ALTEX SOFT

ОТЧЁТ

№ отчёта	*6f41499b-024e-4f74-a557-97cc591300fb*
Профиль	*Конфигурации*
Задание	*Job_2993*
Формирование отчёта	*19.05.2015 16:15:43*
Имя	*Quick_192.168.100.101_1208*
Описание	*Автогенерируемый отчет вкладки "История" для "192.168.100.101" из "Job_2993" задания.*
Хосты [1]	*192.168.100.101*

Хост: 192.168.100.101

CPE	*cpe:/o:ubuntu:ubuntu_linux:14.04*
Начало/завершение сканирования	*19.05.2015 16:04:31 / 19.05.2015 16:07:10*
Профиль	*Имя профиля: root* *Sudo: Нет*
Агент	*Нет*

Конфигурация безопасности Ubuntu

Конфигурация не соответствует эталонной. Всего - 118, соответствие - 42 (36 %)

Соответствие (42) **Несоответствие (72)** **Ошибка (0)**
Не проверено (4) **Не выбрано (0)** **Неизвестно (0)**
Информация (0) **Исправлено (0)** **Неприменимо (0)**

- **Введение**
  - **Общие принципы**
    - **Шифорование передаваемых данных всегда, когда это возможно**
    - **Минимизация ПО для минимизации уязвимостей**
    - **Запуск различных сетевых сервисов на отдельных системах**
    - **Настройка специальных программных средств для улучшения устойчивости системы**
    - **Наименьшие привилегии**
  - **Как использовать данное руководство**
    - **Следование разделам полностью и по порядку**
    - **Тестирование не на рабочих системах**
    - **Наличие командной строки суперпользователя**
    - **Соглашения по форматированию**
    - **Перезагрузка системы**
- **Системные настройки**
  - **Установка и обслуживание ПО**
    - **Разметка диска**
      - Директория /tmp располагается на отдельном разделе
      - Директория /var располагается на отдельном разделе

- ✗ Директория /var/log располагается на отдельном разделе
- ✗ Директория /home располагается на отдельном разделе

- ⏸ **Обновление программного обеспечения**
  - ⏸ Все обновления ПО должны быть установлены
  - ⏸ Проверка валидности документа sources.list
- ⏸ **Проверка целостности ПО**
  - ⏸ Проверка системы перед внесением изменений

- ✗ **Права доступа к файлам и маски**
  - ✓ **Ограничение параметров монтирования разделов**
    - ✓ Добавление nodev, nosuid опции для съемных носителей
    - ✓ Добавление опции nodev для /home и /tmp разделов
  - ⏸ **Ограничения динамического монтирования и отключения файловых систем**
  - ✗ **Проверка прав доступа у важных файлов и директорий**
    - ✗ **Проверка прав доступа у файлов, содержащих информацию о локальные учётных записях**
      - ✗ Ограничить права на crontab файл
      - ✓ Установить umask для пользователей по умолчанию
      - ✓ Проверка владельца shadow файла
      - ✓ Проверка группы владельца файла shadow
      - ✓ Проверка прав доступа файла shadow
      - ✓ Проверка владельца файла group
      - ✓ Проверка группы владельца файла group
      - ✓ Проверка прав доступа к файлу group
      - ✓ Проверка владельца файла passwd
      - ✓ Проверка группы владельца файла passwd
      - ✓ Проверка прав доступа к файлу passwd
    - ✓ **Проверка прав доступа для файлов внутри важных системных директорий**
      - ✓ Проверка прав доступа разделяемых библиотек
      - ✓ Проверка, что владельцем разделяемых библиотек является суперпользователь
      - ✓ Проверка прав доступа исполняемых файлов
      - ✓ Проверка, что владельцем системных исполняемых файлов является суперпользователь
    - ✓ Отсутствие '.' или Group/World-Writable Directory в $PATH
  - ✗ **Ограничение программ от возможного опасного повидения**
    - ✗ Отключить дампы памяти

- ✗ **SELinux**
  - ✗ **Включение SELinux**
    - ⏸ **Установка SELinux**
    - ✗ Проверка, что SELinux установлен
    - ✓ Проверка, что SELinux не отключен в настройках GRUB
    - ✗ Проверка, что SELinux задан в режим Enforcing

- ✗ **Учётные записи и контроль доступа**
  - ✗ **Защита учётных записей с помощью ограничения входа по паролю**
    - ✗ **Ограничение входа суперпользователя**
      - ✗ Включить системы учёта
      - ✗ Ограничить доступ к root через su
      - ✓ Ограничение входа суперпользователя в виртуальную консоль
      - ✗ Ограничение входа суперпользователя через последовательный порт

- ✗ Обеспечение безопасности оболочки при входе под системной учётной записью
- ✓ Проверка, что только у суперпользователя UID 0

✓ **Проверка правильности хранения и существования хэшей паролей**

- ✓ Удалить файлы .netrc
- ✓ Предотвращение входа в аккаунт с пустым паролем
- ✓ Проверка на скрытость хэшей паролей во всех аккаунтах

✗ **Установка параметров срока действия пароля**

- ✗ Установка минимальной длины пароля при входе
- ✗ Установка минимального срока действия пароля
- ✗ Установка максимального срока действия пароля
- ✓ Установка предупреждения о сроке действия пароля

✗ **Защита аккаунтов с помощью настройки PAM**

✗ **Установка требований качества пароля**

✗ **Установка требований качества пароля, используя pam_cracklib**

- ✓ Убедиться, что не символа '+' в файле /etc/passwd, /etc/shadow, /etc/group
- ✗ Установка минимального количества цифровых символов для устойчивости пароля
- ✗ Установка минимального количества заглавных символов для устойчивости пароля
- ✗ Установка минимального количества специальных символов для устойчивости пароля
- ✗ Установка минимального количества строчных символов для устойчивости пароля
- ✗ Установка минимального количества различающихся символов для устойчивости пароля

✗ **Установка блокировки после неудачных попыток ввода пароля**

- ✗ Установка запрета после неудачных попыток ввода пароля
- ✗ Ограничение повторного использования пароля

✓ **Защита доступа к физической консоли**

- ✓ Требование аутентификации для однопользовательского режима

⏸ **Настройка блокировки экрана**

✗ **Настройка сети и брандмауэра**

✗ **Параметры ядра, которые влияют на сеть**

✗ **Параметры сети только для хостов**

- ✗ Отключение параметра ядра для отправки перенаправлений ICMP по умолчанию
- ✗ Отключение параметра ядра для отправки перенаправлений ICMP для всех интерфейсов
- ✓ Отключение параметра ядра для IP Forwarding

✗ **Параметры ядра, влияющие на сеть для хостов и маршрутизаторов**

- ✗ Отключение параметра ядра для приема ICMP перенаправлений для всех интерфейсов
- ✗ Отключение параметра ядра для принятия безопасных перенаправлений для всех интерфейсов
- ✗ Включение параметра ядра для журналирования Martian Packets
- ✗ Настройка параметра ядра для задания максимального числа осиротевших сокетов
- ✗ Отключение параметра ядра для принятия Source-Routed пакетов по умолчанию
- ✗ Отключение параметра ядра для приема ICMP перенаправлений по умолчанию
- ✗ Отключение параметра ядра для приема защищенных перенаправлений по умолчанию
- ✓ Включение параметра ядра для игнорирования ICMP Broadcast Echo запросов
- ✓ Включение параметра ядра для использования TCP Syncookies
- ✓ Включение параметра ядра для использования фильтрации обратного пути у всех интерфейсов
- ✓ Включение параметра ядра для использования фильтрации обратного пути по умолчанию

⏸ **Беспроводные сети**

⏸ **Отключение беспроводной сети посредством конфигурации ПО**

- **IPv6**
  - **Отключение поддержки IPv6 только при необходимости**
  - **Настройка IPv6, если необходимо**
    - **Отключение автоматической конфигурации**
  - **IPTables и Ip6tables**
  - **Просмотр и активация правил по умолчанию**
  - **Усиление набора правил по умолчанию**
  - **Редкие сетевые протоколы**
- **Настройка Syslog**
- **Проверка, что все журналы ротируются logrotate**
  - Проверка, что Logrotate периодически запускается
- **Система учета с журналированием (auditd)**
  - Включение аудита процессов, которые запускаются раньше, чем служба аудита
  - **Настройка хранения данных auditd**
    - Настройка auditd количества нераспределенных журналов
    - Настройка auditd максимального размера файла журнала
    - Настройка auditd действия при достижении максимального размера журнала
    - Настройка действия admin_space_left при недостаточном месте на диске
    - Настройка auditd для использования плагина audispd
  - **Настройка комплекса правил auditd**
    - **Запись событий, изменяющих информацию о дате и времени**
      - Запись событий, изменяющих время через adjtimex
      - Запись событий, изменяющих время через settimeofday
      - Запись событий, изменяющих время через stime
      - Запись событий, изменяющих время через clock_settime
      - Запись событий, изменяющих время файла
    - Запись событий, которые изменяют информацию о пользователях/группах
    - Запись событий, которые изменяют системное сетевое окружение
    - Журналы аудита системы должны иметь права 0640 или менее разрешающие
    - Журналы аудита системы должны принадлежать суперпользователю
    - Запись событий, которые изменяют системы обязательного контроля доступа
    - **Запись событий, которые изменяют системные права доступа**
      - Запись событий, которые изменяют системные права доступа - chmod
      - Запись событий, которые изменяют системные права доступа - chown
      - Запись событий, которые изменяют системные права доступа - fchmod
      - Запись событий, которые изменяют системные права доступа - fchmodat
      - Запись событий, которые изменяют системные права доступа - fchown
      - Запись событий, которые изменяют системные права доступа - fchownat
      - Запись событий, которые изменяют системные права доступа - fremovexattr
      - Запись событий, которые изменяют системные права доступа - fsetxattr
      - Запись событий, которые изменяют системные права доступа - lchown
      - Запись событий, которые изменяют системные права доступа - lremovexattr
      - Запись событий, которые изменяют системные права доступа - lsetxattr
      - Запись событий, которые изменяют системные права доступа - removexattr
      - Запись событий, которые изменяют системные права доступа - setxattr
    - Проверка, что auditd собирает информацию о не авторизованных доступах к файлам

- ✗ Проверка, что auditd собирает информацию об использовании привилегированных команд
- ✗ Проверка, что auditd собирает информацию об экспорте носителей
- ✗ Проверка, что auditd собирает информацию об удалении файлов пользователем
- ✗ Проверка, что auditd собирает действия системного администратора
- ✗ Проверка, что auditd собирает информацию о загрузка и выгрузке модулей ядра

✗ **Службы**

- ✓ **Устаревшие службы**
  - ✓ **Xinetd**
    - ✓ Удаление пакета xinetd
  - ✓ **Telnet**
    - ✓ Удаление пакета telnet-server
  - ✓ **Rlogin, Rsh, и Rexec**
    - ✓ Удаление файлов доверия Rsh
  - ⏸ **Информационная служба сети (NIS)**
  - ✓ **TFTP сервер**
    - ✓ Удаление пакета tftpd
- ⏸ **Базовые службы**
- ✓ **Службы Cron и At**
  - ✓ Включение службы cron
- ✗ **SSH сервер**
  - ✗ **Настройка OpenSSH сервер**
    - ✓ Разрешить только SSH Protocol 2
    - ✓ Выключение в SSH RhostsRSAAuthentication
    - ✓ Отключение SSH поддержки .rhosts файлов
    - ⏸ Ограничение пользователям SSH доступа
    - ✗ Установка SSH интервала времени ожидания
    - ✗ Установка SSH Client Alive Count
    - ✓ Отключение Host-Based аутентификации
    - ✗ Отключение возможности авторизации суперпользователя в SSH
    - ✓ Отключение SSH доступа с пустыми паролями
    - ✗ Включение SSH предупреждающего баннера
    - ✗ Не разрешать SSH переменные окружения
    - ✗ Использование только принятых алгоритмов шифрования
- ⏸ **X Window System**
  - ⏸ **Отключение X Windows**
- ⏸ **Avahi сервер**
  - ⏸ **Отключение Avahi сервера, если это возможно**
- ⏸ **DHCP**
  - ⏸ **Отключение DHCP клиента**
- ⏸ **Network Time Protocol**
- ⏸ **Сервер электронной почты**
  - ⏸ **Настройка SMTP для почтовых клиентов**
- ⏸ **LDAP**
  - ⏸ **Настройка клиентов OpenLDAP**
  - ⏸ **Настройка OpenLDAP сервера**
- ⏸ **NFS и RPC**

Описание параметров

Группа	
Название	**Введение**
Описание	

Цель этого руководства - предоставить рекомендации по конфигурации безопасности и основные руководящие принципы конфигурации системы на базе Ubuntu. Это руководство разработано для системных администраторов, которые владеют базовыми навыками администрирования unix-систем. Все инструкции должны соблюдаться полностью и с пониманием их смысла, чтобы предотвратить возможные неблагоприятные последствия и проблемы в безопасности системы.

Группа	
Название	**Общие принципы**
Описание	

Следующие общие принципы служат основой для большей части рекомендаций из этого руководства и должны влиять на решения по конфигурации системы, которые явно здесь не описанны.

Группа	
Название	**Шифорование передаваемых данных всегда, когда это возможно**
Описание	

Любые передаваемые данные по сети, проводной или беспроводной подвержены пассивному мониторингу. Всякий раз, когда существует практическая возможность для шифрования, она должна использоваться. Даже если предполагается, что данные будут переданы только по локальной сети, они все равно должны быть зашифрованы. Шифрование данных авторизации, таких как пароли, особенно важно. Сети из машин под управлением Ubuntu могут и должны быть сконфигурированны так, чтобы незашифрованные данные вообще не передавались между машинами.

Группа	
Название	**Минимизация ПО для минимизации уязвимостей**
Описание	

Наиболее простой путь избежать уязвимостей в ПО - не устанавливать ПО. В Ubuntu менеджер пакетов позволяет управлять наборами ПО, установленного в системе. Установленное ПО предоставляет несколько путей для возникновения уязвимостей. Пакеты, включающие программы с Suid флагами могут обеспечить атакующего потенциальной возможностью повышения привилегий. Пакеты, включающие сетевые сервисы, могут дать возможность для сетевых атак. Пакеты, содержащие программы, запускаемые под локальными пользователями (т.е. после графического логина), могут предоставлять возможности для запуска троянского ПО и других типов скрытого выполнения кода. Число пакетов, установленных в системе, практически всегда может быть значительно урезано, за исключением ПО, которое необходимо для выполнения возложенных на систему задач.

Группа	
Название	**Запуск различных сетевых сервисов на отдельных системах**
Описание	

Когда это возможно, сервер должен быть сконфигурирован для обслуживания только одного сетевого сервиса. Это ограничит число других сервисов, которые могут быть подвержены риску в случае успешной атаки на один из таких сервисов.

Группа

Название **Настройка специальных программных средств для улучшения устойчивости системы**

Описание

Существует несколько специальных программных средств, которые могут эффективно использоваться для улучшения устойчивости системы и детектирования неизвестных атак. Эти средства могут значительно улучшить устойчивость к атакам ценой сравнительно небольших усилий по их конфигурации. В частности, данное руководство рекомендует использовать IPtables в качестве сетевого экрана системы, SELinux для защиты против уязвимых служб, а так же логиррование и аудит событий для обнаружения проблем.

Группа

Название **Наименьшие привилегии**

Описание

Предоставление наименьших привилегий необходимо как пользователям так и ПО для выполнения задач. Для примера, утилита `sudo` может быть применена для ограничения авторизации как суперпользователь на системах с разграниченим обязанностей администраторов. Другой пример - это предоставление возможности входа в систему только для тех администраторов, которые должны выполнять административные задачи на этой системе. Использование SElinux так же следует принципу наименьших привилегий: политики SELinux позволяют ограничить ПО только теми действиями, которые были специально разрешены. Это могут быть гораздо более строгие ограничения, чем действия, допустимы в традиционной модели Unix привилегий.

Группа

Название **Как использовать данное руководство**

Описание

Администраторы должны придерживаться следующих правил.

Группа

Название **Следование разделам полностью и по порядку**

Описание

Каждый раздел может содержать информацию и рекомендации, обсуждаемые в вышележащем разделе. Каждый раздел должен быть полность прочитан и понят. Интрукции никогда не должны слепо выполняться. Конфигурации системы из главы 2 "Системные настройки" должны быть применены ко всем машинам. Руководства по отдельным сервисам из главы 3 "Службы" должны быть применены ко всем машинам таким образом: если машина является либо клиентом, либо сервером службы - применяются соответствующие правила, иначе служба должна быть отключена в соответствии с инструкциями.

Группа

Название **Тестирование не на рабочих системах**

Описание

Правила из данного руководства должны быть протестированны на тестовых стендах до окончательного развёртывания на рабоччих серверах. Конфигурация тестовых стендов должна как можно ближе приближаться к конфигурации рабочих серверов.

Группа

Название	**Наличие командной строки суперпользователя**
Описание	

Большинство действий, описанных в руководстве, предполагают, что они будут выполены от лица суперпользователя root через командную оболочку `/bin/bash`. Команды с предшествующим знаком # предполагают, что администратор выполнит такую команду от имени суперпользователя, т.е. воспользуется командой `sudo`, когда это возможно, либо будет использовать команду `su` для повышения привилегий, когда `sudo` не может быть использована. Команды, которые могут быть выполнены от лица непривилегированного пользователя, помечаются знаком $.

Группа	
Название	**Соглашения по форматированию**
Описание	

Команды, предназначенные для выполнения в командной строке, а также текст конфигурационных файлов помечается `моноширинным шрифтом`. ***Курсив*** используется для обозначения случаев, когда администратор должен заменить соответствующую информацию в команде или конфигурационом файле.

Группа	
Название	**Перезагрузка системы**
Описание	

Перезагрузка системы явно требуется после некоторых действий для завершения конфигурации системы. Во многих случаях изменения не вступят в силу до перезагрузки. В случае уверенности, что изменения применились правильно и для проверки функциональности всегда перезагружайте систему после применения группы рекомендаций из данного руководства.

Группа	
Название	**Системные настройки**

Группа	
Название	**Установка и обслуживание ПО**
Описание	

Следующий раздел содержит рекомендации, связанные с безопасностью системы в процессе установки и обновления ПО.

Группа	
Название	**Разметка диска**
Описание	

Для обеспечения принципа разделяемости и защищённости данных существуют высокоуровневые системные директории, которые следует располагать на раздельных физических разделах или логических томах. Схема разбиения диска по умолчанию инсталлятором создаёт отдельные логические тома для корневой системы `/`, файлов загрузчика `/boot` и подкачки `swap`.

- Если происходит установка с уже существующей разметкой диска, необходимо установить галочку "Review and modify partitioning." (Просмотр и изменение структуры разделов). Это позволит легко создать дополнительные логические тома внутри уже созданной группы томов, хотя это может потребовать уменьшение логического тома корневого раздела `/` для создания дополнительного свободного пространства. В общем случае, использование логических томов предпочтительно использованию разделов, т.к. они могут быть легко модифицированны позднее.

- Если создаётся произвольная разметка, необходимо создать разделы, упомянутые в предыдущем параграфе (которые нужны инсталлятору в любом случае), а также разделить их, как описано в следующих разделах руководства.

Если система уже была установлена и использовалась схема разбиения по умолчанию, то возможно, хотя и нетривиально, модифицировать её для создания отдельных логических томов для каталогов, перечисленных выше. Использование менеджера логических томов (LVM) делает это возможным.

Параметр Критичность: Низкий

Название **Директория /tmp располагается на отдельном разделе**

Описание

Директория `/tmp` доступна для всех на запись и используется для хранения временных файлов. Необходимо убедиться во время установки, что она располагается на отдельном разделе или логическом томе, либо перенести её позднее, используя LVM.

Параметр Критичность: Низкий

Название **Директория /var располагается на отдельном разделе**

Описание

Директория `/var` используется службами и другими системными сервисами для хранения часто изменяющихся данных. Необходимо убедиться во время установки, что она располагается на отдельном разделе или логическом томе, либо перенести её позднее, используя LVM.

Параметр Критичность: Низкий

Название **Директория /var/log располагается на отдельном разделе**

Описание

Директория `/var/log` служит для хранения системных логов. Необходимо убедиться во время установки, что она располагается на отдельном разделе или логическом томе, либо перенести её позднее, используя LVM.

Параметр Критичность: Низкий

Название **Директория /home располагается на отдельном разделе**

Описание

Если домашние директории пользователей будут хранится локально, необходимо в процессе установки создать отдельный раздел под `/home`, либо перенести его позднее, используя LVM. Если директория `/home` будет монтироваться с другой системы, например, с NFS сервера, тогда создание отдельного раздела под `/home`, в процессе установки не является необходимостью, и точка монтирования может быть сконфигурирована позже.

Группа

Название **Обновление программного обеспечения**

Описание

Утилита командной строки `apt-get` используется для установки и обновления ПО. Также система предоставляет графический пакетный менеджер: `synaptic`. `synaptic` - графическая обёртка для `apt-get`, которая позволяет пользователям устанавливать и обновлять пакеты.

Система Ubuntu содержит встроенный каталог установленных программ, которая содержит метаданные всех установленных пакетов. Утилиты `apt-get` и `synaptic` взаимодействуют с базой данных для обеспечения целостности всех метаданных в соответствии с установленным ПО и обновлениями безопасности, поэтому их использование крайне предпочтительно.

Параметр Критичность: Высокий

Название **Все обновления ПО должны быть установлены**

Описание

Для получения всех последних обновлений системы необходимо выполнить команду
`# apt-get update`
. Ubuntu-администраторам рекомендуется подписаться на рассылку (http://lists.Ubuntu.org/Ubuntu-security-announce/), чтобы быть в курсе проблем безопасности.

Параметр Критичность: Высокий

Название **Проверка валидности документа sources.list**

Описание

Необходимо регулярно проверять валидность документа sources.list, потому команды apt-get, dselect, aptitude опираются на него.

Группа

Название **Проверка целостности ПО**

Описание

И AIDE (Advanced Intrusion Detection Environment) и система управления пакетами предоставляют механизмы для проверки целостности установленного ПО. AIDE - приемник хорошо известного ПО для проверки целостности Tripwire. Система управления пакетами может производить проверку целостности путём сравнения информации из её базы метаданных с файлами, установленными в системе

Проверка целостности не может *предотвратить* вторжение в систему, но может детектировать, что оно произошло. Требования по проверки целостности могут сильно зависеть от окружения, в котором будет использоваться система.

Параметр Критичность: Средний

Название **Проверка системы перед внесением изменений**

Описание

Убедитесь, что ваша система функционирует должным образом прежде чем изменить правила. После применения данной конфигурации найти неисправности будет сложнее.

Группа

Название **Права доступа к файлам и маски**

Описание

В традиционных Unix системах, безопасность в значительной мере опирается на права доступа для файлов и директорий, для предотвращения несанкционированного доступа пользователей от чтения и изменения файлов, к которым им не следует иметь доступ. Соблюдение принципа наименьших привелегий - предоставление минимальных прав доступа для каждого файла, директории и файловой системы в зависимости от их назначения.

Некоторые команды в этом разделе сканируют файловую систему для поиска файлов или каталогов с определенными характеристиками и предназначены для запуска на каждом локальном разделе данной машины. Когда переменная *PART* появляется в одной из команд ниже, это означает, что команда предназначена для запуска неоднократно с именем каждого локального раздела заменяющего часть команды *PART* по очереди.

Следующая команда выводит список разделов с файловой системой ext4 на локальной машине, которая является фаловой системой по умолчанию.

```
$ mount -t ext4 | awk '{print $3}'
```
Если ваша система использует тип локальной файловой системы, отличный от ext4, то вы должны изменить эту команду.

Группа

Название **Ограничение параметров монтирования разделов**

Описание

Система разделов может быть установлена с определенными параметрами, которые ограничивают какие файлы в данном разделе могут выполняться. Эти опции задаются в `/etc/fstab` конфигурационном файле, и используются для усложнения задачи различных типов вредоносного поведения.

Параметр Критичность: Низкий

Название **Добавление nodev, nosuid опции для съемных носителей**

Описание

Необходимо добавить опцию `nodev, nosuid` в четвёртую колонку файла /etc/fstab для строки, которая отвечает за монтирование различных подключаемых разделов (cdrom или floppy).

Параметр Критичность: Низкий

Название **Добавление опции nodev для /home и /tmp разделов**

Описание

Опция nodev предотвращает интерпретирование файлов в качестве символьного или блочного устройства. Истинные символьные и блочные устройства должны находиться только в каталоге `/dev` на корневом разделе или в `chroot` окружении, собраном для системных сервисов. Необходимо добавить опцию `nodev` в четвёртую колонку файла `/etc/fstab` для строки, которая отвечает за монтирование /home и /tmp разделов.

Группа

Название **Ограничения динамического монтирования и отключения файловых систем**

Описание

Linux включает в себя ряд средств для автоматизированного добавления и удаления файловых систем на работающей системе. Эти средства могут повысить удобство, но все они приносят некоторый риск - будь то прямой риск, позволяющий обычным пользователям представить произвольные файловые системы на машине, или риск того, что программные ошибки в автоматизированном монтировании сами позволят злоумышленнику скомпрометировать систему.

Эта команда может быть использована для вывода списка типов файловых систем, которые доступны в данный момент выполняемого ядра:
```
# find /lib/modules/`uname -r`/kernel/fs -type f -name '*.ko'
```
Если эти файловые системы не требуется, то они должны быть явно отключено в соответствующем `/etc/modprobe.d` файле конфигурации.

Будьте осторожны при включении любого такого объекта, а также необходимо понять, что лучшее управление конфигурацией или обучение пользователей может решать те же задачи с меньшим риском.

Группа

Название **Проверка прав доступа у важных файлов и директорий**

Описание

Права доступа для многих системных файлов должны быть установлены должным образом, чтобы быть уверенным, что важная информация достаточно защищена. В данном разделе рассматриваются ограничения прав доступа для важных

системных файлов, которые могут быть проверены, для гарантии их целостности.

Группа

Название **Проверка прав доступа у файлов, содержащих информацию о локальные учётных записях**

Описание

Значения прав доступа по умолчанию для системных файлов, которые представляют собой важные базы данных безопасности, такие как `passwd`, `shadow`, `group` и `gshadow` должны сохраняться. Многие утилиты нуждаются в доступе на чтение к файлу `passwd` для нормального функционирования, однако доступ на чтение к файлу `shadow` позволяет производить атаки, направленные на взлом паролей, и должен быть отключён.

Параметр Критичность: Средний

Название **Ограничить права на crontab файл**

Описание

Системные файлы crontab доступны только демону cron (с привилегиями суперпользователя) и команде crontab (запускаемая от root). Если непривилегированным пользователям дать права на чтение или (что ещё хуже) модификацию системных crontab файлы, то это может привести к повышению привилегий локального пользователя. Для правильного задания прав и группы, необходимо выполнить команды:

```
# chmod 400 /etc/crontab
# chmod -R 770 /var/spool/cron/
# chown -R 0 /var/spool/cron/
```

Параметр Критичность: Средний

Название **Установить umask для пользователей по умолчанию**

Описание

По умолчанию значение umask = 077 - значение, согласованное в рамках процесса консенсуса DISA и NSA. Файлы и директории, созданные пользователем, не могут быть прочитаны другими пользователями. Что бы установить umask для пользователей по умолчанию, необходимо выполнить команды:

```
# echo "umask 077" >> $FILE
#chown root:root $FILE
#chmod 444 $FILE
```

где $FILE это /etc/csh.login, /etc/csh.cshrc, /etc/bash.bashrc, если такие директории существуют. А так же необходимо выполнить

```
# echo "umask 077" >> $FILE
#chown root:root $FILE
```

где $FILE это /root/.profile, /root/.bash_profile, /root/.bashrc, /root/.cshrc, /root/.tcshrc, если такие файлы существуют.

Параметр Критичность: Средний

Название **Проверка владельца shadow файла**

Описание

Для правильного задания владельца файла `/etc/shadow`, необходимо выполнить команду

```
# chown root /etc/shadow
```

Параметр Критичность: Средний

Название **Проверка группы владельца файла shadow**

Описание

Для правильного задания группы владельца файла `/etc/shadow`, необходимо выполнить команду
```
# chgrp shadow /etc/shadow
```

Параметр Критичность: Средний

Название **Проверка прав доступа файла shadow**

Описание

Для правильного задания прав доступа к файлу `/etc/shadow`, необходимо выполнить команду:
```
# chmod 640 /etc/shadow
```

Параметр Критичность: Средний

Название **Проверка владельца файла group**

Описание

Для правильной установки владельца файла `/etc/group`, необходимо выполнить команду
```
# chown root /etc/group
```

Параметр Критичность: Средний

Название **Проверка группы владельца файла group**

Описание

Для правильной установки группы владельца файла `/etc/group`, необходимо выполнить команду:
```
# chgrp root /etc/group
```

Параметр Критичность: Средний

Название **Проверка прав доступа к файлу group**

Описание

Для правильной установки прав доступа файла `/etc/group`, необходимо выполнить команду:
```
# chmod 644 /etc/group
```

Параметр Критичность: Средний

Название **Проверка владельца файла passwd**

Описание

Для правильной установки владельца файла `/etc/passwd`, необходимо выполнить команду:
```
# chown root /etc/passwd
```

Параметр Критичность: Средний

Название **Проверка группы владельца файла passwd**

Описание

Для правильной установки группы владельца файла `/etc/passwd`, необходимо выполнить команду:
```
# chgrp root /etc/passwd
```

Параметр Критичность: Средний

Название **Проверка прав доступа к файлу passwd**

Описание

Для правильной установки прав доступа файла `/etc/passwd`, необходимо выполнить команду:

```
# chmod 0644 /etc/passwd
```

Группа

Название **Проверка прав доступа для файлов внутри важных системных директорий**

Описание

Некоторые директории содержат файлы, защищённость и целостность которых особенно важна и которые могут быть уязвимы после неправильной настройки системы, в частности, если ПО устанавливается в обход пакетного менеджера.

Параметр Критичность: Средний

Название **Проверка прав доступа разделяемых библиотек**

Описание

Системные разделяемые библиотеки, которые линкуются с выполняемыми файлами в процессе загрузки и работы системы, располагаются в следующих директориях по умолчанию:

```
/lib
/lib64
/usr/lib
/usr/lib64
```

Если любой из файлов в этой директории имеет права на запись для всех пользователей или для пользователей из группы владельца, то их необходимо скорректировать командой

```
# chmod go-w путь к файлу
```

Параметр Критичность: Средний

Название **Проверка, что владельцем разделяемых библиотек является суперпользователь**

Описание

Системные разделяемые библиотеки, которые линкуются с выполняемыми файлами в процессе загрузки и работы системы, располагаются в следующих директориях по умолчанию:

```
/lib
/lib64
/usr/lib
/usr/lib64
```

```
# chown root путь к файлу
```

Параметр Критичность: Средний

Название **Проверка прав доступа исполняемых файлов**

Описание

Системные исполняемые файлы располагаются в следующих директориях по умолчанию:

```
/bin
/usr/bin
/usr/local/bin
```

```
/sbin
/usr/sbin
/usr/local/sbin
```
Все файлы из этих директорий не должны быть доступны на запись для всех учётных записей, в том числе входящих в группу владельца. Если любой из файлов в этих директориях имеет права на запись для всех пользователей или для пользователей из группы владельца, то их необходимо скорректировать командой
```
# chmod go-w путь к файлу
```

Параметр	Критичность: Средний
Название	**Проверка, что владельцем системных исполняемых файлов является суперпользователь**
Описание	

Системные исполняемые файлы располагаются в следующих директориях по умолчанию:
```
/bin
/usr/bin
/usr/local/bin
/sbin
/usr/sbin
/usr/local/sbin
```
Все файлы в этих директориях должны иметь владельцем суперпользователя `root`. Если будут найдены файлы, имеющие другого владельца, необходимо его скорректировать путём выполнения команды
```
# chown root путь к файлу
```

Параметр	Критичность: Средний
Название	**Отсутствие '.' или Group/World-Writable Directory в $PATH**
Описание	

Проверка на отсутствие '.' или Group/World-Writable Directory в $PATH. Для установки данных правил необходимо использовать команду:
```
find `echo $PATH | tr ':' ' '` -type d -exec chmod go-w {} \;
```
Для групп и остальных, права доступа к директориям в $PATH не должны быть доступны для записи.

Группа	
Название	**Ограничение программ от возможного опасного повидения**
Описание	

Рекомендации в данном разделе предназначены для обеспечения системных функций защиты от потенциально опасного активного выполнения программы. Эти меры защиты применяются при инициализации системы или уровня ядра, и защищают от некоторых видов плохо настроенных или скомпрометированных программ.

Параметр	Критичность: Средний
Название	**Отключить дампы памяти**
Описание	

Дампы памяти могут занимать большой объём диска и содержать конфиденциальные данные. Файл limits.conf может быть использован для предоставления возможности дампа памяти индивидуальным пользователям или группы пользователей. В файл /etc/security/limits.conf необходимо добавить либо раскомментировать строки:
```
* soft core 0
* hard core 0
```

Группа	

Название	**SELinux**

Описание

SELinux является настройкой ядра Linux, которая может защищать от неправильных или скомпрометированных программ. SELinux осуществляет идею того, что программы должны быть ограничены в том, к каким файлам они могут обращаться и какие действия они могут выполнять. По умолчанию политика SELinux, используется на Ubuntu, достаточно развита и отлажена, должна быть доступна практически на любой машине с минимальной конфигурацией и низким значением подготовки системных администраторов. Данная политика защищает системные службы - включая большинство из общих видимых сетевых служб, таких как почтовые серверы, ftp серверы, и DNS серверы - от доступа к файлам, к которым эти службы не должны обращаться в процессе своей работы. Данное действие может предотвратить огромное количество возможных повреждений от сетевых атак против служб, от троянских программ, и др. Данное руководство реккомендует, чтобы SELinux был включен по умолчанию(targeted) в каждой системе, если эта система имеет требования, которые делают строгую политику соответствующей.

Группа

Название	**Включение SELinux**

Описание

Неоходимо отредактировать файл `grub.conf`, удостоверившить, что SELinux включен в каждой из строк параметров ядра. Директива `SELINUX=enforcing` включает SELinux во время загрузки. Если SELinux подозревается в причастности к проблемам во время загрузки, можно загрузиться только в предупреждающем режиме для отладки `SELINUX=permissive`. По умолчанию конфигурация SELinux должна быть настроена так, чтобы большинство систем загружались без серьёзных проблем. Некоторые приложения, которые требуют нестандартных системных привелегий, таких как приложения виртуальной машины, могут быть не совместимы с SELinux в данной конфигурации по умолчанию. Тем не менее, это должно быть редкостью, и поддержка приложений SELinux продолжает улучшаться. В других случаях, SELinux может выявить необычные или небезопасные по поведению программы. Директива `SELINUXTYPE=targeted` настраивает по умолчанию целенаправленную политику безопасности.

Группа

Название	**Установка SELinux**

Описание

1. Если Вы не используете стандартное ядро Linux, предоставленное Debian, Вы должны убедиться, что Вы используете совместимое с SELinux и с файловой системой.
2. Получить политики по умолчанию и базовый набор SELinux утилит можно, выполнив: apt-get install selinux-basics selinux-policy-default auditd
3. Далее следует выполнить: update-initramfs -u
4. После чего необходимо настроить GRUB, PAM и создать /.autorelabel, выполнив: selinux-activate
5. Выполните перезагрузку. Это займет некоторое время, чтобы промаркировать файловые системы, а затем система автоматически перезагрузится второй раз.
6. Выполнив check-selinux-installation можно проверить правильно ли выполнена установка и посмотреть проблемы SELinux. (ПРИМЕЧАНИЕ: предупреждение о /etc/pam.d/login - это ложный результат)

Теперь Вы должны иметь рабочую систему SELinux, которая находится в режиме permissive. После того, как Вы убедитесь в том, что система работает, необходимо включить SELinux в настройках GRUB и задать режим enforcing.

Параметр Критичность: Средний

Название	**Проверка, что SELinux установлен**

Описание

Если пакет selinux-basics не установлен, необходимо выполнить команду: `apt-get install selinux-basics`

Источники

CCE-26956-3
http://cce.mitre.org

Параметр Критичность: Средний

Название **Проверка, что SELinux не отключен в настройках GRUB**

Описание

С помощью специального аргумента из параметров загрузки ядра в файле `/boot/grub/grub.cfg`, SELinux может быть отключен во время загрузки. Необходимо удалить все вхождения строки `selinux=0` из параметров ядра в этом файле, чтобы избежать выключения SELinux при загрузке.

Источники

CCE-26956-3
http://cce.mitre.org

Параметр Критичность: Средний

Название **Проверка, что SELinux задан в режим Enforcing**

Описание

SELinux должен быть установлен в режим `enforcing` во время загрузки системы. В файле `/etc/selinux/config`, необходимо добавить или исправить следующие строки для настройки системы, чтобы выполнить загрузку в принудительном режиме:
`SELINUX=enforcing`

Источники

CCE-26969-6
http://cce.mitre.org

Группа

Название **Учётные записи и контроль доступа**

Описание

В традиционной безопасности Unix, если злоумышленник получает доступ к определённой учётной записи входа в систему, то он может выполнять любые действия или получить доступ к любому файлу, к которому имеет доступ данная учётная запись. Кроме того, усложнение получения доступа неавторизованных пользователей к командной строке аккаунта, особенно привилегированных, является необходимой частью безопасности системы. В данном разделе представлены механизмы для ограничения доступа к учётным записям под Ubuntu.

Группа

Название **Защита учётных записей с помощью ограничения входа по паролю**

Описание

Традиционно, учётные записи Unix доступны и предоставляют имя и пароль в программу входа, которые проверяются на корректность использования в `/etc/passwd` и `/etc/shadow` файлах. Вход в систему по паролю уязвим к подбору слабых паролей, к сниффингу пакетов, и к MITM-атаке, против введённых паролей по-сети или в небезопасных консолях. Таким образом, механизмы для доступа к учётным записям при помощи ввода имени и пароля должны быть ограничены тем, кому они оперативно необходимы.

Группа

Название **Ограничение входа суперпользователя**

Описание

Прямой вход через суперпользователя должен быть доступен только при экстренной необходимости. В нормальных ситуациях, администратор должен получить доступ к системе с помощью уникальной непривелигерованной учёной

записи, и использовать su или sudo для выполнения привеллигерованных команд. Контроль учётной записи суперпользователя осуществляется ведением журнала аудита для организаций с несколькими администраторами. Блокирование каналов, через которые администратор может напрямую соединиться, также уменьшает возможности для подбора пароля к учётной записи суперпользователя. Программа login использует файл /etc/securetty для определения того, через какие интерфейсы может войти суперпользователь. Виртуальные устройства /dev/console и /dev/tty* представляют собой систему консолей (доступную через Ctrl-Alt-F1, Ctrl-Alt-F6 клавиатурные последовательности, установленные по умолчанию). По умолчанию файл безопасности также содержит /dev/vc/*. Вероятно, они будут устаревшими в большинстве сред, но они могут быть сохранены для совместимости. Суперпользователь не должен иметь возможности авторизации по сети через интернет протоколы. Другие разделы данного описавают, как предотвратить вход суперпользователя через SSH.

Параметр	Критичность: Средний
Название	**Включить системы учёта**
Описание	

Система учёта собирает базовые системные данные каждые 10 минут. Информацию о системной активности можно получить выполнив команду sar или посмотрев отчёт в папке /var/log/sysstat/sar. Чтобы включить систему учёта, вставьте строку ENABLED="true" в файл
/etc/default/sysstat
Если файла нет, то необходимо установить пакет sysstat командой:

```
# apt-get install sysstat
```

Параметр	Критичность: Средний
Название	**Ограничить доступ к root через su**
Описание	

Эта настройка поможет предотвратить несанкционированный доступ к системе. Для того чтобы разрешить использование su только пользователями, находящимися в группе sudo, необходимо в /etc/pam.d/su добавить строку:

```
auth       required     pam_wheel.so use_uid
```

Затем создать группу sudo, если её не существует:

```
addgroup sudo
```

и добавить в нее необходимых пользовеателей:

```
usermod -a -G sudo username
```

Параметр	Критичность: Средний
Название	**Ограничение входа суперпользователя в виртуальную консоль**
Описание	

Ограничение входа суперпользователя через виртуальную консоль, обеспечивается отсутствием строк в /etc/securetty:

```
vc/1
vc/2
vc/3
vc/4
```

Параметр	Критичность: Низкий
Название	**Ограничение входа суперпользователя через последовательный порт**
Описание	

Ограничение входа суперпользователя через последовательный порт обеспечивается отсутствием строк в /etc/securetty:

```
ttyS0
```

ttyS1

и т.д.

Параметр	Критичность: Средний
Название	**Обеспечение безопасности оболочки при входе под системной учётной записью**
Описание	

Некоторые учётные записи не связаны с конкретными пользователями в системе, и существуют, чтобы выполнять некоторые административные функции. Если злоумышленник сможет зайти под этими учётными записями, то он не должен получить доступ к оболочке.

Информация об ассоциированном командном интерпретаторе по умолчанию хранится в конце каждой строки в /etc/passwd. Системными аккаунтами являются аккаунты, у которых ID меньше 500. Пользовательский ID хранится в третьем поле. Если любая системная учётная запись (отличная от суперпользователя) имеет вход в оболочку, то это должно быть запрещено командой:
usermod -s /usr/sbin/nologin *имя учетной записи*

Параметр	Критичность: Средний
Название	**Проверка, что только у суперпользователя UID 0**
Описание	

Если любая учётная запись, отличная от суперпользователя, имеет UID 0, то данный недочёт должен быть исследован, а аккаунты должны быть удалены или им необходимо присвоить другой UID.

Группа	
Название	**Проверка правильности хранения и существования хэшей паролей**
Описание	

По умолчанию хэши пароля для локальных аккаунтов хранятся во втором поле (colon-separated) в /etc/shadow. Данный файл доступен для чтения только процессам, запущенным с полномочиями суперпользователя. Пользователям запрещается случайный доступ к другим хашам паролей, чтобы избежать попытки взломать их. Тем не менее, остаются шансы на ошибку системы при хранение хэшей паролей в общедоступных файлах, таких как /etc/passwd, или даже хранение открытых паролей в системе. Использование представленных системой инструментов для создания/изменения паролей должно позволить администраторам избежать подобных ошибок.

Параметр	Критичность: Высокий
Название	**Удалить файлы .netrc**
Описание	

Файлы .netrc могут содержать пароли в незашифрованном виде, что может подвергнуть систему нападению.

Параметр	Критичность: Высокий
Название	**Предотвращение входа в аккаунт с пустым паролем**
Описание	

Если учётная запись настроена на аутентификацию по паролю, но пароль не задан, то вход в аккаунт возможен без аутентификации. Необходимо удалить все экземпляры параметра nullok в /etc/pam.d/common-password, чтобы запретить вход по пустым паролям.

Параметр Критичность: Средний

Название **Проверка на скрытость хэшей паролей во всех аккаунтах**

Описание

Если любой хэш пароля хранится в файле `/etc/passwd` (во втором поле, вместо `x`), то причины данной ошибки должны быть рассмотрены. Необходимо сбросить пароль аккаунта и сохранить хэш надлежащим образом, или удалить учётную запись полностью.

Группа

Название **Установка параметров срока действия пароля**

Описание

Файл `/etc/login.defs` контролирует несколько настроек пароля. Такие программы, как `passwd`, `su`, и `login` учитывают `/etc/login.defs`,чтобы определить действия по отношению к устаревшим паролям, его длины и срокам действия предупреждений. Для получения дополнительной информации можно обратиться к странице с документацией `login.defs(5)`.

Пользователи должны изменять свои пароли с целью уменьшения риска их компроментированности. Тем не менее, необходимость частой смены паролей должна быть сбалансирована с риском того, что пользователи могут их использовать или будут записывать, если вынуждены слишком часто его менять. Рекомендуется принудительная смена паролей каждые 90-360 дней, в зависимости от обстоятельств. Необходимо установить соответствующее значение для `PASS_MAX_DAYS` и применить его к существующим аккаунтам с флагом `-M`.

Настройка `PASS_MIN_DAYS` (`-m`) запрещает смену пароля в течении 7 дней после его первого изменения, чтобы избежать его зацикливания. Если вы используете данные настройки, объясните сотрудникам, чтобы они обращались к администратору для смены паролей, только в чрезвычайных случаях, если новый пароль ставится под угрозу. Настройка `PASS_WARN_AGE` (`-W`) даёт пользователю 7 дней предупреждений при в ходе, что срок действия их паролей истекает.

Например, для каждого существующего пользователя *USER*, срок действия параметров может быть исправлен на 180 дней максимального возрата пароля, 7 дней - минимальный срок пароля, и 7 дней - период предупреждений, следующей командой:

```
# chage -M 180 -m 7 -W 7 USER
```

Параметр Критичность: Средний

Название **Установка минимальной длины пароля при входе**

Описание

Для установки норматива длины пароля для новых учётных записей, необходимо отредактировать файл: `/etc/pam.d/common-password`, добавив:

```
min=8
```

Пример:

```
password [success=2 default=ignore]  pam_unix.so obscure sha512 min=8
```

Если используется модуль pam_cracklib, то конфигурация примет вид:

```
password    requisite           pam_cracklib.so minlen=8
```

Параметр Критичность: Средний

Название **Установка минимального срока действия пароля**

Описание

Для того, чтобы задать минимальный срок действия пароля для новых аккаунтов, необходимо отредактировать файл `/etc/login.defs`, добавив или исправив следующие строки: соответственно:

```
PASS_MIN_DAYS 7
```

Значение в 1 день является достаточным для многих сред. Требование DoD 60.

Параметр	Критичность: Средний
Название	**Установка максимального срока действия пароля**
Описание	

Для того, чтобы задать максимальный срок действия пароля для новых аккаунтов, необходимо отредактировать файл `/etc/login.defs`, добавив или исправив следующие строки: соответствующими:
`PASS_MAX_DAYS 90`
Значение в 180 дней является достаточным для многих сред. Требование DoD 60.

Параметр	Критичность: Низкий
Название	**Установка предупреждения о сроке действия пароля**
Описание	

Для того, чтобы отображать пользователям предупреждение о количестве оставшихся дней до истечения срока действия пароля, необходимо отредактировать файл `/etc/login.defs`, добавив или исправив строки:
`PASS_WARN_AGE 7`

Группа	
Название	**Защита аккаунтов с помощью настройки PAM**
Описание	

PAM или Подключаемые Модули Аутентификации - это система, которая реализует модульную аутентификацию для Linux программ. PAM предоставляет гибкую и настраиваемую архитектуру для аутентификации, и должен быть настроен так, чтобы минимизировать воздействие ненужного риска. Данный раздел содержит информацию о том, как это выполнить. PAM реализован в виде набора общих объектов, которые загружаются и вызываются каждый раз, когда приложение аутентифицирует пользователя. Как правило, приложение должно быть запущено с правами суперпользователя потому, что модулям PAM необходимо получать доступ к важным хранилищам информации об аккаунте, такий как /etc/shadow. Традиционные привилегированные приложения или службы, ожидающие подключения по сети (например, SSHD) или SUID программы (например, sudo) уже соответствует этому требованию. Приложение SUID суперпользователя, обеспечивает чтобы программы, которые не являются SUID или привилегированными сами по себе, могли по-прежнему использовать PAM.

PAM использует директорию `/etc/pam.d` для определения информации о настройке конкретного приложения. Например, если программа при входе пытается авторизовать пользователя, то библиотеки PAM следуют указанным инструкциям в файле `/etc/pam.d/login` для определения того, какие меры должны быть предприняты.

Очень важным файлом в `/etc/pam.d` является `/etc/pam.d/common-password`. Этот файл, который входит во многие другие файлы настройки PAM, по умолчанию определяет меры системы аутентификации. Редактирование данного файла - отличный способ сделать общие изменения, например для реализации центральной служы аутентификации.

Группа	
Название	**Установка требований качества пароля**
Описание	

По умолчанию PAM модуль `pam_cracklib` обеспечивает проверку стойкости паролей. Он выполняет ряд проверок, таких как проверка, что пароль не является словарным словом, состоит из определенной длины, не повторяет предыдущий пароль.

Модуль `pam_passwdqc` также обеспечивает возможность соблюдения строгих требований к стойкости пароля.

Страницы с документацией `pam_cracklib(8)` и `pam_passwdqc(8)` предоставляют информацию о возможностях и конфигурации каждого из них.

Группа	
Название	**Установка требований качества пароля, используя pam_cracklib**
Описание	

PAM модуль `pam_cracklib` может быть сконфигурирован для удовлетворения потребностей различных политик.

Например, чтобы настроить `pam_cracklib` требовать по крайней мере один символ верхнего регистра, символ нижнего регистра, цифру и другие (специальные) символы, необходимо найти следующую строку в `/etc/pam.d/common-password`:

```
password requisite pam_cracklib.so try_first_pass retry=3
```

, а затем изменить её следующим образом:

```
password required pam_cracklib.so try_first_pass retry=3 minlen=14 dcredit=-1
ucredit=-1 ocredit=-1 lcredit=0
```

Параметны могут быть модифицированы для обеспечения соблюдения политики безопасности вашей организации. Обсуждение каждого параметра смотрите ниже.

Параметр	Критичность: Низкий
Название	**Убедиться, что не символа '+' в файле /etc/passwd, /etc/shadow, /etc/group**
Описание	

Символ "+" в различных файлах является указателем на вставку в конкретное место данных из NIS карт для системы. Эти символы могут позволить злоумышленникам получить привилегии к доступу в систему, поэтому их нужно удалить, если они существуют.

Параметр	Критичность: Низкий
Название	**Установка минимального количества цифровых символов для устойчивости пароля**
Описание	

Параметр модуля pam_cracklib `dcredit` контролирует требования по использованию цифр в пароле. При установке отрицательного числа, любой пароль должен будет содержать цифры. При установке положительного числа, pam_cracklib будет давать +1 дополнительной длины для каждой цифры. Необходимо установить модуль pam_cracklib и добавить в файл /etc/pam.d/common-password `dcredit=-1` после pam_cracklib.so для обязательного использования цифр в пароле. Пример:

```
password requisite            pam_cracklib.so retry=3 minlen=8 difok=3 dcredit=-1
ucredit=-1 ocredit=-1 lcredit=-1
```

Параметр	Критичность: Низкий
Название	**Установка минимального количества заглавных символов для устойчивости пароля**
Описание	

Параметр модуля pam_cracklib `ucredit=` контролирует требования по использованию заглавных букв в пароле. При установке отрицательного числа, любой пароль должен будет содержать заглавные буквы. При установке положительного числа, pam_cracklib будет давать +1 дополнительной длины для каждого заглавного символа. Необходимо установить модуль pam_cracklib и добавить в файл /etc/pam.d/common-password `ucredit=-1` после pam_cracklib.so для обязательного использования заглавных символов в паролях. Пример:

```
password requisite            pam_cracklib.so retry=3 minlen=8 difok=3 dcredit=-1
ucredit=-1 ocredit=-1 lcredit=-1
```

Параметр	Критичность: Низкий

Название	**Установка минимального количества специальных символов для устойчивости пароля**

Описание

Параметр модуля pam_cracklib `ocredit=` контролирует требования по использованию специальных (или "других") символов в пароле. При установке отрицательного числа, любой пароль должен будет содержать специальные (или "другие") символы. При установке положительного числа, pam_cracklib будет давать +1 дополнительной длины для каждого специального сивола. Необходимо установить модуль pam_cracklib и добавить в файл /etc/pam.d/common-password `ocredit=-1` после pam_cracklib.so для обязательного использования специальных символов в паролях. Пример:

```
password requisite            pam_cracklib.so retry=3 minlen=8 difok=3 dcredit=-1
ucredit=-1 ocredit=-1 lcredit=-1
```

Параметр Критичность: Низкий

Название	**Установка минимального количества строчных символов для устойчивости пароля**

Описание

Параметр модуля pam_cracklib `lcredit=` контролирует требования по использованию строчных символов в пароле. При установке отрицательного числа, любой пароль должен будет содержать прописные символы. При установке положительного числа, pam_cracklib будет давать +1 дополнительной длины для каждого прописного символа. Необходимо установить модуль pam_cracklib и добавить в файл /etc/pam.d/common-password `lcredit=-1` после pam_cracklib.so для обязательного использования прописных символов в паролях. Пример:

```
password requisite            pam_cracklib.so retry=3 minlen=8 difok=3 dcredit=-1
ucredit=-1 ocredit=-1 lcredit=-1
```

Параметр Критичность: Низкий

Название	**Установка минимального количества различающихся символов для устойчивости пароля**

Описание

Параметр модуля pam_cracklib `difok` контролирует требования по использованию различающихся символов во время изменения пароля. Необходимо установить модуль pam_cracklib и добавить в файл /etc/pam.d/common-password `difok=`*3* после pam_cracklib.so для обязательного использования различающихся символов во время изменения пароля. Требование DoD - 4. Пример:

```
password requisite            pam_cracklib.so retry=3 minlen=8 difok=3 dcredit=-1
ucredit=-1 ocredit=-1 lcredit=-1
```

Группа

Название	**Установка блокировки после неудачных попыток ввода пароля**

Описание

PAM модуль `pam_faillock` обеспечивает возможность блокировки учетных записей пользователей после ряда неудачных попыток входа. Документация по данному модулю доступна в `/usr/share/doc/pam-VERSION/txts/README.pam_faillock`.

Параметр Критичность: Средний

Название	**Установка запрета после неудачных попыток ввода пароля**

Описание

Чтобы настроить систему на блокировку учетной записи после 3 неверных попыток входа, необходимо отредактировать файл `/etc/pam.d/common-auth`, добавив следующие строки:

```
auth required pam_tally.so silent deny=3 unlock_time=36000 audit
```

```
account required pam_tally.so
```

Параметр Критичность: Средний

Название **Ограничение повторного использования пароля**

Описание

Не позволяйте пользователям повторно использовать последние пароли. Это может быть достигнуто с помощью параметра `remember` для PAM модуля `pam_unix`. В файле `/etc/pam.d/common-password` необходимо присвоить `remember=5` в строке, ссылающейся на модуль `pam_unix.so`, как показано ниже:

```
password    [success=2 default=ignore]  pam_unix.so existing_options remember=5
```

DoD рекомендует 24 пароля.

Группа

Название **Защита доступа к физической консоли**

Описание

Невозможно полностью защитить систему от злоумышленника с физическим доступом, поэтому защита пространства, в котором находится система, должна рассматриваться как необходимый шаг. Тем не менее, есть несколько шагов, которые, могут сделать это более трудным для атакующего - быстро и незаметно изменить систему этой консоли.

Параметр Критичность: Средний

Название **Требование аутентификации для однопользовательского режима**

Описание

Однопользовательский режим нужен для восстановления системы, обеспечивая единый доступ суперпользователя в систему, предоставляя опции загрузки при запуске. По умолчанию, если выбран однопользовательский режим, аутентификация не выполняется.

Необходимо добавить ввод пароля суперпользователя, даже если система запускается в однопользовательском режиме, дополнив или исправив строку в файле `/etc/init.d/rcS.conf`:

```
exec /sbin/sulogin
```

Группа

Название **Настройка блокировки экрана**

Описание

Когда пользователю необходимо временно оставить компьютер, под которым он работает, экран блокировки должен предотвратить доступ к аккаунту сторонними лицами. Обучение пользователей особенно важно для эффективности блокировки экрана.

Автоматическая блокировка экрана предназначена только в качестве подстраховки для тех случаев, когда пользователь забыл заблокировать экран.

Группа

Название **Настройка сети и брандмауэра**

Описание

Большинство машин должны быть подключены к сети какого-либо рода, и это влечет за собой существенный риск сетевых атак. В этом разделе обсуждаются вопросы безопасности и влияние решений о сетях, которые должны быть сделаны при настройке системы.

В этом разделе также обсуждается брандмауэры, контроль доступа к сети, и другие структуры безопасности сети, которые позволяют на уровне системных правил могут ограничить способность нападавших для подключения к вашей системе. Этими правилами можно указать, какой сетевой трафик должен быть разрешен или запрещен из определенных IP адресов, хостов и сетей. Правилами также можно указать, какие службы системы доступны из сети для определенных хостов или сетей.

Группа

Название **Параметры ядра, которые влияют на сеть**

Описание

Утилита `sysctl` используется для установки параметров, которые затрагивают операции ядра Linux. Параметры ядра, которые влияют на сети и имеют последствия для безопасности, описаны здесь.

Группа

Название **Параметры сети только для хостов**

Описание

Если система не будет использоваться в качестве маршрутизатора, то после настройки некоторых параметров ядра хост не должен выполнять маршрутизацию сетевого трафика.

Параметр Критичность: Средний

Название **Отключение параметра ядра для отправки перенаправлений ICMP по умолчанию**

Описание

Чтобы установить параметр ядра `net.ipv4.conf.default.send_redirects` во время работы, необходимо выполнить следующую команду:

```
# sysctl -w net.ipv4.conf.default.send_redirects=0
```

Если это не системное значение по умолчанию, необходимо добавить следующую строку в `/etc/sysctl.conf`:

```
net.ipv4.conf.default.send_redirects = 0
```

Параметр Критичность: Средний

Название **Отключение параметра ядра для отправки перенаправлений ICMP для всех интерфейсов**

Описание

Чтобы установить параметр ядра `net.ipv4.conf.all.send_redirects` во время работы, необходимо выполнить следующую команду:

```
# sysctl -w net.ipv4.conf.all.send_redirects=0
```

Если это не системное значение по умолчанию, необходимо добавить следующую строку в `/etc/sysctl.conf`:

```
net.ipv4.conf.all.send_redirects = 0
```

Параметр Критичность: Средний

Название **Отключение параметра ядра для IP Forwarding**

Описание

Чтобы установить параметр ядра `net.ipv4.ip_forward` во время работы, необходимо выполнить следующую команду:

```
# sysctl -w net.ipv4.ip_forward=0
```

Если это не системное значение по умолчанию, необходимо добавить следующую строку в `/etc/sysctl.conf`:

```
net.ipv4.ip_forward = 0
```

Группа

Название **Параметры ядра, влияющие на сеть для хостов и маршрутизаторов**

Описание

Некоторые параметры ядра должны быть установлены для систем, которые действуют либо как хосты, либо как маршрутизаторы, для улучшения способности системы защиты против определенных типов атак на протокол IPv4.

Параметр Критичность: Средний

Название **Отключение параметра ядра для приема ICMP перенаправлений для всех интерфейсов**

Описание

Чтобы установить параметр ядра `net.ipv4.conf.all.accept_redirects` во время работы, необходимо выполнить следующую команду:

```
# sysctl -w net.ipv4.conf.all.accept_redirects=0
```

Если это не системное значение по умолчанию, необходимо добавить следующую строку в `/etc/sysctl.conf`:

```
net.ipv4.conf.all.accept_redirects = 0
```

Параметр Критичность: Средний

Название **Отключение параметра ядра для принятия безопасных перенаправлений для всех интерфейсов**

Описание

Чтобы установить параметр ядра `net.ipv4.conf.all.secure_redirects` во время работы, необходимо выполнить следующую команду:

```
# sysctl -w net.ipv4.conf.all.secure_redirects=0
```

Если это не системное значение по умолчанию, необходимо добавить следующую строку в `/etc/sysctl.conf`:

```
net.ipv4.conf.all.secure_redirects = 0
```

Параметр Критичность: Низкий

Название **Включение параметра ядра для журналирования Martian Packets**

Описание

Чтобы установить параметр ядра `net.ipv4.conf.all.log_martians` во время работы, необходимо выполнить следующую команду:

```
# sysctl -w net.ipv4.conf.all.log_martians=1
```

Если это не системное значение по умолчанию, необходимо добавить следующую строку в `/etc/sysctl.conf`:

```
net.ipv4.conf.all.log_martians = 1
```

Параметр Критичность: Низкий

Название **Настройка параметра ядра для задания максимального числа осиротевших сокетов**

Описание

Чтобы установить параметр ядра `net.ipv4.tcp_max_orphans` во время работы, необходимо выполнить следующую команду:

```
# sysctl -w net.ipv4.tcp_max_orphans=256
```

Если это не системное значение по умолчанию, необходимо добавить следующую строку в `/etc/sysctl.conf`:

```
net.ipv4.tcp_max_orphans = 256
```

Параметр	Критичность: Средний
Название	**Отключение параметра ядра для принятия Source-Routed пакетов по умолчанию**
Описание	

Чтобы установить параметр ядра `net.ipv4.conf.default.accept_source_route` во время работы, необходимо выполнить следующую команду:

```
# sysctl -w net.ipv4.conf.default.accept_source_route=0
```

Если это не системное значение по умолчанию, необходимо добавить следующую строку в `/etc/sysctl.conf`:

```
net.ipv4.conf.default.accept_source_route = 0
```

Параметр	Критичность: Низкий
Название	**Отключение параметра ядра для приема ICMP перенаправлений по умолчанию**
Описание	

Чтобы установить параметр ядра `net.ipv4.conf.default.accept_redirects` во время работы, необходимо выполнить следующую команду:

```
# sysctl -w net.ipv4.conf.default.accept_redirects=0
```

Если это не системное значение по умолчанию, необходимо добавить следующую строку в `/etc/sysctl.conf`:

```
net.ipv4.conf.default.accept_redirects = 0
```

Параметр	Критичность: Средний
Название	**Отключение параметра ядра для приема защищенных перенаправлений по умолчанию**
Описание	

Чтобы установить параметр ядра `net.ipv4.conf.default.secure_redirects` во время работы, необходимо выполнить следующую команду:

```
# sysctl -w net.ipv4.conf.default.secure_redirects=0
```

Если это не системное значение по умолчанию, необходимо добавить следующую строку в `/etc/sysctl.conf`:

```
net.ipv4.conf.default.secure_redirects = 0
```

Параметр	Критичность: Низкий
Название	**Включение параметра ядра для игнорирования ICMP Broadcast Echo запросов**
Описание	

Чтобы установить параметр ядра `net.ipv4.icmp_echo_ignore_broadcasts` во время работы, необходимо выполнить следующую команду:

```
# sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=1
```

Если это не системное значение по умолчанию, необходимо добавить следующую строку в `/etc/sysctl.conf`:

```
net.ipv4.icmp_echo_ignore_broadcasts = 1
```

Параметр	Критичность: Средний
Название	**Включение параметра ядра для использования TCP Syncookies**
Описание	

Чтобы установить параметр ядра `net.ipv4.tcp_syncookies` во время работы, необходимо выполнить следующую команду:

```
# sysctl -w net.ipv4.tcp_syncookies=1
```

Если это не системное значение по умолчанию, необходимо добавить следующую строку в `/etc/sysctl.conf`:

```
net.ipv4.tcp_syncookies = 1
```

Параметр Критичность: Средний

Название **Включение параметра ядра для использования фильтрации обратного пути у всех интерфейсов**

Описание

Чтобы установить параметр ядра `net.ipv4.conf.all.rp_filter` во время работы, необходимо выполнить следующую команду:

```
# sysctl -w net.ipv4.conf.all.rp_filter=1
```

Если это не системное значение по умолчанию, необходимо добавить следующую строку в `/etc/sysctl.conf`:

```
net.ipv4.conf.all.rp_filter = 1
```

Параметр Критичность: Средний

Название **Включение параметра ядра для использования фильтрации обратного пути по умолчанию**

Описание

Чтобы установить параметр ядра `net.ipv4.conf.default.rp_filter` во время работы, необходимо выполнить следующую команду:

```
# sysctl -w net.ipv4.conf.default.rp_filter=1
```

Если это не системное значение по умолчанию, необходимо добавить следующую строку в `/etc/sysctl.conf`:

```
net.ipv4.conf.default.rp_filter = 1
```

Группа

Название **Беспроводные сети**

Описание

Беспроводные сети, такие как 802.11 (WiFi) и Bluetooth, могут представлять риск для безопасности чувствительных или секретных систем и сетей. Беспроводное сетевое оборудование с гораздо большей вероятностью входит в состав ноутбука или переносных систем, чем в настольные компьютеры или серверы.

Удаление аппаратуры обеспечивает наибольшую гарантию того, что беспроводные возможности будут отключены. Политики часто включают в себя положения для запрета приобретения оборудования, включающего в себя беспроводные возможности, которые будут использоваться в чувствительных местах. Если нет возможности убрать беспроводное оборудование, то политика допускает использовать данное устройство только после отключения беспроводных возможностей с помощью программного обеспечения.

Группа

Название **Отключение беспроводной сети посредством конфигурации ПО**

Описание

Если невозможно удалить беспроводное оборудование из рассматриваемого устройства, отключите его в программном обеспечении. Следующие методы могут отключить программное обеспечение для беспроводных сетей, но учтите, что эти методы не препятствуют вредоносным программам или повторной активации устройства небрежными пользователями.

Группа

Название **IPv6**

Описание

В систему включена поддержка Internet Protocol версии 6. Основным и часто упоминаемым улучшением по сравнению с IPv4 является его огромный рост количества доступных адресов. Другой важной особенностью является поддержка автоматической настройки многих параметров сети.

Группа	
Название	**Отключение поддержки IPv6 только при необходимости**
Описание	

Несмотря на конфигурацию, которая предлагает, что поддержка IPv6 была отключена, автонастройка локального IPv6-адреса происходит даже тогда, когда назначается только IPv4-адрес. Единственный способ эффективно предотвращать запуск IPv6 сетевого стека, указать системе, чтобы не активировать IPv6 модуль ядра.

Группа	
Название	**Настройка IPv6, если необходимо**
Описание	

Главной особенностью IPv6 является возможность автоматической настройки сетевых устройств, используя информацию от DHCP сервера. С точки зрения безопасности, ручная настройка важных сведений о конфигурации предпочтительнее, чем принимать их от сети.

Группа	
Название	**Отключение автоматической конфигурации**
Описание	

Отключить принятие системой изменений маршрутизатора и перенаправления можно, добавив или исправив следующую строку в `/etc/sysconfig/network` (отметим, что это не отключит отправку данных маршрутизатором):
`IPV6_AUTOCONF=no`

Группа	
Название	**IPTables и Ip6tables**
Описание	

Брандмауэр называется Netfilter, включен как часть ядра Linux и распространяется вместе с системой. Он включен по умолчанию. Этот брандмауэр контролируется программой iptables, и все возможности часто называют этим именем. Аналогичная программа для фильтрации IPv6 назвается ip6tables.

В отличие от TCP Wrappers, поддержка и соблюдение правил которого зависит от сетевых серверных приложений, в Netfilter фильтрация происходит на уровне ядра. Перед программой можно даже обрабатывать данные из сетевых пакетов. Таким образом, любая программа в системе зависит от написанных правил.

В этом разделе приводится основная информация об улучшении конфигураций iptables и ip6tables. Для получения более полной информации, которая может позволить построить сложные правила с учетом вашей среды, пожалуйста, обратитесь к ссылкам в конце этого раздела.

Группа	
Название	**Просмотр и активация правил по умолчанию**
Описание	

Просмотреть на данный момент правила iptables можно, выполнив команду:
```
# iptables -nL --line-numbers
```
Команда для ip6tables аналогична.

Если правила брандмауэра не отображаются (то есть, нет правил), необходимо включить его и убедиться, что он запускается при начальной загрузке, выполнив следующие команды (аналогично для ip6tables):
```
# service iptables restart
```

Правила iptables по умолчанию:

```
Chain INPUT (policy ACCEPT)
num  target     prot opt source       destination
1    ACCEPT     all  --  0.0.0.0/0    0.0.0.0/0    state RELATED,ESTABLISHED
2    ACCEPT     icmp --  0.0.0.0/0    0.0.0.0/0
3    ACCEPT     all  --  0.0.0.0/0    0.0.0.0/0
4    ACCEPT     tcp  --  0.0.0.0/0    0.0.0.0/0    state NEW tcp dpt:22
5    REJECT     all  --  0.0.0.0/0    0.0.0.0/0    reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT)
num  target     prot opt source       destination
1    REJECT     all  --  0.0.0.0/0    0.0.0.0/0    reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source       destination
```

Для `ip6tables` правила по умолчанию, по сути, те же самые.

Группа

Название **Усиление набора правил по умолчанию**

Описание

Правила по умолчанию могут быть усилены. Системные скрипты, которые активируют правила брандмауэра, ожидают, что они будут определены в файлах конфигурации iptables и ip6tables в каталоге `/etc/sysconfig`. Многие из строк в этих файлах похожи на аргументы командной строки, которые будут представлены в программах `/sbin/iptables` или `/sbin/ip6tables` - но некоторые из них совсем другие.

Следующие рекомендации описывают, как усилить набор правил по умолчанию в конфигурационном файле.

Изменения могут быть сделаны прямо в `/etc/sysconfig/iptables` и `/etc/sysconfig/ip6tables`. Инструкция распространяется на оба файла, если не указано иное. Конфигурация для ip6tables будет либо аналогичная либо явно указана.

Группа

Название **Редкие сетевые протоколы**

Описание

Система включает в себя поддержку нескольких сетевых протоколов, которые обычно не используются. Хотя уязвимости в коде ядра сети не часто обнаруживаются, последствия могут быть драматичными. Отключение поддержки редких сетевых протоколов снижает риск атак системы, направленных на ее реализацию этих протоколов.

Группа

Название **Настройка Syslog**

Описание

Служба syslog является механизмом журналирования по умолчанию в Unix в течение многих лет. Она имеет ряд недостатков, в том числе несовместимый формата журнала, отсутствие аутентификации для полученных сообщений, а также отсутствие шифрования и надежного транспорта сообщений, отправляемых по сети. Однако, из-за своей долгой истории, журнал является де-факто стандартом, который поддерживают практически все Unix приложения.

В этом разделе описывается как настроить rsyslog для лучшего эффекта, и как использовать инструменты, предоставляемые системой для поддержания и мониторинга журналов.

Группа

Название	Проверка, что все журналы ротируются logrotate

Описание

Необходимо отредактировать файл `/etc/logrotate.d/syslog`. Найдите первую строку, которая должна выглядеть следующим образом:

```
/var/log/messages /var/log/secure /var/log/maillog /var/log/spooler \
  /var/log/boot.log /var/log/cron {
```

Необходимо изменить эту строку так, чтобы она содержала один пробел между списком каждого файла журнала, указанных в `/etc/rsyslog.conf`.

Все журналы, использующиеся в системе, должны регулярно ротироваться иначе лог-файлы будут потреблять дисковое пространство с течением времени, что в конечном итоге мешает работе системы. Файл `/etc/logrotate.d/syslog` - это конфигурационный файл, используемый утилитой `logrotate` , которая сохраняет все файлы журнала, указанные `/etc/logrotate.conf`. Настройки по умолчанию являются достаточными для целей данного руководства.

Обратите внимание, что `logrotate` запускается каждую ночь `/etc/cron.daily/logrotate`. При особой активности журналы должны ротироваться чаще, чем один раз в день, используя другие механизмы.

Параметр	Критичность: Низкий
Название	**Проверка, что Logrotate периодически запускается**

Описание

Служба `logrotate` должна быть запущена.

Группа	
Название	**Система учета с журналированием (auditd)**

Описание

Служба аудита обеспечивает существенные возможности для записи деятельности системы. По умолчанию, служба аудита об отказах SELinux AVC и некоторых типов событий, связанных с безопасностью, таких как вход в систему, изменение аккаунта, и проверки подлинности выполняется программами, такие как sudo. В конфигурации по умолчанию, `auditd` имеет скромные требования к дисковому пространству, и не должен заметно повлиять на производительность системы.

Сетевое окружение часто имеет существенные требования журналирования и `auditd` может быть настроен для удовлетворения этих требований. Изучение некоторых примеров записей аудита показывает, как Linux система аудита удовлетворяет общим требованиям. Следующий пример из документации Fedora доступен на `http://docs.fedoraproject.org/en-US/Fedora/13/html/Security-Enhanced_Linux/sect-Security-Enhanced_Linux-Fixing_Problems-Raw_Audit_Messages.html` показывает значительный объем информации, захваченных в двух типичных "сырых" сообщений аудита, а затем разбивка самых важных областей. В этом примере сообщение SELinux связан и сообщает об отказе AVC (и связан с системными вызовами), что произошло, когда Apache HTTP сервер пытался получить доступ к `/var/www/html/file1` файлу (помеченный `samba_share_t` типом):

```
type=AVC msg=audit(1226874073.147:96): avc:  denied  { getattr } for pid=2465
comm="httpd"
path="/var/www/html/file1" dev=dm-0 ino=284133
scontext=unconfined_u:system_r:httpd_t:s0
tcontext=unconfined_u:object_r:samba_share_t:s0 tclass=file

type=SYSCALL msg=audit(1226874073.147:96): arch=40000003 syscall=196 success=no exit=-
13
a0=b98df198 a1=bfec85dc a2=54dff4 a3=2008171 items=0 ppid=2463 pid=2465 auid=502
uid=48
gid=48 euid=48 suid=48 fsuid=48 egid=48 sgid=48 fsgid=48 tty=(none) ses=6 comm="httpd"
exe="/usr/sbin/httpd" subj=unconfined_u:system_r:httpd_t:s0 key=(null)
```

- `msg=audit(1226874073.147:96)`

    - Число в скобках является неформатированным штампом времени для события, которое может быть преобразовано в стандартное время, используя `date` команду.
- `{ getattr }`
    - Пункт в скобках указывает, что доступ был запрещен. `getattr` указывает на исходный процесс и пытается прочитать информацию о состоянии целевого файла. Это происходит перед чтением файлов. Это действие запрещено для связи с файлом, имеющем неправильную метку. Часто наблюдаются следующие разрешения `getattr`, `read`, и `write`.
- `comm="httpd"`
    - Исполняемый файл, который запустил процесс. Полный выполняемый путь находится в `exe=` секции системного вызова (`SYSCALL`) сообщение в этом случае: `exe="/usr/sbin/httpd"`.
- `path="/var/www/html/file1"`
    - Путь к объекту (цели) процесса, пытающегося получить доступ.
- `scontext="unconfined_u:system_r:httpd_t:s0"`
    - SELinux контекст процесса, который пытался отрицать действие. В этом случае, это SELinux контекст HTTP-сервера Apache, который работает в `httpd_t` домене.
- `tcontext="unconfined_u:object_r:samba_share_t:s0"`
    - SELinux контекст объекта (цели) процесса, пытающегося получить доступ. В этом случае, это контекст SELinux `file1`. Примечание: `samba_share_t` тип не доступен для процессов, запущенных в `httpd_t` домене.
- Из сообщения системных вызовов (`SYSCALL`) два элемента представляют интерес:
    - `success=no`: указывает, является ли отказ (AVC) приведенным в исполнение или нет.`success=no` указывает, что системный вызов был не успешным (SELinux отказано в доступе). `success=yes` указывает, что системный вызов был успешным - так можно увидеть разрешенные домены или неограниченные домены, таких как `initrc_t` и `kernel_t`.
    - `exe="/usr/sbin/httpd"`: полный путь к исполняемому файлу, который запустил процесс, в данном случае `exe="/usr/sbin/httpd"`.

Параметр	Критичность: Средний
Название	**Включение аудита процессов, которые запускаются раньше, чем служба аудита**
Описание	

Чтобы убедиться, что все процессы могут быть проверены, даже те, которые запускаются раньше, чем служба аудита, необходимо добавить аргумент `audit=1` в строку ядра в `/etc/default/grub`, например так:
`GRUB_CMDLINE_LINUX_DEFAULT="quiet audit=1"`
Затем выполните команду
`# update-grub`

Группа	
Название	**Настройка хранения данных auditd**
Описание	

Система аудита записывает данные в `/var/log/audit/audit.log`. По умолчанию служба `auditd` производит ротацию лог-файлов по размеру (6MB), сохраняя максимум 30 МБ данных в общем, и отказывается писать записи, когда диск переполнен. Это сводит к минимуму риск заполнения данными аудита ее разделов и влияния на другие службы. Это также сводит к минимуму риск временно отключить службу системы аудита, если она не может записать журнал аудита (который должен быть настроен на это). Для нагруженной системы или системы, которая тщательно журналирует деятельность, настройки по умолчанию для хранения данных может быть недостаточно. Размер файла журнала будет сильно зависеть от того, какие типы событий журналируются. Для начала необходимо настроить аудит для регистрации всех событий, представляющих интерес. После, контролируя размер журнала вручную некоторое время, необходимо определить, какой размер файла позволит вам сохранить необходимые данные для правильного периода времени.

Использование отдельного раздела для `/var/log/audit` предотвращает журналам службы `auditd` нарушать функциональность системы если они заполнятся, и, что более важно, избегает излишнюю активность в `/var` от заполнения раздела и остановки аудита. (Журналы аудита являются ограниченными по размеру, и поэтому вряд ли будут расти неограниченно, если не настроены так) Служба `auditd` может быть сконфигурирована на остановку машину, если ей не хватает места. **Примечание:** Поскольку более старые журналы удаляются, необходимо настроить `auditd` таким образом, чтобы они не мешали ротироваться старым журналам, прежде чем они могут быть просмотрены. *Если ваша*

система настроена на остановку, когда ведение журнала не может быть выполнено, убедитесь, что это не может произойти в нормальных условиях! Проверьте, что `/var/log/audit` нахадится в отдельном разделе, и этот раздел больше, чем максимальный объем данных `auditd` который будет сохраняться в нормальном режиме.

Параметр Критичность: Средний

Название **Настройка auditd количества нераспределенных журналов**

Описание

Определите, сколько лог-файлов `auditd` следует сохранить, когда происходит ротация лог-файлов. Необходимо отредактировать файл `/etc/audit/auditd.conf`, добавив или изменив следующую строку, подставляя вместо *NUMLOGS* корректное значение:

```
num_logs = NUMLOGS
```

Установите значение 5 для общедоступных систем. Обратите внимание, что при значении менее 2 ротация не происходит.

Параметр Критичность: Средний

Название **Настройка auditd максимального размера файла журнала**

Описание

Определение количество данных аудита (в мегабайтах), которые должны быть сохранены в каждом файле журнала. Необходимо отредактировать файл `/etc/audit/auditd.conf`, добавив или изменив следующую строку, подставляя верное значение для *STOREMB*:

```
max_log_file = STOREMB
```

Установите значение в `6` (MB) или выше для общедоступных систем. Большие значения, конечно, поддерживают сохранение еще больших данных аудита.

Параметр Критичность: Средний

Название **Настройка auditd действия при достижении максимального размера журнала**

Описание

По умолчанию действие при достижении максимального размера журналов, происходит ротация лог-файлов, отказываясь от старых. Необходимо отредактировать файл `/etc/audit/auditd.conf`, добавив или изменив следующую строку, подставляя соответствующий *ACTION*:

```
max_log_file_action = ACTION
```

Возможные значения для *ACTION* описаны в `auditd.conf` странице с документацией. Они включают:

- `ignore`
- `syslog`
- `suspend`
- `rotate`
- `keep_logs`

Установите значение *`ACTION`* в `rotate` чтобы убедиться, что происходит ротация лог-файлов. Это значение по умолчанию. Данная настройка не чувствительна к регистру.

Параметр Критичность: Средний

Название **Настройка действия admin_space_left при недостаточном месте на диске**

Описание

Служба `auditd` может быть настроена на принятие действия, когда дисковое пространство заканчивается, но ещё не заполнилось полностью. Необходимо отредактировать файл `/etc/audit/auditd.conf`, добавить или изменить следующую строку, подставляя *ACTION* соответственно:

```
admin_space_left_action = ACTION
```

Возможные значения для *ACTION* описаны в `auditd.conf` странице с документацией. Они включают:

- ignore
- syslog
- email
- exec
- suspend
- single
- halt

Установите значение в single чтобы перевести систему в однопользовательский режим для корректирующих действий. Для некоторых систем, необходимость возможности перевешивает необходимость записи всех действий, и различные параметры должны быть определены.

Параметр Критичность: Средний

Название	**Настройка auditd для использования плагина audispd**
Описание	

Для настройки службы auditd для использования плагина audispd, необходимо установить active строку /etc/audisp/plugins.d/syslog.conf в значение yes. Перезапуск службы auditd выполняется командой:

```
# service auditd restart
```

Группа

Название	**Настройка комплекса правил auditd**
Описание	

Служба auditd может выполнять комплексный мониторинг активности системы. В этом разделе описываются рекомендуемые параметры конфигурации комплексного аудита, но полное описание возможностей аудита системы выходит за рамки данного руководства. Существует почтовая рассылка *linux-audit@redhat.com* , чтобы содействовать общественному обсуждению системы аудита.

Подсистема аудита поддерживает обширную коллекцию событий, в том числе:

- Трассировка произвольных системных вызовов (определяются по имени или номеру) на вход или выход.
- Фильтрация по PID, UID, системным вызовам аргументов (с некоторыми ограничениями), и т.д.
- Мониторинг конкретных файлов для изменения содержимого файлов или метаданных.

Правила аудита при запуске контролируются файлом /etc/audit/audit.rules. Добавление правил для удовлетворения требований аудита Вашей организации. Каждая строка в /etc/audit/audit.rules представляет собой ряд аргументов, которые могут быть переданы в auditctl и могут быть индивидуально протестированы во время выполнения. Более подробная информация доступна в /usr/share/doc/audit-*VERSION* и на соответствующих страницах с документацией.

При копировании любых наборов правил из примера аудита из /usr/share/doc/audit-VERSION, не забудьте закомментировать строки, содержащие arch=, которые не подходят для архитектуры вашей системы. Затем необходимо просмотреть и понять следующие правила, которые особенно необходимы для соответствующей архитектуры.

После рассмотрения всех правил, читая следующие разделы и редактируя при необходимости, новые правила могут быть активированы командой:

```
# service auditd restart
```

Группа

Название	**Запись событий, изменяющих информацию о дате и времени**
Описание	

Произвольное изменение системного времени может быть использовано для сокрытия нечестной деятельности в лог-файлы, а также, чтобы запутать сетевые службы, которые сильно зависят от точного системного времени. Все изменения системного времени должны быть проверены.

Параметр Критичность: Низкий

Название **Запись событий, изменяющих время через adjtimex**

Описание

На 32-битной системе необходимо добавить в `/etc/audit/audit.rules`:

```
# audit_time_rules
-a always,exit -F arch=b32 -S adjtimex -k audit_time_rules
```

На 64-битной системе необходимо также добавить в `/etc/audit/audit.rules`:

```
# audit_time_rules
-a always,exit -F arch=b64 -S adjtimex -k audit_time_rules
```

Параметр -k позволяет получать спецификацию ключа в виде строки, которая может быть использована для улучшения отчетности через ausearch и aureport и всегда должен быть использован. Некоторые системные вызовы могут быть определены в той же строке, чтобы сэкономить место, это желательно, но не обязательно. См. пример нескольких комбинированных системных вызовов:

```
-a always,exit -F arch=b64 -S adjtimex -S settimeofday -S clock_settime
-k audit_time_rules
```

Параметр Критичность: Низкий

Название **Запись событий, изменяющих время через settimeofday**

Описание

На 32-битной системе необходимо добавить в `/etc/audit/audit.rules`:

```
# audit_time_rules
-a always,exit -F arch=b32 -S settimeofday -k audit_time_rules
```

На 64-битной системе необходимо также добавить в `/etc/audit/audit.rules`:

```
# audit_time_rules
-a always,exit -F arch=b64 -S settimeofday -k audit_time_rules
```

Параметр -k позволяет получать спецификацию ключа в виде строки, которая может быть использована для улучшения отчетности через ausearch и aureport и всегда должен быть использован. Некоторые системные вызовы могут быть определены в той же строке, чтобы сэкономить место, это желательно, но не обязательно. См. пример нескольких комбинированных системных вызовов:

```
-a always,exit -F arch=b64 -S adjtimex -S settimeofday -S clock_settime
-k audit_time_rules
```

Параметр Критичность: Низкий

Название **Запись событий, изменяющих время через stime**

Описание

На 32-битной системе необходимо добавить в `/etc/audit/audit.rules`:

```
# audit_time_rules
-a always,exit -F arch=b32 -S stime -k audit_time_rules
```

На 64-битной системе параметр "-S time" не используется. Параметр -k позволяет получать спецификацию ключа в виде строки, которая может быть использована для улучшения отчетности через ausearch и aureport и всегда должен быть использован. Некоторые системные вызовы могут быть определены в той же строке, чтобы сэкономить место, это желательно, но не обязательно. См. пример нескольких комбинированных системных вызовов:

```
-a always,exit -F arch=b64 -S adjtimex -S settimeofday -S clock_settime
-k audit_time_rules
```

Параметр Критичность: Низкий

Название **Запись событий, изменяющих время через clock_settime**

Описание

На 32-битной системе необходимо добавить в `/etc/audit/audit.rules`:

```
# audit_time_rules
-a always,exit -F arch=b32 -S clock_settime -k audit_time_rules
```
На 64-битной системе необходимо также добавить в `/etc/audit/audit.rules`:
```
# audit_time_rules
-a always,exit -F arch=b64 -S clock_settime -k audit_time_rules
```
Параметр -k позволяет получать спецификацию ключа в виде строки, которая может быть использована для улучшения отчетности через ausearch и aureport и всегда должен быть использован. Некоторые системные вызовы могут быть определены в той же строке, чтобы сэкономить место, это желательно, но не обязательно. См. пример нескольких комбинированных системных вызовов:
```
-a always,exit -F arch=b64 -S adjtimex -S settimeofday -S clock_settime
-k audit_time_rules
```

	Параметр	Критичность: Низкий
	Название	**Запись событий, изменяющих время файла**
	Описание	

Необходимо добавить в `/etc/audit/audit.rules`:
```
-w /etc/localtime -p wa -k audit_time_rules
```
Параметр -k позволяет получать спецификацию ключа в виде строки, которая может быть использована для улучшения отчетности через ausearch и aureport и всегда должен быть использован.

	Параметр	Критичность: Низкий
	Название	**Запись событий, которые изменяют информацию о пользователях/группах**
	Описание	

Необходимо добавить следующее в `/etc/audit/audit.rules` для того, чтобы фиксировать события, которые вносят изменения в пользователей:
```
# audit_account_changes
-w /etc/group -p wa -k audit_account_changes
-w /etc/passwd -p wa -k audit_account_changes
-w /etc/gshadow -p wa -k audit_account_changes
-w /etc/shadow -p wa -k audit_account_changes
-w /etc/security/opasswd -p wa -k audit_account_changes
```

	Параметр	Критичность: Низкий
	Название	**Запись событий, которые изменяют системное сетевое окружение**
	Описание	

Необходимо добавить следующее в `/etc/audit/audit.rules`, настраивая архитектуру либо b32 или b64, необходимую для вашей системы:
```
# audit_network_modifications
-a exit,always -F arch=ARCH -S sethostname -S setdomainname -k
audit_network_modifications
-w /etc/issue -p wa -k audit_network_modifications
-w /etc/issue.net -p wa -k audit_network_modifications
-w /etc/hosts -p wa -k audit_network_modifications
-w /etc/sysconfig/network -p wa -k audit_network_modifications
```

	Параметр	Критичность: Низкий
	Название	**Журналы аудита системы должны иметь права 0640 или менее разрешающие**
	Описание	

Изменить права файла журналов аудита можно командой:
```
# chmod 0640 audit_file
```

Параметр Критичность: Низкий

Название **Журналы аудита системы должны принадлежать суперпользователю**

Описание

Чтобы правильно установить владельца `/var/log`, необходимо выполнить команду:
```
# chown root /var/log
```

Параметр Критичность: Низкий

Название **Запись событий, которые изменяют системы обязательного контроля доступа**

Описание

Необходимо добавить в `/etc/audit/audit.rules`:
```
-w /etc/selinux/ -p wa -k MAC-policy
```

Группа

Название **Запись событий, которые изменяют системные права доступа**

Описание

Как минимум, система аудита должна записывать изменения прав доступа к файлам для всех пользователей, включая суперпользователя. Отметим, что "-F arch=b32" строка должна присутствовать даже на 64-битной системе. Эти команды идентифицируют системные вызовы для аудита. Даже если система 64-битная она все равно может выполнять некоторые 32 системные вызовы. Кроме того, эти правила могут быть сконфигурированы различными способами для достижения желаемого эффекта. Примером этого является то, что "-S" вызовы могут быть разделены и размещены на отдельных линиях, однако, это менее эффективно. Необходимо добавить следующее в `/etc/audit/audit.rules`:
```
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat \
    -F auid>=500 -F auid!=4294967295 -k perm_mod
    -a always,exit -F arch=b32 -S chown -S fchown -S fchownat \
    -S lchown -F auid>=500 -F auid!=4294967295 -k perm_mod
    -a always,exit -F arch=b32 -S setxattr -S lsetxattr \
    -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr \
    -F auid>=500 -F auid!=4294967295 -k perm_mod
```
Если система 64-разрядная, то эти строки должны быть продублированы и arch=b32 заменить на arch=b67 следующим:
```
-a always,exit -F arch=b64 -S chmod -S fchmod -S fchmodat \
    -F auid>=500 -F auid!=4294967295 -k perm_mod
    -a always,exit -F arch=b64 -S chown -S fchown -S fchownat \
    -S lchown -F auid>=500 -F auid!=4294967295 -k perm_mod
    -a always,exit -F arch=b64 -S setxattr -S lsetxattr \
    -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr \
    -F auid>=500 -F auid!=4294967295 -k perm_mod
```

Параметр Критичность: Низкий

Название **Запись событий, которые изменяют системные права доступа - chmod**

Описание

Как минимум, система аудита должна записывать изменения прав доступа к файлам для всех пользователей, включая суперпользователя. Необходимо добавить следующее `/etc/audit/audit.rules`:
```
-a always,exit -F arch=b32 -S chmod -F auid>=500 -F auid!=4294967295 \
    -k perm_mod
```
If the system is 64 bit then also add the following:

```
-a always,exit -F arch=b64 -S chmod  -F auid>=500 -F auid!=4294967295 \
    -k perm_mod
```

Параметр	Критичность: Низкий
Название	**Запись событий, которые изменяют системные права доступа - chown**
Описание	

Как минимум, система аудита должна записывать изменения прав доступа к файлам для всех пользователей, включая суперпользователя. Необходимо добавить следующее `/etc/audit/audit.rules`:

```
-a always,exit -F arch=b32 -S chown -F auid>=500 -F auid!=4294967295 \
    -k perm_mod
```

If the system is 64 bit then also add the following:

```
-a always,exit -F arch=b64 -S chown -F auid>=500 -F auid!=4294967295 \
    -k perm_mod
```

Параметр	Критичность: Низкий
Название	**Запись событий, которые изменяют системные права доступа - fchmod**
Описание	

Как минимум, система аудита должна записывать изменения прав доступа к файлам для всех пользователей, включая суперпользователя. Необходимо добавить следующее `/etc/audit/audit.rules`:

```
-a always,exit -F arch=b32 -S fchmod -F auid>=500 -F auid!=4294967295 \
    -k perm_mod
```

If the system is 64 bit then also add the following:

```
-a always,exit -F arch=b64 -S fchmod -F auid>=500 -F auid!=4294967295 \
    -k perm_mod
```

Параметр	Критичность: Низкий
Название	**Запись событий, которые изменяют системные права доступа - fchmodat**
Описание	

Как минимум, система аудита должна записывать изменения прав доступа к файлам для всех пользователей, включая суперпользователя. Необходимо добавить следующее `/etc/audit/audit.rules`:

```
-a always,exit -F arch=b32 -S fchmodat -F auid>=500 -F auid!=4294967295 \
    -k perm_mod
```

If the system is 64 bit then also add the following:

```
-a always,exit -F arch=b64 -S fchmodat -F auid>=500 -F auid!=4294967295 \
    -k perm_mod
```

Параметр	Критичность: Низкий
Название	**Запись событий, которые изменяют системные права доступа - fchown**
Описание	

Как минимум, система аудита должна записывать изменения прав доступа к файлам для всех пользователей, включая суперпользователя. Необходимо добавить следующее `/etc/audit/audit.rules`:

```
-a always,exit -F arch=b32 -S fchown -F auid>=500 -F auid!=4294967295 \
    -k perm_mod
```

If the system is 64 bit then also add the following:

```
-a always,exit -F arch=b64 -S fchown -F auid>=500 -F auid!=4294967295 \
    -k perm_mod
```

Параметр Критичность: Низкий

Название **Запись событий, которые изменяют системные права доступа - fchownat**

Описание

Как минимум, система аудита должна записывать изменения прав доступа к файлам для всех пользователей, включая суперпользователя. Необходимо добавить следующее `/etc/audit/audit.rules`:

```
-a always,exit -F arch=b32 -S fchownat -F auid>=500 -F auid!=4294967295 \
    -k perm_mod
```

If the system is 64 bit then also add the following:

```
-a always,exit -F arch=b64 -S fchownat -F auid>=500 -F auid!=4294967295 \
    -k perm_mod
```

Параметр Критичность: Низкий

Название **Запись событий, которые изменяют системные права доступа - fremovexattr**

Описание

Как минимум, система аудита должна записывать изменения прав доступа к файлам для всех пользователей, включая суперпользователя. Необходимо добавить следующее `/etc/audit/audit.rules`:

```
-a always,exit -F arch=b32 -S fremovexattr -F auid>=500 -F auid!=4294967295 \
    -k perm_mod
```

If the system is 64 bit then also add the following:

```
-a always,exit -F arch=b64 -S fremovexattr -F auid>=500 -F auid!=4294967295 \
    -k perm_mod
```

Параметр Критичность: Низкий

Название **Запись событий, которые изменяют системные права доступа - fsetxattr**

Описание

Как минимум, система аудита должна записывать изменения прав доступа к файлам для всех пользователей, включая суперпользователя. Необходимо добавить следующее `/etc/audit/audit.rules`:

```
-a always,exit -F arch=b32 -S fsetxattr -F auid>=500 -F auid!=4294967295 \
    -k perm_mod
```

If the system is 64 bit then also add the following:

```
-a always,exit -F arch=b64 -S fsetxattr -F auid>=500 -F auid!=4294967295 \
    -k perm_mod
```

Параметр Критичность: Низкий

Название **Запись событий, которые изменяют системные права доступа - lchown**

Описание

Как минимум, система аудита должна записывать изменения прав доступа к файлам для всех пользователей, включая суперпользователя. Необходимо добавить следующее `/etc/audit/audit.rules`:

```
-a always,exit -F arch=b32 -S lchown -F auid>=500 -F auid!=4294967295 \
    -k perm_mod
```

If the system is 64 bit then also add the following:

```
-a always,exit -F arch=b64 -S lchown -F auid>=500 -F auid!=4294967295 \
    -k perm_mod
```

Параметр Критичность: Низкий

Название **Запись событий, которые изменяют системные права доступа - lremovexattr**

Описание

Как минимум, система аудита должна записывать изменения прав доступа к файлам для всех пользователей, включая суперпользователя. Необходимо добавить следующее `/etc/audit/audit.rules`:

```
-a always,exit -F arch=b32 -S lremovexattr -F auid>=500 -F auid!=4294967295 \
    -k perm_mod
```

If the system is 64 bit then also add the following:

```
-a always,exit -F arch=b64 -S lremovexattr -F auid>=500 -F auid!=4294967295 \
    -k perm_mod
```

Параметр Критичность: Низкий

Название **Запись событий, которые изменяют системные права доступа - lsetxattr**

Описание

Как минимум, система аудита должна записывать изменения прав доступа к файлам для всех пользователей, включая суперпользователя. Необходимо добавить следующее `/etc/audit/audit.rules`:

```
-a always,exit -F arch=b32 -S lsetxattr -F auid>=500 -F auid!=4294967295 \
    -k perm_mod
```

If the system is 64 bit then also add the following:

```
-a always,exit -F arch=b64 -S lsetxattr -F auid>=500 -F auid!=4294967295 \
    -k perm_mod
```

Параметр Критичность: Низкий

Название **Запись событий, которые изменяют системные права доступа - removexattr**

Описание

Как минимум, система аудита должна записывать изменения прав доступа к файлам для всех пользователей, включая суперпользователя. Необходимо добавить следующее `/etc/audit/audit.rules`:

```
-a always,exit -F arch=b32 -S removexattr -F auid>=500 -F auid!=4294967295 \
    -k perm_mod
```

If the system is 64 bit then also add the following:

```
-a always,exit -F arch=b64 -S removexattr -F auid>=500 -F auid!=4294967295 \
    -k perm_mod
```

Параметр Критичность: Низкий

Название **Запись событий, которые изменяют системные права доступа - setxattr**

Описание

Как минимум, система аудита должна записывать изменения прав доступа к файлам для всех пользователей, включая суперпользователя. Необходимо добавить следующее `/etc/audit/audit.rules`:

```
-a always,exit -F arch=b32 -S setxattr -F auid>=500 -F auid!=4294967295 \
    -k perm_mod
```

If the system is 64 bit then also add the following:

```
-a always,exit -F arch=b64 -S setxattr -F auid>=500 -F auid!=4294967295 \
    -k perm_mod
```

Параметр Критичность: Низкий

Название **Проверка, что auditd собирает информацию о не авторизованных доступах к файлам**

Описание

Как минимум, система аудита должна записывать информацию о авторизованных доступах к файлам для всех пользователей, включая суперпользователя. Следующее необходимо добавить в `/etc/audit/audit.rules`,

устанавливая ARCH либо b32 или b64, необходимую для вашей системы:
```
-a always,exit -F arch=ARCH -S creat -S open -S openat -S truncate \
    -S ftruncate -F exit=-EACCES -F auid>=500 -F auid!=4294967295 -k access
-a always,exit -F arch=ARCH -S creat -S open -S openat -S truncate \
    -S ftruncate -F exit=-EPERM -F auid>=500 -F auid!=4294967295 -k access
```

Параметр	Критичность: Низкий
Название	**Проверка, что auditd собирает информацию об использовании привилегированных команд**
Описание	

Как минимум, система аудита должна записывать информацию о выполнении привилегированных команд для всех пользователей, включая суперпользователя. Чтобы найти соответствующие биты SETUID программы, выполните команду:
```
# find / -xdev -type f -perm -4000 -o -perm -2000 2>/dev/null
```
Затем, для каждого бита SETUID программы в системе необходимо добавить строку в `/etc/audit/audit.rules`, где *SETUID_PROG_PATH* это полный путь к каждому биту SETUID программ в списке:
```
-a always,exit -F path=SETUID_PROG_PATH -F perm=x -F auid>=500 -F auid!=4294967295 -k
privileged
```

Параметр	Критичность: Низкий
Название	**Проверка, что auditd собирает информацию об экспорте носителей**
Описание	

Как минимум, система аудита должна записывать информацию о событиях экспорта носителя для всех пользователей, включая суперпользователя. Следующее необходимо добавить в `/etc/audit/audit.rules`, устанавливая ARCH либо b32 или b64, необходимую для вашей системы:
```
-a always,exit -F arch=ARCH -S mount -F auid>=500 -F auid!=4294967295 -k export
```

Параметр	Критичность: Низкий
Название	**Проверка, что auditd собирает информацию об удалении файлов пользователем**
Описание	

Как минимум, система аудита должна записывать информацию об удалении файлов для всех пользователей, включая суперпользователя. Следующее необходимо добавить в `/etc/audit/audit.rules`, устанавливая ARCH либо b32 или b64, необходимую для вашей системы:
```
-a always,exit -F arch=ARCH -S unlink -S unlinkat -S rename -S renameat \
    -F auid>=500 -F auid!=4294967295 -k delete
```

Параметр	Критичность: Низкий
Название	**Проверка, что auditd собирает действия системного администратора**
Описание	

Как минимум, система аудита должна записывать действия администратора для всех пользователей, включая суперпользователя. Следующее необходимо добавить в `/etc/audit/audit.rules`:
```
-w /etc/sudoers -p wa -k actions
```

Параметр	Критичность: Низкий
Название	**Проверка, что auditd собирает информацию о загрузка и выгрузке модулей ядра**
Описание	

Следующее необходимо добавить в `/etc/audit/audit.rules` для того, чтобы захватывать события загрузки и выгрузки модулей ядра, устанавливая ARCH либо b32 или b64, необходимую для вашей системы:

```
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit -F arch=ARCH -S init_module -S delete_module -k modules
```

Группа

Название **Службы**

Описание

Лучшая защита от уязвимостей ПО это работать с меньшим количеством ПО. В этом разделе описывается как проверять ПО, которое установлено в систему и отключение ПО, в котором нет необходимости. Затем перечисляются пакеты ПО, установленные на умолчанию в систему Ubuntu, и даются рекомендации о том, какие из них можно безопасно отключить.

Ubuntu обеспечивает удобный вариант минимальной установки, который устанавливает самое необходимое для функционирования системы. При создании серверов на базе Ubuntu настоятельно рекомендуется выбирать минимум пакетов, а затем доустановить необходимые.

Группа

Название **Устаревшие службы**

Описание

В этом разделе рассматриваются ряд видимых в сети служб, которые исторически создают проблемы для безопасности системы, и для которых отключение или строгое ограничение было наилучшим имеющимся решением на некоторое время. В результате этого, многие из этих служб не установлены как часть системы по умолчанию.

Организации, которые работают с этими службами должны перейти на более безопасные аналоги как можно скорее. Если есть необходимость запусить одну из этих устаревших служб, следует позаботиться, чтобы ограничить службу как можно больше, например, путем настройки брандмауэров, таких как `iptables`, чтобы разрешить доступ к уязвимым службам только с тех удаленных хостов, с которых необходимо их использовать.

Группа

Название **Xinetd**

Описание

Служба `xinetd` выступает в качестве ожидающей подключения для выделенных портов некоторых сетевых услуг (в основном устаревших) и может быть использована для обеспечения контроля доступа и сохранения логов. Это в основном устаревшая функция, и она не устанавливается по умолчанию. Старшая служба Inetd не доступна даже как часть системы.

Параметр Критичность: Низкий

Название **Удаление пакета xinetd**

Описание

Пакет `xinetd` может быть удален командой:

```
# apt-get remove xinetd
```

Группа

Название **Telnet**

Описание

Протокол Telnet не обеспечивает конфиденциальность и целостность информации, передаваемой по сети. Он включает в себя проверку подлинности информации, такой как пароли. Организации, которые используют Telnet, должны активно переходить на более безопасный протокол.

Параметр Критичность: Высокий

Название **Удаление пакета telnet-server**

Описание

Для удаления пакета `inetutils-telnetd` выполните команду:

```
# apt-get remove inetutils-telnetd
```

Группа

Название **Rlogin, Rsh, и Rexec**

Описание

Berkeley r-commands - устаревшие службы, которые позволяют осуществлять удаленный доступ открытым текстом без шифрования и являются небезопасными.

Параметр Критичность: Высокий

Название **Удаление файлов доверия Rsh**

Описание

Файлы `/etc/hosts.equiv` и `~/.rhosts` (в домашней директории пользователей) содержат список удаленных хостов и пользователей, которым доверяет локальная система при использовании службы rshd. Для удаления этих файлов, выполните команды:

```
# rm /etc/hosts.equiv
# rm /etc/shosts.equiv
# rm /root/.rhosts
# rm /root/.shosts
$ rm ~/.rhosts
$ rm ~/.shosts
```

Группа

Название **Информационная служба сети (NIS)**

Описание

Информационная служба сети, известная как 'Yellow Pages' (YP), и его преемник NIS+ устарели после Kerberos, LDAP, и других современных служб централизованной аутентификации. NIS не должны использоваться, поскольку они страдают проблемами безопасности, присущих им, такие как недостаточная защита важной информации об аутентификации.

Группа

Название **TFTP сервер**

Описание

TFTP представляет собой облегченную версию FTP протокола, который традиционно используется для настройки сетевого оборудования. Тем не менее, TFTP обеспечивает слабую безопасность, поэтому современные версии сетевых операционных систем часто поддерживают конфигурацию с помощью SSH или других, более безопасных протоколов. TFTP сервер должен быть запущен, только если нет более безопасного метода поддержки существующего оборудования.

Параметр Критичность: Средний

Название **Удаление пакета tftpd**

Описание

Пакет `tftpd` может быть удален командой:

```
# apt-get remove tftpd
```

Группа

Название **Базовые службы**

Описание

В данном разделе рассматриваются базовые службы, которые установлены на Ubuntu по умолчанию, которые не рассматриваются в других разделах. Некоторые из этих служб могут прослушивать сеть и должны рассматриваться с особой осторожностью. Другие службы используются локальными системными утилитами, которые могут быть опасными. В общем, системные службы должны быть отключены, если они не требуются.

Группа

Название **Службы Cron и At**

Описание

Службы cron и at используется, чтобы добавлять команды, которые будут выполнены в более позднее время. Обе службы должны быть настроены защищенно.

Параметр Критичность: Средний

Название **Включение службы cron**

Описание

Служба `cron` используется для периодического выполнения команд в назначенное время. Это требуется почти всем системам для выполнения необходимых задач по обслуживанию.

Группа

Название **SSH сервер**

Описание

Протокол SSH рекомендуется для удаленного входа в систему и удаленной передачи файлов. SSH обеспечивает конфиденциальность и целостность данных, передаваемых между двумя системами, а также аутентификацию сервера, с помощью криптографии с открытым ключом. Реализация, включенная в систему называется OpenSSH, более подробная документация доступна на веб-сайте, http://www.openssh.org. Служба называется `sshd` и предоставляется в пакете `openssh-server`.

Группа

Название **Настройка OpenSSH сервер**

Описание

Если система должна выступать в качестве SSH сервера, то определенные изменения должны быть внесены в конфигурационный файл службы OpenSSH `/etc/ssh/sshd_config`. Следующие рекомендации могут быть применены к этому файлу. Смотрите `sshd_config(5)` страницу с документацией для детальной информации.

Параметр	Критичность: Высокий
Название	**Разрешить только SSH Protocol 2**
Описание	

Соединения должны быть разрешены только по SSH протоколу версии 2. Необходимо проверить настройки по умолчанию в `/etc/ssh/sshd_config` и убедиться, что там есть следующая строка:
`Protocol 2`

Параметр	Критичность: Высокий
Название	**Выключение в SSH RhostsRSAAuthentication**
Описание	

Файл /etc/ssh/sshd_config должен содержать 'RhostsRSAAuthentication no'. Необходимо проверить настройки по умолчанию в `/etc/ssh/sshd_config` и убедиться, что там есть следующая строка:
`RhostsRSAAuthentication no`

Параметр	Критичность: Средний
Название	**Отключение SSH поддержки .rhosts файлов**
Описание	

SSH может эмулировать поведение устаревших команд RSH, позволяющих пользователям включить небезопасный доступ к своим аккаунтам через `.rhosts` файлы.

Для отключения такого поведения, необходимо исправить или дополнить следующую строку в `/etc/ssh/sshd_config`:
`IgnoreRhosts yes`

Параметр	Критичность: Низкий
Название	**Ограничение пользователям SSH доступа**
Описание	

По умолчанию SSH настроен разрешать любым пользовательским аккаунтам подключаться к системе. Для того, чтобы указать пользователей, которым разрешен вход через SSH и запрещать всем остальным пользователям, необходимо исправить или дополнить следующую строку в `/etc/ssh/sshd_config`:
`DenyUsers USER1 USER2`
Где `USER1` и `USER2` пользователи, которым запрещен вход.

Параметр	Критичность: Низкий
Название	**Установка SSH интервала времени ожидания**
Описание	

SSH разрешает администраторам устанавливать время ожидания. После того, как время ожидания истекло, пользователь автоматически выходит из системы.

Для установки времени ожидания необходимо отредактировать строку в `/etc/ssh/sshd_config` как показано ниже:
`ClientAliveInterval` **`interval`**
Время ожидания **interval** указывается в секундах. Чтобы установить ожидание в 15 минут, необходимо установить значение **interval** в 900.

Если время ожидания уже установлено для входа в оболочку, то это значение будет вытеснять любые SSH настройки, сделанные здесь. Имейте в виду, что некоторые процессы могут помешать SSH правильно определять то, что

пользователь находится в режиме ожидания.

Источники
CCE-26919-1 http://cce.mitre.org

Параметр Критичность: Низкий

Название	**Установка SSH Client Alive Count**
Описание	

Необхомибо убедиться, что SSH тайм-аут происходит именно тогда, когда `ClientAliveCountMax` установлен, отредактируйте файл `/etc/ssh/sshd_config`, добавив следующее:

```
ClientAliveCountMax 0
```

Источники
CCE-26282-4 http://cce.mitre.org

Параметр Критичность: Средний

Название	**Отключение Host-Based аутентификации**
Описание	

Host-based аутентификация является более безопасной, чем `.rhosts`. Однако, не рекомендуется, чтобы хосты в одностороннем порядке доверяли друг другу, даже в пределах организации.

Для отключения host-based аутентификации, необходимо исправить или дополнить следующую строку в `/etc/ssh/sshd_config`:

```
HostbasedAuthentication no
```

Параметр Критичность: Средний

Название	**Отключение возможности авторизации суперпользователя в SSH**
Описание	

Суперпользователю никогда не должно быть позволено войти в систему непосредственно через сеть. Чтобы отключить возможность авторизации суперпользователя в SSH, необходимо исправить или дополнить следующую строку в `/etc/ssh/sshd_config`:

```
PermitRootLogin no
```

Параметр Критичность: Высокий

Название	**Отключение SSH доступа с пустыми паролями**
Описание	

Чтобы явно запретить удаленный вход из аккаунтов с пустыми паролями, необходимо исправить или дополнить следующую строку в `/etc/ssh/sshd_config`:

```
PermitEmptyPasswords no
```

Любые аккаунты с пустыми паролями должны быть отключены немедленно, и PAM конфигурация должна запретить пользователям возможность задавать пустые пароли.

Параметр Критичность: Средний

Название	**Включение SSH предупреждающего баннера**

Описание

Чтобы включить предупреждающий баннер необходимо убедиться, что он соответствует всей системе, и исправить или дополнить следующую строку в `/etc/ssh/sshd_config`:

```
Banner /etc/issue
```

В другом разделе содержится информация о том, как создать соответствующий системный предупреждающий баннер.

Параметр Критичность: Низкий

Название **Не разрешать SSH переменные окружения**

Описание

Чтобы не передавать параметры окружения службе SSH, необходимо исправить или дополнить следующую строку в `/etc/ssh/sshd_config`:

```
PermitUserEnvironment no
```

Источники

CCE-27201-3
http://cce.mitre.org

Параметр Критичность: Средний

Название **Использование только принятых алгоритмов шифрования**

Описание

Необходимо ограничиться шифрованием только теми алгоритмами, которые FIPS-утверждены. Следующая строка в `/etc/ssh/sshd_config` демонстрирует использование FIPS-утвержденных алогитмов:

```
Ciphers aes128-ctr,aes192-ctr,aes256-ctr
```

Страница с документацией `sshd_config(5)` содержит список поддерживаемых алгоритмов.

Источники

CCE-26555-3
http://cce.mitre.org

Группа

Название **X Window System**

Описание

The X Window System implementation included with the system is called X.org.

Группа

Название **Отключение X Windows**

Описание

Если нет критически важных причин в системе для использования графического интерфейса пользователя, убедитесь, что X не запускается автоматически при загрузке системы и удалите пакеты программного обеспечения X Windows. Обычно нет причин для запуска X Windows на выделенном сервере, так как он увеличивает потребление ресурсов системы и возможности атаки. Администраторы сервера должны входить в систему через SSH или текстовую консоль.

Группа

Название **Avahi сервер**

Описание

Служба Avahi реализует протоколы DNS Service Discovery и Multicast DNS, которые позволяют системе автоматически определять ресурсы в сети, такие как принтеры или веб-сервера. Эта возможность также известна как mDNSresponder и является основной частью из Zeroconf сетей.

Группа

Название **Отключение Avahi сервера, если это возможно**

Описание

Поскольку служба Avahi держит открытым сетевой порт, она подлежит сетевым атакам. Ее отключение может уменьшить уязвимость системы к таким атакам.

Группа

Название **DHCP**

Описание

Протокол динамической настройки узла (DHCP) позволяет системам запрашивать и получать IP-адреса и другие параметры конфигурации с сервера.

В общем, узлы используют DHCP чтобы позволить большой пул мобильных или неизвестных машин либо для стандартизации установок, избегая статических, индивидуальных конфигураций IP адресов для хостов. Рекомендуется максимально предотвращать использование DHCP. Так как DHCP аутентификация плохо поддерживается, DHCP-клиенты открыты для атак от поддельных DHCP серверов. Такие сервера могут дать клиентам неверную информацию (например, вредоносный сервер DNS адресов), которые могут их компрометировать.

Если машина должна действовать в качестве клиента или сервера DHCP, необходимо настроить его защищенно с использованием указаний в этом разделе. Это руководство рекомендует выполнять настройки сети на клиентах с помощью ручного редактирования соответствующих файлов `/etc/sysconfig`. Кроме того, можно использовать графический интерфейс программ system-config-network и system-config-network-tui, но эти программы переписывают файлы конфигурации с нуля на основе их значения по умолчанию - это уничтожит любые ручные изменения - и поэтому должны быть использованы с осторожностью.

Группа

Название **Отключение DHCP клиента**

Описание

DHCP является методом по умолчанию для сетевой конфигурации, предоставляемый системой установки, и общий для многих сетей. Тем не менее, ручное управление IP-адресами для систем подразумевает большую степень управления и отчетности сетевой активности.

Группа

Название **Network Time Protocol**

Описание

Network Time Protocol используется для управления системными часами в сети. Компьютерные часы не очень точны, так что время будет изменяться непредсказуемо на неуправляемых системах. Центральные протоколы времени могут быть использованы как для обеспечения одного времени между сетью машин, так и для соответствия времени с внешним миром.

Локальная синхронизация времени рекомендуется для всех сетей. Если каждая машина в сети надежно сообщает то же время, как и любая другая машина, то это сильно упрощает соотношение сообщений в журнале в случае аттак. Кроме того, ряд криптографических протоколов (таких как Kerberos) используют метки для предотвращения некоторых видов атак. Если ваша сеть не была синхронизирована по времени, эти протоколы могут быть недостоверными или даже

непригодными для использования.

В зависимости от специфики сети, глобальная точность времени может быть так же важна, как и локальная синхронизация. Если ваша сеть подключена к Интернету, рекомендуется использовать публичный сервер времени или один из предоставляемых вашим провайдером, так как глобально точный тайминг может быть необходим, если вам нужно расследовать или отследить атаку, которая возникла за пределами вашей сети.

Типичная настройка сети включает в себя небольшое число внутренних систем, работающих в качестве серверов NTP, а остальные получают информацию времени от этих внутренних серверов.

Более подробную информацию о том, как настроить ПО NTP сервера, включая настройку криптографической аутентификации для временных данных, можно ознакомиться на http://www.ntp.org.

Группа	
Название	**Сервер электронной почты**
Описание	

Сервера электронной почты используются для отправки и получения писем по сети. Почта это очень распространенный сервис, и агент пересылки сообщений (MTAs) является очевидной целью сетевых атак. Необходимо проверить, что машины не работают с MTA излишне, и настроить необходимые MTA защищенно насколько это возможно.

Очень мало систем должны быть настроены напрямую получать электронную почту по сети. Вместо этого пользователи должны использовать почтовые клиенты для получения почты с центрального сервера, который поддерживает такие протоколы, как IMAP или POP3. Тем не менее, для большинства систем является нормальным самостоятельно отправлять электронную почту, например, чтобы назначенные задания могли отправить отчет администратору. Большинство MTA, в том числе Postfix, поддерживает представление только в режиме, в котором почта может быть отправлена с локальной системы на центральном узле MTA (или доставляется в локальную учетную запись), но система не может получать почту непосредственно через сеть.

В Ubuntu разрешается выбор альтернативного программного обеспечения почтовых серверов (например, Sendmail), но Postfix установлен по умолчанию и является предпочтительным. Postfix был написан с учетом требований безопасности и может быть более эффективно использоваться в SELinux. Более подробная информация доступна на веб-сайте http://www.postfix.org.

Группа	
Название	**Настройка SMTP для почтовых клиентов**
Описание	

В этом разделе рассматриваются настройки для Postfix только в виде конфигурации электронной почты.

Группа	
Название	**LDAP**
Описание	

LDAP является популярной службой каталогов, то есть стандартизированным способом поиска информации из центральной базы данных. Он относительно прост в настройке Ubuntu для получения аутентификационной информации из LDAP сервера. Если в вашей сети для аутентификации используется LDAP, убедитесь, что настройки клиентов и сервера безопасны.

Группа	
Название	**Настройка клиентов OpenLDAP**
Описание	

Это руководство рекомендует сконфигурировать OpenLDAP клиентов вручную, редактируя соответствующие

конфигурационные файлы. Ubuntu обеспечивает автоматизированный инструмент для настройки AuthConfig и графические оболочки к нему `system-config-authentication`. Однако, эти инструменты не дают достаточной гибкости для настройки. Инструменты authconfig не позволяют указать расположение файлов сетрификатов SSL, который пригодится при попытке использовать SSL по нескольким протоколам.

Группа	
Название	**Настройка OpenLDAP сервера**
Описание	

Этот раздел содержит рекомендации по настройке OpenLDAP сервера для безопасного представления информации и использования в Центральной Службе Аутентификации (CAS). Это не полное руководство по поддержанию OpenLDAP сервера, но тем не менее может быть полезно в обеспечении инфраструктуры OpenLDAP.

Группа	
Название	**NFS и RPC**
Описание	

Network File System является популярной распределенной файловой системой для Unix окружения, и очень широко распространена. Этот раздел рассматривает обстоятельства, при которых можно отключить NFS и его зависимости, и подробные шаги, которые должны быть предприняты для обеспечания безопасности NFS конфигурации. Этот раздел имеет отношение к машинам, которые работают как NFS-клиенты, так и NFS-сервера.

Группа	
Название	**Настройка NFS-клиентов**
Описание	

Шаги, описанные в этом разделе, подходят к машинам, работающим как NFS-клиенты.

Группа	
Название	**Монтирование удаленных файловых систем с ограничивающими параметрами**
Описание	

Необходимо отредактировать файл `/etc/fstab`, в котором для всех файловых систем, тип которых (столбец 3) `nfs` или `nfs4`, добавив текст `,nodev,nosuid` в список параметров монтирования в столбце 4. Если необходимо, также добавить `,noexec`.

См. раздел "Монтирование удаленных файловых систем с ограничивающими параметрами" для описания эффектов этих параметров. В общем, запуск файлов, монтируемых при помощи NFS, следует рассматривать рискованным из-за возможности того, что противник может перехватить запрос и заменить выполняемый файл вредоносным. Разрешение setuid файлов, которые будут выполняться с удаленных серверов, особенно опасны потому, что требуют клиентам расширить root-уровень доверия к серверу NFS.

Группа	
Название	**Samba(SMB) Microsoft Windows File Sharing Server**
Описание	

При правильной настройке служба Samba позволяет Linux-машинам обеспечить доступ к файлам и принтерам в Microsoft Windows. Есть два программных пакета, обеспечивающих поддержку Samba. Первый, `samba-client`, предоставляет ряд утилит командной строки, которые предоставляют машине клиента доступ к Samba-общедоступным ресурсам. Второй, называется `samba`, предоставляет Samba сервис. Именно этот второй пакет позволяет Linux машинам выступать в роли Active Directory сервера, контроллера домена, или членом домена. Только `samba-client` пакет устанавливается

по умолчанию.

Группа	
Название	**Настройки Samba, если необходимо**
Описание	

Все настройки службы Samba могут быть найдены в `/etc/samba/smb.conf`. Настройки делятся на `[global]` раздел конфигурации и раздел пользовательских общих ресурсов, которые должны описывать общедоступные файлы и принтеры в системе. По умолчанию Samba работает в режиме пользователя и позволяет клиентским машинам доступ к локальным домашним директориям и принтерам.Рекомендуется, чтобы эти параметры были изменены или установлены дополнительные ограничения.

Конец отчета. RedCheck 1.4.1.1.
RedCheckID: 6DF9800A-476F-43D7-B922-36DDF894130F.