Обеспечение безопасности ОС семейства Linux

Обеспечение безопасности рабочей станции

- Оценка безопасности рабочей станции
- Защита BIOS и загрузчика системы
- Парольная защита
- Административные средства
- Доступные сетевые службы

Обеспечение безопасности сервера

- Защита служб с помощью оболочек TCP и xinetd
- Защита HTTP-сервера Apache
- Защита FTP
- Определение открытых портов

Обеспечение безопасности рабочей станции

- Защита окружения Linux начинается с рабочей станции. Будь то защита личного компьютера или целого предприятия, политика безопасности начинается с отдельного компьютера. И вообще, компьютерная сеть защищена настолько, насколько защищён её самый уязвимый узел.
- Оценивая безопасность рабочей станции Linux, примите во внимание следующее:
- *Защита BIOS и загрузчика системы* — Сможет ли неавторизованный пользователь получить физический доступ к компьютеру и загрузиться без пароля в монопольном режиме или режиме восстановления?

Обеспечение безопасности рабочей станции

- *Парольная защита* — Насколько сильны пароли пользователей системы?
- *Административные средства* — Кто имеет учётные записи в системе и какие административные права им даны?
- *Доступные сетевые службы* — Какие службы принимают запросы из сети и должны ли они вообще работать?
- *Персональные брандмауэры* — Необходим ли брандмауэр, и, если да, то какого типа?
- *Средства связи с улучшенной защитой* — Какие средства следует использовать для связи между рабочими станциями, а какие — нет?

Обеспечение безопасности рабочей станции

- **Защита BIOS и загрузчика системы**
- Главный способ – защита физического доступа.
- **Парольная защита**
- Пароли — основной способ определения подлинности пользователя, используемый в Linux. Вот почему парольная защита чрезвычайно важна для защиты пользователя, рабочей станции и сети.
- По соображениям безопасности программа установки задействует в системе *MD5* (*Алгоритм выборки сообщения — Message-Digest Algorithm*) и теневые пароли. Настоятельно рекомендуется не изменять этих настроек.

Обеспечение безопасности рабочей станции

- Если во время установки отключить пароли MD5, будет использоваться старый стандарт шифрования данных *DES* (*Data Encryption Standard*). В этом стандарте пароли ограничены восемью алфавитно-цифровыми символами (знаки препинания и другие спецсимволы запрещены) и используется скромное 56-битное шифрование.
- Если во время установки отключить теневые пароли, все пароли, прошедшие одностороннее преобразование, сохраняются в доступном всем на чтение файле /etc/passwd, что делает систему уязвимой для атак автономного подбора пароля. Если взломщик получит доступ к компьютеру под именем обычного пользователя, он сможет скопировать файл /etc/passwd на свой компьютер и сколько угодно подбирать пароли с помощью различных программ.

Обеспечение безопасности рабочей станции

- Если в этом файле окажутся небезопасные пароли, их взлом будет всего лишь делом времени.
- Теневые пароли спасают от такой атаки, так как хэши паролей сохраняются в файле /etc/shadow, доступном на чтение только пользователю root.
- Это вынуждает потенциального взломщика перебирать пароли удалённо, подключаясь к сетевой службе компьютера, например, к SSH или FTP. Перебор пароля таким способом выполняется гораздо медленнее и легко обнаруживается, так как в системных файлах будут зафиксированы сотни попыток входа. Конечно, если взломщик нападёт на систему со слабыми паролями ночью, до рассвета он сможет получить доступ и скрыть свои следы, подправив файлы журналов.

Обеспечение безопасности рабочей станции

- Самое главное, что должен сделать пользователь для защиты своей учётной записи от взлома пароля — задать сильный пароль.
- ***Создание сильных паролей***
- Придумывая сильный пароль, следуйте приведённым ниже рекомендациям:
- *Не делайте следующего:*
- *Не используйте только слова или числа* — Никогда не используйте в пароле только слова или числа.
- Вот примеры небезопасных паролей:
  - 8675309
  - juan
  - hackme

Обеспечение безопасности рабочей станции

- *Не используйте известных слов* — Следует избегать имён собственных, слов из словаря и фраз из телевизионных передач или книг, даже если они включают в себя цифры.
- Вот примеры небезопасных паролей:
  - john1
  - DS-9
  - mentat123
- *Не используйте слов из других языков* — Программы подбора пароля часто перебирают пароль по списку, включающему словари многих языков. Полагаться на иностранные языки с целью защитить пароль не безопасно.

Обеспечение безопасности рабочей станции

- Вот примеры небезопасных паролей:
  - cheguevara
  - bienvenido1
  - 1dumbKopf
- *Не используйте сленг хакеров* — Если вы думаете, что относитесь к элите, потому что используете в своём пароле сленг, подумайте ещё раз. Сленг включён во многие списки слов.
- Вот примеры небезопасных паролей:
  - H4X0R
  - 1337

Обеспечение безопасности рабочей станции

- *Не используйте личные сведения* — Избегайте употребления личных сведений. Если взломщик узнает, кто вы, задача отгадывания пароля становится проще. Ниже перечислены сведения, которые не следует использовать, придумывая пароль:
- Вот примеры небезопасных паролей:
  - Ваше имя
  - Имена домашних животных
  - Имена членов семьи
  - Любые дни рождения
  - Ваш номер телефона или индекс

Обеспечение безопасности рабочей станции

- *Не переворачивайте известных слов* — Хорошие программы подбора пароля всегда переворачивают стандартные слова, поэтому переворачивание плохого пароля не делает его лучше.
- *Не записывайте свой пароль* — Никогда не записывайте свой пароль на бумаге. Гораздо безопаснее запомнить его.
- *Не используйте один пароль на всех компьютерах* — Важно придумать отдельные пароли для разных компьютеров. Тогда, если будет скомпрометирован один компьютер, все остальные компьютеры не окажутся в опасности.

Обеспечение безопасности рабочей станции

- *Делайте следующее:*
- *Придумывайте пароль длиной не меньше восьми символов* — Чем длиннее пароль, тем лучше. Если вы используете пароли MD5, следует выбирать пароли из 15 символов и длиннее. Используя пароли DES, создавайте их максимально длинными (восемь символов).
- *Смешивайте буквы верхнего и нижнего регистра* — Система Red Hat Enterprise Linux чувствительна к регистру, поэтому смешивайте регистр, чтобы усилить свой пароль.
- *Смешивайте буквы и цифры* — Добавив пароли цифры, особенно, вставляя их в середину (а не просто в начало или конец), вы также увеличиваете стойкость пароля.

Обеспечение безопасности рабочей станции

- *Включайте не алфавитно-цифровые символы* — Специальные символы (например, &, $ и >) значительно усиливают пароль (их нельзя использовать в паролях DES).
- *Придумайте пароль, который вы можете запомнить* — Лучший в мире пароль вовсе не хорош, если вы не можете его запомнить; используйте сокращения или другие приёмы, облегчающие запоминание паролей.
- После знакомства с этими правилами, может показаться, что создать пароль, соответствующий всем критериям хорошего пароля и не попадающий в категорию плохих — очень сложно. К счастью, есть алгоритм создания запоминаемых, безопасных паролей.

Обеспечение безопасности рабочей станции

- **Методика создания безопасного пароля**
- Есть множество способов создания безопасных паролей. Один из самых популярных — использование сокращений. Например:
- Вспомните какую-нибудь фразу, например:
- «по лесам, по горам, сегодня здесь, завтра там.».
- Затем сделайте из неё сокращение (включая знаки препинания).
- пл,пг,сз,зт.
- Усложните его, заменив буквы цифрами и специальными символами. Например, подставьте 3 вместо з, а символ (() вместо с:
- пл,пг,(3,3т.

Обеспечение безопасности рабочей станции

- Увеличьте сложность ещё больше, сделав большой хотя бы одну букву, например П.
- пл,Пг,(3,3т.
- *И, наконец, никогда и нигде не используйте показанный здесь пароль*.
- Хотя придумывать безопасные пароли крайне необходимо, также важно правильно с ними обращаться, особенно для системных администраторов в больших организациях. В следующем разделе подробно описано, как правильно создавать пароли пользователей и управлять ими в организации.

Обеспечение безопасности рабочей станции

- *Создание паролей пользователей в организации*
- Если в организации работает значительное число пользователей, системные администраторы могут принудить их использовать сильные пароли двумя способами. Они могут создавать пароли для пользователей или позволить им создавать пароли самостоятельно, проверяя при этом качество этих паролей.
- Создание паролей для пользователей гарантирует, что пароли хороши, но это становится непосильной задачей по мере роста организации. При этом также увеличивается опасность того, что пользователи начнут записывать свои пароли.

Обеспечение безопасности рабочей станции

- Поэтому многие системные администраторы предпочитают, чтобы пользователи придумывали себе пароли сами, и при этом постоянно проверяют их качество, вынуждая пользователей периодически менять пароли, ограничивая срок их действия.
- **Требование сильных паролей**
- Системные администраторы сделают правильный ход, если в целях защиты сети от вторжения будут проверять, насколько сильны используемые в организации пароли. Когда пользователю предлагается создать или сменить пароль, они могут использовать приложение командной строки passwd, поддерживающее *PAM* (*Pluggable Authentication Modules*), и, таким образом, будет произведена проверка, легко ли взломать пароль с помощью PAM-модуля pam_cracklib.so.

Обеспечение безопасности рабочей станции

- Так как PAM можно настраивать, вы можете добавить дополнительные процедуры проверки качества пароля, например pam_passwdqc (доступный по адресу http://www.openwall.com/passwdqc/) или написать новый модуль. За списком существующих модулей PAM обратитесь по адресу http://www.kernel.org/pub/linux/libs/pam/modules.html. За дополнительной информацией о PAM, обратитесь к главе *Подключаемые модули проверки подлинности (PAM)* в *Справочном руководстве Red Hat Enterprise Linux*.
- Однако следует заметить, что пароли проходят эту проверку в момент создания, и это средство не так действенно, как запуск программы перебора паролей для проверки всех паролей, используемых в организации.

Обеспечение безопасности рабочей станции

- В Red Hat Enterprise Linux будет работать множество программ подбора пароля, но ни одна из них не поставляется с системой. Ниже приведён краткий список наиболее распространённых программ взлома пароля:
- ***John The Ripper*** — быстрая и гибкая программа подбора пароля. Она может использовать несколько списков слов и подбирать пароль методом грубой силы. Она доступна по адресу http://www.openwall.com/john/.
- ***Crack*** — возможно, наиболее известная программа взлом паролей. **Crack** также очень быстрая программа, хотя и не так проста в использовании, как **John The Ripper**. Её можно найти по адресу http://www.crypticide.com/users/alecm/.

Обеспечение безопасности рабочей станции

- ***Slurpie*** — программа **Slurpie** похожа на **John The Ripper** и **Crack**, но она рассчитана на работу сразу на нескольких компьютерах, и позволяет провести распределённый взлом пароля. Её, а также другие средства организации распределённой атаки, можно найти по адресу http://www.ussrback.com/distributed.htm.
- Всегда, прежде чем приступать в своей организации к перебору паролей, получите на это письменное разрешение.

Обеспечение безопасности рабочей станции

- **Срок действия пароля**
- Ограничение срока действия пароля — ещё один приём, используемый системными администраторами. Он означает, что по истечении заданного времени (обычно 90 дней) пользователю предлагается сменить пароль. Смысл этого состоит в том, что если пользователь будет вынужден периодически менять пароль, подобранный взломщиком пароль будет действовать ограниченное время. Однако это имеет и негативные последствия — пользователи могут начать записывать пароли.
- Для определения срока действия пароля в Linux в основном используются две программы: команда chage и графическое приложение **Менеджер пользователей** (system-config-users).

Обеспечение безопасности рабочей станции

- Параметр -M команды chage определяет максимальный срок действия пароля в днях. Например, чтобы срок действия пароля пользователя истекал через 90 дней, выполните:
- **`chage -M 90 <username>`**
- Замените в этой команде *<username>* именем пользователя. Чтобы периодическая смена пароля не требовалась, обычно используют значение 99999 после параметра -M (при этом период смены будет немногим больше 273 лет).

Обеспечение безопасности рабочей станции

- Определить политики срока действия пароля также можно в графическом приложении **Менеджер пользователей (User Manager)**. Чтобы запустить это приложение, выберите в **Приложения** (на панели) => **Системные параметры** => **Пользователи и группы** или введите в приглашении оболочки system-config-users (например, в терминале XTerm или GNOME). Перейдите на вкладку **Пользователи**, выберите пользователя из списка и щёлкните в меню кнопки **Свойства** (или выберите в главном меню **Файл** => **Свойства**).
- Затем перейдите на вкладку **Сведения о пароле** и определите, сколько дней действует пароль.

Обеспечение безопасности рабочей станции

- **Административные средства**
- Управляя домашним компьютером, пользователь должен выполнять некоторые действия под именем root или получить привилегии root, с помощью программ *setuid*, например sudo или su. Программы setuid — это программы, работающие с кодом пользователя (*UID*) владельца программы, а не запускающего их пользователя. В подробном списке файлов эти программы выделяются маленькой буквой s в разделе владельца, как показано ниже:
- -rwsr-xr-x 1 root root 473 May 1 08:09 /bin/su
- Однако системные администраторы организации должны определить, какие административные права должны иметь пользователи на своих компьютерах.

Обеспечение безопасности рабочей станции

- С помощью PAM-модуля pam_console.so некоторые действия, обычно разрешённые только пользователю root, например, перезагрузку и извлечение съёмных устройств, можно разрешить первому вошедшему на физическую консоль пользователю. Однако выполнение других важных административных задач, таких как изменение параметров сети, настройка новой мыши или подключение сетевых устройств невозможно без прав администратора. В следствие этого системные администраторы должны решить, какие административные полномочия должны получить пользователи их сети.

Обеспечение безопасности рабочей станции

- ***Разрешение доступа root***
- Если пользователи организации доверяют друг другу и разбираются в компьютерах, возможно, допустимо назначить им права root. Наделение их правами root будет означать, что простые операции, такие как добавление устройств или настройка сетевых интерфейсов, будут выполнять сами пользователи, освобождая администраторов для решения важных проблем, например, сетевой безопасности.
- С другой стороны, назначение отдельным пользователям прав root может создать, например, следующие проблемы:

Обеспечение безопасности рабочей станции

- *Неверная настройка компьютера* — Пользователи с правами root, могут неправильно настроить свои компьютеры, после чего им потребуется помощь, или, что ещё хуже, могут создать дыры в безопасности, не догадываясь об этом.
- *Запуск небезопасных служб* — Пользователи с правами root могут запускать на своих компьютерах небезопасные службы, например FTP или Telnet, что ставит под угрозу их имена и пароли, передаваемые по сети открытым текстом.
- *Запуск почтовых вложений под именем root* — Хотя вирусы для Linux — редкость, но всё же они есть. И они представляют собой угрозу, только если их запускает пользователь root.

Обеспечение безопасности рабочей станции

- Если по этим или другим причинам администратору не хочется, чтобы пользователи имели права root, пароль root следует хранить в секрете и запретить доступ к первому уровню выполнения или монопольному режиму, защитив загрузчик паролем.
- **Отключение оболочки root**
- Чтобы запретить пользователям непосредственный вход под именем root, системный администратор может задать для root оболочку /sbin/nologin в файле /etc/passwd. Это предотвратит доступ к учётной записи root с помощью команд, использующих оболочку, например su и ssh.
- Программы, не нуждающиеся в оболочке, например, почтовые клиенты или команда sudo, по-прежнему могут работать под именем root.

Обеспечение безопасности рабочей станции

- **Запрет входа root**
- Чтобы ещё больше ограничить доступ к учётной записи root, администраторы могут запретить вход под именем root с консоли, отредактировав файл /etc/securetty. В этом файле перечислены все устройства, с которых может регистрироваться root. Если файл не существует, пользователь root сможет войти в систему с любого устройства, будь то консоль или сетевой интерфейс. Это опасно, так как пользователь может входить в систему, используя Telnet, а при этом его пароль передаётся по сети в открытом виде. По умолчанию, в Red Hat Enterprise Linux файл /etc/securetty разрешает root подключаться только с физически подключенной к компьютеру консоли.

Обеспечение безопасности рабочей станции

- Чтобы запретить вход root, очистите содержимое этого файла, выполнив следующую команду:
- `echo > /etc/securetty`
- Пустой файл /etc/securetty *не* предотвращает удалённый доступ root с помощью набора инструментов OpenSSH, так как консоль открывается после проверки подлинности.
- **Запрет входа root через SSH**
- Чтобы запретить регистрацию root с использованием протокола SSH, отредактируйте файл настроек демона SSH (/etc/ssh/sshd_config). Измените строку, в которой написано:
- # PermitRootLogin yes на следующую:
- PermitRootLogin no

Обеспечение безопасности рабочей станции

- **Отключение root с помощью PAM**
- PAM-модуль /lib/security/pam_listfile.so даёт большие возможности по отключению учётных записей. Администратор может указать для этого модуля список пользователей, не имеющих разрешения на вход. Ниже приведён пример использования модуля для демона FTP-сервера vsftpd в файле конфигурации PAM /etc/pam.d/vsftpd (символ \ в конце первой строке *не* нужен, если всё помещается в одной строке):
- **`Auth required /lib/security/pam_listfile.so item=user\ sense=deny file=/etc/vsftpd.ftpusers onerr=succeed`**

Обеспечение безопасности рабочей станции

- Это указание PAM прочитать файл /etc/vsftpd.ftpusers и закрыть доступ к службе перечисленным в нём пользователям. Администратор волен выбирать имя этого файла и вести отдельные списки для разных служб или использовать один список для запрета доступа к нескольким службам сразу.
- Если администратор желает запретить доступ к нескольким службам, подобную строку можно добавить в конфигурацию PAM для этих служб, например, в /etc/pam.d/pop и /etc/pam.d/imap для почтовых клиентов или /etc/pam.d/ssh для клиентов SSH.

Обеспечение безопасности рабочей станции

- *Ограничение доступа root*
- Вместо того, чтобы полностью закрывать доступ пользователю root, администратор может разрешить доступ только к программам setuid, например, к su или sudo.
- **Команда su**
- Когда пользователь выполняет команду su, ему предлагается ввести пароль root, и после проверки он попадает в приглашение оболочки root.
- Зарегистрировавшись с помощью команды su, пользователь *является* пользователем root и имеет все права администратора системы. Кроме этого, если пользователь стал root, с помощью команды su он может стать любым другим пользователем системы, не зная его пароля.

Обеспечение безопасности рабочей станции

- Учитывая мощь этой программы, администраторам в организациях, возможно, захочется ограничить круг лиц, имеющих к ней доступ.
- Проще всего это можно сделать, добавив пользователей в специальную административную группу *wheel*. Для этого выполните от имени root следующую команду:
- usermod -G wheel <*username*>
- В этой команде замените <*username*> именем пользователя, которого вы хотите добавить в группу wheel.
- Чтобы проделать то же самое с помощью **Менеджера пользователей**, выберите в меню **Приложения** (на панели) => **Системные параметры** => **Пользователи и группы.**

Обеспечение безопасности рабочей станции

- Другой способ - введите в приглашении оболочки команду system-config-users. Перейдите на вкладку **Пользователи**, выберите пользователя из списка и щёлкните в меню кнопки **Свойства** (или выберите в главном меню **Файл** => **Свойства**). Затем перейдите на вкладку **Группы** и отметьте группу wheel. Затем откройте файл настройки PAM для команды su (/etc/pam.d/su) в текстовом редакторе и уберите комментарий [#] в следующей строке:
- **auth required /lib/security/$ISA/pam_wheel.so use_uid** Сделав, это вы откроете доступ к этой программе только пользователям группы администраторов wheel. Пользователь root по умолчанию включён в группу wheel.

Обеспечение безопасности рабочей станции

- **Команда sudo**
- Команда sudo предоставляют другую возможность получить права администратора. Когда доверенные пользователи указывают перед административной командой sudo, им предлагается ввести *их собственный* пароль. Затем, если его подлинность подтверждается и ему разрешена данная команда, эта команда будет выполняться, как будто она запущена пользователем root.
- Общий формат команды sudo показан ниже:
- **`sudo <command>`**
- В этом примере *<command>* нужно заменить командой, обычно выполняемой пользователем root user, например, mount.

Обеспечение безопасности рабочей станции

- Пользователи, запускающие команду sudo должны, покидая свой компьютер, выходить из системы, так как если выполнить эту команду ещё раз в течение пяти минут, она не спросит пароль. Эту настройку можно изменить в файле конфигурации /etc/sudoers.
- Только пользователи, перечисленные в файле /etc/sudoers, могут выполнить команду sudo, и эта команда будет выполнена в оболочке *пользователя*, а не root. Это значит, что оболочка root может быть полностью отключена.
- Команда sudo ведёт исчерпывающий аудит. Каждая успешная попытка входа регистрируется в файле /var/log/messages, а выполненная команда, вместе с именем выполняющего её пользователя в файле /var/log/secure.

Обеспечение безопасности рабочей станции

- Другим преимуществом команды sudo является то, что администратор может открыть пользователям доступ только к нужным им командам.
- Администраторы, желающие отредактировать файл конфигурации sudo, /etc/sudoers, должны использовать команду visudo.
- Чтобы дать кому-то все привилегии администратора, введите visudo и добавьте в раздел привилегий пользователя примерно такую строку:
- **`juan ALL=(ALL) ALL`**
- В этом примере пользователь juan может использовать sudo с любого компьютера и выполнить любую команду.

Обеспечение безопасности рабочей станции

- В приведённом ниже примере показано, как можно очень тонко настраивать sudo:
- `%users  localhost=/sbin/shutdown -h now`
- В данном примере любой пользователь, работающий на консоли, может выполнить команду /sbin/shutdown -h now.
- Подробное описание параметров этого файла можно найти на странице man sudoers.

Обеспечение безопасности рабочей станции

- **Доступные сетевые службы**
- Тогда как доступ пользователей к средствам администрирования — важный вопрос, волнующий администраторов в организации, чёткое понимание того, какие сетевые службы работают, крайне важно для всех, кто администрирует систему Linux и работает в ней.
- Многие службы, существующие в Linux, являются сетевыми. Если на компьютере работает сетевая служба, это значит, что серверное приложение, называемое *демоном*, ожидает подключений к одному или нескольким сетевым портам. Каждую из этих служб следует рассматривать, как возможное направление атаки.

Обеспечение безопасности рабочей станции

- ***Опасности служб***
- Сетевые службы в системе Linux могут быть опасны. Ниже приведён список некоторых основных угроз безопасности:
- *Атаки типа отказ в обслуживании (DoS - Denial of Service Attacks)* — При атаке такого типа служба забрасывается запросами, и система может просто остановиться, пытаясь обработать все запросы и ответить на них.
- *Атаки уязвимых сценариев* — Если веб-сервер выполняет на своей стороне сценарии, взломщик может провести атаку на сценарии, написанные с ошибками. Такие атаки часто приводят к переполнению буфера или позволяют взломщику изменить файлы на этом компьютере.

Обеспечение безопасности рабочей станции

- *Атаки на переполнение буфера* — Службы, подключенные к портам с 0 по 1023, должны работать от имени администратора. Если в этом приложении происходит переполнение буфера, нападающий сможет получить доступ к системе с правами пользователя, запустившего демона. Так как переполнения буфера нередки, взломщики применяют автоматические программы для выявления систем с такими уязвимостями и, получив к ним доступ, они используют инструменты скрытого управления (rootkits) для сохранения этого доступа.
- Угроза атак на переполнение буфера снижается благодаря реализованной в Red Hat Enterprise Linux технологии защиты и сегментации исполняемой памяти *ExecShield*, поддерживаемой одно и много-процессорными ядрами x86.

Обеспечение безопасности рабочей станции

- ExecShield снижает опасность переполнения буфера, разделяя виртуальную память на исполняемые и неисполняемые сегменты. Любой программный код, пытающийся запуститься вне исполняемого сегмента (это может быть вредоносный код внедрённый благодаря переполнению буфера) вызывает ошибку сегментации и завершается.
- Реализация Execshield также поддерживает технологию *No eXecute (Не исполнять)* (NX) на платформах AMD64 и технологию *eXecute Disable (Исполнение запрещено)* (XD) для систем Itanium и Intel® EM64T. Эти технологии, работающие совместно с ExecShield, предотвращают запуск вредоносного кода в неисполняемом разделе виртуальной памяти с точностью до 4 Кбайт кода, и снижают угрозу атак на переполнение буфера.

Обеспечение безопасности рабочей станции

- Чтобы снизить вероятность атак на сетевые службы, все ненужные службы должны быть отключены.
- ***Идентификация и настройка служб***
- В целях усиления безопасности многие сетевые службы, установленные в Red Hat Enterprise Linux, по умолчанию выключены. Однако есть и некоторые исключения:
- cupsd — Сервер печати, используемый в Red Hat Enterprise Linux по умолчанию.
- lpd — Альтернативный сервер печати.
- xinetd — Суперсервер, управляющий подключениями к подчинённым серверам, например, vsftpd и telnet.
- sendmail — Почтовый агент Sendmail по умолчанию включен, но настроен на приём соединений только от локального узла.

Обеспечение безопасности рабочей станции

- sshd — Служба OpenSSH, ставшая безопасной заменой Telnet.
- Определяя, какие службы следует оставить, лучше руководствоваться здравым смыслом и перестраховаться, чем что-то упустить. Например, если у вас нет принтера, отключите службу cupsd. То же самое касается portmap. Если вы не подключаете тома NFSv3 и не используете NIS (служба ypbind), portmap следует отключить.
- В Linux входят три программы, предназначенные для включения и отключения служб. Это **Настройка служб (Services Configuration Tool)** (system-config-services), **ntsysv** и chkconfig.

Обеспечение безопасности рабочей станции

- Но просто определить, какие службы запускаются при загрузке, недостаточно. Хорошие системные администраторы также должны проверять открытые порты.
- ***Небезопасные службы***
- Некоторые сетевые протоколы по своей природе менее защищены, чем другие. К ним относятся все службы, которые:
- *передают по сети имена и пароли открытым текстом* — многие старые протоколы, такие как Telnet и FTP, не шифруют данные при проверке подлинности, поэтому их нужно избегать везде, где это возможно.
- *передают по сети важные данные в открытом виде* — Многие протоколы передают данные по сети незашифрованными.

Обеспечение безопасности рабочей станции

- В число этих протоколов входят Telnet, FTP, HTTP и SMTP. Во многих сетевых файловых системах, в частности, NFS и SMB, данные также передаются по сети незашифрованными. Как использовать эти протоколы, чтобы не допустить утечки важных данных, должен решать пользователь.
- Кроме этого, службы удалённого дампа памяти, подобные netdump, передают по сети содержимое памяти в открытом виде. В памяти могут находиться пароли, или, что ещё хуже, записи базы данных и другая важная информация.
- Другие службы, вроде finger и rwhod, показывают информацию о пользователях системы.

Обеспечение безопасности рабочей станции

- В качестве примеров служб, небезопасных по природе, можно привести следующие:
- rlogin
- rsh
- telnet
- vsftpd
- Следует избегать использования программ удалённого входа и оболочки (rlogin, rsh и telnet), и использовать SSH.
- Протокол FTP не так опасен, как удалённые оболочки, но, тем не менее, чтобы избежать проблем, FTP-сервер нужно настраивать аккуратно.

Обеспечение безопасности рабочей станции

- К службам, которые нужно настраивать очень аккуратно и защищать брандмауэром, относятся:
- finger
- identd
- netdump
- netdump-server
- nfs
- rwhod
- sendmail
- smb (Samba)
- yppasswdd
- ypserv
- ypxfrd

Обеспечение безопасности сервера

- Когда компьютер работает в открытой сети в качестве сервера, он становится целью для атак. Поэтому укрепление системы и блокировка служб крайне важны для системного администратора.
- Прежде чем углубиться в эти вопросы, ознакомьтесь со следующими общими советами по усилению безопасности сервера:
- Своевременно обновляйте службы, чтобы исправить недавно найденные уязвимости.
- Используйте безопасные протоколы, везде, где это возможно.
- Если это возможно, выделяйте для каждого типа сетевых служб отдельный компьютер.
- Внимательно следите за подозрительной активностью на всех серверах.

Обеспечение безопасности сервера

- **Защита служб с помощью оболочек TCP и xinetd**
- *Оболочки TCP* позволяют управлять доступом к различным службам. Большинство современных сетевых служб, таких как SSH, Telnet и FTP, используют оболочки TCP, стоящие на страже между входящими запросами и службой.
- Преимущества оболочек TCP увеличиваются, если используется xinetd — суперслужба, дающая дополнительные возможности управления доступом, ведением журнала, привязкой, перенаправлением и использованием ресурсов.
- Будет правильным использовать правила брандмауэра IPTables вместе с оболочками TCP и xinetd для двойного ограничения доступа к службам.

Обеспечение безопасности сервера

- ***Усиление безопасности с помощью оболочек TCP***
- За полным списком возможностей оболочек TCP и описанием управляющего языка, обратитесь к странице man hosts_options.
- **Оболочки TCP и баннеры соединений**
- Послав клиентам, подключающимся к службе, устрашающий баннер, вы скроете информацию о системе, в которой работает сервер, и в то же время дадите возможному взломщику понять, что системой заправляет бдительный администратор. Чтобы сделать для службы баннер с помощью TCP оболочек, воспользуйтесь параметром banner.

Обеспечение безопасности сервера

- В этом примере будет создан баннер для службы vsftpd. Для начала создайте файл баннера. Он может находиться где угодно в системе, но он должен носить имя демона. Например, файл можно назвать /etc/banners/vsftpd.
- Содержимое файла будет примерно таким:
- **220-Hello, %c**
- **220-All activity on ftp.example.com is logged.**
- **220-Act up and you will be banned.**
- Вместо маркера %c будут подставлены сведения о клиенте, например, имя пользователя и компьютера или его IP-адрес, что делает соединение еще более устрашающим.

Обеспечение безопасности сервера

- Чтобы этот баннер выдавался для всех входящих соединений, добавьте в файл /etc/hosts.allow следующую строку:
- **`vsftpd : ALL : banners /etc/banners/`**
- **Оболочки TCP и предупреждения об атаке**
- Если при попытке атаки на сервер были пойманы какие-то узлы или сети, оболочки TCP, следуя указанию spawn, могут сообщать вам о последующих атаках этих узлов или сетей.
- В этом примере предполагается, что при попытке нападения на сервер был пойман взломщик из сети 206.182.68.0/24. Следующая строка, помещённая в файл /etc/hosts.deny, запрещает подключение и регистрирует попытку в специальном файле:

Обеспечение безопасности сервера

- **`ALL : 206.182.68.0 : spawn /bin/ 'date' %c %d >> /var/log/intruder_alert`**
- Вместо маркера %d будет подставлено имя службы, к которой пытался обратиться взломщик.
- Чтобы разрешить подключение с регистрацией в журнале, поместите указание spawn в файл /etc/hosts.allow.
- Так как указание spawn может выполнить любую команду оболочки, создайте специальный сценарий, сообщающий администратору или выполняющий серию команд в случае, если конкретный клиент пытается подключиться к серверу.

Обеспечение безопасности сервера

- **Оболочки TCP и улучшенное ведение журнала**
- Если соединения одной службы более интересны, чем другой, уровень ведения журнала этой службы можно увеличить с помощью параметра severity.
- Предположим, что человек, пытающийся подключиться к порту 23 (порт Telnet) на FTP-сервере — взломщик. Чтобы выявить его, установите флаг emerg, вместо флага по умолчанию info, и запретите соединение.
- Для этого поместите в /etc/hosts.deny следующую строку:
- `in.telnetd : ALL : severity emerg`

Обеспечение безопасности сервера

- При этом будет использовано стандартное средство ведения журнала authpriv, но приоритет поднимется с обычного info до emerg, и сообщения будут выводиться прямо на консоль.
- ***Усиление защиты с помощью xinetd***
- Суперсервер xinetd — ещё одно полезное средство управления доступом к подчинённым ему службам. В этом разделе рассматривается, как с помощью xinetd можно устанавливать ловушки для служб и ограничивать ресурсы, используемые службами xinetd, для предотвращения атак типа отказ в обслуживании. За более полным списком возможностей обратитесь к страницам man, посвящённым xinetd и xinetd.conf.

Обеспечение безопасности сервера

- **Установка ловушки**
- Важной возможностью xinetd является его способность добавлять узлы в глобальный список no_access. Узлам из этого списка запрещены подключения к службам, управляемым xinetd, в течение заданного периода времени или до перезапуска xinetd. Для этого служит атрибут SENSOR. С помощью этой возможности можно легко заблокировать узлы, сканирующие порты сервера.
- Определяя SENSOR, первым делом нужно выбрать службу, которую вы не планируете использовать. В этом примере выбрана служба Telnet.
- Отредактируйте файл /etc/xinetd.d/telnet и измените строку flags следующим образом:

Обеспечение безопасности сервера

- **`flags = SENSOR`**
- Добавьте в скобках следующую строку:
- **`deny_time = 30`**
- Она запрещает доступ на 30 минут узлу, пробующему подключиться к порту. Другими приемлемыми значениями атрибута deny_time является FOREVER (навсегда), означающее, что запрет будет действовать до перезапуска xinetd, и NEVER (никогда), допускающее подключение и регистрирующее его.
- И, наконец, последняя строка будет такой:
- **`disable = no`**

Обеспечение безопасности сервера

- Использование SENSOR — это хороший способ выявить и не допустить подключения плохих узлов, но у него есть два недостатка:
- Он не спасает от скрытого сканирования.
- Нападающий, знающий, что работает SENSOR, может устроить атаку типа отказ в обслуживании против конкретных узлов, подключаясь к запрещённому порту с их IP-адресами.
- **Управление ресурсами сервера**
- Ещё одной важной возможностью xinetd является его способность ограничивать ресурсы, используемые подчинёнными ему службами.
- Это выполняется с помощью следующих указаний:

Обеспечение безопасности сервера

- cps = <число_подключений> <период_ожидания> — Ограничивает число подключений к службе за секунду. Здесь допускаются только целые значения.
- instances = <число_подключений> — Ограничивает общее число подключений к службе. Здесь указывается целое значение или UNLIMITED (без ограничений).
- per_source = <число_подключений> — Ограничивает число подключений к службе с одного узла. Здесь указывается целое значение или UNLIMITED (без ограничений).
- rlimit_as = <число[K|M]> — Ограничивает объём памяти, который может занимать служба, в килобайтах или мегабайтах. Здесь указывается целое значение или UNLIMITED (без ограничений).

Обеспечение безопасности сервера

- rlimit_cpu = <число_секунд> — Ограничивает процессорное время, отнимаемое службой. Здесь указывается целое значение или UNLIMITED (без ограничений).
- Эти указания могут предотвратить задавливание системы службой xinetd, и таким образом, отказ в обслуживании.
- **Защита HTTP-сервера Apache**
- HTTP-сервер Apache — одна из самых стабильных и защищённых служб, входящих в состав Linux. Для защиты Apache придумано несчётное количество параметров и приёмов, слишком много, чтобы подробно разбирать их здесь.

Обеспечение безопасности сервера

- Настраивая HTTP-сервер Apache, обязательно ознакомьтесь с прилагаемой к нему документацией. В том числе познакомьтесь документацией к Stronghold, доступной по адресу http://www.redhat.com/docs/manuals/stronghold/.
- Ниже перечислены параметры конфигурации, использовать которые нужно очень осторожно.
- ***FollowSymLinks***
- Это указание по умолчанию включено, поэтому будьте очень внимательны, создавая символические ссылки в корневом каталоге документов веб-сервера. Например, не стоит создавать символические ссылки на /.

Обеспечение безопасности сервера

- ***Указание Indexes***
- Это указание по умолчанию включено, но это может быть нежелательно. Чтобы предотвратить просмотр посетителями списков файлов на сервере, уберите это указание.
- ***Указание UserDir***
- Указание UserDir по умолчанию отключено, так как с его помощью можно определить существующие в системе учётные записи. Чтобы разрешить на сервере просмотр каталогов пользователей, определите следующие указания:
- **`UserDir enabled UserDir disabled root`**

Обеспечение безопасности сервера

- Эти указания разрешают просмотр каталогов всех пользователей, за исключением /root/. Чтобы добавить пользователей в список запрещённых учётных записей, перечислите их через пробел в строке UserDir disabled.
- ***Не удаляйте указание IncludesNoExec***
- По умолчанию модуль включений на стороне сервера (server-side includes) не может выполнять команды. Настоятельно рекомендуется не изменять этот параметр, если у вас нет на то веских причин, так как это может позволить взломщику выполнять команды в вашей системе.

Обеспечение безопасности сервера

- ***Ограничьте доступ к каталогам с исполняемыми файлами***
- Убедитесь в том, что во всех каталогах, содержащих сценарии или CGI, разрешение на запись имеет только root. Это можно сделать, выполнив следующие команды:
- **`chown root <directory_name>`**
- **`chmod 755 <directory_name>`**
- А также обязательно проверяйте, правильно ли работают сценарии в вашей системе, *прежде* чем запустить их в работу.

Обеспечение безопасности сервера

- **Защита FTP**
- *File Transport Protocol (Протокол передачи файлов)*, или *FTP* — пожилой TCP-протокол, разработанный для передачи файлов по сети. Так как обмен данными с сервером, в том числе и при проверке подлинности, происходит в открытом виде, этот протокол считается небезопасным и при его настройке следует соблюдать осторожность.
- Red Hat Enterprise Linux предлагает два FTP сервера.
- gssftpd — основанный на xinetd FTP-демон, поддерживающий Kerberos, и поэтому не передающий по сети учётные данные в открытом виде.

Обеспечение безопасности сервера

- vsftpd — отдельная, ориентированная на безопасность реализация службы FTP.
- Следующие рекомендации касаются настройки FTP-службы vsftpd.
- ***Заголовок с приветствием FTP***
- Прежде чем пользователь передаст имя и пароль, он увидит заголовок с приветствием. По умолчанию, в этом заголовке будут указаны сведения о версии, а с их помощью взломщики могут определить слабые места в вашей системе.
- Чтобы изменить заголовок с приветствием для vsftpd, добавьте в файл /etc/vsftpd/vsftpd.conf следующее указание:

Обеспечение безопасности сервера

- **ftpd_banner=<*insert_greeting_here*>**
- Замените в этом указании *<insert_greeting_here>* текстом приветствия.
- Для многострочных заголовков лучше использовать отдельный файл. Чтобы упростить управление разными заголовками, поместите их в один каталог /etc/banners/. В этом примере заголовок для FTP-соединений находится в /etc/banners/ftp.msg. Ниже показано, как может выглядеть этот файл:
- **##**
  # Hello, all activity on ftp.example.com #
- **#is logged. #**
  ##

Обеспечение безопасности сервера

- Чтобы служба vsftpd ссылалась на этот файл заголовка, добавьте в файл /etc/vsftpd/vsftpd.conf следующее указание:
- **`banner_file=/etc/banners/ftp.msg`**
- Также дополнительные заголовки в ответ на входящие подключения можно отправлять с помощью оболочек TCP.
- ***Анонимный доступ***
- Присутствие каталога /var/ftp/ включает анонимную учётную запись.
- Проще всего создать этот каталог можно, установив пакет vsftpd. Этот пакет настраивает дерево каталогов для анонимных пользователей и даёт им в этих каталогах только право чтения.

Обеспечение безопасности сервера

- По умолчанию анонимный пользователь не может записывать ни в один каталог.
- Разрешая анонимный доступ к FTP-серверу, проверьте, где находятся важные данные.
- **Анонимная закачка**
- Чтобы анонимные пользователи могли закачивать файлы, рекомендуется создать каталог в /var/ftp/pub/ с правом только на запись.
- Для этого введите:
- `mkdir /var/ftp/pub/upload`
- Затем измените разрешения, чтобы анонимные пользователи не видели, что находится в каталоге:
- `chmod 730 /var/ftp/pub/upload`

Обеспечение безопасности сервера

- Этот каталог в **`ls -la`** будет выглядеть так:
- **`drwx-wx--- 2 root ftp 4096 Feb 13 20:05 upload`**
- Администраторы, разрешающие анонимным пользователям читать и писать в каталоги, часто обнаруживают, что их сервера становятся складом пиратского программного обеспечения.
- Кроме этого, для службы vsftpd добавьте в файл /etc/vsftpd/vsftpd.conf следующую строку:
- **`anon_upload_enable=YES`**

Обеспечение безопасности сервера

- ***Учётные записи пользователей***
- Так как в протоколе FTP имена и пароли пользователей передаются по незащищённым сетям в открытом виде, будет правильно, если вы запретите доступ к серверу пользователям с их учётными данными.
- Чтобы отключить учётные записи пользователей для vsftpd, добавьте в /etc/vsftpd/vsftpd.conf следующее указание:
- `local_enable=NO`

Обеспечение безопасности сервера

- **Ограничение учётных записей пользователей**
- Запретить доступ к FTP серверу определённым пользователям, например, root или другим с привилегиями sudo, легче всего с помощью файла PAM. Файл конфигурации PAM для vsftpd называется /etc/pam.d/vsftpd.
- Также можно отключить учётные записи непосредственно в самой службе.
- Чтобы отключить учётные записи пользователей в vsftpd, добавьте имя пользователя в /etc/vsftpd.ftpusers.

Обеспечение безопасности сервера

- **Определение открытых портов**
- После настройки сетевых служб важно обратить внимание на порты, принимающие подключения на сетевых интерфейсах. Любые открытые порты могут быть доказательством вторжения.
- Просмотреть открытые порты можно двумя способами. Менее надёжный способ — опросить сетевой стек с помощью команды netstat -an или lsof -i. Этот способ не очень надёжен, так как эти программы не подключаются к компьютеру по сети, а просто определяют, что происходит в системе. По этой причине, эти приложения часто подменяются нападающими. Таким способом взломщики пытаются скрыть свои следы, если они незаконно открыли порты.

Обеспечение безопасности сервера

- Другим более надёжным способом проверки открытых портов является использование сканера портов, например nmap.
- Следующая команда, запущенная с консоли, определяет, какие порты ждут TCP-соединений из сети:
- nmap -sT -O localhost
- Эта команда выводит примерно следующие результаты:
- **Starting nmap 3.55 (http://www.insecure.org/nmap/) at 2004-09-24 13:49 EDT**
- **Interesting ports on localhost.localdomain (127.0.0.1):**

Обеспечение безопасности сервера

- (The 1653 ports scanned but not shown below are in state: closed)
- PORT STATE SERVICE
- 22/tcp open ssh
- 111/tcp open rpcbind
- 113/tcp open auth
- 834/tcp open unknown
- Здесь видно, что работает portmap, так как запущена служба sunrpc. Однако есть и некая таинственная служба, открывшая порт 834. Чтобы проверить, не связан ли этот порт с какой-либо известной службой, введите:
- `cat /etc/services | grep 834`

Обеспечение безопасности сервера

- Эта команда не возвращает результата. Это означает, что хотя порт находится в зарезервированном диапазоне (от 0 до 1023) и для его открытия нужны права root, он не связан ни с одной известной службой.
- Затем проверьте, что о нём сообщит команда netstat или lsof. Чтобы проверить порт 834 с помощью netstat, выполните следующую команду:
- **`netstat -anp | grep 834`**
- Команда возвращает следующий результат:
- **`tcp 0 0 0.0.0.0:834 0.0.0.0:* LISTEN 653/ypbind`**

Обеспечение безопасности сервера

- То, что команда netstat показала этот порт, успокаивает, так как злоумышленник, открывший порт на взломанном компьютере, скорее всего, не захочет, чтобы эта команда его вывела. Кроме этого, параметр [p] показывает код процесса (PID) службы, открывшей порт. В данном случае открытый порт принадлежит RPC-службе ypbind (NIS), работающей совместно со службой portmap.
- Команда lsof показывает похожие сведения, так как она также может связать открытые порты со службами:
- `lsof -i | grep 834`

Обеспечение безопасности сервера

- Эти инструменты позволяют узнать о состоянии работающих на компьютере служб многое. Они очень гибки и могут предоставить массу информации о сетевых службах и их конфигурации. Поэтому очень рекомендуется обратиться к страницам man, посвящённым lsof, netstat, nmap и services.