



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Auditing Systems, Applications, and the Cloud (Audit 507)"
at <http://www.giac.org/registration/gсна>

Audit of a University's MySQL Server running on SuSE 8.0 Linux

**GSNA Practical Assignment
Version 3.1, Option #1**

Charles Crawford

Abstract

A department for a University has launched a project in which several Intrusion Detection sensors and port and vulnerability scanning clusters will be logging data to a central server. The overall goal of this project is to have a central repository updated in real time of all IP addresses on their network. This database will house information such as IDS alerts, NESSUS scans and NMAP scans for these IP Addresses. As an alert is registered in the IDS sensor or as a vulnerability is found from a probe, a lookup can automatically occur finding the host and notifying appropriate contacts.

The security of this database especially in regards to its integrity and enforcing non-repudiation is critical. This database is running MySQL version 11.18 Distribution 3.23.52 on a Dell PowerEdge box with SuSE Linux 8.0.

For the purpose of this audit and since this box is already in production, we will assume that the current integrity of the box is clean, in other words it has not been compromised. We will develop an audit checklist to audit this system and to help enforce system hardening. This checklist will include both the operating system and the database instance.

© SANS Institute 2005, Author retains full rights.

Table of Contents

Abstract.....	2
Table of Contents	3
The System to be Audited.....	5
System Components Overview	6
The Risks	7
Threat Impact Analysis	8
Security Results Database.....	9
Vulnerability Analysis	9
Current State of Practice	11
Ten MySQL Best Practices	11
Securing Linux	12
MySQL Database Audit Checklist.....	14
Checklist Item 1 – Nonprivileged account for MySQL instance.....	14
Ten MySQL Best Practices	14
Checklist Item 2 – MySQL installation Directory security.....	15
Ten MySQL Best Practices	15
Checklist Item 3 - Set a password for the “root” User.....	15
Ten MySQL Best Practices	15
Checklist Item 4 – Hide MySQL from rest of world.....	16
Ten MySQL Best Practices	16
Checklist Item 5 – UnPatched MySQL Application.....	17
Checklist Item 6 – Personnel MySQL database administration experience.....	18
Checklist Item 7 – MySQL Global Option File	18
Checklist Item 8 – Renamed MySQL root account.....	19
Ten MySQL Best Practices	19
Checklist Item 9 – No anonymous accounts.....	20
Checklist Item 10 – Remove Default users /db	20
SuSe Linux Audit Checklist	21
Checklist Item 11 – Host communication restrictions	21
Checklist Item 12 – System hardening – Services	23
Checklist Item 13 – System Patched / Updated.....	24
Checklist Item 14 – Limited user Accounts	25
Checklist Item 16 – System Logging.....	26
Checklist Item 18 – User staffing/training	28
Checklist Item 19 – System hardening – File Permissions.....	28
Conducting the Audit – Testing and Findings.....	30
Checklist Item 1 – Nonprivileged account for MySQL instance.....	30
Ten MySQL Best Practices	30
Checklist Item 3 - Set a password for the “root” User.....	31
Ten MySQL Best Practices	31
Checklist Item 4 – Hide MySQL from rest of world.....	32
Ten MySQL Best Practices	32

Checklist Item 5 – UnPatched MySQL Application.....	34
Checklist Item 11 – Host communication restrictions	35
Checklist Item 12 – System hardening – Services	38
Checklist Item 13 – System Patched / Updated.....	40
Checklist Item 14 – Limited user Accounts	41
Checklist Item 18 – User staffing/training	43
Checklist Item 19 – System hardening – File Permissions.....	44
Audit Report	45
Executive Summary	45
Findings	46
Finding Details	46
Checklist Item 1 – Nonprivileged account for MySQL instance.....	47
Checklist Item 3 - Set a password for the “root” User	47
Checklist Item 4 – Hide MySQL from rest of world.....	48
Checklist Item 5 – UnPatched MySQL Application	50
Checklist Item 11 – Host communication restrictions.....	50
Checklist Item 12 – System hardening – Services.....	51
Checklist Item 13 – System Patched / Updated.....	52
Checklist Item 14 – Limited user Accounts	53
Checklist Item 18 – User staffing/training	54
Checklist Item 19 – System hardening.....	55
Recommendations:.....	56
Costs:.....	56
Works Consulted	56

© SANS Institute 2005, Author retains full rights.

The System to be Audited

This audit will be conducted against a Dell PowerEdge 2650 running MySQL and SuSE Linux 8.0. Interesting and possibly difficult hurdles that will be faced during this audit relate to the lack of information specific SuSE Linux. SuSE Linux has recently begun to get more attention with its recent alliance with Novell.

A brief listing of the database server's hardware and software is:

- Dell PowerEdge 2650 Chassy
- 4 GB Ram
- Dual 3.2 GHz Pentium Processor
- 2 18GB SCSI Drives RAID 0
- 3 36GB SCSI drives RAID 10
- 2 Power Supplies
- CD-Rom
- Floppy
- 10/100/1000 NIC
- MySQL 11.18 Distrib 3.23.52 for pc-linux (i686)
- Syslog

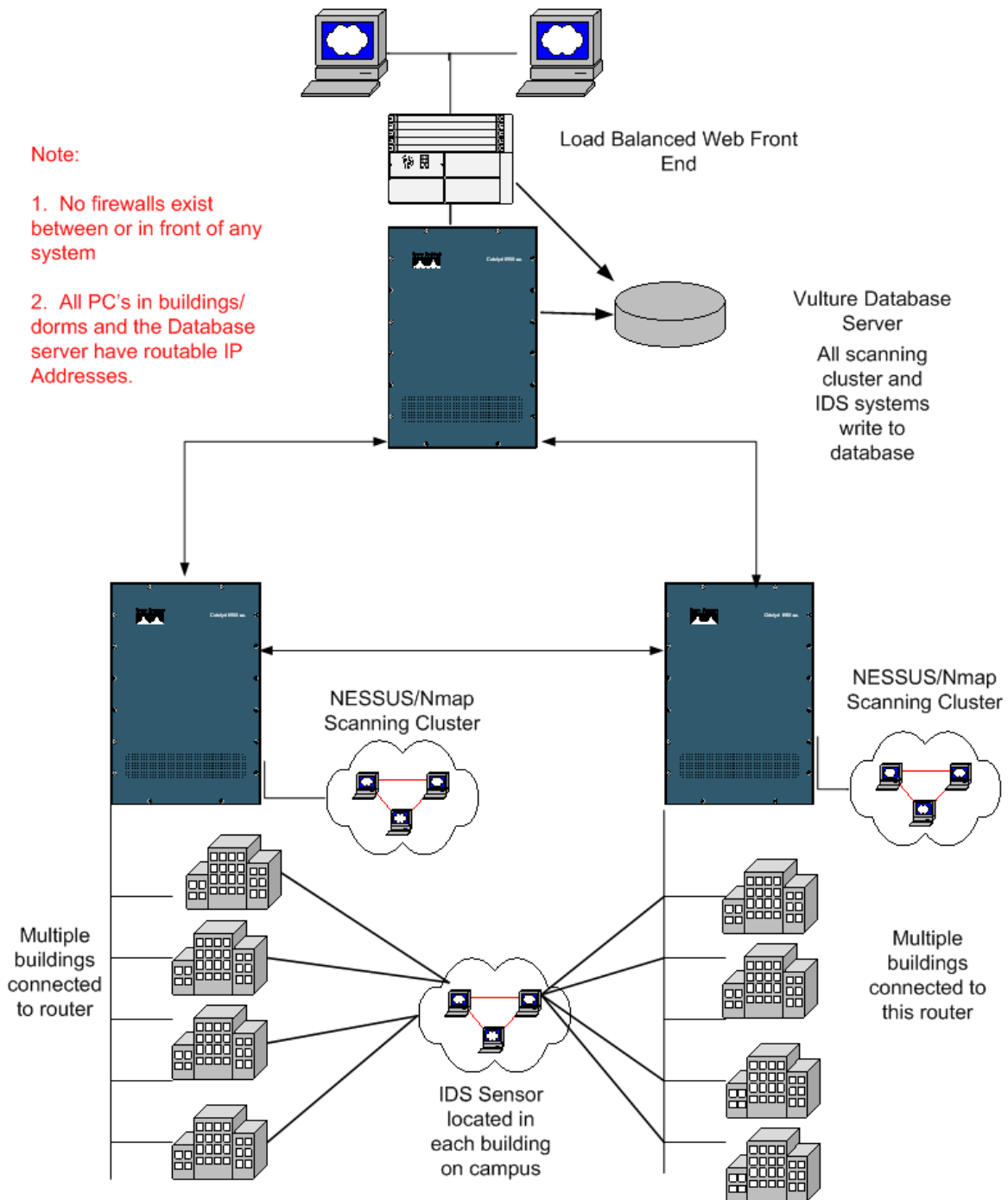
A topology diagram of the systems that input and extract information into and from this database is provided in the next page. The name of the project this database belongs to is CIRCE, (Computer Incident Reconnaissance Collection Engine)

This database is to be hardened to only accept connections from scanning cluster hosts, IDS sensors, and certain system administrator machines. To be more specific, there will be over 60 IDS sensors, 8 scanning hosts 2 LDAP trees, a scheduling server, 2 load balanced web front end servers, 5 developers, and at least 4 system administrators needing to touch this database server is some way or another.

Because of the criticality of this database to keep this CIRCE system running and the importance of the data residing on this system to not be tampered with (thus the enforcing of data integrity) or stolen, it is extremely important this system be highly available, and secure.

To add to the complication, this system was designed for a decentralized environment. It was intended for departmental system administrators to log into the web front end and only see data that resides on CIDR blocks (Classless Inter-Domain Routing) that they are in control over. Therefore, role based access and viewing must also be enforced.

System Components Overview



The Risks

This section will outline and document the risks associated with this system. Before we go into definitions and examples of risk, we must also remember that this system resides on a major research university network. Universities are notorious for being wide open and having any type of virus infestation, operating system and application vulnerability imaginable. University networks can be a script kiddies, hackers, and phreakers playground.

Let's first layout some key terms that we will be using throughout this document. I will reference "Information Security Managers Handbook Volume 4" by Harold Tipton and Micki Krause for these terms, although you can find these definitions in many reference materials including www.nist.gov and the ISC2 CISSP study guide.

Threats: A threat is a force that could affect an organization or an element of an organization. Threats can be either external or internal to an organization.

A threat can be man made or something that occurs in nature, (IE being in the heartland, Tornadoes, Wild Fires, etc).

Vulnerability: A weakness or condition of an organization that could permit a threat to take advantage of the weakness to affect its performance.

An obvious example, unpatched operating systems on computer workstations.

Safeguards: Or controls, measures that are designed to prevent, detect, protect, or sometimes react to reduce the likelihood – or to completely mitigate the possibility – of a threat to exploit an organization's vulnerabilities.

A typical safeguard could include firewalls both host based or network based, antivirus software, intrusion prevention and security awareness could all fall into this category.

After implementing safeguards to take care of threats and hopefully address vulnerabilities you are now left with what is called **residual risk**. To clarify, residual risk is the examination of each vulnerability along with its existing safeguard.

Likelihood: An overall rating that indicates the probability that a potential vulnerability may be exercised.

Being a university with little to no control of network traffic, the likelihood of a vulnerability being exercised will be higher than a normal commercial or private network environment.

Impact: The loss resulting from the successful threat exercise of vulnerability.

Threat Impact Analysis

Threat	Impact
Wide Open University Network	Easy reconnaissance – Increased likelihood of probing and scanning for vulnerabilities. Essentially most universities are developed with little or no security in place, especially heavy research institutions. Without basic ingress or egress filtering, or simple firewalls or packet filters in place, scanning and port probing occur constantly. Performance degradation on network bandwidth Easy DOS or DDOS target (Denial of service or Distributed Denial of Service)
Academic Freedom	Due to this being a major research university, users are accustomed to doing what they want on the network when they want to. Very little policies exist on acceptable use.
Hardware failure	No logging of malicious or nefarious activity or vulnerability scanning. A compromise can occur without being logged.

Key Person Dependency	If this database is only managed by one individual and that individual is gone during a time where the database needs to be reindexed, rebuilt, etc many problems can occur.
Power Failure	System resides in an older building with power issues
Disaster (either Natural or Human)	Building has been attacked "bombed" in the past. Also located in "Tornado Alley".

Security Results Database

Implementing security in a network that was intentionally built to be open and decentralized has been a challenge. In a world where arguing the right of privacy and academic freedom is a daily occurrence, yet the requirement to keep Research Grants, FERPA, HIPAA (Health Information Protection Accountability Act), SOX (Sarbanes Oxley), and GLBA (Graham Leach Bliley) covered entities secure is scattered throughout.

Role of Security Results Database	Information Asset Affected
Store information on all campus IDS alerts, vulnerability audits, and Nmap probes. Also acts as Campus critical system syslog server.	<p>Security monitoring for malicious campus activity. The IDS sensors will still be working, but accessing the alerts will not be possible.</p> <p>Also all automatic correlation of vulnerable systems to an IP and location will be affected. Tracking down vulnerable systems in a decentralized environment will take much longer than the time we have to address the vulnerability.</p> <p>Centralized syslogging of activity on campus critical systems will not be possible.</p>

Vulnerability Analysis

Vulnerability as defined above is a weakness or condition of an organization that could permit a threat to take advantage of the weakness to affect its performance.

The exposure factor in this case is expressed in a magnitude of either: Low, Medium or Hi. The potential impact being what the impact to the organization would be if the vulnerability were exploited. The potential impact is addressed in relation to which of the 3 primary objectives of security is related, Confidentiality, Integrity or Availability.

Vulnerability	Degree of Exposure	Potential Impact
Unpatched Operating System	High	<ul style="list-style-type: none"> • Data loss • Integrity of data • System vulnerabilities now in wrong hands
Unpatched MySql application	High	<ul style="list-style-type: none"> • Data loss • Integrity of data • System vulnerabilities now in wrong hands
Denial of service	High	<ul style="list-style-type: none"> • No logging of malicious or nefarious activity on campus
Weak Passwords MySQL Database	Low	<ul style="list-style-type: none"> • Easy access to systems without strong passwords
Weak passwords Operating System	Med	<ul style="list-style-type: none"> • Easy access to systems without strong passwords
Lack of System Hardening	High	<ul style="list-style-type: none"> • Integrity of data • Data Loss
Insufficient Logging	Low	<ul style="list-style-type: none"> • Data integrity <ul style="list-style-type: none"> ○ Lack of audit trail in case of compromise or attempted compromise. ○ Lack of audit trail for change control
Insecure Remote Administration	Low	<ul style="list-style-type: none"> • Data Integrity – Hijacked session and data manipulation • Possible Data Availability in case of

		hijacked session turned into a Denial of Service
Insufficient Access Controls	Med	<ul style="list-style-type: none"> Unauthorized user access by session hijacking, brute force, etc can result in <ul style="list-style-type: none"> Data Availability Data Integrity
Lack of Power in Building	Med	<ul style="list-style-type: none"> Due to loss of power or building data availability can be an issue
Lack of Expertise in Database Administration	Med	<ul style="list-style-type: none"> Due to improper training and experience, this system can be misconfigured and allow unauthorized access. System integrity, availability affected
Lack of Expertise in SuSE Linux Administration	Med	<ul style="list-style-type: none"> Due to improper training and experience, this system can be misconfigured and allow unauthorized access. System integrity, availability affected

Current State of Practice

Ten MySQL Best Practices

by [George Reese](#), coauthor of [Managing & Using MySQL, 2nd Edition](#)
07/11/2002 URL:
<http://www.onlamp.com/pub/a/onlamp/2002/07/11/MySQLtips.html>

Outlined in this site explains 10 simple steps an admin should perform prior to implementing a MySQL server into production. Many times the issue of

convenience versus security is faced in an administrators day to day job function. What time frame is the project under, how soon does this system need to be “productional”. This site lists the 10 best practices with “how to’s” for quick and easy reference.

- 1 Set a password for the “root” User and then rename the user
- 2 Hide MySQL from the Internet
- 3 Protect the MySQL installation directory from access by other users
- 4 Don’t store binary data in MySQL
- 5 Stick to ANSI SQL
- 6 Create your own sequence generation scheme
- 7 Do not mix display code and database code
- 8 Normalize with zeal, denormalize sparingly.
- 9 Use connection pooling in Web servers and application servers
- 10 Tune your queries with EXPLAIN SELECT

MySQL Administrator Best Practices

URL: <http://dev.mysql.com/tech-resources/articles/mysql-administrator-best-practices.html>

This site goes on to explain the importance of optimizing the Performance of the database server by ensuring you have a well designed database schema and fine tuned server to run the MySQL instance. The site also explains the importance of user administration and privilege granting along with disaster recovery and the need for a good backup/restore plan. Finally the site explains the need for space management. Many times databases can fluctuate in size or growth anticipation of data is not taken into consideration when designing or sizing the server.

Making MySQL Secure Against Attackers

URL: http://dev.mysql.com/doc/mysql/en/Security_against_attack.html

Auditing a MySQL database Server

By Jeff Hoover URL:

http://www.giac.org/practical/GSNA/Jeff_Hoover_GSNA.pdf

This document is a good paper providing a checklist to audit a MySQL database. Also lists references to other sources for MySQL hardening and administration.

Securing MySQL: step-by-step:

<http://www.securityfocus.com/infocus/1726>, Artur Maj, August 28, 2003

Securing Linux

The Rookery: Security Tools in Linux Distributions, Part II

Posted on Monday, October 07, 2002 by [Bobby S. Wen](#)

URL: <http://www.linuxjournal.com/article.php?sid=6362>

This site offers a great explanation of the SuSE linux installation and the different security packages available. It lists applications that are installed by default as well as applications that should be (Snort, Nessus, Scanlod, Tripwire, Arpwatch, etc).

The site goes on to explain the use of SuSE linux's YaST2 security setting control tool. A great tool that allows the user to have an interactive graphical user interface.

An example or suggested best practice for "Seccheck". A SuSE linux tool used for checking and assessing host security. It lists items to be checked both daily and weekly.

Other Resources on Linux

- <http://ccfaq.valar.co.uk/modules.php?name=News&file=article&sid=105> A great over on linux permissions
- <http://shelob.temple.edu/suse/local/SuSE-Linux-Adminguide-8.2.0.1x86.pdf>
- <http://www.sans.org/rr/papers/32/1294.pdf>
- http://www.securitydocs.com/Operating_System/
Offers great hardening guides and best practices information for different operating systems.
- <http://www.linuxvoodoo.org/resources/guides/>
Provides links to user guides, administrator guides both for the OS and kernel level.
- <http://www.linuxhq.com/guides/index.html>
Excellent site providing links to information for Getting started, System Administrators, Network Administrators, programmers and discussing the Linux Kernel.
- http://www.suse.com/us/private/products/suse_linux/prof/security.html
- http://www.suse.com/us/private/products/suse_linux/prof/yast.html
- http://www.justlinux.com/nhf/Security/Securely_Installing_Linux.html

MySQL Database Audit Checklist

Checklist Item 1 – Nonprivileged account for MySQL instance

Reference	<p>Auditing a MySQL database Server By Jeff Hoover URL: http://www.giac.org/practical/GSNA/Jeff_Hoover_GSNA.pdf</p> <p>Ten MySQL Best Practices by George Reese, coauthor of Managing & Using MySQL, 2nd Edition 07/11/2002 URL: http://www.onlamp.com/pub/a/onlamp/2002/07/11/MySQLtips.html</p>
Risk	Low- Running applications or daemons in a “root” privilege mode can allow potential escalation for an unauthorized attacker if they were to gain access to the box. Data Integrity, availability and confidentiality are at risk
Testing	<p>Assuming you are at a command or shell prompt on the server, check the my.cnf file running under the /etc directory on the system. A simple “<i>cat /etc/my.cnf</i>” should display the results needed to make this determination.</p> <p>The results should be displayed: [mysqld] User=name</p> <p>View current processes running on the system as well to ensure that the MySQL server instance is running as the specified user</p> <p>“<i>ps -aux grep -l mysql</i>”</p>
Compliance Criteria	The MySQL server should be running as mysql or another unprivileged user
Test Nature – Objective or Subjective	Objective

Evidence	
Finding	

Checklist Item 2 – MySQL installation Directory security

Reference	Ten MySQL Best Practices by George Reese , coauthor of Managing & Using MySQL, 2nd Edition 07/11/2002 URL: http://www.onlamp.com/pub/a/onlamp/2002/07/11/MySQLtips.html Securing MySQL: step-by-step: http://www.securityfocus.com/infocus/1726 , Artur Maj, August 28, 2003
Risk	Low – Not having proper permissions on this directory can allow a potential unauthorized user to manipulate data. Data Integrity and Availability are most at risk.
Testing	The MySQL directory on a default installation resides at /usr/local/mysql Assuming you are at a command or shell prompt of the server, by navigating to that directory, (cd /usr/local) and typing “ls -la” you should see what permissions reside with what directory
Compliance Criteria	The directory should be owned by mysql:mysql with permissions of rwx for the owner (mysql) rwx-----
Test Nature-Objective or Subjective	Objective
Evidence	
Finding	

Checklist Item 3 - Set a password for the “root” User

Reference	Ten MySQL Best Practices by George Reese , coauthor of Managing & Using MySQL, 2nd Edition
------------------	--

	<p>07/11/2002 URL: http://www.onlamp.com/pub/a/onlamp/2002/07/11/MySQLtips.html</p> <p>Securing MySQL: step-by-step: http://www.securityfocus.com/infocus/1726, Artur Maj, August 28, 2003</p> <p>Auditing a MySQL database Server By Jeff Hoover URL: http://www.giac.org/practical/GSNA/Jeff_Hoover_GSNA.pdf</p>
Risk	High - running an application without a password can easily allow an unauthorized user to gain additional access to information
Testing	<p>This can be accomplished a couple of ways, assuming you have console access to the database server or are on a system that has remote access to the system.</p> <ol style="list-style-type: none"> 1. Running this from the shell prompt of the server: mysql -h host -u user -p 2. Run the query below against the mysql.user table (case sensitive) <p style="text-align: center;">SELECT User, Host FROM mysql.user WHERE Password = “;</p>
Compliance Criteria	Zero rows should be returned from this query
Test Nature- Objective or Subjective	Objective
Evidence	
Finding	

Checklist Item 4 – Hide MySQL from rest of world

Reference	<p>Ten MySQL Best Practices</p> <p>by George Reese, coauthor of Managing & Using MySQL, 2nd Edition</p> <p>07/11/2002 URL: http://www.onlamp.com/pub/a/onlamp/2002/07/11/MySQLtips.html</p>
------------------	--

Risk	High– Having this system exposed allows potential unauthorized access resulting in Availability and Integrity issues
Testing	<p>2 tests should be run from 2 locations.</p> <ol style="list-style-type: none"> 1 run Nmap from an IP or a host that is allowed (or should be allowed) to talk to the database server. This Nmap instance is to verify that only specific services are running. <p>Running a simple NMap against this host to look for MySQL will take care of this. (flags are case sensitive)</p> <p>From a shell prompt or a command prompt type</p> <p style="text-align: center;"><i>Nmap -sS -O -v -p 1-65535 (IP of system)</i></p> <ol style="list-style-type: none"> 2. From a shell prompt or a command prompt from a random location and a different IP address than the one used above run the following command: Ping (IP of system)
Compliance Criteria	<p>A default installation of MySQL runs on port 3306. The Nmap result should only list 3306 and SSH port 22 for secure remote administration.</p> <p>The second test should time out if you are on a host that is not supposed to talk directly to this system. Messages received may be “request timed out”, Destination Host Unreachable”, etc</p>
Test Nature – Objective or Subjective	Objective
Evidence	
Finding	

Checklist Item 5 – UnPatched MySQL Application

Reference	Personal Best Practice
Risk	High – Unpatched sytems can allow unauthorized users to exploit a vulnerability. Integrity and Availability
Testing	You can check which version of MySQL you are running by

	going to the bin directory and executing Mysqldadmin version
Compliance Criteria	The MySQL version should be up to date and patched. You can verify any vulnerabilities or what the newest version is by looking at www.securityfocus.com/bid or http://dev.mysql.com/downloads/ for new updates or security patches
Test Nature – Objective or Subjective	Objective
Evidence	
Finding	

Checklist Item 6 – Personnel MySQL database administration experience

Reference	Personal Experience
Risk	High – Inexperienced or untrained admin can configure a box improperly or insecure allowing an unauthorized user to gain access. Data Integrity, Confidentiality and Availability can be affected.
Testing	Interviewing the current Database administrator to check on past database experience, training attended, certifications, etc
Compliance Criteria	Proof of past projects, current training, certifications should be presented.
Test Nature – Objective or Subjective	Subjective
Evidence	
Finding	

Checklist Item 7 – MySQL Global Option File

Reference	Securing MySQL: step-by-step: http://www.securityfocus.com/infocus/1726 , Artur Maj, August 28, 2003
------------------	--

Risk	<p>Med – Restricting rights on this file is crucial as it holds specific configuration information for the MySQL database, including directory layout, and possible passwords.</p> <p>Data Integrity, confidentiality and availability can be affected</p>
Testing	<p>Navigate to the my.cnf file under the /etc directory. Performing a simple “ls -la “ command should display permissions for this file</p>
Compliance Criteria	<p>The directory should be owned by mysql.mysql with permissions of rwx for the owner (mysql) rwx-----</p>
Test Nature – Objective or Subjective	<p>Objective</p>
Evidence	
Finding	

Checklist Item 8 – Renamed MySQL root account

Reference	<p>Ten MySQL Best Practices</p> <p>by George Reese, coauthor of Managing & Using MySQL, 2nd Edition 07/11/2002 URL: http://www.onlamp.com/pub/a/onlamp/2002/07/11/MySQLtips.html</p> <p>Making MySQL Secure Against Attackers URL: http://dev.mysql.com/doc/mysql/en/Security_against_attack.html</p> <p>Securing MySQL: step-by-step: http://www.securityfocus.com/infocus/1726, Artur Maj, August 28, 2003</p>
Risk	<p>Med – Running applications or daemons in a “root” privilege mode can allow potential escalation for an unauthorized attacker if they were to gain access to the box. Data Integrity, availability and confidentiality are at risk</p>
Testing	<p>The mysql.user table should not have an entry for root Running a query against this table should return zero results.(case sensitive) and assuming you have console access to the database server or are on a system that has remote access to the system.</p>

	Select mysql.user, Host From user Where User ='root'
Compliance Criteria	The selected query should return no results
Test Nature – Objective or Subjective	Objective
Evidence	
Finding	

Checklist Item 9 – No anonymous accounts

Reference	Making MySQL Secure Against Attackers URL: http://dev.mysql.com/doc/mysql/en/Security_against_attack.html Auditing a MySQL database Server By Jeff Hoover URL: http://www.giac.org/practical/GSNA/Jeff_Hoover_GSNA.pdf
Risk	Low – Allowing anonymous connections to a database and server greatly reduces any security in place. Data integrity and availability are at risk
Testing	Assuming you have console access to the database server or are on a system that has remote access to the system run the query below against the mysql.user table to ensure that all accounts do not have an empty user field. SELECT {user, Host}FROM mysql.user WHERE user =";
Compliance Criteria	The selected query should return no results
Test Nature – Objective or Subjective	Objective
Evidence	
Finding	

Checklist Item 10 – Remove Default users /db

Reference	Securing MySQL: step-by-step: http://www.securityfocus.com/infocus/1726 , Artur Maj, August 28, 2003
Risk	Med – By having extra databases installed in a default configuration, allows another vector in which an unauthorized person can attempt to exploit. Data Integrity, availability are at risk
Testing	Assuming you have console access to the database server or are on a system that has remote access to the MySQL system you can enter the following command: once logged into MySQL, type <i>show databases</i> ;
Compliance Criteria	Only the relevant and used databases should be returned. Default database such as test should not be listed. Other databases no longer used should not be available or listed as well.
Test Nature – Objective or Subjective	Objective
Evidence	
Finding	

SuSe Linux Audit Checklist

Checklist Item 11 – Host communication restrictions

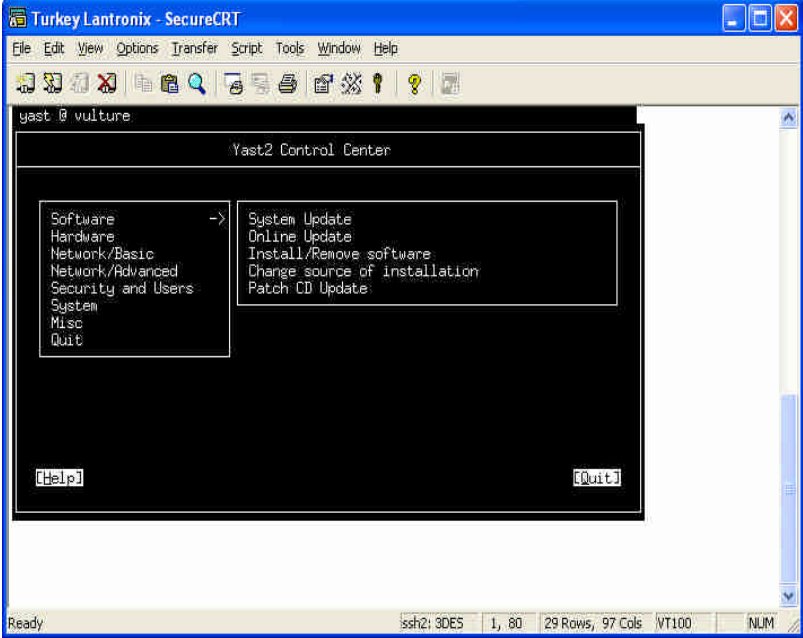
Reference	http://www.securityfocus.com/printable/infocus/1419
Risk	High – Without restrictions in place for allowing or denying which hosts can talk to this system, potential unauthorized access can be made. An attacker can run exploits from any source. System Availability and Integrity are at risk
Testing	Several areas can be examined. Assuming you are at a command or shell prompt on the server,

	<ol style="list-style-type: none"> 1. Typing “cat /etc/hosts.allow” or “cat /etc/hosts.deny” 2. Typing “<i>netstat -rn</i>” in case any host routes are implemented instead of a default route are great examples. 3. Ping from random hosts. Go to a prompt on a workstation and type “Ping xxx.xxx.xxx (IP of Database Server)”
Compliance Criteria	<ol style="list-style-type: none"> 1. Look for statements similar to “Example 2: grant access from local net, reject with message from elsewhere. # in.telnetd : ALL EXCEPT LOCAL : ALLOW # in.telnetd : ALL : \ # twist /bin/echo -e "\n\raccess from %h declined.\n\rGo away.";sleep 2 # # # Example 3: run a different instance of rsyncd if the connection comes # from network 172.20.0.0/24, but regular for others: # rsyncd : 172.20.0.0/255.255.255.0 : twist /usr/local/sbin/my_rsyncd-script” 2. The “netstat -rn” command should return the routing table on the system. Look to see if a default route is in place. This can be found by looking for a “0.0.0.0” in the destination field followed by an address in the gateway field. If a default gateway is listed, static routes are probably not in place and this system is probably accessible anywhere on the network. Also look for specific routes. These are displayed by having a full IP in the destination, followed by the gateway address and finally the subnet address. If specific routes are listed, it is likely that an attempt has been made to only allow specific hosts to talk to this system. 3. Pinging from random hosts will give you a variety of replies. A “reply from” means successful communication to this host, ie this host is allowed to talk to this server. Other replies may be “request timed out” or “destination host unreachable”. Either the host is not allowed to talk to this server or the

	<p>location where you are pinging from does not know how to get to the destination.</p> <p>If you can successfully ping a host, make sure that the IP range you are pinging from is supposed to be talking to this system.</p>
Test Nature – Objective or Subjective	Objective
Evidence	
Finding	

Checklist Item 12 – System hardening – Services

Reference	<p>http://www.justlinux.com/nhf/Security/Securely_Installing_Linux.html http://www.securityfocus.com/printable/infocus/1419 The Rookery: Security Tools in Linux Distributions, Part II Posted on Monday, October 07, 2002 by Bobby S. Wen URL: http://www.linuxjournal.com/article.php?sid=6362</p>
Risk	High – Having unnecessary services running allows many more potential areas to be exploited.
Testing	<p>Several areas can be examined.</p> <ol style="list-style-type: none"> 1. Using the SuSE Linux YaST tool (typing <i>yast2</i>) from a prompt:

	 <p>a. You can navigate to the install remove software section to look for unneeded software running</p> <p>b. One could also examine the <code>/etc/inet.d</code> file. Simply typing <code>grep -v "^#" /etc/inetd.conf</code>. This will show all services that will be set to run.</p> <p>c. Typing <code>netstat -an</code> at a prompt will also list what ports your machine is listening for connections on.</p>
Compliance Criteria	Results of these tests should imply that only SSH (port 22) and MySQL port 3306 is running on this system. Other services such as FTP (port 21), SMTP (port 25), etc should not be running on this server.
Test Nature – Objective or Subjective	Objective
Evidence	
Finding	

Checklist Item 13 – System Patched / Updated

Reference	http://www.justlinux.com/nhf/Security/Securely_Installing_Linux.html http://www.securityfocus.com/printable/infocus/1419 http://www.suse.com/us/private/products/suse_linux/prof/security.html http://www.suse.com/us/private/products/suse_linux/prof/yast.html http://shelob.temple.edu/suse/local/SuSE-Linux-Adminguide-
------------------	---

	8.2.0.1x86.pdf
Risk	High – Unpatched systems can allow unauthorized users to exploit a vulnerability. Integrity and Availability are at Risk
Testing	With SuSE Linux you can run the YaST Tool to check for system updates. Simply typing “ <i>yast2 online_update .auto.get security</i> ” at a command or shell prompt on the server
Compliance Criteria	No patches should be found or need to be installed if this system is fully patched. If a list of patches to be installed is returned, this system is not patched.
Test Nature – Objective or Subjective	Objective
Evidence	
Finding	

Checklist Item 14 – Limited user Accounts

Reference	http://www.justlinux.com/nhf/Security/Securely_Installing_Linux.html
Risk	Med – Provides another vector that an unauthorized user can try to exploit. Another account to manage
Testing	Using SuSE Linux’s YaST tool, you can simply type <i>yast2</i> at a command or shell prompt and navigate to the Security and Users section. You can view groups and system groups along with user ID’s on the system

	<div> <div> YaST @ vulture (ui-ncurses-2.6.24) </div> <div> <div> in the system at the same time. To avoid confusion, each user must have a unique identity if they want to use Linux. Furthermore, every user at least belongs to one group. In this dialog, you can get information about existing groups. To shift to the user dialog, push the radio button Users administration </div> <div> <div> User and group administration () Users administration(x) Groups administration </div> <table border="1"> <thead> <tr> <th>Group name</th><th>Group ID</th><th>Group members</th></tr> </thead> <tbody> <tr><td>root</td><td>0</td><td>root</td></tr> <tr><td>bin</td><td>1</td><td>bin,daemon</td></tr> <tr><td>daemon</td><td>2</td><td>daemon,mysql</td></tr> <tr><td>sys</td><td>3</td><td></td></tr> <tr><td>tty</td><td>5</td><td></td></tr> <tr><td>disk</td><td>6</td><td></td></tr> <tr><td>lp</td><td>7</td><td>lp</td></tr> <tr><td>www</td><td>8</td><td></td></tr> <tr><td>knmem</td><td>9</td><td></td></tr> <tr><td>wheel</td><td>10</td><td></td></tr> <tr><td>mail</td><td>12</td><td>mail</td></tr> <tr><td>news</td><td>13</td><td>news</td></tr> <tr><td>uucp</td><td>14</td><td>uucp</td></tr> </tbody> </table> <div> [x] Also view system groups [Add][Edit] [Delete] [Back] [Abort] [Finish] </div> </div> </div> </div>	Group name	Group ID	Group members	root	0	root	bin	1	bin,daemon	daemon	2	daemon,mysql	sys	3		tty	5		disk	6		lp	7	lp	www	8		knmem	9		wheel	10		mail	12	mail	news	13	news	uucp	14	uucp
Group name	Group ID	Group members																																									
root	0	root																																									
bin	1	bin,daemon																																									
daemon	2	daemon,mysql																																									
sys	3																																										
tty	5																																										
disk	6																																										
lp	7	lp																																									
www	8																																										
knmem	9																																										
wheel	10																																										
mail	12	mail																																									
news	13	news																																									
uucp	14	uucp																																									
Compliance Criteria	All accounts on this system should be valid and in use. Verify that user accounts belong to active users and are still in use.																																										
Test Nature – Objective or Subjective	Objective																																										
Evidence																																											
Finding																																											

Checklist Item 16 – System Logging

Reference	http://www.securityfocus.com/printable/infocus/1419
Risk	Med – System logging is crucial to identifying system anomalies and assisting with system forensics.
Testing	<p>Examine the /etc/syslog.conf file by typing “cat /etc/syslog.conf” at a command or shell prompt on the server.</p> <p>A sample syslog output looks like</p> <pre>/etc/syslog.conf - Configuration file for syslogd(8) # # For info about the format of this file, see "man syslog.conf". # # # print most on tty10 and on the xconsole pipe</pre>

```

#
kern.warn;*.err;authpriv.none    /dev/tty10
kern.warn;*.err;authpriv.none    /dev/xconsole
*.emerg                           *

# enable this, if you want that root is informed
# immediately, e.g. of logins
#*.alert                          root

#
# all email-messages in one file
#
mail.*                            -/var/log/mail

#
# all news-messages
#
# these files are rotated and examined by "news.daily"
news.crit                        -/var/log/news/news.crit
news.err                        -/var/log/news/news.err
news.notice                     -/var/log/news/news.notice
# enable this, if you want to keep all news messages
# in one file
#news.*                          -/var/log/news.all

#
# Warnings in one file
#
*.=warn;*.=err                  -/var/log/warn
*.crit                          /var/log/warn

#
# save the rest in one file
#
*.*;mail.none;news.none        -/var/log/messages

#
# enable this, if you want to keep all messages
# in one file
#*.*                             -/var/log/allmessages

#
# Some foreign boot scripts require local7
#
local0,local1.*                 -/var/log/localmessages
local2,local3.*                 -/var/log/localmessages

```

	local4,local5.* -/var/log/localmessages local6,local7.* -/var/log/localmessages
Compliance Criteria	<p>This system also serves as the centralized syslog server so there would be no need to redirect messages to another server.</p> <p>Ensure that logging has not been commented out. An example is shown below. Note the “#” symbol showing it is commented out.</p> <pre># kern.warn;*.err;authpriv.none /dev/tty10 # kern.warn;*.err;authpriv.none /dev/xconsole *.emerg *</pre>
Test Nature – Objective or Subjective	Objective
Evidence	
Finding	

Checklist Item 18 – User staffing/training

Reference	Personal Experience
Risk	High – Inexperienced or untrained admin can configure a box improperly or insecure allowing an unauthorized user to gain access. Data Integrity, Confidentiality and Availability can be affected.
Testing	Interviewing the current Database administrator to check on past database experience, training attended, certifications, etc
Compliance Criteria	Proof of past projects, current training, certifications should be presented.
Test Nature – Objective or Subjective	Subjective
Evidence	
Finding	

Checklist Item 19 – System hardening – File Permissions

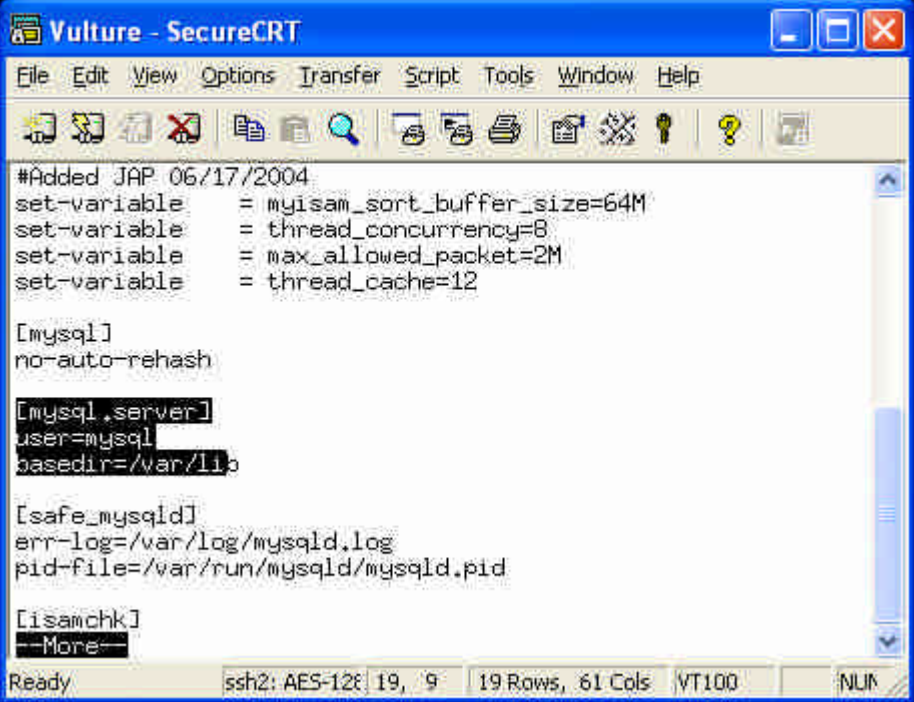
Reference	http://www.justlinux.com/nhf/Security/Securely_Installing_Linux.html http://www.securityfocus.com/printable/infocus/1419 http://ccfaq.valar.co.uk/modules.php?name=News&file=article&sid=105
------------------	---

	<p>The Rookery: Security Tools in Linux Distributions, Part II Posted on Monday, October 07, 2002 by Bobby S. Wen</p> <p>URL: http://www.linuxjournal.com/article.php?sid=6362</p>																					
Risk	Med – Having lax file permissions on system files can allow an authorized or unprivileged user to view information in another directory they shouldn't have access to.																					
Testing	<p>Typing “ls-la” at a command or shell prompt on the server</p> <p>Or</p> <p>Other areas to look at are the permissions.easy , permissions.local, permissions.paranoid and the permissions.secure files on the system.</p>																					
Compliance Criteria	<p>Ensure that permissions are set so that access is only given to the users that need access.</p> <p>The graph below (courtesy of http://ccfaq.valar.co.uk/modules.php?name=News&file=article&sid=105) outlines several examples you may be see while conducting this test.</p> <p>For example:</p> <table><tr><th>Permissions</th><th>Description</th><th>Commands Required</th></tr><tr><td>-rw-r--r--</td><td>For a file that only you will be editing. It allows everyone to read it, but only you may edit it.</td><td>chmod 644 filename</td></tr><tr><td>-rw-rw-r--</td><td>For a file that you and the members of the group will edit. It allows everyone to read it, but only you and the group may edit it.</td><td>chmod 664 filename</td></tr><tr><td>-rw-rw-rw-</td><td>This one is bad. It allows absolutely anyone to edit your file. Avoid this one at all costs! unless needed of course</td><td>chmod 666 filename</td></tr><tr><td>drwxr-xr-x</td><td>For a directory in which only you can create and delete files. It allows everyone to find files inside of it, but only you can add files, rename them, or remove them. (In many cases, the owner of a file can remove it regardless of the directory's permissions, but this is a special case.)</td><td>chmod 755 directoryname</td></tr><tr><td>drwxrwxr-x</td><td>For a directory in which you and the group can create and delete files. It allows everyone to find files inside of it, but only you and the group can add, rename, or remove files. (The same special case applies as for the previous example.)</td><td>chmod 775 directoryname</td></tr><tr><td>drwxrwxrwx</td><td>This one is bad. It allows absolutely anyone to mess with your files. Avoid this one like the plague!</td><td>chmod 777 directory / filename</td></tr></table>	Permissions	Description	Commands Required	-rw-r--r--	For a file that only you will be editing. It allows everyone to read it, but only you may edit it.	chmod 644 filename	-rw-rw-r--	For a file that you and the members of the group will edit. It allows everyone to read it, but only you and the group may edit it.	chmod 664 filename	-rw-rw-rw-	This one is bad . It allows absolutely anyone to edit your file. Avoid this one at all costs! unless needed of course	chmod 666 filename	drwxr-xr-x	For a directory in which only you can create and delete files. It allows everyone to find files inside of it, but only you can add files, rename them, or remove them. (In many cases, the owner of a file can remove it regardless of the directory's permissions, but this is a special case.)	chmod 755 directoryname	drwxrwxr-x	For a directory in which you and the group can create and delete files. It allows everyone to find files inside of it, but only you and the group can add, rename, or remove files. (The same special case applies as for the previous example.)	chmod 775 directoryname	drwxrwxrwx	This one is bad . It allows absolutely anyone to mess with your files. Avoid this one like the plague!	chmod 777 directory / filename
Permissions	Description	Commands Required																				
-rw-r--r--	For a file that only you will be editing. It allows everyone to read it, but only you may edit it.	chmod 644 filename																				
-rw-rw-r--	For a file that you and the members of the group will edit. It allows everyone to read it, but only you and the group may edit it.	chmod 664 filename																				
-rw-rw-rw-	This one is bad . It allows absolutely anyone to edit your file. Avoid this one at all costs! unless needed of course	chmod 666 filename																				
drwxr-xr-x	For a directory in which only you can create and delete files. It allows everyone to find files inside of it, but only you can add files, rename them, or remove them. (In many cases, the owner of a file can remove it regardless of the directory's permissions, but this is a special case.)	chmod 755 directoryname																				
drwxrwxr-x	For a directory in which you and the group can create and delete files. It allows everyone to find files inside of it, but only you and the group can add, rename, or remove files. (The same special case applies as for the previous example.)	chmod 775 directoryname																				
drwxrwxrwx	This one is bad . It allows absolutely anyone to mess with your files. Avoid this one like the plague!	chmod 777 directory / filename																				
Test Nature – Objective or Subjective	Objective																					
Evidence																						
Finding																						

Conducting the Audit – Testing and Findings

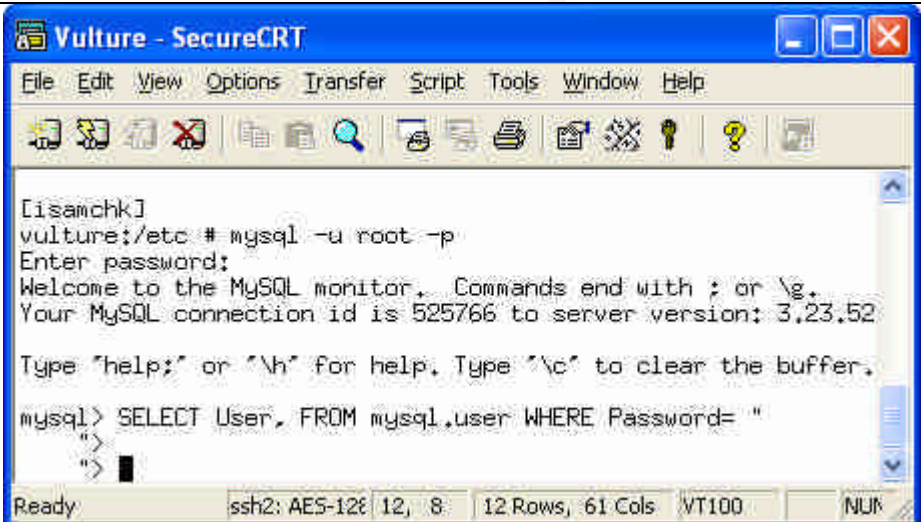
Checklist Item 1 – Nonprivileged account for MySQL instance

Reference	Auditing a MySQL database Server By Jeff Hoover URL: http://www.giac.org/practical/GSNA/Jeff_Hoover_GSNA.pdf Ten MySQL Best Practices by George Reese , coauthor of Managing & Using MySQL, 2nd Edition 07/11/2002 URL: http://www.onlamp.com/pub/a/onlamp/2002/07/11/MySQLtips.html
Risk	Low- Running applications or daemons in a “root” privilege mode can allow potential escalation for an unauthorized attacker if they were to gain access to the box. Data Integrity, availability and confidentiality are at risk
Testing	Assuming you are at a command or shell prompt on the server, check the my.cnf file running under the /etc directory on the system. A simple “ <i>cat /etc/my.cnf</i> ” should display the results needed to make this determination. The results should be displayed: [mysqld] User=name
Compliance Criteria	The MySQL server should be running as mysql or another unprivileged user
Test Nature – Objective or Subjective	Objective

Evidence	
Finding	An account called "mysql" exists and is not privileged

Checklist Item 3 - Set a password for the "root" User

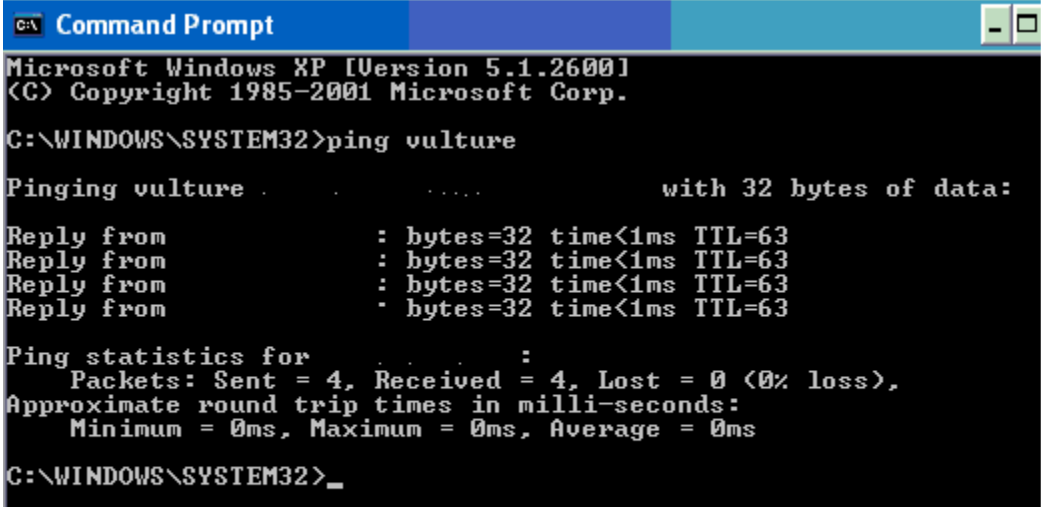
Reference	<p>Ten MySQL Best Practices</p> <p>by George Reese, coauthor of Managing & Using MySQL, 2nd Edition 07/11/2002 URL: http://www.onlamp.com/pub/a/onlamp/2002/07/11/MySQLtips.html</p> <p>Securing MySQL: step-by-step: http://www.securityfocus.com/infocus/1726, Artur Maj, August 28, 2003</p> <p>Auditing a MySQL database Server By Jeff Hoover URL: http://www.giac.org/practical/GSNA/Jeff_Hoover_GSNA.pdf</p>
Risk	High- running an application without a password can easily allow an unauthorized user to gain additional access to information.
Testing	<p>This can be accomplished a couple of ways.</p> <ol style="list-style-type: none"> 1. Running this from the shell or command prompt of the server: <pre>mysql -h host -u user -p</pre>

	<p>2. Running the query below against the mysql.user table (case sensitive)</p> <p>SELECT User, Host FROM mysql.user WHERE Password = ";</p>
Compliance Criteria	Zero rows should be returned from this query
Test Nature-Objective or Subjective Evidence	<p>Objective</p> 
Finding	Both the mysql and root users have passwords

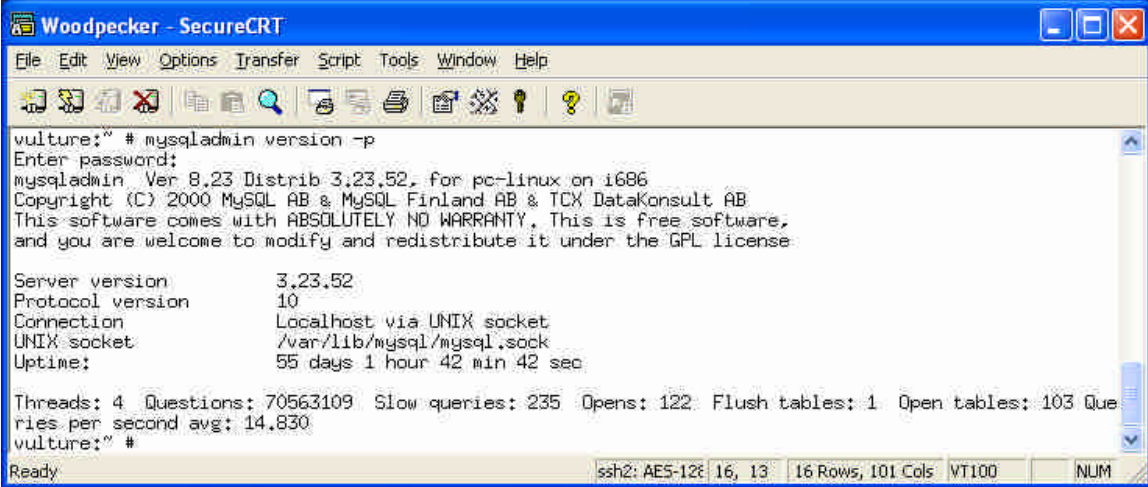
Checklist Item 4 – Hide MySQL from rest of world

Reference	<p>Ten MySQL Best Practices</p> <p>by George Reese, coauthor of Managing & Using MySQL, 2nd Edition 07/11/2002 URL: http://www.onlamp.com/pub/a/onlamp/2002/07/11/MySQLtips.html</p>
Risk	High– Having this system exposed allows potential unauthorized access resulting in Availability and Integrity issues
Testing	<p>2 tests should be run from 2 locations.</p> <ol style="list-style-type: none"> 1 run Nmap from an IP or a host that is allowed (or should be allowed) to talk to the database server. This Nmap instance is to verify that only specific services are running.

	<p>Running a simple NMap against this host to look for MySQL will take care of this. (flags are case sensitive)</p> <p>From a shell or command prompt type:</p> <p><i>Nmap -sS -O -v -p 1-65535 (IP of system)</i></p> <p>2. From a shell prompt or a command prompt from a random location and a different IP address than the one used above run the following command: <i>Ping (IP of system)</i></p>
Compliance Criteria	<p>A default installation of MySQL runs on port 3306. The Nmap result should only list 3306 and SSH port 22 for secure remote administration.</p> <p>The second test should time out if you are on a host that is not supposed to talk directly to this system. Messages received may be "request timed out", Destination Host Unreachable", etc</p>
Test Nature – Objective or Subjective	Objective
Evidence	<pre> crawford@192.168.1.100:~\$ nmap -sS -O -v -p 1-65535 vulture Starting nmap V. 3.00 (www.insecure.org/nmap/) Host vulture.192.168.1.100 appears to be up ... good. Initiating SYN Stealth Scan against vulture.192.168.1.100 Adding open port 22/tcp Adding open port 3306/tcp The SYN Stealth Scan took 1 second to scan 65535 ports. For OSscan assuming that port 22 is open and port 1 is closed and neither are firewalled For OSscan assuming that port 22 is open and port 1 is closed and neither are firewalled For OSscan assuming that port 22 is open and port 1 is closed and neither are firewalled Interesting ports on vulture.192.168.1.100: (The 65533 ports scanned but not shown below are in state: closed) Port State Service 22/tcp open ssh 3306/tcp open mysql No exact OS matches for host (If you know what OS is running on it, see http://www.insecure.org/cgi-bin/nmap TCP/IP fingerprint: SInfo(V=3.00P=i586-suse-linux%D=12/7%Time=41B5FF9D%O=22%C=1) TSeq(Class=RI%gcd=1%SI=308C24%IPID=I%TS=100HZ) TSeq(Class=RI%gcd=1%SI=309160%IPID=I%TS=100HZ) TSeq(Class=RI%gcd=1%SI=308EB4%IPID=I%TS=100HZ) T1(Resp=Y%DF=Y%W=16A0%ACK=S++%Flags=AS%Dps=MNNTNW) T2(Resp=N) T3(Resp=N) T4(Resp=Y%DF=Y%W=0%ACK=0%Flags=R%Dps=) T5(Resp=Y%DF=Y%W=0%ACK=S++%Flags=AR%Dps=) T6(Resp=Y%DF=Y%W=0%ACK=0%Flags=R%Dps=) T7(Resp=Y%DF=Y%W=0%ACK=S++%Flags=AR%Dps=) PU(Resp=Y%DF=N%TOS=C0%IPLEN=164%RIPTL=148%RID=E%RIPCK=E%UCK=E%ULEN=134%DAT=E) Uptime 151,007 days (since Fri Jul 9 13:58:18 2004) TCP Sequence Prediction: Class=random positive increments Difficulty=3182260 (Good luck!) IPID Sequence Generation: Incremental Nmap run completed -- 1 IP address (1 host up) scanned in 18 seconds </pre> <p>Ping Host 1 – Should be able to talk to host</p>

	 <p>The screenshot shows a Windows XP Command Prompt window. The title bar reads 'C:\ Command Prompt'. The window content shows the following text:</p> <pre> Microsoft Windows XP [Version 5.1.2600] (C) Copyright 1985-2001 Microsoft Corp. C:\WINDOWS\SYSTEM32>ping vulture Pinging vulture with 32 bytes of data: Reply from : bytes=32 time<1ms TTL=63 Reply from : bytes=32 time<1ms TTL=63 Reply from : bytes=32 time<1ms TTL=63 Reply from : bytes=32 time<1ms TTL=63 Ping statistics for : Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms C:\WINDOWS\SYSTEM32>_ </pre>
<p>Finding</p>	<p>This system is accessible from the world. Nmap and Pings were successfully accomplished from different IP addresses and different Internet Service Providers.</p>

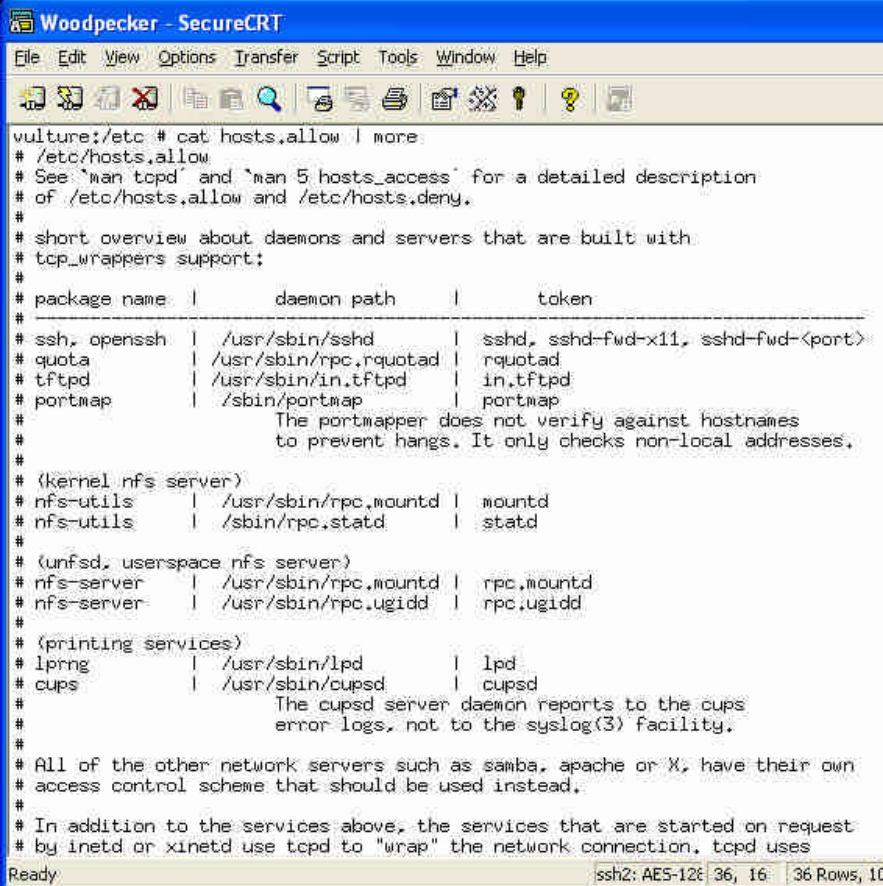
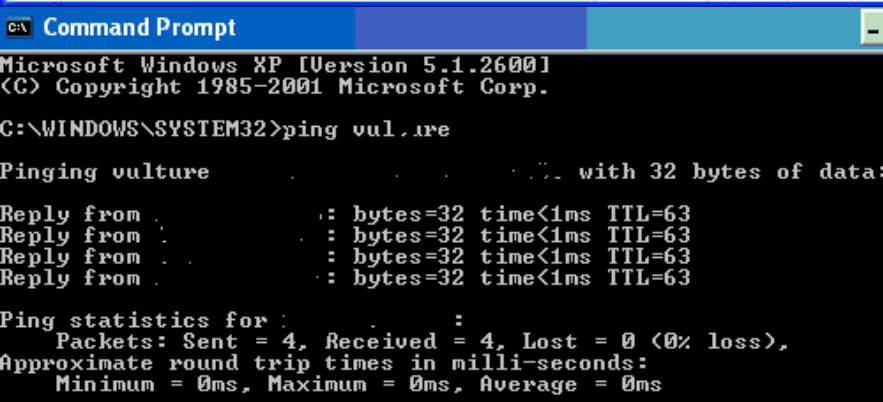
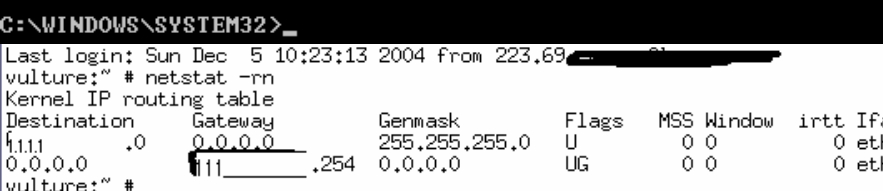
Checklist Item 5 – UnPatched MySQL Application

Reference	Personell Best Practice
Risk	High – Unpatched sytems can allow unauthorized users to exploit a vulnerability. Integrity and Availability are at risk
Testing	You can check which version of MySQL you are running by going to the bin directory and executing Mysqladmin version
Compliance Criteria	The MySQL version should be up to date and patched. You can verify any vulnerabilities or what the newest version is by looking at www.securityfocus.com/bid or http://dev.mysql.com/downloads/ for new updates or security patches
Test Nature – Objective or Subjective	Objective
Evidence	 The screenshot shows a terminal window titled 'Woodpecker - SecureCRT'. The command 'mysqladmin version -p' has been executed. The output text is as follows: vulture:~ # mysqladmin version -p Enter password: mysqladmin Ver 8.23 Distrib 3.23.52, for pc-linux on i686 Copyright (C) 2000 MySQL AB & MySQL Finland AB & TCX DataKonsult AB This software comes with ABSOLUTELY NO WARRANTY. This is free software, and you are welcome to modify and redistribute it under the GPL license Server version: 3.23.52 Protocol version: 10 Connection: Localhost via UNIX socket UNIX socket: /var/lib/mysql/mysql.sock Uptime: 55 days 1 hour 42 min 42 sec Threads: 4 Questions: 70563109 Slow queries: 235 Opens: 122 Flush tables: 1 Open tables: 103 Que- ries per second avg: 14.830 vulture:~ # The status bar at the bottom of the window indicates 'Ready', 'ssh2: AES-128', '16, 13', '16 Rows, 101 Cols', 'VT100', and 'NUM'.
Finding	The version of MySQL is out of date. The current version of MySQL is 5.0.1. A major vulnerability exists with this current version. http://www.linuxdevcenter.com/pub/a/linux/2002/12/16/insecurities.html

Checklist Item 11 – Host communication restrictions

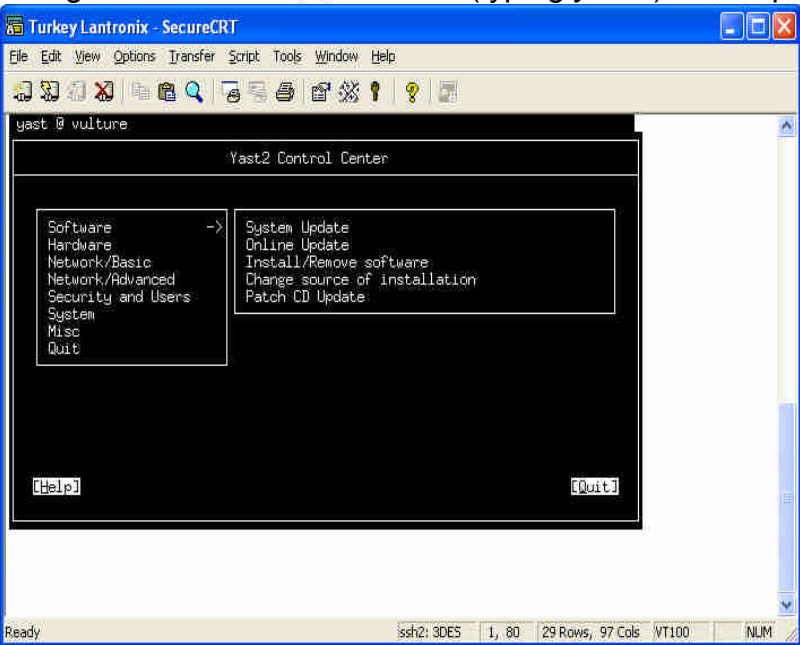
Reference	http://www.securityfocus.com/printable/infocus/1419
Risk	High – Without restrictions in place for allowing or denying which hosts can talk to this system, potential unauthorized access can be made. An attacker can run exploits from any source. System Availability and Integrity are at risk
Testing	Several areas can be examined. Assuming you are at a command or shell prompt on the server,

	<ol style="list-style-type: none"> 1. Typing “<i>cat /etc/hosts.allow</i>” or “<i>cat /etc/hosts.deny</i>” 2. Typing “<i>netstat -rn</i>” in case any host routes are implemented instead of a default route are great examples. 3. Ping from random hosts. Go to a prompt on a workstation and type “<i>Ping xxx.xxx.xxx</i> (IP of Database Server)”
Compliance Criteria	<ol style="list-style-type: none"> 1. Look for statements similar to “Example 2: grant access from local net, reject with message from elsewhere. # in.telnetd : ALL EXCEPT LOCAL : ALLOW # in.telnetd : ALL : \ # twist /bin/echo -e "\n\raccess from %h declined.\n\rGo away.";sleep 2 # # # Example 3: run a different instance of rsyncd if the connection comes # from network 172.20.0.0/24, but regular for others: # rsyncd : 172.20.0.0/255.255.255.0 : twist /usr/local/sbin/my_rsyncd-script” 2. The “<i>netstat -rn</i>” command should return the routing table on the system. Look to see if a default route is in place. This can be found by looking for a “0.0.0.0” in the destination field followed by an address in the gateway field. If a default gateway is listed, static routes are probably not in place and this system is probably accessible anywhere on the network. Also look for specific routes. These are displayed by having a full IP in the destination, followed by the gateway address and finally the subnet address. If specific routes are listed, it is likely that an attempt has been made to only allow specific hosts to talk to this system. 3. Pinging from random hosts will give you a variety of replies. A “reply from” means successful communication to this host, ie this host is allowed to talk to this server. Other replies may be “request timed out” or “destination host unreachable”. Either the host is not allowed to talk to this server or the location where you are pinging from does not know how to get to the destination. <p>If you can successfully ping a host, make sure that the IP range you are pinging from is supposed to be talking to this system</p>
Test Nature	Objective

<p>– Objective or Subjective Evidence</p>	
	<div data-bbox="516 306 1396 1186">  <pre> vulture:/etc # cat hosts.allow more # /etc/hosts.allow # See 'man tcpd' and 'man 5 hosts_access' for a detailed description # of /etc/hosts.allow and /etc/hosts.deny. # # short overview about daemons and servers that are built with # tcp_wrappers support: # # package name daemon path token # # ssh, openssh /usr/sbin/sshd sshd, sshd-fwd-x11, sshd-fwd-<port> # quota /usr/sbin/rpc.rquotad rquotad # tftpd /usr/sbin/in.tftpd in.tftpd # portmap /sbin/portmap portmap # # The portmapper does not verify against hostnames # to prevent hangs. It only checks non-local addresses. # # (kernel nfs server) # nfs-utils /usr/sbin/rpc.mountd mountd # nfs-utils /sbin/rpc.statd statd # # (unfsd, userspace nfs server) # nfs-server /usr/sbin/rpc.mountd rpc.mountd # nfs-server /usr/sbin/rpc.ugidd rpc.ugidd # # (printing services) # lprng /usr/sbin/lpd lpd # cups /usr/sbin/cupsd cupsd # # The cupsd server daemon reports to the cups # error logs, not to the syslog(3) facility. # # All of the other network servers such as samba, apache or X, have their own # access control scheme that should be used instead. # # In addition to the services above, the services that are started on request # by inetd or xinetd use tcpd to "wrap" the network connection. tcpd uses </pre> </div> <div data-bbox="467 1165 495 1197">1.</div> <div data-bbox="516 1186 1396 1585">  <pre> C:\WINDOWS\SYSTEM32>ping vul.lre Pinging vulture [223.69.255.254] with 32 bytes of data: Reply from 223.69.255.254: bytes=32 time<1ms TTL=63 Reply from 223.69.255.254: bytes=32 time<1ms TTL=63 Reply from 223.69.255.254: bytes=32 time<1ms TTL=63 Reply from 223.69.255.254: bytes=32 time<1ms TTL=63 Ping statistics for 223.69.255.254: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms </pre> </div> <div data-bbox="467 1596 495 1627">2.</div> <div data-bbox="516 1585 1396 1774">  <pre> C:\WINDOWS\SYSTEM32>netstat -rn Last login: Sun Dec 5 10:23:13 2004 from 223.69.255.254 vulture:~ # netstat -rn Kernel IP routing table Destination Gateway Genmask Flags MSS Window irtt Iface 0.0.0.0 0.0.0.0 255.255.255.0 UG 0 0 0 eth0 </pre> </div>
<p>Finding</p>	<p>No communication restrictions exist. This system is accessible</p>

	via SSH from any host

Checklist Item 12 – System hardening – Services

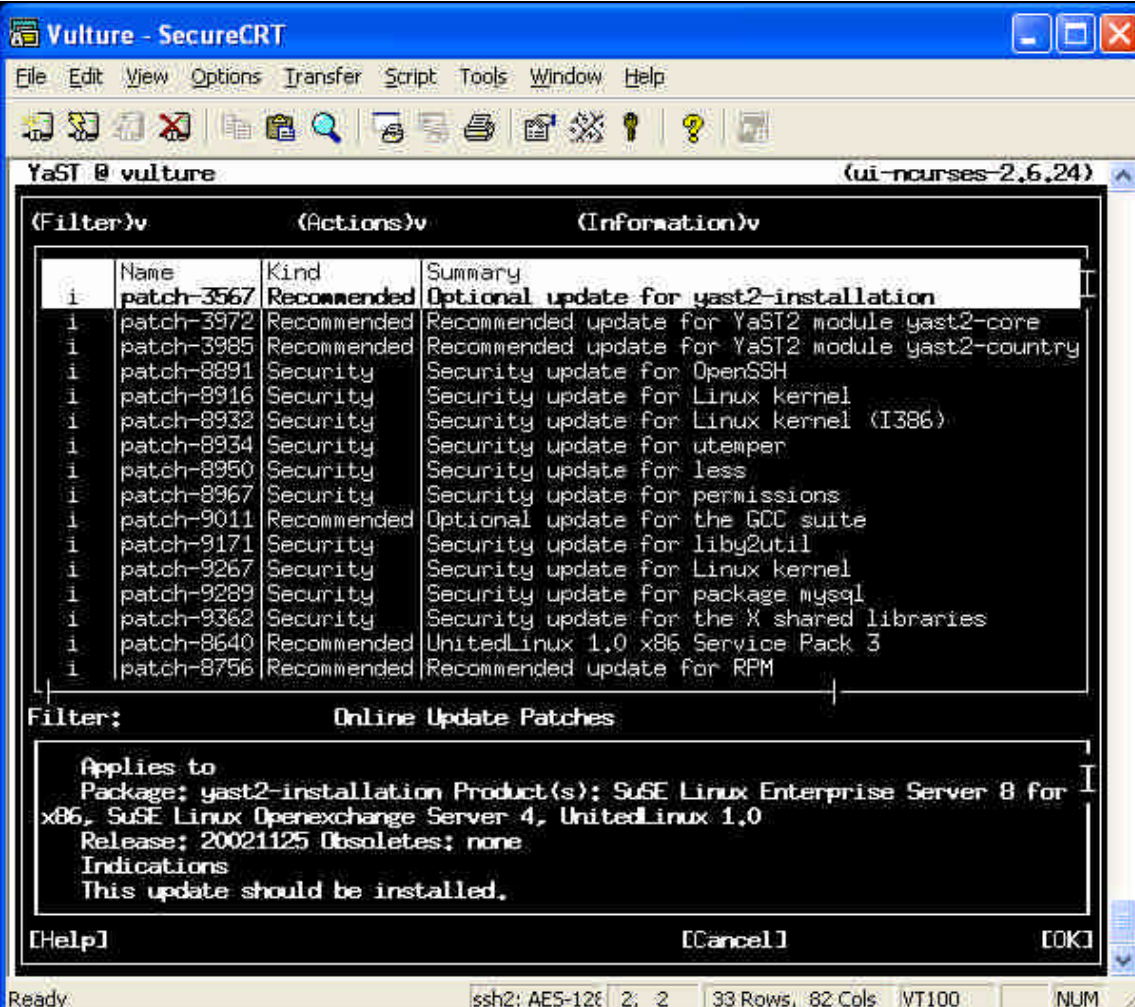
Reference	<p>http://www.justlinux.com/nhf/Security/Securely_Installing_Linux.html http://www.securityfocus.com/printable/infocus/1419 The Rookery: Security Tools in Linux Distributions, Part II Posted on Monday, October 07, 2002 by Bobby S. Wen</p> <p>URL: http://www.linuxjournal.com/article.php?sid=6362</p> <ul style="list-style-type: none"> http://shelob.temple.edu/suse/local/SuSE-Linux-Adminguide-8.2.0.1x86.pdf
Risk	High – Having unnecessary services running allow that many more potential areas to be exploited.
Testing	<p>Several areas can be examined.</p> <p>1. Using the SuSE Linux YaST tool (typing <i>yast2</i>) from a prompt:</p>  <ol style="list-style-type: none"> You can navigate to the install remove software section to look for unneeded software running One could also examine the <code>/etc/init.d</code> directory. Simply typing <code>'ls -la more '</code> in the <code>init.d</code> directory . This will show all services that will be set to run. Typing <code>"netstat -an"</code> at a prompt will also list what ports your machine is listening for connections on.

Compliance Criteria	Results of these tests should imply that only SSH (port 22) and MySQL port 3306 is running on this system. Other services such as FTP (port 21), SMTP (port 25), etc should not be running on this server.
Test Nature – Objective or Subjective	Objective
Evidence	<pre> vulture:/etc/init.d # ls -la more total 263 drwxr-xr-x 11 root root 1664 Sep 17 09:50 . drwxr-xr-x 36 root root 3992 Dec 7 12:32 .. -rw-r--r-- 1 root root 6960 Apr 15 2003 README -rwxr----- 1 root root 1640 Apr 2 2003 SuSEfirewall2_final -rwxr----- 1 root root 1625 Apr 2 2003 SuSEfirewall2_init -rwxr----- 1 root root 1868 Apr 2 2003 SuSEfirewall2_setup -rwxr-xr-x 1 root root 3653 Oct 16 2002 atd -rwxr-xr-x 1 root root 3517 Aug 30 2002 boot -rwxr-xr-x 1 root root 2274 Aug 8 2002 boot.clock -rwxr-xr-x 1 root root 4149 Aug 5 2002 boot.crypto drwxr-xr-x 2 root root 512 May 19 2004 boot.d -rwxr-xr-x 1 root root 2854 Mar 15 2002 boot.idedma -rwxr-xr-x 1 root root 2980 Oct 30 2003 boot.ipconfig -rwxr--r-- 1 root root 764 Oct 16 2002 boot.isapnp -rwxr-xr-x 1 root root 1549 Nov 4 2002 boot.klog -rwxr-xr-x 1 root root 1786 Jul 8 2002 boot.ldconfig -rwxr--r-- 1 root root 414 May 20 2004 boot.local -rwxr-xr-x 1 root root 5329 Oct 30 2003 boot.localfs -rwxr-xr-x 1 root root 2582 Aug 21 2002 boot.localnet -rwxr--r-- 1 root root 3156 May 4 2004 boot.lvm -rwxr--r-- 1 root root 1442 Jun 2 2004 boot.md -rwxr-xr-x 1 root root 1416 Apr 15 2003 boot.proc -rwxr-xr-x 1 root root 942 Oct 16 2002 boot.restore_permissions -rwxr-xr-x 1 root root 1479 Jul 4 2003 boot.swap -rwxr-xr-x 1 root root 1053 Oct 16 2002 boot.sysctl -rwxr--r-- 1 root root 3914 Oct 16 2002 cron -rwxr--r-- 1 root root 5095 Oct 16 2002 fbset -rwxr-xr-x 1 root root 3459 Oct 16 2002 gpm -rwxr-xr-x 1 root root 5784 Sep 4 2003 halt -rwxr--r-- 1 root root 379 May 20 2004 halt.local -rwxr--r-- 1 root root 1369 Oct 16 2002 hotplug Timer </pre>

	<pre> tcp 0 0 0.0.0.0:3306 0.0.0.0:* LISTEN off (0.00/0/0) tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN off (0.00/0/0) tcp 0 0 127.0.0.1:25 0.0.0.0:* LISTEN </pre>
Finding	This system appears to have minimal services running. MySQL, SSH and SMTP are the only services running. All of these services are required for the application to run.

Checklist Item 13 – System Patched / Updated

Reference	http://www.justlinux.com/nhf/Security/Securely_Installing_Linux.html http://www.securityfocus.com/printable/infocus/1419 http://www.suse.com/us/private/products/suse_linux/prof/security.html http://www.suse.com/us/private/products/suse_linux/prof/yast.html http://shelob.temple.edu/suse/local/SuSE-Linux-Adminguide-8.2.0.1x86.pdf
Risk	High – Unpatched systems can allow unauthorized users to exploit a vulnerability. Integrity and Availability
Testing	<p>With SuSE Linux you can run the YaST Tool to check for system updates.</p> <p>Simply typing “<i>yast2 online_update .auto.get security</i>” at a command or shell prompt on the server</p>
Compliance Criteria	No patches should be found or need to be installed if this system is fully patched. If a list of patches to be installed is returned, this system is not patched.
Test Nature – Objective or Subjective	Objective

Evidence	 <p>The screenshot shows the YaST2 Online Update Patches window. The window title is "YaST @ vulture" and the version is "(ui-ncurses-2.6.24)". The window contains a table of patches with columns: Name, Kind, and Summary. The patches are listed as follows:</p> <table><tr><th>Name</th><th>Kind</th><th>Summary</th></tr><tr><td>patch-3567</td><td>Recommended</td><td>Optional update for yast2-installation</td></tr><tr><td>patch-3972</td><td>Recommended</td><td>Recommended update for YaST2 module yast2-core</td></tr><tr><td>patch-3985</td><td>Recommended</td><td>Recommended update for YaST2 module yast2-country</td></tr><tr><td>patch-8891</td><td>Security</td><td>Security update for OpenSSH</td></tr><tr><td>patch-8916</td><td>Security</td><td>Security update for Linux kernel</td></tr><tr><td>patch-8932</td><td>Security</td><td>Security update for Linux kernel (I386)</td></tr><tr><td>patch-8934</td><td>Security</td><td>Security update for utemper</td></tr><tr><td>patch-8950</td><td>Security</td><td>Security update for less</td></tr><tr><td>patch-8967</td><td>Security</td><td>Security update for permissions</td></tr><tr><td>patch-9011</td><td>Recommended</td><td>Optional update for the GCC suite</td></tr><tr><td>patch-9171</td><td>Security</td><td>Security update for liby2util</td></tr><tr><td>patch-9267</td><td>Security</td><td>Security update for Linux kernel</td></tr><tr><td>patch-9289</td><td>Security</td><td>Security update for package mysql</td></tr><tr><td>patch-9362</td><td>Security</td><td>Security update for the X shared libraries</td></tr><tr><td>patch-8640</td><td>Recommended</td><td>UnitedLinux 1.0 x86 Service Pack 3</td></tr><tr><td>patch-8756</td><td>Recommended</td><td>Recommended update for RPM</td></tr></table> <p>Below the table, there is a section titled "Filter:" and "Online Update Patches". It contains the following information:</p> <pre>Applies to Package: yast2-installation Product(s): SuSE Linux Enterprise Server 8 for x86, SuSE Linux Openexchange Server 4, UnitedLinux 1.0 Release: 20021125 Obsoletes: none Indications This update should be installed.</pre> <p>At the bottom of the window, there are buttons for [Help], [Cancel], and [OK]. The status bar at the bottom shows "Ready", "ssh2: AES-128 2, 2", "33 Rows, 82 Cols", "VT100", and "NUM".</p>	Name	Kind	Summary	patch-3567	Recommended	Optional update for yast2-installation	patch-3972	Recommended	Recommended update for YaST2 module yast2-core	patch-3985	Recommended	Recommended update for YaST2 module yast2-country	patch-8891	Security	Security update for OpenSSH	patch-8916	Security	Security update for Linux kernel	patch-8932	Security	Security update for Linux kernel (I386)	patch-8934	Security	Security update for utemper	patch-8950	Security	Security update for less	patch-8967	Security	Security update for permissions	patch-9011	Recommended	Optional update for the GCC suite	patch-9171	Security	Security update for liby2util	patch-9267	Security	Security update for Linux kernel	patch-9289	Security	Security update for package mysql	patch-9362	Security	Security update for the X shared libraries	patch-8640	Recommended	UnitedLinux 1.0 x86 Service Pack 3	patch-8756	Recommended	Recommended update for RPM
Name	Kind	Summary																																																		
patch-3567	Recommended	Optional update for yast2-installation																																																		
patch-3972	Recommended	Recommended update for YaST2 module yast2-core																																																		
patch-3985	Recommended	Recommended update for YaST2 module yast2-country																																																		
patch-8891	Security	Security update for OpenSSH																																																		
patch-8916	Security	Security update for Linux kernel																																																		
patch-8932	Security	Security update for Linux kernel (I386)																																																		
patch-8934	Security	Security update for utemper																																																		
patch-8950	Security	Security update for less																																																		
patch-8967	Security	Security update for permissions																																																		
patch-9011	Recommended	Optional update for the GCC suite																																																		
patch-9171	Security	Security update for liby2util																																																		
patch-9267	Security	Security update for Linux kernel																																																		
patch-9289	Security	Security update for package mysql																																																		
patch-9362	Security	Security update for the X shared libraries																																																		
patch-8640	Recommended	UnitedLinux 1.0 x86 Service Pack 3																																																		
patch-8756	Recommended	Recommended update for RPM																																																		
Finding	This system is in need of patching. Several security patches are not installed.																																																			

Checklist Item 14 – Limited user Accounts

Reference	http://www.justlinux.com/nhf/Security/Securely_Installing_Linux.html
Risk	Med – Provides another vector that an unauthorized user can try to exploit. Another account to manage
Testing	Using SuSE Linux's YaST tool, you can simply type <i>yast2</i> at a command or shell prompt on the server and navigate to the Security and Users section. You can view groups and system groups along with user ID's on the system

	<div>YaST @ vulture</div> <div>(ui-ncurses-2,6,24)</div> <div>in the system at the same time. To avoid confusion, each user must have a unique identity if they want to use Linux. Furthermore, every user at least belongs to one group.</div> <div>In this dialog, you can get information about existing groups.</div> <div>To shift to the user dialog, push the radio button Users administration</div> <div>Users administration</div> <div>User and group administration</div> <div>() Users administration(x) Groups administration</div> <div><table><thead><tr><th>Group name</th><th>Group ID</th><th>Group members</th></tr></thead><tbody><tr><td>root</td><td>0</td><td>root</td></tr><tr><td>bin</td><td>1</td><td>bin,daemon</td></tr><tr><td>daemon</td><td>2</td><td>daemon,mysql</td></tr><tr><td>sys</td><td>3</td><td></td></tr><tr><td>tty</td><td>5</td><td></td></tr><tr><td>disk</td><td>6</td><td></td></tr><tr><td>lp</td><td>7</td><td>lp</td></tr><tr><td>www</td><td>8</td><td></td></tr><tr><td>kmem</td><td>9</td><td></td></tr><tr><td>wheel</td><td>10</td><td></td></tr><tr><td>mail</td><td>12</td><td>mail</td></tr><tr><td>news</td><td>13</td><td>news</td></tr><tr><td>uucp</td><td>14</td><td>uucp</td></tr></tbody></table></div> <div>[x] Also view system groups</div> <div>[Add][Edit]</div> <div>[Delete]</div> <div>[Back]</div> <div>[Abort]</div> <div>[Finish]</div>	Group name	Group ID	Group members	root	0	root	bin	1	bin,daemon	daemon	2	daemon,mysql	sys	3		tty	5		disk	6		lp	7	lp	www	8		kmem	9		wheel	10		mail	12	mail	news	13	news	uucp	14	uucp
Group name	Group ID	Group members																																									
root	0	root																																									
bin	1	bin,daemon																																									
daemon	2	daemon,mysql																																									
sys	3																																										
tty	5																																										
disk	6																																										
lp	7	lp																																									
www	8																																										
kmem	9																																										
wheel	10																																										
mail	12	mail																																									
news	13	news																																									
uucp	14	uucp																																									
Compliance Criteria	All accounts on this system should be valid and in use. Verify that user accounts belong to active users and are still in use.																																										
Test Nature – Objective or Subjective	Objective																																										
Evidence	<div>Vulture - SecureCRT</div> <div>File Edit View Options Transfer Script Tools Window Help</div> <div>YaST @ vulture</div> <div>(ui-ncurses-2,6,24)</div> <div>Linux is a multiuser system. Several different users can be logged in the system at the same time. To avoid confusion, each user must have a unique identity if they want to use Linux. Furthermore, every user at least belongs to one group.</div> <div>In this dialog, you can get information about existing users.</div> <div>To shift to the group dialog push the radio button Groups administration.</div> <div>To create a new user, push the button Add.</div> <div>To edit or delete an existing user, select one user from the list and click</div> <div>User and group administration</div> <div>(x) Users administration() Groups administration</div> <div><table><thead><tr><th>Login</th><th>Name</th><th>UID</th><th>Groups</th></tr></thead><tbody><tr><td>users</td><td>users</td><td>500</td><td>users,uucp,dialout,audio</td></tr><tr><td>uucp</td><td>uucp</td><td>501</td><td>users,uucp,dialout,audio</td></tr></tbody></table></div> <div>[x] Also view system users</div> <div>[Add][Edit]</div> <div>[Delete]</div> <div>[Back]</div> <div>[Abort]</div> <div>[Finish]</div>	Login	Name	UID	Groups	users	users	500	users,uucp,dialout,audio	uucp	uucp	501	users,uucp,dialout,audio																														
Login	Name	UID	Groups																																								
users	users	500	users,uucp,dialout,audio																																								
uucp	uucp	501	users,uucp,dialout,audio																																								

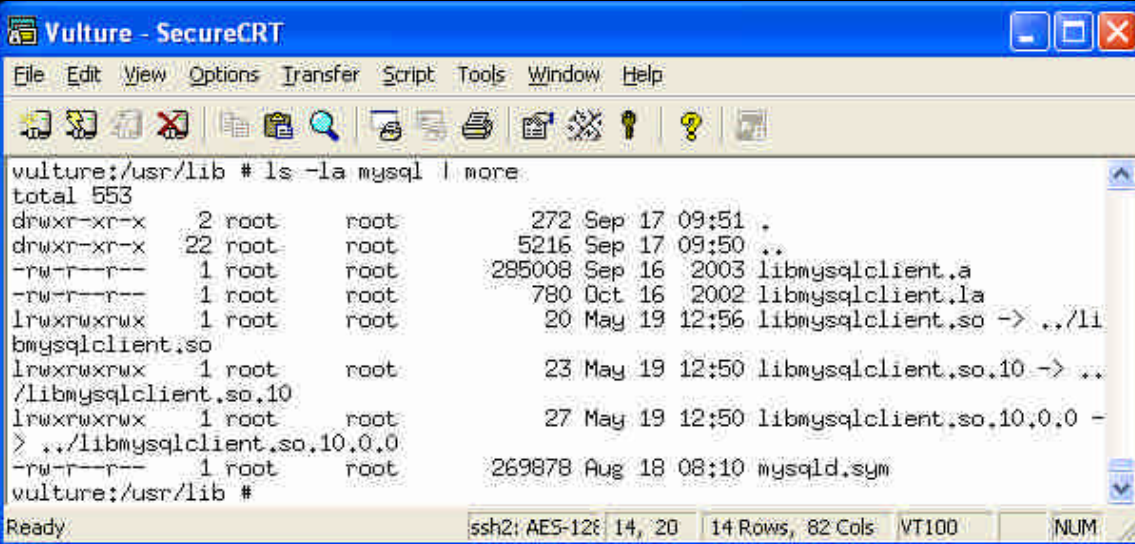
	<div><div><p>Linux is a multiuser system. Several different users can be logged in the system at the same time. To avoid confusion, each user must have a unique identity if they want to use Linux. Furthermore, every user at least belongs to one group. In this dialog, you can get information about existing users. To shift to the group dialog push the radio button Groups administration. To create a new user, push the button Add. To edit or delete an existing user, select one user from the list and click</p></div><div><p>User and group administration (x) Users administration () Groups administration</p><table><thead><tr><th>Login</th><th>Name</th><th>UID</th><th>Groups</th></tr></thead><tbody><tr><td>root</td><td>root</td><td>0</td><td>root</td></tr><tr><td>bin</td><td>bin</td><td>1</td><td>bin</td></tr><tr><td>daemon</td><td>Daemon</td><td>2</td><td>daemon,bin</td></tr><tr><td>lp</td><td>Printing daemon</td><td>4</td><td>lp</td></tr><tr><td>mail</td><td>Mailer daemon</td><td>8</td><td>mail</td></tr><tr><td>news</td><td>News system</td><td>9</td><td>news</td></tr><tr><td>uucp</td><td>Unix-to-Unix CoPy system</td><td>10</td><td>uucp</td></tr><tr><td>games</td><td>Games account</td><td>12</td><td>users</td></tr><tr><td>man</td><td>Manual pages viewer</td><td>13</td><td>man</td></tr><tr><td>at</td><td>Batch jobs daemon</td><td>25</td><td>at</td></tr><tr><td>wwwrun</td><td>WWW daemon apache</td><td>30</td><td>nogroup</td></tr><tr><td>ftp</td><td>FTP account</td><td>40</td><td>ftp</td></tr><tr><td>named</td><td>Nameserver daemon</td><td>44</td><td>named</td></tr><tr><td>postfix</td><td>Postfix Daemon</td><td>51</td><td>postfix</td></tr><tr><td>mysql</td><td>MySQL database admin</td><td>60</td><td>daemon</td></tr><tr><td>sshd</td><td>SSH daemon</td><td>71</td><td>sshd</td></tr><tr><td>ntp</td><td>NTP daemon</td><td>74</td><td>nogroup</td></tr><tr><td>User A and B</td><td></td><td>500</td><td>users,uucp,di</td></tr><tr><td>nobody</td><td>nobody</td><td>501</td><td>users,uucp,di</td></tr><tr><td></td><td></td><td>65534</td><td>nobody,nogrou</td></tr></tbody></table><div><div>[x] Also view system users</div><div>[Add][Edit] [Delete]</div><div>[Back] [Abort] [Finish]</div></div></div></div>	Login	Name	UID	Groups	root	root	0	root	bin	bin	1	bin	daemon	Daemon	2	daemon,bin	lp	Printing daemon	4	lp	mail	Mailer daemon	8	mail	news	News system	9	news	uucp	Unix-to-Unix CoPy system	10	uucp	games	Games account	12	users	man	Manual pages viewer	13	man	at	Batch jobs daemon	25	at	wwwrun	WWW daemon apache	30	nogroup	ftp	FTP account	40	ftp	named	Nameserver daemon	44	named	postfix	Postfix Daemon	51	postfix	mysql	MySQL database admin	60	daemon	sshd	SSH daemon	71	sshd	ntp	NTP daemon	74	nogroup	User A and B		500	users,uucp,di	nobody	nobody	501	users,uucp,di			65534	nobody,nogrou
Login	Name	UID	Groups																																																																																		
root	root	0	root																																																																																		
bin	bin	1	bin																																																																																		
daemon	Daemon	2	daemon,bin																																																																																		
lp	Printing daemon	4	lp																																																																																		
mail	Mailer daemon	8	mail																																																																																		
news	News system	9	news																																																																																		
uucp	Unix-to-Unix CoPy system	10	uucp																																																																																		
games	Games account	12	users																																																																																		
man	Manual pages viewer	13	man																																																																																		
at	Batch jobs daemon	25	at																																																																																		
wwwrun	WWW daemon apache	30	nogroup																																																																																		
ftp	FTP account	40	ftp																																																																																		
named	Nameserver daemon	44	named																																																																																		
postfix	Postfix Daemon	51	postfix																																																																																		
mysql	MySQL database admin	60	daemon																																																																																		
sshd	SSH daemon	71	sshd																																																																																		
ntp	NTP daemon	74	nogroup																																																																																		
User A and B		500	users,uucp,di																																																																																		
nobody	nobody	501	users,uucp,di																																																																																		
		65534	nobody,nogrou																																																																																		
Finding	Very few users exist on this system. Normal system accounts and groups exist, only 2 admin accounts and a root account exist.																																																																																				

Checklist Item 18 – User staffing/training

Reference	Personal Experience
Risk	High – Inexperienced or untrained admin can configure a box improperly or insecure allowing an unauthorized user to gain access. Data Integrity, Confidentiality and Availability can be affected.
Testing	<p>Interviewing the current Database administrator to check on past database experience, training attended, certifications, etc</p> <p>Interview with HR Manager, review administrators application and Resume</p>
Compliance Criteria	Proof of past projects, current training, certifications should be presented.
Test Nature – Objective or Subjective	Subjective
Evidence	Interviewed HR, reviewed Resume and Interviewed staff
Finding	Both staff members responsible for managing this system have well over 5 years of Linux and MySQL administration. They only have 1 year of SuSE Linux administration.

Checklist Item 19 – System hardening – File Permissions

Reference	<p>http://www.justlinux.com/nhf/Security/Securely_Installing_Linux.html http://www.securityfocus.com/printable/infocus/1419 http://ccfaq.valar.co.uk/modules.php?name=News&file=article&sid=105 The Rookery: Security Tools in Linux Distributions, Part II Posted on Monday, October 07, 2002 by Bobby S. Wen</p> <p>URL: http://www.linuxjournal.com/article.php?sid=6362</p> <ul style="list-style-type: none">http://shelob.temple.edu/suse/local/SuSE-Linux-Adminguide-8.2.0.1x86.pdf																		
Risk	Med – Having lax file permissions on system files can allow an authorized or unprivileged user to view information in another directory they shouldn't have access to.																		
Testing	<p>Typing “ls-la” at a command or shell prompt on the server</p> <p>Or</p> <p>Other areas to look at are the permissions.easy , permissions.local, permissions.paranoid and the permissions.secure files on the system.</p>																		
Compliance Criteria	<p>Ensure that permissions are set so that access is only given to the users that need access.</p> <p>The graph below (courtesy of http://ccfaq.valar.co.uk/modules.php?name=News&file=article&sid=105) outlines several examples you may be see while conducting this test.</p> <p>For example:</p> <table><thead><tr><th>Permissions</th><th>Description</th><th>Commands Required</th></tr></thead><tbody><tr><td>-rw-r--r--</td><td>For a file that only you will be editing. It allows everyone to read it, but only you may edit it.</td><td>chmod 644 filename</td></tr><tr><td>-rw-rw-r--</td><td>For a file that you and the members of the group will edit. It allows everyone to read it, but only you and the group may edit it.</td><td>chmod 664 filename</td></tr><tr><td>-rw-rw-rw-</td><td>This one is bad. It allows absolutely anyone to edit your file. Avoid this one at all costs! unless needed of course</td><td>chmod 666 filename</td></tr><tr><td>drwxr-xr-x</td><td>For a directory in which only you can create and delete files. It allows everyone to find files inside of it, but only you can add files, rename them, or remove them. (In many cases, the owner of a file can remove it regardless of the directory's permissions, but this is a special case.)</td><td>chmod 755 directoryname</td></tr><tr><td>drwxrwxr-x</td><td>For a directory in which you and the group can create and delete files. It allows everyone to find files inside of it, but only you and the group can add, rename, or remove files. (The same special case applies as for the previous example.)</td><td>chmod 775 directoryname</td></tr></tbody></table>	Permissions	Description	Commands Required	-rw-r--r--	For a file that only you will be editing. It allows everyone to read it, but only you may edit it.	chmod 644 filename	-rw-rw-r--	For a file that you and the members of the group will edit. It allows everyone to read it, but only you and the group may edit it.	chmod 664 filename	-rw-rw-rw-	This one is bad . It allows absolutely anyone to edit your file. Avoid this one at all costs! unless needed of course	chmod 666 filename	drwxr-xr-x	For a directory in which only you can create and delete files. It allows everyone to find files inside of it, but only you can add files, rename them, or remove them. (In many cases, the owner of a file can remove it regardless of the directory's permissions, but this is a special case.)	chmod 755 directoryname	drwxrwxr-x	For a directory in which you and the group can create and delete files. It allows everyone to find files inside of it, but only you and the group can add, rename, or remove files. (The same special case applies as for the previous example.)	chmod 775 directoryname
Permissions	Description	Commands Required																	
-rw-r--r--	For a file that only you will be editing. It allows everyone to read it, but only you may edit it.	chmod 644 filename																	
-rw-rw-r--	For a file that you and the members of the group will edit. It allows everyone to read it, but only you and the group may edit it.	chmod 664 filename																	
-rw-rw-rw-	This one is bad . It allows absolutely anyone to edit your file. Avoid this one at all costs! unless needed of course	chmod 666 filename																	
drwxr-xr-x	For a directory in which only you can create and delete files. It allows everyone to find files inside of it, but only you can add files, rename them, or remove them. (In many cases, the owner of a file can remove it regardless of the directory's permissions, but this is a special case.)	chmod 755 directoryname																	
drwxrwxr-x	For a directory in which you and the group can create and delete files. It allows everyone to find files inside of it, but only you and the group can add, rename, or remove files. (The same special case applies as for the previous example.)	chmod 775 directoryname																	

	<code>drwxrwxrwx</code> <code>x</code>	This one is bad . It allows absolutely anyone to mess with your files. Avoid this one like the plague!	<code>chmod 777 directory / filename</code>
Test Nature – Objective or Subjective	Objective		
Evidence			
Finding	Directory permissions setup on the MySQL directory appear to be sufficient and restricted to appropriate accounts.		

Audit Report

Executive Summary

The focus of this audit was to assess the current state of a SuSE 8 Linux box running MySQL. This box contains Intrusion Detection alerts, port mappings and vulnerabilities that are mapped to individual IP addresses on a university's network. This server is also storing syslog information for campus critical systems to log to. This box is crucial to any forensics and incident handling for this University.

In order for any of this information to be trusted, this audit was aimed to verify any Integrity issues that may exist or expose vulnerabilities that could compromise the availability, Integrity or confidentiality of the data on this system.

Ten tests were performed on the system in question to verify the integrity and security of the system. For the most part, it was apparent that due diligence was performed in the setup of this system. However there are a couple of areas of concern in regards to system maintenance, administration and system hardening.

It should be noted that most of these issues can be addressed with little to no cost to the University and can be addressed fairly quickly. Although not within the scope of this audit, the University should rethink about running their syslog box on another dedicated syslog server.

Findings

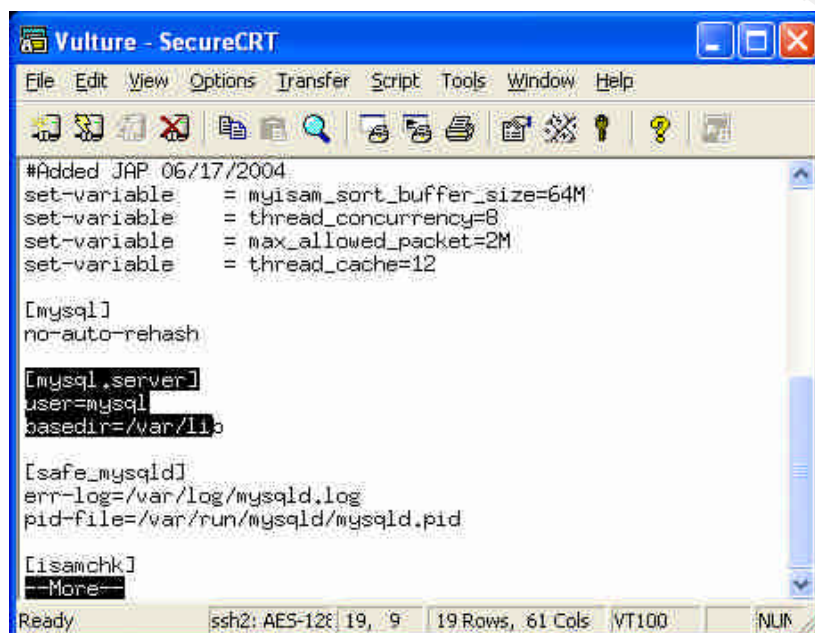
Checklist Number	Description	Subjective/Objective	Pass/Fail
1	NonPrivileged account for MySQL	Objective	Pass
3	Set a Password for the "root" user	Objective	Pass
4	Hide MySQL from rest of the world	Objective	Failed
5	UnPatched MySQL Application	Objective	Failed
11	Host Communication Restrictions	Objective	Failed
12	System Hardening	Objective	Pass
13	System Patched	Objective	Failed
14	Limited User Accounts	Objective	Pass
18	User Staffing/training	Subjective	Pass
19	System hardening	Objective	Pass

Finding Details:

Checklist Item 1 – Nonprivileged account for MySQL instance

Running applications or daemons in a “root” privilege mode can allow potential escalation for an unauthorized attacker if they were to gain access to the box. This is especially a concern in regards to databases. MySQL uses a configuration file called my.cnf which tells the program or daemon what to run the process under. Examining this file illustrated that there is a mysql user id that is configured.

The illustration below illustrates the “cat” command we issued against the my.cnf.



```
#Added JAP 06/17/2004
set-variable      = myisam_sort_buffer_size=64M
set-variable      = thread_concurrency=8
set-variable      = max_allowed_packet=2M
set-variable      = thread_cache=12

[mysql]
no-auto-rehash

[mysql.server]
user=mysql
basedir=/var/lib

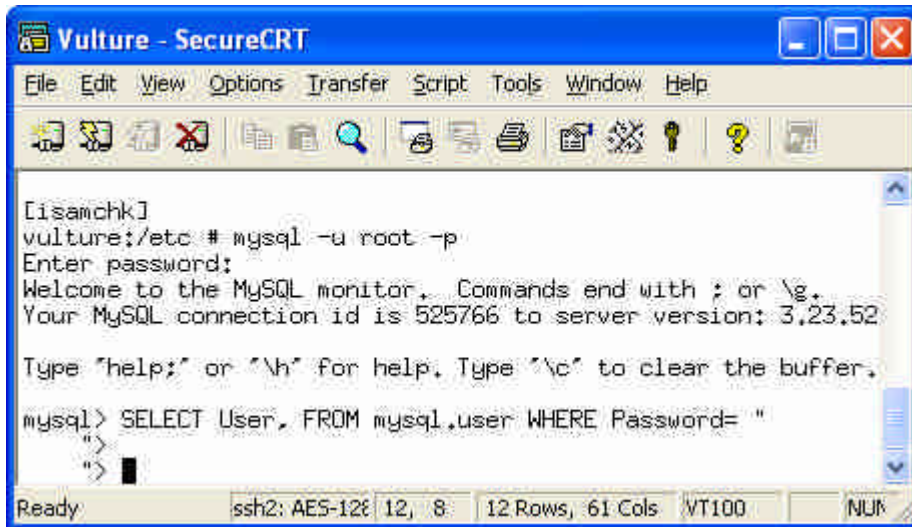
[safe_mysqld]
err-log=/var/log/mysqld.log
pid-file=/var/run/mysqld/mysqld.pid

[isamchk]
--More--
```

Checklist Item 3 - Set a password for the “root” User

Running an application without a password can easily allow an unauthorized user to gain additional access to information. A simple query can be run within MySQL to verify that a password is required or exists.

The screen shot below shows the result of the query, and verifies that there indeed is a password for the root account.



Checklist Item 4 – Hide MySQL from rest of world

Having this system exposed allows potential unauthorized access resulting in Availability and Integrity issues. Without any mechanisms in place, probes and brute force attempt can easily be performed against this system.

To test to see if this system is hidden, port probes were conducted from various locations. Unfortunately this system appears to be accessible anywhere. The screen shot below shows the results of our probes.

```

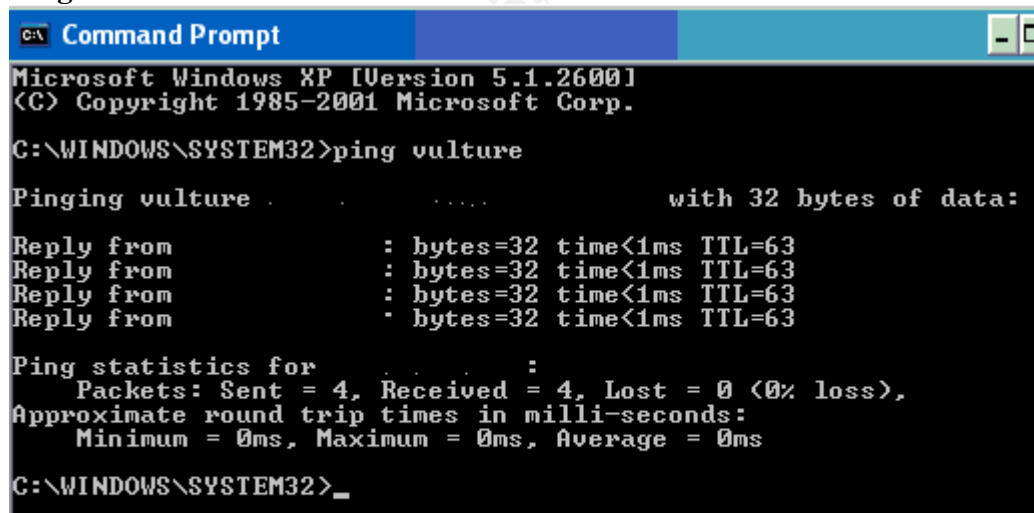
crawford@kali:~$ nmap -sS -O -v -p 1-65535 vulture
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Host vulture appears to be up ... good.
Initiating SYN Stealth Scan against vulture
Adding open port 22/tcp
Adding open port 3306/tcp
The SYN Stealth Scan took 1 second to scan 65535 ports.
For OSscan assuming that port 22 is open and port 1 is closed and neither are firewalled
For OSscan assuming that port 22 is open and port 1 is closed and neither are firewalled
For OSscan assuming that port 22 is open and port 1 is closed and neither are firewalled
Interesting ports on vulture:
(The 65533 ports scanned but not shown below are in state: closed)
Port      State      Service
22/tcp    open       ssh
3306/tcp   open       mysql
No exact OS matches for host (If you know what OS is running on it, see http://www.insecure.org/cgi-bin/nme
TCP/IP fingerprint:
SInfo(V=3.00%P=i586-suse-linux%D=12/7%Time=41B5FF9D%D=22%C=1)
TSeq(Class=RI%gcd=1%SI=308C24%IPID=I%TS=100HZ)
TSeq(Class=RI%gcd=1%SI=309160%IPID=I%TS=100HZ)
TSeq(Class=RI%gcd=1%SI=308EB4%IPID=I%TS=100HZ)
T1(Resp=Y%DF=Y%W=16A0%ACK=S++%Flags=AS%Dps=MNNNTNW)
T2(Resp=N)
T3(Resp=N)
T4(Resp=Y%DF=Y%W=0%ACK=0%Flags=R%Dps=)
T5(Resp=Y%DF=Y%W=0%ACK=S++%Flags=AR%Dps=)
T6(Resp=Y%DF=Y%W=0%ACK=0%Flags=R%Dps=)
T7(Resp=Y%DF=Y%W=0%ACK=S++%Flags=AR%Dps=)
PU(Resp=Y%DF=N%TOS=C0%IPLEN=164%RIPTL=148%RID=E%RIPCK=E%UCK=E%ULEN=134%DAT=E)

Uptime 151.007 days (since Fri Jul 9 13:58:18 2004)
TCP Sequence Prediction: Class=random positive increments
Difficulty=3182260 (Good luck!)
IPID Sequence Generation: Incremental

Nmap run completed -- 1 IP address (1 host up) scanned in 18 seconds

```

Ping Host 1 – Should be able to talk to host



```

C:\WINDOWS\SYSTEM32>ping vulture

Pinging vulture [192.168.1.100] with 32 bytes of data:

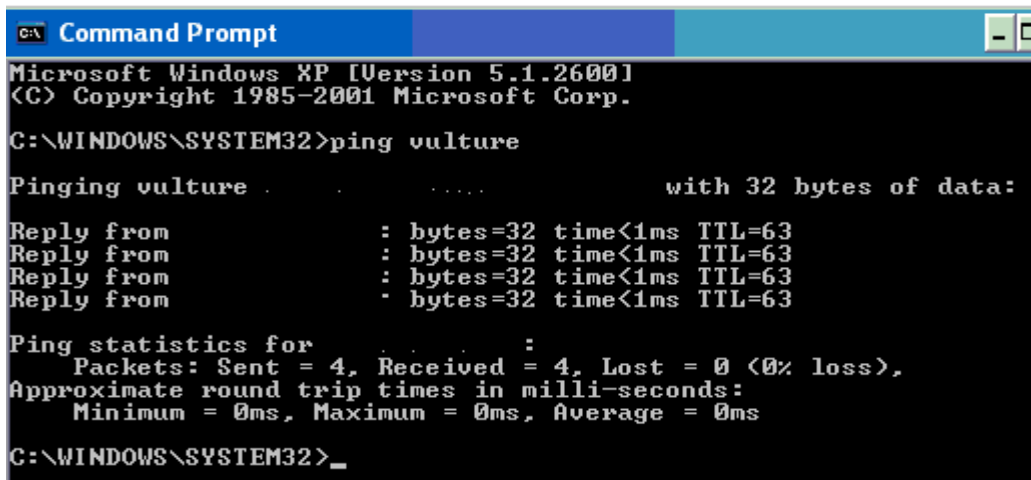
Reply from 192.168.1.100: bytes=32 time<1ms TTL=63
Reply from 192.168.1.100: bytes=32 time<1ms TTL=63
Reply from 192.168.1.100: bytes=32 time<1ms TTL=63
Reply from 192.168.1.100: bytes=32 time<1ms TTL=63

Ping statistics for 192.168.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\WINDOWS\SYSTEM32>

```

Ping Host 2 – Should not be able to talk to host



```
C:\ Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\SYSTEM32>ping vulture

Pinging vulture [192.168.1.100] with 32 bytes of data:

Reply from 192.168.1.100: bytes=32 time<1ms TTL=63
Reply from 192.168.1.100: bytes=32 time<1ms TTL=63
Reply from 192.168.1.100: bytes=32 time<1ms TTL=63
Reply from 192.168.1.100: bytes=32 time<1ms TTL=63

Ping statistics for 192.168.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\WINDOWS\SYSTEM32>_
```

Checklist Item 5 – UnPatched MySQL Application

Keeping a system patched and updated is one of the best first lines of defense in keeping an attacker out. Leaving systems unpatched allowed an attacker to exploit vulnerabilities which can lead to Integrity issues with the data and system.

A query was run against MySQL to examine which version is currently installed. A comparison was then made against the MySQL website to see what is the most current version. A Google search was also performed to search for any vulnerabilities with the current version of MySQL. One was found, which appears to be critical.

Checklist Item 11 – Host communication restrictions

Having this system exposed allows potential unauthorized access resulting in Availability and Integrity issues. Without any mechanisms in place, probes and brute force attempt can easily be performed against this system.

To test to see if this system is hidden, port probes were conducted from various locations. Unfortunately this system appears to be accessible anywhere. The screen shot below shows the results of our probes.

Woodpecker - SecureCRT

```

vulture:/etc # cat hosts.allow | more
# /etc/hosts.allow
# See `man tcpd` and `man 5 hosts_access` for a detailed description
# of /etc/hosts.allow and /etc/hosts.deny.
#
# short overview about daemons and servers that are built with
# tcp_wrappers support:
#
# package name | daemon path | token
# -----
# ssh, openssh | /usr/sbin/sshd | sshd, sshd-fwd-x11, sshd-fwd-<port>
# quota | /usr/sbin/rpc.rquotad | rquotad
# tftpd | /usr/sbin/in.tftpd | in.tftpd
# portmap | /sbin/portmap | portmap
#
# The portmapper does not verify against hostnames
# to prevent hangs. It only checks non-local addresses.
#
# (kernel nfs server)
# nfs-utils | /usr/sbin/rpc.mountd | mountd
# nfs-utils | /sbin/rpc.statd | statd
#
# (unfsd, userspace nfs server)
# nfs-server | /usr/sbin/rpc.mountd | rpc.mountd
# nfs-server | /usr/sbin/rpc.ugidd | rpc.ugidd
#
# (printing services)
# lprng | /usr/sbin/lpd | lpd
# cups | /usr/sbin/cupsd | cupsd
#
# The cupsd server daemon reports to the cups
# error logs, not to the syslog(3) facility.
#
# All of the other network servers such as samba, apache or X, have their own
# access control scheme that should be used instead.
#
# In addition to the services above, the services that are started on request
# by inetd or xinetd use tcpd to "wrap" the network connection. tcpd uses

```

Ready ssh2: AES-128 36, 16 36 Rows, 101 Cols VT100 NUM

3.

Command Prompt

```

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\SYSTEM32>ping vuln.re

Pinging vulture [192.168.1.1] with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=63
Reply from 192.168.1.1: bytes=32 time<1ms TTL=63
Reply from 192.168.1.1: bytes=32 time<1ms TTL=63
Reply from 192.168.1.1: bytes=32 time<1ms TTL=63

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\WINDOWS\SYSTEM32>_

```

```

Last login: Sun Dec 5 10:23:13 2004 from 223.69.1.1
vulture:~ # netstat -rn
Kernel IP routing table
Destination        Gateway            Genmask           Flags    MSS Window  irtt Iface
0.0.0.0            0.0.0.0           0.0.0.0           U        0 0        0 eth0
0.0.0.0            192.168.1.254    0.0.0.0           UG       0 0        0 eth0
vulture:~ #

```

4.

Checklist Item 12 – System hardening – Services

Having unnecessary services running on a system, increases the potential for an attacker to exploit another application or service. By reducing the amount of unneeded services running on a server, overall exposure of the box is limited

Several locations on the server were examined to determine what services are set to run and what is installed. The screen shot below shows the result of a “*netstat -ano*” command. This command shows what services are currently listening for connections. Overall this system is tightened down, it appears that only 3 services are listening for remote connections on this system. All 3 services are required for this application to run correctly.

```
. Timer
tcp      0    0 0.0.0.0:3306      0.0.0.0:*        LISTEN
off (0.00/0/0)
tcp      0    0 0.0.0.0:22        0.0.0.0:*        LISTEN
off (0.00/0/0)
tcp      0    0 127.0.0.1:25       0.0.0.0:*        LISTEN
```

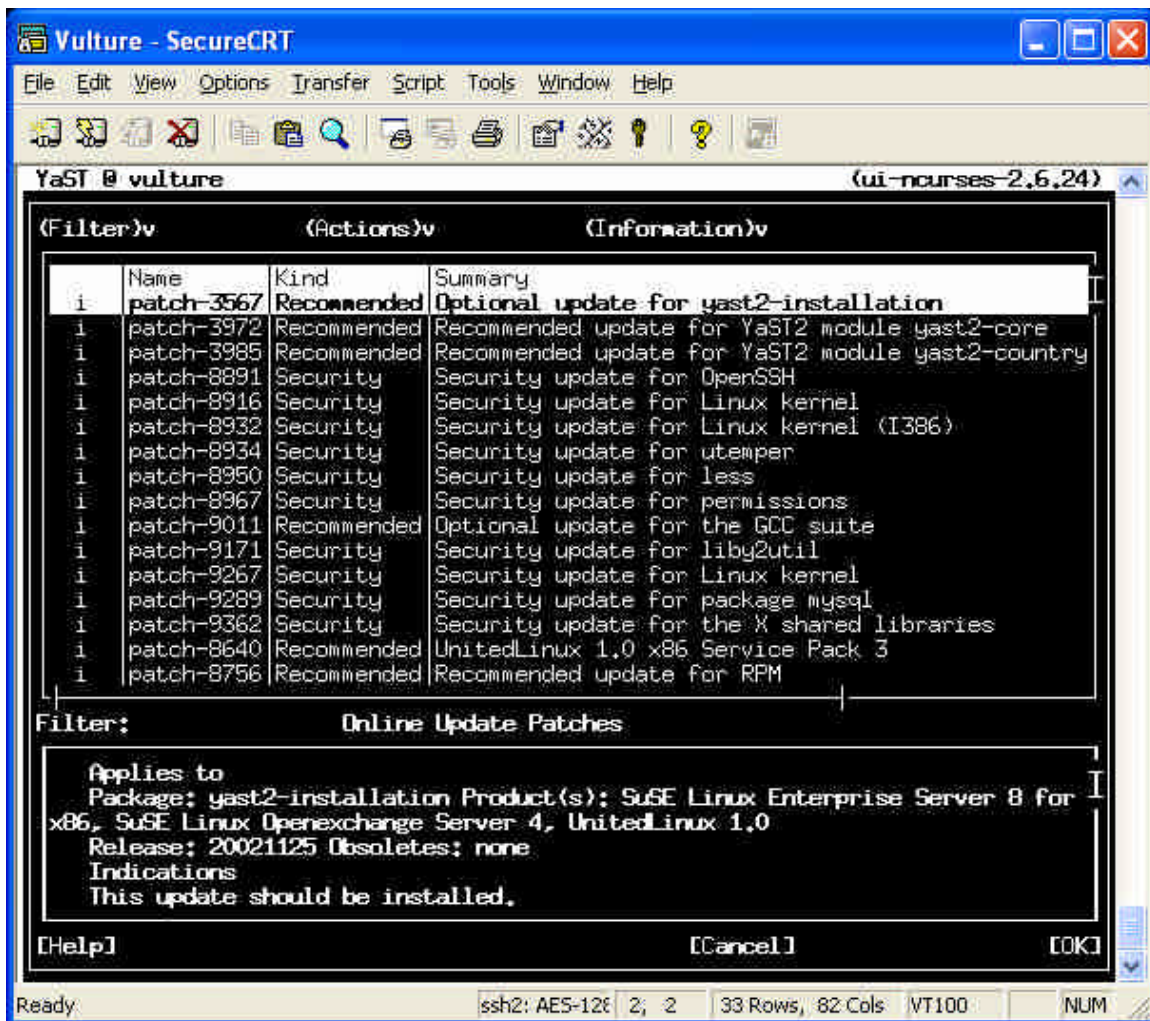
Checklist Item 13 – System Patched / Updated

Keeping a system patched and updated is one of the best first lines of defense in keeping an attacker out. Leaving systems unpatched allowed an attacker to exploit vulnerabilities which can lead to Integrity issues with the data and system.

SuSE linux comes with a utility called YaST. By running the following command, we were able to check and verify what patches are not installed: “*yast2 online_update*”.

The output below shows that many security patches are currently not installed. There are numerous vulnerabilities that this system is at risk to.

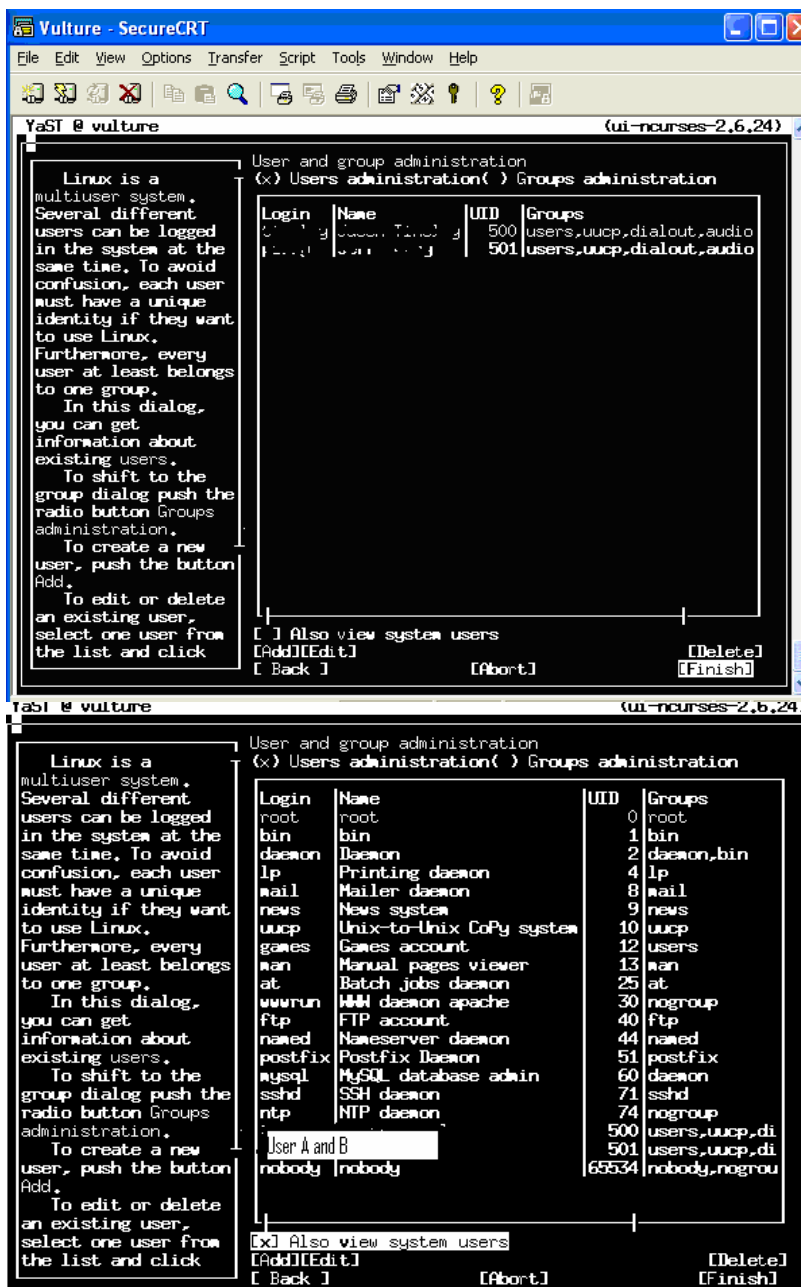
© SANS Institute. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or by any information storage or retrieval system, without the prior written permission of SANS Institute.



Checklist Item 14 – Limited user Accounts

A key to a secure system is limiting the amount of users that exist on the system. The less users that exist, reduces the overhead for maintaining the accounts.

Using SuSE Linux YaST tool, one can simply view the users, groups and system accounts currently on the system. In reviewing this system, it appears that there is a very limited amount of accounts on this system.



Checklist Item 18 – User staffing/training

Managing a server, especially a database server takes skill. An untrained or inexperienced admin running a database server can accidentally misconfigure the box leaving it open for a compromise. The integrity and availability of the data is at risk.

This item is purely subjective to the auditor. Numerous interviews were held with Human Resources, the system administrator, the administrator's supervisor. The administrators resume was viewed as well.

The result of the interviewed illustrated that these administrators had good experience in the realm of system and database administration. Both administrator's however were fairly new to SuSE linux.

Checklist Item 19 – System hardening

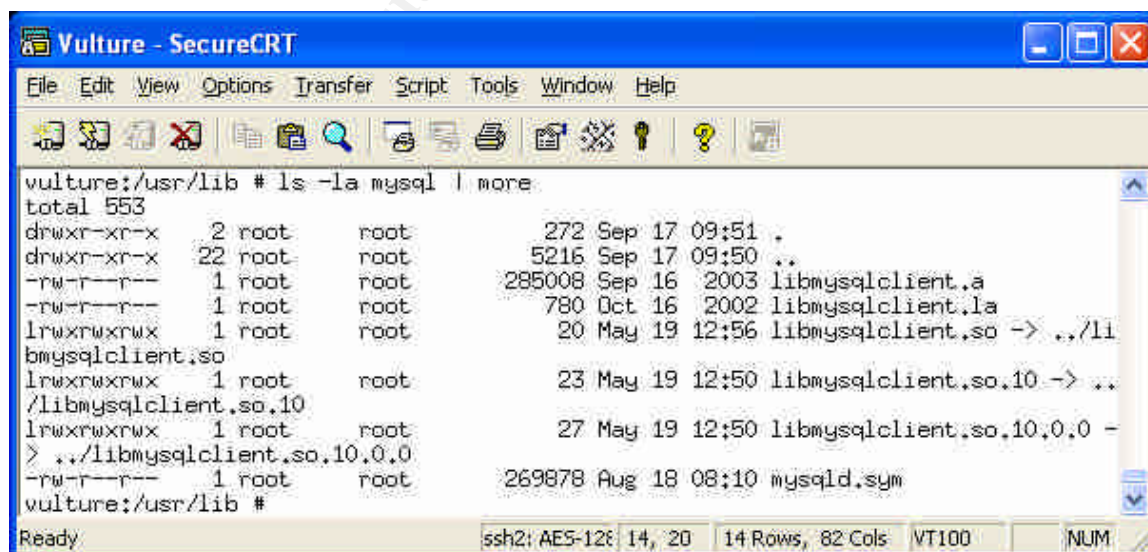
Having lax file permissions on system files can allow an authorized or unprivileged user to view information in another directory they shouldn't have access to.

Several areas on the SuSE Linux operating system can be examined to see how secure the file permissions were set, including examining the permissions.local, permissions.easy, permissions.hard and permissions.paranoid file.

In regards to this audit we also examined the MySQL directory by performing an *"ls-la"* command.

It appears that the file system and MySQL directories have the appropriate permissions applied to them.

The screenshot below shows the output from the *ls-la* command against the MySQL directory.



```
vulture: /usr/lib # ls -la mysql | more
total 553
drwxr-xr-x  2 root  root    272 Sep 17 09:51 .
drwxr-xr-x 22 root  root   5216 Sep 17 09:50 ..
-rw-r--r--  1 root  root   285008 Sep 16 2003 libmysqlclient.a
-rw-r--r--  1 root  root    780 Oct 16 2002 libmysqlclient.la
lrwxrwxrwx  1 root  root     20 May 19 12:56 libmysqlclient.so -> ../li
libmysqlclient.so
lrwxrwxrwx  1 root  root     23 May 19 12:50 libmysqlclient.so.10 -> ..
/libmysqlclient.so.10
lrwxrwxrwx  1 root  root     27 May 19 12:50 libmysqlclient.so.10.0.0 -
> ../libmysqlclient.so.10.0.0
-rw-r--r--  1 root  root   269878 Aug 18 08:10 mysqld.sym
vulture: /usr/lib #
```


Recommendations:

The recommendations to the findings above can be broken up to two areas enforcing the concept of defense in depth. The recommendations below outline the need for restricting and hiding the server and system patching. These recommendations can come at a minimal cost to the university.

1. This system should be put behind a Network based firewall. This firewall should be configured to only allow specific hosts in and also restrict outbound access from this host. This Firewall should also perform NAT (Network Address Translation) to further hide this server
2. On the server itself, further restrictions should be set. Route restrictions should be put in place so that only specific hosts can talk to this system. This can be accomplished in a multitude of ways. Modifying the system route table, editing host.deny or hosts.allow files or this operating system also comes with a host based firewall. This firewall should be enabled and configured regardless if any of the options previously stated are used.
3. The Operating system is in severe need of updating. This can be accomplished simply by running the command "*yast2 online_update*". The update process itself can be automated.
4. The MySQL instance on this server is in need up upgrading as well. As stated above, there is a vulnerability with this server.

Costs:

The hardware that this application runs on is very well suited and should not need to be modified in anyway. The only cost to the university, for the documented recommendations, should be with the cost of the firewall, network cables, as well as the "man hours" needed to implement the recommendations listed above. This is also assuming that the licensing for the Operating system is legitimate.

Works Consulted

Ten MySQL Best Practices

by [George Reese](#), coauthor of [Managing & Using MySQL, 2nd Edition](#)

07/11/2002 URL:

<http://www.onlamp.com/pub/a/onlamp/2002/07/11/MySQLtips.html>

MySQL Administrator Best Practices

URL: <http://dev.mysql.com/tech-resources/articles/mysql-administrator-best-practices.html>

Making MySQL Secure Against Attackers

URL: http://dev.mysql.com/doc/mysql/en/Security_against_attack.html

Auditing a MySQL database Server

By Jeff Hoover URL: http://www.giac.org/practical/GSNA/Jeff_Hoover_GSNA

Securing MySQL: step-by-step:

<http://www.securityfocus.com/infocus/1726>, Artur Maj, August 28, 2003

The Rookery: Security Tools in Linux Distributions, Part II

Posted on Monday, October 07, 2002 by [Bobby S. Wen](#)

Suse Linux Administrator Guide

<http://shelob.temple.edu/suse/local/SuSE-Linux-Adminguide-8.2.0.1x86.pdf>

Linux Kernel Hardening

By Taylor Merry URL: <http://www.sans.org/rr/papers/32/1294.pdf>

“Information Security Managers Handbook Volume 4” by Harold Tipton and Micki Krause

Risk Management Guide:

<http://www.csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>

Miscellaneous Web Sites related to Linux and MySQL security

http://www.securitydocs.com/Operating_System/

<http://www.linuxvoodoo.org/resources/guides/>

<http://www.linuxhq.com/guides/index.html>

http://www.suse.com/us/private/products/suse_linux/prof/security.html

http://www.suse.com/us/private/products/suse_linux/prof/yast.html

http://www.justlinux.com/nhf/Security/Securely_Installing_Linux.html

<http://ccfaq.valar.co.uk/modules.php?name=News&file=article&sid=105>