

自带系统维护和入侵检测功能的 BBS 服务器
(分析设计说明书)

参赛院校: 北京交通大学

参赛队员: 黄峰 洪元志 董振辉

指导老师: 常宏达 邹强

完成日期: 2008. 11. 22

目录

综述	1
1、 背景和应用领域	2
2 、 作品特点和设计思路	2
3、 运行硬件环境要求	2
4、 功能描述	3
4.1 BBS服务功能	3
4.2 系统维护功能	3
4.3 安全防护功能	4
5、 工作原理	4
5.1 BBS服务器	4
5.2 系统维护	5
5.3 安全防护	5
6、 体系结构和关键技术点	5
6.1 体系结构	5
6.2 关键技术点	6
7、 功能模块设计	7
7.1 网络服务模块	7
7.2 系统维护模块	9
7.3 安全防护模块	26
7.4 其他常用工具模块	28
8、 相关技术比较和分析	29
9、 总结	29

综述

为了方便 BBS 服务器的管理者更加方便地搭建起一个适合自己要求的安全的 BBS 的平台，我们打造了这款 liveCD。尽管初衷是提供 BBS 服务，但通过安装其它组件也可以作为其它网络服务器，如 wiki 等。由于网络服务也应该注意它的数据备份和安全设置，所以我们又配备了其它的系统维护和安全工具。于是，最终我们将该 liveCD 功能定位为自带系统维护和入侵检测功能的 BBS 服务器。

首先是网络服务的功能。在 liveCD 中我们保留了 Apache、MySQL、Samba、等系统自带的软件。其中的 Apache 部分我们已经配置好，在安装配置 BBS 服务器程序后，用户只需根据自己的需要配置一下 MySQL 数据库，即可提供简单的 BBS 服务。

作为一张系统维护盘，我们集成了 partimage、afick、testdisk、photorec、shred、sysstat 等系统维护工具。partimage 是一个磁盘的 ghost 备份工具，如果说服务器要换容量更大的磁盘或者就是要换台服务器，那么这个工具绝对的是最好的选择，克隆的速度很快。afick 是一个文件校验的软件，它是验证文件的哈希值，来判断是否被篡改过，这个对寻找黑客在你服务器上做了那些手脚是很有帮助的。testdisk 是检测磁盘恢复分区信息的软件、针对分区表被删除以及 MBR（master boot record）被修改的恢复分区信息软件，主要用来恢复损坏的分区以及拯救无法引导的磁盘。photorec 是一个文件恢复的软件，在文件被误删除的情况下，可以使用该软件来进行恢复。shred 与 photorec 相反，是完全的删去文件，它用重写存储区的方法，使得需要保密而不需再用的数据不会被他人恢复看到。sysstat 这个工具，可以说是 linux & Unix 以及 FreeBSD 最常用的工具。它的主要用途就是观察服务负载，比如 CPU 和内存的占用率、网络的使用率以及磁盘写入和读取速度等。

该 liveCD 还作为一张网络安全盘使用，提供入侵检测功能。这里我们选用了 snort 这一目前应用最为广泛的一个 IDS 产品，它是一个轻量级的网络入侵检测软件，在运行时只占用极少的网络资源，对原有网络性能影响很小。作为嗅探器，snort 对发往同一网络的其他主机的流量进行捕获，然后进行分析。它采用误用检测模型，即首先建立入侵行为特征库，然后在检测过程中，将收集到的数据包和特征代码进行比较，以得出是否入侵的结论。

从方便用户使用的角度出发，我们集成了以上三个部分功能，制作了该 liveCD，为使用者提供全面的功能服务。

1、 背景和应用领域

BBS (Bulletin Board System)，翻译为中文就是“电子公告板”。早期的BBS与一般街头和校园内的公告板性质相同，只不过是电脑来传播或获得消息而已。一直到个人计算机开始普及之后， BBS才开始渐渐普及开来。近些年来，由于爱好者们的努力，BBS的功能得到了很大的扩充。目前，通过BBS系统可随时取得国际最新的软件及信息，也可以通过BBS系统来和别人讨论计算机软件、硬件、Internet、多媒体、程序设计以及医学等等各种有趣的话题。但是由于现有因特网存在的一些安全问题和规模上的难以控制和管理等问题，BBS服务器不可避免地会遇到一些网络黑客的攻击，前一段时间知名论坛 360 安全论坛，UBUNTU中文论坛等BBS服务器就因为遭受到了不明攻击，导致论坛会员们在很长一段时间无法登录服务器。在一套可靠的系统上运用系统维护软件和网络安全软件来保证BBS论坛安全，保证数据及时恢复和备份，是至关重要的一件事情。

正是因为如此，我们制作了这张名为“自带系统维护和入侵检测功能的 BBS 服务器”的 liveCD。本作品使用 phpBB3 作为 BBS 服务程序，Web 服务和数据库则分别由 Apache 和 MySQL 提供。除基本 BBS 服务外，还提供了系统维护和入侵检测功能，其中系统维护工具有 testdisk&photorec、systat、partimage 和 afick 等，入侵检测 IDS 由 snort 和相关组件完成。故该 LiveCD 除了能作为应急盘提供 BBS 服务外，还能作为应用盘通过集成的工具为用户提供系统维护和安全检测功能。

2 、 作品特点和设计思路

本作品基于红旗 Asianux 3 workstation 版构建系统平台，在系统安装过程中精简了大量不相关的功能模块和软件包，在精简后的系统中安装了我们自己定制的工具和软件。系统无需在硬盘上安装即可直接从光驱启动，通过内存虚拟硬盘可以提供 BBS 服务、系统维护和入侵检测等功能，具有简单、安全、功能全面的特点。

设计思路是，在系统安装过程中保留 Asianux 3.0 平台中的开发编译环境和工具，通过在开源社区中寻找相关源代码和缺失组件完成相应功能模块的安装和配置。

3、 运行硬件环境要求

最低要求：

主频 700M 的 x86 处理器
128 MB 系统内存（ RAM ）
8 GB 的磁盘空间
显卡能支持 1024x768 分辨率
CD - ROM 驱动器
有网卡进行 Internet 网络连接

推荐配置：

主频 1.2 GHz 以上的 x86 处理器
256 MB 以上系统内存 (RAM)
60 GB 以上的磁盘空间
显卡能支持 1024x768 分辨率
CD - ROM 驱动器
有网卡进行 Internet 网络连接

4、 功能描述

4.1 BBS 服务功能

这里我们保留了 Asianux 3.0 自带的部分软件包,包括 Apache、MySQL、gFTP 等,这些组件将会为其他程序提供相应功能。同时也保留了 fdisk 和 shred 的其它实用工具。

BBS 服务简单说就是留言板,来访客户通过网页形式,在网页上登记个人信息或注册账号,然后就可以发表个人观点。通过填写留言,向服务器的数据库提交留言后,数据库再将留言发送到网页中。其他用户就可以通过浏览网页查看到每个人留言板的内容,形成一种交流方式。

BBS 服务程序就是要在网页和数据库之间建立一种数据的交互方式,而且还要保证数据的安全性和准确性。对于复杂的 BBS 还允许建立用户帐户,为用户设立不同权限,以及维护和备份 BBS 服务。

4.2 系统维护功能

系统维护功能的任务是改正软件系统在使用过程中发现的隐含错误,扩充在使用过程中用户提出的新的功能及性能要求,其目的是维护软件系统的正常运作。在 liveCD 中我们集成了 Testdisk& PhotoRec、Sysstat、partimage、afick 等系统维护工具。

partimage是一个磁盘的ghost备份工具,如果说服务器要换容量更大的磁盘或者就是要换台服务器,那么这个工具绝对的是最好的选择,克隆的速度很快。afick是一个文件校验的软件,它是验证文件的哈希值,来判断是否被篡改过,这个对寻找黑客在你服务器上做了那些手脚是很有帮助的。testdisk 是检测磁盘恢复分区信息的软件、针对分区表被删除以及MBR (master boot record) 被修改的恢复分区信息软件,主要用来恢复损坏的分区以及拯救无法引导的磁盘。photorec是一个文件恢复的软件,在文件被误删除的情况下,可以使用该软件来进行恢复。shred 与photorec相反,是完全的删去文件,它用重写存储区的方法,使得需要保密而不需再用的数据不会被他人恢复看到。sysstat这个工具,可以说是linux & Unix 以及Freebsd最常用的工具。它的主要用途就是观察服务负载,比如CPU和内存的占用率、网络的使用率以及磁盘写入和读取速度等。

4.3 安全防护功能

在 liveCD 中的安全防护功能由 snort 工具和 sysstat 工具实现。

入侵检测 (Intrusion Detection) 是对入侵行为的检测。它通过收集和分析网络行为、安全日志、审计数据、其它网络上可以获得的信息以及计算机系统中若干关键点的信息,检查网络或系统中是否存在违反安全策略的行为和被攻击的迹象。入侵检测作为一种积极主动地安全防护技术,提供了对内部攻击、外部攻击和误操作的实时保护,在网络系统受到危害之前拦截和响应入侵。因此被认为是防火墙之后的第二道安全闸门,在不影响网络性能的情况下能对网络进行监测。入侵检测通过执行以下任务来实现:监视、分析用户及系统活动;系统构造和弱点的审计;识别反映已知进攻的活动模式并向相关人士报警;异常行为模式的统计分析;评估重要系统和数据文件的完整性;操作系统的审计跟踪管理,并识别用户违反安全策略的行为。入侵检测是防火墙的合理补充,帮助系统对付网络攻击,扩展了系统管理员的安全管理能力(包括安全审计、监视、进攻识别和响应),提高了信息安全基础结构的完整性。它从计算机网络系统中的若干关键点收集信息,并分析这些信息,看看网络中是否有违反安全策略的行为和遭到袭击的迹象。

snort 的功能主要有:

实时通信分析和信息包记录。

包装有效载荷检查。

协议分析和内容查询匹配。

探测缓冲溢出、秘密端口扫描、CGI 攻击、SMB 探测、操作系统入侵尝试。

对系统日志、指定文件、Unix socket 或通过 Samba 的 winpopus 进行实时报警。

sysstat 这个工具,可以说是 linux & Unix 以及 Freebsd 最常用的工具。它的主要用途就是观察服务负载,比如 CPU 和内存的占用率、网络的使用率以及磁盘写入和读取速度等。它的主要任务是配合 snort 的使用。

这个包一但安装下去,一般包括如下的几个命令可以使用:

sar、iostat、sa1、sa2、sadb、mpstat、sadc、sysstat

这几个命令中,有的是服务,有的是查看结果的命令。也有的是即时服务器 CPU,内存以及网络的使用率。

5、工作原理

5.1 BBS 服务器

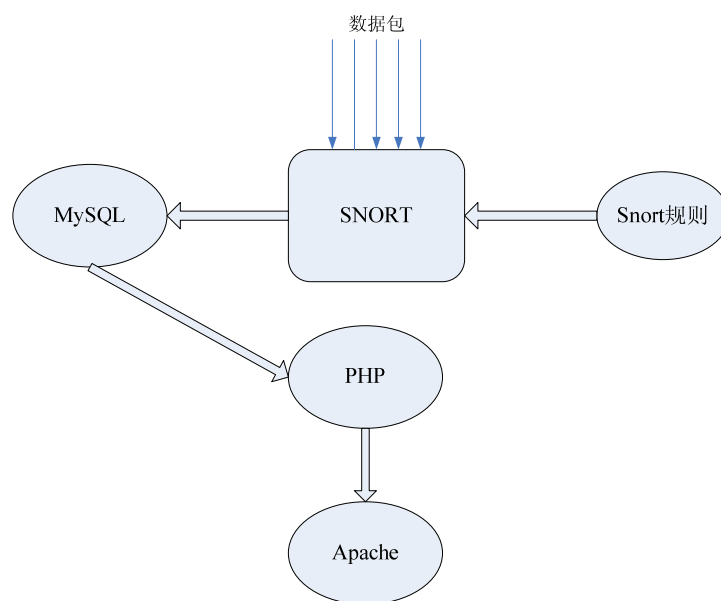
建立 BBS 服务前,要在服务器中建立 Web 服务和数据库。Web 服务是保证 BBS 服务可以和浏览用户之间的交流,而数据库则是用来保存用户的留言内容和用户的注册信息。

BBS 服务程序就是要在网页和数据库之间建立一种数据的交互方式,而且还要保证数据的安全性和准确性。对于复杂的 BBS 还允许建立用户帐户,为用户设立不同权限,以及维护和备份 BBS 服务。

5.2 系统维护

这部分功能通过二进制安装和源码安装两种方式，我们在安装过程中解决了安装和配置工程中的问题，最后在 liveCD 上提供了多种系统维护工具。

5.3 安全防护



snort 的工作原理如上图所示，各模块的功能为：

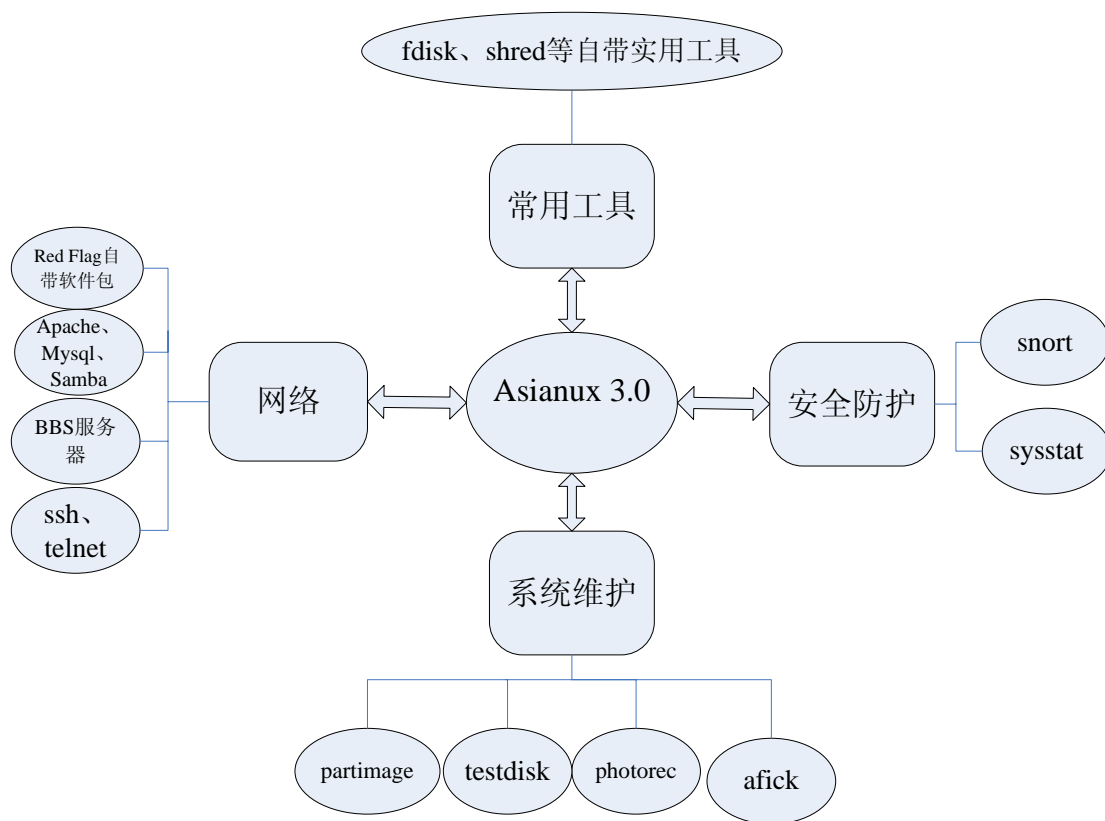
SNORT 软件抓取网络上的数据包，分析检测，然后将入侵 alert 写入 alert 文件和 MySQL 数据库；MySQL 数据库存放 SNORT 写入的入侵 alert；Apache 和 PHP 负责将 MySQL 里面的入侵 alert 以网页的形式显示出来。

其中，新的 snort 规则可以从 Snort 网站上获取。

6、 体系结构和关键技术点

6.1 体系结构

我们制作的这张 livecd 的目的是提供简单 BBS 服务的同时也提供系统维护和安全检测等功能。在保留了部分系统自带工具的前提下，我们加入了很多从开源社区找到的软件和工具，集成到了我们的 liveCD 中，整体的结构框图如下图所示：



liveCD 结构框图

由框图可以看出，整个结构分为网络、安全防护、系统维护和常用工具四个部分。网络部分通过保留 Apache 和 MySQL 等常用自带软件外，我们加入了 BBS 服务软件，从而可以提供简单的网页和 BBS 服务。系统维护部分通过集成 partimage、testdisk、photorec 和 afick 等常用系统工具来完成。安全防护部分我们采用 snort 入侵检测工具并结合 sysstat 工具来实现。常用工具部分有选择的保留了部分系统自带工具。

6.2 关键技术点

6.2.1 系统安装的选择

要将一个完全安装有 3 张 cd(不含两张工具盘)的系统集合在一个小于 750M 的 livecd，有两种方案：一种方案是完全安装，在装完所需软件后在卸载一些不需要的东西，其优点是很容易添加其它软件，遇到问题也会比较少，因为完全安装集合了很多的库文件。但完全安装后制作的 livecd 有将近 1G，各软件间的相互依赖关系使得后面精简系统过程出现了很大的问题。第二种方案是尽量最小的安装，能满足一般的添加软件和一般命令的使用即可，之后需要什么组件再添。制作 liveCD 过程中，我们选择了第二套方案。在安装系统的时候只定制了以下软件包：

```
chinese-support
base-x
```


basesystem-optional
database-tools
gnome-libs
kde-desktop
legacy-software-development
server
system-tools
web-browsers

系统安装完后有只有 1844M，经过进一步优化和安装相应组件后，最后做出的 liveCD 只有 520M。

6.2.2 livecd 制作

kernel-live-2.6.24.4-4.1.i686.rpm 安装需要 mkinitrd 模块，但系统自带的 mkinitrd 模块与该软件包不符合，所以在运行 `rpm -ivh k*.rpm --nodeps --force` 后，我们建立了软链接 `ln -s vmlinuz.2.6.24.4-4live vmlinuz`，使得该 liveCD 制作软件可以使用。

之后制作 liveCD 的步骤参照红旗在网上的 liveCD 制作教程完成，经过实机测试，达到了预期效果。

6.2.3 开机自动登入的设置

作为一张能在不同情况时使用的 livecd，我们认为没有必要保留密码，所以取消了开机密码输入，设置为自动登入。方法是 `vi /usr/share/config/kdm/kdmrc` 中找到 `[X-:0-Core]`，找到 `AutoLoginUser=`（应为 root，如果在控制中心设过以后，这会出现那个用户），在下面加一行信息 `AutoLoginPass=`（填上安装系统时设置的 root 密码）。

6.2.4 软件安装和配置的问题

这部分内容比较多，详细的关键技术点在“7、功能模块设计”部分进行了详细阐述，这里不再赘述。

7、 功能模块设计

7.1 网络服务模块

在 BBS 服务器模块中，我们集合了 Asianux 3.0 自带的部分红旗软件包包括 Apache、MySQL、gFTP 等，这些是构成 BBS 服务器的主要工具软件。另外我们提供了 SSH 客户端和服务及 Samba 服务，这些组件将会为其他程序提供相应

功能。同时也保留了 fdisk 和 shred 这些工具，为的是能够对服务器的硬盘提供基本的查询检测功能。

安装:

先使用源码安装 phpBB3 然后安装中文支持语言包.

```
unzip -e phpBB-3.0.2.zip
```

```
unzip -e zh_CN.zip
```

解压缩完成后，生成目录 phpBB3 和 zh_CN，将 zh_CN 拷贝到 phpBB3/language 目录下，并改名为 en，将原 en 文件备份为 en.old，这样 BBS 的语言就默认为中文了（当然也可设为英文）。

下载地址：<http://www.phpbb.com/downloads/olympus.php>

配置:

解压缩成功后，在当前目录生成新目录 phpBB3，复制该目录到 apache 服务指定的目录中，可以通过浏览器来访问 phpBB3 目录中的网页。由于 BBS 服务程序使用的编程语言为 PHP，所以要注意 web 服务对 PHP 的支持。

由于 apache 是 Asianux 3.0 系统默认的 web 服务程序，以配置 apache 服务举例，启用 PHP 模块，在目录/etc/httpd/conf.d/php.conf。

```
#
# PHP is an HTML-embedded scripting language which attempts to make it
# easy for developers to write dynamically generated webpages.
#
LoadModule php5_module modules/libphp5.so

#
# Cause the PHP interpreter to handle files with a .php extension.
#
AddHandler php5-script .php
AddType text/html .php

#
# Add index.php to the list of files that will be served as directory
# indexes.
#
DirectoryIndex index.php

#
# Uncomment the following line to allow PHP to pretty-print .phps
# files as PHP source code:
#
#AddType application/x-httpd-php-source .phps
```

文件使用系统默认的设置，如果没有修改过该文件，保持原状态即可。

检查 PHP 的配置文件/etc/php.ini。修改文件中 457 行的参数。

```
453 ;
454 ; You should do your best to write your scripts so that they do not require
455 ; register_globals to be on; Using form variables as globals can easily lead
456 ; to possible security problems, if the code is not very well thought of.
457 register_globals = On
458
```

参数 register-globals 的默认设置为 Off，应该改为 On。

查看 web 服务的配置文件，/etc/httpd/conf/httpd.conf 中的 web 目录的设置。

```
#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
#
DocumentRoot "/var/www/html"
```

由于本地 web 服务器的目录为/var/www/html，所以将 BBS 服务程序复制到该目录下，复制后的目录权限要允许运行 apache 服务的用户可读。

打开客户端的浏览器，在地址栏输入<http://localhost/phpBB3/index.php>，对于第一次访问未配置的 BBS，会自动转到 BBS 的服务主页：

<http://localhost/phpBB3/install/install.php>。

界面如下图所示：



由于我们在系统中安装了 MySQL 数据库，所以用户可以按照自己的需求为 BBS 建立数据库，设置管理权限，配置 BBS 服务等，这里不再详细讲解。

7.2 系统维护模块

为了满足管理人员在清除系统运行中发生的故障和错误，并对系统进行必要的修改与完善的需要，我们在 liveCD 中集成了 Testdisk& PhotoRec、Sysstat、partimage、afick 等系统维护工具。

7.2.1 Testdisk

TestDisk 是恢复分区信息的软件、针对分区表被删除以及 MBR (master boot record) 被修改的恢复分区信息软件，主要用来恢复损坏的分区以及拯救无法引导的磁盘，缺省扫描中，TestDisk 可能并不是扫描所有的扇区，未必能找全潜在的正确分区布局，在完成普通扫描结果后，屏幕底部会有一个"[Search!]"的选项，

执行它就是扫描所有扇区。

由于错误的使用分区工具而带来的分区丢失，硬盘磁盘分区遭到损坏的情况下，使用TestDisk可以复原已损坏的分区。TestDisk支持在 Windows、Linux、Unix、Mac OS 等系统上执行。TestDisk 还支持包括 FAT、NTFS、Ext2、Ext3、ReiserFS、RAID 等在内的广泛的文件系统。

为了防备在运行 BBS 的 liveCD 的运行中发生硬盘数据损坏的意外情况，我们在 liveCD 中添加了恢复硬盘分区表和硬盘数据的功能。下面我们配合 BBS 论坛实例，故意破坏已有的硬盘分区表，之后用 Testdisk 工具进行恢复。

安装

先安装 progsreiserfs-0.3.0.4-1.2.el5.rf.i386.rpm

然后安装 testdisk-6.9-1.rh9.rf.i386.rpm

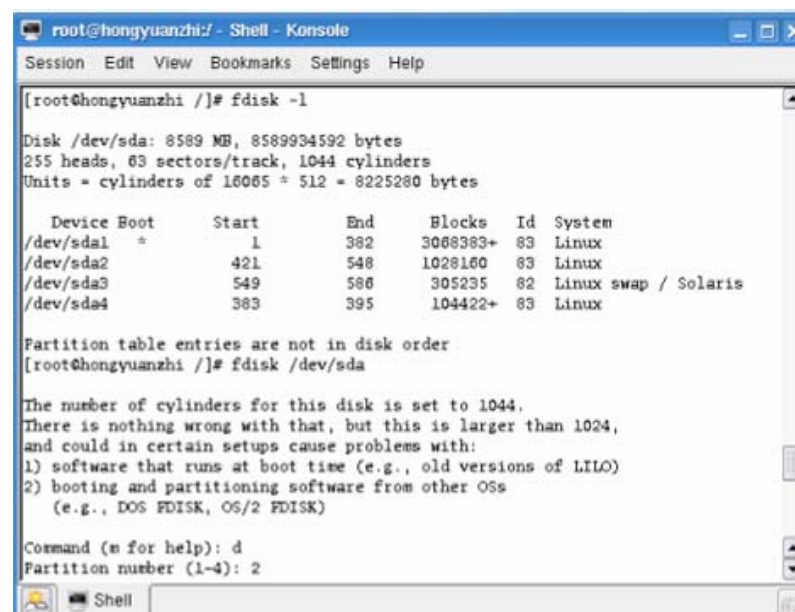
安装完成后，即可使用 TestDisk 和 Photorec 两个工具。下载地址：

<http://rpmfind.net/linux/rpm2html/search.php?query=libreiserfs-0.3.so.0>

<http://dag.wieers.com/rpm/packages/testdisk/>

配置使用

这是 liveCD 上原来正确的分区表：



```
root@hongyuanzhi:~# fdisk -l

Disk /dev/sda: 8589 MB, 858934592 bytes
255 heads, 63 sectors/track, 1044 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1  *           1           382     3068363+   83  Linux
/dev/sda2              421          548     1028160   83  Linux
/dev/sda3              549          586     305235    82  Linux swap / Solaris
/dev/sda4              383          395     104422+    83  Linux

Partition table entries are not in disk order
root@hongyuanzhi:~# fdisk /dev/sda

The number of cylinders for this disk is set to 1044.
There is nothing wrong with that, but this is larger than 1024,
and could in certain setups cause problems with:
 1) software that runs at boot time (e.g., old versions of LILO)
 2) booting and partitioning software from other OSs
   (e.g., DOS FDISK, OS/2 FDISK)

Command (m for help): d
Partition number (1-4): 2
```

进行误操作后，删除了一个/home 分区的分区表

```
root@hongyuanzhi:~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

WARNING: Re-reading the partition table failed with error 16: Device or resource
busy.
The kernel still uses the old table.
The new table will be used at the next reboot.
Syncing disks.
[root@hongyuanzhi /]# fdisk -l

Disk /dev/sda: 8589 MB, 8589934592 bytes
255 heads, 63 sectors/track, 1044 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1  *           1           382     3068383+   83  Linux
/dev/sda5             549           586     305235    82  Linux swap / Solaris
/dev/sda4             383           395     104422+   83  Linux

Partition table entries are not in disk order
[root@hongyuanzhi /]#
```

因为分区表被破坏，无法正常进入系统，需要恢复原先的分区表。此时只能进入命令行界面。以 root 权限登陆，输入 testdisk。出现如下修复界面：

```
TestDisk 6.8, Data Recovery Utility, August 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

TestDisk is free software, and
comes with ABSOLUTELY NO WARRANTY.

Select a media (use arrow keys, then press Enter):
Disk /dev/sda - 8587 MB / 8189 MiB

[Proceed ] [ Quit ]

Note: Disk capacity must be correctly detected for a successful recovery.
If a disk listed above has incorrect size, check HD jumper settings, BIOS
detection, and install the latest OS patches and disk drivers.
```

首先，选择恢复操作中的 log 文件（testdisk.log）的纪录方式。

- [Create] 新建
- [Append] 追加
- [No Log] 不纪录

```
TestDisk 6.8, Data Recovery Utility, August 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
```

```
TestDisk is a data recovery designed to help recover lost partitions
and/or make non-booting disks bootable again when these symptoms
are caused by faulty software, certain types of viruses or human error.
It can also be used to repair some filesystem errors.
```

```
Information gathered during TestDisk use can be recorded for later
review. If you choose to create the text file, testdisk.log , it
will contain TestDisk options, technical information and various
outputs; including any folder/file names TestDisk was used to find and
list onscreen.
```

```
Use arrow keys to select, then press Enter key:
```

```
[ Create ] Create a new log file
[ Append ] Append information to log file
[ No Log ] Don't record anything
```

选择 log 文件的记录方式

选择了 log 文件的记录方式后、显示了处于连接状态的磁盘设备。然后选择要恢复的磁盘分区、选择 [Proceed]。在这里选择装有 Linux 的硬盘 [Disk /dev/sda]。

```
TestDisk 6.8, Data Recovery Utility, August 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
```

```
TestDisk is free software, and
comes with ABSOLUTELY NO WARRANTY.
```

```
Select a media (use Arrow keys, then press Enter):
```

```
Disk /dev/sda - 8587 MB / 8189 MiB
```

```
[Proceed] [ Quit ]
```

```
Note: Disk capacity must be correctly detected for a successful recovery.
If a disk listed above has incorrect size, check HD jumper settings, BIOS
detection, and install the latest OS patches and disk drivers.
```

在列出的磁盘设备中，选择要恢复的分区，然后选择磁盘分区的种类。Linux 选 [Intel]。

之后选择 [Analyse]，对分区进行分析。

分析之后显示了当前分区的状态。然后选择 [Proceed]、显示分析结果。

```
TestDisk 6.8, Data Recovery Utility, August 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sda - 8595 MB / 8197 MiB - CHS 1045 255 63
Partition      Start      End      Size in sectors
* Linux         0      1 1    301 254 63    6136767 [/]
P Linux        382     0 1    394 254 63    208845 [WIKIBBS]
P Linux        420     0 1    547 254 63    2056320 [/home]
P Linux Swap    548     0 1    585 254 63    610470

Structure: Ok. Use Up/Down Arrow keys to select partition.
Use Left/Right Arrow keys to CHANGE partition characteristics:
*=Primary bootable P=Primary L=Logical E=Extended D=Deleted
Keys A: add partition, L: load backup, T: change type, P: list files,
Enter: to continue
EXT3 Large file Sparse superblock, 3142 MB / 2996 MiB
```

分区状态表示

分区结构以绿色文字表示。和分析之前的画面相比、Linux 的分区增加了一项，这个就是被误删除了的分区，选择之。

按 [P] 键，该分区根部的文件和索引被表示出来，假如显示正确的画，分析结果就可以正确的推算。然后用这个方法，对其他的盘符进行操作。

```
TestDisk 6.8, Data Recovery Utility, August 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sda - 8595 MB / 8197 MiB - CHS 1045 255 63
Partition      Start      End      Size in sectors
* Linux         0      1 1    301 254 63    6136767 [/]
P Linux        382     0 1    394 254 63    208845 [WIKIBBS]
P Linux        420     0 1    547 254 63    2056320 [/home]
P Linux Swap    548     0 1    585 254 63    610470

Structure: Ok. Use Up/Down Arrow keys to select partition.
Use Left/Right Arrow keys to CHANGE partition characteristics:
*=Primary bootable P=Primary L=Logical E=Extended D=Deleted
Keys A: add partition, L: load backup, T: change type, P: list files,
Enter: to continue
EXT3 Sparse superblock, 106 MB / 101 MiB
```

分区的分析结果,可以看出原先被破坏的分区表项[WIKIBBS]已被恢复回来了。

按 [Enter] 键，显示分析结果被反映到磁盘。并且被恢复。现在的状态，恢复的信息还没有被写到硬盘上，必须选择 [Write]，才能真正的被写到磁盘上。写操作执行的确认信息显示的时候，按 [Y] 键确认之。

写操作执行完毕，需要重新启动，按 [Enter] 键。

最后退出 [Quit]，TestDisk 结束。系统重新启动。之后就可以进入正常的系统图形界面了。这说明了我們挽救了发生硬盘启动故障的 BBS 服务器，这对一个运行良好 BBS 服务器是至关重要的。

7.2.2 PhotoRec

图片的上传和下载在BBS论坛中是很重要的一部分。JPEG等图片文件或HTML、PDF、ZIP、TXT、办公文书等文件被误删除的情况下，可以使用PhotoRec的软件来进行恢复。使用工具PhotoRec进行文件恢复实际上、要对恢复前后磁盘的差异进行比较。比如，如果要恢复只安装了Linux的硬盘内的文件的话，KNOPPIX等的OneCD Linux在外挂硬盘被恢复的时候是必须的。另外PhotoRec由于是使用命令行进行操作的软件，所以要启动终端来执行。

以下是我們使用 PhotoRec 软件模拟恢复论坛上的图片数据的过程。

以root权限启动PhotoRec。

```
# photorec
```

下图中，显示了已连接磁盘设备，准备恢复的文件在那个设备上就选择之，然后再选择 [Proceed]。

在这里选择 [Disk /dev/sda]。

```
PhotoRec 6.9, Data Recovery Utility, February 2008
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

PhotoRec is free software, and
comes with ABSOLUTELY NO WARRANTY.

Select a media (use Arrow keys, then press Enter):
Disk /dev/sda - 10733 MB / 10236 MiB (RO) - VMware, VMware Virtual S
Disk /dev/sdb - 1073 MB / 1024 MiB (RO) - VMware, VMware Virtual S

[Proceed] [Quit]

Note: Disk capacity must be correctly detected for a successful recovery.
If a disk listed above has incorrect size, check HD jumper settings, BIOS
detection, and install the latest OS patches and disk drivers.
```

接下来，选择恢复的磁盘分区格式，选择 [Intel]。

注：FAT、NTFS、ext2 / 3、HFS+ 等几种磁盘分区格式与之对应，提供被选择。


```

PhotoRec 6.9, Data Recovery Utility, February 2008
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sda - 10733 MB / 10236 MiB (R0) - VMware, VMware Virtual S

Please select the partition table type, press Enter when done.
[Intel] Intel/PC partition
[EFI GPT] EFI GPT partition map (Mac i386, some x86_64...)
[Mac] Apple partition map
[None] Non partitioned media
[Sun] Sun Solaris partition
[XBox] Xbox partition
[Return] Return to disk selection

Note: Do NOT select 'None' for media with only a single partition. It's very
rare for a drive to be 'Non-partitioned'.

```

接下来，选择要恢复的分区。画面下方 [File Opt] 中有可供恢复的文件种类提供被选择。

```

PhotoRec 6.9, Data Recovery Utility, February 2008
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sda - 10733 MB / 10236 MiB (R0) - VMware, VMware Virtual S

Partition      Start      End      Size in sectors
D No partition  0  0  1  1304 254 63  20964825 [Whole disk]
1 * Linux      0  1  1  1227 254 63  19727757 [/]
2 P Linux Swap 1228 0  1  1303 254 63  1228940

[ Search ] [Options] [File Opt] [ Quit ]
                        Start file recovery

```

```
PhotoRec 6.9, Data Recovery Utility, February 2008
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

1 * Linux                                0  1  1  1227 254 63  19727757 [/]

To recover lost files, PhotoRec need to know the filesystem type where the
file were stored:
[ EXT2/EXT3 ] EXT2/EXT3 filesystem
[ Other      ] FAT/NTFS/HFS+/ReiserFS/...
```

选择恢复整个分区。

```
PhotoRec 6.9, Data Recovery Utility, February 2008
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

1 * Linux                                0  1  1  1227 254 63  19727757 [/]

Please choose if all space need to be analysed:
[ Free ] Scan for file from ext2/ext3 unallocated space only
[ Whole ] Extract files from whole partition
```

选择 [Search]、该画面表示为制定被恢复的文件索引 recup_dir.x（注）。该索引是执行 photorec 命令而做成的文件。

recup_dir.x 保存地址的选择

注：recup_dir.x 的「x」从 1 开始进行排列。

```
PhotoRec 6.9, Data Recovery Utility, February 2008
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Do you want to save recovered files in /root ? [Y/N]
Do not choose to write the files to the same partition they were stored on.

To select another directory, use the arrow keys.
drwxr-xr-x  0  0  4096 16-Aug-2008 13:48 Desktop
drwxr-xr-x  0  0  4096 15-Nov-2008 15:16 ..
drwxr-xr-x  0  0  4096 15-Nov-2008 15:36 .
```

按 [Y] 键开始进行恢复。可看到时间进度和被恢复出的文件类型和数目。

```
PhotoRec 6.9, Data Recovery Utility, February 2008
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sda - 10733 MB / 10236 MiB (RO) - VMware, VMware Virtual S
Partition      Start      End      Size in sectors
1 * Linux      0  1  1  1227 254 63  19727757 [/]

Pass 1 - Reading sector 1664834/19727757, 580 files found
Elapsed time 0h00m40s - Estimated time for achievement 0h07m13
txt: 580 recovered

Stop
```

恢复完成，可看到被恢复出的目录列表。

```

recup_dir.1      recup_dir.126 recup_dir.26 recup_dir.53 recup_dir.80
recup_dir.10     recup_dir.127 recup_dir.27 recup_dir.54 recup_dir.81
recup_dir.100    recup_dir.128 recup_dir.28 recup_dir.55 recup_dir.82
recup_dir.101    recup_dir.129 recup_dir.29 recup_dir.56 recup_dir.83
recup_dir.102    recup_dir.13  recup_dir.3  recup_dir.57 recup_dir.84
recup_dir.103    recup_dir.130 recup_dir.30 recup_dir.58 recup_dir.85
recup_dir.104    recup_dir.131 recup_dir.31 recup_dir.59 recup_dir.86
recup_dir.105    recup_dir.132 recup_dir.32 recup_dir.6  recup_dir.87
recup_dir.106    recup_dir.133 recup_dir.33 recup_dir.60 recup_dir.88
recup_dir.107    recup_dir.134 recup_dir.34 recup_dir.61 recup_dir.89
recup_dir.108    recup_dir.135 recup_dir.35 recup_dir.62 recup_dir.9
recup_dir.109    recup_dir.136 recup_dir.36 recup_dir.63 recup_dir.90
recup_dir.11     recup_dir.137 recup_dir.37 recup_dir.64 recup_dir.91
recup_dir.110    recup_dir.138 recup_dir.38 recup_dir.65 recup_dir.92
recup_dir.111    recup_dir.139 recup_dir.39 recup_dir.66 recup_dir.93
recup_dir.112    recup_dir.14  recup_dir.4  recup_dir.67 recup_dir.94
recup_dir.113    recup_dir.140 recup_dir.40 recup_dir.68 recup_dir.95
recup_dir.114    recup_dir.141 recup_dir.41 recup_dir.69 recup_dir.96
recup_dir.115    recup_dir.15  recup_dir.42 recup_dir.7  recup_dir.97
recup_dir.116    recup_dir.16  recup_dir.43 recup_dir.70 recup_dir.98
recup_dir.117    recup_dir.17  recup_dir.44 recup_dir.71 recup_dir.99
recup_dir.118    recup_dir.18  recup_dir.45 recup_dir.72 sys
recup_dir.119    recup_dir.19  recup_dir.46 recup_dir.73 testdisk.log
recup_dir.12     recup_dir.2  recup_dir.47 recup_dir.74
lroot@localhost ~]#

```

7.2.3 sysstat

安装:

```
#tar zxvf sysstat-8.0.4.1.tar.gz
```

```
#cd sysstat-8.0.4.1
```

#make config 这步可以省略，因为我们在安装的过程中，发现在有些发行版中出错，如果不用这个命令，可以直接安装到其默认的/usr/local/lib 目录中。make config 这个命令就是用来配置 sysstat 安装的，比如安装路径，log 存放等，显示代码如下：

```
Installation directory: [/usr/local]
```

```
sadc directory: [/usr/local/lib/sa]
```

```
System activity directory: [/var/log/sa]
```

```
Clean system activity directory? [n]
```

```
Enable National Language Support (NLS)? [y]
```

```
Linux SMP race in serial driver workaround? [n]
```

```
sa2 uses daily data file of previous day? [n]
```

```
Number of daily data files to keep: [7]
```

```
Group for manual pages: [man]
```

```
Set crontab to start sar automatically? [n]
```

```
#make
```

```
#make install
```

下载网址: <http://pagesperso-orange.fr/sebastien.godard/download.html>，这里我们使用的是sysstat-8.0.4.1 版本。

配置使用:

可以简单的用下面的命令，如果更复杂一点，可以用 `man` 来查看所有命令的用法。比如 `iostat`、`mpstat`、`iostat -p` 等

如果是想让服务器自动运行，并且想每个小时都有一个数据反馈，我们可以用 `cron` 来让执行 `sa1 sa2`，这样就有一份日志文件存在 `/var/log/sa/` 目录中，运行 `sar` 就能知道所有过去时间每个小时运行情况。另外可以写一个命令到一个文件中，把这个文件设置为 755 的执行权限，放在 `/etc/cron.hourly` 目录中，这样我们管理 BBS 服务器就很容易了。

以下是操作过程：

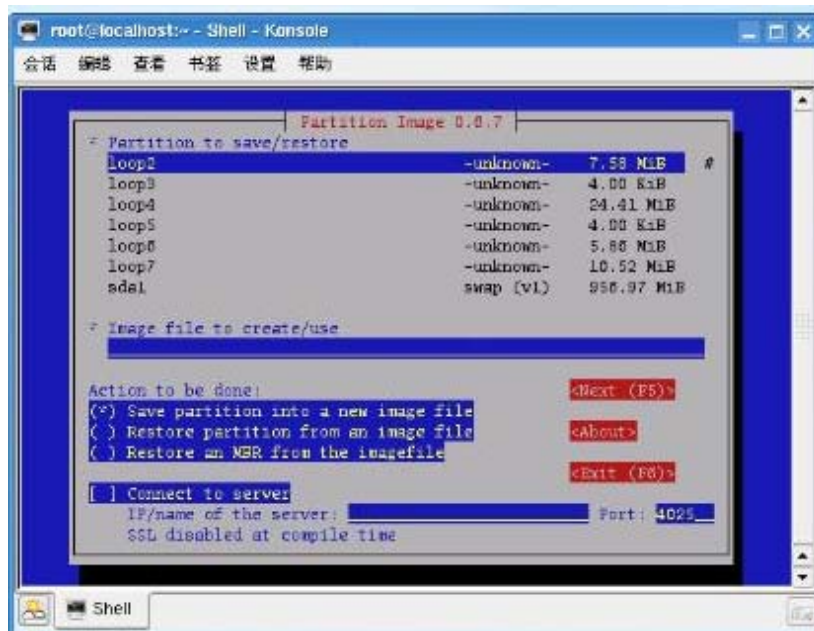
```
#cd /etc/cron.hourly/ 进入目录
# touch sa1ho 创建文件，这个文件名可以自己来命名
# chmod 755 sa1ho
```

然后在这个文件中写入下面的一行 `/usr/local/lib/sa/sa1&`
这样每一个小时，就有日志文件写入 `/var/log/sa/` 目录中了，当然还有一个 `/usr/local/lib/sa/sa2` 的命令，也可以写一个文件到 `/etc/cron.weekly/` 目录中。

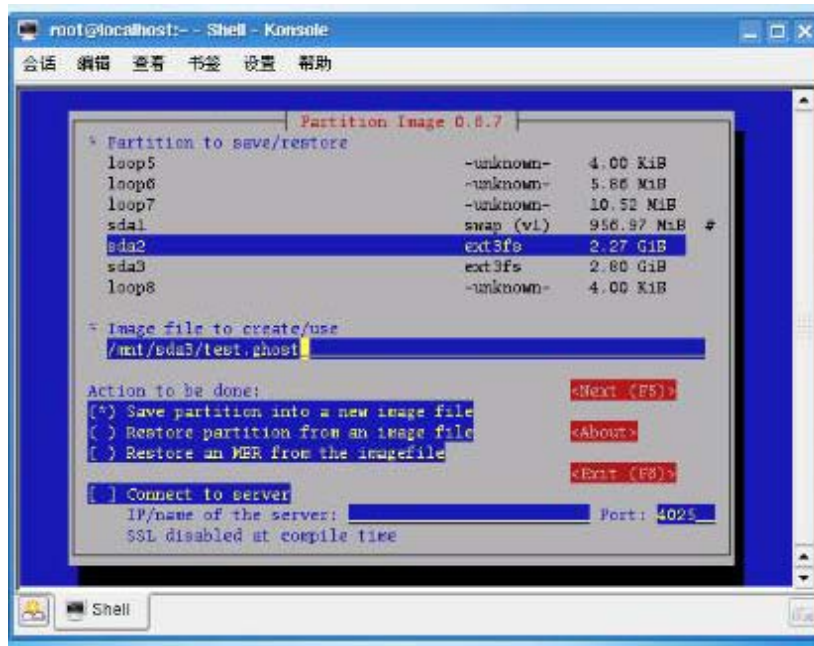
7.2.4 partimage

对于 `partimage` 问题描述，我们在安装时候有个库文件缺失，而系统有个比这个软件所需的更新的库文件，由于缺失就不能安装，所以在装的时候将 `newt.0.51` 强制安装。之后就能装上 `partimage`。

对于一个 BBS 服务器系统来说，及时地备份硬盘上的数据是很重要的。我们结合了 BBS 服务器的实例，在终端运行 `partimage`，来进行硬盘备份。我们的磁盘分区是这样的，一个 2.27G 的主分区 (`sda2`)，一个 1G 的交换分区 (`sda1`)，一个 2.8GG 的空盘 (`sda3`)。要备份的是主分区里面的内容。里面的一个 `ubuntu` 的 `desktop cd` 版的 `linux` 系统。



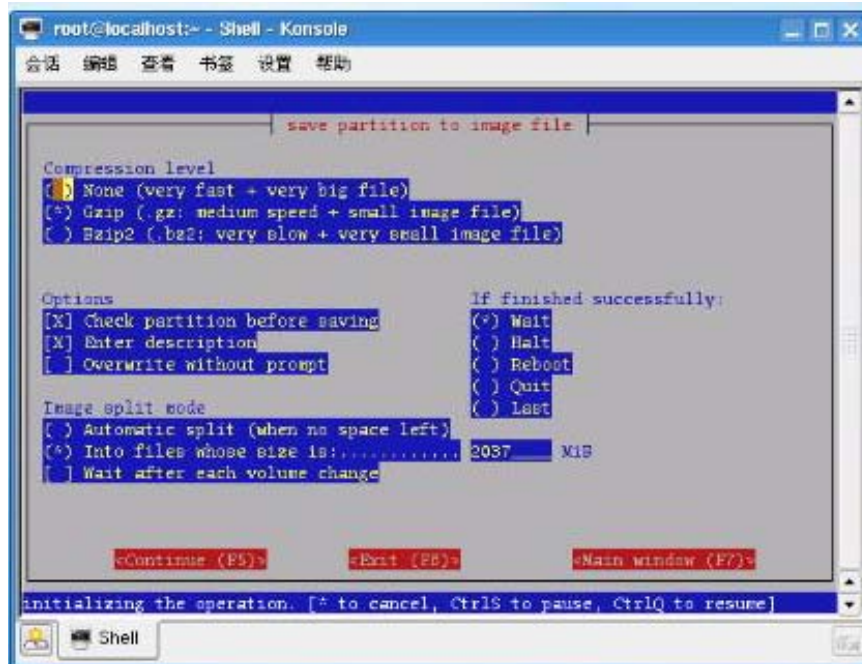
选择你要克隆的分区 (`sda2`)，在 `Image file to create/use` 填入你的克隆文件存放地点



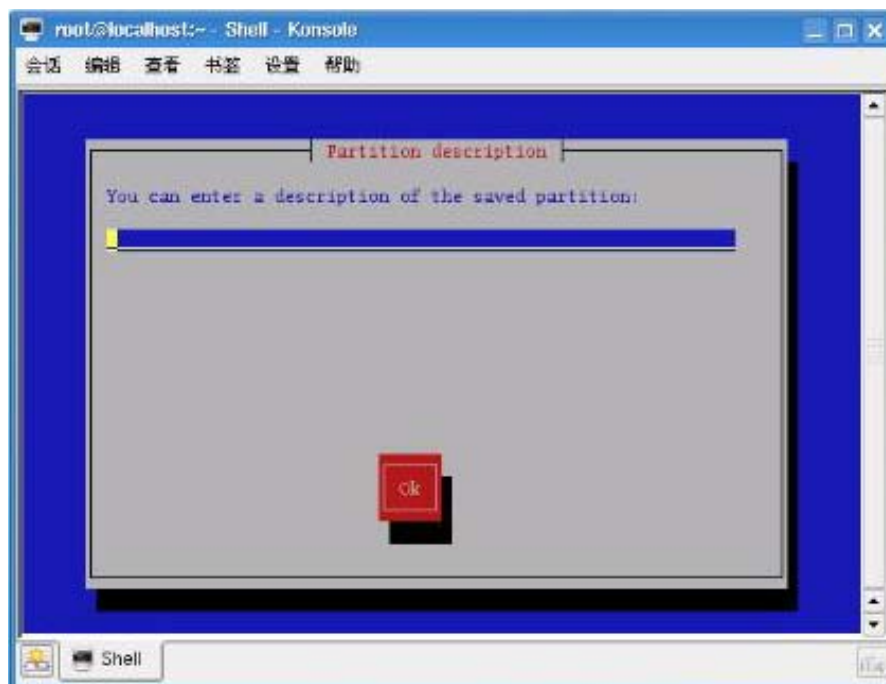
F5 下一步
如果出现这样的画面



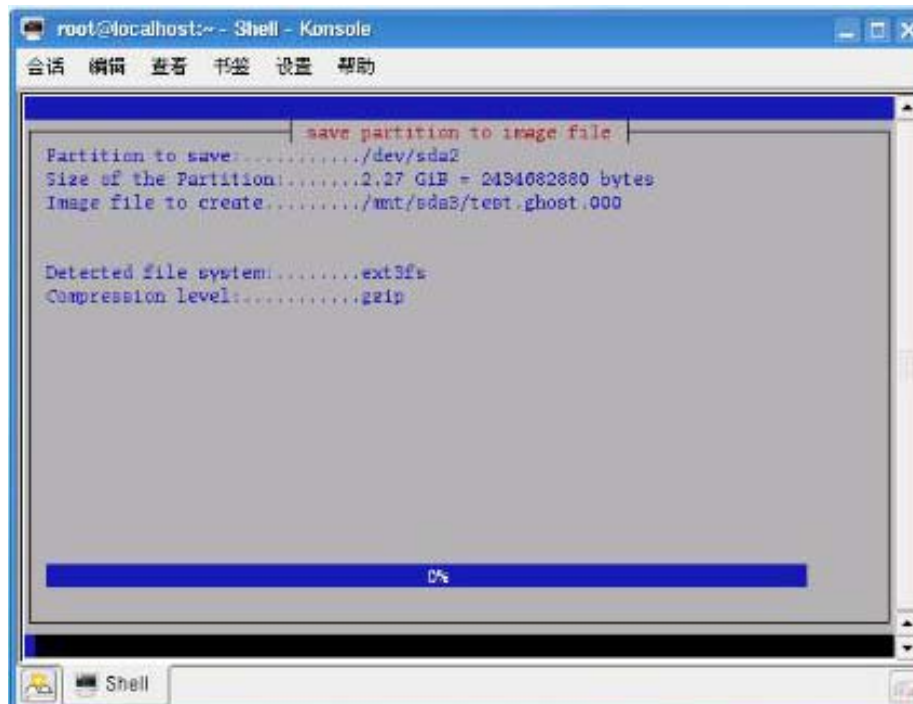
那么先退出，用 `umount` 命令将 `sda2` 卸载了。然后再开始。
如果已经 `umount` （`umount /mnt/sda2`）好了，将会看到下面的画面。



其中的选项默认就行，也可以根据需要修改。我的是默认按 F5 下一步



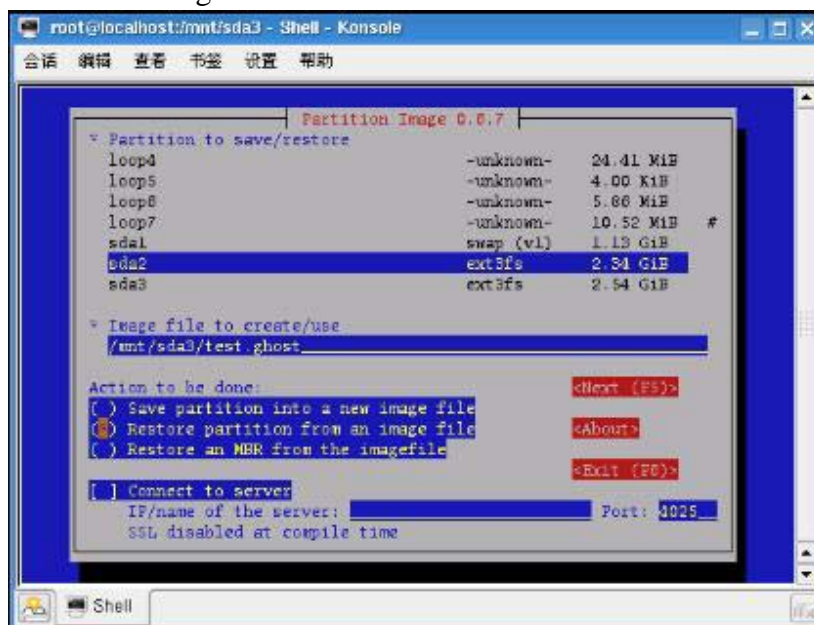
输入对这个克隆的描述。随便，不输也行。
输好了按 Enter.



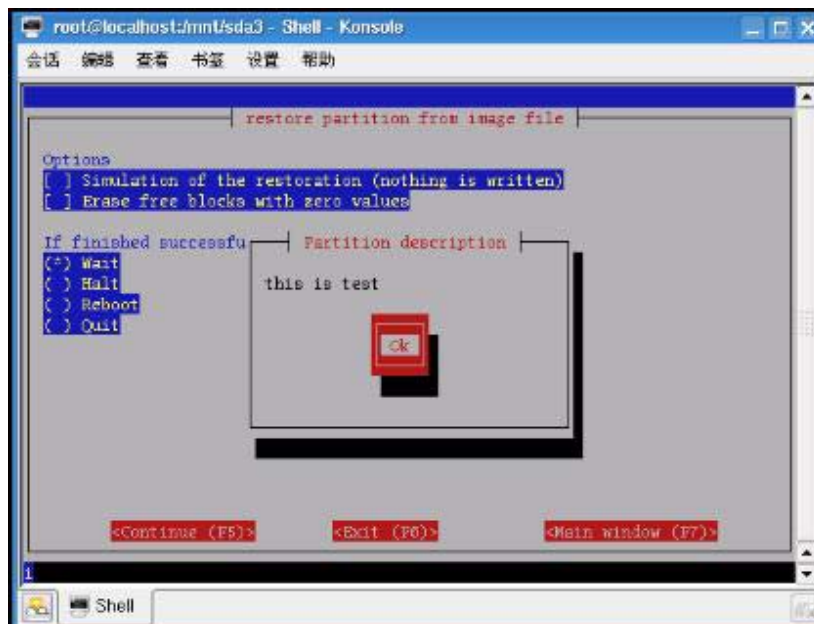


利用 partimage 的 ghost 还原功能

同样运行 partimage，我把 ghost 文件拷到了 sda3 中，所以选择的路径就是 /mnt/sda3/test.ghost

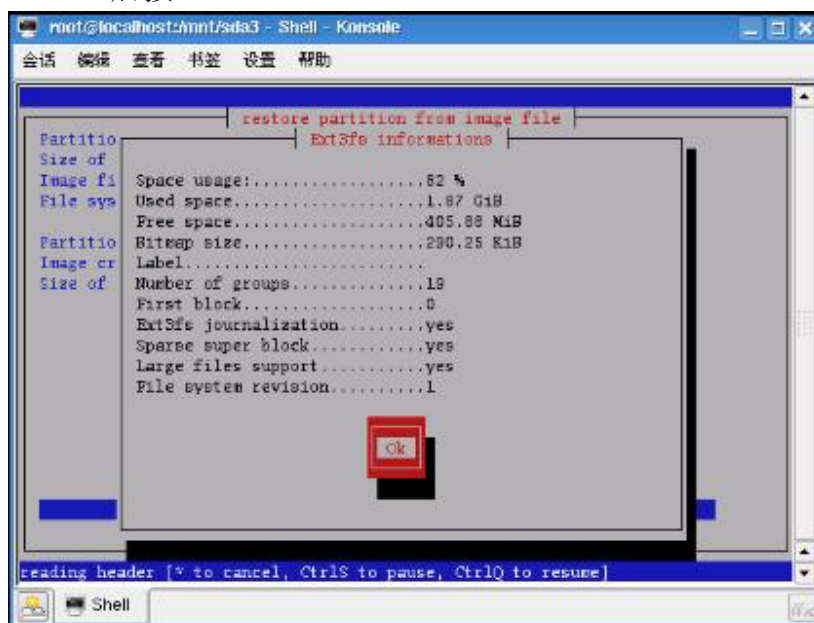


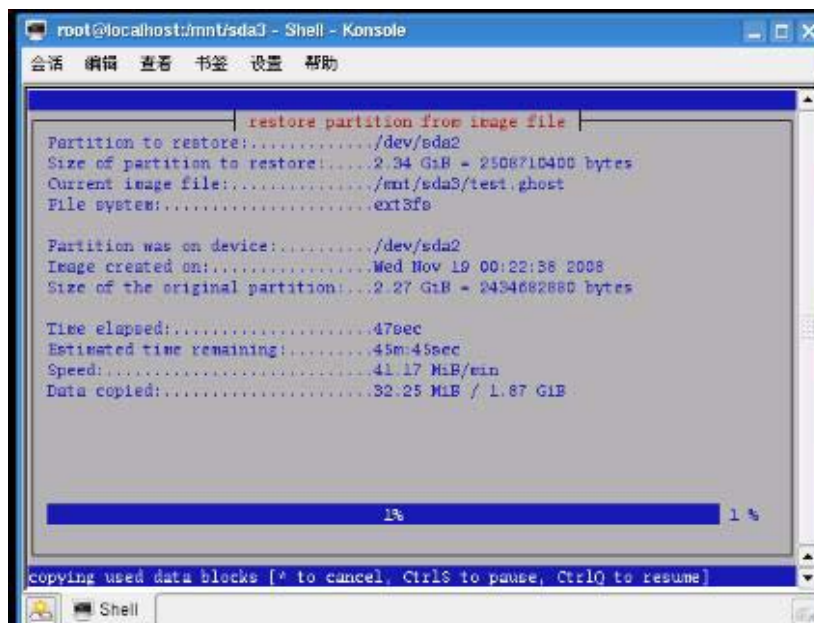
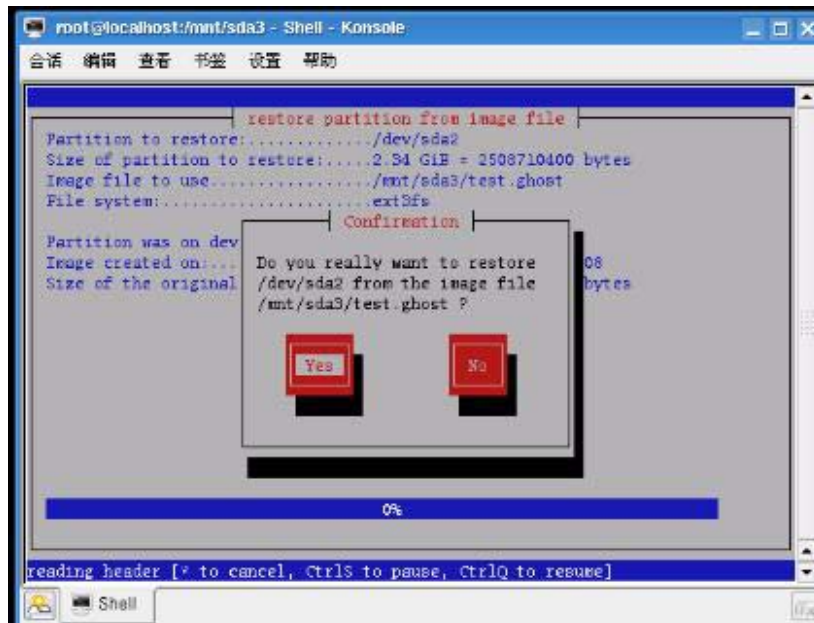
选择 Restore partition from an image file.F5 下一步,同样 sda2 要先 umount



出现的文字是我们创建时候对它的描述。

OK 后按 F5







7.3 安全防护模块

在 liveCD 中我们应用了带有 MySQL 数据库的 SNORT 模块构成了带有入侵检测功能的安全防护模块。

安装:

1. 安装 libpcap-1.0.0


```
tar -xzf libpcap-1.0.0.tar.gz
cd libpcap-1.0.0
./configure
make
make install
```
2. 安装 snort-2.8.3.1


```
建立 snort 配置文件和日志目录
mkdir /etc/snort
mkdir /var/log/snort
tar -zxvf snort-2.8.3.1.tar.gz
cd snort-2.8.3.1
./configure
make
make install
```

下载地址: <http://www.tcpdump.org/>
<http://www.snort.org/dl/>

```
root@localhost:usr/local/src/php-4.4.9 - Shell - Konsole
会话 编辑 查看 书签 设置 帮助

S5 G 2: 0      (0.000%)
Total: 0
=====
Action Stats:
ALERTS: 0
LOGGED: 0
PASSED: 0
=====
Snort exiting
[root@localhost php-4.4.9]# snort -v
Running in packet dump mode

--- Initializing Snort ---
Initializing Output Plugins!
Verifying Preprocessor Configurations!
***
*** interface device lookup found: eth0
***

Initializing Network Interface eth0
Decoding Ethernet on interface eth0

--- Initialization Complete ---

o*~ -> Snort! <*-
o*~)~ Version 2.8.3.1 (Build 17)
      By Martin Roesch & The Snort Team: http://www.snort.org/team.html
      (C) Copyright 1998-2008 Sourcefire Inc., et al.
      Using PCRE version: 6.6 06-Feb-2006

Not Using PCAP_FRAMES

Not Using PCAP_FRAMES
*** Caught Int-Signal
Run time prior to being shutdown was 1.945584 seconds
=====
Packet Wire Totals:
Received:      0
Analyzed:      0 (0.000%)
Dropped:       0 (0.000%)
Outstanding:   0 (0.000%)
=====
Breakdown by protocol (includes rebuilt packets):
  ETH: 0 (0.000%)
  ETHdisc: 0 (0.000%)
  VLAN: 0 (0.000%)
  IPv6: 0 (0.000%)
  IPv6 EXT: 0 (0.000%)
  IPv6opts: 0 (0.000%)
  IPv6disc: 0 (0.000%)
  IP4: 0 (0.000%)
  IP4disc: 0 (0.000%)
  TCP 6: 0 (0.000%)
  UDP 6: 0 (0.000%)
  ICMP6: 0 (0.000%)
  ICMP-IP: 0 (0.000%)
  TCP: 0 (0.000%)
  UDP: 0 (0.000%)
  ICMP: 0 (0.000%)
  TCPdisc: 0 (0.000%)
  UDPdisc: 0 (0.000%)
  ICMPdis: 0 (0.000%)
  FRAG: 0 (0.000%)
```

配置使用:

主要是安装规则和配置文件, 步骤如下:

1、cd rules (在 snort 安装目录下)

```
cp * /etc/snort
```

```
cd /etc
```

```
cp snort.conf /etc/snort
```

```
cp *.config /etc/snort
```

2、修改 snort.conf(/etc/snort/snort.conf)

```
var HOME_NET 10.2.2.0/24
```

```
var RULE_PATH ./rules 修改为 var RULE_PATH /etc/snort/
```

工作模式

Snort 可以工作在 3 种工作模式, 分别如下:

1) 嗅探器 sniffer:

命令: snort -v [-d][-X]

Snort 使用 Libpcap 包捕获库, 即 TCPDUMP 使用的库。在这种模式下, Snort 使用网络接口的混杂模式读取并解析共享信道中的网络分组。BPF 表达式可用来过滤流量。

-v verbose

-d 转储应用层数据

-X 转储从链路层开始的原始包

2) 分组日志模式

命令: snort -l dir [-h hn][-b]

这种模式下以 ASCII 格式记录解析出的分组。

-l directory snort 将把日志放在这个目录下

-h X.X.X.X 设置本地子网号

-b 日志使用 TCPDUMP 二进制格式

3) 入侵检测模式

命令: snort -c snort.conf [-l dir]

必须载入规则库才能进入入侵检测模式。即

#./snort -c snort.conf

snort 将报警信息放入/var/log/snort 目录下, 可以用-l 选项来改变目录。

当我们采用入侵检测模式时, 必须载入规则库才能进行检测, 载入规则库后, snort 网络数据和规则集进行模式匹配, 从而检测可能的入侵企图。Snort 规则库是不断更新的, 可以在 www.snort.org 上下载到最新的 snort 规则库。snort 使用一种简单的轻量级的规则描述语言来描述 它的规则配置信息, 它灵活而强大。通过对特征规则以及网上资料的分析, 发现对于特征字段, 运行攻击代码时用 ethereal 或其它 sniffer 工具来截获数据包, 然后根据数据包的解码内容, 来分析特征字段, 然后书写 snort 的规则。在《用 Snort 从原理上检测 MS05-051 攻击》一文中, 可以看出, snort 主要是用 ethereal 截获数据包后, 提取匹配的要害, 然后用 snort 中的关键字来书写规则, 这样就得到了 snort 的特征规则。

7.4 其他常用工具模块

由于 liveCD 的各个模块都涉及到网络服务, 所以我们也集成了常用的网络工具, 像 apache samba ftp nfs 等等。另外, 为了用户的简洁使用性, 我们将红旗的图形化界面工具也加入到 livecd 中。由于 apache 和 MySQL 在前面应用中已经有所涉及, 下面只对 gFTP 进行一下简单介绍。

gFTP是X Window下的一个用Gtk开发的多线程FTP客户端工具。gftp官方网站 <http://www.gftp.org/>。它与主要有以下一些特性:

1. 支持 FTP, HTTP、HTTPS、SSL和 SSH 协定, 支持ftp/http代理传输支持;
2. 支持 FXP 文件传输 (在两个 ftp server 间传输文件);
3. 允许多文件传输下载伫列;
4. 支持下载整个目录和文件;
5. 有书签选单让使用者可以快速选取远端;
6. 支持断点续传;
7. 支持远端目录快取;

8. 支持拖曳文件，即Drag and Drop;
9. 支持FTP 和 HTTP 代理服务器；
10. 允许 passive 或是 非 passive 文件传输；
11. 全目录下载；
12. SSH连接和数据传输

由于 gFTP 支持多种协议，为了更加安全可以把 SSH 协议作为默认协议，通过使用 SSH，可以把所有传输的数据进行加密，而且能够防止 DNS 欺骗和 IP 欺骗。使用 SSH，还可以将传输的数据压缩，所以可以加快传输的速度。SSH 可以为 FTP 提供一个安全的“通道”。

SSH 最常见的应用就是，用它来取代传统的 Telnet、FTP 等网络应用程序，通过 SSH 登录到远方机器执行你想进行的工作与命令。在不安全的网路通讯环境中，它提供了很强的验证（authentication）机制与非常安全的通讯环境。

这样通过配置了 SSH 的 gFTP，该 liveCD 可以提供安全 ftp 下载和 ssh 安全远程访问。

8、相关技术比较和分析

BBS 论坛是有相同的兴趣爱好的人进行讨论的平台，是人们应用互联网络进行学习，经验交流的很好的方式。随着计算机硬件价格的下调，各种软件的普及，建立一个 BBS 论坛不再是件难事。然而随着互联网络规模的不断扩大，安全及硬盘数据备份问题也成为考验 BBS 服务器系统的主要方面。如果 BBS 论坛建设的爱好者们想快速建立起一个相对安全并且容易管理的 BBS 服务，我们这张 liveCD 即能给予最好的体验。

相对来说，在专业的 BBS 服务器上运行的系统要求的硬件配置高，软件配置专业，普通的 BBS 爱好者无法也没有必要采用。相对于其他专业的 BBS 论坛服务器系统，在减少成本的同时，我们这张 liveCD 更加简洁精悍，在提供最基本的 BBS 服务器模块的同时，也能够保证 BBS 论坛数据安全，因为我们能提供较好的系统维护和安全检测功能。所以说，我们这张 liveCD 是 BBS 建立爱好者首选。

9、 总结

本作品基于红旗 Asianux 3.0 构建系统平台，在系统安装过程中精简了大量不相关的功能模块和软件包，在精简过的系统安装了自己定制的工具和软件。无需在硬盘上安装即可直接从光驱启动的系统，通过内存虚拟硬盘可以提供 BBS 服务、系统维护和入侵检测等功能，具有简单、安全、功能全面的特点。

在制作该 liveCD 的过程我们发现，Asianux 3.0 是一个不错的开发平台，我们在开源社区中找到的开源软件基本都能安装上，遇到的问题不是很多，另外安装配置界面也比较人性化。在这个优秀的平台上，我们的一些想法才得以实现。

最后，我们要对“红旗杯”的主办方——中国电子商务协会与北京中科红旗软件技术有限公司表示衷心的感谢，正是因为有这个竞赛才使得我们得到一个展示自己、锻炼能力的平台。此外，我们还要感谢北京交通大学两位老师的悉心培

训和指导，使我们在竞赛过程中学到了很多关于操作系统和开源技术的知识。另外，作为一个团队，在竞赛过程中培养出的合作和沟通的团队精神，也使我们今后受益匪浅。