



**SANS IT Audit**  
with Tanya Baccam

# IT Audit: Security Beyond the Checklist

Copyright SANS Institute  
Author Retains Full Rights

This paper is from the SANS IT Audit site. Reposting is not permitted without express written permission.

## Interested in learning more?

Check out the list of upcoming events offering  
"20 Critical Security Controls: Planning, Implementing and Auditing (SEC440)"  
at <http://it-audit.sans.org><http://it-audit.sans.org/events/>

# **Auditing a Systems Security Consultant's Laptop Running Fedora Core 2**

**GSNA Practical Version 3.2 – Option 1**

**Author: Yolanda Martinez**

**Date: December 20, 2004**

© SANS Institute 2004, Author retains full rights.

## Abstract

At the SANS Track 7 class, I heard the best words that summarize what auditing is about:

*“Auditing is a measure of conformance”<sup>1</sup>*

Those simple words provide the perfect foundation for this document and what I am trying to accomplish.

The purpose of this report is to illustrate the process of auditing and verifying conformance to specific policies, procedures, security guidelines and best security practices of a systems security consultant's laptop. The laptop belongs to Sirius, Inc., a small fictitious systems security auditing and consulting organization. The laptop runs Fedora Core 2 as its only operating system.

The document is divided into 4 main sections:

- The first section identifies the target system to be audited, the threats, risks and vulnerabilities of the system.
- The second section presents an audit check list and testing procedure based on the findings of the first section.
- The third section shows the current state and behavior of the system using the check list and testing procedure developed on the second section.
- The fourth section provides a summary of the findings and recommendations to maintain or improve the security of the system.

## Table of Content

<a href="#">Abstract</a> .....	2
<a href="#">Table of Content</a> .....	3
<a href="#">Table of Tables</a> .....	4
<a href="#">Section 1 – Research in Audit, Measurement Practice and Control</a> .....	5
<a href="#">Issues About Auditing an “Auditing” Laptop</a> .....	5
<a href="#">Preliminary Audit Meeting</a> .....	5
<a href="#">Identification of the System to be Audited</a> .....	6
<a href="#">Computer Model, Operating System &amp; Software Installed</a> .....	7
<a href="#">The Purpose of the System</a> .....	10
<a href="#">Evaluate the Risk to the System</a> .....	10
<a href="#">Threats Identified</a> .....	11
<a href="#">The Laptop as an Auditing Tool</a> .....	11
<a href="#">General Threats to Laptop</a> .....	12
<a href="#">Vulnerabilities identified</a> .....	15
<a href="#">Determination of Impact and Risk as a Result of Realized Threats</a> .....	17
<a href="#">Summary of Identified Risks</a> .....	27
<a href="#">Current State of Practice</a> .....	28
<a href="#">State of Practice for the Laptop running Fedora C2</a> .....	28
<a href="#">State of Practice for the Auditing Tool</a> .....	29
<a href="#">Control Analysis</a> .....	31
<a href="#">List of Control Categories</a> .....	31
<a href="#">Section 2 – Audit Check List</a> .....	33
<a href="#">Scope</a> .....	33
<a href="#">Conventions and Format</a> .....	33
<a href="#">Checklist Item Template</a> .....	34
<a href="#">Check List</a> .....	34
<a href="#">Section 3 – Audit Testing, Evidence and Findings</a> .....	45
<a href="#">Results of the Audit</a> .....	45
<a href="#">Section 4 – Audit Report</a> .....	61
<a href="#">Exit Meeting</a> .....	61
<a href="#">Executive Summary</a> .....	61
<a href="#">Conclusion</a> .....	71
<a href="#">Appendix A</a> .....	72
<a href="#">Appendix B</a> .....	75
<a href="#">Appendix C</a> .....	77
<a href="#">Appendix D</a> .....	81
<a href="#">Appendix E</a> .....	84
<a href="#">Appendix F</a> .....	86
<a href="#">Appendix G</a> .....	92
<a href="#">Appendix H</a> .....	93
<a href="#">References</a> .....	99

## Table of Tables

Table 1.1 - Human Threats .....	14
Table 1.2 - Operational Threats .....	14
Table 1.3 - Human Threats .....	14
Table 1.4 – Risk-Level Matrix .....	18
Table 1.5 – Estimating Risk .....	20
Table 1.6 – High Risk Summary .....	24

© SANS Institute 2004, Author retains full rights.

## Section 1 – Research in Audit, Measurement Practice and Control

### Issues About Auditing an “Auditing” Laptop

Due to the nature of security auditor’s job, his/her laptop needs to be able to connect to various networks. Some of those networks cannot be trusted. Therefore, the system must have appropriate mechanisms and configurations to allow it to perform the auditing functions, protect itself, and prevent unauthorized access.

At different times, the system may contain clients’ sensitive and confidential information collected during assessments, audits and analysis projects. The system must have the appropriate tools to protect this data and avoid disclosure of information while it resides in the laptop.

The laptop must be able to protect itself from various forms of attacks such as virus, worms and Trojans. These can produce adverse results including data or system modification, and can even turn the system into a vector of attack against the various networks to which it needs to connect.

Either one of the situations could result in the loss of credibility, affect the reputation, or have very bad financial and legal consequences for the auditor’s organization.

Another important consideration when analyzing a laptop used for security audits and assessments is the type of applications and tools installed in it. Many of the well known security tools are not for general consumption. These tools can cause a lot of problems when they are not configured properly. They must be used ethically and must be used with the appropriate authorization.

This document will present the audit process of an auditing laptop that takes into consideration that it is a mobile system, with a specialized purpose

### Preliminary Audit Meeting

Before we can even start any research or take any steps on the audit process, meeting with the management team of the organization that owns the system to be audited is recommended.

The meeting will allow the auditor to:

- Explain the purpose of the audit and set clear expectations.
- Gather documentation including contact information, policies, procedures, charts, etc.
- Provide an estimated timeframe for the audit.
- Explain what will not happen during the audit.

Although it might seem strange to talk about what “will not happen”, it is almost as important as what “will happen” during the audit process. Audit processes can create an environment of tension. In many occasions, I have seen that operational groups or the groups being audited feel scrutinized by the “outsider”, and they don’t like “outsiders” touching their systems.

In this case, the auditor is dealing with an organization familiar with security auditing and assessment processes. Therefore the staff understands why these steps are necessary.

Even though Sirius’ staff is familiar with the process, it is still important to explain that the auditor will not be left alone with the system. The auditor will not type any commands on the system console or perform any changes on the system. A system administrator in charge of the system should type the commands requested by the auditor. All these measures are recommended to prevent any future accusations that the system was modified during the audit.

This is the list of documents presented during the preliminary meeting:

- “Information Sensitivity Policy” (please see [Appendix A](#))
- “Sirius Ethics Policy” (please see [Appendix B](#))
- “Sirius – InfoSec Acceptable Use Policy” (please see [Appendix C](#))
- “Sirius Password Policy” (please see [Appendix D](#))
- “InfoSec Laptop Security Tips” (please see [Appendix E](#))
- “Sirius – Standard Operating Procedure-Secure Laptop Configuration” (please see [Appendix F](#))
- “Setting up john the ripper” (please see [Appendix G](#))
- “Setting up Nessus” (please see [Appendix H](#))

Once the auditor gathers as much data as possible and the organization and the auditor know what they are going to accomplish, the audit process can begin.

## Identification of the System to be Audited

David Hoelzer conveyed to us during the SANS Track 7 course, that “the scope or auditable identity is the definition of what it is we are actually responsible for evaluating or administering.”<sup>2</sup>

Based on this explanation, the defined target system for this report is an auditor’s laptop, Dell Latitude CS 200 laptop running Fedora Core 2 as the only operating system. The laptop is the main tool Sirius Inc., gives to the auditor to perform his/her job.

I would like to point out that the system utilized for this report is an old system and does not have the optimum hardware to provide the best performance with the tools installed in it. However, since the main purpose for this report is to provide a methodology to conduct a security audit for this auditor’s laptop, the same methodology and principles can be applied to a laptop with newer or better hardware configuration.

## Computer Model, Operating System & Software Installed

### Hardware

Model: Dell Latitude CS 200

CPU: Mobile Pentium II

Speed: 396 MHz

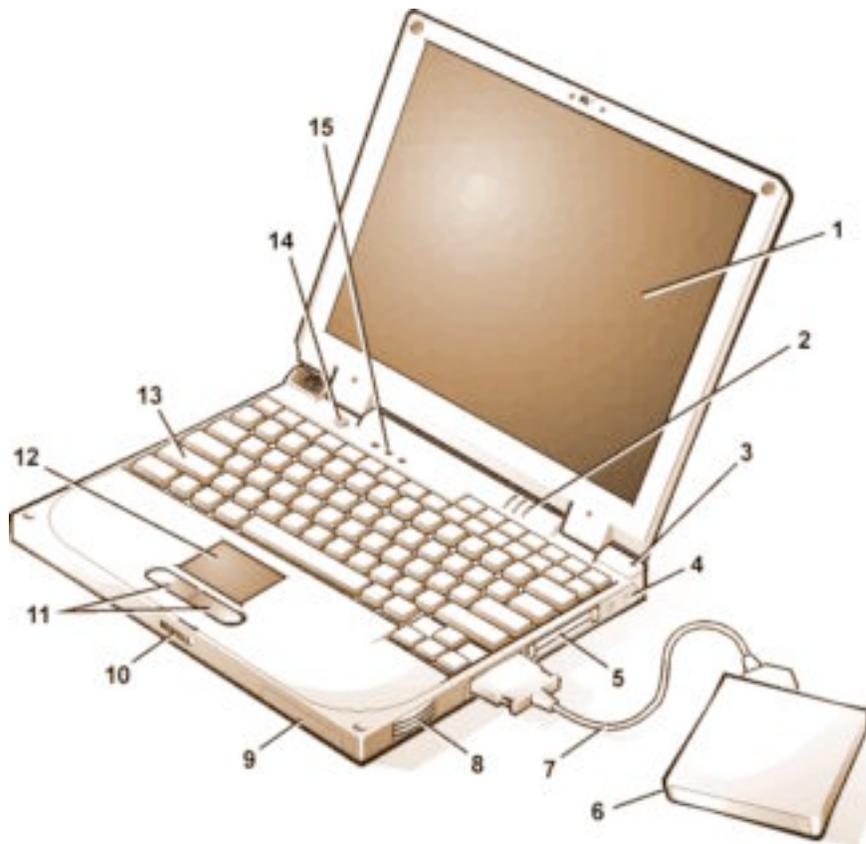
Memory: 128 MD SDRAM 66 MHz

Ports: Parallel, VGA, PS/2, USB, Docking connector

Cards: PCMCIA modem & 10/100 Base T combo card

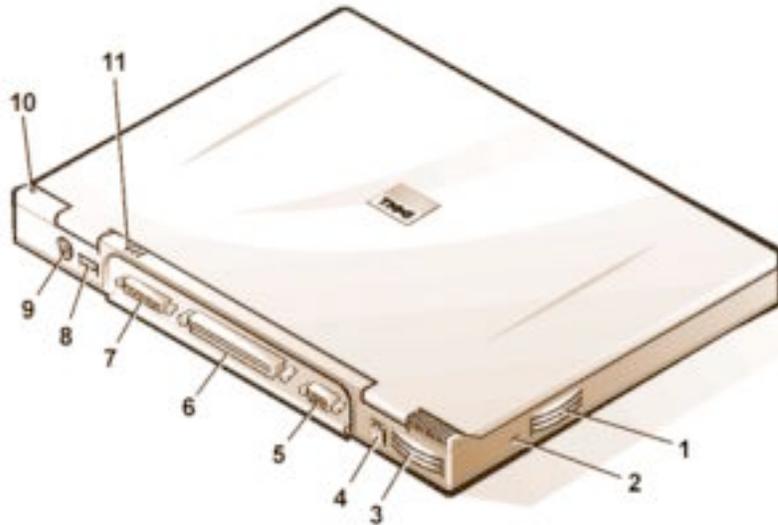
The Introduction: Dell™ Latitude™ CS/CSx Portable Computers User's Guide from Dell Inc.’s support website provides diagrams of the laptop and its features.<sup>3</sup>

**Figure 1.1 - Front/Right View of the Computer**



1 Display	9 Hard-disk drive bay
2 System status indicators (3)	10 Display latch
3 Integrated microphone	11 Touch pad buttons
4 Audio jacks (2)	12 Touch pad
5 PC Card slots (2)	13 Keyboard
6 External media bay	14 Power button
7 Media bay cable (attached to media bay connector on computer)	15 Keyboard status indicators (3)
8 Speaker	

**Figure 1.2 - Back/Left View of the Computer**



1 Air vent	7 Parallel connector
2 Security cable slot	8 USB connector
3 Air vent	9 PS/2 connector
4 AC adapter connector	10 Integrated microphone
5 Video connector	11 System status indicators
6 Docking connector	

**OS & Main Software Applications**

OS: Fedora Release 2 – i386 base

Office Suite: Open Office

Graphics Tools: Dia, Gimp

Anti-Virus: Panda Antivirus for Linux Version 7.01.00-1 08/2004

## The Purpose of the System

The laptop is mainly used as a tool for various auditing or security assessment tasks, as well as for general office work (i.e., access e-mails, browse the Internet, write documents/spreadsheets/graphs).

The laptop needs to connect to Sirius' network, to clients' networks and to the auditor's home network.

At different times, the system may contain clients' sensitive and confidential information collected during assessments, audits and analysis projects.

The laptop has various tools for security analysis and audits. These are some of the tools installed:

Port scanner: Nmap  
Password cracker tool: john the ripper  
System auditing tools: Nessus, tripwire  
Packet filters/firewalls: iptables  
Sniffer: snort, tcpdump  
Other miscellaneous tools: md5sum, chkrootkit

It is important to keep in mind that the auditor's laptop may have privileged access to customer's networks and may be used to run scans that could cause damage to the customer's systems in the event that the tools are not used and set up properly.

## Evaluate the Risk to the System

In the publication Risk Management Guide for Information Technology Systems, the authors Stonebumer, Goguen and Feringa define **Risk** as "a function of the **likelihood** of a given **threat-source's** exercising a particular potential **vulnerability**, and the resulting **impact** of that adverse event on the organization."<sup>4</sup>

Stonebumer, Goguen and Feringa further explain that in order to determine the possible occurrence or likelihood of a future adverse event, the threats to the IT system must be analyzed in combination with the vulnerabilities and the controls that the system has in place to protect it. An important aspect they take into account when performing a risk assessment is the evaluation of the impact or

extent of the damage inflicted on the system and resources if the threat takes advantage of the vulnerability.

In the previous sections I identified the system and its purpose. In the following sections, I will analyze the different variables that determine the risk of that system, following steps 2 through 7 from the methodology that Stonebumer, Goguen and Feringa proposed in their document:

- Step 2 – Threat Identification
- Step 3 – Vulnerability Identification
- Step 4 – Control Analysis
- Step 5 – Likelihood Determination
- Step 6 – Impact Analysis
- Step 7 – Risk Determination<sup>5</sup>

Note: I will follow all the steps, although in a slightly different order.

## Threats Identified

Stonebumer, Goguen and Feringa state that a threat does not represent a risk if there is no vulnerability to exploit. But they elaborate even further and point at **threat-source** as another component of the threat. They define threat-source as “either (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) a situation and method that may accidentally trigger a vulnerability.”<sup>6</sup>

In order to identify threats of the auditing system, I will analyze it from two points of view. First, I consider the laptop as an auditing tool and the threats that it could pose to the environments where it plugs in, and the systems that it audits. Second, I outline the general considerations of a laptop.

### The Laptop as an Auditing Tool

A system that is used for security audits and assessments requires tools and applications that must be used carefully. Many of these tools analyze known vulnerabilities and have the capacity to exploit them. For that reason, the tools need to have appropriate settings to avoid damaging or disrupting the systems that need to be analyzed.

Take Nessus for example, a well known open source auditing tool. This tool is very versatile and it is capable of discovering thousands of security vulnerabilities

thanks to its features set and plug-ins. Each of the plug-ins tests the target system based on a known vulnerability and the application compares the response against stored values. Unfortunately the same power that helps the auditor find vulnerabilities, can intentionally or accidentally cause system crashes and denial of service. Harry Anderson on his article "Introduction to Nessus," describes this issue:

"Plug-ins are categorized in several different and sometimes confusing ways. One method of plug-in grouping is by category. Most importantly, some plug-ins are categorized as Dangerous/Denial of Service (DOS). These plug-ins will actually perform a DOS attack and crash systems that have these particular problems. Needless to say these should not be blindly run on production systems."<sup>7</sup>

Some well known auditing tools like l0phtcrack and john the ripper allow the user to crack passwords. Other tools like tcpdump and ethereal allow the user to view the content of packets in a network and gather sensitive information. Many of the tools that can be used to diagnose and analyze, can be used for nefarious purposes.

In short, not only do these tools have to be set up and used properly, but the information gathered must be treated with outmost care and must be kept strictly confidential.

### **General Threats to Laptop**

Since a laptop is a mobile asset, it faces different threats than a large asset that can be physically secured and properly guarded. The nature of the auditor's job requires constant traveling, which increases considerably the probability of getting the laptop stolen or damaged.

According to the 2003 CSI/FBI Computer Crime and Security Surveys, laptop theft resulted in a financial loss of \$6,830,500 within the surveyed companies.<sup>8</sup> This same category showed some improvement on the 2004's survey indicating that laptop theft resulted in financial loss of \$6,734,500.<sup>9</sup> One could speculate that the slight improvement from 2003 to 2004 could indicate that training and awareness programs might be producing good results. On the other hand, it is important to emphasize that the survey also indicates a significant decline on the percentage of organizations that reported security incidents to law enforcement. 51% of the respondents cited "Negative publicity would hurt stock/image" as the main reason for not reporting the incident to law enforcement.<sup>10</sup> Needless to say, laptop theft and its negative consequences are very important matters to consider.

A lot of the times, people traveling with laptops are not as careful or as vigilant as they should, which presents the perfect opportunity that thieves can take advantage of.

Louwers and VanDenburgh in their article Data Confidentiality in an Electronic Environment, highlight a very important point “the cost of a laptop is immaterial in comparison to the potential loss of proprietary data.”<sup>11</sup> This matter applies directly to the nature of the auditor’s laptop, as it might hold clients’ confidential information.

Laptops left unattended even for a few minutes, present the perfect opportunity for a simple thief or a sophisticated industrial spy. Louwers and VanDenburgh give us numerous examples in their article, some of which had ample news media coverage:

- “Qualcomm’s CEO had his laptop stolen at a presentation to national business journalists. He left his laptop (containing highly sensitive company documents) unattended at the podium as he spoke directly with journalists after his presentation.
- The U.S. State Department had a laptop stolen from its Washington, D.C., headquarters. The stolen laptop contained names of foreign agents working for the U.S. government.
- A recent Justice Department audit revealed the loss of over 400 laptop computers containing sensitive information involving ongoing investigations.
- As a summer forest fire raged outside the Los Alamos nuclear lab, the hard drives for the laptops of the U.S. nuclear response team were discovered missing and possibly stolen. The hard drives were later found in an unsecured area that had previously been searched. Even when hardware is recovered, there is always the possibility that data has been copied.
- Visa has had repeated problems with laptop thefts. In 1996, Visa International had a laptop containing 314,000 client account numbers stolen from its California facility. The thief simply walked off with the laptop in the normal course of a workday.”<sup>12</sup>

In the case of Sirius, our small auditing and consulting firm, it is vital to analyze the risk of the laptop given to the auditor, so the proper controls or mitigation measures can be put in place to avoid theft or accidental disclosure of information.

Thomas R. Peltier in his book Information Security Risk Analysis<sup>13</sup> presents a long list of threats with their respective definitions. From his list, I compiled three tables: Human Threat, Operational Threats and Environmental Threats. These

are some examples that are applicable to the auditor's laptop. Obviously in reality the list is endless, but for practical purposes I grouped them in a way that could include as many events as possible.

**Table 1.1 - Human Threats**

<b>Human Threats</b>	
<b>Accidental</b>	<b>Intentional</b>
Alteration of Data	Alteration of Data
Data Corruption	Data Corruption
Denial of Service	Denial of Service
Disclosure of Information	Disclosure of Information
	Employee Sabotage
Theft	Theft
Unauthorized Access	Unauthorized Access
Unauthorized Use	Unauthorized Use
User Error	User Error
	Vandalism

**Table 1.2 - Operational Threats**

<b>Operational Threats</b>	
<b>Accidental</b>	<b>Intentional</b>
Alteration of Data	Alteration of Data
Alteration of Software	Alteration of Software
Application Error	
Data Corruption	Data Corruption
Hardware failure	
Operating System Crash	
System Overload	

**Table 1.3 - Human Threats**

<b>Environmental Threats</b>
Electrical fluctuations
Extreme Temperatures
Fire
Flood
Lightning
Liquid Spills
Strong Impacts

## Vulnerabilities identified

Stonebumer, Goguen and Feringa define **vulnerability** as “a flaw or weakness in system security procedures, design, implementation or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system’s security policy.”<sup>14</sup>

This definition gives a good framework to select the possible weaknesses that could affect the laptop. The list that contains all the possible vulnerabilities for a specific system could be as long as the imagination allows and could range from clearly identified conditions, to highly unlikely events like a meteor crash or abduction by aliens. To list all those vulnerabilities is not practical. Therefore, I narrowed the list to generic known conditions and disregarded the highly unlikely events. For example, I will use “Not secure configuration of OS or application” to group conditions like: allowing Remote Procedure Calls (RPC), running unnecessary services, allowing clear text connections like telnet or tftp, etc. Although, I am using generic conditions in this section, I will expand and list some specific conditions in the next chapters and steps of the audit.

For clarity’s sake, I will also group the potential vulnerabilities or generic conditions into three categories: Management-Human, Operational and Environmental.

### Management-Human Vulnerabilities

- Lack of policies, procedures and guidelines
- Lack of Training
- Lack of Security Awareness program
- No background checks
- Terminated employees
- Lack of employee satisfaction
- Overloaded employees

### Operational Vulnerabilities

- Misconfigured OS or application
- Un-patched OS or application
- Lack of adequate access controls
- Encryption application not deployed
- Disabled or out-of-date virus scanner
- Weak Authentication
- Non-secure connections
- Not adequate backup process

### Environmental Vulnerabilities

- Lack of Physical Security
- No protection from electrical fluctuation or outage

- Equipment is unable to withstand extreme temperatures
- Equipment not protected against liquids spills
- Equipment is unable to withstand strong impacts
- Portability of the equipment

The section “The Twenty Most Critical Internet Security Vulnerabilities” from the [SANS website](#)<sup>15</sup> offers a very good source of information about the most critical vulnerabilities in the Internet.

This SANS Top-20 2004 is actually two Top Ten lists: the ten most commonly exploited vulnerable services in Windows and the ten most commonly exploited vulnerable services in UNIX and Linux. Although there are thousands of security incidents each year affecting these operating systems, the overwhelming majority of successful attacks target one or more of these twenty vulnerable services.<sup>16</sup>

In the SANS’ list we find the following specific vulnerabilities that are relevant to this laptop’s audit:

#### U3 – Authentication

Passwords, pass phrases and/or security codes are used in virtually every interaction between users and information systems. Most forms of user authentication, as well as file and data protection, rely heavily on user or vendor supplied passwords. The most common password vulnerabilities are:

- User accounts that have weak or nonexistent passwords;
- User accounts with widely known or openly displayed passwords;
- System or software created administrative level accounts with widely known, weak, or nonexistent passwords; and
- Weak or well known password hashing algorithms and/or user password hashes that are stored with weak security and that are visible to anyone.<sup>17</sup>

The U3 – Authentication vulnerability falls under the category: Operational Vulnerability (Weak Authentication) from the list above. Other examples in this category are non-expiring passwords, and authentication processes over insecure networks that pass credentials in the clear.

#### U10 – Kernel

The core component operating systems is the kernel. The kernel is responsible for a number of low level interactions between the operating system and hardware, memory, scheduling, interprocess communications, file systems, and others. Because the kernel has privileged access to all aspects of the system, a kernel level compromise can be devastating. Risks from kernel vulnerabilities include Denial of service, execution of

arbitrary code with system privileges, unrestricted access to the file system, or root level access. Many vulnerabilities are exploitable remotely, and are especially dangerous when the avenue of attack is by way of a provided service published to the Internet. In some cases, by sending a malformed icmp packet, the kernel could get stuck in a loop, consuming all of the CPU resources and rendering the machine useless, causing a Denial of Service.<sup>18</sup>

For the purpose of my analysis, I considered the U10 – Kernel vulnerability under the categories Operational - Un-patched OS and in some cases misconfigured OS, from the list shown before.

We can also find numerous vulnerabilities at the SecurityFocus' web site "<http://www.securityfocus.com/bid/>"<sup>19</sup>, where it is possible to query vulnerabilities by vendor, version and title. Most of the listed vulnerabilities fall under the category "Un-patched OS or application."

There are other great sources of information about well known vulnerabilities. Some of them are:

The United States Computer Emergency Readiness Team: <http://www.us-cert.gov/>

The Common Vulnerability and Exposures site: <http://cve.mitre.org/>

## Determination of Impact and Risk as a Result of Realized Threats

After establishing the lists of threats and vulnerabilities, it is necessary to determine the **likelihood** of occurrence of those threats and the **impact** they will have on the system in the event that they take advantage of the system's weaknesses.

Stonebumer, Goguen and Feringa, provide a method to determine the likelihood and impact.<sup>20</sup> They explain that in order to estimate or rate the probability that a vulnerability may be used, it is necessary to consider three factors:

- The capacity and motivation of the threat
- The nature of the vulnerability
- The controls in place and their effectiveness to protect and mitigate the vulnerability

The consideration of these factors determines the likelihood rated into 3 levels: high, medium and low, according to the capacity of the threat to exercise the vulnerability and or the controls in place are not capable to stop the threat.

The other variable that needs consideration according to the method presented is the impact that a threat will have on the system in the event that it uses a vulnerability. The authors consider that in addition to the evaluation of the system's and the data's criticality and sensitivity, it is necessary to examine the negative results that the event produces in the light of the security goals: integrity, availability and confidentiality.

- **“Loss of Integrity.** System and data integrity refers to the requirement that information be protected from improper modification.
- **Loss of Availability.** Loss of system functionality and operational effectiveness.
- **Loss of Confidentiality.** System and data confidentiality refers to the protection of information from unauthorized disclosure.”<sup>21</sup>

Stonebumer, Goguen and Feringa also classify the impact in three levels: high, medium and low, according to the cost and effort that it takes to repair the resulting damage. Repairing the damage is not only considered the repairs to equipment or data. It also entails financial cost due to legal action against the organization, PR cost to repair the erosion to the credibility and public's trust in the organization, etc.

By comparing the different likelihood levels against the impact levels, Stonebumer, Goguen and Feringa provide a Risk-Level Matrix that helps us calculate and determine the risk to the system.

**Table 1.4 – Risk-Level Matrix**<sup>22</sup>

Threat Likelihood	Impact		
	Low (10)	Medium (50)	High (100)
High (1.0)	Low 10 x 1.0 = 10	Medium 50 x 1.0 = 50	High 100 x 1.0 = 100
Medium (0.5)	Low 10 x 0.5 = 5	Medium 50 x .5 = 25	Medium 100 x 0.5 = 50
Low (0.1)	Low 10 x 0.1 = 1	Low 50 x 0.1 = 5	Low 100 x 0.1 = 10

*Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (>1 to 10)*

By pairing the different threats, vulnerabilities, the likelihood of occurrence and the impact on the system in the following table, I will estimate the possible risk of the auditor's laptop. Unfortunately, there is no scientific and exact way to determine risk. At best, what we can do research, find statistics and gather data from trusted sources to help us get a better sense of the reality and variables that can affect a specific system.

© SANS Institute 2004, Author retains full rights.

**Table 1.5 – Estimating Risk: Pairing Vulnerabilities, Threats, Likelihood and Impact**

<b>Vulnerability</b>	<b>Threats</b>	<b>Possible Outcome</b>	<b>Likelihood</b>	<b>Impact</b>	<b>Risk</b>
Lack of policies and procedures	Disclosure of Information	<ul style="list-style-type: none"> <li>▪ Legal and economic penalties</li> <li>▪ Negative effect on reputation &amp; credibility</li> </ul>	High 1.0	High 100	High 100
	User error	<ul style="list-style-type: none"> <li>▪ Loss of productivity</li> <li>▪ Affect relationship with customer</li> </ul>	Medium 0.5	Medium 50	Medium 25
	Alteration of data	<ul style="list-style-type: none"> <li>▪ Loss of productivity</li> <li>▪ Affect relationship with customer</li> </ul>	Medium 0.5	Medium 50	Medium 25
Lack of training	Disclosure of Information	<ul style="list-style-type: none"> <li>▪ Legal and economic penalties</li> <li>▪ Negative effect on reputation &amp; credibility</li> </ul>	Medium 0.5	Medium 50	Medium 25
	User error	<ul style="list-style-type: none"> <li>▪ Loss of productivity</li> <li>▪ Affect relationship with customer</li> </ul>	High 1.0	Medium 50	Medium 50
	Alteration of data	<ul style="list-style-type: none"> <li>▪ Loss of productivity</li> <li>▪ Affect relationship with customer</li> </ul>	High 1.0	Medium 50	Medium 50
Lack of security awareness program	Disclosure of Information	<ul style="list-style-type: none"> <li>▪ Legal and economic penalties</li> <li>▪ Negative effect on reputation &amp; credibility</li> </ul>	High 1.0	High 100	High 100
	Theft	<ul style="list-style-type: none"> <li>▪ Loss of equipment</li> <li>▪ Loss of data</li> <li>▪ Legal and economic penalties</li> <li>▪ Negative effect on reputation &amp; credibility</li> </ul>	Medium 0.5	High 100	High 50

Vulnerability	Threats	Possible Outcome	Likelihood	Impact	Risk
No background checks	Disclosure of Information	<ul style="list-style-type: none"> <li>▪ Legal and economic penalties</li> <li>▪ Negative effect on reputation &amp; credibility</li> </ul>	Medium 0.5	High 100	High 50
	Alteration of data	<ul style="list-style-type: none"> <li>▪ Loss of productivity</li> <li>▪ Affect relationship with customer</li> </ul>	Medium 0.5	High 100	High 50
	Theft	<ul style="list-style-type: none"> <li>▪ Loss of equipment</li> <li>▪ Loss of data</li> <li>▪ Legal and economic penalties</li> <li>▪ Negative effect on reputation &amp; credibility</li> </ul>	Medium 0.5	High 100	High 50
Terminated Employee	Theft	<ul style="list-style-type: none"> <li>▪ Loss of equipment</li> <li>▪ Loss of data</li> <li>▪ Legal and economic penalties</li> <li>▪ Negative effect on reputation &amp; credibility</li> </ul>	Medium 0.5	High 100	High 50
	Alteration of data	<ul style="list-style-type: none"> <li>▪ Loss of productivity</li> <li>▪ Affect relationship with customer</li> </ul>	Medium 0.5	High 100	High 50
	Vandalism	<ul style="list-style-type: none"> <li>▪ Loss of equipment</li> <li>▪ Loss of data</li> <li>▪ Loss of productivity</li> </ul>	Medium 0.5	High 100	High 50
	Unauthorized access	<ul style="list-style-type: none"> <li>▪ Loss of data</li> <li>▪ Disclosure of Information</li> <li>▪ Legal and economic penalties</li> <li>▪ Negative effect on reputation &amp; credibility</li> </ul>	Medium 0.5	High 100	High 50

Vulnerability	Threats	Possible Outcome	Likelihood	Impact	Risk
Lack of employee satisfaction	User error	<ul style="list-style-type: none"> <li>▪ Loss of productivity</li> <li>▪ Affect relationship with customer</li> </ul>	Medium 0.5	Medium 50	Medium 25
	Sabotage	<ul style="list-style-type: none"> <li>▪ Loss of equipment</li> <li>▪ Loss of data</li> <li>▪ Loss of productivity</li> </ul>	Medium 0.5	Medium 50	Medium 25
Overloaded employee	Accidental user error	<ul style="list-style-type: none"> <li>▪ Loss of productivity</li> <li>▪ Affect relationship with customer</li> </ul>	High 1.0	Medium 50	Medium 50
	Accidental alteration of data or data corruption	<ul style="list-style-type: none"> <li>▪ Loss of productivity</li> <li>▪ Affect relationship with customer</li> </ul>	High 1.0	Medium 50	Medium 50
	Liquid spills	<ul style="list-style-type: none"> <li>▪ Loss of equipment</li> <li>▪ Loss of productivity</li> </ul>	Medium 1.0	Medium 50	Medium 50
	Strong impact	<ul style="list-style-type: none"> <li>▪ Loss of equipment</li> <li>▪ Loss of productivity</li> </ul>	Medium 1.0	Medium 50	Medium 50
Misconfigured OS or application	Unauthorized access	<ul style="list-style-type: none"> <li>▪ Loss of data</li> <li>▪ Disclosure of Information</li> <li>▪ Legal and economic penalties</li> <li>▪ Negative effect on reputation &amp; credibility</li> </ul>	High 1.0	High 100	High 100
	Alteration of data or data corruption	<ul style="list-style-type: none"> <li>▪ Loss of data</li> <li>▪ Loss of productivity</li> <li>▪ Affect relationship with customer</li> </ul>	High 1.0	High 100	High 100
	Operating system crash	<ul style="list-style-type: none"> <li>▪ Loss of data</li> <li>▪ Loss of productivity</li> </ul>	Medium 1.0	Medium 50	Medium 50

Unpatched OS or application	Unauthorized access	<ul style="list-style-type: none"> <li>▪ Loss of data</li> <li>▪ Disclosure of Information</li> <li>▪ Legal and economic penalties</li> <li>▪ Negative effect on reputation &amp; credibility</li> </ul>	High 1.0	High 100	High 100
	Alteration of data or data corruption	<ul style="list-style-type: none"> <li>▪ Loss of data</li> <li>▪ Loss of productivity</li> <li>▪ Affect relationship with customer</li> </ul>	High 1.0	High 100	High 100
	Operating system or application crash	<ul style="list-style-type: none"> <li>▪ Loss of data</li> <li>▪ Loss of productivity</li> </ul>	Medium 0.5	Medium 50	Medium 25
Lack of adequate access controls	Unauthorized access	<ul style="list-style-type: none"> <li>▪ Loss of data</li> <li>▪ Disclosure of Information</li> <li>▪ Legal and economic penalties</li> <li>▪ Negative effect on reputation &amp; credibility</li> </ul>	Medium 0.5	High 100	High 50
	Alteration of data or data corruption	<ul style="list-style-type: none"> <li>▪ Loss of data</li> <li>▪ Loss of productivity</li> <li>▪ Affect relationship with customer</li> </ul>	Low 0.1	Medium 50	Low 5
	Unauthorized use	<ul style="list-style-type: none"> <li>▪ Loss of data</li> <li>▪ Loss of productivity</li> <li>▪ Disclosure of Information</li> <li>▪ Legal and economic penalties</li> </ul>	Medium 0.5	High 100	High 50
Encryption application not deployed (or used)	Disclosure of Information	<ul style="list-style-type: none"> <li>▪ Legal and economic penalties</li> <li>▪ Negative effect on reputation &amp; credibility</li> </ul>	High 1.0	High 100	High 100
Disabled or out-of-date virus scanner. <u>Note:</u> At	Unauthorized access	<ul style="list-style-type: none"> <li>▪ Loss of data</li> <li>▪ Disclosure of Information</li> </ul>	Low 0.1	High 100	Low 10

this moment viruses for this Linux are less common than for Windows.		<ul style="list-style-type: none"> <li>▪ Legal and economic penalties</li> <li>▪ Negative effect on reputation &amp; credibility</li> </ul>			
<b>Vulnerability</b>	<b>Threats</b>	<b>Possible Outcome</b>	<b>Likelihood</b>	<b>Impact</b>	<b>Risk</b>
Disabled or out-of-date virus scanner <u>Note:</u> this is a Linux laptop. At this moment virus for this OS are less common than for Windows.	Disclosure of Information	<ul style="list-style-type: none"> <li>▪ Legal and economic penalties</li> <li>▪ Negative effect on reputation &amp; credibility</li> </ul>	Low 0.1	High 100	Low 10
	Alteration of data or data corruption	<ul style="list-style-type: none"> <li>▪ Loss of data</li> <li>▪ Loss of productivity</li> <li>▪ Affect relationship with customer</li> </ul>	Low 0.1	High 100	Low 10
	Denial of Service	<ul style="list-style-type: none"> <li>▪ Loss of productivity</li> <li>▪ Affect relationship with customer</li> <li>▪ Negative effect on reputation &amp; credibility</li> </ul>	Low 0.1	High 100	Low 10
Weak authentication	Unauthorized access	<ul style="list-style-type: none"> <li>▪ Loss of data</li> <li>▪ Disclosure of Information</li> <li>▪ Legal and economic penalties</li> <li>▪ Negative effect on reputation &amp; credibility</li> </ul>	Medium 0.5	High 100	High 50
Non-secure connections	Disclosure of Information	<ul style="list-style-type: none"> <li>▪ Legal and economic penalties</li> <li>▪ Negative effect on reputation &amp; credibility</li> </ul>	High 1.0	High 100	High 100
	Alteration of data or data corruption	<ul style="list-style-type: none"> <li>▪ Loss of data</li> <li>▪ Loss of productivity</li> <li>▪ Affect relationship with customer</li> </ul>	Medium 0.5	High 100	High 50
Not adequate backup	Alteration of data or data	<ul style="list-style-type: none"> <li>▪ Loss of data</li> </ul>	Low	Medium	Low

process	corruption	<ul style="list-style-type: none"> <li>Loss of productivity</li> <li>Affect relationship with customer</li> </ul>	0.1	50	5
Lack of physical security	Theft	<ul style="list-style-type: none"> <li>Loss of equipment</li> </ul>	High 1.0	High 100	High 100
<b>Vulnerability</b>	<b>Threats</b>	<b>Possible Outcome</b>	<b>Likelihood</b>	<b>Impact</b>	<b>Risk</b>
Lack of physical security	Theft	<ul style="list-style-type: none"> <li>Loss of data</li> <li>Loss of productivity</li> <li>Affect relationship with customer</li> </ul>	High 1.0	High 100	High 100
	Disclosure of Information	<ul style="list-style-type: none"> <li>Legal and economic penalties</li> <li>Negative effect on reputation &amp; credibility</li> </ul>	High 1.0	High 100	High 100
	Unauthorized access	<ul style="list-style-type: none"> <li>Loss of data</li> <li>Disclosure of Information</li> <li>Legal and economic penalties</li> <li>Negative effect on reputation &amp; credibility</li> </ul>	High 1.0	High 100	High 100
No protection from electrical fluctuation or outage	Electrical fluctuation	<ul style="list-style-type: none"> <li>Loss of equipment</li> <li>Loss of data</li> <li>Loss of productivity</li> </ul>	Low 0.1	Medium 50	Low 5
Equipment is unable to withstand extreme temperatures	Equipment operated or left in a place without proper temperature control	<ul style="list-style-type: none"> <li>Loss of equipment</li> <li>Loss of data</li> <li>Loss of productivity</li> </ul>	Low 0.1	Medium 50	Low 5
Equipment not protected against liquid spills	Liquid spills	<ul style="list-style-type: none"> <li>Loss of equipment</li> <li>Loss of data</li> <li>Loss of productivity</li> </ul>	Low 0.1	Medium 50	Low 5
Equipment is unable to withstand strong impacts	Dropped laptop or laptop left on roof of car and user drives away	<ul style="list-style-type: none"> <li>Loss of equipment</li> <li>Loss of data</li> <li>Loss of productivity</li> </ul>	Low 0.1	Medium 50	Low 5
Portability of equipment	Theft	<ul style="list-style-type: none"> <li>Loss of data</li> <li>Disclosure of Information</li> </ul>	High 1.0	High 100	High 100

		<ul style="list-style-type: none"><li>▪ Legal and economic penalties</li><li>Negative effect on reputation &amp; credibility</li></ul>			
--	--	--	--	--	--

© SANS Institute 2004, Author retains full rights.

## Summary of Identified Risks

In order to have a focused and controlled audit, I concentrated on the High risk items (Risk = 100) from the Table 1.5 – “Estimating Risk: Pairing Vulnerabilities, Threats, Likelihood and Impact”.

The following table summarizes those high risk items. There is an exception to the high risk scale. At the time of writing, there are less virus and Trojan applications written for Linux, compared to the amount of viruses written for an operating system like Windows. Therefore at the moment, the risk can be considered low. Since “less” does not mean “non-existent” and the current situation could rapidly change with Linux’s growing popularity, Sirius Inc., prefers to not take the risk and requires up-to-date virus scanner as part of the default laptop configurations. Hence, I added this item to the list of risks that need to be checked during the audit process.

**Table 1.6 – High Risk Summary**

<b>Risk Code</b>	<b>Vulnerability</b>
H1	Lack of policies and procedures
H2	Lack of security awareness
O1	Misconfigured OS or application
O2	Unpatched OS or application
O3	Encryption application not deployed
O4	Disabled or out-of-date virus scanner
E1	Lack of physical security
E2	Portability of the equipment

In order to tie the summary of risks with the different items that I will have in the Check List section, I added a “risk code”. The risk code is a simple combination of letter and a sequential number. The letter is an abbreviation of their respective classification: **H** = human, **O** = operational, **E** = environmental.

In the following section, I will present a list of resources that provide information or guides related to security best practices.

### State of Practice for the Laptop running Fedora C2

If we consider the long history of Unix, and the 13 years of evolution and great contribution from millions of people to Linux since Linus Torvald decided to write his own operating system, we have an invaluable amount of accumulated experience and knowledge that we can tap into.

The problem is that it is easy to get lost, given the amount of information available. Therefore, it is recommended to go to reputable and well know sources of information, to find guidance about best security practices and secure implementation.

Some of those great sources of information are organizations like: National Institute of Security Standards (NIST); SysAdmin, Audit, Network, Security (SANS) Institute; the Center for Internet Security (CIS); Most of these sites provide links to other trusted sources of information.

NIST - Computer Security Division's sites offer very good documentation:  
Computer Security Resource Center (CSRC) Technology Security –  
Practices & Checklists / Implementation Guides  
<http://csrc.nist.gov/pcig/cig.html><sup>23</sup>

Security Configuration Checklist Program for IT Products  
<http://checklists.nist.gov/><sup>24</sup>

The Center for Internet Security (CIS): Benchmark/Tools, CIS Level-1  
Benchmark and Scoring Tool for Linux  
[http://www.cisecurity.org/bench\\_linux.html](http://www.cisecurity.org/bench_linux.html)<sup>25</sup>

This site offers a great step-by-step guide or benchmark to secure a Linux system. It is also possible to download a scoring tool "CISscan-1.4.2-1.0.i386.rpm" that can test the implemented security against the benchmark and provides a report and score. Individuals can download these tools and documents without cost, but they need to read carefully the "**Agreed Terms of Use**", to avoid any copyright and intellectual property law infringements.

Another excellent guide for secure Linux configurations is SANS' "Securing Linux: A Survival Guide for Linux Security."<sup>26</sup>

SANS InfoSec Reading Room web site <http://www.sans.org/rr/> and the Global Information Assurance Certification (GIAC) Posted Practicals site <http://www.giac.org/cert.php>, offer a great amount of documents from different Information Security topics.

BASTILLE <http://www.bastille-linux.org/><sup>27</sup>

Bastille is a great hardening script that can be used on different Linux distributions like Red Hat, Debian, Mandrake, SuSE and TurboLinux. They also have versions that support HP-UX and Mac OS X.

The users can run the tool on a verbose mode, providing text that explains each specific step in the hardening process and how that vulnerability can be exploited. It not only helps users run more secure systems, but at the same time it is an instructional tool for the community.

Unfortunately, at the time of this writing there is no tested version for Fedora. For that reason I did not run the script on the laptop. Although, considering the great service that Bastille offers, it was worth mentioning.

### **State of Practice for the Auditing Tool**

Again, it is important to consider the purpose of the system and the tools installed in it. There is an incredible amount of tools available over the Internet that can be used for analysis, discovery, troubleshooting, testing, etc. There are very important issues to keep in mind with those applications.

There are hackers in the security community that are highly skilled, they like to share and help the community with their findings or their experience. They develop and/or improve tools and warn the community about possible problems or vulnerabilities with existing operating systems, applications, protocols, etc.

Unfortunately, some hackers (some people call them: crackers) like to modify the source code of those tools and applications in a negative way. They install back doors and even install malicious code in them. Therefore, it is crucial to get those tools from reliable sources and if possible verify their respective digital signatures or their md5hashes before installing them.

Sources of tools and applications:

- Fedora's download site:  
<http://download.fr.fedora.us/fedora/fedora/2/i386/RPMS.stable/>
- Freshmeat:  
<http://freshmeat.net/>
- Nessus:  
[http://www.nessus.org/nessus\\_2\\_2.html](http://www.nessus.org/nessus_2_2.html)
- A hacker's site with a large number of security tools - Insecure.org:  
<http://www.insecure.org/tools.html>
- Security Focus – Tools Archive:  
<http://www.securityfocus.com/tools>

- Tools and applications for Fedora Core 2:  
<http://newrpms.sunsite.dk/apt/redhat/en/i386/fc2/RPMS.newrpms/>

Other Resources:

- SANS Reading Room:  
<http://www.sans.org/rr/>
- A book about security tools for people that need a place to start:  
Mike Shema, Bradley C. Johnson, "Anti-Hacker Tool Kit, Second Edition",  
(New York: McGraw-Hill/Osborne, 2004)
- A more advanced book about security concepts:  
Cyrus Peikari, Anton Chuvakin, "Security Warrior" (Sebastopol: O'Reilly,  
2004), p.190-198.
- These are introductory articles about Nessus and its basic configuration:  
Harry Anderson, "Introduction to Nessus", SecurityFocus, October 23, 2003,  
URL: <http://www.securityfocus.com/printable/infocus/1741>  
Harry Anderson, "Nessus, Part2: Scanning", SecurityFocus, December 16,  
2003, URL: <http://www.securityfocus.com/printable/infocus/1753>  
Harry Anderson, "Nessus, Part3: Analyzing Reports", SecurityFocus,  
December 16, 2003, URL:  
<http://www.securityfocus.com/printable/infocus/1759>
- A complete book about Nessus from the same author of the tool:  
Renaud Deraison, Raven Alder, Jimmy Alderson, Andy Johnston, George A.  
Theall, "NESSUS Network Auditing", (Rockland: Syngress Publishing, Inc.,  
2004)
- Security News and newsgroups - Infosyssec:  
<http://www.infosyssec.com/infosyssec/>
- Edgeos Inc., has a very nice compilation of security tools:  
[http://www.edgeos.com/resources/supported\\_apps/](http://www.edgeos.com/resources/supported_apps/)

On the next section, I will present information about different controls and how they can help mitigate or reduce the vulnerabilities of the system that I am analyzing.

## Control Analysis

In this section, I will analyze the controls that Sirius has in place in an attempt to reduce the likelihood of threats exercising previously identified vulnerabilities.

Stonebumer, Goguen and Feringa in their publication present two control methods or categories:

**Technical Controls** are safeguards that are incorporated into computer hardware, software or firmware (e.g., access control mechanisms, identification and authentication mechanisms, encryption methods, intrusion detection software). **Non-Technical Controls** are management and operational controls, such as security policies; operational procedures, physical and environmental security.”<sup>28</sup>

In addition to the control methods, the authors also present 2 subcategories:

“**Preventive Controls** inhibit attempts to violate security policy and include such control as access control enforcement, encryption, and authentication. **Detective Controls** warn of violations or attempted violations of security policy and include such controls as audit trails, intrusion detection methods, and checksums.”<sup>29</sup>

Organizations may choose to use a combination of these methods and subcategories of controls. For example, organizations can have a technical controls like password rules at the OS level, to enforce a non-technical control like a security password policy.

I will layout the control categories mentioned before in the following list, and I will use these categories in the audit check list of section 2 of this document.

### List of Control Categories

Technical	
<b>Preventive</b>	<b>Detective</b>
<ul style="list-style-type: none"><li>Authentication controls</li><li>Protected communications</li><li>File/Directory encryption</li><li>Enforcement of access controls (Application, OS &amp; system configuration)</li></ul>	<ul style="list-style-type: none"><li>Access controls and configuration audits</li><li>Intrusion detection systems</li><li>Virus detection and eradication</li></ul>
Non-technical	
<b>Preventive</b>	<b>Detective</b>
<ul style="list-style-type: none"><li>Policies, SOPs (Ethical use, Data classification, Ethical use, Laptop)</li></ul>	<ul style="list-style-type: none"><li>Environmental Controls (smoke detectors, alarms, security)</li></ul>

- configuration, Security tips)
- Tutorials (encryption primers)
- Security awareness programs
- Personnel security controls (separation of duties, least privilege, computer access registration and termination)
- Locks and security cables (server racks/enclosures with locks, security cables to tie laptop, locked cabinets)
- systems, temperature controls)
- Periodic system audits
- Periodic and revision of security controls

I would like to emphasize that technical controls without clearly defined security policies to follow, can easily fail in their efforts to protect, as these controls don't have the appropriate direction. Organizations can have the best technology at their disposal, but these solutions (i.e., applications, appliances, systems) might not be as efficient or could be poorly implemented. Without clear policies, the controls could be set as lax, or as strict as the person setting the system considers it necessary that day. At best, these controls can impose random rules on users with varied degrees of restrictions. It is like attempting to obtain a goal without defining success.

Julie Allen in her book, "The CERT Guide To System and Network Security Practices", states this same principle:

"Security policies define the rules that regulate how your organization manages and protects its information and computing resources to achieve security objectives."<sup>30</sup>

In a few words, in order to have a strong foundation for good security practices, organizations need to be aware that technical controls are simply the enforcement of its own security policies.

Since policies and procedures are so important, I will re-examine them on the Section 2 -Audit Check List of this document.

## Section 2 – Audit Check List

### Scope

In order to identify the scope, I bring back the definition of auditing that I highlighted in the “Abstract” section of this document:

*“Auditing is a measure of conformance”<sup>31</sup>*

With that definition in mind, the objective is to elaborate a check list that evaluates if Sirius has clearly defined security policies, procedures and guidelines and most importantly, if our target system - the auditor’s laptop, conforms to those policies and procedures.

### Conventions and Format

The system commands are presented in bold courier-new font:

```
# apt-get --version
```

The system’s responses to the commands are presented in normal courier-new:

```
# apt-get 3.425.xx for fedora Berkley
```

During the audit process it is important to use tools that are independent from the ones installed in the target system. For that reason the auditing tools, should either be downloaded from a trusted source and mounted as “read only”, or better yet burn a CD with all the tools, mount the CD and use those tools. I used a CD that has a large collection of trusted tools in a directory `/audit-tools`.

For example the site NetAdminTools.com “Building a Security Audit Toolkit”, URL: <http://www.netadmintools.com/part279.html><sup>32</sup>, offers a good step-by-step guide to prepare a trusted chkrootkit toolkit. The site provides detailed information about all the different tools that chkrootkit needs in static form (awk, cut, echo, egrep, find, head, id, ls, netstat, ps, strings, sed, and uname), so the chkrootkit uses those static applications instead of the ones installed in the system.

Mounting the CD with the trusted audit tools and copying them:

```
# cd /  
# mount /dev/cdrom /mnt  
# cp /mnt/audit-tools /tmp  
# umount /dev/cdrom  
# cd /tmp
```

We now have in the /tmp directory a copy of /audit-tools from the CD that I will use for the audit.

The full path of the applications that we need to use will always be /tmp/audit-tools or /tmp/audit-tools/bin.

For example, I will present in the check list:

```
# awk
```

In reality the application used was the one located at:

```
# /tmp/audit-tools/awk
```

I will only write the entire path, whenever I consider it is necessary to avoid confusion.

## Checklist Item Template

The different items in the checklist will follow the format presented by William Karwisch in his research paper for auditing a corporate e-mail gateway.<sup>33</sup>

Checklist Item -1. Checklist name	
<b>Reference:</b>	Indicates the source of the checklist item.
<b>Control Category:</b>	Indicates the type of control, according to the <b>List of Control Categories</b> presented in the previous section
<b>Risk Code:</b>	Indicates the vulnerability being checked with this test from <b>Table 1.6</b>
<b>Compliance:</b>	Indicates how the compliance is evaluated
<b>Testing:</b>	Provides a testing procedure
<b>Test Type:</b>	Specifies if it is Objective vs. Subjective and/or Stimulus-Response
<b>Evidence:</b>	Provides results from the test
<b>Status:</b>	Pass or Fail
<b>Findings &amp; Comments:</b>	Conclusions drawn from the evidence

The last 3 items of the checklist (Evidence, Status, Findings & Comments) will not be included in this section as they will be addressed on “Section 3 – Audit Testing, Evidence and Findings.”

## Check List

Checklist Item -1. Defined Security Policies	
<b>Reference:</b>	“SANS Institute Policy Project”, <a href="http://www.sans.org/resources/policies/">http://www.sans.org/resources/policies/</a> “Securing Linux A Survival Guide for Linux Security” <sup>34</sup> and best security practices.
<b>Control</b>	Non-Technical, Preventive

<b>Category:</b>	
<b>Risk Code:</b>	H1
<b>Compliance:</b>	The security policies are the foundation of any security program. They provide the rules that the members of the organization must follow. Sirius must have well defined security policies.
<b>Testing:</b>	The policies must clearly convey purpose, scope, as well as, general statements that guide the members of an organization. It cannot be too detailed or provide specific technologies.
<b>Test Type:</b>	Subjective
<b>Evidence:</b>	<Information presented on Section 3>
<b>Status:</b>	<Information presented on Section 3>
<b>Findings &amp; Comments:</b>	<Information presented on Section 3>

<b>Checklist Item -2. Security Tips or Guidelines</b>	
<b>Reference:</b>	“SANS Institute Policy Project”: Is it a Policy, a Standard or a Guideline?, <a href="http://www.sans.org/resources/policies/#name">http://www.sans.org/resources/policies/#name</a>
<b>Control Category:</b>	Non-Technical, Preventive
<b>Risk Code:</b>	H2
<b>Compliance:</b>	Documents that server as “guidelines” are a series of recommendations about well known practices.
<b>Testing:</b>	The guidelines are suggestions about well known security practices. The document must provide clear advice and promote awareness.
<b>Test Type:</b>	Subjective
<b>Evidence:</b>	<Information presented on Section 3>
<b>Status:</b>	<Information presented on Section 3>
<b>Findings &amp; Comments:</b>	<Information presented on Section 3>

<b>Checklist Item -3. Laptop Install Procedure</b>	
<b>Reference:</b>	“SANS Institute Policy Project”: Is it a Policy, a Standard or a Guideline?, <a href="http://www.sans.org/resources/policies/#name">http://www.sans.org/resources/policies/#name</a>
<b>Control Category:</b>	Non-Technical, Preventive
<b>Risk Code:</b>	H1
<b>Compliance:</b>	“Procedures are detailed, documented step-by-step actions to be taken to achieve a specific task” <sup>35</sup>
<b>Testing:</b>	The document must clearly convey purpose, requirements, as well as, detail steps to follow.
<b>Test Type:</b>	Subjective
<b>Evidence:</b>	<Information presented on Section 3>
<b>Status:</b>	<Information presented on Section 3>
<b>Findings &amp; Comments:</b>	<Information presented on Section 3>

<b>Checklist Item -4. BIOS – Password Protected</b>	
<b>Reference:</b>	David Koconis, Jim Murray, Jos Purvis, Darrim Wassom, “Securing Linux A Survival Guide for Linux Security” <sup>36</sup>
<b>Control Category:</b>	Technical, Preventive
<b>Risk Code:</b>	O1
<b>Compliance:</b>	The BIOS communicates between the OS and the computer’s hardware. The laptop must require a password during startup process (before OS boot loader).
<b>Testing:</b>	Password is necessary to modify the BIOS settings and get to the boot loader
<b>Test Type:</b>	Objective
<b>Evidence:</b>	<Information presented on Section 3>
<b>Status:</b>	<Information presented on Section 3>
<b>Findings &amp; Comments:</b>	<Information presented on Section 3>

<b>Checklist Item -5. Boot Loader – Password Protected</b>	
<b>Reference:</b>	David Koconis, Jim Murray, Jos Purvis, Darrim Wassom, “Securing Linux A Survival Guide for Linux Security.”
<b>Control Category:</b>	Technical, Preventive
<b>Risk Code:</b>	O1
<b>Compliance:</b>	The laptop must require password during the boot up time and before it loads the operating system.
<b>Testing:</b>	Boot loader will fail until correct password is entered. And /etc/grub.conf must not have clear text password stored in it.
<b>Test Type:</b>	Objective and Stimulus-Response
<b>Evidence:</b>	<Information presented on Section 3>
<b>Status:</b>	<Information presented on Section 3>
<b>Findings &amp; Comments:</b>	<Information presented on Section 3>

<b>Checklist Item -6. Check for rootkits</b>	
<b>Reference:</b>	<a href="http://www.chkrootkit.org/">http://www.chkrootkit.org/</a> <sup>37</sup> <a href="http://www.netadmintools.com/part279.html">http://www.netadmintools.com/part279.html</a> <sup>38</sup>
<b>Control Category:</b>	Technical, Detective
<b>Risk Code:</b>	O4
<b>Compliance:</b>	The <code>chkrootkit</code> is a tool (shell script) that looks for signatures of root kits installed (i.e., trojaned or infected system binaries) in the target system. Instructions found at NetAdminTools.com “Building a Security Audit Toolkit”, URL:

	<a href="http://www.netadmintools.com/part279.html">http://www.netadmintools.com/part279.html</a> <sup>39</sup> A clean output should show “not infected” or “no suspect files” or “nothing found” next to the list of files analyzed.
<b>Testing:</b>	Run the command: <pre># ./chkrootkit</pre> As suggested at the NetAdmintools.com site, it is recommended to run a chkrootkit tool that uses trusted binaries and applications. <pre># ./chkrootkit -p /tmp/audit-tools/bin</pre> “-p” provides the path to the trusted binaries where we copied the CD audit tools and applications as explained in the section above “Conventions and Format”
<b>Test Type:</b>	Objective and Stimulus-Response
<b>Evidence:</b>	<Information presented on Section 3>
<b>Status:</b>	<Information presented on Section 3>
<b>Findings &amp; Comments:</b>	<Information presented on Section 3>

<b>Checklist Item -7. No Empty Passwords</b>	
<b>Reference:</b>	David Koconis, Jim Murray, Jos Purvis, Darrim Wassom, “Securing Linux A Survival Guide for Linux Security” <sup>40</sup>
<b>Control Category:</b>	Technical, Preventive
<b>Risk Code:</b>	O1
<b>Compliance:</b>	All user accounts in the system must require a password to login.
<b>Testing:</b>	Accounts with empty passwords put the system at risk. To check that the second field of the /etc/shadow file is blank enter the following command: <pre># awk -F: '(\$2 == "") {print \$1}' /etc/shadow</pre> The output list the accounts that do not have a password set.
<b>Test Type:</b>	Objective and Stimulus-Response
<b>Evidence:</b>	<Information presented on Section 3>
<b>Status:</b>	<Information presented on Section 3>
<b>Findings &amp; Comments:</b>	<Information presented on Section 3>

<b>Checklist Item -8. Password Strength</b>	
<b>Reference:</b>	Mike Shema, Bradley C. Johnson, “Anti-Hacker Tool Kit” <sup>41</sup> (John the Ripper)
<b>Control Category:</b>	Technical, Preventive
<b>Risk Code:</b>	O1
<b>Compliance:</b>	Passwords that do not comply with the organization’s password policy will be easier to crack. I used the password cracking tool John the

	Ripper. In theory with the appropriate time and resources, passwords can get cracked. I will assume that if "john the ripper" is not able to crack the passwords within 1 hour, they are considered strong enough.
<b>Testing:</b>	Do not use the application already installed in the laptop. Use the john the ripper application located in /tmp. Run the trusted application against a copy of /etc/shadow for 1 hour  <pre># cp /etc/shadow /home/yoly/laptop-audit/shadow-audit # cd /tmp/audit-tools/john-1.6/src/run # ./john /home/yoly/laptop-audit/shadow-audit</pre> The previous command runs the application john the ripper against the file "shadow-audit"  <b>Test::</b> The application john the ripper needs to run for 1 hour and must not be able to crack the passwords.
<b>Test Type:</b>	Objective and Stimulus-Response
<b>Evidence:</b>	<Information presented on Section 3>
<b>Status:</b>	<Information presented on Section 3>
<b>Findings &amp; Comments:</b>	<Information presented on Section 3>

<b>Checklist Item -9. Disabled Xinetd Services (telnet, ftp, rpc, shell, rsh, login, rlogin, tfpt, imap, pop3)</b>	
<b>Reference:</b>	David Koconis, Jim Murray, Jos Purvis, Darrim Wassom, "Securing Linux A Survival Guide for Linux Security" <sup>42</sup>
<b>Control Category:</b>	Technical, Preventive
<b>Risk Code:</b>	O1
<b>Compliance:</b>	Xinetd services (telnet, ftp, rpc, shell, rsh, login, rlogin, tfpt, imap, pop3) should be turned off.
<b>Testing:</b>	Xinetd managed applications all store their configuration files in the /etc/xinetd.d directory. Each configuration file has a "disable" statement which can be set to either "yes" or "no". This governs whether xinetd is allowed to start them or not.  <pre># netstat -a   grep &lt;service name&gt;</pre> The service should not be listening. There should be no output from this command.  To confirm, also run the tool <b>nmap</b> from another workstation with the following command:

	<pre> <b>nmap -sT -PT -PI -F -vv -T 3 &lt;IP address of target host&gt;</b>  The following options are listed in the <b>nmap</b> man pages:  -sT    TCP connect() scan: This is the most basic form of TCP scanning.  -PT    Use TCP "ping" to determine what hosts are up. Instead of sending ICMP echo request packets and waiting for a response, we spew out TCP ACK packets throughout the target network (or to a single machine) and then wait for responses to trickle back. Hosts that are up should respond with a RST.  -PI    This option uses a true ping (ICMP echo request) packet.  -F     Fast scan mode.  -vv    Very verbose mode. -T     &lt;Paranoid Sneaky Polite Normal Aggressive Insane&gt; These are canned timing policies for conveniently expressing your priorities to Nmap. Normal is the default Nmap behaviour, which tries to run as quickly as possible without overloading the network or missing hosts/ports... You can also reference these by number (0-5). For example, '-T 0' gives you Paranoid mode and '-T 5' is Insane mode.  Run with T3 option: normal </pre>
<b>Test Type:</b>	Objective & Stimulus-Response
<b>Evidence:</b>	<Information presented on Section 3>
<b>Status:</b>	<Information presented on Section 3>
<b>Findings &amp; Comments:</b>	<Information presented on Section 3>

<b>Checklist Item -10. Disabled Boot Services</b>	
<b>Reference:</b>	"Linux Benchmark v1.1.0", July 29, 2003, Center for Internet Security (CIS) <sup>43</sup>
<b>Control Category:</b>	Technical, Preventive
<b>Risk Code:</b>	O1
<b>Compliance:</b>	Exploits can take advantage of vulnerable services that are running in the machine. If the services are not necessary, it is better to turn them off to reduce the risk.
<b>Testing:</b>	Check the services that are currently configured to start when the system boots. <code># /sbin/chkconfig --list</code>
<b>Test Type:</b>	Objective & Stimulus-Response
<b>Evidence:</b>	<Information presented on Section 3>
<b>Status:</b>	<Information presented on Section 3>
<b>Findings &amp; Comments:</b>	<Information presented on Section 3>

<b>Checklist Item -11. Auditing Applications Installed</b>	
<b>Reference:</b>	Personal Experience. There are many tools that can be used during an audit process. I am listing some of the most commons ones that I have used. Most of these tools were explained and/or utilized at the SANS Track 7 course "Auditing Networks, Perimeters and Systems." <sup>44</sup>
<b>Control Category:</b>	Technical
<b>Risk Code:</b>	O1
<b>Compliance:</b>	The audit laptop needs at least the following tools installed in it: <ul style="list-style-type: none"> <li>• Chkrootkit – Tool to detect trojaned binaries, sniffer logs, and rootkit configuration files</li> <li>• Ethereal – graphical front end to packet-capture applications</li> <li>• john the ripper – password cracker application</li> <li>• nessus – remote vulnerability scanner</li> <li>• netstat – application that shows the network status</li> <li>• Nmap – port scanner, OS fingerprinting application</li> <li>• md5sum – integrity checker application</li> <li>• ping – basic network diagnostic tool</li> <li>• snort – intrusion detection system</li> <li>• tcpdump – command line packet sniffer</li> <li>• tripwire – file system integrity checker. Host-based intrusion detection system</li> <li>• whois – tool that queries whois databases for information about a domain name or an IP address</li> </ul>
<b>Testing:</b>	The application must be found either with: <code># rpm -qa   grep &lt;application&gt;</code> or doing a <code>find</code> or <code>which &lt;application&gt;</code>
<b>Test Type:</b>	Objective & Stimulus-Response
<b>Evidence:</b>	<Information presented on Section 3>

<b>Status:</b>	<Information presented on Section 3>
<b>Findings &amp; Comments:</b>	<Information presented on Section 3>

<b>Checklist Item -12. Nessus Proper Configuration</b>	
<b>Reference:</b>	Renaud Deraison, Raven Alder, Jimmy Alderson, Andy Johnston, George A. Theall, "NESSUS Network Auditing", (Rockland: Syngress Publishing, Inc., 2004)  Harry Anderson, "Introduction to Nessus", SecurityFocus, October 23, 2003, URL: <a href="http://www.securityfocus.com/printable/infocus/1741">http://www.securityfocus.com/printable/infocus/1741</a>
<b>Control Category:</b>	Technical, Preventive
<b>Risk Code:</b>	O1
<b>Compliance:</b>	The server and client need to be properly set up according to the set up guidelines provided. Please see <b>Appendix H</b> .
<b>Testing:</b>	Provide the nessusd.conf file to check the options enabled and their configuration according to best practices to avoid a Denial of Service on the target systems, and according to the capacity of the laptop. *safe_checks must be enabled The max_threads and max_checks options need to be set to low numbers. This will result on slow scans, but it is necessary since the laptop does not have an optimum hardware configuration.  Verify that the gui client application works correctly.
<b>Test Type:</b>	Objective
<b>Evidence:</b>	<Information presented on Section 3>
<b>Status:</b>	<Information presented on Section 3>
<b>Findings &amp; Comments:</b>	<Information presented on Section 3>

<b>Checklist Item -13. OS &amp; Applications with latest patches installed</b>	
<b>Reference:</b>	"The Twenty Most Critical Internet Security Vulnerabilities (Updated)" URL: <a href="http://www.sans.org/top20/">http://www.sans.org/top20/</a> <sup>45</sup> "Red Hat Linux 9: Red Hat Linux Security Guide" URL: <a href="http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/security-guide/ch-security-update">http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/security-guide/ch-security-update</a> up2date Agent - is a program for updating packages on Red Hat Linux yum – yellowdog updater modified
<b>Control Category:</b>	Technical, Preventive
<b>Risk Code:</b>	O2
<b>Compliance:</b>	The laptop must be up to date on patch levels for the OS and applications installed in it
<b>Testing:</b>	To check that the laptop has the latest patches we can use either up2date or yum. For up2date use the following command line: <code># up2date -uv</code> "-u, --update" Completely update the system. All relevant packages will be downloaded (a

	<p>possibly installed, if you have configured Update Agent to do so).  “-v, - -verbose” print more information about what Update Agent is doing.</p> <p>For yum (yellow dog updater, modified)  <b># yum check-update</b>  “check-update” downloads a complete set of headers for base packages for Fedora Core as any released updates for Fedora Core.  <b># yum upgrade</b>  “upgrade” will present a list of packages that will be upgraded, newly installed, and obsolete. Choose “y” will download and install the packages. Yum will inform when there aren’t new packages to install.</p> <p>For compliance the laptop must have the latest versions and updates of the applications and not require any new updates for install</p>
<b>Test Type:</b>	Objective & Stimulus-Response
<b>Evidence:</b>	<Information presented on Section 3>
<b>Status:</b>	<Information presented on Section 3>
<b>Findings &amp; Comments:</b>	<Information presented on Section 3>

<b>Checklist Item -14. Encryption Application Deployed</b>	
<b>Reference:</b>	According to Sirius policy (please see Appendix A) data classified as Restricted Confidential must be protected while it is stored in the laptop.
<b>Control Category:</b>	Technical, Preventive
<b>Risk Code:</b>	O3
<b>Compliance:</b>	The laptop must have an asymmetric key encryption application installed and configured. GnuPG is a very good open source application. It can be used for file encryption, digital signature/verification.
<b>Testing:</b>	Check that the gnupg rpm is installed. Another alternative to gnupg (or gpg) is KGpg. KGpg is a KDE GUI version compatible with gnupg. It was designed by Jean-Baptiste Mardelle. The encryption application should be installed and configured.
<b>Test Type:</b>	Objective and Stimulus-Response
<b>Evidence:</b>	<Information presented on Section 3>
<b>Status:</b>	<Information presented on Section 3>
<b>Findings &amp; Comments:</b>	<Information presented on Section 3>

<b>Checklist Item -15. Installed Virus Scanner</b>	
<b>Reference:</b>	Virus attacks are not classified as high risk for this system at the

	moment, but as the popularity of this operating system continues growing, viruses will become a bigger problem.
<b>Control Category:</b>	Technical, Detective
<b>Risk Code:</b>	O4
<b>Compliance:</b>	A virus scanner must be installed on the laptop. A Linux version of the software can be found at: <a href="http://www.pandasoftware.com/download/">http://www.pandasoftware.com/download/</a>
<b>Testing:</b>	The laptop must have the pavcl - Panda Antivirus for Linux 7.0-1. from Panda Software International Check with: <pre># rpm -qa   grep -i pav</pre>
<b>Test Type:</b>	Objective & Stimulus-Response
<b>Evidence:</b>	<Information presented on Section 3>
<b>Status:</b>	<Information presented on Section 3>
<b>Findings &amp; Comments:</b>	<Information presented on Section 3>

<b>Checklist Item -16. Laptop Steel Cable</b>	
<b>Reference:</b>	Personal experience.
<b>Control Category:</b>	Non-Technical, Preventive
<b>Risk Code:</b>	E1, E2
<b>Compliance:</b>	<p>Sirius provides to all laptop users a laptop steel cable to secure as an additional physical security measure.</p>  <p><b>Note:</b> Laptop cable - picture source: Innovative Security Products Inc., <a href="http://www.wesecure.com/">http://www.wesecure.com/</a><sup>47</sup></p> <p>Although this control is not infallible it is a deterrent and a preventive measure.</p>

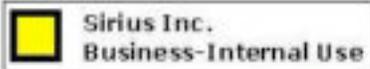
<b>Testing:</b>	User needs to have the cable and explain how it is used.
<b>Test Type:</b>	Objective
<b>Evidence:</b>	<Information presented on Section 3>
<b>Status:</b>	<Information presented on Section 3>
<b>Findings &amp; Comments:</b>	<Information presented on Section 3>

© SANS Institute 2004, Author retains full rights.

## Section 3 – Audit Testing, Evidence and Findings

### Results of the Audit

Note: The entire checklist item will not be included in this section. I will only present the evidence, status and findings.

<b>Checklist Item -1. Defined Security Policies</b>	
<b>Evidence:</b>	During the preliminary meeting Sirius provided the following policies: “Information Sensitivity Policy” (please see <a href="#">Appendix A</a> ); “Ethics Policy” (please <a href="#">Appendix B</a> ); “InfoSec Acceptable Use Policy” (please <a href="#">Appendix C</a> ); “Password Policy” (please <a href="#">Appendix D</a> ).
<b>Status:</b>	Pass
<b>Findings &amp; Comments:</b>	Needs signature as evidence that the employee read the policy. The documents clearly define the purpose and scope. They are easy to understand.  All the documents provided follow the requirements indicated in the “Information Sensitivity Policy”. For example all documents presented are tagged with the “Business-Internal Use” tag:  

<b>Checklist Item -2. Security Tips or Guidelines</b>	
<b>Evidence:</b>	Sirius provided the document: “InfoSec Laptop Security Tips” ( <a href="#">Appendix E</a> ).
<b>Status:</b>	Pass
<b>Findings &amp; Comments:</b>	The document provides clear information and it promotes security awareness.

<b>Checklist Item -3. Laptop Install Procedure</b>	
<b>Evidence:</b>	Sirius provided the document: “Standard Operating Procedure Secure Laptop Configuration” ( <a href="#">Appendix F</a> ).
<b>Status:</b>	Pass
<b>Findings &amp; Comments:</b>	The document is clear and explains all the steps that are necessary to perform the basic installation and correct the most important vulnerabilities. The CIS “Linux Benchmark v 1.1.0” provides additional settings and configurations to make the system more secure.

<b>Checklist Item -4. BIOS – Password Protected</b>	
<b>Evidence:</b>	The laptop requires a password during system startup.

<b>Status:</b>	Fail
<b>Findings &amp; Comments:</b>	During the test, the laptop did not require the password at startup time. It went directly into the boot loader screen. This is a very important preventive measure and needs to be set up.

<b>Checklist Item -5. Boot Loader – Password Protected</b>	
<b>Evidence:</b>	During system boot up in order to load the OS installed GRUB requires to enter a password.  /etc/grub.conf has the following entry in it:  password --md5 \$1\$pjUtZ0\$dD00WfISdkHXivPXaI81c0
<b>Status:</b>	Pass
<b>Findings &amp; Comments:</b>	The boot loader requires a password to load the OS and the password is not stored in clear text in the boot loader configuration file. It provides additional protection in the event that the laptop gets stolen.

<b>Checklist Item -6. Check for rootkits</b>	
<b>Evidence:</b>	<pre># ./chkrootkit -p /tmp/audit-tools/bin ROOTDIR is '/' Checking `amd'... not found Checking `basename'... not infected Checking `biff'... not found Checking `chfn'... not infected Checking `chsh'... not infected Checking `cron'... not infected Checking `date'... not infected Checking `du'... not infected Checking `dirname'... not infected Checking `echo'... not infected Checking `egrep'... not infected Checking `env'... not infected Checking `find'... not infected Checking `fingerd'... not found Checking `gpm'... not infected Checking `grep'... not infected Checking `hdparm'... not infected Checking `su'... not infected Checking `ifconfig'... not infected Checking `inetd'... not tested Checking `inetdconf'... not found Checking `identd'... not found Checking `init'... not infected Checking `killall'... not infected Checking `ldsopreload'... not infected</pre>

```

Checking `login'... not infected
Checking `ls'... not infected
Checking `lsof'... not infected
Checking `mail'... not infected
Checking `mingetty'... not infected
Checking `netstat'... not infected
Checking `named'... not found
Checking `passwd'... not infected
Checking `pidof'... not infected
Checking `pop2'... not found
Checking `pop3'... not found
Checking `ps'... not infected
Checking `pstree'... not infected
Checking `rpcinfo'... not infected
Checking `rlogind'... not found
Checking `rshd'... not found
Checking `slogin'... not infected
Checking `sendmail'... not infected
Checking `sshd'... not infected
Checking `syslogd'... not infected
Checking `tar'... not infected
Checking `tcpd'... not infected
Checking `tcpdump'... not infected
Checking `top'... not infected
Checking `telnetd'... not found
Checking `timed'... not found
Checking `traceroute'... not infected
Checking `vdir'... not infected
Checking `w'... not infected
Checking `write'... not infected
Checking `aliens'... no suspect files
Searching for sniffer's logs, it may take a while... nothing
Searching for HiDrootkit's default dir... nothing found
Searching for t0rn's default files and dirs... nothing found
Searching for t0rn's v8 defaults... nothing found
Searching for Lion Worm default files and dirs... nothing fo
Searching for RSHA's default files and dir... nothing found
Searching for RH-Sharpe's default files... nothing found
Searching for Ambient's rootkit (ark) default files and dirs
found
Searching for suspicious files and dirs, it may take a while
/usr/lib/perl5/vendor_perl/5.8.3/i386-linux-thread-multi/aut
/usr/lib/perl5/5.8.3/i386-linux-thread-multi/.packlist /usr/
3.3/etc/settings/.qt_plugins_3.3rc.lock /usr/lib/qt-
3.3/etc/settings/.qtrc.lock /lib/modules/2.6.7-
1.494.2.2/build/scripts/.sumversion.o.cmd /lib/modules/2.6.7-
1.494.2.2/build/scripts/.elfconfig.h.cmd /lib/modules/2.6.7-

```

```

1.494.2.2/build/scripts/kconfig/.libkconfig.so.cmd /lib/modu
1.494.2.2/build/scripts/kconfig/.conf.o.cmd /lib/modules/2.6
1.494.2.2/build/scripts/kconfig/.mconf.o.cmd /lib/modules/2.
1.494.2.2/build/scripts/kconfig/.zconf.tab.o.cmd /lib/module
1.494.2.2/build/scripts/kconfig/.conf.cmd /lib/modules/2.6.7
1.494.2.2/build/scripts/.pnmtologo.cmd /lib/modules/2.6.7-
1.494.2.2/build/scripts/.empty.o.cmd /lib/modules/2.6.7-
1.494.2.2/build/scripts/.modpost.o.cmd /lib/modules/2.6.7-
1.494.2.2/build/scripts/basic/.fixdep.cmd /lib/modules/2.6.7
1.494.2.2/build/scripts/basic/.docproc.cmd /lib/modules/2.6.
1.494.2.2/build/scripts/basic/.split-include.cmd /lib/module
1.494.2.2/build/scripts/.kallsyms.cmd /lib/modules/2.6.7-
1.494.2.2/build/scripts/.conmakehash.cmd /lib/modules/2.6.7-
1.494.2.2/build/scripts/.modpost.cmd /lib/modules/2.6.7-
1.494.2.2/build/scripts/.bin2c.cmd /lib/modules/2.6.7-
1.494.2.2/build/scripts/.mk_elfconfig.cmd /lib/modules/2.6.7
1.494.2.2/build/scripts/.file2alias.o.cmd /lib/modules/2.6.7
1.494.2.2/build/.config /lib/modules/2.6.8-
1.521/build/scripts/mod/.sumversion.o.cmd /lib/modules/2.6.8
1.521/build/scripts/mod/.elfconfig.h.cmd /lib/modules/2.6.8-
1.521/build/scripts/mod/.empty.o.cmd /lib/modules/2.6.8-
1.521/build/scripts/mod/.modpost.o.cmd /lib/modules/2.6.8-
1.521/build/scripts/mod/.modpost.cmd /lib/modules/2.6.8-
1.521/build/scripts/mod/.mk_elfconfig.cmd /lib/modules/2.6.8
1.521/build/scripts/mod/.file2alias.o.cmd /lib/modules/2.6.8
1.521/build/scripts/kconfig/.libkconfig.so.cmd /lib/modules/
1.521/build/scripts/kconfig/.conf.o.cmd /lib/modules/2.6.8-
1.521/build/scripts/kconfig/.mconf.o.cmd /lib/modules/2.6.8-
1.521/build/scripts/kconfig/.zconf.tab.o.cmd /lib/modules/2.
1.521/build/scripts/kconfig/.conf.cmd /lib/modules/2.6.8-
1.521/build/scripts/.pnmtologo.cmd /lib/modules/2.6.8-
1.521/build/scripts/basic/.fixdep.cmd /lib/modules/2.6.8-
1.521/build/scripts/basic/.docproc.cmd /lib/modules/2.6.8-
1.521/build/scripts/basic/.split-include.cmd /lib/modules/2.
1.521/build/scripts/.kallsyms.cmd /lib/modules/2.6.8-
1.521/build/scripts/.conmakehash.cmd /lib/modules/2.6.8-
1.521/build/scripts/.bin2c.cmd /lib/modules/2.6.8-1.521/buil
/lib/modules/2.6.9-1.3_FC2/build/scripts/mod/.sumversion.o.c
/lib/modules/2.6.9-1.3_FC2/build/scripts/mod/.elfconfig.h.cm
/lib/modules/2.6.9-1.3_FC2/build/scripts/mod/.empty.o.cmd
/lib/modules/2.6.9-1.3_FC2/build/scripts/mod/.modpost.o.cmd
/lib/modules/2.6.9-1.3_FC2/build/scripts/mod/.modpost.cmd
/lib/modules/2.6.9-1.3_FC2/build/scripts/mod/.mk_elfconfig.c
/lib/modules/2.6.9-1.3_FC2/build/scripts/mod/.file2alias.o.c
/lib/modules/2.6.9-1.3_FC2/build/scripts/kconfig/.libkconfig
/lib/modules/2.6.9-1.3_FC2/build/scripts/kconfig/.conf.o.cmd
/lib/modules/2.6.9-1.3_FC2/build/scripts/kconfig/.mconf.o.cm

```

```

/lib/modules/2.6.9-1.3_FC2/build/scripts/kconfig/.zconf.tab.
/lib/modules/2.6.9-1.3_FC2/build/scripts/kconfig/.conf.cmd
/lib/modules/2.6.9-1.3_FC2/build/scripts/.pnmtologo.cmd /lib
1.3_FC2/build/scripts/basic/.fixdep.cmd /lib/modules/2.6.9-
1.3_FC2/build/scripts/basic/.docproc.cmd /lib/modules/2.6.9-
1.3_FC2/build/scripts/basic/.split-include.cmd /lib/modules/
1.3_FC2/build/scripts/genksyms/.genksyms.o.cmd /lib/modules/
1.3_FC2/build/scripts/genksyms/.parse.o.cmd /lib/modules/2.6
1.3_FC2/build/scripts/genksyms/.genksyms.cmd /lib/modules/2.
1.3_FC2/build/scripts/genksyms/.lex.o.cmd /lib/modules/2.6.9
1.3_FC2/build/scripts/.kallsyms.cmd /lib/modules/2.6.9-
1.3_FC2/build/scripts/.conmakehash.cmd /lib/modules/2.6.9-
1.3_FC2/build/.config /lib/modules/2.6.5-
1.358/build/scripts/.sumversion.o.cmd /lib/modules/2.6.5-
1.358/build/scripts/.elfconfig.h.cmd /lib/modules/2.6.5-
1.358/build/scripts/kconfig/.libkconfig.so.cmd /lib/modules/
1.358/build/scripts/kconfig/.conf.o.cmd /lib/modules/2.6.5-
1.358/build/scripts/kconfig/.mconf.o.cmd /lib/modules/2.6.5-
1.358/build/scripts/kconfig/.zconf.tab.o.cmd /lib/modules/2.
1.358/build/scripts/kconfig/.conf.cmd /lib/modules/2.6.5-
1.358/build/scripts/.pnmtologo.cmd /lib/modules/2.6.5-
1.358/build/scripts/.empty.o.cmd /lib/modules/2.6.5-
1.358/build/scripts/.modpost.o.cmd /lib/modules/2.6.5-
1.358/build/scripts/basic/.fixdep.cmd /lib/modules/2.6.5-
1.358/build/scripts/basic/.docproc.cmd /lib/modules/2.6.5-
1.358/build/scripts/basic/.split-include.cmd /lib/modules/2.
1.358/build/scripts/.kallsyms.cmd /lib/modules/2.6.5-
1.358/build/scripts/.conmakehash.cmd /lib/modules/2.6.5-
1.358/build/scripts/.modpost.cmd /lib/modules/2.6.5-
1.358/build/scripts/.bin2c.cmd /lib/modules/2.6.5-
1.358/build/scripts/.mk_elfconfig.cmd /lib/modules/2.6.5-
1.358/build/scripts/.file2alias.o.cmd /lib/modules/2.6.5-1.3

Searching for LPD Worm files and dirs... nothing found
Searching for Ramen Worm files and dirs... nothing found
Searching for Maniac files and dirs... nothing found
Searching for RK17 files and dirs... nothing found
Searching for Ducoci rootkit... nothing found
Searching for Adore Worm... nothing found
Searching for ShitC Worm... nothing found
Searching for Omega Worm... nothing found
Searching for Sadmin/IIS Worm... nothing found
Searching for MonKit... nothing found
Searching for Showtee... nothing found
Searching for OpticKit... nothing found
Searching for T.R.K... nothing found
Searching for Mithra... nothing found

```

	<pre> Searching for LOC rootkit... nothing found Searching for Romanian rootkit... nothing found Searching for HKRK rootkit... nothing found Searching for Suckit rootkit... nothing found Searching for Volc rootkit... nothing found Searching for Gold2 rootkit... nothing found Searching for TC2 Worm default files and dirs... nothing fou Searching for Anonoying rootkit default files and dirs... no Searching for ZK rootkit default files and dirs... nothing f Searching for ShKit rootkit default files and dirs... nothin Searching for AjaKit rootkit default files and dirs... nothi Searching for zaRwT rootkit default files and dirs... nothin Searching for Madalin rootkit default files... nothing found Searching for anomalies in shell history files... nothing fo Checking `asp'... not infected Checking `bindshell'... INFECTED (PORTS: 3049) Checking `lkm'... nothing detected Checking `rexedcs'... not found Checking `sniffer'... eth0: PF_PACKET(/sbin/dhclient) Checking `w55808'... not infected Checking `wted'... nothing deleted Checking `scalper'... not infected Checking `slapper'... not infected Checking `z2'... nothing deleted # </pre>
<b>Status:</b>	Pass
<b>Findings &amp; Comments:</b>	<p>According to the validations provided by the application chkrootkit, the laptop does not have moment of the audit.</p> <p>I situated this check as one of the initial items on the list, as I considered very important to stages of the audit that the system had not been compromised with modified or trojaned ap we have the verification, we can trust the system more. This doesn't mean that we could tr There are other covert channels or type of rootkits that chkrootkit might not detect, but i overall detection tool.</p> <p>The laptop has the chkrootkit application installed and the user runs it when she remember validation task is very important and should be done on a regular basis.</p>

<b>Checklist Item -7. No Empty Passwords</b>	
<b>Evidence:</b>	<pre># awk -F: '(\$2 == "") {print \$1}' /etc/shadow #</pre>
<b>Status:</b>	Pass
<b>Findings &amp; Comments:</b>	There is no output list after entering the command. Therefore there are no user accounts with empty passwords. This system is compliant

<b>Checklist Item -8. Password Strength</b>	
<b>Evidence:</b>	<pre># ./john /home/yoly/laptop-audit/shadow-audit Loaded 2 passwords with 2 different salts (FreeBSD MD5 [32/32]) guesses: 0  time: 0:01:13:50 (3)  c/s: 773 trying: soupar Session aborted #</pre>
<b>Status:</b>	Pass
<b>Findings &amp; Comments:</b>	<p>According to Sirius "Password" Policy the user passwords must be at least 7 characters long and contain alphanumeric and special characters. Obviously that with enough time and resources passwords can be cracked, but a password that complies with Sirius' Password Policy is very secure and hard to crack. In this case, the tool was not able to crack the passwords in 1h and 13 min.</p>

<b>Checklist Item -9. Disabled Xinetd Services (telnet, ftp, rpc, shell, rsh, login, rlogin, tftp, imap, pop3)</b>	
<b>Evidence:</b>	<pre># netstat -a   grep telnet # # netstat -a   grep ftp # # netstat -a   grep rpc # # netstat -a   grep shell # # netstat -a   grep rsh # # netstat -a   grep login # # netstat -a   grep rlogin # # netstat -a   grep tftp # # netstat -a   grep imap # # netstat -a   grep pop3 #</pre> <p><b><u>nmap results:</u></b> I ran nmap from a windows machine in the same network. The target IP is 192.168.0.33</p>

	<pre> C:\nmap -sT -PT -PI -F -vv -T 3 192.168.0.33  Starting nmap V. 3.00 ( www.insecure.org/nmap ) Host (192.168.0.33) appears to be up ... good. Initiating Connect() Scan against (192.168.0.33) Adding open port 25/tcp Adding open port 1241/tcp Adding open port 22/tcp Adding open port 110/tcp The Connect() Scan took 434 seconds to scan 1150 ports. Interesting ports on (192.168.0.33): (The 1146 ports scanned but not shown below are in state: filtered) Port      State      Service 22/tcp    open      ssh 25/tcp    open      smtp 110/tcp   open      pop-3 1241/tcp  open      msg Nmap run completed -- 1 IP address (1 host up) scanned in 445 seconds </pre>
<b>Status:</b>	Initial Fail (pop3 accepting connections). After further analysis – final result: <b>Pass</b>
<b>Findings &amp; Comments:</b>	<p>The xinetd services listed were not listening or were not found.</p> <p>According to nmap, pop3 allows connections to it. That service is supposed to be disabled.</p> <p>To confirm that it is not allowing connections run the following command:</p> <pre>C:\telnet 192.168.0.33 110</pre> <p>The connection failed when attempting to telnet to the target host (192.168.0.33) on port 110. This is probably a false positive and will be disregarded.</p>

<b>Checklist Item -10. Disabled Boot Services</b>	
<b>Evidence:</b>	<pre> # /sbin/chkconfig --list random          0:off  1:off  2:on   3:on 4:on  5:on  6:off pcmcia          0:off  1:off  2:on   3:on 4:on  5:on  6:off rawdevices      0:off  1:off  2:off  3:on 4:on  5:on  6:off readahead       0:off  1:off  2:off  3:off 4:off  5:on  6:off yum             0:off  1:off  2:off  3:off </pre>

4:off	5:off	6:off			
nfslock		0:off	1:off	2:off	3:off
4:off	5:off	6:off			
mdmpd		0:off	1:off	2:on	3:on
4:on	5:on	6:off			
saslauthd		0:off	1:off	2:off	3:off
4:off	5:off	6:off			
netdump		0:off	1:off	2:off	3:off
4:off	5:off	6:off			
nfs		0:off	1:off	2:off	3:off
4:off	5:off	6:off			
portmap		0:off	1:off	2:off	3:off
4:off	5:off	6:off			
irqbalance		0:off	1:off	2:off	3:on
4:on	5:on	6:off			
ntpd		0:off	1:off	2:off	3:off
4:off	5:off	6:off			
syslog		0:off	1:off	2:on	3:on
4:on	5:on	6:off			
psacct		0:off	1:off	2:off	3:off
4:off	5:off	6:off			
vncserver		0:off	1:off	2:off	3:off
4:off	5:off	6:off			
netplugd		0:off	1:off	2:off	3:off
4:off	5:off	6:off			
kudzu		0:off	1:off	2:off	3:on
4:on	5:on	6:off			
sendmail		0:off	1:off	2:off	3:off
4:off	5:off	6:off			
rpcsvcgssd		0:on	1:off	2:off	3:on
4:off	5:on	6:on			
gpm		0:off	1:off	2:on	3:on
4:on	5:on	6:off			
readahead_early		0:off	1:off	2:off	3:off
4:off	5:on	6:off			
apmd		0:off	1:off	2:on	3:on
4:on	5:on	6:off			
nscd		0:off	1:off	2:off	3:off
4:off	5:off	6:off			
atd		0:off	1:off	2:off	3:off
4:off	5:off	6:off			
rpcgssd		0:on	1:off	2:off	3:on
4:off	5:on	6:on			
xinetd		0:off	1:off	2:off	3:off
4:off	5:off	6:off			
isdn		0:off	1:off	2:on	3:on
4:on	5:on	6:off			

xfst	0:off	1:off	2:on	3:on
4:on	5:on	6:off		
snmpd	0:off	1:off	2:off	3:off
4:off	5:off	6:off		
winbind	0:off	1:off	2:off	3:off
4:off	5:off	6:off		
anacron	0:off	1:off	2:on	3:on
4:on	5:on	6:off		
snmptrapd	0:off	1:off	2:off	3:off
4:off	5:off	6:off		
netfs	0:off	1:off	2:off	3:on
4:on	5:on	6:off		
rpcidmapd	0:on	1:off	2:off	3:on
4:off	5:on	6:on		
rhnsd	0:off	1:off	2:on	3:on
4:on	5:on	6:off		
lisa	0:off	1:off	2:off	3:off
4:off	5:off	6:off		
smartd	0:off	1:off	2:on	3:on
4:on	5:on	6:off		
cron	0:off	1:off	2:on	3:on
4:on	5:on	6:off		
irda	0:off	1:off	2:off	3:off
4:off	5:off	6:off		
sshd	0:off	1:off	2:on	3:on
4:on	5:on	6:off		
nessusd	0:off	1:off	2:off	3:on
4:on	5:on	6:off		
mdmonitor	0:off	1:off	2:on	3:on
4:on	5:on	6:off		
network	0:off	1:off	2:on	3:on
4:on	5:on	6:off		
acpid	0:off	1:off	2:off	3:on
4:on	5:on	6:off		
autofs	0:off	1:off	2:off	3:on
4:on	5:on	6:off		
messagebus	0:off	1:off	2:off	3:on
4:on	5:on	6:off		
iptables	0:off	1:off	2:on	3:on
4:on	5:on	6:off		
snortd	0:off	1:off	2:on	3:on
4:on	5:on	6:off		
microcode_ctl	0:off	1:off	2:off	3:on
4:on	5:on	6:off		
cpuspeed	0:off	1:on	2:on	3:on
4:on	5:on	6:off		
cups	0:off	1:off	2:on	3:on

	4:on 5:on 6:off [root@localhost /]#
<b>Status:</b>	Pass
<b>Findings &amp; Comments:</b>	This configuration passes the test. But these settings might need to get modified in the future as some applications could require services that are turned off at the moment.

<b>Checklist Item -11. Auditing Applications Installed</b>	
<b>Evidence:</b>	<pre># rpm -qa   grep ethereal ethereal-0.10.5-0.2.2 # rpm -qa   grep tcpdump tcpdump-3.8.2-6.FC2.1 # rpm -qa   grep nmap nmap-3.50-3 # rpm -qa   grep chkrootkit chkrootkit-0.44-1.1.fc2.dag # rpm -qa   grep nessus nessus-server-2.2.0-17.rhfc2.at libnessus-2.2.0.14.rhfc2.at # rpm -qa   grep snort snort-2.2.0-1.1.fc2.dag # rpm -qa   grep tripwire tripwire-2.3.1-20.fdr.1.2 # rpm -qa   grep mhash mhash-08.18-0.fdr.1.2 # rpm -qa   grep net-tools net-tools-1.60-25.1 # which netstat /bin/netstat # which ping /bin/ping # which whois /usr/bin/whois</pre>
<b>Status:</b>	Pass
<b>Findings &amp; Comments:</b>	<p>All the tools required are installed. The application <code>mhash</code> supports md5 algorithm.</p> <p>Sirius has a small document that provides the installation procedure for john the ripper (please see <a href="#">Appendix G</a>). The application was installed according to the procedure.</p>

<b>Checklist Item -12. Nessus Proper Configuration</b>	
<b>Evidence:</b>	This is the <code>nessusd.conf</code> file found on <code>/etc/nessus:</code>

```
# less nessus.conf

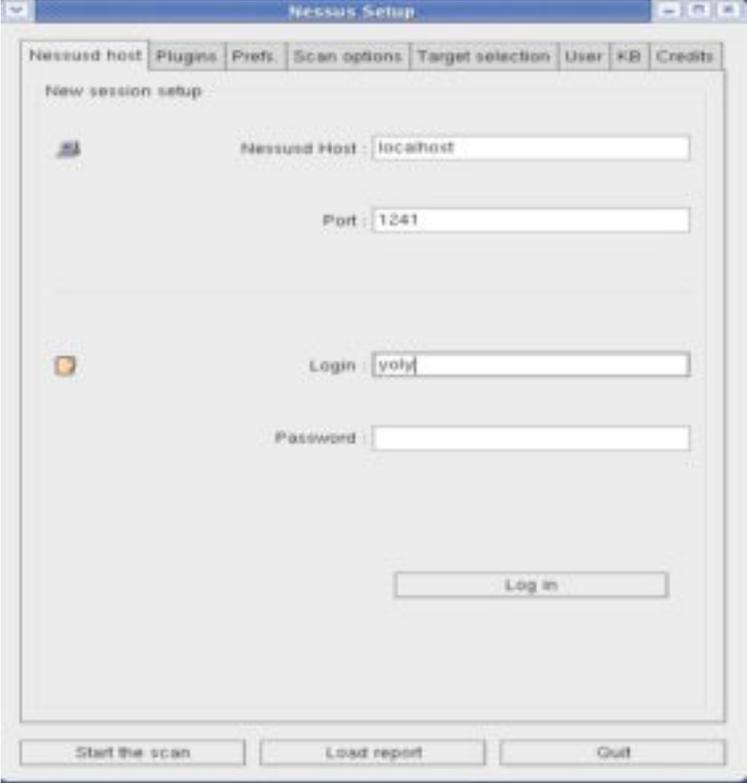
# See the manpage for nessusd(8) for more
information.
#

# Server options
plugins_folder = /usr/lib/nessus/plugins
logfile = /var/nessus/logs/nessusd.messages
max_threads = 10
users = /etc/nessus/nessusd.users
rules = /etc/nessus/nessusd.rules
### safe_checks must be enabled. Only disable
for specific tests
safe_checks = yes
language = english
#language = francais
checks_read_timeout = 5
max_checks = 5
plugins_timeout = 15
dumpfile = /dev/null
auto_enable_dependencies = yes
optimize_test = yes

# Crypto options
peks_username = nessusd
peks_keylen = 1024
peks_keyfile = /etc/nessus/nessusd.private-keys
peks_usrkeys = /etc/nessus/nessusd.user-keys
peks_pwdfail = 5

#
# Added by nessus-mkcert
#
cert_file=/usr/com/nessus/CA/servercert.pem
key_file=/var/nessus/CA/serverkey.pem
ca_file=/usr/com/nessus/CA/cacert.pem
# If you decide to protect your private key
with a password,
# uncomment and change next line
# pem_password=password
# If you want to force the use of a client
certificate, uncomment next line
# force_pubkey_auth = yes
(END)
```

Screenshot of the client login screen:

	<p>After entering command <code># nessus &amp;</code></p>  <p>The client application also shows the “safe checks” enabled.</p>
<b>Status:</b>	Pass
<b>Findings &amp; Comments:</b>	<p>The application was setup according to the guidelines provided. It is recommended to install and run the nessus server from another host with a better hardware configuration and use the client application from this laptop. This will allow a better performance of the tool, as well as better capacity to store log files that will provide useful information for troubleshooting and better analysis.</p>

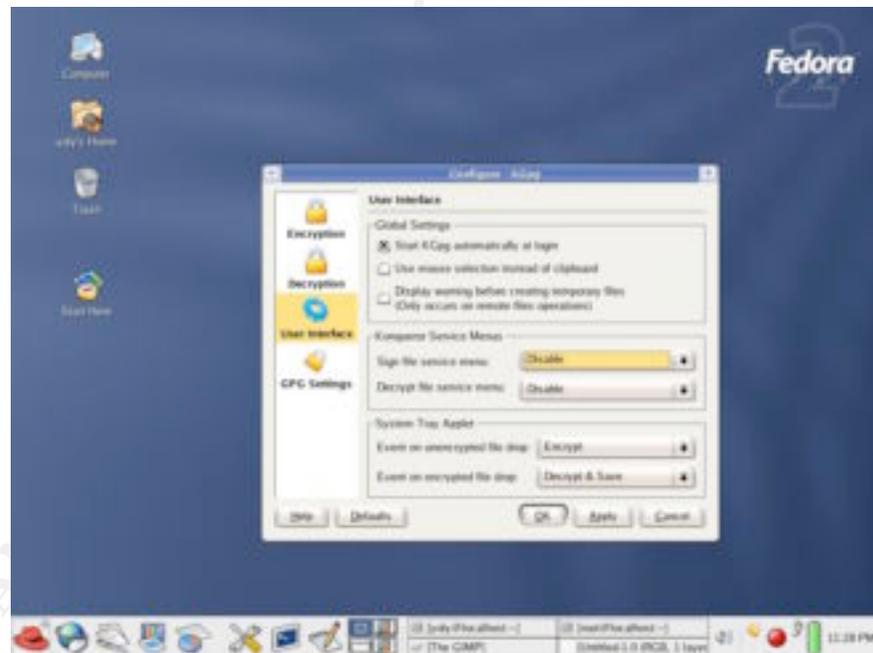
<b>Checklist Item -13. OS &amp; Applications with latest patches installed</b>	
<b>Evidence:</b>	<p>This is the output after running yum’s updatr</p> <pre> # yum check-update Gathering header information file(s) from server(s) Server: Fedora Core 2 - i386 - Base Server: Fedora Core 2 - i386 - Released Updates Finding updated packages Downloading needed headers Name                               Arch  Version ----- gaim                               i386  1:1.1.0-0.FC2  updates-released </pre>

	glib2	i386	2.4.8-1.fc2	updates-released
	gtk2	i386	2.4.14-1.fc2	updates-released
	kernel	i686	2.6.9-1.6_FC2	updates-released
	libpng	i386	2:1.2.8-1.fc2	updates-released
	samba-client	i386	3.0.9-1.fc2	updates-released
	samba-common	i386	3.0.9-1.fc2	updates-released
	xorg-x11	i386	6.7.0-11	updates-released
	xorg-x11-100dpi-fonts	i386	6.7.0-11	updates-
	xorg-x11-75dpi-fonts	i386	6.7.0-11	updat
	xorg-x11-Mesa-libGL	i386	6.7.0-11	updat
	xorg-x11-Mesa-libGLU	i386	6.7.0-11	updat
	xorg-x11-base-fonts	i386	6.7.0-11	updat
	xorg-x11-devel	i386	6.7.0-11	updat
	xorg-x11-font-utils	i386	6.7.0-11	updat
	xorg-x11-libs	i386	6.7.0-11	updat
	xorg-x11-libs-data	i386	6.7.0-11	updat
	xorg-x11-tools	i386	6.7.0-11	updat
	xorg-x11-twm	i386	6.7.0-11	updat
	xorg-x11-xauth	i386	6.7.0-11	updat
	xorg-x11-xdm	i386	6.7.0-11	updat
	xorg-x11-xfs	i386	6.7.0-11	updat
	#			
<b>Status:</b>	Fail			
<b>Findings &amp; Comments:</b>	The laptop does not have all the latest patches and updates. The laptop's user updates the intervals. She sometimes performs updates on a daily basis, but at times when she is too busy as a result, the laptop could run without updates, increasing the vulnerability of the system.			

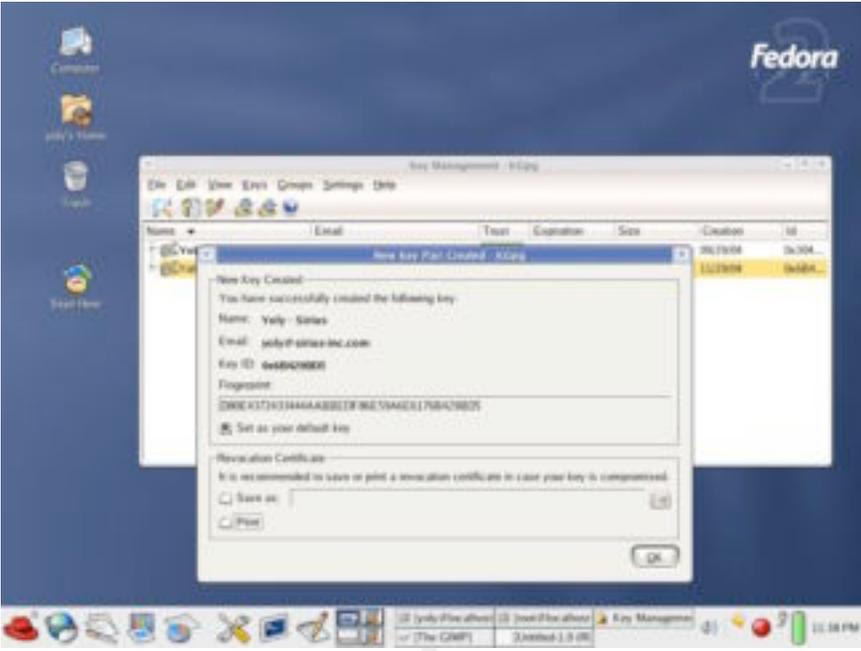
<b>Checklist Item -14. Encryption Application Deployed</b>	
<b>Evidence:</b>	<pre># which kpgp /usr/bin/kpgp  <b>Directory /projects for Sirius' clients (encrypted files):</b> # cd /home/yoly/projects # ls -al total 580 drwxrwx---  2 yoly yoly  4096 Nov 29 22:25 . drwx----- 30 yoly yoly  4096 Nov 30 22:09 .. -rw-rw----  1 yoly yoly  3795 Nov 29 22:23 0626.txt.asc -rw-rw----  1 yoly yoly   2928 Nov 29 22:21 1244info.txt.asc -rw-rw----  1 yoly yoly 80201 Nov 29 22:22 1369.rtf.asc -rw-rw----  1 yoly yoly 121315 Nov 29 22:25</pre>

```
2004-04-22-scanreport.pdf.asc
-rw-rw----  1 yoly yoly   8245 Nov 29 22:25
2004-07_client0234-externalscan-alert.doc.asc
-rw-rw----  1 yoly yoly  12527 Nov 29 22:22
ned1169.rtf.asc
-rw-rw----  1 yoly yoly   7117 Nov 29 22:22
pgpinstructions_0493.rtf.pgp
-rw-rw----  1 yoly yoly   4282 Nov 29 22:24
qlscandocumentplan.doc.pgp
-rw-rw----  1 yoly yoly 222167 Nov 29 22:24
riskassessmentreport-2004-03-10.pdf.pgp
-rw-rw----  1 yoly yoly   3889 Nov 29 22:23
v0459.txt.asc
-rw-rw----  1 yoly yoly  80227 Nov 29 22:22
v1099.rtf.asc
#
```

**Screen shot of the kpgp setup:**



**Screen shot of the user's key generation:**

	
<b>Status:</b>	Pass
<b>Findings &amp; Comments:</b>	<p>The application Kpgp 1.1.2 is installed and configured. This application is using KDE 3.2.2-8.fc2.</p> <p>The directory <code>/projects</code> in the users' home directory <code>/home/yoly</code>, shows that all the files in it are encrypted. This is the only directory where the consultant stores clients' and projects files.</p>

<b>Checklist Item -15. Installed Virus Scanner</b>	
<b>Evidence:</b>	<pre># rpm -qa   grep -i pav pavcl-7.01.00-1</pre>
<b>Status:</b>	Pass
<b>Findings &amp; Comments:</b>	Panda Antivirus is installed. As explained in the previous section, it is not a high requirement at the moment, but Sirius prefers to have a proactive stand with this matter.

<b>Checklist Item -16. Laptop Steel Cable</b>	
<b>Evidence:</b>	The user carries the steel cable on the laptop's carrying case, and uses the cable when it is necessary to leave the laptop at the office overnight.
<b>Status:</b>	Pass
<b>Findings &amp; Comments:</b>	The user prefers to never leave the laptop unattended when she is out of the office, even though she has the possibility to use the steel cable. She takes the laptop with her, even during "bathroom breaks". Although she trusts the strength of the cable, she does not trust the

strength of the plastic location where the laptop gets attached to.
---

## Section 4 – Audit Report

### Exit Meeting

As important as the Preliminary Meeting is the Exit Meeting. During this meeting, the auditor presents the Executive Summary. The auditor can give an overview: list the positive findings; explained what was learned during the process; and provide advice about how to improve the state of the target system.

### Executive Summary

#### Introduction

The purpose of this report is to provide the audit results of the Dell Latitude CS 200 “Systems Security Consultant’s Laptop” running Fedora Core 2. The audit verified the conformance of the laptop to Sirius’ policies, procedures and security guidelines. It analyzed the measures that the laptop had in place in order to perform its functions in a secure way.

Since the laptop is mainly used to perform security audits and assessments purposes, it needs to connect to secured and non-secured networks. Hence, it was necessary to verify that the laptop had adequate mechanisms to protect itself, to prevent unauthorized access and to avoid putting the clients’ systems and their information at risk.

The most significant findings of the audit are:

#### Main Findings (Positive)

- Very good security policies, procedures and guidelines
- Good password strength on user account passwords
- Very good use of file encryption tool to protect relevant information

#### Main Findings (Negative)

- BIOS password not set
- Lack of systematic integrity checking mechanism
- Lack of systematic OS & Application updates/patches

### Summary of Auditing Findings

#### Security Policies, Procedures and Guidelines

Sirius presented very good security policies, procedures and guideless. They are clear and easy to understand. The documents were tailored based on recommendations and guidelines from the “SANS Security Policy Project”, URL: <http://www.sans.org/resources/policies/> .

It is important to remember that these documents are not static and they need to evolve as the organization evolves. Although the core and main principals the documents are based on don't change, they should be revised and updated from time to time. Those changes can consist of additions of new definitions, additions of new terms, general editing, or even separate the document into smaller documents to facilitate its interpretation.

### BIOS – Password Protected

The laptop failed the BIOS password check at the moment of the audit. It needed to be properly set up, as it is a very good preventive measure. Although it does not make the data completely unrecoverable, in case of laptop theft this measure can provide an extra layer of protection. The issue was corrected by the system administrator at the moment of the audit.

A note of advice, it is very important to remember this password, since it is very difficult to change it or reset it without it. “Unlike desktop computers, most laptops store the BIOS password in a chip that cannot be erased simply by resetting the CMOS battery. Dell laptops have a ‘master password’ unique to each machine that you can use if you forget your BIOS password. You must contact Dell via telephone and after complete verification of your ownership of the computer, they will provide you with the necessary password.”<sup>48</sup>

### Boot Loader – Password Protected

GRUB, the boot loader was password protected. GRUB can store the password in clear text or can store a md5hash of the password instead. The grub.conf file showed that the password was not stored in the clear. This represents yet another layer of protection for the system.

### Check for rootkits

chkrootkit provides a wide series of tests. The output of the chkrootkit showed that the laptop did not have a rootkit installed when the audit was performed.

Another very good integrity checking tool is Tripwire (<http://www.tripwire.org/>). This tool is well known for its capabilities as host-based intrusion detection. Tripwire's policy file needs to be tuned to indicate the specific directories that

should be checked and stored in a database. When necessary Tripwire checks the state of the system against the information stored in the database. If the values don't match this indicates that something changed. It is important to reset and update the database every time there is a known system change to avoid false positives.

### No Empty Passwords and Password Strength

During the audit, all the user accounts had passwords. In addition, the passwords were not easily cracked. Although with enough time and power passwords can be cracked, at least the ones used in the system comply with Sirius' policy and follow best security practices.

(Please see [Appendix D](#))

### Disabled Xinetd Services & Disabled Boot Services

The laptop passed these tests. The services were disabled according to the "Secure Laptop Configuration" SOP ([Appendix E](#)). It is possible that some of these services will have to get re-enabled, as some applications need them in order to function properly. In the event that this is necessary, the user should report the changes to the IT team. They should verify that the modification on the security configuration is really necessary and the modification should be documented.

### Auditing Applications Installed

The laptop has all the auditing tools required. There are many other available tools that can be used for assessments, auditing and troubleshooting tasks. It is very important to download them from trusted sources and verify the digital signatures or md5hashes provided by the trusted source. It is also recommended to verify that they do not contain malicious payload by installing them first in a testing or lab environment, not on the production system. Once the new tool is isolated, it can be virus scanned. Check for possible and unexpected changes in the system using integrity checking tools. Sniff the traffic to make sure the tool does not open unexpected connections or attempts to call home. Once the new tool goes through rigorous checks, it can be put in production.

Sirius as a security auditing organization needs to be extra careful with the tools used at clients' networks. Not only do the auditing and assessment team needs to have good knowledge and understanding of the tools, but the tools utilized need to be trusted tools. This way the tools cannot turn into inadvertent or accidental vectors of attack to those networks, which could have very negative

effect on the reputation of the organization, in addition to legal and economic penalties.

### Nessus Proper Configuration

Nessus was properly installed and had proper configuration according to the set up procedures and recommendations (see [Appendix H](#)). The set up took into consideration the capacity of the laptop and the system's hardware configuration. This system does not have a configuration that supports adequate performance of the tool and it will be difficult for the user to perform the auditing task with it.

As indicated before, the person that uses this tool needs to have good knowledge and understanding of it. If not used or configured properly, it can cause a lot of problems. Some applications and systems do not react well to the tests performed by the tool and they might crash. Therefore this tool must be used after receiving appropriate authorization and during scheduled downtime.

### OS & Applications with latest patches installed

The laptop did not have all the latest patches and updates at the moment of the audit. The issue was corrected immediately. This is the output after running the updating application.

<b>Remediation:</b>	<pre># yum update Gathering header information file(s) from server(s) Server: Fedora Core 2 - i386 - Base Server: Fedora Core 2 - i386 - Released Updates Finding updated packages Downloading needed headers xorg-x11-xauth-0-6.7.0-11 100%  =====  70 kB 00:00 gtk2-0-2.4.14-1.fc2.i386. 100%  =====  16 kB 00:00 gaim-1-1.1.0-0.FC2.i386.h 100%  =====  21 kB 00:00 xorg-x11-Mesa-libGLU-0-6. 100%  =====  70 kB 00:00 samba-common-0-3.0.9-1.fc 100%  =====  11 kB 00:00 xorg-x11-xf86-video-intel-0-6.7.0-11.i 100%  =====  71 kB 00:00 xorg-x11-libs-0-6.7.0-11. 100%  =====  73 kB 00:00 xorg-x11-twm-0-6.7.0-11.i 100%</pre>
---------------------	--

=====	70 kB	00:00
xorg-x11-Mesa-libGL-0-6.7	100%	
=====	70 kB	00:00
xorg-x11-libs-data-0-6.7.	100%	
=====	75 kB	00:00
samba-client-0-3.0.9-1.fc	100%	
=====	10 kB	00:00
xorg-x11-tools-0-6.7.0-11	100%	
=====	72 kB	00:00
xorg-x11-0-6.7.0-11.i386.	100%	
=====	98 kB	00:00
glib2-0-2.4.8-1.fc2.i386.	100%	
=====	6.6 kB	00:00
xorg-x11-base-fonts-0-6.7	100%	
=====	83 kB	00:00
xorg-x11-font-utils-0-6.7	100%	
=====	70 kB	00:00
libpng-2-1.2.8-1.fc2.i386	100%	
=====	4.0 kB	00:00
xorg-x11-devel-0-6.7.0-11	100%	
=====	134 kB	00:00
xorg-x11-100dpi-fonts-0-6	100%	
=====	82 kB	00:00
xorg-x11-75dpi-fonts-0-6.	100%	
=====	81 kB	00:00
xorg-x11-xdm-0-6.7.0-11.i	100%	
=====	71 kB	00:00
xorg-x11-Xvfb-0-6.7.0-11.	100%	
=====	70 kB	00:00
perl-Cyrus-0-2.2.10-3.fc2	100%	
=====	6.7 kB	00:00
xorg-x11-ISO8859-2-75dpi-	100%	
=====	76 kB	00:00
netatalk-2-1.6.4-2.2.i386	100%	
=====	9.0 kB	00:00
xorg-x11-syriac-fonts-0-6	100%	
=====	71 kB	00:00
xorg-x11-ISO8859-14-100dp	100%	
=====	76 kB	00:00
cyrus-imapd-utils-0-2.2.1	100%	
=====	6.7 kB	00:00
cyrus-imapd-murder-0-2.2.	100%	
=====	5.9 kB	00:00
xorg-x11-ISO8859-9-75dpi-	100%	
=====	76 kB	00:00
xorg-x11-ISO8859-15-100dp	100%	
=====	76 kB	00:00

```

libpng10-0-1.0.18-1.fc2.i 100%
|=====| 2.9 kB      00:00
xorg-x11-ISO8859-15-75dpi 100%
|=====| 76 kB      00:00
xorg-x11-doc-0-6.7.0-11.i 100%
|=====| 73 kB      00:00
libpng10-devel-0-1.0.18-1 100%
|=====| 2.7 kB      00:00
libpng-devel-2-1.2.8-1.fc 100%
|=====| 3.9 kB      00:00
xorg-x11-Xnest-0-6.7.0-11 100%
|=====| 70 kB      00:00
gtk2-devel-0-2.4.14-1.fc2 100%
|=====| 39 kB      00:00
cyrus-imapd-nntp-0-2.2.10 100%
|=====| 5.9 kB      00:00
cyrus-imapd-devel-0-2.2.1 100%
|=====| 6.9 kB      00:00
glib2-devel-0-2.4.8-1.fc2 100%
|=====| 11 kB      00:00
xorg-x11-ISO8859-14-75dpi 100%
|=====| 76 kB      00:00
samba-0-3.0.9-1.fc2.i386. 100%
|=====| 29 kB      00:00
cyrus-imapd-0-2.2.10-3.fc 100%
|=====| 15 kB      00:00
netatalk-devel-2-1.6.4-2. 100%
|=====| 5.4 kB      00:00
xorg-x11-cyrillic-fonts-0 100%
|=====| 73 kB      00:00
xorg-x11-ISO8859-9-100dpi 100%
|=====| 76 kB      00:00
xorg-x11-sdk-0-6.7.0-11.i 100%
|=====| 104 kB     00:00
xorg-x11-truetype-fonts-0 100%
|=====| 70 kB      00:00
samba-swat-0-3.0.9-1.fc2. 100%
|=====| 24 kB      00:00
xorg-x11-ISO8859-2-100dpi 100%
|=====| 76 kB      00:00
Resolving dependencies
Dependencies resolved
I will do the following:
[install: kernel 2.6.9-1.6_FC2.i686]
[update: samba-client 3.0.9-1.fc2.i386]
[update: xorg-x11-xauth 6.7.0-11.i386]
[update: samba-common 3.0.9-1.fc2.i386]

```

```

[update: xorg-x11-tools 6.7.0-11.i386]
[update: xorg-x11-devel 6.7.0-11.i386]
[update: xorg-x11 6.7.0-11.i386]
[update: xorg-x11-xfs 6.7.0-11.i386]
[update: gtk2 2.4.14-1.fc2.i386]
[update: glib2 2.4.8-1.fc2.i386]
[update: xorg-x11-100dpi-fonts 6.7.0-11.i386]
[update: xorg-x11-libs 6.7.0-11.i386]
[update: gaim 1:1.1.0-0.FC2.i386]
[update: xorg-x11-75dpi-fonts 6.7.0-11.i386]
[update: xorg-x11-base-fonts 6.7.0-11.i386]
[update: xorg-x11-xdm 6.7.0-11.i386]
[update: xorg-x11-twm 6.7.0-11.i386]
[update: xorg-x11-font-utils 6.7.0-11.i386]
[update: libpng 2:1.2.8-1.fc2.i386]
[update: xorg-x11-Mesa-libGL 6.7.0-11.i386]
[update: xorg-x11-Mesa-libGLU 6.7.0-11.i386]
[update: xorg-x11-libs-data 6.7.0-11.i386]
Is this ok [y/N]:y
<output cut to save space>
....

Completing update for samba-client - 23/43
Completing update for xorg-x11-xauth - 24/43
Completing update for samba-common - 25/43
Completing update for xorg-x11-tools - 26/43
Completing update for xorg-x11-devel - 27/43
Completing update for xorg-x11 - 28/43
Completing update for xorg-x11-xfs - 29/43
Completing update for gtk2 - 30/43
Completing update for glib2 - 31/43
Completing update for xorg-x11-100dpi-fonts -
32/43
Completing update for xorg-x11-libs - 33/43
Completing update for gaim - 34/43
Completing update for xorg-x11-75dpi-fonts -
35/43
Completing update for xorg-x11-base-fonts -
36/43
Completing update for xorg-x11-xdm - 37/43
Completing update for xorg-x11-twm - 38/43
Completing update for xorg-x11-font-utils -
39/43
Completing update for libpng - 40/43
Completing update for xorg-x11-Mesa-libGL -
41/43
Completing update for xorg-x11-Mesa-libGLU -

```

	<pre> 42/43 Completing update for xorg-x11-libs-data - 43/43 Kernel Updated/Installed, checking for bootloader Grub found - making this kernel the default Installed: kernel 2.6.9-1.6_FC2.i686 Updated: samba-client 3.0.9-1.fc2.i386 xorg- x11-xauth 6.7.0-11.i386 samba-common 3.0.9- 1.fc2.i386 xorg-x11-tools 6.7.0-11.i386 xorg- x11-devel 6.7.0-11.i386 xorg-x11 6.7.0-11.i386 xorg-x11-xf86 6.7.0-11.i386 gtk2 2.4.14- 1.fc2.i386 glib2 2.4.8-1.fc2.i386 xorg-x11- 100dpi-fonts 6.7.0-11.i386 xorg-x11-libs 6.7.0- 11.i386 gaim 1:1.1.0-0.FC2.i386 xorg-x11-75dpi- fonts 6.7.0-11.i386 xorg-x11-base-fonts 6.7.0- 11.i386 xorg-x11-xdm 6.7.0-11.i386 xorg-x11-twm 6.7.0-11.i386 xorg-x11-font-utils 6.7.0-11.i386 libpng 2:1.2.8-1.fc2.i386 xorg-x11-Mesa-libGL 6.7.0-11.i386 xorg-x11-Mesa-libGLU 6.7.0- 11.i386 xorg-x11-libs-data 6.7.0-11.i386 Transaction(s) Complete # </pre>
--	---

**Important:** Not having the latest patches adds unnecessary risk to the system. This task is a very important compensating control and must be performed in a methodical and organized manner.

### Encryption Application Deployed

The encryption application GnuPG (or Kpgp) is deployed. The user follows the “Information Sensitivity” policy (see **Appendix A**) and she diligently encrypts clients’ data, as well as, documents from important projects. This is a very important compensating control. In the event of laptop theft, the organization would have some minor economic losses in terms of hardware and productivity. But since the sensitive data is not easy to retrieve, the cost will be negligible compared to what Sirius would suffer if the data was stored in clear text instead.

The laptop also has installed a tool called PuTTY

```
# rpm -qa | grep putty
putty-0.56-0.fdr.1.2
```

PuTTY is a free implementation of Telnet and SSH, used for secure connections and secure file transfers. It is a client application and a series of tools that

support ssh, scp and sFTP. All these tools promote the compliance of Sirius "Information Sensitivity" policy.  
PuTTY can be found at: <http://www.chiark.greenend.org.uk/~sgtatham/putty/> .

### Installed Virus Scanner

The laptop has the virus scanner from panda software <http://www.pandasoftware.com/> . It is recommended to use it and update it on a regular basis. At this time, viruses for Linux are not as common as it happens with Windows based systems, but this situation will change as the operating system's popularity increases.

### Laptop Steel Cable

One of the main ideas behind security measures that provide access control (technical or physical) is to present a deterrent. But these deterrents are not infallible. With enough power, time and determination the deterrents can be beaten or overpowered. Obviously the idea is that having a deterrent is better than not having anything at all. But in addition, the deterrent must be as effective as possible. In the case of the audit, the laptop passed the steel cable check. But the way it is implemented makes it a very weak deterrent. The cable itself is strong and has a descent lock. Unfortunately the control falls short as it attaches to the plastic side of the laptop. With minimal force and with minimal damage to laptop, a thief can get release it from the cable.

### **Audit Recommendations & Compensating Controls**

It is highly recommended to perform application/OS updates, virus scans, and integrity checks of the files and applications on a regular basis. Since the laptop's user is very busy and might forget, these tasks can be scripted so they run at specific times and send small reports to the user. Paul J. Santos in his document "How-To Make Linux System Auditing a Little Easier" URL: <http://www.sans.org/rr/whitepapers/auditing/81.php><sup>49</sup> provides examples and scripts that help to automate the integrity checking tasks. Scripting these controls will help protect the system and maintain its compliance with policy.

The security auditing tools must always be carefully used and properly configured, in order to avoid problems on clients' environments. The person that uses these tools must understand how they work and should use them in a testing environment to get familiarized with them before using them at the clients' sites. Equally important is to ensure that the tools installed in the laptop can be trusted. Periodic security training with reputable organizations is also

recommended for the security auditor. This will help him/her to maintain appropriate skills levels and maintain current knowledge of Information Security.

In order to turn the laptop steel cable into a more secure or more effective deterrent, the laptop should have a metallic plate behind the liquid crystal display and glued to the laptop's plastic cover with strong adhesive. The cable can then attach to this plate, instead of attaching to the soft plastic side of the laptop. A small 2" x 3" steel plate costs about \$3.00 dollars. A simple solution like this one will force the thief to make a lot more damage to the laptop and a lot more noise in order to steal it, and makes the physical control a much better and more effective deterrent.

Example of these plates can be found at Flexguard Security Products, Inc. site URL: <http://www.flexguard.com/>

If installed according the vendor's instructions, it takes more than 1,400 pounds to remove it.



Image source: [http://www.flexguard.com/cat\\_plates.html](http://www.flexguard.com/cat_plates.html)<sup>50</sup>

© SANS Institute 2004, Author retains full rights.

## Conclusion

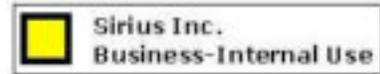
A very important concept to remember is that having physical and technical controls is good for the laptop. But ultimately, it is the user's responsibility to protect the system and to take unnecessary risk such as:

- Not updating/patching the applications and OS on a regular basis
- Not running the systems integrity checkers and verifying the results on a regular basis
- Downloading and installing "untrusted" applications and tools
- Leaving the laptop unattended and un-locked

The laptop is not a static entity; therefore, it is recommended to periodically verify its level of compliance with Sirius' policies and procedures.

© SANS Institute 2004, Author retains full rights.

## Appendix A



### Information Sensitivity Policy

**Date:** January 10, 2004

**Important:** This Policy was based on security policy templates and guidelines found at the SANS.org site <http://www.sans.org/resources/policies/><sup>51</sup>.

#### 1.0 Purpose

The Information Sensitivity Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of Sirius without proper authorization.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All employees must familiarize themselves with the information labeling and handling guidelines that follow this introduction.

Questions about the proper classification of a specific piece of information should be addressed to your manager. Questions about this policy should be addressed to InfoSec.

#### 2.0 Scope

All Sirius information is categorized into three main classifications:

- Sirius Confidential
- Sirius Business - Internal Use Only
- Sirius Public Information

#### 3.0 Policy

The Sensitivity Guidelines below provides details on how to protect information at varying sensitivity levels. They must be followed carefully. Documents must be clearly marked with the respective logo.

##### 3.1. Confidential



*Note: Sirius Confidential information must be marked with the Confidential logo. Users should be aware that this information is very sensitive and must protect it as such.*

Sirius Confidential is information that must be protected very closely, such as trade secrets, development programs, potential acquisition targets, and other information integral to the success of our company.

A subset of Sirius Confidential information is "Sirius Third Party Confidential" information. This is confidential information belonging or pertaining to another corporation which has been entrusted to Sirius by that company under non-disclosure agreements and other contracts. **All clients' data is considered Sirius Confidential, even if clients have given to it a lower classification level. All confidential shall be encrypted or protected while it is stored or in transit.**

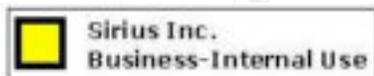
Examples of confidential information include everything from joint development efforts to vendor lists, customer orders, and supplier information. Information in this category ranges from extremely sensitive to information about the fact that we've connected a supplier / vendor into Sirius's network to support our operations.

Sirius personnel are encouraged to use common sense and best judgment in securing Sirius Confidential information to the proper extent. **If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their manager and treat the data as "Confidential" while the correct classification is established.**

**Handling:**

- This data must not be copied or shared without explicit permission.
- All confidential shall be encrypted or protected while it is stored or in transit.
- Hard copies versions of this type of data must be secured when not in use.
- When disposing hard copies, they must be carefully destroyed (i.e., use shredder).
- Use the most secure means available to transmit the information outside the company.

3.2. **Business-Internal Use Only:** General corporate information; some personnel and technical information



Sirius Business – Internal Use Only contains information such as telephone directories, general corporate information, personnel information, organizational charts, memos, policies, which does not require as stringent a degree of protection. This type of data cannot be distributed, without proper authorization.

*Note: Sirius Business-Internal Use only information must be marked with the Business-Internal Use logo. Users should be aware that this information is sensitive and must be protect it as such.*

**Handling:**

- This data must not be distributed or shared without explicit permission.
- Only distribute to Sirius employees and non-employees with signed non-disclosure agreements who have a business need to know.

- Keep from view of unauthorized people; erase whiteboards, do not leave in view on tabletop.
- 3.3. **Public Information:** Sirius Public information is data that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to Sirius, Inc.



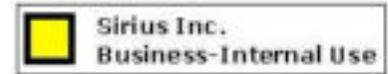
*Note: Marking of Sirius Public information with the Public Information logo is at the discretion of the owner or custodian of the information. Users should be aware that although the information can be freely shared, it may be protected by copyright. Permission from publisher or author may be required.*

#### **4.0 Enforcement**

- 4.1. Any infractions of this code of ethics will not be tolerated and Sirius will act quickly in correcting the issue if the ethical code is broken.
- 4.2. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment

© SANS Institute 2004, Author retains rights.

## Appendix B



### Ethics Policy

**Date:** January 10, 2004

**Important:** This Policy was based on security policy templates and guidelines found at the SANS.org site [www.sans.org/resources/policies/](http://www.sans.org/resources/policies/)<sup>52</sup>

#### 1.0 Overview

Sirius purpose for this ethics policy is to establish a culture of openness, trust and integrity in business practices. Effective ethics is a team effort involving the participation and support of every Sirius employee. All employees should familiarize themselves with the ethics guidelines that follow this introduction.

Sirius is committed to protecting employees, partners, vendors and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. When Sirius addresses issues proactively and uses correct judgment, it will help set us apart from competitors.

Sirius will not tolerate any wrongdoing or impropriety at anytime. Sirius will take the appropriate measures act quickly in correcting the issue if the ethical code is broken. Any infractions of this code of ethics will not be tolerated.

#### 2.0 Purpose

Our purpose for authoring a publication on ethics is to emphasize the employee's and consumer's expectation to be treated to fair business practices. This policy will serve to guide business behavior to ensure ethical conduct.

#### 3.0 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at Sirius, including all personnel affiliated with third parties.

#### 4.0 Policy

##### 4.1. Executive Commitment to Ethics

- 4.1.1. Top brass within Sirius must set a prime example. In any business practice, honesty and integrity must be top priority for executives.
- 4.1.2. Executives must have an open door policy and welcome suggestions and concerns from employees. This will allow employees to feel comfortable discussing any issues and will alert executives to concerns within the work force.
- 4.1.3. Executives must disclose any conflict of interests regard their position within Sirius.

##### 4.2. Employee Commitment to Ethics

- 4.2.1. Sirius employees will treat everyone fairly, have mutual respect, promote a team environment and avoid the intent and appearance of unethical or compromising practices.

- 4.2.2. Every employee needs to apply effort and intelligence in maintaining ethics value.
- 4.2.3. Employees must disclose any conflict of interests regard their position within Sirius.
- 4.2.4. Employees will help Sirius to increase customer and vendor satisfaction by providing quality products and timely response to inquiries.
- 4.3. Company Awareness
  - 4.3.1. Promotion of ethical conduct within interpersonal communications of employees will be rewarded.
  - 4.3.2. Sirius will promote a trustworthy and honest atmosphere to reinforce the vision of ethics within the company.
- 4.4. Maintaining Ethical Practices
  - 4.4.1. Sirius will reinforce the importance of the integrity message and the tone will start at the top. Every employee, manager, director needs consistently maintain an ethical stance and support ethical behavior.
  - 4.4.2. Employees at Sirius should encourage open dialogue, get honest feedback and treat everyone fairly, with honesty and objectivity.
  - 4.4.3. Sirius has established a best practice disclosure committee to make sure the ethical code is delivered to all employees and that concerns regarding the code can be addressed.
- 4.5. Unethical Behavior
  - 4.5.1. Sirius will avoid the intent and appearance of unethical or compromising practice in relationships, actions and communications.
  - 4.5.2. Sirius will not tolerate harassment or discrimination.
  - 4.5.3. Unauthorized use of company trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our company will not be tolerated.
  - 4.5.4. Sirius will not permit impropriety at any time and we will act ethically and responsibly in accordance with laws.
  - 4.5.5. Sirius employees will not use corporate assets or business relationships for personal use or gain.

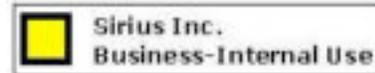
## **5.0 Enforcement**

- 5.1. Any infractions of this code of ethics will not be tolerated and Sirius will act quickly in correcting the issue if the ethical code is broken.
- 5.2. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment

## **6.0 Revision History**

January 10, 2004 – First edition. Version 1.

## Appendix C



### InfoSec Acceptable Use Policy

**Date:** January 10, 2004

**Important:** This Policy was based on security policy templates and guidelines found at the SANS.org site [www.sans.org/resources/policies/](http://www.sans.org/resources/policies/)<sup>53</sup>

#### 1.0 Overview

InfoSec's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Sirius. Sirius established a culture of openness, trust and integrity. InfoSec is committed to protecting Sirius' employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Sirius. These systems are to be used for business purposes in serving the interests of the company, of our clients and customers in the course of normal operations. Effective security is a team effort involving the participation and support of every Sirius employee and affiliate who deals with information and/or information systems. It is the responsibility of every employee to know these guidelines, and to conduct their activities accordingly.

#### 2.0 Purpose

The purpose of this policy is to outline the acceptable use of Sirius' computer equipment. These rules are in place to protect the employee and Sirius. Inappropriate use exposes Sirius to risks including virus attacks, compromise of network systems and services, and legal issues.

#### 3.0 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at Sirius, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Sirius.

#### 4.0 Policy

##### 4.1 General Use and Ownership

1. While Sirius' network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of Sirius. Because of the need to protect Sirius' network, management cannot guarantee the confidentiality of information stored on any network device belonging to Sirius.
2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. If there is any uncertainty, employees should consult their supervisor or manager.

3. InfoSec recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see InfoSec's Information Sensitivity Policy.
4. For security and network maintenance purposes, authorized individuals within Sirius may monitor equipment, systems and network traffic at any time.
5. Sirius reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

#### 4.2 Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either Business-Internal Use Only or Restricted Confidential, as defined by corporate confidentiality guidelines, details of which can be found in Information Sensitivity policy. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly, user level passwords should be changed every six months.
3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by locking the when the host will be unattended.
4. Use encryption of information in compliance with InfoSec's Acceptable Encryption Use policy.
5. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the "InfoSec Laptop Security Tips". Protect the data in it in accordance with the Information Sensitivity policy.
6. Postings by employees from a Sirius email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Sirius, unless posting is in the course of business duties.
7. All hosts used by the employee that are connected to the Sirius Internet/Intranet/Extranet, whether owned by the employee or Sirius, shall be continually executing approved virus-scanning software with a current virus signatures. Unless overridden by departmental or group policy.
8. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

#### 4.3. Unacceptable Use

The following activities are, in general, prohibited. Under no circumstances is an employee of Sirius authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Sirius-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

##### System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Sirius.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Sirius or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using a Sirius computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any Sirius account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior notification to InfoSec is made.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
15. Providing information about, or lists of, Sirius employees to parties outside Sirius.

#### Email and Communications Activities

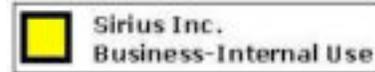
1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within Sirius' networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Sirius or connected via Sirius' network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

## **5.0 Enforcement**

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

© SANS Institute 2004, Author retains full rights.

## Appendix D



### Password Policy

**Date:** January 11, 2004

**Important:** This Policy was based on security policy templates and guidelines found at the SANS.org site [www.sans.org/resources/policies/](http://www.sans.org/resources/policies/)<sup>54</sup>

#### 1.0 Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Sirius's entire corporate network. As such, all Sirius employees (including contractors and vendors with access to Sirius systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

#### 2.0 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

#### 3.0 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Sirius facility, has access to the Sirius network, or stores any non-public Sirius information.

#### 4.0 General

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.
- All production system-level passwords must be part of the InfoSec administered global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four months.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- All user-level and system-level passwords must conform to the guidelines described below.

#### 4.1 Guidelines

##### A. General Password Construction Guidelines

Passwords are used for various purposes at Sirius. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than seven characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
  - Names of family, pets, friends, co-workers, fantasy characters, etc.
  - Computer terms and names, commands, sites, companies, hardware, software.
  - The words "Sirius", "sanjose", "sanfran" or any derivation.
  - Birthdays and other personal information such as addresses and phone numbers.
  - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
  - Any of the above spelled backwards.
  - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#\$%^&\*()\_+|~-=\`{ } [ ] : ; ' < > ? , . / )
- Are at least seven alphanumeric characters long.
- Are not a specific word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line.

## **B. Password Protection Standards**

Do not use the same password for Sirius accounts as for other non-Sirius access.

Do not share Sirius passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential Sirius information.

Here is a list of "don't's":

- Don't reveal a password over the phone to ANYONE
- Don't send passwords in an email message
- Don't reveal or share your passwords with anyone
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them call someone in the Information Security Department.

Do not use the "Remember Password" feature of applications (e.g., Eudora, Outlook, Netscape Messenger, Internet Explorer, Mozilla ).

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Change passwords at least once every six months (except system-level passwords which must be changed quarterly). The recommended change interval is every four months.

If an account or password is suspected to have been compromised, report the incident to InfoSec and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by InfoSec or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

### **C. Application Development Standards**

Application developers must ensure their programs contain the following security precautions.

Applications:

- should support authentication of individual users, not groups.
- should not store passwords in clear text or in any easily reversible form.
- passwords should not be hard coded.

### **D. Use of Passwords and Passphrases for Remote Access Users**

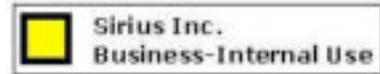
Access to the Sirius Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

### **5.0 Enforcement**

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

© SANS Institute 2004, Author retains full rights.

## Appendix E



### InfoSec Laptop Security Tips

**Date:** January 10, 2004

**Important:** This document was based on the laptop security tips found on the Innovated Security Products, Inc., web site.<sup>55</sup>

#### 1.0 Purpose

The purpose of this document is to provide guidelines and security tips for laptop Sirius laptop users:

1. **Never leave your laptop unattended, even for a moment.**  
Many thieves work in groups; one will distract you while the other carefully removes your laptop in its case.
2. **Utilize a laptop security cable.**  
Sirius Inc., gives every laptop user a specialized steel cable. Although this security measure is not infallible it provides an additional deterrent for laptop theft. Always secure the laptop using the provided cable. Never leave the laptop unlocked and at plain sight when you leave the office. Another time to be cautious is during meetings. Laptops are used, a quick break is called and when everyone returns, some of the laptops are missing. Remember thieves have better access than you might think and are very quick.
3. **Be certain to back up all important data daily.**  
Remember the hardest thing to replace when a laptop is stolen is the lost data.
4. **Encrypt the most important data.**  
Remember as per Sirius' Information Sensitivity Policy, "**All clients' data is considered Sirius Restricted Confidential, even if clients have given to it a lower classification level. All Confidential shall be encrypted or protected while it is stored or in transit.**"  
  
The most valuable part of a stolen laptop is the data. Many groups have cash bounties out for particular information that can be resold for identity theft or competitive use.
5. **Protect the data and access of the computer with strong password and or a hardware key device.**  
Remember to follow carefully Sirius' Password Policy. Passwords must contain both upper and lower case characters (e.g., a-z, A-Z). They must include numbers and special characters. They must be at least seven characters long.

### Some Things to THINK about

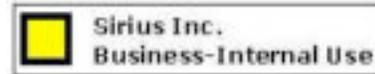
We can all learn to be more attentive to the people and our surroundings, so that we can protect our property and our lives.

1. Always be aware of your surroundings and the people in them.
2. **Realize that you are the prospective PREY or VICTIM.**
3. Always keep your belongings in your sight and preferably in direct contact with your body or a tether device.
4. Be suspicious of unusual activity and keep your property closer to you until this activity is over and any threat has diminished.
5. The use of laptop security cables to lock down your property or lock it together will significantly reduce the risk of theft.
6. Put a label or tape your business card to the top of your laptop. Too many business travelers are using the same brand and model of laptops leading to confusion and in some cases the picking up of someone else's laptop when going through security. The business card or label provides identification quickly when retrieving your laptop or trying to prove ownership in a mix up or attempted theft.

A better understanding of how a successful theft of property is accomplished is the key to prevention. Always remember that you are the person in charge of Sirius Inc., property. The extra attention to prevention can save an enormous amount of time trying to deal with and recover after the theft of property. You and the decisions that you make are the single most important resources in the prevention of theft.

© SANS Institute 2004, All rights reserved. Author retains full rights.

## Appendix F



### Standard Operating Procedure Secure Laptop Configuration

**Date:** January 12, 2004

#### 1.0 Purpose

The purpose of this document is to provide detailed procedures for the hardening and secure configuration of a Fedora 2.0 Laptop.

**Important: This document is based on the Step-by-Step guide "Securing Linux: A Survival Guide for Linux Security"<sup>56</sup> and the Center for Internet Security's (CIS) "Linux Level-1 Benchmark."<sup>57</sup>**

Please consult the guides for additional information (See **Reference** section at the end of this document).

Individuals can download the tools and documents from the CIS' site without cost, but they need to read carefully the "**Agreed Terms of Use**" to avoid any copyright and intellectual property law infringements.

#### 2.0 Requirements

The following requirements need to be in place, in order to be able to perform the secure configuration:

- Authorization to perform the procedure
- Laptop with completed basic installation of the Operating System
- Basic knowledge of Linux
- Basic knowledge of vi editor
- Administrative privileges and knowledge of the system's root password
- Follow the Sirius Password Policy

#### 3.0 Procedure

##### 3.1 BIOS configuration

This will protect the laptop from hardware configuration changes to the system.

- Boot up the laptop.
- Press the key "F2" on the keyboard to enter the BIOS setup.
- Press the arrow key until getting to the page that has the word "password:"
- Enter and confirm the desired password. (Follow "Sirius Password Policy")
- Note: From now on, the user will need to type the selected password during the boot up process.

##### 3.2 GRUB configuration

This step converts the GRUB password into MD5 format.<sup>58</sup> GRUB can store the password in clear text and that is not an acceptable format.

- At the prompt type:

- \$ /sbin/grub-md5-crypt
- Enter the password and confirm. (Follow "Sirius Password Policy")
- Copy the resulting hash of the password (It is a long string of characters)
  
- \$ su -
- #vi /etc/grub.conf
  
- At the line **password** type "--md5" leave a space and paste the resulting hash of the password
  
- Save the changes and close the file
  
- Note: From now on during the OS selection screen, the user needs to type "p". This will prompt for a password. The user needs to type the selected password.

### 3.3 Modification of Network Parameters

To increase network security it is necessary to modify /etc/sysctl.conf. In the Securing Linux Step-by-Step Guide the authors provide a brief explanation of each configuration.<sup>59</sup>

- Edit the file /etc/sysctl.conf .Make sure it has the following configurations:

```
net.ipv4.ip_forward = 0
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.tcp_max_syn_backlog = 4096
net.ipv4.conf.all.rp_filter = 1
net.ipv4.tcp_syncookies = 1
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
```

- Save changes and close the file.
- Perform the following actions:

```
$ su -

# chown root:root /etc/sysctl.conf
# chmod 0600 /etc/sysctl.conf
# /etc/rc.d/init.d/network restart
```

### 3.4 Disallow Remote Root Login

- Edit /etc/securetty and make sure it has the following configuration:

```
$ su -

# vi /etc/securetty
tty1
tty2
```

```
tty3
tty4
tty5
tty6
```

- Save changes and close the file.
- Perform the following actions:

```
# chown root:root /etc/securetty
# chmod 400 /etc/securetty
```

### 3.5 Disable Ctrl-Alt-Del

- Edit `/etc/inittab` and make sure the following line is commented out (it has a '#' at the beginning of the line):

```
# ca::ctrlaltdel:/sbin/shutdown -t3 -r now
```

### 3.6 Modify Warning Banners

- Edit the following files `/etc/motd`, `/etc/issue` and `/etc/issue.net`. In the *Securing Linux Step-by-Step Guide* the authors provide a brief explanation of each file.<sup>60</sup> Make sure each one of them has the following information:

```
This system is for authorized use only. All activity may
be monitored.
```

### 3.7 Password Aging Modification

- Change the password aging definitions of user accounts in `/etc/passwd` (in this case UID 500 and greater, to age every 180 days and user cannot be change earlier that 2 days):<sup>61</sup>

```
$ su -
```

```
# awk -F: ' $3 >= 500 { system ("change -M 180 -m 2 " $1)
}' /etc/passwd
```

- The *Securing Linux Step-by-Step* guide shows how to change the definitions for new accounts.<sup>62</sup>

### 3.8 Remove Unnecessary Accounts (users, groups)

- To remove unnecessary accounts, perform the following actions:

```
$ su -
```

```
#for file in /etc/{passwd,shadow,group} ; do /bin/cp
-p $file $file.orig ; done
```

```
# for user in uucp operator games gopher ; do
/usr/sbin/userdel $user ; done
# for group in dip gopher games uucp ; do
/usr/sbin/delgroup $group ; done
```

- The first line makes a backup of the original files
- The second line deletes the unnecessary user accounts
- The second line deletes the unnecessary group accounts

### 3.9 Lock System Accounts

Interactive log in should be disabled on system accounts. Enter the following command:

```
# for user in bin daemon adm ftp sync lp mail news
nobody ; do /usr/bin/usermod -L -s /dev/null $user ;
done
```

### 3.10 Verify No Empty Passwords

To check that the second field of the /etc/shadow file is blank enter the following command:

```
# awk -F: '($2 == "") {print $1}' /etc/shadow
```

### 3.11 Tighten Default umask

Edit lines in /etc/bashrc & /etc/csh.cshrc

Change umask 022 to umask 077

Change umask 002 to umask 007

### 3.12 Disable xinetd based services (telnet, wuftp, rlogin, rsh, rexec, tftp, snmpd)

cd /etc/xinetd.d

```
for file in chargen chargen-udp cups-lpd daytime \
daytime-udp echo echo-udp eklogin finger gssftp imap \
imaps ipop2 ipop3 krb5-telnet klogin kshell ktalk \
ntalk \
pop3s rexec rlogin rsh rsync servers services sgi_fam \
talk telnet tfpt time time-udp vsftpd wu-ftpd ; do
    chkconfig $file off
done
```

### 3.13 Disable Standard Boot Services

**IMPORTANT:** This step is based on the procedure provided on the "Linux Benchmark v1.1.0", July 29, 2003, Center for Internet Security (CIS), URL: [http://www.cisecurity.org/bench\\_linux.html](http://www.cisecurity.org/bench_linux.html), p.12.

```
for file in apmd canna FreeWnn gpm hpoj innd irda isdn \
```

```

kdcrotate lvs mars-nwe oki4daemon privoxy rstartd
rusersd \
rwalld rhod spamassassin wine
do
    chkconfig --level 12345 $file off
done
for file in nfs nfslock autofs ypbind ypserv yppasswdd
\
    portmap smb netfs lpd apache httpd tux snmpd \
    named postgresql mysqld webmin squid \
do
    chkconfig --level 12345 $file off
done
for user in rpc rpcuser lp apache http httpd named dns
\
    mysql postgres squid
do
    /usr/sbin/usermod -L $user
done

```

### 3.14 Setup rpm updater: YUM (Yellowdog Updater Modified) or up2date

#### # yum check-update

"check-update" downloads a complete set of headers for base packages for Fedora Core as well as any released updates for Fedora Core.

#### # yum upgrade

"upgrade" will present a list of packages that will be upgraded, newly installed, and obsolete. Choose "y" will download and install the packages. Yum will inform when there aren't new packages to install.

For further information about yum please read Robert G. Brown's article, "YUM: Yellowdog Updater, Modified",

[http://www.phy.duke.edu/~rgb/General/yum\\_article/yum\\_article.pdf](http://www.phy.duke.edu/~rgb/General/yum_article/yum_article.pdf)<sup>63</sup>

## 4.0 Check List

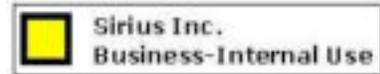
Task	Completed (Yes/No)	Comments
BIOS configuration		
GRUB configuration		
Modification of Network Parameters		
Disallow Remote Root Login		
Disable Ctrl-Alt-Del		
Modify Warning Banners		

Password Aging Modification		
Remove Unnecessary Accounts (users, groups)		
Lock System Accounts		
Verify No Empty Passwords		
Tighten Default umask		
Disable xinetd based services (telnet, wuftp, rlogin, rsh, rexec, tftp, snmpd)		
Disable Standard Boot services (to deactivate unnecessary rc-scripts)		
Setup rpm updater: YUM (Yellowdog Updater Modified) or up2date		

Comments: The task list needs to specify the name of the person that perform the configuration and the time of completion of the tasks.

© SANS Institute 2004, Author retains full rights.

## Appendix G



### Setting up john the ripper

Download or copy the tool from a trusted source into the directory where it is going to get installed and untar the file:

Important: It is recommended to copy the tools from the operations' file server:  
siriusops:/audit-tools/trusted

```
# tar -xvfz john-1.6.tar.gz.tar
```

**Important:** Read the README file and follow instructions.

After untaring the tar file, a new directory john-1.6 gets created. Change to the new directory

```
# cd john-1.6
```

```
# ls
```

```
doc README run src
```

According to the README file the sources are in the /src directory.

```
# cd src
```

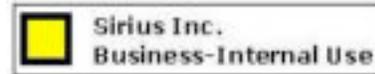
If the type of system where the tool is going to get installed is not properly listed use the "generic" option.

```
# make generic
```

The previous command creates the John binary in /run/john

© SANS Institute 2004, Author retains full rights.

## Appendix H



### Setting up Nessus

#### 1.0 Purpose

This document presents the installation procedure and suggested settings for the security auditing tool Nessus, on a Fedora Core 2. The main purpose is to serve as a guideline or as a quick installation guide. It never pretends to replace documents that follow a more thorough approach. This is a very powerful tool that can intentionally or accidentally cause system crashes and denial of service. Therefore it needs to be used carefully. Better descriptions of the tool and its features can be found in the publications or links presented in the following section of this document.

#### 2.0 Reference

- Renaud Deraison, Raven Alder, Jimmy Alderson, Andy Johnston, George A. Theall, "NESSUS Network Auditing", (Rockland: Syngress Publishing, Inc., 2004)
- Harry Anderson, "Introduction to Nessus", SecurityFocus, October 23, 2003, URL: <http://www.securityfocus.com/printable/infocus/1741>
- Harry Anderson, "Nessus, Part2: Scanning", SecurityFocus, December 16, 2003, URL: <http://www.securityfocus.com/printable/infocus/1753>
- Harry Anderson, "Nessus, Part3: Analyzing Reports", SecurityFocus, December 16, 2003, URL: <http://www.securityfocus.com/printable/infocus/1759>
- Edgeos Inc., has a compilation of documents in their Nessus Knowledge Base: <http://www.edgeos.com/nessuskb/>

#### 3.0 Procedure

There are different ways to install Nessus. This document presents two of the possible options. Option 1 – Downloading and installing RPMs and Option 2 – installing with shell script.

##### Option 1: Downloading RPMs

The Nessus rpm for Fedora Core 2 can be found at:  
<http://rpm.pbone.net/index.php3/stat/4/idpl/1527768/com/nessus-server-2.2.0-17.rhfc2.at.i386.rpm.html>

If you download and install the rpm it is possible that you will get the following error:  
**# rpm -ivh nessus-server-2.2.0-17.rhfc2.at.i386.rpm**  
warning: nessus-server-2.2.0-17.rhfc2.at.i386.rpm: V3 DSA  
signature: NOKEY, key ID 66534c2b

```
error: Failed dependencies:
  libhosts_gatherer.so.2 is needed by nessus-server-2.2.0-
17.rhfc2.at
  libnasl.so.2 is needed by nessus-server-2.2.0-
17.rhfc2.at
  libnessus.so.2 is needed by nessus-server-2.2.0-
17.rhfc2.at
  libpcap-nessus.so.2 is needed by nessus-server-2.2.0-
17.rhfc2.at
```

To solve the dependencies problem, the libraries can get downloaded from the <http://rpm.pbone.net/index.php3>

In order to be able to run Nessus' graphical client, make sure that you have installed the library "gtk+-devel"

If you don't have it you can either download the rpm and install it or run the following command:  
**# yum install gtk+-devel**

### **Option 2: Installing with the shell script**

Lynx, the text-based browser is necessary for this option.

Run the command:

```
# lynx -source http://install.nessus.org | sh
```

**Note:** This is the fastest but least recommended way to install Nessus. This method runs commands from a web server in clear text. As stated in the book "NESSUS Network Auditing"<sup>64</sup>, there are three possible ways that an attacker can take advantage of the security vulnerabilities of this method. First, the TCP session can be hijacked and the attacker can inject data. Second, this method does not offer any integrity check, so in the event that the servers where you are getting the files from were compromised, there is no way to verify that you downloaded bad files. Third, the attacker can poison your DNS data and you can end up downloading the files from a different system than the one that has the good files. All these attacks can result on the installation of trojaned or backdoored files.

After installation you should have the following files:

In /usr/bin/bin:

nasl, nasl-config, nessus, nessus-config (the last two files are for the client application)

In /usr/bin/sbin:

nessus-adduser, nessud, nessus-rmuser, nessus-check-signature, nessus-mkcert uninstall-nessus (nessud is the server)

In /etc/nessus:

nessud.conf, nessud.rules nessud.users

In /usr/lib/nessus:  
plugins

To add a user to the nessus server, use the following command:

**#!/nessus-adduser**

Using /var/tmp as a temporary file holder

Add a new nessusd user

-----

Login : yoly

Authentication (pass/cert) [pass] : pass

Login password :

Login password (again) :

User rules

-----

nessusd has a rules system which allows you to restrict the hosts

that yoly has the right to test. For instance, you may want him to be able to scan his own host only.

Please see the nessus-adduser(8) man page for the rules syntax

Enter the rules for this user, and hit ctrl-D once you are done:

(the user can have an empty rules set)

Login : yoly  
Password : \*\*\*\*\*  
DN :  
Rules :

Is that ok ? (y/n) [y] y

user added.

#

### generating the certificate

**#!/nessus-mkcert**

```
-----
-----
                                Creation of the Nessus SSL
Certificate
-----
-----
```

This script will now ask you the relevant information to create the SSL certificate of Nessus. Note that this information will \*NOT\* be sent to anybody (everything stays local), but anyone with the ability to connect to your Nessus daemon will be able to retrieve this information.

```
CA certificate life time in days [1460]: 360
Server certificate life time in days [365]: 360
Your country (two letter code) [FR]: US
Your state or province name [none]: NJ
Your location (e.g. town) [Paris]: Glen Ridge
Your organization [Nessus Users United]: Sirius
```

```
-----
-----
                                Creation of the Nessus SSL
Certificate
-----
-----
```

Congratulations. Your server certificate was properly created.

/etc/nessus/nessusd.conf updated

The following files were created :

- . Certification authority :
  - Certificate = /usr/com/nessus/CA/cacert.pem
  - Private key = /var/nessus/CA/cakey.pem
- . Nessus Server :
  - Certificate = /usr/com/nessus/CA/servercert.pem
  - Private key = /var/nessus/CA/serverkey.pem

Press [ENTER] to exit

```
#
```

To start the server and run it in the background, use the following command:

```
# ./nessusd -D
```

To check that is running check port 1241 the port that nessus server is listening, use the command:

```
# netstat -an |grep 1241
tcp        0          0 0.0.0.0:1241        0.0.0.0:*
LISTEN
```

#### 4.0 Configuration Options

The man pages for nessusd provides the different configuration options. In order to modify the configuration options for the server, use the editor of your choice. For example:

```
# vi /etc/nessus/nessusd.conf
```

These are some of the configuration options that require special attention:

Option	Function - Comment
safe_checks	This option is used for disabling checks that might cause denial of service (DoS). Enter the following line in the configuration file if you want this option enabled: safe_checks = yes  <b>Important:</b> If you need to perform a scan without the safe_checks option enabled, make sure to you get the proper consent and use it during proper scheduled outage time.
max_checks	This option determines the number of plugins that will run against each host being tested.  <b>Important:</b> Too many plugins at the same time might disable the target host.
max_threads	This option determines the number of simultaneous tests to perform. Remember: # of processes = max_checks X max_hosts This option needs to be properly balanced. Also needs to be tuned according to the capacity of the system performing the scan and the capacity of the network.  <b>Important:</b> Too many threads can affect the network

	performance.
non_simult_ports	Some services can crash if they receive simultaneous connections from the same host. From the nessusd man pages: "The syntax of this option is "port1[, port2....]". Note that you can use the KB notation of nessusd to designate a service formally. Ex: "139, Services/www", will prevent nessusd from making two connections at the same time on port 139 and on every port which hosts a web server." <sup>65</sup>
check_reads_timeout	This option indicates the number of seconds that the security check will wait when performing a recv(). This value should be increase when performing the scan over a slow link.
plugins_timeout	This option determines the maximum lifetime in seconds the plugins. As explained in the NNESSUS Network Auditing book, "This option allows you to make sure your server is never caught in an endless loop because of a non-finishing plugin." <sup>66</sup>
dumpfile	Some plugins issue messages, if you need to record those messages you can designate the file name where you want the output. If you need to preserve disk space it is suggested to set this option to: dumpfile = /dev/null
auto_enable_dependencies	"Nessus plugins use the result of each other to execute their job. For instance, a plugin which logs into the remote SMB registry will need the results of the plugin which finds the SMB name of the remote host and the results of the plugin which attempts to log into the remote host." <sup>67</sup>  Add the following line the nessusd.conf if you want this option enabled: auto_enable_dependencies = yes

**Note:** Please read the nessusd man pages for additional options.

Make sure to update the latest plugins on a regular base. Enter the following command:

```
# /usr/local/sbin/nessus-update-plugins
```

## References

---

<sup>1</sup> David Hoelzer, SANS Track 7 Auditing Networks, Perimeters & Systems, 7.1 – Auditing Principles & Concepts, Class documentation Version 032304, (page 1-22), SANS Washington D.C. July 26 – 31, 2004.

<sup>2</sup> David Hoelzer, SANS Track 7 Auditing Networks, Perimeters & Systems, 7.1 – Auditing Principles & Concepts, (pp. 1-13 to 1-14).

<sup>3</sup> “Introduction: Dell™ Latitude™ CS/CSx Portable Computers User's Guide”, DELL Documents. 04 Nov. 1999. Dell Computer Corporation. August 16, 2004, URL: [http://support.jp.dell.com/docs/systems/pmac2cm/en/en\\_uq/intro.htm](http://support.jp.dell.com/docs/systems/pmac2cm/en/en_uq/intro.htm).

<sup>4</sup> Gary Stonebumer, Alice Goguen and Alexis Feringa, “Risk Management Guide for Information Technology Systems”, (Gaithersburg: National Institute of Standards and Technology, Computer Security Division, Special Publication 800-30, July 2002), 8. October 11, 2004.  
URL: <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>.

<sup>5</sup> Gary Stonebumer, Alice Goguen and Alexis Feringa, 8.

<sup>6</sup> Gary Stonebumer, Alice Goguen and Alexis Feringa, 12.

<sup>7</sup> Harry Anderson, “Introduction to Nessus”, Infocus, October 28, 2003, SecurityFocus, November 12, 2004, URL: <http://www.securityfocus.com/printable/infocus/1741>.

<sup>8</sup> Robert Richardson, 2003 CSI/FBI Computer Crime and Security Survey, Computer Security Institute Publications, July 29, 2004, URL: [http://www.visionael.com/products/security\\_audit/FBI\\_CSI\\_2003.pdf](http://www.visionael.com/products/security_audit/FBI_CSI_2003.pdf), 10.

<sup>9</sup> Lawrence A. Gordon and Martin P. Loeb, 2004 CSI/FBI Computer Crime and Security Survey, Computer Security Institute Publications, July 29, 2004, URL: [http://i.cmpnet.com/gocsi/db\\_area/pdfs/fbi/FBI2004.pdf](http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf), 10.

<sup>10</sup> Lawrence A. Gordon, 14.

---

<sup>11</sup> Timothy J. Louwers and William M. VanDenburgh, "Data Confidentiality in an Electronic Environment," The CPA Journal, March 2003, N. pag., August 16, 2004, URL: <http://www.nysscpa.org/cpajournal/2003/0303/features/f032403.htm>.

<sup>12</sup> Timothy J. Louwers and William M. VanDenburgh, N. pag.

<sup>13</sup> Thomas R. Peltier, Information Security Risk Analysis, (Boca Raton: Auerbach Publications, 2001), 203.

<sup>14</sup> Gary Stonebumer, Alice Goguen and Alexis Feringa, 15.

<sup>15</sup> "The Twenty Most Critical Internet Security Vulnerabilities (Updated)", SANS Portal, Version 5.0 October 8, 2004, SANS Institute, October 14, 2004, URL: <http://www.sans.org/top20/>.

<sup>16</sup> "The Twenty Most Critical Internet Security Vulnerabilities (Updated)", SANS Portal.

<sup>17</sup> "The Twenty Most Critical Internet Security Vulnerabilities (Updated)", SANS Portal.

<sup>18</sup> "The Twenty Most Critical Internet Security Vulnerabilities (Updated)", SANS Portal.

<sup>19</sup> "Vulnerabilities" SecurityFocus. October 12, 2004, SecurityFocus, October 14, 2004. URL: <http://www.securityfocus.com/bid/>.

<sup>20</sup> Stonebumer, Goguen and Feringa, 21.

<sup>21</sup> Stonebumer, Goguen and Feringa, 22.

<sup>22</sup> Stonebumer, Goguen and Feringa, 25.

---

<sup>23</sup> “Unix Security Technical Implementation Guide – Version 4 Release 4”, Defense Information Systems Agency (DISA), September 15, 2003, Computer Security Resource Center (CSRC): Information Technology Security Practices & Checklists / Implementation Guides, (NIST, Computer Security Division), Link to document listed as: UNIX STIG with updated LINUX version (407 KB), October 28, 2004, URL: <http://csrc.nist.gov/pcig/cig.html>.

<sup>24</sup> Murugiah Souppaya, John P. Wack, Anthony Harris, Paul M. Johnson and Karen Kent, “Guide for Checklist Users and Developers”, Computer Security Resource Center (CSRC), Security Configuration Checklists Program for IT Products, (NIST, Computer Security Division, Special Publication 800-70 (DRAFT) ), October 28, 2004, URL: <http://checklists.nist.gov/>.

<sup>25</sup> “Linux Benchmark v1.1.0”, July 29, 2003, The Center for Internet Security (CIS), July 12, 2004, URL: [http://www.cisecurity.org/bench\\_linux.html](http://www.cisecurity.org/bench_linux.html).

<sup>26</sup> David Koconis, Jim Murray, Jos Purvis, Darrim Wassom, “Securing Linux A Survival Guide for Linux Security” Version 1.0, SANS Step-by-Step Series, SANS Press, February 2003, pp. 1 – 23.

<sup>27</sup> Bastille Linux, October 15, 2004, URL: <http://www.bastille-linux.org/>.

<sup>28</sup> Stonebumer, Goguen and Feringa, 20.

<sup>29</sup> Stonebumer, Goguen and Feringa, 20.

<sup>30</sup> Julie H. Allen, “The CERT Guide To System and Network Security Practices”, (Boston: Addison-Wesley, 2001) p. 6.

<sup>31</sup> David Hoelzer, SANS Track 7 Auditing Networks, Perimeters & Systems, 7.1 – Auditing Principles & Concepts, pp. 1-22.

<sup>32</sup> NetAdminTools.com “Building a Security Audit Toolkit” (September 22, 2004) URL: <http://www.netadmintools.com/part279.html>.

---

<sup>33</sup> William Karwisch, "Auditing A Corporate E-mail Gateway Running Postfix on Linux: An Administrator's Perspective", (GSNA Practical version 2.1-option 1, November 8, 2003), Global Information Assurance Certification (GIAC Systems and Network Auditor), July 20, 2004, URL: [http://www.giac.org/practical/GSNA/William\\_Karwisch\\_GSNA.pdf](http://www.giac.org/practical/GSNA/William_Karwisch_GSNA.pdf).

<sup>34</sup> David Koconis, Jim Murray, Jos Purvis, Darrim Wassom, p. 1.

<sup>35</sup> Shon Harris, "Mike Meyer's Certification Passport CISSP" (New York: McGraw-Hill/Osborne, 2002), p.16.

<sup>36</sup> David Koconis, Jim Murray, Jos Purvis, Darrim Wassom, p. 1.

<sup>37</sup> "chkrootkit locally checks for signs of a rootkit", chkrootkit - locally check for signs of a rootkit, September 22, 2004, chkrootkit project, September 22, 2004, URL: <http://www.chkrootkit.org/>.

<sup>38</sup> NetAdminTools.com, URL: <http://www.netadmintools.com/part279.html>.

<sup>39</sup> NetAdminTools.com, URL: <http://www.netadmintools.com/part279.html>.

<sup>40</sup> David Koconis, Jim Murray, Jos Purvis, Darrim Wassom, p. 14.

<sup>41</sup> Mike Shema, Bradley C. Johnson, "Anti-Hacker Tool Kit, Second Edition", (New York: McGraw-Hill/Osborne, 2004), pp. 216 – 228.

<sup>42</sup> David Koconis, Jim Murray, Jos Purvis, Darrim Wassom, p. 15.

<sup>43</sup> "Linux Benchmark v1.1.0", July 29, 2003, The Center for Internet Security (CIS), p.12.

<sup>44</sup> David Hoelzer, SANS Track 7

<sup>45</sup> "The Twenty Most Critical Internet Security Vulnerabilities (Updated)", SANS Portal.

---

<sup>46</sup> “Red Hat Linux 9: Red Hat Linux Security Guide”, Redhat Documentation, 2004, Red Hat Inc., September 30, 2004, URL: <http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/security-guide/ch-security-updates.html>.

<sup>47</sup> Innovative Security Products Inc., <http://www.wesecure.com/>, Image source, URL: <http://www.wesecure.com/secure-notebook-tn.jpg>, (image accessed: November 2, 2004).

<sup>48</sup> “Welcome to the Inspiron & Latitude BIOS FAQ!”, 2004, Bay Wolf, November 28, 2004, <http://www.bay-wolf.com/bios.htm#8>

<sup>49</sup> Paul J. Santos, “How-To Make Linux System Auditing a Little Easier”, GSEC Practical Assignment V.1.4, September 15, 2002, SANS InfoSec Reading Room – Auditing & Assessment, December 15, 2004, URL: <http://www.sans.org/rr/whitepapers/auditing/81.php>.

<sup>50</sup> Flexguard Security Products, Inc., <http://www.flexguard.com/>, (Image accessed December 12, 2004), URL : [http://www.flexguard.com/cat\\_plates.html](http://www.flexguard.com/cat_plates.html).

<sup>51</sup> “Information Sensitivity Policy”, 2004, The SANS Institute – Security Policy Project, August 10, 2004, URL: [http://www.sans.org/resources/policies/Information\\_Sensitivity\\_Policy.pdf](http://www.sans.org/resources/policies/Information_Sensitivity_Policy.pdf).

<sup>52</sup> “Ethics Policy”, 2004, The SANS Institute – Security Policy Project, August 10, 2004, URL: [http://www.sans.org/resources/policies/Ethics\\_Policy.pdf](http://www.sans.org/resources/policies/Ethics_Policy.pdf).

<sup>53</sup> “Acceptable Use Policy”, 2004, The SANS Institute – Security Policy Project, August 10, 2004, URL: [http://www.sans.org/resources/policies/Acceptable\\_Use\\_Policy.pdf](http://www.sans.org/resources/policies/Acceptable_Use_Policy.pdf)

<sup>54</sup> “Password Policy”, 2004, The SANS Institute – Security Policy Project, August 10, 2004, URL: [http://www.sans.org/resources/policies/Password\\_Policy.pdf](http://www.sans.org/resources/policies/Password_Policy.pdf)

<sup>55</sup> “Laptop Security & Notebook Security Tips”, Innovated Security Products, Inc., (November 11, 2004), URL: <http://www.wesecure.com/laptop-security.htm>

<sup>56</sup> David Koconis, Jim Murray, Jos Purvis, Darrim Wassom, pp. 1 – 23.

---

<sup>57</sup> “Linux Benchmark v1.1.0”, July 29, 2003, [The Center for Internet Security \(CIS\)](#).

<sup>58</sup> David Koconis, Jim Murray, Jos Purvis, Darrim Wassom, p 7.

<sup>59</sup> David Koconis, Jim Murray, Jos Purvis, Darrim Wassom, p 9.

<sup>60</sup> David Koconis, Jim Murray, Jos Purvis, Darrim Wassom, p 11.

<sup>61</sup> David Koconis, Jim Murray, Jos Purvis, Darrim Wassom, p 12.

<sup>62</sup> David Koconis, Jim Murray, Jos Purvis, Darrim Wassom, p 12.

<sup>63</sup> Robert G. Brown, “YUM: Yellowdog Updater, Modified”, December 17, 2003, Duke University Physics Department, October 10, 2004, URL: [http://www.phy.duke.edu/~rgb/General/yum\\_article/yum\\_article.pdf](http://www.phy.duke.edu/~rgb/General/yum_article/yum_article.pdf)

<sup>64</sup> Renaud Deriason, Raven Alder, Jimmy Alderson, Andy Johnston, George A. Theall, “NESSUS Network Auditing” (Rockland: Syngress Publishing, Inc., 2004), p. 47.

<sup>65</sup> “nessusd”, 2004, Tenable Network Security™, November 15, 2004, URL: <http://www.nessus.org/doc/nessusd.html>.

<sup>66</sup> Renaud Deriason, Raven Alder, Jimmy Alderson, Andy Johnston, George A. Theall, p. 73,

<sup>67</sup> “nessusd”, 2004, Tenable Network Security™.

# Upcoming SANS IT Audit Training

CLICK HERE TO  
**{REGISTER NOW}**



**AUDIT CHECKLIST**  
 Audit Satisfactory  
 Nonconformances Found  
 Observations Made

Community SANS @ CANHEIT	Ottawa, ON	Jun 13, 2013 - Jun 14, 2013	Community SANS
SANSFIRE 2013	Washington, DC	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS vLive - SEC566: Implementing and Auditing the Twenty Critical Security Controls - In-Depth	SEC566 - 201307,	Jul 08, 2013 - Aug 07, 2013	vLive
Community SANS Chicago	Chicago, IL	Jul 08, 2013 - Jul 12, 2013	Community SANS
SANS Rocky Mountain 2013	Denver, CO	Jul 14, 2013 - Jul 20, 2013	Live Event
Critical Security Controls Summit	Washington, DC	Aug 12, 2013 - Aug 18, 2013	Live Event
Community SANS Dallas	Dallas, TX	Aug 19, 2013 - Aug 22, 2013	Community SANS
SANS vLive - AUD507: Auditing Networks, Perimeters, and Systems	AUD507 - 201309,	Sep 02, 2013 - Oct 16, 2013	vLive
SANS CyberCon Fall 2013	Online, VA	Sep 09, 2013 - Sep 14, 2013	CyberCon
Network Security 2013	Las Vegas, NV	Sep 14, 2013 - Sep 23, 2013	Live Event
Community SANS Miami	Miami, FL	Sep 16, 2013 - Sep 19, 2013	Community SANS
Network Security 2013 - SEC566: Implementing and Auditing the Twenty Critical Security Controls - In-Depth	Las Vegas, NV	Sep 16, 2013 - Sep 20, 2013	vLive
Mentor Session - SEC 566	Troy, MI	Oct 01, 2013 - Dec 10, 2013	Mentor
Community SANS Washington @ GWU	Washington, DC	Oct 07, 2013 - Oct 10, 2013	Community SANS
SANS Baltimore 2013	Baltimore, MD	Oct 14, 2013 - Oct 19, 2013	Live Event
SOS SANS October Singapore 2013	Singapore, Singapore	Oct 21, 2013 - Nov 02, 2013	Live Event
SANS Chicago 2013	Chicago, IL	Oct 28, 2013 - Nov 02, 2013	Live Event
Community SANS New York	New York, NY	Nov 04, 2013 - Nov 07, 2013	Community SANS
SANS Sydney 2013	Sydney, Australia	Nov 11, 2013 - Nov 23, 2013	Live Event
SANS London 2013	London, United Kingdom	Nov 16, 2013 - Nov 25, 2013	Live Event
Community SANS Toronto	Toronto, ON	Nov 18, 2013 - Nov 21, 2013	Community SANS
SANS vLive - SEC566: Implementing and Auditing the Twenty Critical Security Controls - In-Depth	SEC566 - 201312,	Dec 02, 2013 - Jan 15, 2014	vLive
Community SANS Vancouver	Burnaby, BC	Dec 09, 2013 - Dec 12, 2013	Community SANS
North America ICS Security Summit & Training 2014	Lake Buena Vista, FL	Mar 11, 2014 - Mar 20, 2014	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced