Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

Auditing a Gentoo Linux Workstation

GNSA Practical Version 3.1 (February 24, 2004)
Option #1: Device, System or Application Auditing

Prepared by: **Christopher Navarro**
Date: **June 30, 2004**

Abstract

The following document contains an audit check list for assessing the security of a Gentoo Linux System acting as a workstation. This document contains information gathered from industry accepted standards published by authorities in the field such as ISO, ICSA, NIST, CIS among others.

Table of Contents

1 Research in Audit, Measurement Practice and Control

Identify System to be Audited

The following documentation describes the security audit of a laptop workstation. The scope of the process will be limited to auditing the prevention of unauthorized physical access to the machine, auditing the security of the system startup process and finally, auditing of the preservation of user privacy from other system users and from other network users.

This laptop is used primarily as a network client in the main office for about 70% of the time and 30% of the time connected to client's networks.. The machine serves to access network resources which include email, file servers, database servers, web servers, several print servers and the Internet. As a network client this system includes but is not limited to software such as an email client, a web browser, an office suite, a printing system and a graphics authoring application. The workstation is in a network protected by a firewall and connected to the Internet by means of a T1 line. The following diagram illustrates the setup:
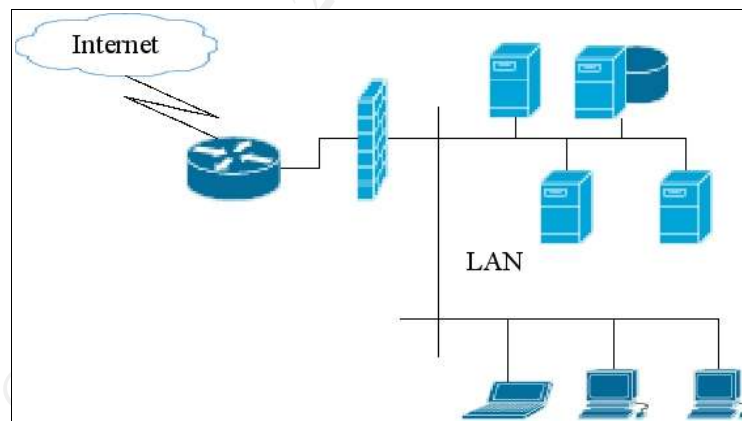

Figure 1: *Workstation's Network Diagram*

The following table illustrates the physical characteristics of the laptop:

Manufacturer	Toshiba
Model	Satellite 1905-S227
CPU	Intel(R) Pentium(R) 4 CPU 1.60GHz stepping 02
Physical Memory	512 Mb, PC133 SODIMM512 Mb, PC133 SODIMM
Hard Disk	TOSHIBA MK3017GAP, ATA DISK drive, 30 Gb
Optical Disk	UJDA720 DVD/CDRW, ATAPI CD/DVD-ROM drive
Network Interface	Intel Pro 100

Table 1 Laptop physical characteristics

The file system is laid out much in the same way as most distributions. The root file system is located on the main partition with 23Gb of space. The /boot directory is located on a separate partition with 42 Mb. There is also a separate partition to hold the /home directory with 4.3Gb of space and finally there is a swap partition with 840 Mb of space. All file systems are formated with the Third Extended File System format (ext3).

The ext3 file system is based on the ext2 system so all existing utilities for ext2 can be used on ext3. The ext3 provides **availability**, since no consistency checks are required after an unclean system shutdown; **data integrity** since the default is to maintain the data consistent with the state of the file system; and **speed** since the file system optimizes hard drive head motion. The ext3 achieves all these improvements over ext2 through the use of a journal, which defaults to maintaining data integrity while it is possible to tune it for better throughput.

The system uses GNU Grub[1] to load the Gentoo Linux Distribution. The Gentoo Linux distribution strives to be a very customizable system. Gentoo Linux is very easy to optimize for just about any application.   Ranging from workstation to server, Gentoo Linux can handle any job very well.

Gentoo Linux is a sources based distribution. That is, every part of the system must be compiled from source. This makes every installation a tailored system for both the hardware it is running on and for it's intended usage. Gentoo Linux has one of the most advanced package management systems seen to date; Portage.

Portage contains a series of ebuild[2] scripts that automate all the steps necessary to get an application installed in a system. The ebuild scripts tell the system to get the source code, how to configure and compile the application and where it should be installed along with it's configuration files.

---

1 Grub is a multi boot loader , it loads the kernel so the kernel can load the rest of the system.
2 Bash scripts that guide in the automated configuration, compilation and installation of a program.

Portage even takes it a step further than other package management tools by installing any dependent packages before installing the desired application. This means that, for example, if you have a system with no X11 based graphical user interface installed and you try to install OpenOffice, then *emerge*[3] will download and compile the latest versions of XFree86. Depending on the user's preferences, Gnome or KDE would also be emerged followed by a plethora of other programs and libraries that are required. Finally it would emerge the Open Office code.

Installing Gentoo is no easy task, since there is no installation wizard, the user must follow an installation manual and enter each and every command at the console. On the other hand, anyone who installs a Gentoo system acquires an incredible insight into the inner workings of GNU/Linux.

Gentoo Linux is a BSD[4] compatible system although recent development in Portage hints to a move into System V[5] compatibility, perhaps to standardize Gentoo support for the Linux Standard Base project, LSB[6].

Evaluate the most significant risks to the system

About Information Security

The ISO 17799:2000(E) says the following regarding information security:

> *"Information security protects information from a wide range of threats in order to ensure business continuity, minimize business damage and maximize return on investments and business opportunities."*

In essence information security is the preservation of confidentiality, integrity and availability[2] as related to maintaining business continuity. Confidentiality is maintained by limiting who has access to the information; only those with explicit authorization may have access to it. The integrity of the information is kept by ensuring that only those with explicit permission may modify the data. Finally the availability is kept by ensuring that authorized users have access to the information when required.

In order to provide information security, an organization first needs to determine the risks associated with the information and assets that are to be protected, hence the need for risk assessment.

About Risk Assessment

Using information from the standard provided in the ISO17799:2000(E), risk assessment can be defined as: the process of determining the impact that a loss

---

3   emerge is a command to add/remove packages in a Gentoo system.
4   Berkeley Software Distribution, an implementation of the UNIX operating system.
5   The other major flavor of UNIX, developed by AT&T
6   LSB is "a set of standards that will increase compatibility among Linux distributions and enable software applications to run on any compliant system[1]

of confidentiality, integrity or availability of information may have on a business while also considering how likely is an event to occur that would result in a loss.

The Certified Information Systems Security Professional Study Guide[3] describes two accepted methods of measuring risk, the quantitative and the qualitative.

The quantitative method tries to represent risk using objective factors, for example expressing risk as the result of the probability of an event to occur multiplied by the potential loss should the event occur. This method tries to assign discrete values that because of their nature make it more difficult to measure risk since some of the factors are intangible.

The qualitative method is subjective in nature. This method assigns threats a ranking value to evaluate their risks, costs, and effects. This method is more widely used to measure information security risks.

A method of performing risk analysis must be adopted to properly determine the risk involved with an asset. The method used for this audit is the one illustrated by Nancy A. Renfroe and Joseph L. Smith in their research article "Threat/Vulnerability Assessments & Risk Analysis"[4]. Although the article is aimed at risk assessment as pertained to government buildings, the method is very simple to use. Achieving information security is currently, a very complex process and therefore, adopting a simple method of risk analysis improves the probability of more companies actually accepting it. The risk analysis method consists in three steps: A threat assessment, a vulnerability assessment and finally the risk assessment is derived.

A threat assessment is performed to determine the threats related to an asset. The assessment consists on evaluating how likely each threat is to occur by examining existing information regarding the threat. The impact of the a loss of confidentiality, integrity or availability of the asset would pose on business continuity is also determined. The Impact of an attack to the system can be measured in the following way:

	Level	Description
1	Devastating	The system is lost or inaccessible
2	Severe	The system is crippled but not lost
3	Noticeable	The system is not performing to standards
4	Minor	The system is unaffected

Table 2 *Impact Level*

The next step in the risk assessment method is a vulnerability assessment. This assessment consists in determining the potential impact in business continuity that an attack poses as well as how vulnerable a system is to the identified

threats. The vulnerabilities of an asset can be ranked in the following way:

Level	Description
Very High	An attack results in a system compromise and there are no countermeasures in place
High	An attack results in a system compromise and there are few countermeasures in place
Moderate	An attack does not result in a system compromise or there are sufficient countermeasures in place
Low	Low probability of attack success

Table 3 *Vulnerability Level*

Renfroe and Smith[4] further explain that the resulting risk levels can be illustrated with the following matrix:

Impact	Vulnerability			
	Very High	High	Moderate	Low
Devastating				
Severe				
Noticeable				
Minor				

Table 4 *Resultant Risk Levels*

The following table summarizes the resultant risk assessments as described by Renfroe and Smith:

Level	Description
HIGH	Risks in this category should be given priority. Attacks in this level will result in loss of business continuity. Action should be taken immediately to counteract the associated attack.
MEDIUM	Risks at this level have a fair chance to result in loss of business continuity and can be addressed in the near future.
LOW	Risks in this category are not a threat to business continuity. These threats should be addressed only when convenient to the organization.

Table 5 Risk Levels Descriptions

Risk Analysis

Description of the assets

To the consultant and the type of work he performs, he is very reliant on the availability of the system thus it is of utmost importance. However, there are other assets that are also important. The following table lists the major assets related to the laptop workstation.

Asset	Description
System Availability	The system is completely relied upon for the work performed by it's user.
Business related documentation	The user creates many documents as part of his everyday tasks.
Personal documentation	The user stores personal files in the system.
Access to the Internet	This workstation is used to access the Internet for research purposes.
Entertainment	The system is used to view DVDS and as a music player during after hours

Table 6 List of Assets related to the system

Evaluation of Threats

The following is a risk analysis of the major threats to the Laptop workstation.

Threat 1
Theft of the device

Threat Assessment

Vulnerability: High

The nature of the device makes it very easy to steal. The only preventative measures that can be taken with this vulnerability is to store the device in a safe place or to use a restrain system to attach it to an unmovable object.

Impact: Devastating

The theft of the device would result in both a complete loss of the information and a denial of service for the user. If the theft occurs during a trip, the likelihood of restoring the information, assuming a back up exists and the replacement of the device becomes minimal.

The CSI/FBI 2004 Computer Crime and Security Survey[5] states that for out of the $141,496,560 in computer losses this year $6,734,500 were lost due to laptop theft, this accounts for 5% of the total loss.

Resultant Risk Level: **High**

Threat 2
Unauthorized access to the device from the network

Threat Assessment

Vulnerability: High

The nature of the attack would result in a system compromise. Since this system, is a workstation and not a server, the probability for an unauthorized remote access is dependent upon unknown software flaws in one of the system's client applications and the existence of an exploit. Therefore the vulnerability level cannot be cataloged as "Very High"

Impact: Devastating

If an attack to gain access to the system remotely were to succeed the entire system could be assumed lost since it would be at the mercy of the attacker.

Resultant Risk Level: **High**

Threat 3

Natural disaster or accident

Threat Assessment

Vulnerability: Very High

Since a natural disaster or an accident cannot be prevented there are very few countermeasures that can be taken.

Impact: Devastating

If a natural disaster or an accident occurs that involves the laptop, the result would most likely be a loss since the device is very sensitive to environmental conditions.

Resultant Risk Level: High

Threat 4

Lack of user training

Threat Assessment

Vulnerability: Very High

The vulnerability results in loss of productivity at a minimum and has potential to completely render the system unusable if the user has root access.

Impact: Devastating

Assuming the worst case scenario, that being the user has root access to the system, then it can be assumed that the system is lost.

Resultant Risk Level: High

Threat 5

BIOS boot password not set

Threat Assessment

Vulnerability: Low

No direct access to the system is achieved by merely starting the system.

Impact: Minor

There is nothing wrong with allowing the system to run.

Resultant Risk Level: Low

Threat 6

BIOS setup password not set

Threat Assessment

Vulnerability: Very High

Anyone could change the first boot device to boot off a CDROM with tools to access the hard drive.

Impact: Devastating

Complete unauthorized access to the system is achieved.

Resultant Risk Level: HIGH

Threat 7

Boot loader password not set

Threat Assessment

Vulnerability: Very High

If a boot loader password is not used, it is possible to boot the system in single user mode, which grants the user a root shell to perform "system maintenance"

Impact: Devastating

Root access to the system results.

Resultant Risk Level: High

Threat 8

Weak user passwords used

Threat Assessment

Vulnerability: Very High

Weak user passwords are easy to compromise

Impact: Devastating

Access to the user's data and all other systems that the user has access to results.

Resultant Risk Level: High

Threat 9

Incorrect permissions on system configuration files

Threat Assessment

Vulnerability: High

Any authenticated user can make modifications to the system's configuration, there is a potential for complete system compromise

Impact: Severe

The system can become unstable and even unbootable.

Resultant Risk Level: **High**

Threat 10

Unnecessary user accounts exist

Threat Assessment

Vulnerability: Moderate

Stale user accounts can be compromised and be used for unauthorized access to the system.

Impact: Minor

Only the user data is compromised, not the complete system.

Resultant Risk Level: **Low**

Threat 11

Unknown software bug

Threat Assessment

Vulnerability: High

A system bug could cause the system to become unavailable or to be subject to remote exploitation

Impact: Severe

Loss of business continuity may result.

Resultant Risk Level: **High**

What is the current state of practice

Perhaps now that Linux is gaining more market share there will be more documentation available. The following is a list of resources detailing the current state of practice regarding the security of Linux workstations. Please refer to the references section for the detailed bibliographic descriptions of the resources listed below.

Resource	Comments
Gentoo Linux X86 Handbook	Gentoo does not have an installation wizard. This manual proves invaluable to getting the system installed. You learn a lot about how Linux works along the way.
Gentoo Linux Security Guide	This document provides a baseline of security for the Gentoo Linux user.
Unix System Administration Handbook	Covers all concepts in system administration and basics of security. It's the little bible of system administration.
ISO17799:2000(E)	This is the Information security standard. It covers all all aspects from physical security to system security.
The CIS Linux Benchmark v1.1.0	This document provides a security policy for administrators to follow. Along with policy items and recommendations a rationale is given.
The SANS reading room	Incredible source of peer documentation.
Risk Management Guide for Information Technology Systems	An NIST document on how to perform risk management of information technology assets, a valuable source from the Department of Commerce
Mac OS X Single User Mode Root Access	Valid points about the security of single user mode in *nix machines

***Table 7** Linux Security Resources*

2 Create an Audit Checklist

The following is a list of check to perform given the scope of this document.

Preliminary tests	
1	
1.1 Verify Existence of a laptop security cable	
References	[6] [2] [7]
Risk	The nature of a laptop makes it very vulnerable to theft. This results in a loss of confidentiality, integrity and availability of the asset.
Testing Procedure	Search the surroundings and carrying case of the laptop for a cable. Ask the user for the existence of a security cable for the device.
Expected Result:	Existence of a laptop cable.
Test Nature	Both objective and subjective
Evidence	
Findings	
1.2 Verify the system does not contain a root kit	
References	Personal Experience: It is always a good idea to establish the trustworthiness of the tools in the system to be audited.

Risk	Complete loss of the system. All subsequent tests in this audit program will be flawed.
Testing Procedure	1. Start the system using a bootable CDROM with security tools such as Knoppix-STD
	2. Mount the audited system's root partition and perform the following command
| | ```
# mount -t auto -o ro /dev/hda4 /mnt/hda4
# chkrootkit -r /mnt/hda4 > chkrootk
``` |
	3. Observe the screen output
Expected Result	There should be no infected files found in the output from the chkrootkit command.
Test Nature	Objective
Evidence	
Findings	

1.3 Verify the system is updated with the latest OS patches

References	[8]
Risk	Software bugs can lead to system instability at a minimum and at worse complete loss of confidentiality, integrity or availability of the information.

Testing Procedure	1.Login to the system as root and enter the following commands at the console:
	
	`# emerge sync`
	This command synchronizes the portage tree, this tree contains the ebuild script that install the latest versions of any application installed in the system. This will ensure that the output of the following command lists the current versions of any applications that have been released; the patches.
	
	`# emerge -p world`
	This command performs a pretended (-p) world (all installed software) update.

Expected Result	There should be no output from the command. The system should be up to date.
Test Nature	Objective
Evidence	
Findings	

System Startup

2

2.1 Verify existence of BIOS boot password

References	[9] [7]
Risk	If the BIOS password is not set unauthorized use of the device is possible.
Testing Procedure	Turn on the Laptop and look at the screen for a password prompt.
Expected Result	There should be a password prompt before the boot loader appears.
Test Nature	Objective
Evidence	
Findings	

2.2 Verify existence of BIOS setup password

References	[9]
Risk	If the BIOS setup password is not set an unauthorized user may change the boot sequence to boot the system from alternate media resulting in both unauthorized and unauthenticated access to the Hard Drive

Testing Procedure	Turn on the laptop and press "F2" or "DEL" or the key that allows access to the BIOS setup menu. Look at the screen for a prompt to enter an access password
Expected Result	There should be a password prompt before the BIOS setup menu appears.
Test Nature	Objective
Evidence	
Findings	

2.3 Verify existence of a boot loader password

References	[8] [7]
Risk	If the boot loader does not prompt for a password, it may be modified to allow the system to be started in single user mode, which may grant the user a root shell to access the system.
Testing Procedure	1.Turn on the laptop and wait for the boot loader screen to appear 2. At the boot loader screen press the letter e 3. If nothing happens, then press the letter p, does a password prompt appear?

Expected Result	The boot loader subsystem should be protected by a password. There should be no reaction from the system when the letter "e" is pressed. A password prompt should be the reaction when the letter "p" is pressed.
Test Nature	Objective
Evidence	
Findings	

2.4 Verify that the system prompts for root password while in single user mode

References	[8] [10]
Risk	If the system is started in single user mode by an unauthorized user and no root password is required, the result would be a total system compromise.

Testing Procedure	1. Turn on the laptop and wait for the boot loader screen to appear
	2. When the boot loader screen appears, at the line that tells which kernel to load press the key "e" on the keyboard. This will enter the edit menu for the boot loader entry.
	3. Find the line that starts with "kernel..." and modify it so it looks like the following, making sure to use the correct kernel name:
	``` kernel /kernel-2.6.7-gentoo-r11 single ```
	4. After altering the kernel line press the "Enter" key to leave the edit mode.
	5. After leaving edit mode press the letter "b" to boot the system using the updated kernel line.
	6. After the system is up, observe if a password is prompted or if the system loads into an open root console.
Expected Result	The system should prompt for the root password in order to allow access to the system console.
Test Nature	Objective
Evidence	
Findings	

2.5 Verify the system is not configured for auto login upon startup

References	[9] Personal Experience: Since other operating systems are allowing the possibility of auto login upon start up, it is only normal to expect that some Linux users will try to change the security of their systems to allow this convenience feature.

Risk	If the laptop is configured to auto login upon startup, unauthorized access to the user's session may result.
Testing Procedure	Turn on the laptop and wait for it to start up. Look at the screen for a password prompt for user access when the system has finished loading.
Expected Result	There should be a password prompt before any user logs into the system.
Test Nature	Objective
Evidence	
Findings	

2.6 Verify the system does not load a graphical user interface automatically

References	[11] [8]
Risk	If a GUI loads automatically, a security concern exists because the GUI may be running as a service with root privileges. The GUI may provide server ports that may allow attack. The GUI may allow any unauthorized user to shutdown or restart the system resulting in a denial of service
Testing Procedure	Turn on the laptop and wait for the system to load. Look for a password prompt in the text console.

Expected Result	A graphical user interface should not load automatically before the user authenticates.
Test Nature	Objective
Evidence	
Findings	

File System Access

3

3.1 Verify the user's HOME directory only has access permissions for its owner

References	[8] [12]
Risk	There may be a loss of confidentiality and integrity if the system allows other users to access other user's home directories.

Testing Procedure	1. Turn on the system and login as root, from the shell prompt execute the following commands: ``` # ls -l /home # ls -l /home/$user # exit ``` 2. Login as an unprivileged user, other user than $user From the shell prompt execute the following commands: ``` # cd /home/$user # ls -l /home/$user ``` Then look at the output of the commands Note: Replace $user with the user name of an existent user
Expected Result	The system should not allow other users access to any other user's data. The permissions for the user directory an the data therein should be 700 or -rwx------ as viewed in the output of the commands
Test Nature	Both subjective and objective
Evidence	
Findings	

3.2 Verify the system does not contain world writable files

References	[8] [7] [11]
Risk	Incorrect permissions on configuration files may result in a security breach since any user may modify the files.

Testing Procedure	1. Login as root and execute the following commands:

```
# cd /tmp
# /usr/bin/find / -type f \( -perm -2 -o -perm -20 \
  \) -exec ls -lg {} \; 2>/dev/null >writablef.txt

# /usr/bin/find / -type d \( -perm -2 -o -perm -20 \
  \) -exec ls -ldg {} \; 2>/dev/null >>writabled.txt
```

2. Then look at the output files.

3. Clean up

```
# rm /tmp/writable*
```

Expected Result	The system should not contain world writable files
Test Nature	Objective
Evidence	
Findings	

3.3 Verify the system contains only the required SUID and SGID files

References	[11] [8] [7] [12]
Risk	SUID and SGID files execute in the security context of the owner or owner group of the file and not the user executing it. If a SUID file contained a flaw this could lead to a system compromise.

Testing Procedure	1. Login as root and execute the following commands: ```# /usr/bin/find / -type f \(-perm -004000 -o -perm \ -002000 \) -exec ls -lg {} \; 2>/dev/null``` 2. Then compare the output of the screen to the list provided in the "Expected Result" section below.
Expected Result	The system should contain the SUID and SGID files listed below and any other files deemed required: ```/bin/su /bin/ping /bin/mount /bin/umount /var/qmail/bin/qmail-queue /usr/bin/chfn /usr/bin/chsh /usr/bin/crontab /usr/bin/chage /usr/bin/expiry /usr/bin/sperl5.6.1 /usr/bin/newgrp /usr/bin/passwd /usr/bin/gpasswd /usr/bin/procmail /usr/bin/suidperl /usr/lib/misc/pt_chown /usr/sbin/unix_chkpwd /usr/sbin/traceroute /usr/sbin/pwdb_chkpwd```
Test Nature	Objective
Evidence	
Findings	

3.4 Verify the use of strong passwords for user authentication

References	[12] [2]
Risk	Weak passwords may allow unauthorized access to users data or possibility the whole system resulting in loss of confidentiality, integrity or availability

Testing Procedure	1. Login to the system as root
	
	2. Install johntheripper by executing this command:
	
	`# emerge johntheripper`
	
	3. Copy the /etc/shadow to a temporary directory
	
	`# cd /tmp`
	`# cp /etc/shadow .`
	
	4. Execute the following commands, allow the command to execute for 30 minutes
	
	`# john shadow`
	
	5. Look at the resultant john.pot file to determine if there are any weak passwords
	
	6. Clean up the system:
	
	`# emerge –unmerge johntheripper`
	`# rm /tmp/john* /tmp/shadow`

Expected Result	There should be no weak passwords in the system
Test Nature	Objective
Evidence	

Findings	

3.5 Verify the $PATH for user root does not contain "."

References	[8] [11] [7]

Risk	Including the current directory "." allows for the potential exposure of running malware as root resulting on loss of confidentiality, integrity or availability.

Testing Procedure	1. Login to the system as root and execute the following command `# echo $PATH` 2. Look at the screen output

Expected Result	There should be no "." at the end of the output

Test Nature	Objective

Evidence	

Findings	

3.6 Verify no UID 0 account exist other than root

References	[8]
Risk	UID 0 accounts are superuser equivalent, exposure to loss of confidentiality, integrity or availability results from a system with more than one UID 0 account by increasing the risk of unauthorized access to a superuser account.
Testing Procedure	1. Login to the system as root and execute the following command `# awk -F: '($3 == 0) {print $1}' /etc/passwd` 2. Look for any output other that the word "root"
Expected Result	There should only be one UID 0 account, root.
Test Nature	Objective
Evidence	
Findings	

Network Access

4

4.1 Verify the system is protected by a host firewall

References	[11] [7]
Risk	Unprotected by a host firewall the system is vulnerable to remote network attacks from the untrusted networks that the machine connects to on a regular basis.

Testing Procedure	1. Question the user for the existence of a firewall
	
	2. Login to the system as root and determine if the kernel supports Netfilter
	
	`# ls /proc/net`
	
	3. If files named ip_tables* are found then determine if a user level firewall tool is installed
	
	`# mkdir /tmp/fw`
	`#  for file in $(ls /usr/portage/net-firewall/) \`
	`    do emerge -s $file |grep installed: \`
	`    /tmp/fw/$file \ done;`
	
	4. Look for any installed applications in the contents of the output files
	
	`#  egrep -i "" `find /tmp/fw -type f -print``
	
	5. Ensure the firewall runs automatically when the system starts up (replace $fwall with the name of the firewall application determined earlier)
	
	`# rc-update -s |grep $fwall`
	
	6. Clean up
	
	`# rm -R /tmp/fw`

Expected Result	There should be a firewall running in the system
Test Nature	Both subjective and objective

Evidence	
Findings	

4.2 Verify the system has no server ports listening

References	[11] [8] [7]
Risk	The existence of listening ports on a system facilitate unauthorized access from the network and open the possibility for a denial of service.
Testing Procedure	1. Make sure the user whom the laptop is assigned is logged into the system running all the applications he/she normally runs.

2. Login as root to a different console in the same system and execute the following command:

```
# netstat -nl |grep :
```

3. Login as root to a different system and execute the following commands

```
# cd /tmp
# nmap -sS -P0 -O -p 1-65535 -oN tports  $ip

# nmap -sU -P0 -O -p 1-65535 -oN uports  $ip
```

Note: Replace $ip with the IP address of the system being audited

4. Look at the output of the commands.

5. Delete the resulting files

```
# rm /tmp/*ports
```

Expected Result	There should not be any open ports. *It is important that the normal user of the system is logged in and all regular applications be open so that the tests performed reflect a real life scenario to the extent possible.
Test Nature	Both subjective and objective
Evidence	
Findings	

3 Conduct the Audit Testing, Evidence and Findings

1.2 Verify the system does not contain a root kit

References	Personal Experience: It is always a good idea to establish the trustworthiness of the tools in the system to be audited.
Risk	Complete loss of the system. All subsequent tests in this audit program will be flawed.
Testing Procedure	1. Start the system using a bootable CDROM with security tools such as Knoppix-STD
	2. Mount the audited system's root partition and perform the following command
	``` # mount -t auto -o ro /dev/hda4 /mnt/hda4 # chkrootkit -r /mnt/hda4 > chrootk ```
	3. Observe the screen output
Expected Result	There should be no infected files found in the output from the chkrootkit command.
Test Nature	Objective
Evidence	

Results of the command chkrootkit -r /mnt/hda4 > chrootk

```
ROOTDIR is `/mnt/hda4/'
Checking `amd'... not found
Checking `basename'... not infected
Checking `biff'... not found
Checking `chfn'... not infected
```

```
Checking `chsh'... not infected
Checking `cron'... not infected
Checking `date'... not infected
Checking `du'... not infected
Checking `dirname'... not infected
Checking `echo'... not infected
Checking `egrep'... not infected
Checking `env'... not infected
Checking `find'... not infected
Checking `fingerd'... not found
Checking `gpm'... not infected
Checking `grep'... not infected
Checking `hdparm'... not infected
Checking `su'... not infected
Checking `ifconfig'... not infected
Checking `inetd'... not tested
Checking `inetdconf'... not found
Checking `identd'... not found
Checking `init'... not infected
Checking `killall'... not infected
Checking `ldsopreload'... not infected
Checking `login'... not infected
Checking `ls'... not infected
Checking `lsof'... not found
Checking `mail'... not found
Checking `mingetty'... not found
Checking `netstat'... not infected
Checking `named'... not found
Checking `passwd'... not infected
Checking `pidof'... not infected
Checking `pop2'... not found
Checking `pop3'... not found
Checking `ps'... not infected
Checking `pstree'... not infected
Checking `rpcinfo'... not infected
Checking `rlogind'... not infected
Checking `rshd'... not infected
Checking `slogin'... not infected
Checking `sendmail'... not infected
Checking `sshd'... not infected
Checking `syslogd'... not tested
Checking `tar'... not infected
Checking `tcpd'... not infected
Checking `tcpdump'... not infected
Checking `top'... not infected
Checking `telnetd'... not infected
Checking `timed'... not found
Checking `traceroute'... not found
Checking `vdir'... not infected
Checking `w'... not infected
Checking `write'... not infected
Checking `aliens'... no suspect files
Searching for sniffer's logs, it may take a while... nothing found
Searching for HiDrootkit's default dir... nothing found
Searching for t0rn's default files and dirs... nothing found
Searching for t0rn's v8 defaults... nothing found
Searching for Lion Worm default files and dirs... nothing found
```

Searching for RSHA's default files and dir... nothing found
Searching for RH-Sharpe's default files... nothing found
Searching for Ambient's rootkit (ark) default files and dirs... nothing found
Searching for suspicious files and dirs, it may take a while...
/usr/lib/.keep /usr/lib/perl5/vendor_perl/5.8.2/i686-
linux/auto/XML/Parser/.packlist /usr/lib/perl5/vendor_perl/5.8.2/i686-
linux/auto/XML/Writer/.packlist /usr/lib/perl5/vendor_perl/5.8.2/i686-
linux/auto/Net/SSLeay/.packlist /usr/lib/perl5/vendor_perl/5.8.2/i686-
linux/auto/Text/Balanced/.packlist /
usr/lib/perl5/vendor_perl/5.8.2/i686-
linux/auto/Parse/RecDescent/.packlist /
usr/lib/perl5/vendor_perl/5.8.2/i686-
linux/auto/Gtk/Gdk/ImlibImage/.packlist /
usr/lib/perl5/vendor_perl/5.8.2/i686-
linux/auto/Gtk/Gdk/Pixbuf/.packlist /
usr/lib/perl5/vendor_perl/5.8.2/i686-linux/auto/Gtk/base/.packlist /
usr/lib/perl5/vendor_perl/5.8.2/i686-linux/auto/Gtk/XmHTML/.packlist /
usr/lib/perl5/vendor_perl/5.8.2/i686-linux/auto/Gnome/.packlist /
usr/lib/perl5/vendor_perl/5.8.2/i686-linux/auto/File/Spec/.packlist /
usr/lib/perl5/vendor_perl/5.8.2/i686-linux/auto/Digest/.packlist /
usr/lib/perl5/vendor_perl/5.8.2/i686-linux/auto/Digest/MD5/.packlist /
usr/lib/perl5/vendor_perl/5.8.2/i686-
linux/auto/Test/Harness/.packlist /
usr/lib/perl5/vendor_perl/5.8.2/i686-linux/auto/Inline/.packlist /
usr/lib/perl5/vendor_perl/5.8.2/i686-linux/auto/Filter/.packlist /
usr/lib/perl5/vendor_perl/5.8.2/i686-
linux/auto/ExtUtils/F77/.packlist /
usr/lib/perl5/vendor_perl/5.8.2/i686-linux/auto/PDL/.packlist /
usr/lib/perl5/vendor_perl/5.8.3/i686-linux/auto/Foomatic/.packlist /
usr/lib/perl5/vendor_perl/5.8.3/i686-
linux/auto/Convert/ASN1/.packlist /
usr/lib/perl5/vendor_perl/5.8.3/i686-linux/auto/MIME/Base64/.packlist /
usr/lib/perl5/vendor_perl/5.8.3/i686-linux/auto/URI/.packlist /
usr/lib/perl5/vendor_perl/5.8.3/i686-linux/auto/IO/Socket/SSL/.packlist
/usr/lib/perl5/vendor_perl/5.8.3/i686-linux/auto/perl-ldap/.packlist /
usr/lib/perl5/vendor_perl/5.8.4/i686-linux/auto/Gaim/.packlist /
usr/lib/perl5/vendor_perl/5.8.4/i686-linux/auto/Net/Daemon/.packlist /
usr/lib/perl5/vendor_perl/5.8.4/i686-linux/auto/Storable/.packlist /
usr/lib/perl5/vendor_perl/5.8.4/i686-
linux/auto/RPC/PlServer/.packlist /
usr/lib/perl5/vendor_perl/5.8.4/i686-linux/auto/DBI/.packlist /
usr/lib/perl5/vendor_perl/5.8.4/i686-linux/auto/DBD/mysql/.packlist /
usr/lib/perl5/vendor_perl/5.8.4/i686-
linux/auto/String/ShellQuote/.packlist /
usr/lib/perl5/vendor_perl/5.8.4/i686-linux/auto/MP3/Info/.packlist /
usr/lib/perl5/5.8.4/i686-linux/.packlist /
usr/lib/locale/ru_RU/LC_MESSAGES/.keep /usr/lib/distcc/bin/.keep /
usr/lib/nsbrowser/plugins/.keep /
usr/lib/mozilla/include/ipc/.headerlist /
usr/lib/mozilla/include/enigmime/.headerlist /
usr/lib/nessus/plugins/.desc /lib/.keep /lib/dev-state/.keep /lib/udev-
state/.keep
/usr/lib/nessus/plugins/.desc
Searching for LPD Worm files and dirs... nothing found
Searching for Ramen Worm files and dirs... nothing found
Searching for Maniac files and dirs... nothing found

```
Searching for RK17 files and dirs... nothing found
Searching for Ducoci rootkit... nothing found
Searching for Adore Worm... nothing found
Searching for ShitC Worm... nothing found
Searching for Omega Worm... nothing found
Searching for Sadmind/IIS Worm... nothing found
Searching for MonKit... nothing found
Searching for Showtee... nothing found
Searching for OpticKit... nothing found
Searching for T.R.K... nothing found
Searching for Mithra... nothing found
Searching for OBSD rk v1... nothing found
Searching for LOC rootkit ... nothing found
Searching for Romanian rootkit ... nothing found
Searching for Suckit rootkit ... nothing found
Searching for Volc rootkit ... nothing found
Searching for Gold2 rootkit ... nothing found
Searching for TC2 Worm default files and dirs... nothing found
Searching for Anonoying rootkit default files and dirs... nothing found
Searching for ZK rootkit default files and dirs... nothing found
Searching for ShKit rootkit default files and dirs... nothing found
Searching for AjaKit rootkit default files and dirs... nothing found
Searching for zaRwT rootkit default files and dirs... nothing found
Searching for anomalies in shell history files... nothing found
Checking `asp'... not infected
Checking `bindshell'... not infected
Checking `lkm'... Checking `rexedcs'... not found
Checking `sniffer'... eth0: not promisc and no PF_PACKET sockets
Checking `w55808'... not infected
Checking `wted'... nothing deleted
Checking `scalper'... not infected
Checking `slapper'... not infected
Checking `z2'... nothing deleted
```

Findings	Pass. No evidence of a root kit was found in the system.

1.3 Verify the system is updated with the latest OS patches	
References	[8]
Risk	Software bugs can lead to system instability at a minimum and at worse complete loss of confidentiality, integrity or availability of the information.

Testing Procedure	1.Login to the system as root and enter the following commands at the console:
	
	`# emerge sync`
	
	This command synchronizes the portage tree, this tree contains the ebuild script that install the latest versions of any application installed in the system. This will ensure that the output of the following command lists the current versions of any applications that have been released; the patches.
	
	`# emerge -p world`
	
	This command performs a pretended (-p) world (all installed software) update.

Expected Result	There should be no output from the command. The system should be up to date.
Test Nature	Objective
Evidence	

Findings	Pass. Although there are new versions of installed applications, there are no security risks involved with this system when compared to the Gentoo Linux Security Advisories page at: http://www.gentoo.org/security/en/glsa/index.xml

System Startup

2

2.1 Verify existence of BIOS boot password

References	[9] [7]
Risk	If the BIOS password is not set unauthorized use of the device is possible.
Testing Procedure	Turn on the Laptop and look at the screen for a password prompt.
Expected Result	There should be a password prompt before the boot loader appears.
Test Nature	Objective
Evidence	No BIOS boot password is required to boot the system. The picture shows that it is disabled

	Findings	Fail. No password was required from the BIOS to load the system.

2.2 Verify existence of BIOS setup password

References	[9]	
Risk	If the BIOS setup password is not set an unauthorized user may change the boot sequence to boot the system from alternate media resulting in both unauthorized and unauthenticated access to the Hard Drive	
Testing Procedure	Turn on the laptop and press "F2" or "DEL" or the key that allows access to the BIOS setup menu. Look at the screen for a prompt to enter an access password	
Expected Result	There should be a password prompt before the BIOS setup menu appears.	
Test Nature	Objective	
Evidence	There was not password prompted when F2 was pressed to enter the BIOS setup menu.	

Findings	Fail. The BIOS setup menu should be configured with a password to prevent unauthorized access.

2.3 Verify existence of a boot loader password

References	[8] [7]
Risk	If the boot loader does not prompt for a password, it may be modified to allow the system to be started in single user mode, which may grant the user a root shell to access the system.
Testing Procedure	1.Turn on the laptop and wait for the boot loader screen to appear
	2. At the boot loader screen press the letter e
	3. If nothing happens, then press the letter p, does a password prompt appear?

Expected Result	The boot loader subsystem should be protected by a password. There should be no reaction from the system when the letter "e" is pressed. A password prompt should be the reaction when the letter "p" is pressed.
Test Nature	Objective
Evidence	A message appeared on the screen prompting for a password to access advanced options otherwise to select the kernel to load. Pressing the letter "e" had no effect, pressing the letter "p" caused a password prompt to appear.

Findings	Pass. The boot loader is protected against unauthorized access to its advanced features

2.4 Verify that the system prompts for root password while in single user mode

References	[8] [10]
Risk	If the system is started in single user mode by an unauthorized user and no root password is required, the result would be a total system compromise.
Testing Procedure	1. Turn on the laptop and wait for the boot loader screen to appear
	2. When the boot loader screen appears, at the line that tells which kernel to load press the key "e" on the keyboard. This will enter the edit menu for the boot loader entry.
	3. Find the line that starts with "kernel..." and modify it so it looks like the following, making sure to use the correct kernel name:
	``` kernel /kernel-2.6.7-gentoo-r11 single ```
	4. After altering the kernel line press the "Enter" key to leave the edit mode.
	5. After leaving edit mode press the letter "b" to boot the system using the updated kernel line.
	6. After the system is up, observe if a password is prompted for or if the system loads into an open root console.
Expected Result	The system should prompt for the root password in order to allow access to the system console.
Test Nature	Objective

Evidence	The system does not prompt for a password when loaded in single user mode


```
● Remounting root filesystem read/write.
● Setting hostname to nikky...
● Calculating module dependencies...
● Checking all filesystems...
/dev/hda1: clean, 47/10048 files, 5773/10
● Mounting local filesystems...
● Mounting USB device filesystem (usbfs
● Activating (possibly) more swap...
● Caching service dependencies...
sh-2.05b#
```

Findings	Fail. The system is completely vulnerable to unauthorized access should an intruder load single user mode.

2.5 Verify the system is not configured for auto login upon startup

References	[9] Personal Experience: Since other operating systems are allowing the possibility of auto login upon start up, it is only normal to expect that some Linux users will try to change the security of their systems to allow this convenience feature.
Risk	If the laptop is configured to auto login upon startup, unauthorized access to the user's session may result.
Testing Procedure	Turn on the laptop and wait for it to start up. Look at the screen for a password prompt for user access when the system has finished loading.
Expected Result	There should be a password prompt before any user logs into the system.
Test Nature	Objective
Evidence	The system loads to a text mode user login prompt.

Findings	Pass. The system is not configured for auto login upon start up

2.6 Verify the system does not load a graphical user interface automatically

References	[11] [8]
Risk	If a GUI loads automatically, a security concern exists because the GUI may be running as a service with root privileges. The GUI may provide server ports that may allow attack. The GUI may allow any unauthorized user to shutdown or restart the system resulting in a denial of service
Testing Procedure	Turn on the laptop and wait for the system to load. Look for a password prompt in the text console.
Expected Result	A graphical user interface should not load automatically before the user authenticates.
Test Nature	Objective
Evidence	
Findings	

File System Access

3

3.1 Verify the user's HOME directory only has access permissions for its owner

References	[8] [12]
Risk	There may be a loss of confidentiality and integrity if the system allows other users to access other user's home directories.
Testing Procedure	1. Turn on the system and login as root, from the shell prompt execute the following commands: ``` # ls -l /home # ls -l /home/$user # exit ``` 2. Login as an unprivileged user, other user than $user From the shell prompt execute the following commands: ``` # cd /home/$user # ls -l /home/$user ``` Then look at the output of the commands Note: Replace $user with the user name of an existent user
Expected Result	The system should not allow other users access to any other user's data. The permissions for the user directory an the data therein should be 700 or -rwx------ as viewed in the output of the commands
Test Nature	Both subjective and objective
Evidence	

1.

2.

Findings	Fail. The permissions are incorrect for some home directories and their contents.

3.2 Verify the system does not contain world writable files

References	[8] [7] [11]
Risk	Incorrect permissions on configuration files may result in a security breach since any user may modify the files.

Testing Procedure	1. Login as root and execute the following commands:
	
	`# cd /tmp`
	`# /usr/bin/find / -type f \( -perm -2 -o -perm -20 \`
	`  \) -exec ls -lg {} \; 2>/dev/null >writablef.txt`
	
	`# /usr/bin/find / -type d \( -perm -2 -o -perm -20 \`
	`  \) -exec ls -ldg {} \; 2>/dev/null >>writabled.txt`
	
	2. Then look at the output files.
	
	3. Clean up
	
	`# rm /tmp/writable*`

Expected Result	The system should not contain world writable files
Test Nature	Objective
Evidence	

1.--excerpts from the resulting writabled.txt file:

```
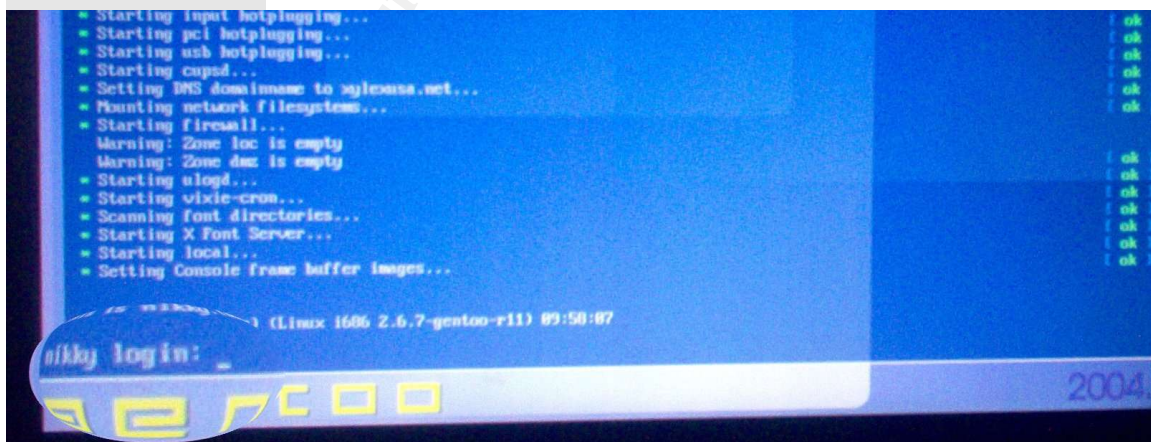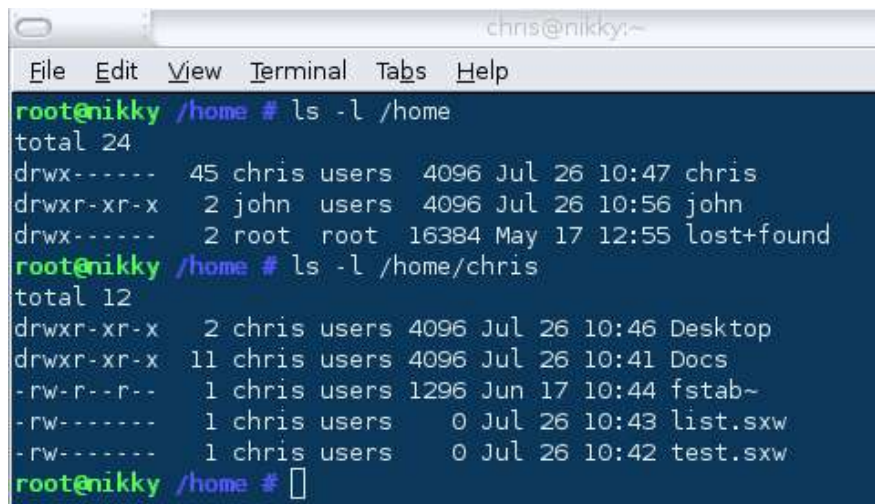...
-rw-rw-r--  1 games 0 Jul 15 14:43 /var/lib/games/gnotski.7.scores
-rw-rw-r--  1 games 0 Jul 15 14:43 /var/lib/games/gnibbles.3.0.scores
-rw-rw-r--  1 games 0 Jul 15 14:43 /var/lib/games/gnotski.2.scores
-rw-rw-r--  1 games 0 Jul 15 14:43 /var/lib/games/gnomine.Large.scores
-rw-rw-r--  1 games 0 Jul 15 14:43 /var/lib/games/glines.scores
...
-rw-rw-r--  1 portage 0 Mar  8 03:56 /var/tmp/portage/ucl-1.01-
r1/temp/successful
-rw-rw-r--  1 portage 0 Mar  8 03:45 /var/tmp/portage/freetype-
2.1.5/temp/successful
-rw-rw-r--  1 portage 0 Mar  8 03:46 /var/tmp/portage/jpeg-6b-
```

```
r3/temp/successful
...
-rw-rw-r--  1 portage 610 Jun 27 21:07 /var/cache/edb/dep/app-
admin/gnome-system-tools-0.33.0
-rw-rw-r--  1 portage 656 Jul  1 08:09 /var/cache/edb/dep/app-
admin/gnome-system-tools-0.34.0
-rw-rw-r--  1 portage 695 Jul 11 15:33 /var/cache/edb/dep/app-
admin/gnome-system-tools-0.34.0-r1
...
-rw-rw-r--  1 root 256 Jul 16 19:09 /usr/portage/metadata/cache/x11-
plugins/wmbattery-2.19-r1
-rw-rw-r--  1 root 366 Jul 18 08:09 /usr/portage/metadata/cache/x11-
plugins/wmblob-1.0.1
-rw-rw-r--  1 root 263 Jul 21 20:11 /usr/portage/metadata/cache/x11-
plugins/wmbutton-0.5
...
-rw-rw-rw-  1 users 84480 Jan 16  2004 /
home/chris/Docs/Mar2004/Docs/Firewall Installation Survey.doc
-rw-rw-rw-  1 users 23040 Jan 12  2004 /
home/chris/Docs/Mar2004/Docs/Foundstone hacking windows.doc
-rw-rw-rw-  1 users 82944 Jan 19  2004 /
home/chris/Docs/Mar2004/Docs/GIAC Prep's Intro to Information
Security.doc
...
```

2. --excerpts from the resulting writabled.txt file:

```
...
drwxrwxrwt  2 root 40 Jul 26 04:50 /dev/shm
drwxrwxr-x  5 lp 4096 Jul 24 16:53 /etc/cups
d-wxrwS--t  2 root 4096 Jun 11 09:33 /etc/distcc
drwxrwxrwt  43 root 8192 Jul 26 11:26 /tmp
drwxrwxrwt  2 root 4096 Jul 26 08:54 /tmp/.ICE-unix
drwxrwxrwt  2 root 4096 Jul 26 08:54 /tmp/.X11-unix
drwxrwxrwt  2 xfs 4096 Jul 26 08:51 /tmp/.font-unix
drwxrwxrwt  2 users 4096 Jul 26 08:54 /tmp/.esd
drwxrwx--T  2 gdm 4096 May  2 15:38 /var/lib/gdm
drwxrwxrwt  3 root 4096 May  6 20:22 /var/run/vmware
drwxrwxrwt  6 root 4096 Jul 26 08:55 /var/tmp
...
drwsrws---  2 portage 4096 Mar 28 10:39 /var/tmp/portage/xmms-1.2.8-
r4/temp
drwsrws---  2 portage 4096 Mar 12 08:35 /var/tmp/portage/acpid-1.0.2-
r2/temp
drwsrws---  2 portage 4096 Mar 12 09:42 /var/tmp/portage/xinetd-
2.3.12/temp
...
drwxrwsr-x  2 portage 4096 Jul 23 08:47 /var/cache/edb/dep/app-
accessibility
drwxrwsr-x  2 portage 8192 Jul 23 08:47 /var/cache/edb/dep/app-admin
drwxrwsr-x  2 portage 4096 Jul 23 08:47 /var/cache/edb/dep/app-antivirus
drwxrwsr-x  2 portage 4096 Jul 23 08:47 /var/cache/edb/dep/app-arch
drwxrwsr-x  2 portage 4096 Jul 23 08:47 /var/cache/edb/dep/app-
benchmarks
drwxrwsr-x  2 portage 4096 Jul 23 08:47 /var/cache/edb/dep/app-cdr
...
```

```
drwxrwxr-x  3 root 4096 Jul 23 09:42 /usr/share/doc/samba-
3.0.5/examples/LDAP
drwxrwxr-x  4 root 4096 Jul 23 09:42 /usr/share/doc/samba-
3.0.5/examples/LDAP/smbldap-tools
drwxrwxr-x  2 root 4096 Jul 23 09:42 /usr/share/doc/samba-
3.0.5/examples/LDAP/smbldap-tools/mkntpwd
...
drwxrwxr-x  2 root 12288 Jul 23 07:54 /usr/portage/metadata/cache/sys-
kernel
drwxrwxr-x  2 root 4096 Jul 23 07:40 /usr/portage/metadata/cache/dev-ada
drwxrwxr-x  2 root 4096 Jul 23 07:40 /usr/portage/metadata/cache/dev-cpp
...
drwxr-xrwx  3 root 4096 May 17 12:56 /apps
drwxr-xrwx  3 root 4096 May 17 12:57 /apps/vmware
drwxr-xrwx  4 root 4096 May 17 13:25 /apps/vmware/vmware
drwxr-xrwx  3 root 4096 May 17 12:57 /apps/vmware/vmware/Machines
...
```

Findings	Fail. There we countless files and directories that had permissions set to world readable and writable.

3.3 Verify the system contains only the required SUID and SGID files

References	[11] [8] [7] [12]
Risk	SUID and SGID files execute in the security context of the owner or owner group of the file and not the user executing it. If a SUID file contained a flaw this could lead to a system compromise.

Testing Procedure	1. Login as root and execute the following commands:
	
	`# /usr/bin/find / -type f \( -perm -004000 -o -perm \`
	` -002000 \) -exec ls -lg {} \; 2>/dev/null`
	
	2. Then compare the output of the screen to the list provided in the "Expected Result" section below.

Expected Result	The system should contain the SUID and SGID files listed below and any other files deemed required:
	
	`/bin/su`
	`/bin/ping`
	`/bin/mount`
	`/bin/umount`
	`/var/qmail/bin/qmail-queue`
	`/usr/bin/chfn`
	`/usr/bin/chsh`
	`/usr/bin/crontab`
	`/usr/bin/chage`
	`/usr/bin/expiry`
	`/usr/bin/sperl5.6.1`
	`/usr/bin/newgrp`
	`/usr/bin/passwd`
	`/usr/bin/gpasswd`
	`/usr/bin/procmail`
	`/usr/bin/suidperl`
	`/usr/lib/misc/pt_chown`
	`/usr/sbin/unix_chkpwd`
	`/usr/sbin/traceroute`
	`/usr/sbin/pwdb_chkpwd`

Test Nature	Objective

Evidence

```
root@nikky /tmp # /usr/bin/find / -type f \( -perm -004000 -o -perm
-002000 \) -exec ls -lg {} \; 2>/dev/null
-rwsr-xr-x  1 root 21604 Jul  7 08:56 /bin/su
-rws--x--x  1 root 29784 Apr 26 16:29 /bin/ping
-rws--x--x  1 root 71912 Feb 19 10:29 /bin/mount
-rws--x--x  1 root 33068 Feb 19 10:29 /bin/umount
-r-sr-xr-x  1 root 4547 Jul 15 11:01 /opt/vmware/bin/vmware
-r-sr-xr-x  1 root 9540 Jul 15 11:01 /opt/vmware/bin/vmware-ping
-r-sr-xr-x  1 root 3302540 Jul 15 11:01 /opt/vmware/lib/bin/vmware-vmx
-r-xr-sr-x  1 man 40552 May 10 16:37 /usr/bin/man
-rwsr-xr-x  1 root 29528 Jul  7 08:56 /usr/bin/chfn
-rwsr-xr-x  1 root 25508 Jul  7 08:56 /usr/bin/chsh
-rwsr-xr-x  1 root 35532 Jul  7 08:56 /usr/bin/chage
-rwxr-sr-x  1 tty 8664 Feb 19 10:29 /usr/bin/write
-rwxr-sr-x  1 slocate 26892 Feb 19 10:25 /usr/bin/slocate
-rwsr-xr-x  1 root 17132 Jul  7 08:56 /usr/bin/expiry
-rwsr-xr-x  1 root 21228 Jul  7 08:56 /usr/bin/newgrp
-rwsr-xr-x  1 root 26380 Jul  7 08:56 /usr/bin/passwd
-rwsr-xr-x  1 root 34416 Jul  7 08:56 /usr/bin/gpasswd
-rws--x--x  1 root 7912 Apr 26 16:29 /usr/bin/tracepath
-rwsr-x---  1 cron 20884 Mar 28 11:14 /usr/bin/crontab
-rwsr-xr-x  1 lp 8828 Jul  7 14:05 /usr/bin/lppasswd
-rwsr-xr-x  1 root 673636 Mar  9 23:09 /usr/bin/gpg
-r-xr-sr-x  1 games 65568 Jul 15 14:43 /usr/bin/gnometris
-r-xr-sr-x  1 games 122828 Jul 15 14:43 /usr/bin/gtali
-r-xr-sr-x  1 games 45548 Jul 15 14:43 /usr/bin/gnotravex
-r-xr-sr-x  1 games 70604 Jul 15 14:43 /usr/bin/mahjongg
-r-xr-sr-x  1 games 74948 Jul 15 14:43 /usr/bin/gnome-stones
-r-xr-sr-x  1 games 49428 Jul 15 14:43 /usr/bin/glines
-r-xr-sr-x  1 games 53772 Jul 15 14:43 /usr/bin/gnomine
-r-xr-sr-x  1 games 29672 Jul 15 14:43 /usr/bin/gnotski
-r-xr-sr-x  1 games 60580 Jul 15 14:43 /usr/bin/gnibbles
-r-xr-sr-x  1 games 89240 Jul 15 14:43 /usr/bin/gnobots2
-r-xr-sr-x  1 games 36308 Jul 15 14:43 /usr/bin/same-gnome
-rwsr-xr-x  1 root 227488 Jun 17 15:01 /usr/bin/xscreensaver
---s--x--x  1 root 6184 Jul 23 09:42 /usr/bin/smbumount
-rwsr-xr-x  1 root 41676 Jun 21 16:42 /usr/bin/ksu
---s--x--x  1 root 8336 Jul 23 09:42 /usr/bin/smbmnt
---s--x--x  1 root 14960 Jul 23 09:42 /usr/bin/mount.cifs
-rwsr-xr-x  1 root 5712 Mar 22 18:17 /usr/bin/restorefont
-rwsr-xr-x  1 root 5492 Mar 22 18:17 /usr/bin/restorepalette
-rwsr-xr-x  1 root 3508 Mar 22 18:17 /usr/bin/dumpreg
-rwsr-xr-x  1 root 6084 Mar 22 18:17 /usr/bin/restoretextmode
-rws--x--x  1 root 1013048 May 10 17:07 /usr/bin/sperl5.8.4
---s--x--x  1 root 95716 Jun 15 15:13 /usr/bin/sudo
-rwsr-xr-x  1 root 14932 Jul  2 11:28 /usr/bin/rcp
-rwsr-xr-x  1 root 11412 Jul  2 11:28 /usr/bin/rlogin
-rwsr-xr-x  1 root 8272 Jul  2 11:28 /usr/bin/rsh
-rws--x--x  1 root 135012 Jun  1 14:01 /usr/lib/misc/ssh-keysign
-rws--x--x  1 root 6168 Jul 15 16:17 /usr/lib/misc/pt_chown
-rwsr-xr-x  1 root 10948 Mar 12 17:28 /usr/lib/xcdroast-
0.98/bin/xcdrwrap
```

```
-rwsr-xr-x  1 root 9868 Mar 17 11:49 /usr/sbin/gnome-pty-helper
-rws--x--x  1 root 11119 Jun 21 14:13 /usr/X11R6/bin/Xwrapper
-rwxr-sr-x  1 utmp 304243 Jun 21 14:13 /usr/X11R6/bin/xterm
-rwsr-xr-x  1 root 16784 Mar 28 11:41 /usr/X11R6/bin/xcardinfo
-rwxr-sr-x  1 utmp 10604 Jul 15 14:14 /usr/libexec/gnome-pty-helper
-rwxr-sr-x  1 mail 10728 Mar 28 09:29 /
usr/libexec/evolution/1.4/camel/camel-lock-helper
-rwsr-xr-x  1 root 5612 Jun 30 14:41 /usr/kde/3.2/bin/kgrantpty
-rwsr-xr-x  1 root 6156 Jun 30 14:41 /usr/kde/3.2/bin/kpac_dhcp_helper
-r-sr-xr-x  1 root 16340 Apr  7 10:03 /sbin/unix_chkpwd
-r-s--x--x  1 root 6684 Apr  7 10:03 /sbin/pam_timestamp_check
-rwsr-xr-x  1 root 14512 Mar 28 11:41 /sbin/cardctl
-r-sr-xr-x  1 root 119916 Apr  7 10:03 /sbin/pwdb_chkpwd
```

Findings	Fail. The system contains many more SUID files than the accepted list.

3.4 Verify the use of strong passwords for user authentication

References	[12] [2]
Risk	Weak passwords may allow unauthorized access to users data or possibility the whole system resulting in loss of confidentiality, integrity or availability

Testing Procedure	1. Login to the system as root
	
	2. Copy the /etc/shadow to a temporary directory on a machine with john the ripper installed
	
	```# cd /tmp```
	```# cp /mnt/floppy/shadow .```
	
	3. Execute the following commands, allow the command to execute for 30 minutes
	
	```# john shadow```
	
	4. Observe the screen output for any weak passwords
	
	5. Clean up the system:
	
	```# rm /tmp/john* /tmp/shadow```

Expected Result	There should be no weak passwords in the system
Test Nature	Objective
Evidence	

4.

Findings	Fail. At least one password was compromised by john in 30 minutes

---

3.5 Verify the $PATH for user root does not contain "."

References	[8] [11] [7]
Risk	Including the current directory "." allows for the potential exposure of running malware as root resulting on loss of confidentiality, integrity or availability.
Testing Procedure	1. Login to the system as root and execute the following command `# echo $PATH` 2. Look at the screen output
Expected Result	There should be no "." at the end of the output
Test Nature	Objective

Evidence	

```
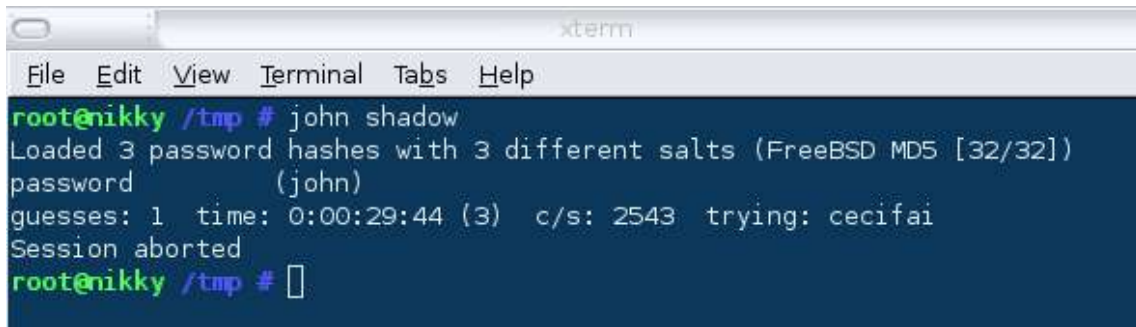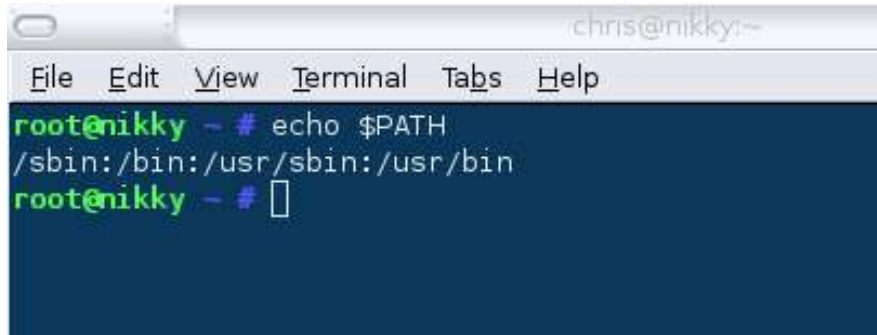root@nikky ~ # echo $PATH
/sbin:/bin:/usr/sbin:/usr/bin
root@nikky ~ # []
```

Findings	Pass. There is no trailing dot in the root path.

3.6 Verify no UID 0 account exist other than root

References	[8]
Risk	UID 0 accounts are superuser equivalent, exposure to loss of confidentiality, integrity or availability results from a system with more than one UID 0 account by increasing the risk of unauthorized access to a superuser account.
Testing Procedure	1. Login to the system as root and execute the following command `# awk -F: '($3 == 0) {print $1}' /etc/passwd` 2. Look for any output other that the word "root"
Expected Result	There should only be one UID 0 account, root.
Test Nature	Objective
Evidence	
Findings	Pass. Only one superuser equivalent account exists in the system.

Network Access

4

4.1 Verify the system is protected by a host firewall

References	[11] [7]
Risk	Unprotected by a host firewall the system is vulnerable to remote network attacks from the untrusted networks that the machine connects to on a regular basis.
Testing Procedure	1. Question the user for the existence of a firewall

2. Login to the system as root and determine if the kernel supports Netfilter

```
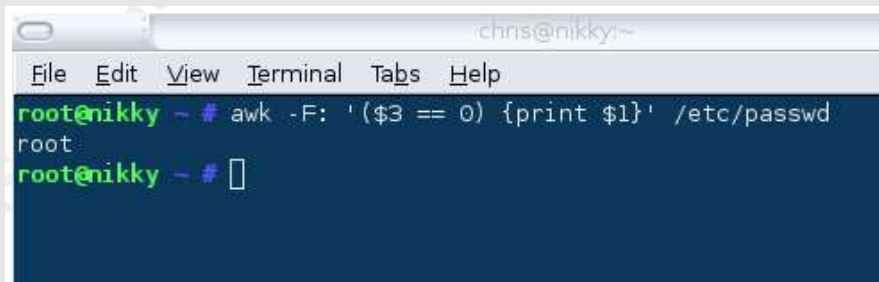# ls /proc/net
```

3. If files named ip_tables* are found then determine if a user level firewall tool is installed

```
# mkdir /tmp/fw
#  for file in $(ls /usr/portage/net-firewall/) \
    do emerge -s $file |grep installed: \
    /tmp/fw/$file \ done;
```

4. Look for any installed applications in the contents of the output files

```
#  egrep -i "" `find /tmp/fw -type f -print`
```

5. Ensure the firewall runs automatically when the system starts up (replace $fwall with the name of the firewall application determined earlier)

```
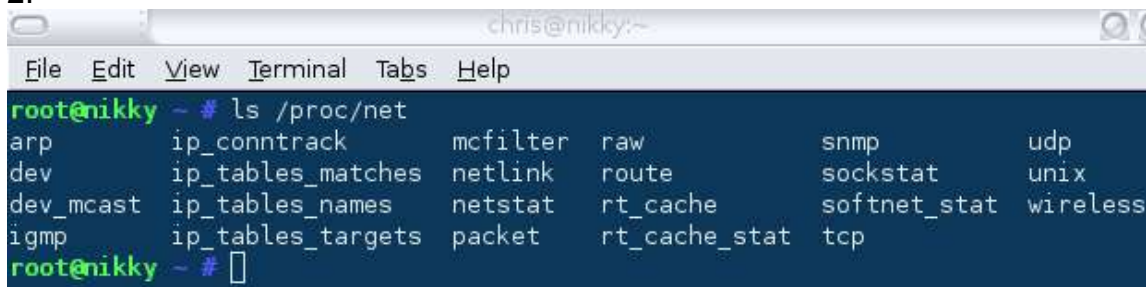# rc-update -s |grep $fwall
```

6. Clean up

```
# rm -R /tmp/fw
```

Expected Result	There should be a firewall running in the system. For #5 the output of the command should state that the firewall service runs in either boot or default runlevel.
Test Nature	Both subjective and objective

Evidence	1. The user is unaware of the existence of a firewall in his machine.

2.


```
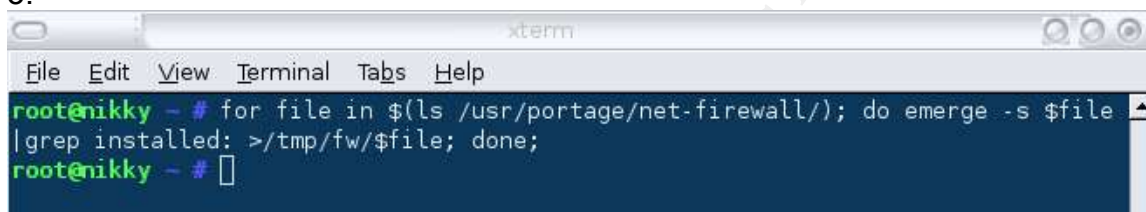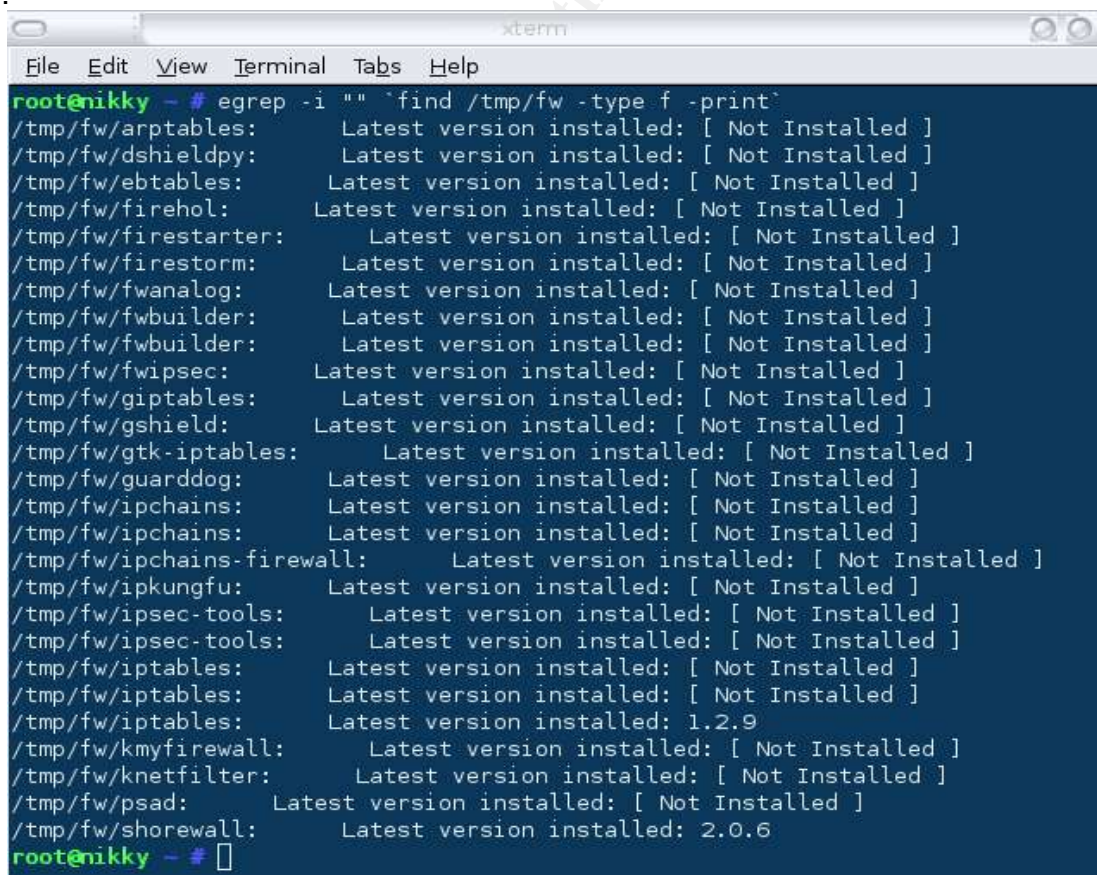root@nikky ~ # ls /proc/net
arp          ip_conntrack        mcfilter    raw              snmp           udp
dev          ip_tables_matches   netlink     route            sockstat       unix
dev_mcast    ip_tables_names     netstat     rt_cache         softnet_stat   wireless
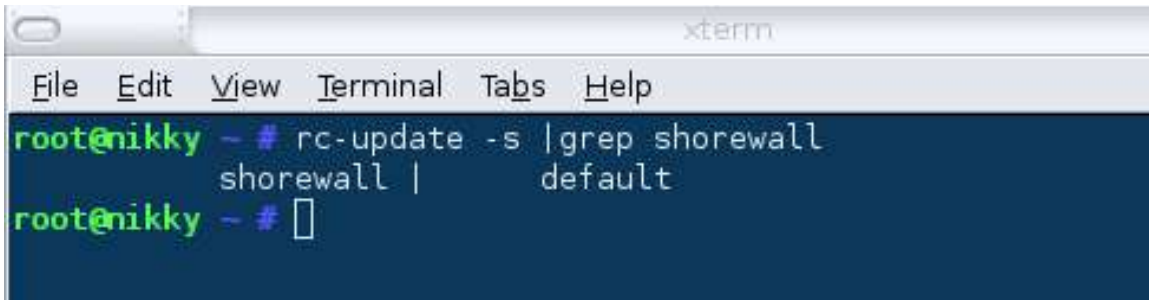igmp         ip_tables_targets   packet      rt_cache_stat    tcp
root@nikky ~ #
```

3.


```
root@nikky ~ # for file in $(ls /usr/portage/net-firewall/); do emerge -s $file
|grep installed: >/tmp/fw/$file; done;
root@nikky ~ #
```

4.


```
root@nikky ~ # egrep -i "" `find /tmp/fw -type f -print`
/tmp/fw/arptables:        Latest version installed: [ Not Installed ]
/tmp/fw/dshieldpy:        Latest version installed: [ Not Installed ]
/tmp/fw/ebtables:         Latest version installed: [ Not Installed ]
/tmp/fw/firehol:        Latest version installed: [ Not Installed ]
/tmp/fw/firestarter:         Latest version installed: [ Not Installed ]
/tmp/fw/firestorm:        Latest version installed: [ Not Installed ]
/tmp/fw/fwanalog:        Latest version installed: [ Not Installed ]
/tmp/fw/fwbuilder:        Latest version installed: [ Not Installed ]
/tmp/fw/fwbuilder:        Latest version installed: [ Not Installed ]
/tmp/fw/fwipsec:        Latest version installed: [ Not Installed ]
/tmp/fw/giptables:        Latest version installed: [ Not Installed ]
/tmp/fw/gshield:        Latest version installed: [ Not Installed ]
/tmp/fw/gtk-iptables:         Latest version installed: [ Not Installed ]
/tmp/fw/guarddog:        Latest version installed: [ Not Installed ]
/tmp/fw/ipchains:        Latest version installed: [ Not Installed ]
/tmp/fw/ipchains:        Latest version installed: [ Not Installed ]
/tmp/fw/ipchains-firewall:         Latest version installed: [ Not Installed ]
/tmp/fw/ipkungfu:        Latest version installed: [ Not Installed ]
/tmp/fw/ipsec-tools:         Latest version installed: [ Not Installed ]
/tmp/fw/ipsec-tools:         Latest version installed: [ Not Installed ]
/tmp/fw/iptables:        Latest version installed: [ Not Installed ]
/tmp/fw/iptables:        Latest version installed: [ Not Installed ]
/tmp/fw/iptables:        Latest version installed: 1.2.9
/tmp/fw/kmyfirewall:         Latest version installed: [ Not Installed ]
/tmp/fw/knetfilter:        Latest version installed: [ Not Installed ]
/tmp/fw/psad:        Latest version installed: [ Not Installed ]
/tmp/fw/shorewall:         Latest version installed: 2.0.6
root@nikky ~ #
```

5.

Findings	Pass. The system does have a firewall installed and it loads automatically when the system starts.

4.2 Verify the system has no server ports listening

References	[11] [8] [7]
Risk	The existence of listening ports on a system facilitate unauthorized access from the network and open the possibility for a denial of service.

Testing Procedure	1. Make sure the user whom the laptop is assigned is logged into the system running all the applications he/she normally runs.	
	2. Login as root to a different console in the same system and execute the following command:	
	``` # netstat -nl |grep : ```	
	3. Login as root to a different system and execute the following commands	
	``` # cd /tmp # nmap -sS -P0 -O -p 1-65535 -oN tports $ip # nmap -sU -P0 -O -p 1-65535 -oN uports $ip ```	
	Note: Replace $ip with the IP address of the system being audited	
	4. Look at the output of the commands.	
	5. Delete the resulting files	
	``` # rm /tmp/*ports ```	
Expected Result	There should not be any open ports.	
	*It is important that the normal user of the system is logged in and all regular applications be open so that the tests performed reflect a real life scenario as much as possible.	
Test Nature	Objective	
Evidence		

2.


```
root@nikky ~ # netstat -nl |grep :
tcp        0      0 0.0.0.0:6000            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:631             0.0.0.0:*               LISTEN
udp        0      0 0.0.0.0:631             0.0.0.0:*
root@nikky ~ # []
```

3.

xterm

File Edit View Terminal Tabs Help

XMSCANER root # nmap -sS -O -P0 -p 1-65535 -oN tports 10.10.10.226

Starting nmap 3.55 (http://www.insecure.org/nmap/) at 2004-07-26 18:33 EDT

xterm

File Edit View Terminal Tabs Help

XMSCANER root # nmap -sU -O -P0 -p 1-65535 -oN uports 10.10.10.226

Starting nmap 3.55 (http://www.insecure.org/nmap/) at 2004-07-26 18:36 EDT

The following is a screenshot of the output of the command

        # tcpdump -ni eth0
from the victim machine

chris@nikky:~

File Edit View Terminal Tabs Help

2(0) win 4096
19:09:26.517304 IP 10.10.10.222.41456 > 10.10.10.226.63449: S 536530402:53653040
2(0) win 2048
19:09:26.517320 IP 10.10.10.222.41456 > 10.10.10.226.26082: S 536530402:53653040
2(0) win 2048
19:09:26.517337 IP 10.10.10.222.41456 > 10.10.10.226.51251: S 536530402:53653040
2(0) win 2048
19:09:26.517353 IP 10.10.10.222.41456 > 10.10.10.226.20334: S 536530402:53653040
2(0) win 4096
19:09:26.785552 IP 10.10.10.222.45790 > 10.10.10.226.42405: UDP, length: 0
19:09:26.785584 IP 10.10.10.222.45790 > 10.10.10.226.24467: UDP, length: 0
19:09:26.785623 IP 10.10.10.222.45790 > 10.10.10.226.31654: UDP, length: 0
19:09:26.785661 IP 10.10.10.222.45790 > 10.10.10.226.49071: UDP, length: 0
19:09:26.785713 IP 10.10.10.222.45790 > 10.10.10.226.38506: UDP, length: 0
19:09:26.785738 IP 10.10.10.222.45790 > 10.10.10.226.62249: UDP, length: 0
19:09:26.785778 IP 10.10.10.222.45790 > 10.10.10.226.18991: UDP, length: 0
19:09:26.785818 IP 10.10.10.222.45790 > 10.10.10.226.36835: UDP, length: 0
19:09:26.785858 IP 10.10.10.222.45790 > 10.10.10.226.45661: UDP, length: 0
19:09:26.785896 IP 10.10.10.222.45790 > 10.10.10.226.21600: UDP, length: 0

40 packets captured
40 packets received by filter
0 packets dropped by kernel
root@nikky - #

--resulting tports file:

```
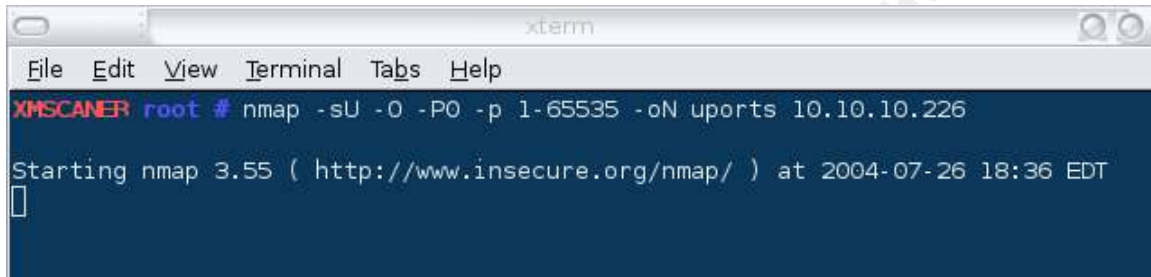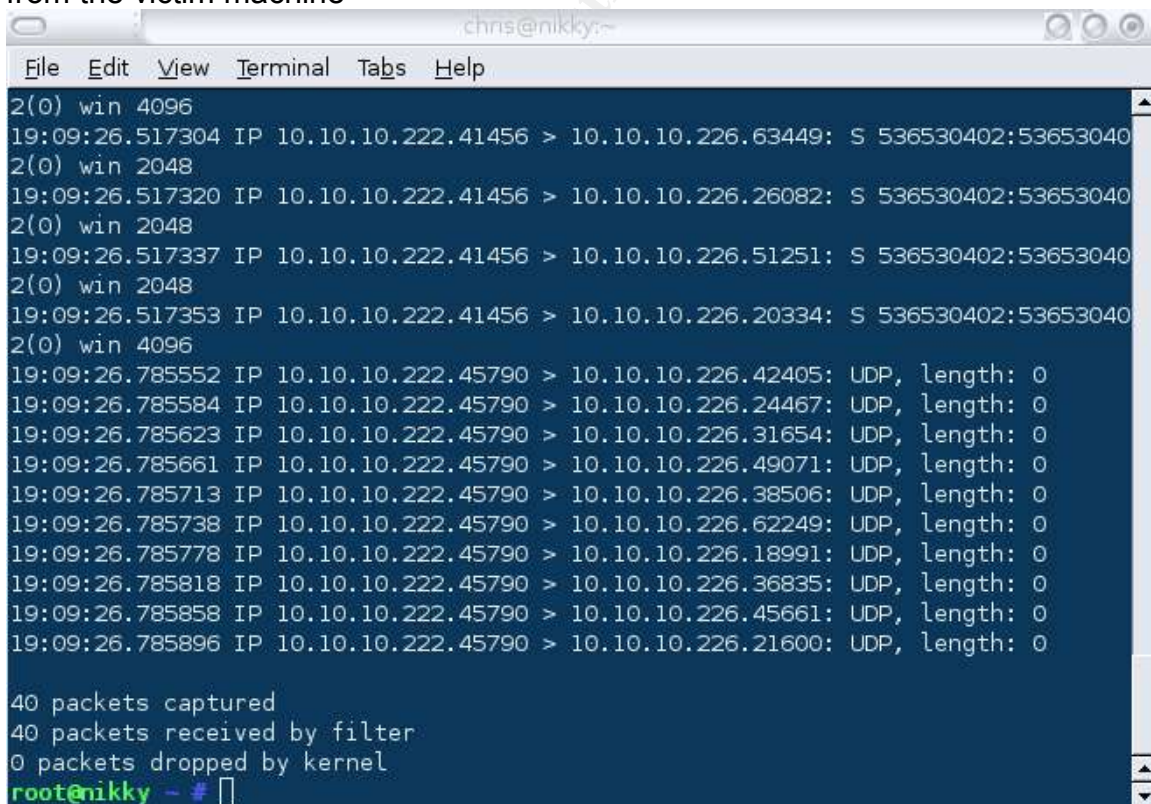# nmap 3.55 scan initiated Mon Jul 26 18:12:58 2004 as: nmap -sS -O -P0
-p 1-65535 -oN tports 10.10.10.226
Warning:  OS detection will be MUCH less reliable because we did not
find at least 1 open and 1 closed TCP port
Interesting ports on nikky (10.10.10.226):
(The 65530 ports scanned but not shown below are in state: filtered)
PORT    STATE   SERVICE
113/tcp closed auth
MAC Address: 00:02:3F:75:93:60 (Compal Electronics)
Too many fingerprints match this host to give specific OS details

# Nmap run completed at Tue Jul 27 08:06:16 2004 -- 1 IP address (1
host up) scanned in 49998.306 seconds
```

--resulting uports file:

```
# nmap 3.55 scan initiated Mon Jul 26 18:13:50 2004 as: nmap -sU -O -P0
-p 1-65535 -oN uports 10.10.10.226
Warning:  OS detection will be MUCH less reliable because we did not
find at least 1 open and 1 closed TCP port
All 65530 scanned ports on nikky (10.10.10.226) are: filtered
Too many fingerprints match this host to give specific OS details

# Nmap run completed at Tue Jul 27 08:58:56 2004 -- 1 IP address (1
host up) scanned in 53209.508 seconds
```

Findings	Pass. The netstat command showed that ports TCP 6000 and 631 and UPD port 631 were listening, this would leave the machine vulnerable to attack if a firewall were not present. However, the machine does not have open ports that can be used to connect from the network since the firewall is filtering all inbound traffic to the machine. There is one concern, on the TCP scan port 113 was found as closed, instead of filtered. This is a Shorewall default, to send a reset packet for port 113. This can be reviewed in the Shorewall FAQ at http://www.shorewall.net/FAQ.htm

4 Audit Report or Risk Assessment

Executive Summary

The IT Management of Company X has contracted Company Y Consulting to design a plan to secure their network. The first step in this plan is to perform an audit of a portable computer used by one of their consultants.

Since the laptop is used in untrusted networks from time to time and also because of the its nature, it was deemed a priority to assess the prevention of unauthorized physical access to the machine, the security of the system startup process and the assessment of the preservation of user privacy from other system users and from other network users.

Upon conducting the survey on the portable system it was determined that it did not meet the minimum security requirements needed to effectively serve as a sound tool for the consultant, given the type of work being performed with it. This machine is a potential security breach every time it is connected to foreign networks. However Company Y Consulting can modify the security standing of this machine so that Company X may continue their business unaffectedly.

Company Y Consulting uses a proven methodology for securing hosts that with time and dedication will ensure your business needs are handled accordingly with the policies you've detailed.

Audit Findings and Audit Recommendations

1 Preliminary tests

Check 1.2:   **PASS**

Verify the system does not contain a root kit

The surveyed system has adequate security in this section. There was no evidence that the system has been compromised.

Recommendations

Perform this test periodically using a trusted bootable CDROM. Company Y Consulting can provide such CDROM if needed.

Check 1.3:   **PASS**

Verify the system is updated with the latest OS patches

No missing security patches were found as compared with the Gentoo Linux Security Advisories. There were seven applications that have updated versions and two that the system marked as new. However, none of the versions of installed packages have security advisories.

The following is a list of the packages suggested to be upgraded:

> x11-misc/xscreensaver-4.16 [4.15]
>
> gnome-base/libgnome-2.6.1.1-r1 [2.6.1.1]
>
> gnome-extra/gnome-utils-2.6.2-r1 [2.6.2]
>
> dev-libs/libxml2-2.6.11 [2.6.9]
>
> dev-libs/libxslt-1.1.8 [1.1.6]
>
> gnome-base/gnome-2.6.2-r1 [2.6.2]
>
> net-fs/samba-3.0.5-r1 [3.0.5]
>
> New: dev-perl/Digest-MD4-1.3
>
> New: dev-perl/Crypt-SmbHash-0.02

Recommendations

Security updates should be applied as soon as possible after they are released. Non security related updates should also be applied but according to a set maintenance process ad are not mission critical. The cost of updating these packages at this point is not justified by the need to update the system.

These packages should be applied only when convenient.

2 System Startup

FAIL

Verify existence of a BIOS boot password

When the system is started there was not password prompt at the BIOS screen. This is a security vulnerability since anyone with physical access to the system may load it and make it available to attack from the network and through it physical console.

Recommendations

Configure the BIOS to prompt for a password upon boot. To do this perform the following steps:

1. Boot the machine and press F2 at the BIOS screen
2. Scroll to the Security Tab
3. Enter a password under the prompt "Set User Password [Enter]"
4. Exit the BIOS setup saving changes by pressing F10 and then the "Enter" key

FAIL

Verify the existence of a BIOS setup password

When a user tries to enter the BIOS setup menu the system does not prompt for a password. This is a security vulnerability because anyone with physical access to the system may configure the BIOS to load the system from alternate media such as CDROM or USB drives and have complete access to the hard drive circumventing any authorization, authentication or accountability restrictions imposed by the operating system.

Recommendations

Configure the BIOS to prompt for a password upon entering the setup menu. To do this perform the following steps:

5. Boot the machine and press F2 at the BIOS screen
6. Scroll to the Security Tab
7. Enter a password under the prompt "Set Supervisor Password [Enter]"
8. Exit the BIOS setup saving changes by pressing F10 and then the "Enter" key

Check 2.3:   **PASS**

Verify the existence of a boot loader password

The boot loader is correctly configured to prompt for a password to allow access to the advanced system loading options.

Recommendations

No recommendations can be made for this subject.

Check 2.4:   **FAIL**

Verify that the system prompts for root password while in single user mode

The system does not prompt for the root password when it is loaded in single user mode. This is a security vulnerability because anyone with physical access to the system may overcome the security established by the Linux OS by loading in single user mode.

Recommendations

Configure the system to prompt for the root password upon entering single user mode. To achieve this perform the following steps:

1. Enter the system as root
2. Edit the /etc/inittab configuration file
3. Find the line that reads

   ```
   l1:S1:wait:/sbin/rc single
   ```
4. Modify it so it looks like the following line

   ```
   l1:S1:wait:/sbin/sulogin single
   ```

Making this modification only takes two minutes and it does not require a system restart.

Check 2.5:   **PASS**

Verify the system is not configured for auto login upon startup

The system requires user authentication before access is granted when started or reloaded. This is the expected behavior.

Recommendations

None regarding this subject.

Check 2.6:   **PASS**

Verify the system does not load a graphical user interface automatically

The system loads to a text based user authentication screen. This is the recommended behavior.

Recommendations

None regarding this subject.

3 File System Access

Check 3.1: **FAIL**

Verify the user's HOME directory only has access permissions for its owner

The permissions are incorrect for some home directories and their contents. This is a security vulnerability because the user's data store in the user's home directory is accessible to unauthorized users either from the network and the system itself.

Recommendations

Modify the permissions of all home directories to only allow access to the owner. To achieve this perform the following procedure.

1. Login to the system as root

2. Enter the following commands at the console

```
chown root:users /home
chmod 750 /home
chmod -R 700 /home/*
```

These commands will ensure that only the owner has access to the files stored in each home directory.

Check 3.2: **FAIL**

Verify the system does not contain world writable files

There are files and directories with permissions to allow access to everyone. This is a security vulnerability because any user with access to the system may modify it's configuration rendering the system unusable.

Recommendations

Change the permissions of all files so that only the owner and the group have access. This task must be performed by an experienced administrator to minimized the risk of crippling the machine.

Change the default UMASK setting to 077 so new files created by the users are accessible to the owner only. The owner is responsible for granting others access permissions to his/her files. To change the default UMASK for all users perform the following steps:
1. As root edit the file /etc/profile
2. Find the line that starts with "umask" and ensure it's set to 077.

FAIL

Verify the system contains only the required SUID and SGID files

There were many SIUD and SGID files found in the system. This is a security vulnerability because previously unknown software flaws may cause one of those files to allow the system to be compromised.

Recommendations

Change the file permissions so that only the files deemed required have the SUID or SGID bits set. This is a very critical task since incorrectly changing permissions may render the system or its services unavailable. Company Y Consulting recommends to develop a plan to research each file and determine if its permissions may be changed. There may be files that can be completely removed form the system, for example games, etc. To determine which package a file belongs to the following command may be used:

```
qpkg -f $file
```

FAIL

Verify the use of strong passwords for user authentication

There were three users found in the systems user database. Two users (chris, and root) had strong passwords however, the third (john) had a very weak password.

Recommendations

Ensure the system has the package cracklib installed. Cracklib is a password checking library. Develop a password strength policy and communicate it to all employees. Also research the possibility of implementing a stronger authentication scheme such as biometrics or USB tokens.

PASS

Verify the $PATH for user root does not contain "."

The path for the user root did not contain a dot. This is the expected configuration.

Recommendations

None regarding this subject.

Check 3.6:	PASS

Verify no UID 0 account exist other than root

The system only contains one account with UID 0, the root user. This is the expected configuration.

Recommendations

None regarding this subject.

4 Network Access

Check 4.1:	PASS

Verify the system is protected by a host firewall

The existence of a firewall was confirmed, this is the expected configuration. However, the user was not aware that a firewall was installed in the system.

Recommendations

The user did not seem aware of the existence of a firewall. This is a concern and should be resolved with user training. The user should attend a two day security awareness class. Company Y Consulting offers such introductory training and more.

Check 4.2:	PASS

Verify the system is protected by a host firewall

No open ports could be found while performing a port scan form a remote machine. This is the expected behavior however, when checked for the local machine, three ports were found listening.

The netstat command showed that ports TCP 6000 and 631 and UPD port 631 were listening, this would leave the machine vulnerable to attack if a firewall were not present.

Recommendations

The user did not seem aware of the existence of a firewall. This is a concern and should be resolved with user training. The user should attend a two day security awareness class. Company Y Consulting offers such introductory training and more.

The firewall ruleset should be modified to drop traffic to port 113 to maintain stealthness of the host in unfriendly networks. To modify the configuration perform the following steps:

1. As root edit the file file

   ```
   /usr/share/shorewall/action.RejectAuth
   ```

2. The perform a firewall restart by running:

   ```
   shorewall clear && shorewall restart
   ```

Bibliography

[1] Linux Standard Base Project. Free Standards Group.
17 Jul. 2004 <www.linuxbase.org>.

[2] International Organization for Standardization. "ISO/IEC 17799:2000(E)
Information technology --Code of practice for information security
management". 2000

[3] Tittel, Ed, Mike Chapple, James Michael Stewart. CISSP Certified Information
Systems Security Professional Study Guide. San Francisco: Sybex, 2003.

[4] Threat/Vulnerability Assessments & Risk Analysis. Applied Research
Associates Inc. 23 Jul. 2004
<www.wbdg.org/design/resource.php?cn=0&rp=27>.

[5] 2004 CSI/FBI Computer Crime and Security Survey. Center for Internet
Security. 23 Jul. 2004 <www.gocsi.com/forms/fbi/pdf.jhtml;jsessioni>.

[6] Laptop Security, Part One: Preventing Laptop Theft. Security Focus.
21 Jul. 2004 <www.securityfocus.com/infocus/1186>.

[7] Linux Security HOWTO. Linuxsecurity.com. 25 Jul. 2004
<www.linuxsecurity.com/docs/LDP/Security-HOWTO/inde>.

[8] Center for Internet Security. "Linux Benchmark v1.1.0". 2004

[9] Laptop Security, Part Two: Preventing Information Loss. Security Focus.
21 Jul. 2004<www.securityfocus.com/infocus/1187>.

[10] Mac OS X Single User Mode Root Access. Securemac.com.
25 Jul. <www.securemac.com/macosxsingleuser.php>.

[11] Gentoo Linux Security Guide. Gentoo Linux. 21 Jul. 2004
<www.gentoo.org/doc/en/gentoo-security.xml>.

[12] Nemeth, Evi, Garth Snyder, Scot Seebass, Trent R. Hein, UNIX System
Administration Handbook Third Edition. New Jersey:Prentice Hall, 2001