details from the makers of RH 8.0)

Now, you have the fundamental components for installation of RH 8.0 and an isolated network for your IBM laptop to sit on after all precautionary securing measures has been taken. There is a tidbit of valuable information that you will want to read if the folks at Red Hat found any issues with the build process after they had already created the installation files and placed them on the download website. This tidbit is the release notes,[42] which will address anything from partitioning to alternative install techniques, like "Kickstart"

Wise Decisions (Little things help)

The design of our system is geared to the thought that less is more, in other words, fewer system components and applications installed, generally implies less overall risk of future undetermined vulnerabilities being exploited. In other words, if you do not have a CDROM burner on your laptop, why install a program that is designed to burn CDROMs and if an exploit is created for the CDROM burner program, you will not have to worry if it isn't installed, right? As an added benefit, less system components generally enhance speed and stability of a system and when we need to perform ongoing maintenance such as file upgrades, the task will be less demanding as there will be fewer files. In addition, for added security and stability, we will try to keep the system files separated from the bookkeeper files. This will be done in two ways. One is that any files that are kept on the laptop will have separate system and user partitions. The other is that all other business related files will be stored on a secure file server on the intranet, using SSH[43] and scp[44], so that the files can be backed up every night. In addition, the files are available for other bookkeepers to share on a "Need to Know" basis. This should also reduce the risk that the

---

[40] http://www.sans.org/rr/

[41] http://www.ciachef.edu/

[42] http://www.redhat.com/docs/manuals/linux/RHL-8.0-Manual/pdf/rhl-relnotes-x86-en-80.pdf

[43] Secure Shell, see Appendix for SSH use.

[44] Secure Copy, see Appendix under SSH.

32

system could be crashed if a users program got out of control and filled any of the file systems. The SANS Reading Room has many examples of secure server installation instructions at http://www.giac.org/GCUX.php, if you need to set up a secure file server or such.

Now on to our secure build!

B O O T

📕 **Boot:** To 'boot' a computer is to start the operating system. A boot can be a "hard boot" or a "soft boot". A restart may be to the lowest level of the CPU's control program (BIOS[45]), or slightly higher, depending on whether it is a hard or soft boot and the design of the computer system. In any case, the "operating system" is restarted from the beginning. http://slencyclopedia.berlios.de/jargon.html

---

Boot to CD 1 of 3 (Here We Go!)
Place the Red Hat Linux 8.0 Installation CD 1 of 3 into your compact disk (CD) tray of your non-networked laptop.

Most of the time, you will need to power on the system in order to eject the CD drive and insert disk 1 0f 3. The CD drive must be the first device that your system accesses during the boot cycle (see overhead bar on Boot). If your laptop does not boot to the CD, it is possible you will have to edit your boot configuration. To get to this menu, you must hold down the "F1" function key of your laptop during the boot cycle when you see the blue **IBM** symbol. You will be presented with a menu that allows you to choose the boot device priority of your laptop. Set this to CD, Floppy, and Hard drive. This is under the "Start up" area; see Figure 5.

---

[45] Basic Input Output System – The initial chip that is accessed for your system hardware start up.

© SANS Institute 2003,   As part of GIAC practical repository.   Author retains full rights.
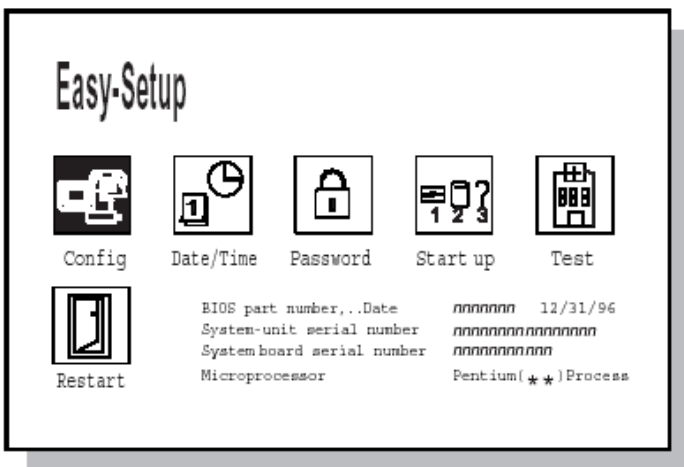
Figure 5 5 IBM BIOS Easy-Setup

This is also a good time to set your BIOS password, under the "Password" area of the original "Easy-Setup" screen. This is all detailed in the IBM User Reference guide link that is captured in the Appendix. Once all BIOS passwords and CD are in place, power off your system and power it on again.

Begin the Graphical Install (Seeing is believing!)
You will now be given this beautiful blue screen header with the Red Hat logo.
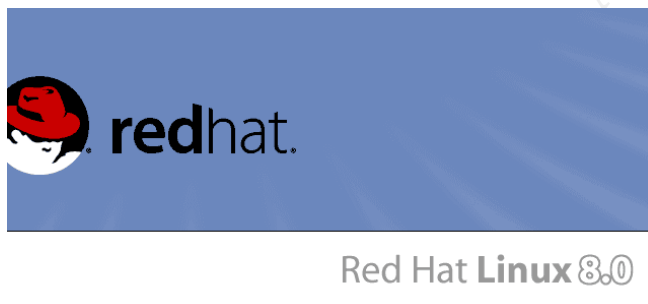
Press the enter key, to begin the graphical mode installation.

After a series of hardware identification and file decompression text lines scroll by, you will be presented with the "**Welcome to Red Hat Linux**" screen where the Next button is pre-selected.

Press the enter key or click the mouse pointer on the Next button to continue.

The next window displays the default language of "English (English)." This step-by-step is for the English version.

34

Press the enter key or click the mouse pointer on the Next button to continue.

The next window is the Keyboard selection where the default is U.S. English.
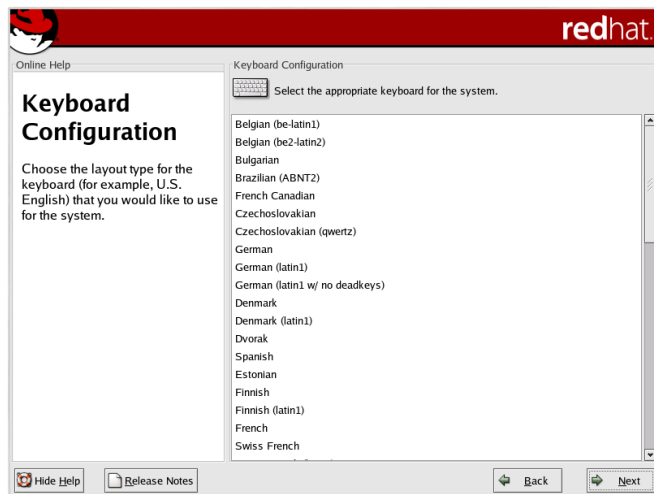
If this is appropriate for your system, press the enter key or click the mouse pointer on the Next button to continue.

Next is the "Mouse Configuration" window, the default selection should be fine.
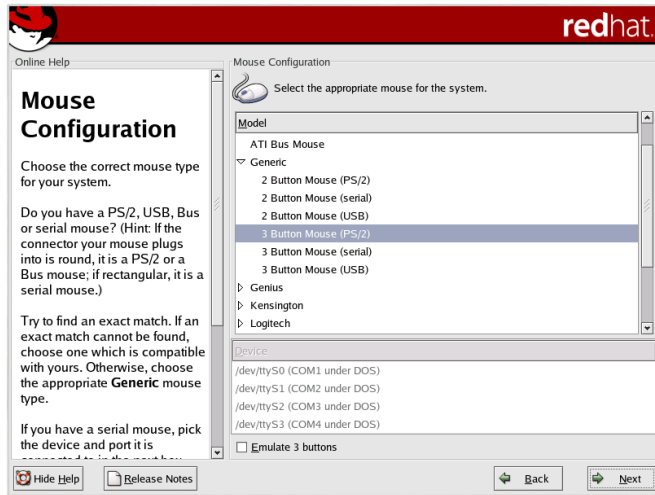
Press the enter key or click the mouse pointer on the <u>N</u>ext button to continue.

For Installation type,
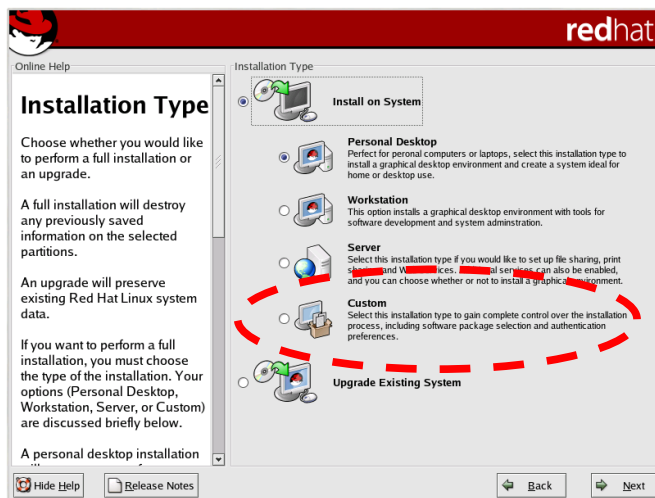
Click on the "Custom" radio button, tab to the <u>N</u>ext button and press the enter key, or click the mouse pointer on the <u>N</u>ext button to continue.

36

This next screen is where we introduce our first security measures for the hard drive via partitioning:
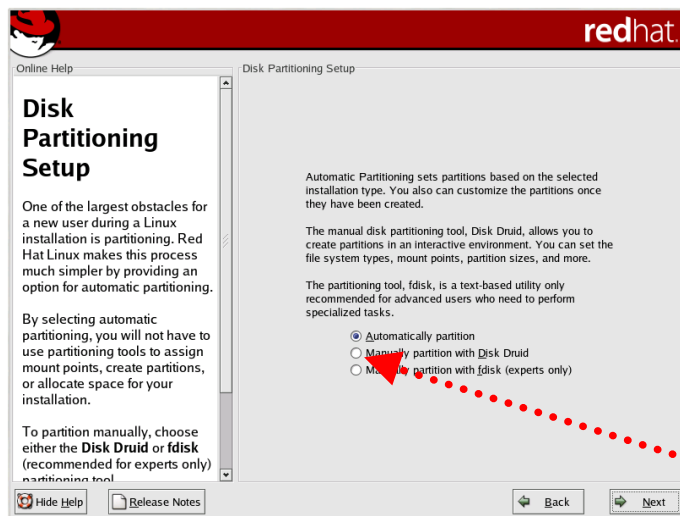
Click on the "Manually partition with Disk Druid" radio button, tab to the Next button and press the enter key, or click the mouse pointer on the Next button to continue.

For this installation, we will be using the IBM DADA 5.1 GB hard drive. If there are already partitioned areas on your hard drive, delete them; we will be using a custom set of partitions to protect our system from issues that will be explained shortly.

PARTITIONING

 Partitioning: Partitioning is a way to take your physical hard drive and divide it into smaller, more manageable chunks. In our case, this also adds security through separation of system and user data storage areas. Partitions are identified using a partition table (somewhat like a logical address book of where the data is written on the hard drive), which is stored in the boot record at the beginning sectors of the disk.

The following graphic is an example of a partition design:

Disk Setup

Online Help

Choose where you would like Red Hat Linux to be installed.

If you do not know how to partition your system or if you need help with using the manual partitioning tools, refer to the *Red Hat Linux Installation Guide*.

If you used automatic partitioning, you can either accept the current partition settings (click **Next**), or modify the setup using the manual partitioning tool.

If you used **fdisk** to partition, you must define *mount points* for your partitions. Use the **Edit** button, once you have selected

Partitioning

Drive /dev/hda (Geom: 784/255/63) (Model: WDC AC26400B)

| New | Edit | Delete | Reset | RAID | LVM |

| Device | Mount Point/ RAID/Volume | Type | Format | Size (MB) | Start | End |

▽ Hard Drives
 ▽ /dev/hda
   /dev/hda1   /boot   ext3   ✓   102   1   13
   /dev/hda2   /   ext3   ✓   5538   14   719
   /dev/hda3   swap   ✓   510   720   784

☐ Hide RAID device/LVM Volume Group members

Hide Help | Release Notes | Back | Next

In our case, we will delete any partitions that exist, then using the newly identified "Free space"; we will use the edit button to create the following partitions and settings:

Device	Mount Point/ RAID/Volume	Type	Format	Size	Start	End

∇ Hard

∇ /dev/hda1	/boot	ext3	P	103	1	14
/dev/hda2	/	ext3	P	3005	15	421
/dev/hda3	/	swap	P	251	422	455
∇ /dev/hda4		Extended	P	1528	456	662
/dev/hda5	/home	ext3	P	509	456	524
/dev/hda6	/opt	ext3	P	1011	525	661
Free		Free space		7	662	662

Once this task has been completed, tab to the Next button and press the enter key, or click the mouse pointer on the Next button to continue.

This will allow us to use specific partitions, such as, home to store user data, (e.g. working copies of files and their accompanying directories) in an area on the hard drive, other than where the Operating System resides. This method will reduce the risk of a user program entering a runaway mode or endless loop where data fills up the free space on the hardware and then causes the system to halt. If the user's data is segmented away from the system files and it becomes too large, it will not cause a system interruption, just deliver an error that there is no remaining space to preserve data. In addition, a benefit to this type of separation is if a hacker were to circumvent a

user's access, that hacker would be limited to the areas of the hard drive that are only assigned to the user and not 'root'[46].

The next screen allows us to choose if we would like to configure the GRUB (Grand Unified Bootloader) boot loader. GRUB is a feature that allows us to choose from more than one operating system when booting the system. We will not load any systems other than RH 8.0, however; the GRUB boot loader allows for a Boot Loader Password and this will add another level of security to our user's future laptop. In addition, Grub allows kernel access and, with a password in place, there is less chance of kernel commands being issued unless the user has appropriate access via the GRUB password. Whenever faced with the decision of adding extra security, it is best to start with it enabled. If it is later determined that there is a business impact and the risk is justified, the choice may be made to disable it, but only if it is a low or manageable risk and is authorized by the management that is accountable if disabling a security feature causes an incident. More about risk later in the Ongoing Maintenance section.
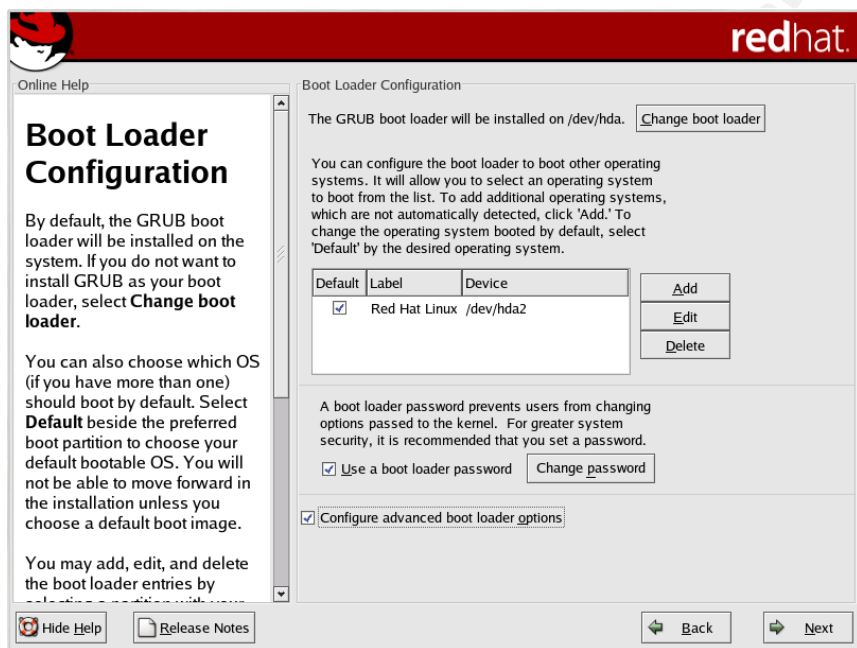
With the mouse pointer, click the "Use a boot loader password" check box.

A window titled "Enter Boot Loader Password" will appear.

Enter the same strong password in both the "Password:" and "Confirm:" fields.

---

[46] The super user of the Linux system or the user account with complete permissions to modify, read, write, and execute anything on the system…. in system administrator lingo, this is "God" on the system.

Generally speaking, a password is one of the first lines of defense. Remember this password and if possible do not write it down. If you must write any passwords down, make sure you store them in a safe place such as a combination safe or a locked cabinet where access is limited to you and one other person, preferably the administrator of your system.

Tab to the OK button and press the enter key, or click the mouse pointer on the OK button to continue.

Now, tab to the Next button and press the enter key, or click the mouse pointer on the Next button to continue.

The next window is the Network Configuration window. Leave it on the default settings, as this system will acquire its information dynamically from our Intranet Dynamic Host Configuration Protocol (DHCP) and Domain Name Services (DNS) server.
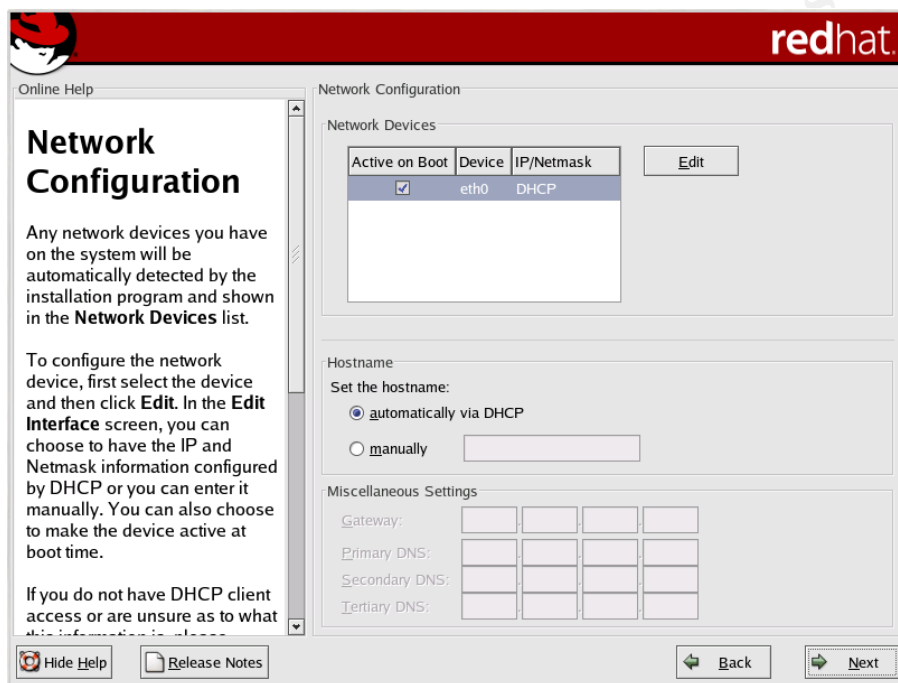
Tab to the Next button and press the enter key, or click the mouse pointer on the Next button to continue.

This window is the firewall configuration window:

Online Help

Firewall Configuration

A firewall sits between your computer and the network, and determines which resources on your computer remote users on the network are able to access. A properly configured firewall can greatly increase the out-of-the-box security of your system.

Choose the appropriate security level for your system.

High Security - By choosing **High Security**, your system will not accept connections that are not explicitly defined by you. By default, only the following connections are allowed:

Hide Help   Release Notes

Firewall Configuration
Select a security level for the system:
○ High   ● Medium   ○ No firewall

○ Use default firewall rules
● Customize

Trusted devices: ☐ eth0

Allow incoming:
☐ WWW (HTTP)
☐ FTP
☐ SSH
☐ DHCP
☐ Mail (SMTP)
☐ Telnet

Other ports:

← Back   → Next

Click on the "High" security level radio button.

By selecting, the "High" firewall security level will only allow DHCP configuration for our network interface and Domain Name Services (DNS) replies.

The settings will deny:

- Active mode FTP (client initiated FTP will work fine),

- Internet Relay Chat (IRC) DCC file transfers,

- Remote X Window System clients (we don't want anyone to use our X server remotely), and

- RealAudio.

In order to reduce the risk of a workstation being used for personal entertainment, our workstations will be stripped of any non-work related software. However, the need to foster a reasonable work life, maintain security, and allow our personnel to have an avenue to reduce stress, policy requires mandatory breaks. A break room is available with a secure computer designed for the employees to check personal email, surf the Internet, and play some PC games during these breaks. There is even a monthly game rotation process, so that they do not get bored with game choices.

Tab to the Next button and press the enter key, or click the mouse pointer on the Next button to continue.

For the "Additional Language Support" screen, make changes as needed and:

41

Press the enter key, or click the mouse pointer on the <u>N</u>ext button to continue.

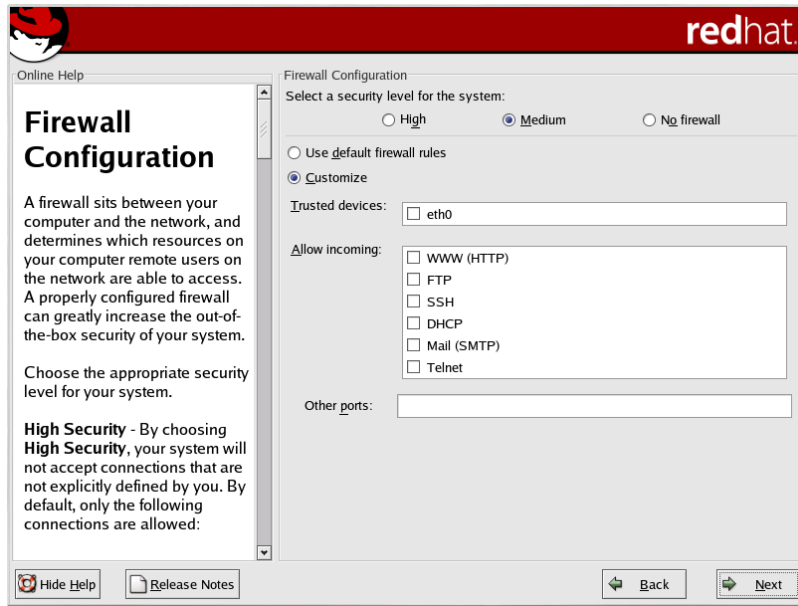For the Time Zone Selection screen,

Select your appropriate location and tab to the <u>N</u>ext button and press the enter key, or click the mouse pointer on the <u>N</u>ext button to continue.

Next is the Account configuration window. This is by far the most important area as far as control of the machine goes. Two accounts will be created here, one for administration, called 'root', and one for normal user functions that are required for a WTB. The account name of 'root' is standard; so for security, it is important that we create a password that is not easily guessed (strong). Being the first line of defense, passwords are generally the first target for hackers, especially the ones that rely on social engineering[47] attack methodologies. These methods could include automated software that use specially created password lists or dictionaries to try various known or common passwords or brute force, which means passwords are guessed with a password-cracking tool using all possible character combinations in a systematic approach that would result in the determination of your password. This usually takes place offline after they have somehow managed to grab your passwords from a network with tools such as sniffers[48]. One way to select a strong password is to use a limerick or a sentence that is easy to recall because of its uniqueness and take the first letter of each word of that sentence, substituting some of the characters with numbers and special characters that are similar (e.g. "@" for an "a") and you now have an easy password to remember. Here is an example: "The brown Fox jumped 0ver the purple fence 1ast @ugust (August). The password might look like this: TbFj0tpf1@. You can see we used the "@" sign to symbolize the "A" of "August", "0" to represent the "o" in over, and the numeral "1" to represent the "l" in last. It takes a little practice and the return is that you don't end up with easily compromised passwords like the bookkeeper's favorite dog or child's name and birth date which are easily guessed with the right amount of socially engineered information or the password is written on a sticky note and taped to the underside of the keyboard because it can't easily be remembered. In addition, if there is a need for the local user to execute a command as the "superuser" ('root' like privileged account) a program called "Sudo[49]" will be available. This program allows specific "superuser" actions if defined in the file /etc/sudoers file. If a privileged command is attempted without "Sudo" privileges, an alert will be sent to the proper authority as defined by the "Sudoers" configuration. This will be covered in detail shortly. Now for the accounts:

Enter a strong "'root' <u>P</u>assword" and tab to the next filed titled "<u>C</u>onfirm" and retype the same password.

---

[47] Social Engineering Definition. http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci531120,00.html

[48] Sniffer, a tool that monitors network traffic. http://whatis.techtarget.com/definition/0,,sid9_gci213016,00.html

[49] Sudo, superuser do, a utility to that provides root like permissions to a regular user.
http://whatis.techtarget.com/definition/0,,sid9_gci214051,00.html

If the password is too short or does not match the first password, you will be alerted to this directly below the "Confirm" field. If the passwords are of proper length and match, you will receive the "'root' password accepted" message and you can now

Tab to the Add button and press the enter key.

Enter a user name for the future workstation user and a system administrator user account (this will be used for initial login if working on the machine, then the admin will "sudo" (see "sudo" help in the Post Installation section) or "su" (switch user) in order to perform 'root' like commands.

Create a temporary seed password that should be changed by the future employee upon receipt.

Tab to the Ok button and press the enter key.

Tab to the Next button and press the enter key, or click the mouse pointer on the Next button to continue.

A window titled "Authentication Configuration" will appear. MD5 passwords allow passwords of up to 256 characters. Shadow passwords provide a secure method of storing your passwords while reducing direct interception by bad people, as they are stored in a separate protected directory than where the user accounts are stored.

Tab to the Next button and press the enter key, or click the mouse pointer on the Next button to continue.

Remove Unneeded Packages (What you don't know, will hurt you!)
At this point, your mouse pointer will change to a small clock icon while the system retrieves package information. Within a few seconds, you will be directed to a window with various package information. In order for the system to be secured properly, it is important not to accept the default package list, but,

Uncheck the "Text-based Internet", "Sound and Video", and the "Graphics", check boxes.

Check the "Select individual packages" check box, tab to the Next button and press the enter key, or click the mouse pointer on the Next button to continue.

You will be directed to an "Individual Package Selection" window. Here is where we get granular with securing our customized install, which will be followed by security alerts, and bug fix updates.

Click on the "Flat View" radio button.

Your mouse pointer will change to an image of a clock while you switch to the "Flat Mode". The right package window will list packages in alphabetical order. The workstation will be

43

designed to perform only word processing, bookkeeper functions via spreadsheets and calculators, along with appropriate presentation tools for meeting reports. Any programs or services that are not directly related to these primary functions, such as program development or games, will be removed. The office generally has piped in cable music so the sound portion of the system will be disabled to eliminate audio distraction from the workstation. If you desire an in-depth understanding of each of the packages and what they can do for you, you must select the package by hovering the mouse pointer over the desired package and click once with your left mouse. The detailed summary will be displayed in the lower window along with the package name and version. If you have the convenience or desire to be educated on the package functions, by all means, please read the summaries, but for now, you will be supplied the following list of unneeded packages (relying on the research that prefaced these decisions by the author), which should be unchecked in order to reduce your overall risk (these choices should increase or decrease depending on your particular program and network needs, so choose wisely when determining your security needs):

Uncheck the box of each these packages e.g. from this R to this £:

£ 4Suite	£ minicom
£ anacron	£ net-snmp
£ at	£ net-snmp-utils
£ attr	£ pilot-link
£ audiofile	£ qt
£ bind-utils	£ rdate
£ finger	£ rdist
£ fortune-mod	£ rpm-404-python
£ gaim	£ rsh
£ gnome-audio	£ rsync
£ gnome-media	£ sox
£ gnome-pilot	£ talk
£ irda-utils	£ wireless-tools
£ isdn4k-utils	£ wvdial
£ lftp	£ xchat
£ lha	£ xisdnload
£ libvorbis	£ ypbind
£ lrzsz	£ yptools

Install Needed Red Hat Packages
Install Tripwire an integrity-checking package.

From the same screen as above, check the box of the Tripwire package (e.g. from this £ to this R) that will increase our ability to assure file integrity:

44

R tripwire – A program to check file integrity. In other words, a program takes a snapshot when you have a secure system and then notifies the administrator if any files have changed since that snapshot.

Tab to the Next button and press the enter key, or click the mouse pointer on the Next button to continue.

Checking dependencies in packages will be displayed and then you will be directed to the Unresolved Dependencies window. Determine if you must make changes or select the "Install the packages that are necessary to satisfy dependencies" radio button, if you agree with the dependencies.

Tab to the Next button and press the enter key, or click the mouse pointer on the Next button to continue.

The "About to Install" window will appear and if you believe you have made all the correct choices,

Tab to the Next button and press the enter key, or click the mouse pointer on the Next button to continue.

A "kickstart" file that can be used for future duplicate builds will be stored in the /'root' directory and entitled anaconda-ks.cfg. Save this in a directory that will be safe from change.

The Installing Packages window will appear and you are on your way to installing the basic system.

Depending on your system, after about 20 minutes, you will be prompted to remove disk 1, insert disk 2, and click the mouse on the OK button to continue installing.

After about 10 more minutes, you will be prompted to remove disk 2, insert disk 3, and click the mouse on the OK button to continue installing.

When disk 3 is complete, you will be prompted to create a boot disk.

The "Yes" radio button is selected by default,

Tab to the Next button and press the enter key, or click the mouse pointer on the Next button to continue. The "Insert a floppy disk" window will appear, click on "Make boot disk".

Once you have completed the creation of your boot disk, a Graphical Interface (X) Configuration window will appear.

Tab to the Next button and press the enter key, or click the mouse pointer on the Next button to continue. Repeat this for the Monitor Configuration window.

45

Click the "Test Setting" button and if all looks correct, click the Yes button, return to the "Customize Graphics Configuration" window, and click the mouse pointer on the Next button to continue. The basic install is now complete, click on the Exit button and the system will now reboot.

Post Installation Risk Reduction

Note: At this point in time, you have made several decisions on your build. There is still a good list of the things that will be added, removed, or modified to make your system secure and reduce risk. A helpful idea for a system administrator is to keep hard copy information or a diary of these changes. A binder labeled with the type of system that you maintain is one way to accomplish this. This will reduce your stress if the system has to be rebuilt and software files of your changes are not available. Update it as you make changes that affect the overall environment or security of your laptop.

Change Boot Priority to the Primary Hard Drive
Use the EZ-setup process described in the Boot to CD 1 of 3 (Here we go!) section to change your boot process to only boot from your primary drive, hd1 (or C:). This will protect your system from someone who has physical access and could boot with a floppy or CD and compromise or disable your laptop.

Customize Date, Time, Update Agent, and NTP
Upon reboot, the system will need to have basic configurations, like Date and Time, Update Agent, Network Time Protocol (NTP) server, and additional CD's information entered. This should match your network needs. In our case, I have added the appropriate information including the NTP server name that will synchronize all our systems. This will be very important if we suffer a break-in, as time correlation is very important for computer incident forensics.

Protect Against the "Three Finger Salute" (Control + Alt + Delete)
One protective measure that is a must and works in parallel with your boot to primary hard drive only change is the "Three Finger Salute" or pressing the Control + Alt + Delete keys capability removal. If available, this would allow would-be hackers with physical access the ability to reboot the laptop at a whim.   To disable this unwanted security vulnerability, perform the following as 'root' from a command line:

Change directories to /etc and make a copy of the inittab file. It is good practice to make a copy of any file before you make changes in case a mistake is made and you need to return to the original configuration.

cd /etc

cp inittab inittab.orig

vi inittab

In the # Trap CTRL-ALT-DELETE section, add a remark symbol (**#**) to the front of the "ca::ctrlaltdel:/sbin/sutdown –t3 –r now line". The result will look like this: #ca::ctrlaltdel:/sbin/sutdown –t3 –r now

Save the change by pressing the escape key once, hold down the shift key and press the ":" key. Enter wq to save and exit and your change is done.

Generate Your GPG Keys (I am the Key Master)
You will now set up your GnuPG public and private keys and then import the Red Hat Public and RPM keys. This step is critical to verify the integrity and checksums of any post-build additions of security alerts, bugfixes, and enhancements. As we have already outlined this process for your secure server, please refer to the section titled "Creating a GPG Keys (You Need Protection) "When finished, return here so you can go on to importing public keys.

Import Public and RPM Keys (The Gate Keeper)
Once finished with your GPG key creation, import the Red Hat public and RPM keys. Please refer to the section titled "Importing Public Keys (I Know You, You Know Me!) When finished, return here to go on to the next part of securing the laptop titled Errata – Security Alerts.

Apply Errata - Security Alerts (Danger Will Robinson, Danger!)
So, you thought, wow! I installed my system, have some important keys, and now, I am ready to play with my new OpenOffice.org Draw program. Well, remember the laptop is still off the network and this step-by-step section has only scratched the surface of the entire process that will protect our binary impaired bookkeepers (although now they are more security conscious from Security 101). The first step to achieving that security nirvana is to add any security and bug fixes that Red Hat has found were necessary since its release. Here is where you take the CD that you burned with the Errata Security Alerts and Bugfixes (back in the "Download Errata" section) from the secure server after verifying the signer and the md5 sums.

Open a terminal window if you are in X windows or from a command line perform the following:

su – 'root'

Enter the password… quiet now, don't tell anyone!

mount /dev/cdrom

To update all applicable RPMs for your particular architecture, perform the following:

rpm – Fvh /mnt/cdrom/*.rpm

For each file that is updated, a line will be echoed to the screen that looks like the following example:

47

1:openssl   ############################### [5%]

When finished refreshing/updating, you will be returned to the command prompt.

Note: Sometimes there may be dependencies that will not be covered with the Security Errata. These will appear when you attempt your updates and you will have to return to your secure server and go through the process of downloading, verifying, and porting these update dependencies to the CDROM that you use to port files to the new laptop, then you can continue with the freshen process of the updates.

Configure SYSLOG (Monitor Activity)

Some logging is turned on when you build your laptop, but we can enhance this by modifying kernel logging and adding a line to alert us about warnings or errors.

Change directories to /etc and make a copy of the syslog.conf file. It is good practice to make a copy of any file before you make changes in case a mistake is made and you need to return to the original configuration.

cd /etc

cp syslog.conf syslog.conf.orig

vi syslog.conf

In the third line of the syslog.conf file, remove the remark symbol (**#**) and modify the /dev/console output destination to /var/log/kernel. Then insert the following line directly below the kernel line: *.warn;*.err /var/log/kernel. Make sure you use the TAB key separate the *.warn;*.err from the /var/log/kernel logging instructions, else it will not work. Save the change by pressing the escape key once, hold down the shift key and press the ":" key. Enter wq to save and exit and your changes are done. Now you have kernel, warnings, and errors being logged to the assigned directories. This will make forensics and security issues easier to track and identify. For added security, a remote SYSLOG server can be set up. This will make sure that if the system is compromised, any logs that before or during the breach were probably ported to the remote server for preservation. A link for a secure SYSLOG server build is provided in the Reference section.

Install Antivirus (So, you need protection, eh?)

There are several anti-viral packages available such as Antivir 2.06[50] or Kaspersky's AV 4.0.2.2[51]. For this project, the author chose to install RAV, which requires you to register for a 30-day free trial, if you want to verify its capability first. You can download it from your

---

[50] Antivir 2.06 Freeware - http://linux.tucows.com/internet/preview/8878.html

[51] Kaspersky's AV for Linux workstation 4.0.2.2 - http://linux.tucows.com/internet/preview/251301.html

48

secure server at http://www.ravantivirus.com/index.php. It sells for approximately $30 plus shipping and it had good reviews[52].

How to download the package and install it:

From your secure server, go to the universal resource locater (URL) http://www.ravantivirus.com/index.php.

Click on the Free Downloads link on the left side of Reliable Antiviruses home page.

Click on the Desktop Protection link titled RAV AntiVirus Desktop for Linux

Fill out the form for RAV registration as required. Hint: You do not have to fill in everything if you don't want to disclose private information. Click on the Start Download button.

You will be directed to a choice of FTP sites, choose the site that best fits your location.

You will be prompted to save the file:
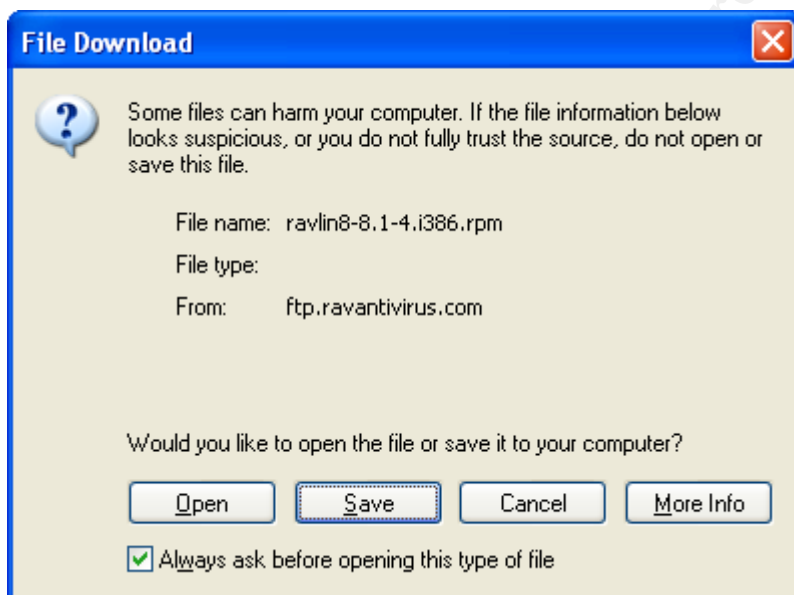
Click the save button and save it in the directory of your choice. It is a good rule of thumb to have a directory specifically for your security controls so can burn all of them at the same time to the CD or tape that you will use to port them to your new laptop build. Once the file exists on your new system, invoke these commands from the terminal window in a directory that you will use for these types of programs:

You will need to create an Application directory for the installation.

---

[52] RAV v8.5 review - http://www.linuxlookup.com/html/reviews/software/rav-antivirus-8.5.html

mkdir /usr/share/gnome/apps/Applications

Install the Ravlin package.

rpm –ivh ravlin8-8.1-4.i386.rpm (this may be different if the program has a newer version)

You will see the following output (the warning is ok, as the rpm will not install if the checksum fails):

Warning: ravlin8-8.1-4.i386.rpm: V3 DSA signature: NOKEY, key ID 1264f46f
Preparing…   ################################# [100%]
1:ravlin8   ################################# [100%]

This is the GUI version of how to install the package:

Insert CDROM, when the file window opens, double click with your mouse on the ravlin8-8.1-4.i386.rpm and the rpm installer will verify that no dependencies exist and after clicking on the OK button, the package will be installed.

For documentation, go to the RAV web site and click on the support link. Click on the RAV antivirus – Product Documentation link and you will see that by clicking on the Linux desktop link, you will be able to view the RAV PDF version of the users guide. This should help you become acquainted with the product. But for now, here is the command to run Rav8 from a command prompt:

ravlin8

You will be given a chance to update the product, but this will need to be done later as we are still not connected to the Internet for added security.

Click on the Later button.

The following screen will appear:

50
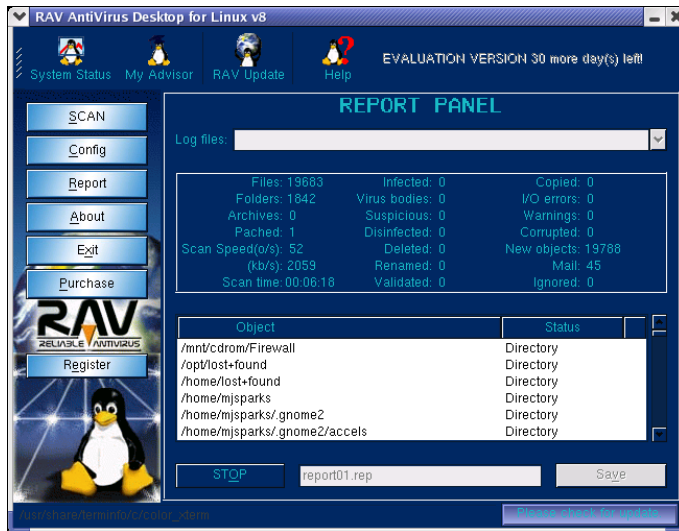
Click on the <u>S</u>can button, select all the directories on your machine, and then click on the <u>S</u>tart Scan button to run your antivirus (AV) program for the first time. It is good to verify that at this point you should not have any worms or viruses that would be known to this AV package.

Later after you have hardened the system and have access to the Internet, make sure you run an update to download the most recent Malware definition table and rerun your AV scan. This should dispel any thoughts of infection on your machine. This can be automated by adding the following lines to a script called Avscan (with these permissions –rwxr-xr permissions) in the /etc/crontab.daily directory. The cron.hourly puts too much load on the system and would interrupt normal duties. This will make sure your system checks for virus definition updates and then run your AV program every hour. Here is a sample of the script, once you create and place it in the directory mentioned, you will have automated virus updating and checking:

#!/bin/sh

/usr/local/bin/ravlin8 - -update=engine|full

/usr/local/bin/ravlin8 - -all - -move - -report=/'root'/AVscan /

Deny Direct 'root' Logins
Remote or local, it is poor security practice to login directly as "'root'". Best practices identify that administrators should create an identifiable regular user account in which the Sudo command or "su" to 'root' is used. Careful, if this system is in a controlled area, you may opt to allow direct 'root' logins for emergency cases. It is possible to lock the user and 'root' out at the same time causing a need for a rescue boot process to occur. You can also make this change with the GUI Login Screen configuration under the System Settings – Login Screen – Security tab. To disable this capability, make a copy of the /etc/securetty file, then type the following command as 'root':

echo > /etc/securetty

Set Login Banner to WTB Authorized Use Only!

Bad people can always challenge attempts at prosecution if you didn't display any messages to the contrary at the time of login. To do this, login and click on the Red Hat icon – System Settings – Login Screen. You will be prompted for the "'root'" password, enter it to continue. You will be faced with the following GDM Setup screen:
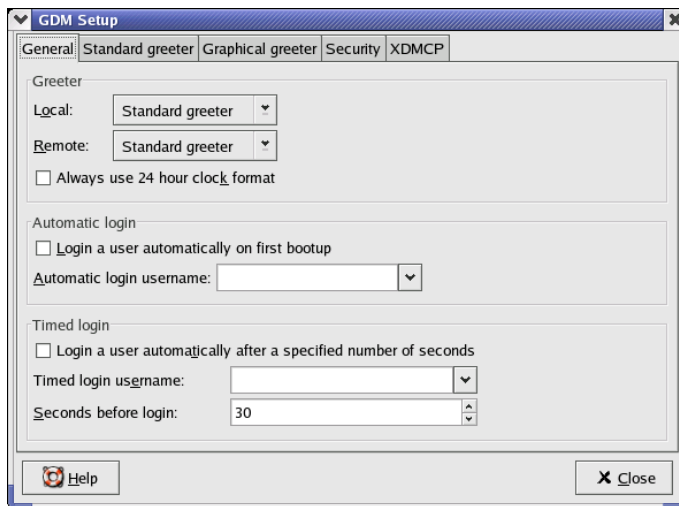
Click on the Standard greeter tab and modify the Welcome string: field to read "Welcome to %n Authorized WTB Use Only, All Others Prosecuted!

Using a logo will limit the amount of text you can display; it is probably better if you just select a background image. See next screenshot of the modified Welcome string:
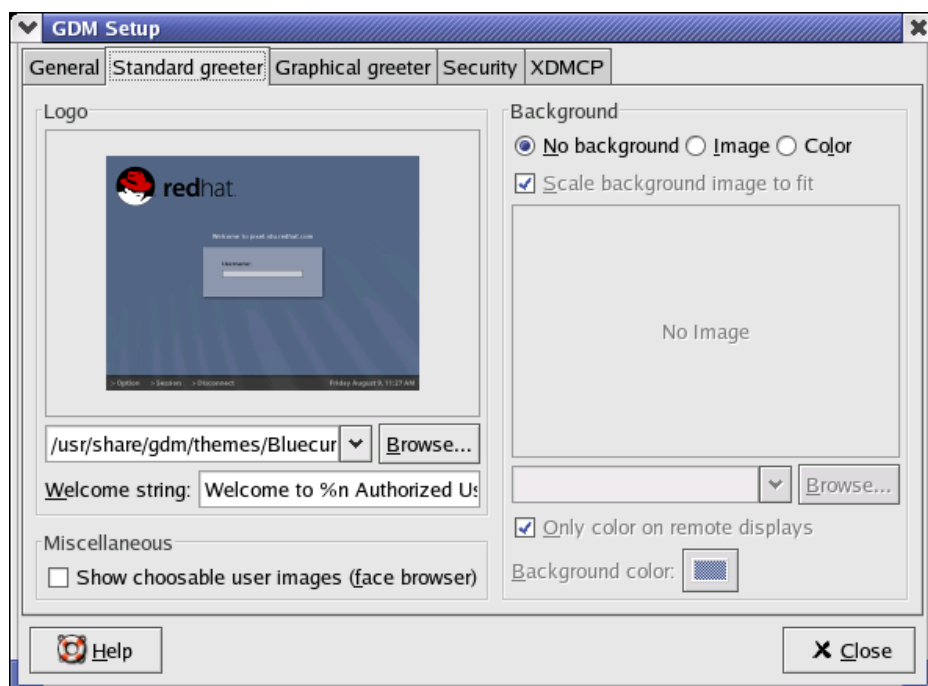
Force User Password Changes

Making sure passwords change periodically, is another step towards layered security. Given enough time and persistence, a hacker will eventually find information about systems and passwords. One way to defeat finding and using passwords, is to limit a password's age. This can be accomplished by forcing user passwords to be changed in 90 days or less. You can force this change with the following command:

chage –M 90 *bookkeeper_user_name*

You can also change this in the Graphical User Manager under the Main Menu Button – System Settings – Users and Groups - Properties. The following is a screen shot of that window:
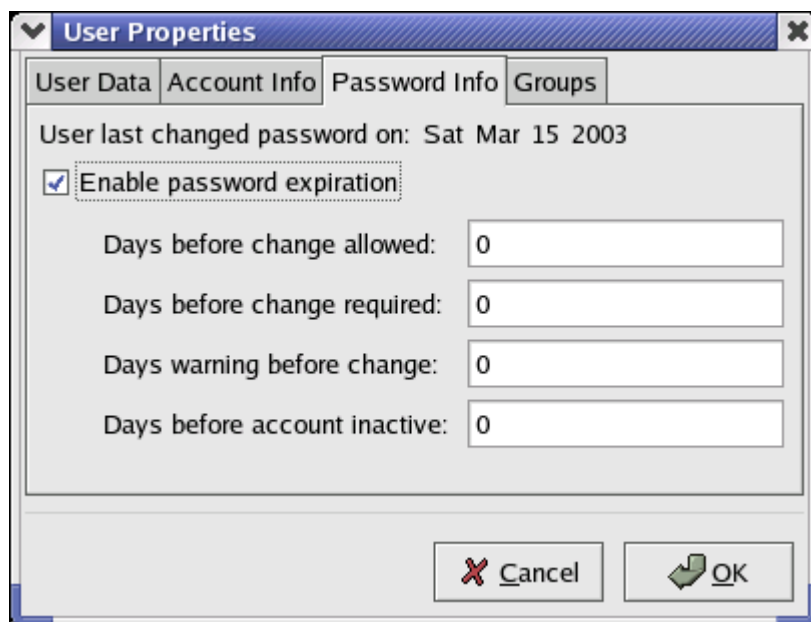
Set Screensaver Timeout lock

If your WTB bookkeeper walks away and forgets to lock the screen, you will want some automatic function to do this for the forgetful person. It is a security feature and reduces the risk of someone taking control of the unattended system by locking the login screen.

Click on the Red Hat icon in the lower left corner of the screen, then Preferences, and Screensaver.
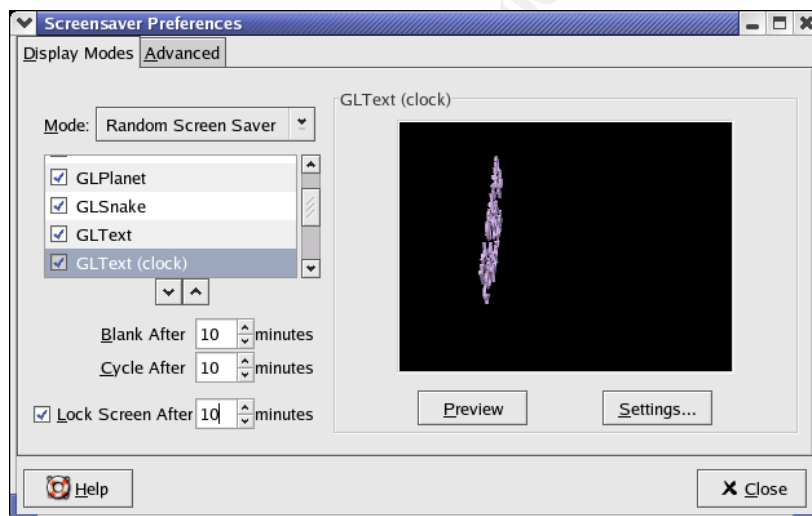
Next check the "Lock Screen After" box and set the time to 10 minutes.

Click the "Close button". You're done!

Sudo Help

Sudo, "Superuser Do", can be used for any post installation work that requires a user to perform commands as a super user or another user. This can be handy for a help desk if they want to make minor changes with the user remotely and reduce help desk overhead. It also reduces the risk related to 'root' versus Sudo use; Sudo activated commands can be traced back to the user who is assigned commands as Sudo can log all command use. The commands that you might want the end user to be able to execute will vary from business to business, so make sure and modify your 'sudoers' file as is appropriate. For more information, consult the Red Hat manual[53]. As with this and all configuration changes, be prudent and make a copy of the original 'sudoers' file first.

Login and switch user to 'root'.

$ su – 'root'

Copy the sudoers file to protect the original.

cp /etc/sudoers /etc/sudoers.orig

Modify the copied sudoers file to protect the original.

An example might be to allow the bookkeeper group to perform a file listing (ls -la) of the protected 'root' directory. This would be entered in the sudoers file as:

visudo

%*bookkeepername* localhost=/bin/ls –la /'root'

Preserve Critical Information

After installation, there are some important files that you will want to copy and store in a safe directory. The following are the files and commands that were performed to preserve the information that can be useful for system duplication or restoration:

Login as your administrator user ID and switch user to "'root'".

Move any file originals that were copied to a directory that you should make titled original_files.

Save a list of RPMs that have been installed.

rpm –qa | sort > /'root'/original_files/RPM_list

---

[53] http://www.redhat.com/docs/manuals/linux/RHL-8.0-Manual/security-guide/s1-wstation-privileges.html

Use the following Perl command to save the same list without version numbers, thanks to Hal Pomeranz[54]

perl –pe 's/-[^-]+-[^-\s]+$//' /'root'/original_files/RPM_list > /'root'/original_files/RPMs_novers

Stopping Unneeded Services

Use of chkconfig or ntsysv to determine what services will be started at boot time. The following is a screenshot of a 'root' activated ntsysv window:
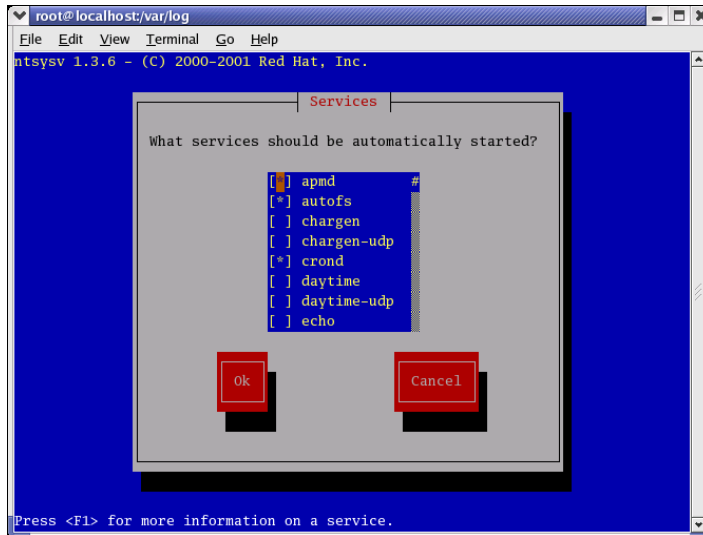
Only the following services should have the asterisk in the yellow brackets, e.g. [*]:

Apmd, autofs, crond, gpm, iptables, keytable, kudzu, lpd, netfs, nfslock, ntpd, pcmcia, portmap, random, rawdevices, rhnsd, sgi_fam, sshd, syslog, xfs, and xinetd.

Prepare for Incident Response

Even with all appropriate measures taken to harden you workstation, the chance of someone compromising your system still exists. Plans to monitor, update, backup, etc. will help you only if you have a plan, process, and identified Incident Response. Take the time to be familiar with sites like SANS that offer specialized training on incident response or others like www.cert.org that offer information on how to recover from an incident[55]. Preparation should include an incident response life cycle, e.g. Monitor, Detect, Respond, and Recover. Make sure and practice the response before an incident in order to have all the kinks worked out. Some links to incident response organizations and how-to documentation are listed in the References section.

---

[54] Hal Pomeranz. Deer Run Associates. hal@deer-run.com. Oakland, CA. http://www.deer-run.com/

[55] http://www.cert.org/tech_tips/win-UNIX-system_compromise.htm

56

Configure Iptables

Because of our initial configurations during the first part of the step-by-step installation, the security level (Iptables) should be set correctly. If you need to change these settings, click on the Red Hat in the lower left corner of your screen, then System Settings, and Security Level where you will be prompted to login with 'root' authority. Once authorized, you will see the following screen:
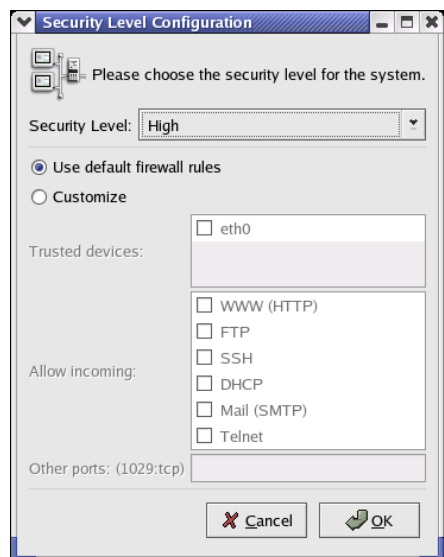
If SSH[56] is used for remote connectivity (more on SSH in the Ongoing Maintenance and Appendix sections), you would have to click on the Customize radio button, check the SSH box to allow incoming SSH connections.

Initialize Tripwire

Now comes the time to take a snapshot of your system prior to connecting to your isolated network so that we know if any unexpected file changes occur. The way we take this snapshot is using a program called Tripwire[57]. Tripwire takes a picture of all your files and directories and then stores this information in a database. After the database is populated with a snapshot of your system, it then runs at regular intervals to identify if this snapshot has changed in any way. This assures the integrity of your files and directories. Certain changes are acceptable on a day-to-day basis and certain changes are not. As the administrator, you will have to determine after review of the changes if updating the database is acceptable. The following are the required steps to set up Tripwire to monitor your system for data integrity assurance (perform as 'root'):

- Customize Tripwire (for detailed Tripwire use, refer to
  http://www.redhat.com/docs/manuals/linux/RHL-8.0-Manual/ref-guide/ch-

---

[56] http://www.ssh.com/

[57] http://www.tripwire.com/

57

tripwire.html#S1-TRIPWIRE-HOWTO) – Configure the Tripwire configuration and policy files.

Configure the Tripwire configuration file.

vi /etc/tripwire/twcfg.txt (Important - if any of the values are left blank, the configuration file will be invalid)

chmod 600 /etc/tripwire/twcfg.txt Change read permissions to 'root' only.

Set the LATEPROMPTING=true – This variable when set to true waits for the longest time possible to prompt the user from entering their password, thus reducing the time that the password resides in memory. Of course, we want to turn this on; it will reduce password exposure time.

LOOSEDIRECTORYCHECKING=true– This variable when set to true limits redundancy by just identifying the file that changes and not the directory associated with that specific file.

SYSLOGREPORTING=true - This variable when set to true reports Tripwire report information to SYSLOG. Be careful, if you do not have your policy fine tuned this could generate too much information.

Configure the Tripwire policy file.

vi /etc/tripwire/twpol.txt – This is where files that you expect to change are identified or ignored by the Tripwire integrity check. Remove the following remarks (**#**) as these files related to disk manipulation should not change on a local workstation:

/sbin/lvchange	**/sbin/lvrename**
/sbin/lvcreate	**/sbin/pvchange**
/sbin/lvextend	**/sbin/pvcreate**
/sbin/lvmchange	**/sbin/pvmove**
/sbin/lvreduce	**/sbin/netconf**
/sbin/lvremove	

: wq to save

- Initialize the database,

As 'root' run the following command:

58

/etc/tripwire/twinstall.sh – This will run the configuration script, which will ask for site and local passphrases that will generate cryptographic keys to protect Tripwire files.

Next, initialize the database:

/usr/sbin/tripwire - -init

- Run the integrity check,

- Identify if changes have been made, if not, run the integrity check at your next scheduled interval,

- If changes have been made (you should have about twenty or so files that should be remarked out in the twpol.txt file), identify if it is a potential security breach. If there is a potential breach, follow your incident response process,

- If not a security breach, update your policy to reflect acceptable changes,

- Update the database or edit the policy to allow the change and

- Return to normally scheduled integrity check process

Note: Tripwire offers a nifty service for pre-canned policies; however, there currently is not a policy for RH8.0. It does provide a nice guideline to understand how the policy should be modified to ignore those files and directories that you would expect to change regularly. You can find this at http://tpt.tripwire.com/tprc/servlet/VersionChoose?platform-name=RedHat+Linux.

Create a Full Backup

Creating a full system backup can be done by mounting a Tape Backup device and copying your entire hard drive twice on two separate tapes. Use the following command:

tar czf backup.tgz /

You will then want to plan a regular backup process to insure availability or return to last known good state if attacked. A good rule of thumb after the initial full backup is a sustaining process that uses six tapes. Four for Monday through Thursday, which are incremental backups, the other two will be used for even or odd Friday full backups. If major changes are to be made, you might want to perform a full backup first.

Connect to an Isolated Network for Final Assessment

This is where we need to assess the security strength of the Laptop from a hacker's perspective. For this last test, Nessus, a vulnerability scanner will be used. The web links and basic instructions for installing this tool are located in the Appendix. Use your isolated network with the secure server or a secure system with Nessus installed.   Enter the following commands from a GUI capable Nessus installed system:

 # nessusd & - Start the Nessus daemon

 # nessus - Start the Nessus client

There are two types of assessments you will want to run; one is the non-destructive and the other is the no-holds-barred setting.

Install Host Intrusion Detection (HIDS)

So, how will you know if your Laptop is under attack or unauthorized behaviors are occurring? One good tool for this is Host Intrusion Detection Systems or HIDS. HIDS is a system that monitors for known attacks, anomalous network behavior, or illegal protocol use. The HIDS program we will use is called Snort.[58]   The following are the instructions for downloading the current RPM along with installation commands:

Download the current Snort RPM at http://www.snort.org/dl/binaries/linux/

Install the RPM as 'root', make sure you have libpcap 0.4 and libpcapso.0.6.3 or greater installed.

rpm –ivh snort-current-version.i386.rpm

Add /etc/snort to your path and your /etc/rc.d/init.d startup directory and voila, you now have a snorting HIDS.

It creates logs in /var/log/snort and these should be ported to your secure syslog server and reviewed daily. For further details on how to ride that hog, become one with the Snort documentation at http://www.snort.org/docs/.

Install MyBooks

Log on as 'root'

Create a user named 'appgen'

Log out, and log back in as 'appgen' in order for the system to setup 'appgen's' basic desktop pieces.

Log out, and log back in as 'root'

From the desktop screen click on setup.sh

Follow the on-screen instructions. Once the installation is finished, log out, and log back in as 'appgen'. Click on the MyBooks icon on the desktop to start MyBooks.

---

[58] http://www.snort.org

60

Ongoing Maintenance

Establish a Change Control Process

Regular changes are to be expected with current software size, changing business needs, or a change in the program code security. What does this mean to you? Well, if you expect to experience a desirable level of availability, you will want to implement changes in a way that is acceptable from a security and business operations standpoint. For security personnel this has always been a balancing act. You will want a change life cycle that incorporates at least the following steps:

- Identify the required change

- Assess the risk of applying or not applying the change

- Develop change components

- Test and validate, test and validate (no there wasn't a keyboard stutter☺). This step as well as apply to production should include a "Second pair of eyes" to validate that everything works as promised.

- Introduce into production. Generally, changes should occur during a non-business interruptive time period called a "Change Window". For many businesses, this would probably be on Saturday at a specific time, which allows for a back out contingency plan if things go unexpectedly wrong.

- Document, backup configurations or files, and then monitor changes for 24 to 48 hours. Preferably, this takes place after the Friday evening full backup. Too often, changes in large operations are implemented and then the team goes home only to be called two to three hours later with a network down situation due to an unmonitored change or loss of unexpected data from a change. The documentation should cover all the granularity of the change, before and after the change, so that there is a record of the change and you can immediately replace the known good configurations if problems occur.

Keep Security Patches Current

Regular security vulnerability patching is an important part of keeping your RH8.0 build secure. If your environment requires moderate to extreme availability, it is a good idea to have a documented change process. This change process would be much like our isolated network validation setup. You would download any current updates, which you will receive if you sign up as a Red Hat Network[59] user or purchase service as it fits your company[60]. Here is a partial example of a Red Hat email alert:

---

[59] https://rhn.redhat.com/

[60] https://rhn.redhat.com/info/purchase_info.pxt

61

I recommend you sign up for at least one type of account to stay current with updates and have some level of support in case there is something you cannot figure out, and then Red Hat can help you. An automated process called "up2date"[61] is available, which can also alert you of new security patches and make them easy to update.

Maintain Regular Backups
In the case of the IBM TP600, all customer and critical data is sent to a secure file server on the Intranet, which is backed up in the evening every day, following the previous backup process defined in the post installation section titled "Create a Full Backup". Once per week, the system administrator, like you, tests restores to make sure these important files can be restored. There should also be a process where secure offsite storage for backup tapes, other than the current day's tapes, is stored. This site should be audited quarterly to verify the integrity of your information and the security of their storage process. Red Hat has a great web page of instructions on the details of "Planning for Disaster" at the following site: http://www.redhat.com/docs/manuals/linux/RHL-8.0-Manual/admin-primer/s1-disaster-backups.html.

Review Syslogs
Once logging is set up and pointed to files either locally or on a secure remote server, you will need to review them to identify signs of security issues. One way is to change into the /var/log directory and "less" the file and hopefully know what you are looking for; this is a real tedious manual method. A nicer way is to go to the main Red Hat button - System Tools – System Logs or redhat-logviewer at the command line, which calls the latest log watching program logwatch-2.6-8.   You should see the following screen with log information that pertains to your screen:

---

61 http://rhn.redhat.com/help/basic/up2date.html

```
File   Edit   Help
Boot Log                 System Log
Cron Log
Kernel Startup Log                              This is the system log file.
FTP Log
Apache Access Log        Aug 16 15:12:19 falcon automount[746]: attempting to mount entry /mnt/redhat
Apache Error Log         Aug 16 15:12:20 falcon automount[706]: attempting to mount entry /home/cpruitt
Mail Log                 Aug 16 15:13:31 falcon automount[3321]: expired /home/cpruitt
                         Aug 16 15:18:41 falcon automount[3375]: expired /mnt/redhat
MySQL Server Log         Aug 16 15:35:47 falcon automount[746]: attempting to mount entry /mnt/redhat
News Log                 Aug 16 15:41:12 falcon automount[3500]: expired /mnt/redhat
RPM Packages             Aug 16 15:51:07 falcon automount[746]: attempting to mount entry /mnt/redhat
Security Log             Aug 16 15:52:50 falcon sudo(pam_unix)[4650]: authentication failure; logname= uid=0 euid=0 tty=pts/2 ruser=
System Log               Aug 16 15:52:50 falcon sudo[4650]: pam_krb5: authentication succeeds for 'tfox'
                         Aug 16 15:53:03 falcon userhelper: pam_timestamp: timestamp file `/var/run/sudo/tfox/unknown:root' is too old
Update Agent Log         Aug 16 15:54:25 falcon userhelper: pam_timestamp: timestamp file `/var/run/sudo/tfox/unknown:root' is only 81
XFree86 Log              Aug 16 15:56:50 falcon userhelper: pam_timestamp: timestamp file `/var/run/sudo/tfox/unknown:root' is only 14
                         Aug 16 15:59:07 falcon login(pam_unix)[962]: check pass; user unknown
                         Aug 16 15:59:07 falcon login(pam_unix)[962]: authentication failure; logname=LOGIN uid=0 euid=0 tty=tty2 rus
                         Aug 16 15:59:07 falcon login[962]: pam_krb5: unable to determine uid/gid for user
                         Aug 16 15:59:07 falcon login[962]: pam_krb5: authentication fails for 'test'
                       🔴 Aug 16 15:59:09 falcon login[962]: FAILED LOGIN 1 FROM (null) FOR test, Authentication failure
                         Aug 16 15:59:11 falcon modprobe: modprobe: Can't locate module char-major-10-134

          Filter for:                                      🔍 Filter        🔄 Reset
```

If you would like to try a different logger, try "Swatch[62]"

Verify User Password Strength

So, you teach security awareness and emphasize that passwords are the first line of defense, but you know humans tend to be a little lazy occasionally. This is a good reason to have a regular audit of user passwords, preferably at least once a month, at the most every ninety days. Take some of the password files and run password-cracking tools against the lists to verify "password strength" policy compliance. Two tools, for this purpose, are "John the Ripper", and "Crack". Here are the links for each of those tools so that you may perform regular password strength testing (get management permission in writing first):

- John the Ripper - http://www.openwall.com/john/

- Crack v1.4 - http://www.crypticide.org/users/alecm/

Remote System Administration

Unfortunately, there is no way to get around the need to provide system support once your secure Laptop build is delivered to the WTB end user. To allow secure remote logins, you will want to configure and allow SSH (secure shell) access for administrators only. Secure shell provides an encrypted connection to and from a system. This can be controlled with your firewall configuration.

Tripwire Report Review

Fortunately, Tripwire captures most of the events that you will really have to worry about and it runs daily. Make sure you look through the daily results (substitute the tripwirefile.twr with the current Tripwire report file) using the following command:

/usr/sbin/twprint –m r –twrfile /var/lib/tripwire/report/*tripwirefile.twr*

Enter this command to force a check with Tripwire:

/usr/sbin/tripwire –check

Then, rerun the previous twprint command to view the newly generated report.

Handling Break-Ins

Pretty much these days, as security goes, you can follow the cliché that "If you build it, they will come"! So with that being said, you will want to have some knowledge of what the appropriate steps would be during a break-in. The following is a good rule of thumb for a break-in that is most likely in progress:

- Detect – How did you find out that you have been hacked? First, make sure to verify you have indeed been comprised along with the confidence of your detection source. Many errors can occur if people are excited because they think they have an intrusion, take it step-by-step, act swiftly, and remain calm. A good incident respondent starts to collect all the evidence such as how the break-in was detected, by whom, when, how…. You get the picture. Then record the information in an incident journal for review during your post mortem.

- Disconnect the attacker's connection – What is allowing the access? If it is the network, disconnect the network cable. Do not shut the machine down as lots of hackers and their kits have processes to clean up their break-in footprints via log cleaners and such when the machine reboots.

- Backup - Make a complete bit-by-bit copy of the compromised system if you intend to interrogate the system for possible prosecution. If prosecution is your goal, computer forensics skills are necessary. You can get this type of training from SANS by taking their certified Forensics Analyst course, either at a conference or onsite - http://www.giac.org/subject_certs.php#GCFA or http://www.sans.org/onsite/track8.php

- Identify and fix the vulnerability – This must be identified before returning your system to the network. The majority of the time, it is best to just rebuild your system (remember you have a copy to look at to make sure you know how the perpetrator got in) and follow the build steps to put all security controls in place. Make sure you apply patches, if available, that protect against the vulnerability.

- Identify losses – What did the compromise deliver to the hacker? Was it confidential customer data or did they just use the system for storage? If it was customer data, there may be a need to disclose this information to the customers and legal authorities.

- Identify the intruder and intrusion path – If you legitimately know where the attack came from, you can block this network with your firewall to deter any future attacks.

64

- Return to normal – Anytime a break-in has been discovered, the best approach is to reinstall a clean operating system, repair the vulnerability that allowed access, apply all current security controls and patches. This is covered in the "identify and fix" section, but it is a good idea to remind responders return to normal.

- Continue monitoring – Just because you fixed the holes or added new controls doesn't mean you should let your guard down. Review your logs regularly and monitor for any further anomalies that might identify recurrence of an attack.

- Post Mortem the Incident – Have a meeting once everything has settled down and appropriate measurers have been taken. This meeting should identify what went right and what went wrong. Identify the gaps, make plans to fix the gaps, and then praise all participants who did the right thing when the heat was on.

Perform Regular Vulnerability Scans

Once the perimeter and host have been secured, it is a lot like building a fence around a building for protection, you need to check and see if there are any holes in the fence from someone trying to break in or an inadequacy in the original erection of the fence. The best way to do this is perform regular vulnerability assessments with tools like Languard[63], Foundscan[64], or Nessus[65]. Along with your automated tool, take a look around the system the old fashion way (manual listings, top commands, sar, vmstat, umask, etc. to see if she is performing the way you would expect) just in case all your fancy tools don't alert you to anything. Some of the best discoveries have happened under casual system use. Heck, every once in a while, I like to run a simple script like:

gawk '/0\:0/ {print $1}' /etc/passwd

This will tell me if anyone other than 'root' has 'root' permissions. The first command is a parsing command, followed by, a search for zero values in the group and user fields, along with printing the line that will display the user that has these 'root' permissions. Easy little one line hacker catcher.

Review Antivirus Logs

Once you have had the antivirus daily program running you will want to verify if all is well by reviewing the saved logs.
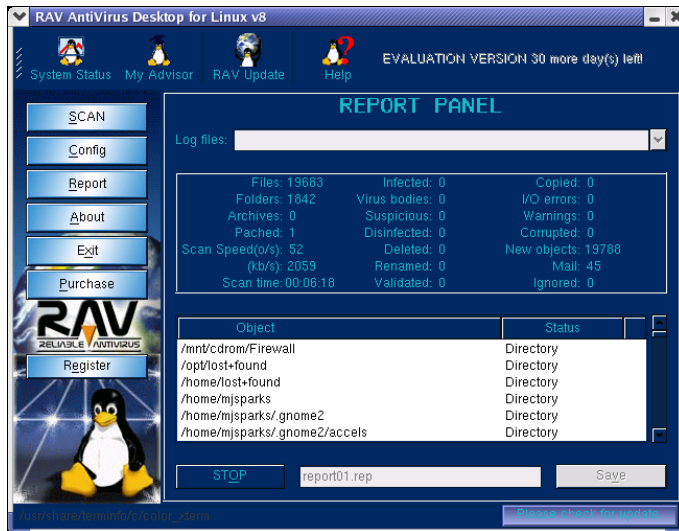
Start RAV

---

[63] http://www.gfi.com/lannetscan/

[64] http://www.foundstone.com/services/mvas.html

[65] http://www.nessus.org/

65

ravlin8

Click on the Report button and you should see a Log files: field, click on the "v" button and select the date of the report you would like to review. If you have been diligent in your security, you should see a clean report.

Check Your Configuration

Test for Open Ports with Nmap

Nmap ("Network Mapper")[66] is an open source tool for network mapping or security auditing. On the isolated network, run Nmap to determine if ports or services that you have disabled are indeed disabled.

nmap *laptop_hostname_or_IP*

You should see "All 1601 scanned ports on (hostname) are: filtered"

Verify Root Cannot Login Directly

This will be an easy test, if you can log in as 'root', go back to the System Settings - Login Screen – Security tab and uncheck the box titled "Allow root to login with GDM".

Verify Absence of Known Vulnerabilities

With the current Nessus plugins[67] installed, run Nessus against your new machine.

From a terminal window of your secure server, start the Nessus daemon.

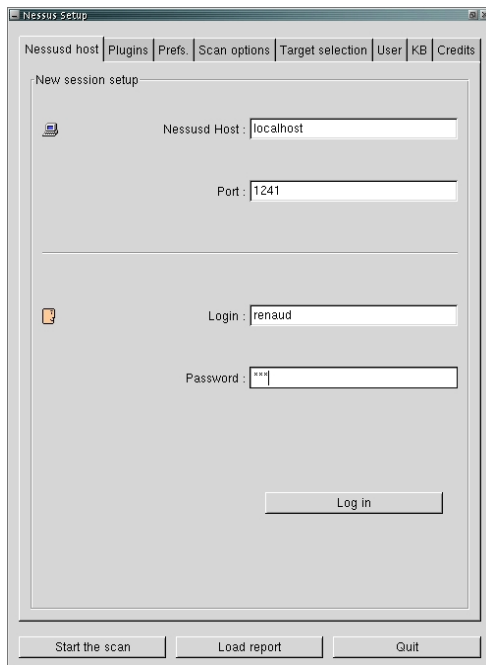**#** nessusd &

---

[66] http://www.insecure.org/nmap/

[67] http://www.nessus.org/scripts.php
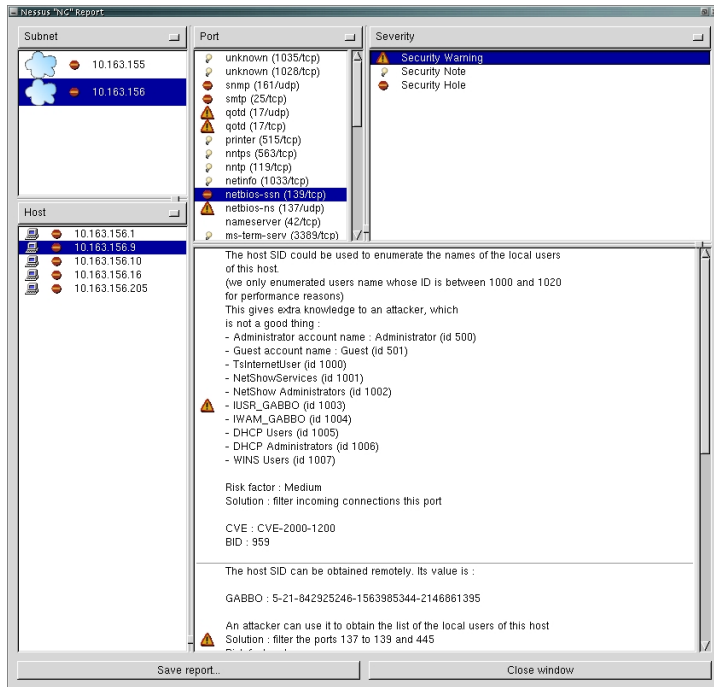
66

Start the Nessus client.

nessus

You will see the following screen:

Enter your password and click the "Log In" button.

Set the appropriate options to scan your laptop and click the "Start the scan" button.

You should receive two general issues related to UDP and TCP along with a low-risk warning about ICMP in a screen that looks similar to the next screen:

The results found during this scan of our new laptop are acceptable for our WTB network.

Review the Tripwire Report
As described in the "Ongoing Maintenance" section, you can force a Tripwire check anytime.

Enter this command to force a check with Tripwire:

/usr/sbin/tripwire –check

Enter this command to read the Tripwire report created by the previous command:

/usr/sbin/twprint –m r –twrfile /var/lib/tripwire/report/*tripwirefile.twr*

Review the Snort Logs
After probing your machine with Nessus and Nmap, your Snort HIDS will generate logs in /var/log/snort. The logs will be in sub-directory names of the attacking IP addresses or hostnames.

Here is a sample of the command to view one of these logs from a Snort identified attack, along with the output:

 # less /var/log/snort/10.2.1.23

=+=+=+=+=+=+=+=+=+=+=+=+==+=+=+=+=+=+=+=+=+=+=

[**] SCAN Amanda client version request [**]

03/24/03-21:40:15.957888 10.2.1.22:1208 -> 10.2.1.23:10081

UDP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:97 DF

=+=+=+=+=+=+=+=+=+=+=+=+==+=+=+=+=+=+=+=+=+=+=

Reassess WTB' Risk

Let's redo our previous risk assessment now that we have identified security needs, applied them, and tested them to ensure their viability.

Scenario Redux: In our previous Risk Assessment, we identified that we had purchased Red Hat Linux 8.0. RH8.0 has been out for a period, and WTB management are concerned about vulnerabilities, threats or chances of malicious software attacks that disclose sensitive data (Confidentiality), evil doers that might block our Internet access (Availability), or unanticipated accidents such as writing over a patented bookkeeping formula (Integrity) that could cause WTB Company serious financial impact. Now that we have added controls, protective software, removed unwanted or needed packages, and services; we need to look at our overall risk for the final time. We do expect to have an Overall Risk total that falls in the Low levels, which we previously stated is an acceptable level to management.

> Threat - Hackers have created exploits that are capable of attacking several packages on Red Hat 8.0. Our current infrastructure and Laptop security cannot stop the hacker directly; nevertheless, the known exploits are not a threat to our current build – **Moderate (2)**

> Vulnerability - WTB Company's initial RH8.0 installation has had current security alert and bug fix patches applied. Countermeasures, at or near, our border firewall prevent known attacks, viruses, or worms from entering into our environment. This is accomplished with a network intrusion detection system (NIDS). Antivirus software has been added to our laptop. Tape backups occur every night and are checked monthly for integrity. **Low (1)**

> Consequence - WTB stands to loose availability and sensitive data if the worm successfully exploits any internal systems **(3)**

> **Overall Risk = Threat X Vulnerability X Consequence = 2 X 1 X 3 = 6 = Low**

Success - Our system is secure and at an acceptable overall risk of low! Congratulations!

References

General

Red Hat Release Notes - http://www.redhat.com/docs/manuals/linux/RHL-8.0-Manual/pdf/rhl-relnotes-x86-en-80.pdf
International Business Machines - www.ibm.com
The Culinary Institute of America - http://www.ciachef.edu/
http://www.linuxplanet.com
http://dcb.sun.com
http://www.redhat.com
http://slencyclopedia.berlios
Covey, Stephen R. 7 Habits of Highly Effective People. New York: Simon & Schuster, 1990.
SSH - http://www.redhat.com/docs/manuals/linux/RHL-8.0-Manual/ref-guide/ch-ssh.html

Defense in Depth, Network, and System Security Related

Stephen Northcutt, Lenny Zeltser, Scott Winters, Karen Fredrick, Ronald W. Ritchey. Inside Network Perimeter Security. Indiana: New Riders, 2003.
SansPress Publications. http://store.sans.org/index.php
Hal Pomeranz. Securing Unix Systems. Maryland: SANSPress, 2002.
Micki Krause and Harold F. Tipton. Information Security Management Handbook Fourth Edition, Volume I. 4th edition. CRC Press - Auerbach Publications, 1999.
Thomas A. Wadlow. The Process of Network Security. Massachusetts: Addison-Wesley, 2000
Secure ID - http://www.rsasecurity.com/products/securid/index.html

Security Organizations and Security Planning Guides

http://www.cert.org
http://csrc.nist.gov/index.html
http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.doc
http://emea.bsi-global.com/InformationSecurity/Overview/index.xalter
http://www.sans.org/rr/

Incident Response – Handling a Break-in

http://www.cert.org/nav/index_red.html
http://www.europe.redhat.com/documentation/HOWTO/Security-HOWTO-10.php3
http://www.europe.redhat.com/documentation/HOWTO/Security-HOWTO-11.php3
http://www.sans.org/rr/incident/

Security Scanners

Languard - http://www.gfi.com/lannetscan/
Foundscan – http://www.foundstone.com/services/mvas.html
Nessus - http://www.nessus.org/
Nmap - http://www.insecure.org/nmap/

Log Monitors

Swatch - http://swatch.sourceforge.net

VI Editor Links

Harold Rodriguez . "Vi Crash course". http://startlinux.co.nz/articles/article_74.php
thebaker@codebake.com thebaker@codebake.com. "Crash course in using vi".
http://www.codebake.com/usingvi.php?displaytype=print&articleid=5

Secure Server Builds

Harpal Parmar. http://www.giac.org/practical/GCUX/Harpal_Parmar_GCUX.pdf. 2003.
John T. Douglass. http://www.giac.org/practical/John_Douglass_GCUX.doc.

General Internet Searches

Google. http://www.google.com
Search. http://www.search.com

Appendix

Startup Changes Warning

When changing your startup sequence, you must be extremely careful when doing write operations (such as copying, saving, or formatting). Your data or programs can be overwritten if you select the wrong drive. For more information about the selectable drive-startup sequence, refer to the ThinkPad User's Guide -
ftp://ftp.pc.ibm.com/pub/pccbbs/mobiles/600usref.pdf

Selectable Drive-Startup Sequence

Selectable drive startup (selectable boot) allows you to control the startup sequence of the drives in your computer. The order in which the computer looks for the drives for your operating system is the drive startup sequence. If you are working with multiple operating systems, you might want to change the drive startup sequence to load the operating system from the hard disk without first checking the diskette drive, or to do a remote program load (RPL).

GnuPG

The following is a brief explanation copied from the online GnuPG Privacy Handbook at http://www.gnupg.org/gph/en/manual.html#INTRO.   GnuPG uses public-key cryptography so that users may communicate securely. In a public-key system, each user has a pair of keys consisting of a *private key* and a *public key*. A user's private key is kept secret; it need never be revealed. The public key may be given to anyone with whom the user wants to communicate. GnuPG uses a somewhat more sophisticated scheme in which a user has a primary keypair and then zero or more additional subordinate keypairs. The primary and subordinate keypairs are bundled to facilitate key management and the bundle can often be considered simply as one keypair.

SSH

SSH is a secure shell protocol that allows an encrypted session between a client and server. This helps protect any data transmission from clear text analysis. In other words, if the bad person is watching your data travel across the network he or she might have an analyzer or sniffer installed to try and capture any clear text information such as passwords. This would aid them in a future attack if they can find the remote user identification and passwords. The following is an excerpt from the Red Hat manual about how an SSH connection takes place.

Event Sequence of an SSH Connection

The following series of events help protect the integrity of SSH communication between two hosts.

First, a secure transport layer is created so the client knows it is communicating with the correct server. Then, the communication is encrypted between the client and server using a symmetric cipher.

To allow SSH for your local domain, modify the /etc/hosts.allow with the following lines:

Allow SSH from our domain

sshd: LOCAL   .ourdomain.com

To SSH to the File Server where you will store company data, use the following commands:

To connect:

ssh secure_file_server.ourdomain.com

You should see the following:

```
The authenticity of host 'secure_file_server.ourdomain.com' can't be established.
DSA key fingerprint is 94:68:3a:3a:bc:f3:9a:9b:01:5d:b3:07:38:e2:11:0c.
Are you sure you want to continue connecting (yes/no)?
```

Yes

```
Warning: Permanently added 'secure_file_server.ourdomain.com' (RSA) to the list of known hosts
```

You will be prompted for your password to the remote server. After entering it, you will have established a secure shell connection to the remote server. You can now pass information to the server securely.

To use SCP (secure copy):

scp *file_to_copy* secure_file_server@server.ourdomain.com :*remote_file*

Consult the SSH instructions in the Red Hat custom guide for further details - http://www.redhat.com/docs/manuals/linux/RHL-8.0-Manual/custom-guide/s1-openssh-client-config.html.

Nessus Installation

Nessus[68] is a security or vulnerability scanner. It is designed to probe a system for any possible security vulnerabilities and then report out if it has found any. Nessus is open source code and downloadable from http://www.nessus.org/download.html. The home page of Nessus, http://www.nessus.org/index2.html, gives you all the links necessary to understand, download, install, and run Nessus against your laptop in order to determine if

---

[68] http://www.nessus.org/index2.html

73

any security vulnerabilities still exist after you have applied controls or countermeasures that intend to protect the laptop. For ease of this step-by-step document, the basic installation and operating instructions have been included that will take place on your secure server which will become the Nessus source that will probe your laptop destination. It is in no way meant to be all-inclusive. For further information, please consult the Nessus literature.

As a normal user, you can download the scripted version install from one of several mirror FTP sites at (make sure import the Nessus public key and verify the MD5 sum):

http://www.nessus.org/nessus_2_0.html

From the Nessus web site.

To compile Nessus the manual way (recommended), you need to download the latest distribution available here. This will take some knowledge to tweak it for your protected system if you want the GUI version. This document will not cover that. You should have these four files and place them in a security tools directory:

      nessus-libraries-x.x.tar.gz
      libnasl-x.x.tar.gz
      nessus-core.x.x.tar.gz
      nessus-plugins.x.x.tar.gz

To expand the files, type the following command in your security tools directory:
      $ gunzip *nessusfile*.tar.gz
      $ tar –xvf *nessusfile*.tar.gz

You must compile them in this order.

Installing nessus-libraries
Compiling nessus-libraries is a simple operation:
      $ cd nessus-libraries
      $ ./configure
      $ make
After this, execute this command as 'root':
      # make install

Installing libnasl
This is straightforward:
cd libnasl
      $ cd libnasl
      $ ./configure
      $ make
After this, execute this command as 'root':

74

make install

Repeat the same operation with nessus-core and nessus-plugins.

Make sure that */usr/local/lib* is in */etc/ld.so.conf*, and type *ldconfig*.

export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/usr/local/lib
(You may want to add this into your ~/.profile)

If you do not want the client to use GTK (if your system lacks X11 for instance), then
you can compile a stripped-down version of the client, which will work on command-line.

To do this, add the --disable-gtk option to configure while building nessus-core:
cd nessus-core; ./configure --disable-gtk ; make && make install
Then, that's it! Nessus is installed on your system.