1. **История, развитие и типы дистрибутивов Linux.**

В самом начале был Unix, созданный в 1969 году. Затем на протяжении восьмидесятых годов создавалось множество проектов на основе Unix, вдохновлённых этой философией. Это были: проект GNU, BSD, MINIX (мини версия Unix).

Но только в 1991 году началась история Linux. Финский студент Линус Торвальдс объединил всё, что он знал о существующих системах в новое ядро, которое смогло захватить мир.

Какова бы ни была истинная причина, он создал бесплатный эмулятор терминала, который был основан на Minix, в свою очередь, основанном на Unix, и это стало основой для работы над ядром операционной системы.

После этого первая версия Linux, которая тогда называлась Freax очень быстро разлетелась по FTP-серверам всего мира, а количество пользователей начало стремительно расти.

Linux превратился в полномасштабную ОС, а Манчестерский вычислительный центр создал один из первых дистрибутивов, в котором использовался комбинированный загрузочный и корневой раздел. Дистрибутив назывался MCC Interim Linux.

### 1992 - 1994 - РАЗВИТИЕ НАСТОЛЬНЫХ СИСТЕМ

В период с 1992 по 1994 мы увидели появление и развитие самых известных и влиятельных дистрибутивов Linux: Slackware и Debian.

**1995 - 1999 - ПОЯВЛЕНИЕ GNOME И KDE**

Окружение KDE (Kool Desktop Environment) появилось в 1996 году. Его основателем был Матиас Эттрих, студент университета Тюбингена. Он предложил не просто набор приложений, а целую среду рабочего стола, в которой они могли выполняться. У пользователей появился выбор пользоваться средой X11 или KDE, написанной на недавно появившемся фреймворке Qt.

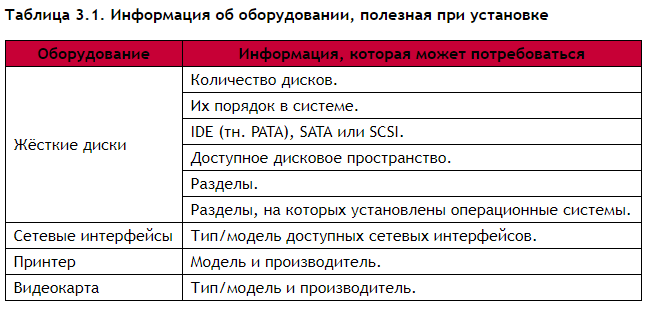
Мигель де Иказа и Федерико Мен объявили о разработке нового окружения рабочего стола, а также приложений для него на основе библиотеки GTK+. Эта новая среда рабочего стола называлась Gnome. Считается, что первой операционной системой, использующей Gnome, была Red Hat Linux.

2)  **Планирование и установка Linux.**

1. Сделать резервную копию существующих данных и документов жёсткого диска, на который вы планируете выполнить установку.

Перед тем как начать, убедитесь, что вы сохранили каждый файл из вашей системы. Если вы впервые устанавливаете на компьютер не родную операционную систему, скорее всего вам придётся переразметить диск, чтобы выделить место для Debian GNU/Linux. Всегда при разметке диска вы должны считать, что теряете всё на диске, вне зависимости от используемого для этого инструмента.

1. Перед началом установки собрать информацию о компьютере и всю необходимую документацию.



1. Найти и/или скачать программу установки и все нужные для вашей машины специальные драйверы или файлы микропрограмм.

Установочные образы можно найти на сервере-зеркале Debian.

1. Создать загрузочный медианоситель, такой как CDs/DVDs/USB, или организовать инфраструктуру загрузки по сети, с помощью которой можно будет запустить программу установки.
2. Загрузить систему установки.

- Одну из первых вещей, которую делает debian-installer, это проверка размера доступной памяти. Если размер ограничен, то эта компонента делает некоторые изменения процесса установки, которые, будем надеяться, позволят установить Debian GNU/Linux на вашу машину.

Первое, что делается для уменьшения потребления памяти программой установки — это выключение переводов в интерфейсе, то есть установка будет производится на английском языке. Конечно, вы сможете выполнить локализацию системы после завершения установки.

Если этого окажется недостаточно, программа установки дальше станет уменьшать потребление памяти загружая только компоненты, которые необходимы для выполнения базовой установки. Это уменьшает функциональность системы установки. Вам будет предоставлена возможность загрузить дополнительные компоненты вручную, но вы должны понимать, что каждая выбранная вами компонента использует память, и это может привести к неудачному завершению установки.

- Затем выбор локализации и клавиатуры.

- Далее настройка сети.

Если в начале этого шага система обнаруживает, что имеется более одного сетевого устройства, то вас попросят указать, какое устройство будет первичным сетевым интерфейсом, то есть какое устройство будет использовано для установки системы.

По умолчанию, debian-installer пытается настроить сетевой интерфейс вашего компьютера автоматически. Если автоматическая настройка завершается с ошибкой постоянно, то вместо неё выберите настройку сети вручную.

При ручной настройке сети вам зададут несколько вопросов о вашей сети, а именно про IP-адрес, маску сети, шлюз, адреса серверов определения имён и имени машины. Кроме того, если используется интерфейс беспроводной сети, то вас попросят ввести личный Wireless ESSID и ключ WEP или ключевую фразу WPA/WPA2.

- Настройка времени и часового пояса

- Добавление пользователей и паролей

Учётная запись root также называемая суперпользовательской — это учётная запись, для которой нет никаких преград в вашей системе. Учётная запись root должна использоваться только для администрирования системы и как можно меньшее время.

- Разметка дисков

- Установка базовой системы

- Установка дополнительного программного обеспечения

- Установка и настройка системного загрузчика

- Завершение установки

1. Загрузить только что установленную систему в первый раз.

**3) Пользователи и группы. Файлы конфигурации. Управление учетными записями пользователей**

Использование: useradd [параметры] ПОЛЬЗОВАТЕЛЬ  
useradd -D  
useradd -D [параметры]

Параметры:  
**-b**, —base-dir БАЗ\_КАТ базовый каталог для домашнего каталога новой  
учётной записи  
**-c**, —comment КОММЕНТАРИЙ поле GECOS новой учётной записи  
**-d**, —home-dir ДОМ\_КАТ домашний каталог новой учётной записи  
**-D**, —defaults показать или изменить настройки  
по умолчанию для useradd  
**-e**, —expiredate ДАТА\_УСТ дата устаревания новой учётной записи  
**-f**, —inactive НЕАКТИВНОСТЬ период неактивности пароля новой учётной записи  
**-g**, —gid ГРУППА имя или ID первичной группы новой  
учётной записи  
**-G**, —groups ГРУППЫ список дополнительных групп новой  
учётной записи  
**-m**, —create-home создать домашний каталог пользователя  
**-M**, —no-create-home не создавать домашний каталог пользователя  
**-N**, —no-user-group не создавать группу с тем же именем что и у  
пользователя  
**-p**, —password ПАРОЛЬ зашифрованный пароль новой учётной записи  
**-r**, —system создать системную учётную запись  
**-R**, —root КАТ\_CHROOT каталог, в который выполняется chroot  
**-s**, —shell ОБОЛОЧКА регистрационная оболочка новой  
учётной записи  
**-u**, —uid UID пользовательский ID новой учётной записи  
**-U**, —user-group создать группу с тем же именем что и у  
пользователя

/etc/passwd – описание локальных учётных записей

/etc/group – создание и удаление групп пользователей

groupadd group\_name

/etc/shadow – хранение паролей

**4) Системы управления пакетами. Их использование. Основные средства управления установкой, обновлением и удалением пакетов.**

Что-бы посмотреть установленные пакеты, используется ключ **–l**

Dpkg, удалить пакет dpkg –r или –P для удаления всех файлов

Что-бы посмотреть содержимое пакета, используется ключ **-c** (content):

Для этого используется ключ **-s** (status)

apt-get remove evolution

**5) Конфигурирование сети в Linux**

### НАСТРОЙКА ДИНАМИЧЕСКОГО ПОЛУЧЕНИЯ IP-АДРЕСА

Добавьте в этот файл такие строки, чтобы запускать интерфейс при загрузке и получать IP-адрес автоматически по DHCP:

/etc/network/interfaces

auto enp0s3  
iface enp0s3 inet dhcp

Синтаксис строки auto прост. Он состоит из самой команды и имени сетевого интерфейса. Рассмотрим подробнее:

**$ iface интерфейс inet тип**

ПОЛУЧЕНИЕ IP-АДРЕСА ПО DHCP

Сначала включаем интерфейс:

 sudo ip link set enp0s3 up

Затем с помощью команды **dhclient** запрашиваем ip:

 sudo dhclient enp0s3

Статический ip

Устанавливаем IP-адрес, маску сети и broadcast-адрес для нашего интерфейса:

 sudo ip addr add 192.168.1.7/255.255.255.0 broadcast 192.168.1.255 dev enp0s3

Указываем IP-адрес шлюза:

 sudo ip route add default via 192.168.1.1

настройка DNS

dns-nameservers 8.8.8.8 4.4.4.4

**6) системы мониторинг и SNMP**

Мониторинг правильной работы сервера, возможность постоянного контроля его основных показателей, производительности и других параметров имеет очень важное значение в производственной среде. Нам нужно своевременно реагировать на различные ошибки и проблемы, справляться с нагрузкой и многое другое. Информация - это ключ к решению любых компьютерных проблем, включая проблемы с оборудованием.

**7) Управление дисковыми устройствами, разделами и файловыми системами в Linux**

Fdisk –l посмотреть все про диски

**e2label** - позволяет изменить метку раздела с файловой системой ext.

**Fdisk /dev/sdb**-создание нового раздела

mkfs.ntfs /dev/sdc1 –раздел NTFS

**8) Резервное копирование**

Составим таблицу основных команд архиватора:

Создание архива tar -cv<z, b, J, ...>f <file>

Извлечение файлов tar -<z, b, J, ...>xvf <archive>

Выявление различий между архивами

tar -df <archive> <file>

Обновление архива tar -uf <archive>

Удаление файла из архива tar --delete -f <archive> <file>

Вывод списка файлов архива tar -tf <archive>

**9) Процессы в Linux. Сигналы. Средства контроля и мониторинга процессов.**

|  |  |  |  |
| --- | --- | --- | --- |
| № | Имя | Назначение | Реакция процесса-получателя |
| 1 | HUP | Hangup — отбой | Демоны перечитывают свои конфигурационные файлы |
| 2 | INT | Interrupt | Прекратить выполнение (перехватывается) |
| 3 | QUIT | Сильнее, чем INT | тоже |
| 4 | ILL | Программная ошибка | Обработать ошибку.  По умолчанию — прекратить выполнение |
| 8 | FPE | Floating point exception, вычислительная ошибка (деление на ноль) | Обработать ошибку.  По умолчанию —прекратить выполнение |
| 9 | KILL | Убить процесс | Немедленно прекратить выполнение. Не перехватывается |
| 11 | SEGV | Segmentation violation. Попытка доступа к чужой области памяти | Обработать ошибку.  По умолчанию — прекратить выполнение |
| 13 | PIPE | Нет процесса, читающего из конвейера | Обработать ошибку.  Корректно завершить выполнение  Перехватывается. |
| 15 | TERM | Termination. Завершить процесс |
| 17 | CHLD | Завершился дочерний процесс | Принять возвращенное им значение |
| 18 | CONT | Продолжить работу | Продолжить работу приостановленного процесса |
| 19 | STOP | Приостановить процесс | Приостановить выполнение |

**11) Межсетевые экраны. Netfilter/iptables и её применение.**

## ЧТО ТАКОЕ IPTABLES?

Подсистема iptables и Netfilter уже достаточно давно встроена в ядро Linux. Все сетевые пакеты, которые проходят через компьютер, отправляются компьютером или предназначены компьютеру, ядро направляет через фильтр iptables. Там эти пакеты поддаются проверкам и затем для каждой проверки, если она пройдена выполняется указанное в ней действие. Например, пакет передается дальше ядру для отправки целевой программе, или отбрасывается.

### ВИДЫ ПАКЕТОВ

Все пакеты делятся на три типа: входящие, исходящие и проходящие. Входящие - это те, которые были отправлены на этот компьютер, исходящие - отправленные из этого компьютера в сеть. А проходящие - это пакеты, которые просто должны быть пересланы дальше, например, если ваш компьютер выступает в качестве маршрутизатора.

Соответственно в фильтре iptables все пакеты делятся на три аналогичные цепочки:

* **Input** - обрабатывает входящие пакеты и подключения. Например, если какой-либо внешний пользователь пытается подключиться к вашему компьютеру по ssh или любой веб-сайт отправит вам свой контент по запросу браузера. Все эти пакеты попадут в эту цепочку;
* **forward** - эта цепочка применяется для проходящих соединений. Сюда попадают пакеты, которые отправлены на ваш компьютер, но не предназначены ему, они просто пересылаются по сети к своей цели. Как я уже говорил, такое наблюдается на маршрутизаторах или, например, если ваш компьютер раздает wifi;
* **output** - эта цепочка используется для исходящих пакетов и соединений. Сюда попадают пакеты, которые были созданы при попытке выполнить ping losst.ru или когда вы запускаете браузер и пытаетесь открыть любой сайт.

Но если вы думаете что можно просто полностью закрыть цепочку Input для увеличения безопасности, то вы очень сильно ошибаетесь. При работе сети используются обе цепочки input и output. Например, вы пытаетесь выполнить ping, данные отправляются через output, но ответ приходит через input. То же самое происходит при просмотре сайтов и других действиях. А вот цепочка forward может вообще не использоваться если ваш компьютер не является маршрутизатором. Так что настройка iptables должна выполняться очень аккуратно.

### ПРАВИЛА И ДЕЙСТВИЯ

Перед тем как перейти к созданию списка правил iptables нужно рассмотреть как они работают и какие бывают. Для каждого типа пакетов можно установить набор правил, которые по очереди будут проверяться на соответствие с пакетом и если пакет соответствует, то применять к нему указанное в правиле действие. Правила образуют цепочку, поэтому input, output и forward называют цепочками, цепочками правил. Действий может быть несколько:

* **ACCEPT** - разрешить прохождение пакета дальше по цепочке правил;
* **DROP** - удалить пакет;
* **REJECT** - отклонить пакет, отправителю будет отправлено сообщение, что пакет был отклонен;
* **LOG** - сделать запись о пакете в лог файл;
* **QUEUE** - отправить пакет пользовательскому приложению.

Настройка iptables для чайников

# НАСТРОЙКА IPTABLES ДЛЯ ЧАЙНИКОВ

Каждый компьютер, подключенный к сети, находится в потенциальной опасности. В сети очень много угроз начиная от программ, которые будут пытаться любым способом проникнуть в систему и заканчивая хакерами, которые хотят получить доступ к нужному им компьютеру. А программное обеспечение, установленное на компьютере, может содержать еще не известные и неисправленные уязвимости, которые и могут стать дырой в безопасности.

Если для домашних компьютеров это не очень актуально, так как они подключены к сети через роутеры и NAT, которые скрывают их от внешней сети, то для серверов это актуально как никогда. В операционной системе Linux в ядро встроен очень гибкий и надежный фаервол iptables.

Именно с помощью этой программы выполняется защита системы от внешних вторжений, перенаправление портов, а также еще очень много действий с трафиком. Но ее минус в том, что она немного сложна в настройке. В этой статье будет рассмотрена настройка iptables для чайников. Я надеюсь, что после нее вы сможете уверенно пользоваться базовыми возможностями iptables.

**$ iptables -t таблица действие цепочка дополнительные\_параметры**

Теперь давайте рассмотрим параметры iptables, таблица указывает таблицу, с которой нужно работать, этот параметр можно упустить, действие - нужное действие, например, создать или удалить правило, а дополнительные параметры описывают действие и правило, которое нужно выполнить.

Осталось рассмотреть основные действия, которые позволяет выполнить iptables:

* **-A** - добавить правило в цепочку;
* **-С** - проверить все правила;
* **-D** - удалить правило;
* **-I** - вставить правило с нужным номером;
* **-L** - вывести все правила в текущей цепочке;
* **-S** - вывести все правила;
* **-F** - очистить все правила;
* **-N** - создать цепочку;
* **-X** - удалить цепочку;
* **-P** - установить действие по умолчанию.

Дополнительные опции для правил:

* **-p** - указать протокол, один из tcp, udp, udplite, icmp, icmpv6,esp, ah, sctp,  
  mh;
* **-s** - указать ip адрес устройства-отправителя пакета;
* **-d** - указать ip адрес получателя;
* **-i** - входной сетевой интерфейс;
* **-o** - исходящий сетевой интерфейс;
* **-j** - выбрать действие, если правило подошло.

 sudo iptables -A INPUT -s 10.10.10.10 -j DROP

iptables -A INPUT -p icmp --icmp-type echo-request -j REJECT