Советы по Slackware

v. 0.1
Автор: Джэк С. Лэй
Перевод: Денис Каледин
Дата последнего обновления: 11/04/02

Эта информация была тщательно собрана мной из разных источников в один документ для того, чтобы помочь мне (и, быть может, другим) настроить систему после установки с нуля. Также эти заметки укажут Вам путь к источникам информации, позволяющим максимально обезопасить Вашу систему, в соответствии с Center for Internet Security.

Разумеется, осуществить вещи, описанные ниже, можно разными способами, но я предлагаю Вам ознакомиться с моим подходом.

«Спросите 8 Slack'еров, как что-то сделать, и получите 10 ответов» - sl в alt.os.linux.slackware

Несколько слов об аппаратных устройствах. Мой компьютер с Slackware служит для firewall/NAT/IDS с двумя сетевыми устройствами. Одно из них – кабельный модем, другое – обычная Ethernet карта, ведущая к хабу. Хаб соединяет сервер с моей рабочей станцией, на которой установлены Slackware и Windows 98SE. Я загружаюсь под Windows, когда я разрабатываю Windows-приложения, также мне необходима контролируемая безопасная среда, отсюда – Slackware Linux сервер.

Этот документ предназначен для пользователя Slackware начального уровня.

Перед тем как изучить данный документ, рекомендую прочитать…

«The Book, Книга»

Несмотря на то, что некоторые положения Slackware Linux Essentials устарели, она, так или иначе, содержит массу полезной информации для новичка в Slackware.

Инсталляция Slackware

Единственное, что я советую при инсталляции Slackware – отключите компьютер от сети до того момента, когда Вы будете уверены в безопасности Вашей системы.

Честно говоря, я слукавил – Мне нравится иметь возможность скачивать Slackware из Интернета и инсталлировать систему с жесткого диска. (инсталлировать с заранее монтированной директории, либо через NFS) (спасибо Патрику Волкердингу и его Slackware)

Пост – инсталляционные заметки

Итак, Вы только что инсталлировали Slackware и зашли в систему как root. Что теперь? Вашей системе требуется небольшой тюнинг. В частности, укрепление защиты от взлома, настройка периферийного оборудования, и, быть может, настройка системы под конкретного пользователя, т.е. под Вас.

Чтение почты пользователя root
Иные источники информации
Создание логов
Настройка среды пользователя
Обеспечение безопасности Slackware
Firewall
Мониторинг безопасности (или IDS)
Примочки – в зависимости от конфигурации Вашей системы они могут либо работать, либо нет

- **Включаем IDS для динамических IP адресов**
- **Пишем скрипты для IP адресов**
- **Синхронизируем время на Вашем компьютере**
- **Монтируем Windows разделы для полномерного чтения/записи**
- **Конфигурируем Xfree86**
- **Переключаемся из Xfree86 в консоль и обратно**
- **Ежедневно запускаем проверку безопасности системы**
- **Интегрируем MyNetWatchMan/Snort**
- **Добавляем учетную запись пользователя для доступа к аудио системе**
- **Включаем Numlock**
- **Изменяем загрузочный уровень (загрузка в графическую оболочку)**
- **Настраиваем принтер**
- **Настраиваем CD-RW привод**
- **О ядре**
- **Инсталлируем исходники нового ядра**
- **Компилируем новое ядро**
- **Заплатки к ядру**
- **LILO и boot_message.txt**
- **Создаем новый загрузочный диск**
- **Изучаем уровни начальной загрузки**
- **Коллективный доступ в Интернет**
  - **-Включаем Dial-on-Demand**
  - **-Отключаем связь с Интернетом**
  - **-Используем кабельный модем**
- **Принудительная проверка файловой системы при загрузке**
- **Повторный старт IDS при изменении IP адреса с помощью dhcpcd**
- **Включаем поддержку Java в браузерах**

Чтение почты пользователя root

Итак, вероятно Вы желаете прочитать письмо Патрика Волкердинга, посланное Вам, т.к. оно содержит полезную информацию о настройке. В таком случае, выполните команду mail (или иную почтовую программу). Первое сообщение будет о регистрации в http://counter.li.org/ (счетчик пользователей Linux). Нас же пока интересует второе письмо, т.к. связи с Интернетом у нас пока нет, и даже если бы она у нас была, доступ в Интернет под root'ом – не самая лучшая идея.

Если Вы желаете последовать советам Патрика, можете оставить его письмо открытым на терминале и занятьсЯ другими вещами на остальных терминалах. Slackware инициализирует 6 виртуальных терминалов, доступных нажатием клмбинации клавиш <Alt><F1-F6>. Первоначально, находясь на первом терминале (F1), перейдите во второй

терминал нажатием <Alt><F2>, войдите в систему и выполняйте любые действия, по мере надобности переключаясь между терминалами. Когда Вы прочтете письмо Патрика и выйдете из почтовой программы, письмо будет сохранено в /root/mbox (в случае использования программы mail и некоторых других). Вы можете просмотреть его (равно как и любой другой файл) процедурой “less mbox”. Для начала убедитесь, что Вы находитесь в директории /root (если Вы только что вошли в систему, так и будет) с помощью команды “cd”. Затем введите “less mbox” и нажмите Enter. Передвижением вверх/вниз по документу служат клавишы курсора, для выхода нажмите “q”.

Теперь, когда Вы знаете где найти информацию, пойдем дальше.

Иные источники информации

Несмотря на то, что я не советую Вам подключаться к Интернету пока безопасность Вашей системы не находится на должном уровне, ниже приведены ссылки на дополнительные источники информации.

Сначала попробуйте найти ответ на интересующий Вас вопрос сами, т.к. более чем вероятно, что подобный вопрос задавался ранее не раз и ответ на него можно найти через легкодоступные источники информации, такие как man, info, /usr/doc/…, либо с помощью поисковой системы google. Если Вы не можете найти ответ, или не можете толком понять предложенные ответы и Вам требуется разъяснение, то вне зависимости от того, где Вы хотите задать Ваш вопрос, взгляните сначала на то, как следует задавать вопросы. При правильной постановке вопроса, шансы получить вопрос возрастают.

И мало что может сравниться с чувством удовлетворенности от того, что Вы нашли ответ сами….быть может я опять лукавлю.

Сайты Slackware (кроме http://www.slackware.com/)

ЧаВо группы новостей Slackware
alt.os.linux.slackware FAQ
Общая информация
http://userlocal.com/.
Информация о скачивании
Wild Wizards Slackware Mirrors
Группы новостей

alt.os.linux.slackware

alt.linux.slakware

Linux

The Linux Documentation Project

linuxnewbie.org

alt.linux* (linux news groups)

alt.os.linux* (linux news groups)

comp.os.linux* (linux news groups)

comp.windows.x.kde, etc...

Создание логов

Лог (журнал) всех изменений системы может прийтись очень кстати в случае фатального сбоя системы (поломка жесткого диска, к примеру), а также когда Вы просто хотите просмотреть все внесенные изменения после инсталляции. Рекомендуется регулярно сохранять лог на внешнем носителе (дискете, CD-RW диске, файле в сети, т.д.).

С помощью любого текстого редактора (я использую “mcedit” из пакета Midnight Commander в slackware/ap) создайте файл в директории /root под названием “install.log”. Я предпочитаю создавать файл dolog в директории /usr/local/sbin следующим образом:

"mcedit /usr/local/sbin/dolog"

```
#!/bin/bash
mcedit /root/install.log
```

После того, как Вы сохраните файл, сделайте его запускаемым командой "chmod +x /usr/local/sbin/dolog". Теперь у Вас есть возможность вызывать “dolog” в любое время под root’ом.

Настройка среды пользователя

Под этим я понимаю внесение изменений в интерфейс командной строки. Также, в случае если Slackware в будущим внесет изменения в эти настройки, изменяя файл /etc/profile , я не хочу делать эту работу заново. Поэтому сначала я создаю файл “mystuff.sh” в /etc/profile.d. Файл /etc/profile выполнит все исполняемые файлы в данной директории, которые содержат расширение, свидетельствующее о том, что используется оболочка(shell). Например, если оболочка /bin/bash или /bin/sh, все файлы с расширением “.sh” будут исполнены. Находясь в системе как root, выполните "mcedit /etc/mystuff.sh"

```
#!/bin/bash
# My stuff

# Following variable used in PS1
export TTYNR=`tty`
export TTYNR=${TTYNR:8}
# Use mcedit to modify files, vice "vi"
export VISUAL=/usr/bin/mcedit

if [ `id -u` = "0" ]; then
```

```
# root - display current time, machine network name, terminal logged in on, and
prompt in red
PS1="\[\033[1;31m\[\t \h$TTYNR:\w\$\[\033[0m\]"
else
# Not root - display current time, machine network name terminal logged in on,
and prompt in yellow
PS1="\[\033[1;32m\[\t \h$TTYNR:\w\$\[\033[0m\]"
fi

export PS1

# get rid of annoying beep:
setterm -bfreq 0

# Setup my alias's
alias dir="ls -l"
alias li="dir|less"
alias cls="clear"
alias see="links"
alias startx="startx -- -dpi 100"
alias df="df -h"
alias ckmd5="md5sum -c CHECKSUMS.md5 | grep -v OK"
alias gpgd="gpg --decrypt"
alias ping="ping -c 1"
```

После того, как Вы сохраните файл, сделайте его запускаемым командой "chmod +x /etc/profile.d/mystuff.sh". Теперь он будет запущен при каждом входе в систему.

Для получения общих сведений о файловых системах, прочтите System Overview и System Startup.

Обеспечение безопасности Slackware

Безопасноть. Какое понятие! Безопасность основана на доверии. В случае с компьютерами, она основана на Вашем доверии к людям, использующим Вашу систему или ее сервисы и доверии к программному обеспечению, установленном на ней. Является ли компьютер без запущенных на нем сервисов безопасной системой? Теперь у Вас есть доступ в Интернет. Вы только что нашли лазейку в Вашей системе безопасности. Плохо ли это? Я не знаю. Только что вы доверились Интернет-браузеру, который используете. Вы доверяете вашему провайдеру. Вы доверились firewall'у. Вы доверяете веб-сайту, который посещаете. Улавливаете, к чему я клоню?

Основные аксиомы безопасности

- ничего не предполагайте, никаких допущений
- не доверяйте никому, не верьте ничему
- ничто не безопасно
- безопасность – это компромисс с удобством использования
- параноя – Ваш друг

Для того чтобы система выполняла Ваши задачи, Вам требуется немного доверия. Вам решать.

Итак, Вы хотите обезопасить свою систему. Заметьте, что это зависит в основном от Ваших предпочтений и от тех сервисов, которые Ваша система будет выполнять. Этот раздел описывает настройку безопасности изолированной системы, имеющей доступ в Интернет и предоставляющей физический доступ только тем, кому Вы доверяете. Собственно говоря, я не буду останавливаться на физической безопасности системы. Оставлю это Вам.

Информация этого раздела предоставляется как есть. Следуя этим инструкциям, вы не получите абсолютно безопасную систему. Вы получите систему, более безопасную, нежели чем система сразу после установки Slackware.

Если Вы последуете советам Джеффри Дентона по укреплению безопасности системы, у Вас будет довольно надежная система.

Еще один ресурс о пост-инсталляционной настройке безопасности Хэнка Лейнингера дляч Slackware 8.0 и 8.1.

Если Вас интересуют добавочные источники по настройке безопасности, посетите: LinuxSecurity.com

Другие изменения/модификации/добавления:

Выполнять команды “at” и “cron” должен иметь возможность только root:
rm /etc/at.deny
echo root > /etc/cron.allow
echo root > /etc/at.allow

Внизу приведена модифицированная версия инструкции по укреплению безопасности системы.

Скопируйте эти строки и вставьте их в /root/chmod.dat

```
chmod 750 /bin/mt-st
chmod 600 /etc/at.allow
chmod 600 /etc/cron*
chmod 600 /etc/ftpusers
chmod 600 /etc/hosts.allow
chmod 600 /etc/hosts.deny
chmod 600 /etc/inetd.conf
chmod 600 /etc/inittab
chmod 600 /etc/lilo.conf
chmod 600 /etc/login.defs
chmod 600 /etc/securetty
chmod 600 /etc/suauth
chmod 440 /etc/sudoers
chmod 600 /etc/syslog.conf
chmod 750 /sbin/badblocks
chmod 750 /sbin/debugfs
chmod 750 /sbin/depmod
```

chmod 750 /sbin/dumpe2fs
chmod 750 /sbin/explodepkg
chmod 750 /sbin/fdisk
chmod 750 /sbin/fsck
chmod 750 /sbin/fsck.ext2
chmod 750 /sbin/fsck.minix
chmod 750 /sbin/ftl_check
chmod 750 /sbin/ftl_format
chmod 750 /sbin/halt
chmod 750 /sbin/hwclock
chmod 750 /sbin/ifconfig
chmod 750 /sbin/ifport
chmod 750 /sbin/ifuser
chmod 750 /sbin/init
chmod 750 /sbin/insmod
chmod 750 /sbin/installpkg
chmod 750 /sbin/isapnp
chmod 750 /sbin/killall5
chmod 750 /sbin/lilo
chmod 750 /sbin/makepkg
chmod 750 /sbin/mke2fs
chmod 750 /sbin/mkfs
chmod 750 /sbin/mkfs.minix
chmod 750 /sbin/mkdosfs
chmod 750 /sbin/mkraid
chmod 750 /sbin/mkswap
chmod 750 /sbin/modinfo
chmod 750 /sbin/pkgtool
chmod 750 /sbin/pnpdump
chmod 750 /sbin/removepkg
chmod 750 /sbin/rpc.portmap
chmod 750 /sbin/quotaon
chmod 750 /sbin/rdev
chmod 750 /sbin/runlevel
chmod 750 /sbin/setserial
chmod 750 /sbin/swapon
chmod 750 /sbin/tune2fs
chmod 750 /sbin/upgradepkg
chmod 750 /sbin/uugetty
chmod 750 /usr/bin/eject
chmod 4750 /usr/bin/gpasswd
chmod 750 /usr/bin/lpq
chmod 750 /usr/bin/lprm
chmod 4750 /usr/bin/lpr
chmod 750 /usr/bin/minicom
chmod 700 /usr/bin/nohup
chmod 700 /usr/bin/script
chmod 500 /usr/lib/news/bin/inndstart
chmod 500 /usr/lib/news/bin/startinnfeed
chmod 750 /usr/sbin/atd
chmod 750 /usr/sbin/atrun
chmod 750 /usr/sbin/crond

```
chmod 750 /usr/sbin/ctrlaltdel
chmod 750 /usr/sbin/dhcpd
chmod 750 /usr/sbin/dhcrelay
chmod 750 /usr/sbin/edquota
chmod 750 /usr/sbin/groupadd
chmod 750 /usr/sbin/groupdel
chmod 750 /usr/sbin/groupmod
chmod 750 /usr/sbin/grpck
chmod 750 /usr/sbin/grpconv
chmod 750 /usr/sbin/grpunconv
chmod 750 /usr/sbin/hdparm
chmod 750 /usr/sbin/imapd
chmod 750 /usr/sbin/in.comsat
chmod 755 /usr/sbin/in.fingerd
chmod 755 /usr/sbin/in.identd
chmod 750 /usr/sbin/in.talkd
chmod 000 /usr/sbin/in.rexecd
chmod 000 /usr/sbin/in.rlogind
chmod 000 /usr/sbin/in.rshd
chmod 750 /usr/sbin/in.telnetd
chmod 000 /usr/sbin/in.tftpd
chmod 750 /usr/sbin/in.timed
chmod 750 /usr/sbin/inetd
chmod 750 /usr/sbin/ipop3d
chmod 750 /usr/sbin/klogd
chmod 2750 /usr/sbin/lpc
chmod 740 /usr/sbin/lpd
chmod 550 /usr/sbin/makemap
chmod 750 /usr/sbin/mouseconfig
chmod 750 /usr/sbin/named
chmod 750 /usr/sbin/newusers
chmod 750 /usr/sbin/nmbd
chmod 750 /usr/sbin/ntpdate
chmod 750 /usr/sbin/ntpq
chmod 750 /usr/sbin/ntptime
chmod 750 /usr/sbin/ntptrace
chmod 750 /usr/sbin/pppd
chmod 750 /usr/sbin/pwck
chmod 750 /usr/sbin/pwconv
chmod 750 /usr/sbin/pwunconv
chmod 550 /usr/sbin/quotastats
chmod 750 /usr/sbin/rpc.bootparamd
chmod 750 /usr/sbin/rpc.mountd
chmod 750 /usr/sbin/rpc.nfsd
chmod 750 /usr/sbin/rpc.rusersd
chmod 750 /usr/sbin/rpc.rwalld
chmod 750 /usr/sbin/rpc.yppasswdd
chmod 750 /usr/sbin/rpc.ypxfrd
chmod 750 /usr/sbin/rpcinfo
chmod 750 /usr/sbin/showmount
chmod 750 /usr/sbin/smbd
chmod 750 /usr/sbin/syslogd
```

```
chmod 750 /usr/sbin/tcpd
chmod 750 /usr/sbin/tcpdchk
chmod 750 /usr/sbin/tcpdmatch
chmod 750 /usr/sbin/tcpdump
chmod 750 /usr/sbin/timeconfig
chmod 750 /usr/sbin/useradd
chmod 750 /usr/sbin/userdel
chmod 750 /usr/sbin/usermod
chmod 750 /usr/sbin/vipw
```

Теперь запустите его:

/bin/bash < chmod.dat

Поставьте защиту от записи на данные файлы:

```
/root/chattr.dat
chattr +i /etc/at.allow
chattr +i /etc/cron.allow
chattr +i /etc/exports
chattr +i /etc/hosts.equiv
chattr +i /etc/hosts.lpd
chattr +i /etc/inetd.conf
chattr +i /etc/lilo.conf
chattr +i /etc/login.access
chattr +i /etc/login.defs
chattr +i /etc/porttime
chattr +i /etc/protocols
chattr +i /etc/securetty
chattr +i /etc/services
chattr +i /etc/suauth
```

/bin/bash < /root/chattr.dat

Следующая модификация будет посылать все в /var/log/messages, чтобы иметь возможность просматривать записи в журнале одним анализатором (logcheck)

```
/etc/syslog.conf:
# /etc/syslog.conf
# Для справки о формате данного файла,  "man syslog.conf"
# и /usr/doc/sysklogd/README.linux.

# Раскомментируйте эту строчку чтобы видеть сообщения ядра на консоли
#kern.* /dev/console

# Записывать 'info' или  выше, но ниже, чем 'warn'.
# Кроме authpriv, cron, mail, и news. Они записываются в другом месте.
*.info;*.!warn;\
auth.none;authpriv.none;cron.none;mail.none;news.none  /var/log/messages
```

```
# Записывать 'warn' или выше.
# Кроме authpriv, cron, mail, и news. Они записываются в другом месте.
*.warn;\
auth.none;authpriv.none;cron.none;mail.none;news.none  /var/log/messages

# Информация об отладке хранится здесь.
*.=debug  /var/log/messages

# Запись сообщений частной аутентификации
authpriv.*;auth.* /var/log/messages

# Записи, связанные с Cron
cron.* /var/log/cron

# Записи, связанные с почтой
mail.* /var/log/maillog

# Сообщения об авариях посылать каждому пользователю.
*.emerg  *

# Записи ошибок news и uucp.
uucp,news.crit  /var/log/spooler

# Раскромментируйте эти строки, если вы хотите хранить все логи INN
# Если INN ( InterNet News daemon) не используется, они Вам не нужны
#news.=crit  /var/log/news/news.crit
#news.=err  /var/log/news/news.err
#news.notice  /var/log/news/news.notice
```

/etc/issue and /etc/issue.net

```
Welcome to \n.\o. \t with \U (\l).
```

Firewall

Firewall очень важен для всех, кто имеет доступ к Интернету. Firewall предотвращает большинство случайных и злонамеренных попыток подвергнуть риску Вашу систему. Помните, что компьютеры взламывали задолго до распространения высокоскоростных соединений, следовательно, если вы подключаетесь к Интернету через модем и телефонную линию, Вам также необходим firewall.

Slackware ищет исполняемый скрипт “rc.firewall” в директории /etc/rc.d/ и, если находит его, посылает ему команду “start” из /etc/rc.d/rc.inet2. Разумеется, этот скрипт может выполнять любые функции, но в основном он используется для обеспечения безопасности интерфейса, который инициализируется скриптом rc.inet1.

Firewall уникален для каждой системы и сервисов, которые она предоставляет. Соответственно, не все firewall-скрипты работают для любой ситуации.

Для изолированного компьютера с выключенными сервисами и имеющим модемный доступ к Интернету ниже приведен простой скрипт firewall, который должен вызываться из /etc/ppp/ip-up.

```
#!/bin/bash
# Удаляем все предыдущие правила
iptables -F
# Блокируем все попытки установить связь из Интернета
iptables -A INPUT -i ppp0 -p tcp --syn -j DROP
```

Ниже приведен довольно простой NAT (или маскарадный) набор правил firewall. Он может быть использован как для модемного соединения (вызван из /etc/ppp/ip-up) или как /etc/rc.d/rc.firewall
Вы можете прописать Ваш интерфейс (IFACE) и IP адрес (IFACEIP) явным образом или использовать нижеприведенный скрипт со скриптами в /usr/local/sbin: getppp0, geteth0, and geteth1.

----- Начало простого NAT firewall скрипта

```
#!/bin/bash
# приведите в соответствие с Вашим устройством доступа к Интернету
#IFACE="eth1"
case $IFACE in
ppp0)
IFACEIP=`getppp0`
;;
eth0)
IFACEIP=`geteth0`
;;
eth1)
IFACEIP=`geteth1`
;;
esac
# Удаляем все предыдущие правила
iptables -F; iptables -t nat -F; iptables -t mangle -F
# Изменяем адреса пакетов на Интернет адрес
iptables -t nat -A POSTROUTING -o $IFACE -j SNAT --to $IFACEIP
# Принимать пакеты с установленными соединениями или связанными с

# ними
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
# Принимать все новые соединения помимо Интернет интерфейса
iptables -A INPUT -m state --state NEW -i ! $IFACE -j ACCEPT
# Если они не приняты вышеуказанными правилами, отключить их
iptables -P INPUT DROP
# Не пересылать пакеты присланные из Интернета в Интернет
iptables -A FORWARD -i $IFACE -o $IFACE -j REJECT
```

----- конец скрипта.

Однако я параноик, и я вставил следующую строчку (которая вызывает мой firewall.init скрипт) в /etc/rc.d/rc.M прямо перед тем, как вызывается скрипт rc.inet1, включающий соединение через кабельный модем. Измените скрипт соответствующим образом.

./etc/rc.d/firewall.init

```
#!/bin/bash
/usr/sbin/iptables -F; /usr/sbin/iptables -t nat -F; /usr/sbin/iptables -t mangle -F
# Замените 1.2.3.4 на ваш IP адрес
/usr/sbin/iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 1.2.3.4

/usr/sbin/iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
/usr/sbin/iptables -A INPUT -m state --state NEW -i ! eth0 -j ACCEPT
/usr/sbin/iptables -P INPUT DROP
/usr/sbin/iptables -A FORWARD -i eth0 -o eth0 -j REJECT
```

Для общей информации, посетите Linux Newbie's Iptables Basics NHF

Официальный источник информации – веб-сайт netfilter

С LinuxSecurity.com, прочтите iptables-tutorial,firewalls, и security documentation.

Иные источники вдохновения - The Linux Documentation Project, LinuxGuruz, и, разумеется, поиск на freshmeat.net и google.com

Для тех, кто использует NAT - Firewall by Jim.

Дабы проверить Ваш firewall, зацените Gibson Research Corporation's ShieldsUP! Или детально просканируйте Вашу систему с помощью сканера портов (желательно с другого компьютера вне Вашей сети или изолированного компьютера) такого как nmap (см. пакет slackware/n/nmap...).

Мониторинг безопасности

Итак, можно считать, что Ваша система вполне безопасна. Теперь Вам необходимо использовать устройства мониторинга безопасности Вашей системы, дабы быть уверенным, что она остается безопасной.

Разумеется, Вы всегда должны обновлять Slackware из директории /patches с Вашего любимого зеркала Slackware. (см. Wild Wizards Slackware Mirrors) для Вашей системы.

Также, все используемые Вами программы должны регулярно обновляться, если в них обнаруживаются изьяны безопасности. Подписавшись на рассылку Slackware-Security, Вы будете в курсе. Рассылка оповестит тревожными сигналами о программном обеспечении, входящем в дистрибутив Slackware.

LinuxSecurity.com Позволит Вам шагать в ногу со временем

Рекомендуемые программы:
aide - База данных, следящая за изменениями в файлах
checkrootkit - Rootkit файловый сканнер

grsecurity – Патчи к ядру, укрепляющие безопасность (включая Buffer Overflow)
icmpinfo- интерпретирует сообщения ICMP (находится в оригинальном пакете Slackware n/tcpip)
iplog - TCP/IP логгер траффика
logsentry (logcheck) – Сканирует системные логи с целью выявления нарушения безопасности
mynetwatchman – Сообщения и ответ на вторжения
portsentry – Обнаружение вторжения по сети в реальном времени (IDS)
snort - Обнаружение вторжения по сети в реальном времени (IDS)
sXid - suid/sgid мониторинг

Примочки

Включаем IDS для динамических IP адресов

Psionic PortSentry 1.1 and 2.0b1 Beta не определяет локальный интерфейс автоматически, и я написал следующую процедуру:

Из /etc/rc.d/rc.inet2, сразу после вызова rc.firewall, вставьте следующие строки:

```
# Включаем опции безопасности
# Конфигурируем portsentry с текущим IP адресом eth0
#echo "Starting PortSentry"
/usr/local/psionic/portsentry2/doports
# Запускаем Portsentry
/usr/local/psionic/portsentry2/portsentry
```

----- Начало скрипта /usr/local/psionic/portsentry2/doports

```
#!/bin/bash
# Автор Jack S. Lai
cp /usr/local/psionic/portsentry2/top /usr/local/psionic/portsentry2/portsentry.conf
echo
'INTERFACE_ADDRESS="`geteth0`"'>>/usr/local/psionic/portsentry2/portsentr
y.conf
cat /usr/local/psionic/portsentry2/bottom
>>/usr/local/psionic/portsentry2/portsentry.conf
cp /usr/local/psionic/portsentry2/ignore
/usr/local/psionic/portsentry2/portsentry.ignore
echo "# Current local Internet address:" >>
/usr/local/psionic/portsentry2/portsentry.ignore
echo `geteth0` >> /usr/local/psionic/portsentry2/portsentry.ignore
echo "" >> /usr/local/psionic/portsentry2/portsentry.ignore
```

----- Конец скрипта

Примечание: /usr/local/psionic/portsentry2/top содержит 24 первые строчки файла portsentry.conf и bottom содержит остаток файла. Ignore - игнорируемые адреса (см. portsentry.ignore).

Это также можно использовать в переменной HOME_NET в snort.

Из /etc/rc.d/rc.inet2, сразу после вызова rc.firewall (или в Вашей секции Опций безопасности), вставьте следующие строки:

```
/etc/snort/dosnort
/usr/local/bin/snort -q -c /etc/snort/snort.conf -D &
```

----- Начало скрипта /etc/snort/dosnort

```
#!/bin/bash
# Автор Jack S. Lai
cp /etc/snort/snort.top /etc/snort/snort.conf
echo 'var HOME_NET '`geteth0`>>/etc/snort/snort.conf
cat /etc/snort/snort.bottom >>/etc/snort/snort.conf
```

----- Конец скрипта

Примечание: /etc/snort/snort.top содержит все до, но не включая строку, определяющую переменную HOME_NET из snort.conf и snort.bottom содержит все строки после нее.

Пишем скрипты для IP адресов

getppp0
/usr/local/sbin/getppp0:

```
#!/bin/bash
ifconfig ppp0 | awk '/inet/ { print $2 }' | awk -F ":" '{ print $2 }'
```

geteth0
/usr/local/sbin/geteth0:

```
#!/bin/bash
/sbin/ifconfig eth0 | awk '/inet/ { print $2 }' | awk -F ":" '{ print $2
}'
```

geteth1
/usr/local/sbin/geteth1:

```
#!/bin/bash
/sbin/ifconfig eth1 | awk '/inet/ { print $2 }' | awk -F ":" '{ print $2
}'
```

Синхронизируем время на Вашем компьютере

Зачем на точное время? Затем, чтобы когда расследуя или сообщая о проблеме безопасности, наши логи должны совпадать с логами нашего провайдера.

Создаем /etc/cron.daily/timecheck (Проверяем и обновляем время с AOL.com, который находится неподалеку от меня)

```
#!/bin/sh
/usr/sbin/ntpdate 205.188.185.33 /sbin/hwclock --systohc
```

Windows разделы

Этот вариант fstab разрешает ВСЕМ ПОЛНЫЙ ДОСТУП к Windows разделам. Не делайте этого, если полностью не доверяете Вашей системе или если она не изолирована.
/etc/fstab
/dev/hda1 /win98 vfat uid=500,gid=500,umask=000,exec,dev,suid,rw 1 0

Конфигурируем Xfree86

Прежде чем приступить к конфигурированию Xfree86, Вы должны знать частоту развертки монитора, тип мыши и видеокарты.

Выполните xf86config чтобы создать /etc/X11/XF86Config
/etc/X11/XF86Config

Для использования ТВ раскомментируйте строку 57 glx
Данные изменения улучшат качество шрифтов в программах типа Netscape
строка 82 перемещаем .../fonts/100dpi/ в начало списка
строка 83 перемещаем .../fonts/100dpi/:unscaled в начало списка, вторая сверху

Изменяем параметры мыши: (для обычной мышки с колесиком)
Option "Protocol" "IMPS/2"
Option "Device" "/dev/mouse"
Option "ZAxisMapping" "4 5"

Переключаемся из Xfree86 в консоль и обратно

После того, как Вы выполнили команду “startx” из загрузочного уровня 3 для загрузки сессии X Windows, Вы можете в любой момент вернуться в консоль командой <Ctrl><Alt><Fx>, где Fx - клавишы F1 – F5. Та консоль с которой Вы выполнили “startx” будет заблокирована, однако другие будут доступны. Для возвращения в Xfree86, нажмите <Alt><F7>, это номер /etc/inittab agetty respawn +1. Например, у меня настроены 11 виртуальных терминалов:

/etc/inittab:

```
<snip>
c1:1235:respawn:/sbin/agetty 38400 tty1 linux
c2:1235:respawn:/sbin/agetty 38400 tty2 linux
c3:1235:respawn:/sbin/agetty 38400 tty3 linux
c4:1235:respawn:/sbin/agetty 38400 tty4 linux
```

```
c5:1235:respawn:/sbin/agetty 38400 tty5 linux
c6:1235:respawn:/sbin/agetty 38400 tty6 linux
c7:1235:respawn:/sbin/agetty 38400 tty7 linux
c8:1235:respawn:/sbin/agetty 38400 tty8 linux
c9:1235:respawn:/sbin/agetty 38400 tty9 linux
c10:1235:respawn:/sbin/agetty 38400 tty10 linux
c11:12345:respawn:/sbin/agetty 38400 tty11 linux
<snip>
```

Я нажимаю <Alt><F12> для возвращения в сеанс X Windows. Не забудьте изменить /etc/securetty и /etc/porttime соответственно!

См. /usr/doc/Linux-HOWTOs/XWindow-User-HOWTO

Ежедневная проверка безопасности системы

mkdir /etc/cron.security (выполнять перед ежедневными задачами cron).
mcedit /etc/cron.security/security
----- Начало скрипта /etc/cron.security/security

```
#!/bin/bash
/usr/local/etc/logcheck.sh
/usr/bin/sxid
/usr/local/sbin/ckr | mail -s "Chkrootkit report from Oahu" jlai@kauai
/usr/local/bin/aide -C | mail -s "AIDE report from Oahu" jlai@kauai
```

---- Конец скрипта
chmod +x /etc/cron.security/security
cd /var/spool/cron/crontabs
crontab -e root
Добавьте что-нибудь подобное к следующей строчке

```
# Выполнять задачи безопасности cron ежедневно в 3:05 (перед logrotate):
05 3 * * * /usr/bin/run-parts /etc/cron.security 1> /dev/null
```

Chkrootkit

У меня пакет chkrootkit находится в /home/secure/chkrootkit. Директория /home у меня на отдельном разделе, что облегчает установку бета версий Slackware без потери личных файлов. /home/secure – директория, доступная только root'у. Для подготовки скрипта, я выполнил следующие шаги после читой установки и до того, как подключил систему к сети!

```
cd /home/secure/chkrootkit
md5sum ../md5.sum
./chkrootkit > ~/chbase
```

Затем я создал /usr/local/sbin/ckr:

```
#!/bin/bash
cd /home/secure/chkrootkit
echo "Checking..."
md5sum * > /root/ckr.sum
diff /home/secure/md5.sum /root/ckr.sum
./chkrootkit > /root/now
diff chbase /root/now
echo "Done."
```

Теперь, когда я выполняю команду “chk” md5sums из директории chkrootkit проверяются против основной системы, затем запускается chkrootkit и сравнивается с первоначальной загрузкой (внося корректировку вручную по мере необходимости). Различия высылаются мне по почте. Также проводится проверка подлинности новых пакетов.

Интегрируем MyNetWatchMan/Snort

Мой mynetwatchman perl agent включает в себя iptables, portsentry, и snort для IDS и мой /etc/mnwclient.rc выглядит следующим образом:

```
login <my login>
password <my password>
interface eth0
log /var/log/messages,/var/log/snort/alert.csv
chain attackalert, IPT, TCP
quiet
```

Файлы для примеров snort и mnwclient неверны, добавьте следующее в snort.conf (или snort.bottom):
output alert_csv: /var/log/snort/alert.csv
proto,timestamp,src,srcport,dst,dstport,icmptype,icmpcode

А вот и rc.mnwclient скрипт:

```
#!/bin/bash
# Автор Jack S. Lai - Submitted to MyNetWatchman.com
# Этот скрипт запускает, останавливает или выдает статус
# клиента MyNetWatchman для Slackware.
#
runcmd="/usr/sbin/mnwclient &"
success=0
noroot=1
badargs=65
noconfig=66
nomnw=67
if [ "$UID" != "$success" ]; then
echo "You must be root to use this program."
exit $noroot
fi
if [ -z "$1" ]; then
echo "Usage: `basename $0` start, stop, status"
```

```
exit $badargs
fi

if [ ! -f /etc/mnwclient.rc ]; then
echo "Cannot run MyNetWatchman client. Missing
/etc/mnwclient.rc"
echo " This file needs to be set with your
login/password,interface,"
echo " and alert name from /var/log/messages..."
exit $noconfig
fi

if [ -x /usr/sbin/mnwclient ]; then
mypid=$(pidof -x mnwclient)
if [ "$1" = "start" ]; then
if [ $mypid ]; then
echo "MyNetWatchman client is already running!"
else
/usr/sbin/mnwclient &
echo "MyNetWatchman client running..."
exit $success
fi
fi
if [ "$1" = "stop" ]; then
if [ $mypid ]; then
kill -TERM $mypid
echo "MyNetWatchman client stopped."
exit $success
else
echo "Can't stop. MyNetWatchman client not running!"
fi
fi
if [ "$1" = "status" ]; then
if [ $mypid ]; then
echo "MyNetWatchman running. Process = $mypid"
else
echo "MyNetWatchman is not running."
fi
exit $success
fi
else
echo "/usr/sbin/mnwclient is not executable! Aborting..."
exit $nomnw
fi
```

Добавляем учетную запись обычного пользователя

Создайте пользователя jlai с дополнительной группой sys (для доступа к звуковой системе)

adduser jlai

Включаем Numlock

Для того чтобы включить Numlock в консоли, добавьте следующие строки в /etc/rc.d/rc.local:

```
# Turn numlock on:
for tty in /dev/tty[1-6]; do
/usr/bin/setleds -D +num < $tty
done
```

Для того чтобы включить Numlock в Xfree86, следуйте инструкциям на Linux from Scratch.

Изменяем загрузочный уровень

По умолчанию в Slackware установлен третий загрузочный уровень, консольный режим. Вы можете изменить его на четвертый (графический) или любой другой, внеся изменения в /etc/inittab:

Измените 3 в строке id:3:initdefault на 4.

Если Вы просто хотите изменить текущий уровень на четвертый, выполните “KDM” иди “telinit 4” под root’ом.

Настраиваем принтер

В данном случае у Вас есть пространство для маневров. Разница будет заключаться в поддержке принтеров и качестве печати. Вы можете последовать советам Патрика Волкердинга в письме Вам, либо руководству mRgOBILIN’a, либо использовать UNIX Printing System (или CUPS) из директории slackware/extra. Более подробная информация о CUPS здесь http://www.cups.org/.

----Совет Патрика Волкердинга, цитата

«Много людей спрашивают меня, как настроить печать в Linux. По моему убеждению, лучший способ это настроить Apsfilter – систему, позволяющую выводить на печать файлы различных форматов (DVI, PS, PDF, text), посылая в буфер принтера командой “lpr”. Для этого выполните следующие шаги:

1. Убедитесь, что драйвер принтера загружается в /etc/rc.d/rc.modules. Это должно выполняться по умолчанию.
2. Установите программное обеспечение LPD. Это пакет “lprng” в секции A. Скорее всего он уже установлен на Вашей системе.
3. Рекомендуется установить и настроить подсистему TCP/IP, по крайней мере для loopback (закольцованный интерфейс). Пакет “tcpip” входит в состав секции N, а скрипт “netconfig” конфигурирует TCP/IP.

4. Apsfilter использует множество других фильтров и подразумевает, что они установлены. Установите "ghostscript" и "gnu-gs-fonts" из секции AP чтобы добавить Ghostscript, если Вы хотите печатать документы формата PostScript. Вам также необходимо установить пакет "libjpeg" из секции L для поддержки изображений JPEG. Если Вы хотите иметь возможность печатать файлы в формате DVI, по крайней мере установите стандартные пакеты TeX из секции T.
5. Установите пакет apsfilter. Этот пакет находится в секции A, если Вы делали полную установку, он у Вас уже инсталлирован. В противном случае, найдите пакет в директории ap и установите его: installpkg apsfilter-*.tgz
6. Перейдите в директорию /usr/share/apsfilter/ и запустите SETUP: ./SETUP

   Программа сделает необходимые записи в /etc/printcap и Вы готовы печатать. Теперь Вы можете использовать netatalk и Samba для того чтобы Mac и Windows компьютеры в Вашей сети могли использовать принтер, подключенный к компьютеру с Linux. »

----конец цитаты

А вот руководство mRgOBLIN'а опубликованное в alt.os.linux.slackware:

Руководство по настройке печати в Slackware Linux
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Автор: mRgOBLIN <mrgoblin at sastk dot org> 2002-03-13
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

-=Введение=-

Slackware Linux (в текущей версии 8.0) использует стиль печати BSD, который, в свою очередь, использует LPD. Большая часть Unix-программ используют формат Postscript, так что если Ваш принтер не поддерживает печать формата Postsscript, Вам понадобится фильтр для перевода формата Postscript в формат, распознаваемый Вашим принтером.

Slackware использует APSFilter (Slackware 8.0 поставляется с apsfilter-6.1.1 and Ghostscript version 5.50)

-=Как это работает?=-

Сначала убедитесь, что Ваш принтер подсоединен к компьютеру, и что ядро поддерживает порт, к которому он подключен. По умолчанию Slackware настраивает параллельный порт и принтер находится в /dev/lp0

Если Вы счастливый обладатель USB-принтера, посетите Linux USB Website (см. секцию Ресурсы ниже)

LPD также поддерживает принтеры последовательных портов и сетевые принтеры.

Выполните:
cat /proc/devices
для просмотра текущих устройств, Вы должны увидеть устройство "lp" в этом списке.

Итак, можно считать, что аппаратная часть настроена. Найдите и запишите все детали о Вашем принтере из базы данных http://www.linuxprinting.org/database.html (мы предполагаем, что печать еще не настроена)
Собрав эту информацию, Вы готовы настроить программное обеспечение принтера.

Для корректной работы принтера установите следующие пакеты:

lpr.tgz
ghostscr.tgz
gsfonts.tgz
a2ps.tgz
apsfilt.tgz
gs_x11.tgz (по желанию)

А также все драйверы и софт, указанные в базе данных. (ссылка выше)

-=Отдельные указания пользователям Slackware 8.0=-

По идее теперь Вы можете сразу перейти к установке APSFilter, однако если у Вас Slackware 8.0, необходимо выполнить предварительные шаги.

Многие сталкиваются с проблемами печати в Slackware 8.0. По моему мнению, это связано с тем, что APSFilter не заменяет запись lp в файле /etc/printcap, поставляемую в Slackware по умолчанию.

Чтобы исправить положение, просто удалите /etc/printcap:

rm /etc/printcap
or back it up like this
mv /etc/printcap /etc/my_orig.printcap

В случае если Вы уже неоднократно устанавливали APSFilter, удалите также директорию /etc/apsfilter:
rm -r /etc/apsfilter/*

Теперь можно идти дальше.

-=Настройка APSFilter=-

Под root'ом зайдите в директорию /usr/lib/apsfilter.
Выполните:
cd /usr/lib/apsfilter

Запустите программу установки:

./SETUP
(точка, слэш, и все заглавные буквы)

Если Вы уже не обновили Ghostscript, Вам инсталлятор предложит Вам это сделать. Если у Вас нет протоположной информации, просто продолжите установку.

Я советую Вам принять месторасположение файлов apsfilter, предлагаемое по умолчанию, в итоге вы попадете в главное меню. Выполните следующие шаги: выберите интерфейс, драйвер, размер бумаги, и разрешительную способность принтера.
Вам будет предложено напечатать пробную страницу, и когда вы останетесь довольны настройками, не забудьте о следующем:
(I) ==> Install printer with values shown above – инсталлировать принтер с вышеопределенными настройками. (повторите этот шаг, если у Вас несколько принтеров).
Это сохранит настройки.

Для того, чтобы изменения настроек подействовали, перезапустите lpd:

lpc restart all
and
lpc status

См. man lpc для получения более подробной информации

Немного везения – и можете смело печатать документы. Задание печати документа теперь посылается на Ваш принтер по умолчанию (lp). Если у Вас несколько принтеров, укажите иной (auto1, например) с помощью опции –P
lpr -Pauto1 somefile.file

Следующий шаг – прочтите Printing-Usage-HOWTO (см. секцию Ресурсы ниже)

-=Полезные команды=-

man <имя команды> для опций

lpr – основной инструмент печати документов

lpq – проверяет наличие заданий в буфере принтера

lprm – удаляет задания из буфера принтера

lpc – программа контроля принтера

-=Локальные ресурсы=-

/usr/doc/apsfilter-6.1.1/
/usr/doc/a2ps-4.13b/
/usr/doc/Linux-HOWTOs/Printing-HOWTO
/usr/doc/Linux-HOWTOs/Printing-Usage-HOWTO

-=Интернет-ресурсы=-

LinuxPrinting.org Website
http://www.linuxprinting.org/

Printing-HOWTO
http://www.linuxdoc.org/HOWTO/Printing-HOWTO/index.html

Printing-Usage-HOWTO
http://www.linuxdoc.org/HOWTO/Printing-Usage-HOWTO.html

Linux USB Website
http://www.linux-usb.org/

GNU Ghostscript Website
http://www.gnu.org/software/ghostscript/ghostscript.html

APSFilter Website
http://www.apsfilter.org/

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Конец файла.
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

---

Настраиваем CD-RW привод

Настройка моего резака IDE Yamaha CRW2100E прошла со свистом. Он у меня подключен как Secondary slave (или hdd), так что /etc/lilo.conf гласит:

append="hdd=ide-scsi" первая строка в /etc/lilo.conf (или в general section).

Соответственно, fstab, гласит:
/dev/sr0 /cdrw auto noauto,user,ro 0 0
указывает на директорию /cdrw для монтирования. (не нравится мне /mnt/cdrw).

Primary master = hda
Primary slave = hdb
Secondary master = hdc
Secondary slave = hdd

Для получения дополнительной информации см. CD-Writing-HOWTO.

О ядре

Инсталлируем исходники нового ядра

Другие дистрибутивы Linux предоставляют модифицированные версии ядер, и Вы можете наткнуться на совет не инсталлировать исходники нового ядра в /usr/src/linux. Однако, к Slackware это не относится. Если Патрик выпускает ядро в виде пакета (package), вы инсталлируете этот пакет (с помощью команды “installpkg”) и ядро будет помещено в /usr/src/linux-version с символической ссылкой, указывающей на /usr/src/linux.

Если же Вы скачали исходники с The Linux Kernel Archives распакуйте их в директорию /usr/src и создайте символическую ссылку..
cd /usr/src

tar xvzf /filepath/filename
ln -s linux-version linux (замените version на номер версии ядра)

Итак, исходники ядра установлены. Мы ведь хотели создать новое ядро, не так ли?

Компилируем новое ядро

Для успешной компиляции ядра нужно время и тренировка. Я так говорю, потому, что никак не получается скомпилировать ядро как надо с первого раза, но это мое сугубо личное мнение.

Преимущества, которые дает компиляция ядра, перевешивают все сложности, связанные с этим процессом. В вашем ядре будут только те опции, которые Вам действительно нужны, и размер его будет меньше, чем размер ядра, поставляемого Slackware по умолчанию.

Для начала создайте следующий файл в директории исходников:

mcedit /usr/src/linux/makeK

```
#!/bin/bash
#make mrproper – только для заплаток к ядру или если Вы уже компилировали ядро
#из этой директории

#make menuconfig -  или make xconfig (из сессии X Windows) - или
#make oldconfig
make dep && make bzImage && make modules && make
modules_install && \
cp -p /boot/vmlinuz /boot/vmlinuz.old && cp arch/i386/boot/bzImage
/boot/vmlinuz && \
cp System.map /boot/System.map && cp .config /boot/config && \
echo Отредактируйте lilo.conf для указания нового ядра. Выполните
lilo и перезагрузитесь.
```

При компиляции ядра впервые, начните с конфигурационного файла, который был использован при загрузке:

cd /usr/src/linux
cp /boot/config .config
make oldconfig

Вы будете оповещены о различиях в версиях ядер. Отвечайте по желанию.

Если Вы находитесь в консольном режиме, выполните “make menuconfig” для внесения изменений в конфигурацию ядра или “make xconfig”, если вы в X Windows.

Заплатки к ядру

Я всегда храню нетронутую копию исходников ядра в директории /usr/src. Например,

cp -pr linux-2.4.19/ linux-2.4.19-clean/
Теперь я могу применять заплатки к ядру, а если что-то пойдет не так, вернуться к чистой копии.

Каждый раз, когда я компилирую ядро, я изменяю четвертую строку в файле Makefile:

EXTRAVERSION = -a (-b, -pre8a, etc...). Затем я компилирую его. Теперь мне не надо волноваться о недостающих модулях каждый раз, когда я загружаю другое ядро, т.к. новые модули сохраняются в директории /lib/modules с полным названием version/extraversion. Как только я доволен ядром, я переименовываю директорию исходников, чтобы она совпадала с именем директории в /lib/modules (или версией Makefile).

mv linux-2.4.19/ linux-2.4.19a/
rm linux
ln -s linux-2.4.19a linux

Допустим, что я хочу добавить изменения из patch-2.4.20-pre8 с The Linux Kernel Archives к моим исходникам ядра linux-2.4.19.

```
Я скачиваю и сохраняю файл в /home/download
cd /usr/src
rm linux
cp -pr linux-2.4.19-clean/ linux-2.4.19/
gzip -dv /home/download/patch-2.4.20-pre8.gz
cp /home/download/patch-2.4.20-pre8 .
patch -p0 < patch-2.4.20-pre8
mv linux-2.4.19/ linux-2.4.20-pre8/
ln -s linux-2.4.20-pre8 linux
cd linux
cp /boot/config .config
make oldconfig
(затем, быть может, "make menuconfig" если я хочу увидеть
ситуацию в целом)
./makeK
```

LILO и boot_message.txt

Не забывайте выполнять команду “lilo” после компиляции нового ядра!

```
# LILO configuration file
# generated by 'liloconfig'
#
# Start LILO global section
restricted
#linear
append="hdd=ide-scsi"
boot = /dev/hda2
message = /boot/boot_message.txt
prompt
```

```
timeout = 50
# compact # быстрее, но не подходит для всех систем
# delay = 5
# VESA framebuffer console @ 1024x768x256
vga = 773
# Normal VGA console
# vga = normal
# VESA framebuffer console @ 1024x768x64k
# vga=791
# VESA framebuffer console @ 1024x768x32k
# vga=790
# VESA framebuffer console @ 1024x768x256
# vga=773
# VESA framebuffer console @ 800x600x64k
# vga=788
# VESA framebuffer console @ 800x600x32k
# vga=787
# VESA framebuffer console @ 800x600x256
# vga=771
# VESA framebuffer console @ 640x480x64k
# vga=785
# VESA framebuffer console @ 640x480x32k
# vga=784
# VESA framebuffer console @ 640x480x256
# vga=769
# ramdisk = 0 # параноидальный вариант
# End LILO global section
# Linux bootable partition config begins
image = /boot/vmlinuz
  root = /dev/hda2
  label = NewLinux
  password=password1
  read-only
# append="hdd-ide-scsi video=sstfb"
image = /boot/vmlinuz-ide-2.4.19
  root = /dev/hda2
  label = OrgLinux
  password=password2
  read-only
image = /boot/vmlinuz.old
  root = /dev/hda2
  label = OldLinux
  password=password3
  read-only
image = /boot/vmlinuz-2.4.18
  root = /dev/hda2
  label = BckLinux
  password=password4
  read-only
# Linux bootable partition config ends
# Start Memtest86 bootstrap
image = /memtest/memtest
```

```
    label = MemTest
    password=memtest
  # End Memtest86

#----- End /etc/lilo.conf
```

/boot/boot_message.txt
Welcome to the LILO Boot Loader!

Please enter the name of the Linux Kernel you would like to boot
at the prompt below. The choices are:

NewLinux - New Custom Kernel (default)
OrgLinux - Originial Slackware 9 Kernel
OldLinux - Last Cusom Kernel Kernel
BckLinux - Backup Custom 2.4.18 Kernel
MemTest - Run memory diagnostics

Создаем новый загрузочный диск

В директории /sbin существует скрипт под названием makebootdisk. Он предлагает на выбор 3 разных загрузочных диска - syslinux (DOS-форматированный диск), lilo (linux-форматированный диск), and simple (устарелый). Также Вы выбираете ядро, например /boot/vmlinuz.

Изучаем уровни начальной загрузки

Первостепенное значения для нас имеет конфигурационный файл /etc/inittab. inittab выполнит скрипты, в зависимости от того какой уровень загрузки (run level) вы собираетесь выполнить.

Например, при уровне, установленном по умолчанию 3, inittab выполнит /etc/rc.d/rc.S (который вызовет /etc/rc.d/rc.modules и rc.serial), заетм /etc/rc.d/rc.M который вызовет... Просто следите за тем, что происходит по мере выполнения файла inittab и все будет в поредке.

Удачи!

Коллективный доступ в Интернет

Включаем Dial-on-Demand

Dial-on-Demand позволяет всем компьютерам, находящимся в одной сети, получать доступ в Интернет через одно модемное соединение. Для этого вставьте следующие

строки в /etc/rc.d/rc.inet2 (сразу после IPV forward). В этом случае, остальные компьютеры сети будут использовать Ваш компьютер как шлюз:

```
# Инициализируем Dial-on-demand
# PPPD_AUTO: 0 = выкл, 1 = вкл. Элементарно, Ватсон ;)
PPPD_AUTO=0
if [ "$PPPD_AUTO" = "1" ]; then
echo "Activating Dial-on-Demand."
# Замените на nameserver или IP адрес Вашего провайдера)
pppd :1.2.3.4
route add -host 255.255.255.255 dev eth0
fi
```

Отключаем связь с Интернетом

```
#!/bin/bash
# killmodem - автор Jack S. Lai
#
# Этот скрипт корректно завершит модемное соединение. Он был написан
# для завершения dial-on-demand PPPD интерфейса до пятиминутного таймаута при #
#запуске
#
MDMPID=`cat /var/run/ppp0.pid`
kill -HUP $MDMPID
```

Кабельный модем

Серверные настройки

После инициализации кабельного модема скриптом netconfig (в процессе его выполнения Вам может понадобиться ввести имя Вашего хоста), - у Вас есть кабельное соединение.

Я привык настраивать только кэширующий сервер имен, т.к. сервер моего провайдера имеет обыкновение ненадолго «падать» по ночам (это довольно неудобно, когда застает врасплох). После настройки кэширующего сервера имен, приостановки в работе более не возникали. Для получения более подробной информации, см. djbns.

Далее я настроил dhcpd (этот демон стартует из /etc/rc.d/rc.local), чтобы он передавал необходимую информацию для обеспечения доступа к Интернету моему Linux/Windows компьютеру в любое время.

```
#
# Конфигурационный файл для ISC dhcpd (см. 'man dhcpd.conf')
#
ddns-update-style interim;
subnet 192.168.1.0 netmask 255.255.255.0 {

        range 192.168.1.2 192.168.1.3;
        default-lease-time 86400;
```

```
        max-lease-time 86400;
        option routers 192.168.1.1;
        option ip-forwarding off;
        option broadcast-address 192.168.1.255;
        option subnet-mask 255.255.255.0;
        option domain-name-servers 192.168.1.1;
        option domain-name "syskahuna.org";
        option netbios-name-servers 192.168.1.1;
        option netbios-dd-server 192.168.1.1;
        option netbios-node-type 8;
        option netbios-scope "";

}
```

Так как IP-адреса компьютеров во внутренней сети всегда остаются неизменными, я добавил следующие строки в файл /etc/hosts для облегчения вызовов ping, ssh, scp, и т.д.

```
#
# hosts
# This file describes a number of hostname-to-address mappings for the
# TCP/IP subsystem. It is mostly used at boot time, when no name servers
# are running. On small systems, this file can be used instead of a
# "named" name server. Just add the names, addresses
# and any aliases to this file...
#
# By the way, Arnt Gulbrandsen <agulbra@nvg.unit.no> says that
127.0.0.1
# should NEVER be named with the name of the machine. It causes
problems
# for some (stupid) programs, irc and reputedly talk. :^)
#
# For loopbacking.
127.0.0.1    localhost
192.168.1.1    oahu.syskahuna.org oahu
192.168.1.2    kauai.syskahuna.org Kauai
```

Отредактируйте файл /etc/rc.d/rc.inet1 для задания IP-адреса второй сетевой карте:

Также можете изменить файл /etc/modules.conf, чтобы разделить две сетевые карты. В моем случае, я намеренно поместил в сервер два разных сетевых адаптера, чтобы не перепутать их.

/etc/modules.conf:

```
alias eth0 sundance
alias eth1 8139too
```

Настройки клиента

Настройте клиент так, чтобы он использовал dhcp для резолюции адресов. Это настроит большинство параметров, необходимых для доступа в Интернет.

Повторный старт IDS при изменении IP адреса с помощью dhcpd

Когда для получения IP-адреса используется dhcpd, для изменения этого адреса порой необходимо также изменить адреса, которые отслеживают запущенные программы IDS. Эта процедура позволит dhcpd запускать скрипты обновления, когда адрес меняется.

Чтобы осуществить данное изменение, я написал rc скрипты для запуска, остановки и перезапуска portsentry, snort, and iptables. Однако демону portsentry также требуется скрипт doport, а snort – скрипт dosnort. Вышеперечисленные функции можно добавить к этим скриптам, но я пошел другим путем. Я изменил файл /etc/rc.d/rc.inet2 для запуска этих скриптов вместо того, чтобы запускать эти программы вызовами напрямую.

----- Начало модификации /etc/rc.d/rc.inet2:

```
# If there is a firewall script, run it before enabling packet forwarding.
# See the HOWTOs on http://www.netfilter.org/ for documentation on
# setting up a firewall or NAT on Linux.
if [ -x /etc/rc.d/rc.firewall ]; then
  /etc/rc.d/rc.firewall start
fi

# Запускаем portsentry
if [ -x /etc/rc.d/rc.portsentry ]; then
  /etc/rc.d/rc.portsentry start
fi

# Запускаем snort
if [ -x /etc/rc.d/rc.snort ]; then
  /etc/rc.d/rc.snort start
fi

# Запускаем icmpinfo
echo "Starting icmpinfo"
/usr/sbin/icmpinfo -v -n -s -l

# Запускаем iplog
echo "Starting iplog"
/usr/local/sbin/iplog

# Запускаем клиент MyNetWatchman.
if [ -x /etc/rc.d/rc.mnwclient ]; then
  /etc/rc.d/rc.mnwclient start
fi
```

----- Конец модификации

----- Начало скрипта /etc/rc.d/rc.portsentry

```
#!/bin/bash
# Запускаем или перезапускаем Portsentry
dostart() {
  echo "Starting Portsentry..."
  /usr/local/psionic/portsentry2/doports
  /usr/local/psionic/portsentry2/portsentry
}

dostop() {
  mypid=$(pidof -x portsentry)
  if [ $mypid ]; then
    # Running - kill it
    echo "Stopping Portsentry: $mypid"
    kill $mypid
  else
    echo "Portsentry is not running! Can't stop."
  fi
}
case "$1" in
'start')
  dostart
  ;;
'stop')
  dostop
  ;;
'restart')
  dostop
  sleep 2
  dostart
  ;;
*)
  # Default to start
  dostart
esac
```

----- Конец скрипта
----- Начало скрипта /etc/rc.d/rc.snort

```
#!/bin/bash
# Запускаем или перезапускаем Snort
# Параметры Snort:
# -c использовать конфигурационный файл

# -q выход
# -D запускать в режиме демона

dostart() {
  echo "Starting Snort"
```

```
  /etc/snort/dosnort
  /usr/bin/snort -q -c /etc/snort/snort.conf -D &
}

dostop() {
  mypid=$(pidof -x snort)
  if [ $mypid ]; then
    # Running - kill it
    echo "Stopping Snort: $mypid"
    kill $mypid
  else
    echo "Snort is not running! Can't stop."
  fi
}
case "$1" in
'start')
  dostart
  ;;
'stop')
  dostop
  ;;
'restart')
  dostop
  sleep 2
  dostart
  ;;
*)
  # Default to start
  dostart
esac
```

----- Конец скрипта

У Вас уже должен быть свой скрипт /etc/rc.d/rc.firewall, запускающий, останавливающий или перезапускающий Ваш firewall.

Теперь изменим /etc/dhcpc/dhcpcd-eth0.exe следующим образом:

```
#!/bin/sh
ipup() {
  echo "(dhcpcd)  IP address not changed: $1" | logger -p user.info
  echo "ipup"
}

ipdown() {
  echo "(dhcpcd)  IP interface down!: $1" | logger -p user.info
  echo "ipdown"
}

ipnew() {
  echo "(dhcpcd)  IP address changed to $1" | logger -p user.info
  echo "ipnew"
```

```
  # Restart firewall and IDS programs:
  if [ -x /etc/rc.d/rc.firewall ]; then
    /etc/rc.d/rc.firewall restart
  fi
# sleep 2
  if [ -x /etc/rc.d/rc.portsentry ]; then
    /etc/rc.d/rc.portsentry restart
  fi
  if [ -x /etc/rc.d/rc.snort ]; then
    /etc/rc.d/rc.snort restart
  fi
}

case "$2" in
'up')
  ipup
  ;;
'new')
  ipnew
  ;;
'down')
  ipdown
  ;;
*)
  # Default to up
  up
esac
```

----- Конец скрипта

Затем создаем ссылку Now we need to create a link: "ln -s /etc/dhcpc/dhcpcd-eth0.exe /etc/dhcpc/dhcpcd.exe”

Итак, теперь каждый раз когда IP-адрес Вашего сервера меняется, Ваши firewall и IDS программы будут перезапущены.

ПРИМЕЧАНИЕ: Этот скрипт допускает, что у Вас уже установлено соединение с Интернетом. Если Вы запускаете его впервые, дайте возможность Вашей системе загрузиться и не перезапускайте firewall и IDS программы путем выключения скрипта запуска.

chmod -x /etc/dhcpc/dhcpcd-eth0.exe

После того, как Вам присвоен IP-адрес, сделайте этот файл запускаемым снова.

Принудительная проверка файловой системы при запуске

Когда Вы просматривали загрузочные скрипты, Вы, вероятно, это обнаружили. Все диски, помеченные в файле fstab (см. **man fstab**) для проверки, будут проверены вызовом из /etc/rc.d/rc.S. Для этого выполните следующую команду:

touch /etc/forcefsck

Включаем поддержку Java в браузерах

Пакет Java 2 Runtime находится в каталоге /extra. Установите его командой installpkg и последуйте совету по настройке ниже. Я скачал Java 2 SDK из http://java.sun.com/j2se/1.4.1/download.html как самораспаковывающийся архив, и, после распаковки, переместил его в /usr/lib:

mv j2sdk1.4.1 /usr/lib

Затем в директории /etc/profile.d создал файл j2sdk.sh
#!/bin/sh
export MANPATH="$MANPATH:/usr/lib/j2sdk1.4.1/man"
export PATH="$PATH:/usr/lib/j2sdk1.4.1/jre/bin"

И наконец, укажим путь Вашему браузеру. В директории плагинов Вашего браузера создайте символические ссылки на необходимые Java библиотеки:

ln -s /usr/lib/j2sdk1.4.1/jre/plugin/i386/ns610/libjavaplugin_oji.so libjavaplugin_oji.so