RED Check

ОТЧЁТ

№ отчёта	*d53ddef6-0165-4856-85ba-ecde243994a6*
Профиль	*Конфигурации*
Задание	*конфигурации clone 2*
Начало/завершение сканирования	*06.05.2022 14:32:01 / 06.05.2022 14:34:11*
Формирование отчёта	*06.05.2022 14:36:37*
Имя	*конфигураци клон 2*
Хосты [1]	*10.17.10.34*

Сводная таблица результатов сканирования

Хост	Конфигурация	Всего	Соответствие
10.17.10.34	Конфигурация аудита безопасности "Дополнительные Сервисы Linux"	15	0
10.17.10.34	Конфигурация аудита безопасности Remote Access Checklist	26	4
10.17.10.34	Конфигурация безопасности ОС ALT	100	35

Хост: 10.17.10.34

sto-app-2c_clone

CPE	*cpe:/o:unix*
Начало/завершение сканирования	*06.05.2022 14:32:01 / 06.05.2022 14:32:44*
Учётные данные	*Имя профиля: new_linux* *Тип: Ssh* *Sudo: Нет*
Метод получения данных	*Безагентный механизм*

Конфигурация аудита безопасности "Дополнительные Сервисы Linux" (версия: 12)

Конфигурация не соответствует эталонной. Всего - 15, соответствие - 0 (0 %)

Несоответствие (13) **Не проверено (2)**

- **Общие параметры**
  - **Auditd**
    - Audit демон не установлен или не запущен
      Критичность: Высокий
    - Auditd не следит за критически важным файлами
      Критичность: Средний
  - **Cron/crontab**
    - Системный crontab
      Критичность: Высокий
    - crontab для пользователей
      Критичность: Высокий
  - **DNS**
    - Конфигурационный файл резолвера имеет неверный формат
      Критичность: Высокий
  - **Email**
    - Файл /etc/aliases
      Критичность: Средний
    - Файл $HOME/.forward
      Критичность: Высокий
    - Конфигурируемые пользователем LDA (procmail)
      Критичность: Высокий
  - **Сервис syslog**
    - Любой пользователь может читать log-файлы
      Критичность: Высокий
    - Криптографическая защита log-файлов в rsyslog
      Критичность: Средний
  - **Файловая система**
    - setuid файлы
      Критичность: Высокий
    - Разделяемые библиотеки
      Критичность: Высокий

- Загрузчик
  Критичность: Высокий
- Инициализационные скрипты
  Критичность: Высокий
- Пользовательские каталоги и файлы
  Критичность: Высокий

CPE	*cpe:/o:unix*
Начало/завершение сканирования	*06.05.2022 14:32:54 / 06.05.2022 14:33:17*
Учётные данные	*Имя профиля: new_linux* *Тип: Ssh* *Sudo: Нет*
Метод получения данных	*Безагентный механизм*

Конфигурация аудита безопасности Remote Access Checklist (версия: 16)

Конфигурация не соответствует эталонной. Всего - 26, соответствие - 4 (15 %)

Соответствие (4) **Несоответствие (18)** **Неприменимо (1)**
Не проверено (3)

Общие параметры

- Использование нестойкой криптосхемы для хранения паролей
  Критичность: Средний
- Большое время жизни пароля
  Критичность: Средний
- Не единственный суперпользователь в системе
  Критичность: Низкий
- Выполнение команды sudo без запроса пароля
  Критичность: Средний
- Небезопасный secure_path в /etc/sudoers
  Критичность: Средний
- Sudo и небезопасный env_keep в /etc/sudoers
  Критичность: Низкий
- Отсутствие регистрация попыток входа в систему
  Критичность: Средний
- Включенный режим маршрутизации
  Критичность: Низкий

SSH

- Небезопасные права доступа
  Критичность: Высокий
- Запрещение X11Forwarding
  Критичность: Средний
- Запрещение пользовательских .rhosts/.shosts файлов
  Критичность: Высокий
- Проверка ip/dns-адреса клиента
  Критичность: Средний
- Запретить беспарольный доступ в систему
  Критичность: Высокий

- Использование HashKnownHosts
  Критичность: Высокий
- Отсутствие ограничений на доступ к серверу
  Критичность: Информация
- Доступ для root
  Критичность: Высокий
- Работа сервера на порту по умолчанию
  Критичность: Информация
- Включена аутентификация по ключу
  Критичность: Информация
- Ограничение попыток неуспешного доступа
  Критичность: Высокий
- DNS SSHFP запись
  Критичность: Информация
- Отсутствие защиты от перебора паролей по сети fail2ban
  Критичность: Высокий
- Использование устаревшей версии протокола
  Критичность: Средний

Remote Access

- Использование устаревших сервисов (telnet, rsh, rcp, etc)
  Критичность: Высокий
- Политика доступа по tcp/udp/ip (порты/приложения): Постоянные приложения
  Критичность: Информация
- Политика доступа по tcp/udp/ip (порты/приложения): inetd приложения
  Критичность: Информация
- Политика фильтрации iptables
  Критичность: Высокий

CPE	*cpe:/o:unix*
Начало/завершение сканирования	*06.05.2022 14:33:26 / 06.05.2022 14:34:11*
Учётные данные	*Имя профиля: new_linux* *Тип: Ssh* *Sudo: Нет*
Метод получения данных	*Безагентный механизм*

Конфигурация безопасности ОС ALT (версия: 4)

Конфигурация не соответствует эталонной. Всего - 100, соответствие - 35 (35 %)

Соответствие (35) **Несоответствие (63)** **Неприменимо (2)**

Системные настройки

Установка и обслуживание ПО

Разметка диска

- Директория /tmp располагается на отдельном разделе
  Критичность: Низкий
- Директория /var располагается на отдельном разделе
  Критичность: Низкий

- Директория /var/log располагается на отдельном разделе
  Критичность: Низкий
- Директория /var/log/audit располагается на отдельном разделе
  Критичность: Низкий
- Директория /home располагается на отдельном разделе
  Критичность: Низкий

Обновление программного обеспечения

- Параметр gpgcheck должен быть включён для всех yum репозиториев
  Критичность: Высокий

Права доступа к файлам и маски

Ограничение параметров монтирования разделов

- Добавление nodev опции для некорневых локальных разделов
  Критичность: Низкий
- Добавление опции nodev для подключаемых разделов
  Критичность: Низкий
- Добавление опции noexec для подключаемых медиа разделов
  Критичность: Низкий

Проверка прав доступа у важных файлов и директорий

Проверка прав доступа у файлов, содержащих информацию о локальных учётных записях

- Проверка владельца shadow файла
  Критичность: Средний
- Проверка группы владельца файла shadow
  Критичность: Средний
- Проверка прав доступа файла shadow
  Критичность: Средний
- Проверка владельца файла group
  Критичность: Средний
- Проверка группы владельца файла group
  Критичность: Средний
- Проверка прав доступа к файлу group
  Критичность: Средний
- Проверка владельца файла gshadow
  Критичность: Средний
- Проверка группы владельца файла gshadow
  Критичность: Средний
- Проверка прав доступа к файлу gshadow
  Критичность: Средний
- Проверка владельца файла passwd
  Критичность: Средний
- Проверка группы владельца файла passwd
  Критичность: Средний
- Проверка прав доступа к файлу passwd
  Критичность: Средний

Проверка прав доступа для файлов внутри важных системных директорий

- Проверка прав доступа разделяемых библиотек
  Критичность: Средний
- Проверка, что владельцем разделяемых библиотек является суперпользователь
  Критичность: Средний

- ✓ Проверка прав доступа исполняемых файлов
  Критичность: Средний
- ✓ Проверка, что владельцем системных исполняемых файлов является суперпользователь
  Критичность: Средний

- ✓ **Ограничение программ от возможного опасного поведения**
  - ✓ Включение рандомизированного расположения виртуального адресного пространства
    Критичность: Средний

- ✗ **Учётные записи и контроль доступа**
  - ✗ **Защита учётных записей с помощью ограничения входа по паролю**
    - ✓ **Ограничение входа суперпользователя**
      - ✓ Ограничение входа суперпользователя в виртуальную консоль
        Критичность: Средний
      - ✓ Ограничение входа суперпользователя через последовательный порт
        Критичность: Низкий
      - ✓ Обеспечение безопасности оболочки при входе под системной учётной записью
        Критичность: Средний
      - ✓ Проверка, что только у суперпользователя UID 0
        Критичность: Средний
    - ✓ **Проверка правильности хранения и существования хэшей паролей**
      - ✓ Предотвращение входа в аккаунт с пустым паролем
        Критичность: Высокий
      - ✓ Проверка на скрытость хэшей паролей во всех аккаунтах
        Критичность: Средний
    - ✗ **Установка параметров срока действия пароля**
      - ✗ Установка минимального срока действия пароля
        Критичность: Средний
      - ✗ Установка максимального срока действия пароля
        Критичность: Средний
      - ✗ Установка предупреждения о сроке действия пароля
        Критичность: Низкий
  - ✗ **Защита аккаунтов с помощью настройки PAM**
    - ✓ Установка минимальной длины пароля
      Критичность: Средний
    - ✗ Установка блокировки после неудачных попыток ввода пароля
      Критичность: Средний
  - ✗ **Защита доступа к физической консоли**
    - ✗ Проверка прав доступа к файлам конфигурации загрузчика
      Критичность: Средний

- ✗ **Настройка сети и брандмауэра**
  - ✗ **Параметры ядра, которые влияют на сеть**
    - ✗ **Параметры сети только для хостов**
      - ✗ Отключение параметра ядра для отправки перенаправлений ICMP по умолчанию
        Критичность: Средний
      - ✗ Отключение параметра ядра для отправки перенаправлений ICMP для всех интерфейсов
        Критичность: Средний
      - ✓ Отключение параметра ядра для IP Forwarding
        Критичность: Средний

- **Параметры ядра, влияющие на сеть для хостов и маршрутизаторов**
  - Отключение параметра ядра для принятия Source-Routed пакетов для всех интерфейсов
    Критичность: Средний
  - Отключение параметра ядра для приема ICMP перенаправлений для всех интерфейсов
    Критичность: Средний
  - Отключение параметра ядра для принятия безопасных перенаправлений для всех интерфейсов
    Критичность: Средний
  - Включение параметра ядра для журналирования Martian Packets
    Критичность: Низкий
  - Отключение параметра ядра для принятия Source-Routed пакетов по умолчанию
    Критичность: Средний
  - Отключение параметра ядра для приема ICMP перенаправлений по умолчанию
    Критичность: Низкий
  - Отключение параметра ядра для приема защищенных перенаправлений по умолчанию
    Критичность: Средний
  - Включение параметра ядра для игнорирования ICMP Broadcast Echo запросов
    Критичность: Низкий
  - Включение параметра ядра для игнорирования Bogus ICMP сообщений об ошибках
    Критичность: Низкий
  - Включение параметра ядра для использования TCP Syncookies
    Критичность: Средний
  - Включение параметра ядра для использования фильтрации обратного пути у всех интерфейсов
    Критичность: Средний
  - Включение параметра ядра для использования фильтрации обратного пути по умолчанию
    Критичность: Средний
- **Беспроводные сети**
  - Отключение Беспроводных сетевых интерфейсов
    Критичность: Низкий
- **Брандмауэр**
  - Найстройка брандмауэра
    Критичность: Средний
- **Настройка OpenSSH сервера**
  - Отключение SSH поддержки .rhosts файлов
    Критичность: Средний
  - Установка SSH интервала времени ожидания
    Критичность: Низкий
  - Установка SSH Client Alive Count
    Критичность: Низкий
  - Отключение Host-Based аутентификации
    Критичность: Средний
  - Отключение возможности авторизации суперпользователя в SSH
    Критичность: Средний
  - Отключение SSH доступа с пустыми паролями
    Критичность: Высокий
  - Включение SSH предупреждающего баннера
    Критичность: Средний
  - Не разрешать SSH переменные окружения
    Критичность: Низкий

- Разрешить только SSH Protocol 2
  Критичность: Высокий
- Выключение в SSH RhostsRSAAuthentication
  Критичность: Высокий

Система учета с журналированием (auditd)

- Включение службы auditd
  Критичность: Средний

Настройка хранения данных auditd

- Настройка auditd количества нераспределенных журналов
  Критичность: Средний
- Настройка auditd максимального размера файла журнала
  Критичность: Средний
- Настройка auditd действия при достижении максимального размера журнала
  Критичность: Средний
- Настройка действия admin_space_left при недостаточном месте на диске
  Критичность: Средний
- Настройка auditd для использования плагина audispd
  Критичность: Средний

Настройка комплекса правил auditd

Запись событий, изменяющих информацию о дате и времени

- Запись событий, изменяющих время через adjtimex
  Критичность: Низкий
- Запись событий, изменяющих время через settimeofday
  Критичность: Низкий
- Запись событий, изменяющих время через stime
  Критичность: Низкий
- Запись событий, изменяющих время через clock_settime
  Критичность: Низкий
- Запись событий, изменяющих время файла
  Критичность: Низкий

- Запись событий, которые изменяют информацию о пользователях/группах
  Критичность: Низкий
- Запись событий, которые изменяют системное сетевое окружение
  Критичность: Низкий
- Журналы аудита системы должны иметь права 0640 или менее разрешающие
  Критичность: Низкий
- Журналы аудита системы должны принадлежать суперпользователю
  Критичность: Низкий

Запись событий, которые изменяют системные права доступа

- Запись событий, которые изменяют системные права доступа - chmod
  Критичность: Низкий
- Запись событий, которые изменяют системные права доступа - chown
  Критичность: Низкий
- Запись событий, которые изменяют системные права доступа - fchmod
  Критичность: Низкий
- Запись событий, которые изменяют системные права доступа - fchmodat
  Критичность: Низкий

- Запись событий, которые изменяют системные права доступа - fchown
  Критичность: Низкий
- Запись событий, которые изменяют системные права доступа - fchownat
  Критичность: Низкий
- Запись событий, которые изменяют системные права доступа - fremovexattr
  Критичность: Низкий
- Запись событий, которые изменяют системные права доступа - fsetxattr
  Критичность: Низкий
- Запись событий, которые изменяют системные права доступа - lchown
  Критичность: Низкий
- Запись событий, которые изменяют системные права доступа - lremovexattr
  Критичность: Низкий
- Запись событий, которые изменяют системные права доступа - lsetxattr
  Критичность: Низкий
- Запись событий, которые изменяют системные права доступа - removexattr
  Критичность: Низкий
- Запись событий, которые изменяют системные права доступа - setxattr
  Критичность: Низкий

- Проверка, что auditd собирает информацию о не авторизованных доступах к файлам
  Критичность: Низкий
- Проверка, что auditd собирает информацию об использовании привилегированных команд
  Критичность: Низкий
- Проверка, что auditd собирает информацию об экспорте носителей
  Критичность: Низкий
- Проверка, что auditd собирает информацию об удалении файлов пользователем
  Критичность: Низкий
- Проверка, что auditd собирает действия системного администратора
  Критичность: Низкий
- Проверка, что auditd собирает информацию о загрузка и выгрузке модулей ядра
  Критичность: Низкий
- Сделать конфигурацию auditd неизменяемой
  Критичность: Низкий

Описание параметров

Группа	
Название	**Общие параметры**

Группа	
Название	**Auditd**

Параметр	
Название	**Audit демон не установлен или не запущен**
Описание	

Значение по умолчанию: зависит от дистрибутива, в RH-based обычно установлен, в Debian-based нет.

Рекомендуемое значение: установить и убедиться, что он запускается автоматически при старте.

Область действия: вся система.

Подробнее: пакет audit и демон auditd предназначены для контроля системы и информирования администратора системы о подозрительных событиях в системе. Конфигурационные файлы /etc/audit/audit.conf и /etc/audit/audit.rules, log-файлы обычно в /var/log/audit каталоге. Стандартный /etc/audit/audit.conf, поставляемый с пакетом, достаточен для работы. Файл правил обычно пуст, и правила в него надо добавлять самостоятельно. В следующем параграфе будут приведены несколько правил, которые можно считать стандартными и использовать как примеры для своих правил. Log-файл audit.log имеет не очень понятный формат, поэтому в рамках auditd проекта были разработаны утилиты для работы с информацией в нём, например: "aulastlog -u root" и "ausearch --start this-week -k identity --raw | aureport --file --summary".

Параметр	
Название	**Auditd не следит за критически важным файлами**
Описание	

Значение по умолчанию: ничего

Рекомендуемое значение: сконфигурировать для наблюдения за важными файлами (/etc/group, /etc/passwd, /etc/shadow, /etc/sudoers, /etc/hosts, и каталогом /etc/sudoers.d (-w path-to-file). Интересующие нас события -- запись в файл и смена аттрибутов файла (-p wa). -k string -- метка события, которой затем помечается событие в лог-файле.

Область действия: вся система.

Подробнее: при взломе системы/сервера злоумышленник постарается изменить важные файлы конфигурации. Можно настроить auditd так, что он будет отслеживать все манипуляции а данными файлами/каталогами и в реальном времени информировать администратора о них. Операции, которые можно указать для опции -p:
- r -- чтение файла
- w -- запись в файл
- x -- выполнение файла
- a -- смена атрибутов файла

Более подробно можно посмотреть в документации на пакет и индивидуальные man- страницы.

Группа	
Название	**Cron/crontab**
Описание	

Cron - системная утилита, которая служит для исполнения заданий в заданное время и с заданным периодом. Состоит из двух частей -- системной, когда задания запускаются от суперпользователя (root), и пользовательский, когда задания выполняются от конкретного пользователя. Конфигурация системной части расположена в файлах:

- /etc/crontab
- /etc/cron.d/*
- /etc/cron.daily/* -- задания, которые исполняются раз в день (00:00)
- /etc/cron.hourly/* -- задания, которые исполняются раз в час (*:00)
- /etc/cron.monthly/* -- задания, которые исполняются раз в месяц (01 00:00)
- /etc/cron.weekly/* -- задания, которые исполняются раз в неделю (понедельник 00:00)

Первые 2 типа имеют формат crontab(5), которые используются для задачи конкретного времени и интервала, остальные просто исполняемые файлы, запускаемые как описано:
- hourly раз в час
- daily раз в день
- weekly раз в неделю
- monthly раз в месяц

	Параметр
Название	**Системный crontab**
Описание	

Значение по умолчанию: никаких изменений не должно быть для инсталлированых пакетов

Рекомендуемое значение: значение по умолчанию

Область действия: вся система.

Подробнее: Если файл изменился, то необходимо сообщить администратору. Права на запись в файлы и каталоги должны быть только у суперпользователя.

	Параметр
Название	**crontab для пользователей**
Описание	

Значение по умолчанию: нет.

Рекомендуемое значение: в зависимости от политики сервера

Область действия: вся система.

Подробнее: для пользователя crontab устанавливаются в каталоге /var/spool/cron/*:

```
# ls -l /var/spool/cron
total 8
-rw-------. 1 user user 1531 Aug 9 20:25 user
-rw-------. 1 root root 3154 Aug 17 19:15 root
```

Файлы в нём в формате crontab(5). Предлагается показать их содержание администратору для определения их валидности. Права на запись и чтение этих файлов должны принадлежать только владельцу.

	Группа
Название	**DNS**
Описание	

DNS - Domain Name System, Система Доменных Имён - распределённая база данных, используемая для “резолвинга” доменных имён в ip-адреса и обратно, а так же другой информации. Защита и поддежка DNS имеет большое значения для защиты как сервера, так и всей вычислительной системы. DNS делится на две части -- сервер, который обслуживает запросы от клиентов, и клиента (resolver), который представляет собой прикладную библиотеку, которая формирует запросы в DNS, посылает их, принимает ответы, декодирует их и возвращает приложению, например:

```
# host google-public-dns-a.google.com
google-public-dns-a.google.com has address 8.8.8.8
google-public-dns-a.google.com has IPv6 address 2001:4860:4860::8888
```

В данном случае команда host запрашивает информацию об ip-адресе хоста google-public-dns-a.google.com, и возвращает ответ - 2 адреса, ip4 и ip6.

Name Service Switch

Данная подсистема связана с локальным резолвером напрямую, она говорит ему, какие источники применять для получения данных. Например, данные на пользователей (passwd) могут читаться из файла (/etc/passwd), из NIS базы данных, и из NIS+ базы данных. Основной файл конфигурации /etc/nsswitch.conf, содержит key-value конфигурацию:

```
passwd: files nisplus
shadow: files nisplus
group: files nisplus
hosts: files mdns4_minimal [NOTFOUND=return] dns myhostname
```

Данная конфигурация говорит, что для получения информации о пользователе (passwd и shadow) и его группе (group) сначала производтя запрос к локальным файлам (/etc/passwd, etc/shadow и /etc/group), и если не нашли ничего в них то к специализированной базе данных NIS+. Если мы хотим получить информацию о имени хоста, то сначала мы обращаемся к локальному файлу /etc/hosts, затем пытаемся использовать Multicas DNS. В нашем случае указано, что если даже ничего не найдено, не пытаться использовать дальнейшие опции (NOTFOUND=return). А далее расположены опции использовать стандарный DNS, и в конце внутренний резолвер gnu libc. Подробнее можно посмотреть на документацию nsswitch.conf(5).

	Параметр	
	Название	**Конфигурационный файл резолвера имеет неверный формат**
	Описание	

Значение по умолчанию: зависит от дистрибутива, минимально должны присутствовать определения nameserever и search.

Рекомендуемое значение: минимум namserver и search для /etc/resolver.conf, 127.0.0.1 для /etc/hosts.

Область действия: вся система.

Как понять: обязательно проверить порядок применения методов доступа к DNS:

```
# grep "^hosts:" /etc/nsswitch.conf
hosts: files mdns4_minimal dns myhostname
```

Администратор должен убедиться, что конфигурация неизменна.
Так как в опциях присутствует опция files, то необходимо удостовериться, что файл /etc/hosts не был изменён. Затем необходимо убедиться, что файл /etc/resolver.conf не был изменён (опция dns присутствует в nsswitch конфигурации hosts).

Подробнее: если злоумышленник сумеет подменить файлы для локального резолвера, он сможет заставить систему использовать свои сервисы вместо правильных. Файл конфигурации /etc/nsswitch.conf определяет, в каком порядке будут использованы сервисы для получения информации из DNS (пример приведён выше), /etc/hosts используется для локальной замены DNS, в нём можно указать имена и адреса своих собственных серверов:

```
127.0.0.1 localhost localhost.localdomain
::1 localhost localhost.localdomain

192.168.0.9 host.test.net ns
192.168.0.10 dev.test.net dev
192.168.0.32 nas.test.net nas
```

Файл /etc/resolver.conf конфигурирует локальный резолвер для доступа к DNS, минимальный рабочий пример:

```
search test.net.
nameserver 192.168.0.10
```

Опция nameserver описывает адрес сервера, который предоставляет сервис DNS (может быть несколько), и search -- список доменов в которых надо искать неквалифицированное имя хоста (неквалифицированное -- которое не имеет в себе точек), например если я задам имя хоста dev, то резолвер сконструирует полное имя dev.test.net и попробует найти адрес для него. В search можно указывать несколько доменов, и резолвер будет искать в том порядке, в каком домены указаны.

Группа	
Название	**Email**
Описание	

Один из широкораспространённых сервисов, который может быть использован для компрометации сервера. Рекомендуется использовать в системе только один (выделенный) сервер для приёма, обработки и отправки почты, на остальный серверах в системе использовать натройку “умный хаб”, и всю почту (кроме локальной) направлять на обработку на него, и уже там контролировать её обработку и передачу.

Параметр	
Название	**Файл /etc/aliases**
Описание	

Значение по умолчанию: зависит от дистрибутива, но обычно все служебные адреса ссылаются на root (т. е. вся почта идёт на служебный адрес root).

Рекомендуемое значение: дописать правило, чтобы почта на служебный адрес root перенаправлялась на личный адрес администратора или администраторов, чтобы случайно не упустить важное письмо.

Область действия: вся система.

Как понять: проверить файл /etc/aliases на корректность:
● алиасы содержат только разрешённых пользователей;
● формат “| command” должен использоваться с осторожностью, с его помощью, если он настроен неправильно, легко быть подверженным атаке “отказ в обслуживании”. Внимательно проверить сами команды, что они исполнимые файлы, что не имеют установленным set-uid бит.
● по возможности не использовать :include:file формат, вместо него использовать специализированное программное обеспечение для обработки списков рассылки.

Подробнее: конфигурационный файл /etc/aliases имеет формат общий для всех MTA:

local-name: alias

где local-name -- локальное имя (без @ и доменной части), а alias может быть обычным почтовым адресом (например root или postmaster@test.net), файлом (/path/to/file), куда будут записываться полученные письма, программой (|/path/to/program), которая будет получать на стандартный вход всё письмо и может его обрабатывать. По возможности не использовать последнюю опцию, вместо этого сохранять почтовые сообщения в файл и по крону обрабатывать их.

	Параметр
Название	**Файл $HOME/.forward**
Описание	

Значение по умолчанию: файл отсутствует

Рекомендуемое значение: файл отсутствует. Если он существует, он должен быть доступен для записи только владельцу.

Область действия: вся система.

Подробнее: данный файл служит для манипуляцией персональной почтой пользователя, там могут быть значения:
● \user -- сохранить письмо в почтовый ящик пользователя user без дальнейшей обработки
● address -- переслать письмо на адрес address, он может быть как квалифицированным (с доменом: user@test.net), так и локальным (user)
● |/path/to/program -- запустить программу и обработать письмо получаемое из stdin потока
Последнее наиболее опасно, так как может быть запущена любая программа от имени пользователя. Рекомендуется все манипуляции с пользовательской почтой производить централизованно.

	Параметр
Название	**Конфигурируемые пользователем LDA (procmail)**
Описание	

Значение по умолчанию: зависит от дистрибутива, sendmail обычно использует procmail в качестве LDA.

Рекомендуемое значение: запретить пользовательские настройки procmail, использовать их централизованно. Запретить .procmailrc в пользовательских каталогах, запретить его создание и редактирование.

Область действия: вся система.

Подробнее: procmail достаточно сложная программа. и неопытный пользователь может неверно сконфигурировать её, в результате чего может как потерять почту, так и отправить её на неверный адрес, что чревато раскрытием секретной информации. Злоумышленник может настроить procmail так, что при получении специфического письма будет совершено какое-либо действие от имени пользователя. Рекомендуется запретить пользователю манипуляции с конфигурацией любого LDA (не только procmail). Для уверенности предлагается создать файл .procmailrc в домашнем каталоге пользователя, поменять его владельца и группу на root.root, запретить доступ на запись и сменить аттрибуты файла на immutable (неизменяемость файла).

Группа	
Название	**Сервис syslog**
Описание	

Используется для принятия информации от других сервисов об их работе, обработке её и сохранении локально или на удалённом сервере. Каталог /var/log -- по умолчанию здесь хранятся все лог-файлы системы.

Параметр	
Название	**Любой пользователь может читать log-файлы**
Описание	

Значение по умолчанию: зависит от системы

Рекомендуемое значение: запись в файлы только суперпользователю, чтение только суперпользователю либо административной группе. Запретить остальным чтение. Внимание: отдельные файлы должны быть доступны всем на чтение, иначе некоторые системные команды перестанут работать, например /var/log/lastlog, который используется командой lastlog, и /var/log/wtmp, который используется командами last, w, who, last.
В минимальной конфигурации только следующие файлы должны иметь отдельные атрибуты, владелец root, группа utmp:

```
# ls -l /var/log/{lastlog,wtmp,btmp}
-rw-rw---- 1 root utmp 0 Oct 1 06:25 /var/log/btmp
-rw-rw-r-- 1 root utmp 292584 Oct 13 20:05 /var/log/lastlog
-rw-rw-r-- 1 root utmp 10752 Oct 13 20:05 /var/log/wtmp
```

● lastlog -- список последних входов пользователей, чтобы все могли воспользоваться данной командой данный файл должен быть доступен на чтение:

```
# lastlog | head -3
Username Port From Latest
root pts/3 Sun Aug 18 20:45:02 +0300 2013
bin **Never logged in**
```

● wtmp -- файл для записи ошибочных заходов на хост, можно рекомендовать запрет на его чтение “всем”, и оставить группе (команда lastb):

```
# lastb | head -3
root ssh:notty 192.126.120.35 Tue Oct 14 20:15 - 20:15 (00:00)
root ssh:notty 192.126.120.35 Tue Oct 14 20:15 - 20:15 (00:00)
greg ssh:notty 190.157.84.130 Tue Oct 14 17:57 - 17:57 (00:00)
```

● btmp -- файл для записи успешных попыток входа на хост

```
# last | head -3
user pts/0 192.168.0.9 Tue Oct 14 20:17 still logged in
user pts/7 192.168.0.9 Tue Oct 14 18:18 - 20:17 (01:59)
user pts/6 212.28.200.143 Tue Oct 14 15:31 still logged in
```

Область действия: вся система.

Подробнее: если любой сможет читать log-файлы, то он сможет и исследовать систему - производить манипуляции и смотреть отклик. Настоятельно рекомендуется настроить как syslog-демон, так и сервис для архивации log-файлов (например logrotate), на создание их сразу с определёнными привилегиями. Например, для rsyslog (/etc/rsyslog.conf):

```
# Set the default permissions for all log files.
#
$FileOwner root
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0750
$Umask 0022
```

и logrotate (/etc/logrotate.conf):

```
/var/log/btmp {
missingok
monthly
create 0660 root utmp
rotate 1
}
```

В данных отрывках приведены примеры как надо настраивать сервисы. Если необходим более высокий уровень секретности, то рекомендуется настроить трансляцию лог-файлов на выделенный log-сервер, возможно в криптографически защищённом виде (зашифрованными и подписанными), в таком случае злоумышленник не сможет подделать или скрыть свои следы в системе.

	Параметр

Название	**Криптографическая защита log-файлов в rsyslog**

Описание

Значение по умолчанию: зависит от дистрибутива и конкретной системы, обычно не используется.

Рекомендуемое значение: в зависимости от политики и настроек системы.

Область действия: вся система.

Подробнее: в последних версиях syslog-пакетов имеется возможность для зашифровывания данных прямо в файлах, но данная возможность не выглядит полезной, так как для зашифровывания необходим ключ, который должен храниться в системе. Если ключ хранится в системе, то злоумышленник, который получил привилегии суперпользователя в системе, имеет возможности найти ключ и расшифровать log-файлы. Более полезной выглядит возможность переправлять их криптографически защищённым способом на центральный хост (криптографически -- аутетифицированным, т. е. защищённым от подделки; зашифрованным -- защищённым от перехвата). Для использования данной возможности в системе должен быть инсталлирован OpenSSL CA (certificate authority), а так же правильно созданы ключи и сертификаты.

Группа

Название	**Файловая система**

Параметр

Название	**setuid файлы**

Описание

Значение по умолчанию: зависит от дистрибутива и конкретной системы.

Рекомендуемое значение: в системе не должно присутствовать неконтролируемых setuid/setgid файлов.

Область действия: вся система.

Подробнее: в unix для выполнения некоторых операций необходимо повышать уровень привилегий пользователя до root, но нежелательно давать ему пароль суперпользователя, для этого введено понятия setuid/setgid для файла, когда при выполнении данного файла права процесса повышаются до прав владельца файла. Хороший пример -- команда ping, создать сокет для icmp операций может только суперпользователь, поэтому на большинстве систем эта программа имеет установленный s-бит:

```
# ls -l /bin/ping
-rwsr-xr-x 1 root root 31104 Apr 12 2011 /bin/ping
```

Параметр

Название	**Разделяемые библиотеки**

Описание

Значение по умолчанию: зависит от дистрибутива и конкретной системы, но обычно только пользователь root имеет право записи в них.

Рекомендуемое значение: только суперпользователь имеет право записи в данный файлы и каталоги. Все остальные случаи должны быть подтверждены администратором.

Область действия: вся система.

Подробнее: если простой пользователь сможет создать свою разделяемую библиотеку в системном каталоге или перезаписать существующую, то он сможет выполнить любую команду в системе и скомпрометировать её.

	Параметр
Название	**Загрузчик**
Описание	

Значение по умолчанию: зависит от дистрибутива и конкретной системы, но обычно только пользователь root имеет право записи в них.

Рекомендуемое значение: только суперпользователь имеет право записи в данный файлы и каталоги. Все остальные случаи должны быть подтверждены администратором.

Область действия: вся система.

Подробнее: если имеется возможность записи в загрузчик, то злоумышленник может скомпрометировать систему заставив загрузить модифицированное ядро.

	Параметр
Название	**Инициализационные скрипты**
Описание	

Значение по умолчанию: зависит от дистрибутива и конкретной системы, но обычно только пользователь root имеет право записи в них.

Рекомендуемое значение: только суперпользователь имеет право записи в данный файлы и каталоги. Все остальные случаи должны быть подтверждены администратором.

Область действия: вся система.

Подробнее: если имеется возможность записи в инициализационные скрипты, то злоумышленник может скомпрометировать систему заставив загрузить свои сервисы при инициализации.

	Параметр
Название	**Пользовательские каталоги и файлы**
Описание	

Значение по умолчанию: зависит от дистрибутива

Рекомендуемое значение: пользовательский каталог должен быть доступен для записи только пользователю, а так же пользовательские файлы инициализации (.bashrc, .login etc, а так же .ssh):

```
# grep -f /etc/shells /etc/passwd | grep -v 'nologin$' | cut -d: -f1,6,7
root:/root:/bin/bash
user:/home/user:/bin/zsh
postgres:/var/lib/pgsql:/bin/bash
sybase:/opt/sybase:/bin/bash
mysql:/var/lib/mysql:/bin/bash
gitosis:/var/lib/gitosis:/bin/sh
gitolite3:/var/lib/gitolite3:/bin/sh
```

Список пользователей, которые имеют командной оболочкой интерактивный шелл. Показаны имя пользователя, его домашний каталог и командная оболочка. Для каждого необходимо проверить что владелец домашнего каталога сам пользователь и только он имеет права на запись:

```
# sudo ls -ld /var/lib/gitosis
drwxr-xr-x. 2 gitosis gitosis 4096 Aug 3 2013 /var/lib/gitosis
```

Необходимо также убедиться в правильности прав доступа к инициализационным файлам (в зависимости от командной оболочки это может быть сложно), для bash это .bash_profile, .bashrc, .bash_logout и .bash_history. Для zsh -- .zshenv, .zprofile, .zshrc .zlogin и .zlogout.

Так же необходимо убедиться в корректности прав доступа к каталогу .ssh и содержащимся в нём файлам:
● доступ к каталогу .ssh должен иметь только владелец:

```
# ll -d .ssh
drwx------. 2 user user 4096 Sep 21 12:54 .ssh/
```

● файлы authorized_keys и приватные половины ключей должны быть доступны только владельцу:

```
-rw-------. 1 user user 14310 Jul 28 20:20 authorized_keys
-rw-------. 1 user user 987 Apr 3 2013 identity
-rw-------. 1 user user 751 Apr 3 2013 id_dsa
-rw-------. 1 user user 314 May 3 20:22 id_ecdsa
-rw-------. 1 user user 1766 Apr 3 2013 id_rsa
```

● все остальные файлы могут иметь права на чтение и для других ползователей:

```
-rw-r--r--. 1 user user 1025 Sep 6 01:35 config
-rw-r--r--. 1 user user 652 Apr 3 2013 identity.pub
-rw-r--r--. 1 user user 612 Apr 3 2013 id_dsa.pub
-rw-r--r--. 1 user user 190 May 3 20:22 id_ecdsa.pub
-rw-r--r--. 1 user user 404 Apr 3 2013 id_rsa.pub
-rw-r--r--. 1 user user 7672 Sep 6 01:35 known_hosts
```

Область действия: вся система.

Подробнее: если имеется возможность записи в инициализационные скрипты, то злоумышленник может скомпрометировать систему заставив при входе в систему выполнить действия от имени пользователя. Если скомпрометировать систему ssh можно заставить пользователя зайти на свой собственный хост, либо украсть ssh-ключи и получить доступ к удалённым хостам. Если скомпрометировать файл .forward, то можно получить доступ к почте пользователя и возможность выполнять команды от его имени.

Группа	
Название	**Общие параметры**

Параметр	
Название	**Использование нестойкой криптосхемы для хранения паролей**
Описание	

Значение по умолчанию: зависит от дистрибутива.

Рекомендуемое значение: первое поле -- имя пользователя, второе поле -- пароль. Второе поле не должно быть пустым (что означает разрешение входа в систему без пароля). Рекомендуемый тип хеширования - SHA512.

Область действия: вся система.

Подробнее: для аутентификации в системе может быть использовано несколько методов, задаваемых администратором. Самая простейшая и широко используемая схема -- вход по паролю, который хранится локально в файле /etc/shadow. Необходимо проконтролировать, что выбрана стойкая схема хранения пароля (ENCRYPT_METHOD), чтобы пароли соответствовали выбранной схеме (type), и чтобы пароль присутствовал (в файле /etc/shadow).

	Параметр
Название	**Большое время жизни пароля**
Описание	

Значение по умолчанию: зависит от системы, но обычно указанные в примере (не заставлять менять пароль).

Рекомендуемое значение: время жизни пароля 3-4 месяца (PASS_MAX_DAYS 90-120), время предупреждения о смене пароля 7 дней, и время жизни после смены пароля минимум 7 дней.

Область действия: вся система.

Подробнее: для повышения защищенности системы рекомендуется установить практику регулярной смены паролей у пользователей, чтобы случайной утечкой не смог воспользоваться злоумышленник. Для отдельного пользователя значения можно установить командой chage.

	Параметр
Название	**Не единственный суперпользователь в системе**
Описание	

Значение по умолчанию: один "root"-пользователь.

Рекомендуемое значение: один "root"-пользователь.

Область действия: вся система.

Подробнее: В общем случае UNIX/Linux не запрещают существование в системе нескольких пользователей с привилегиями суперпользователя. Тем не менее, такой подход не является рекомендуемым, т. к. появляется возможность сокрытия суперпользователя под другим именем, а множество команд в системе опираются на то, что суперпользователь может быть в системе только один, и его имя root. Также злоумышленник может завести для себя дополнительного привилегированного пользователя.

	Параметр
Название	**Выполнение команды sudo без запроса пароля**
Описание	

Значение по умолчанию: зависит от системы.

Рекомендуемое значение: запретить, удалив стоку NOPASSWD:.

Область действия: вся система

Подробнее: стандартный путь передачи отдельным пользователям привилегии суперпользователя без сообщения им его пароля -- команда sudo. Если пользователю разрешено использовать команду sudo, он может выполнить любую команду, требующую привилегий суперпользователя: # sudo dangerous-command
Несмотря на то, что пользователю можно разрешить выполнять команды без ввода пароля, настоятельно рекомендуется отказаться от такой практики, т. к. злоумышленник, получив возможность выполнять команды от лица пользователя, но не знающий его пароля, сможет воспользоваться командой sudo.

	Параметр
Название	**Небезопасный secure_path в /etc/sudoers**
Описание	

Значение по умолчанию: зависит от системы

Рекомендуемое значение: /sbin:/bin:/usr/sbin:/usr/bin, возможно добавить /usr/local/bin и /usr/local/sbin.

Область действия: вся система

Подробнее: данная опция в файле /etc/sudoers показывает значение переменной окружения PATH, которое станет актуальным после повышения привилегий. Если, например, в переменной будет находиться элемент /tmp, то создав специальную программу и поместив её каталог /tmp, можно будет обманом вынудить её выполнить привилегированного пользователя.

	Параметр
Название	**Sudo и небезопасный env_keep в /etc/sudoers**
Описание	

Значение по умолчанию: зависит от системы

Рекомендуемое значение: показанное выше безопасно для использования

Область действия: вся система

Подробнее: многие переменные окружения, облегчающие жизнь пользователя (например, LANG или LC_ALL), логично использовать их и в окружении, предоставляемом командой sudo. Однако существуют небезопасные переменные, которые не рекомендуются к экспорту. К таким переменным, например, относятся LD_PRELOAD_PATH и LD_RUN_PATH, в которых описаны пути для поиска разделяемых библиотеки, а также переменная PATH.

	Параметр
Название	**Отсутствие регистрация попыток входа в систему**
Описание	

Значение по умолчанию: есть

Рекомендуемое значение: убедиться, что файлы существуют и не являются ссылками на /dev/null. Также рекомендованы указанные привилегии доступа ка файлам.

Подробнее: в случае удачного входа в систему событие регистрируется в файле /var/log/wtmp, а неудачное в /var/log/btmp. Посмотреть события можно командами last (удачные) и lastb (неудачные):

```
# last
user pts/6 arto.test.net Tue Jul 8 17:43 still logged in
user pts/0 arto.test.net Tue Jul 8 12:37 still logged in
reboot system boot 3.15.3-200.fc20. Tue Jul 8 15:34 still running
```

Вывод показывает, что два пользователя вошли в систему и остаются в системе, а также одну перегрузку системы.

```
# lastb
root ssh:notty 113.171.10.23 Tue Jul 8 22:55 - 22:55 (00:00)
db2inst1 ssh:notty 113.171.10.23 Tue Jul 8 22:55 - 22:55 (00:00)
db2inst1 ssh:notty 113.171.10.23 Tue Jul 8 22:55 - 22:55 (00:00)
db2inst1 ssh:notty 113.171.10.23 Tue Jul 8 22:55 - 22:55 (00:00)
db2inst1 ssh:notty 113.171.10.23 Tue Jul 8 22:55 - 22:55 (00:00)
```

Вывод показывает пять неудачных попыток входа с адреса 113.171.10.23 и имена, под которыми пытались войти в систему. Рекомендуется для расследования инцидентов и статистики доступа в систему. Также рекомендуется сохранять старые файлы.

	Параметр
Название	**Включенный режим маршрутизации**
Описание	

Значение по умолчанию: зависит от системы, обычно запрещён.

Рекомендуемое значение: если система не маршрутизатор, то запретить.

Подробнее: если данная опция включена, то злоумышленник может попробовать использовать сервер в качестве маршрутизатора для проникновения во внутреннюю сеть предприятия. Рекомендуется запретить данную возможность немедленно: # sysctl -w net.ipv4.ip_forward=0
и постоянно, вставив строку net.ipv4.ip_forward=0 в файл /etc/sysctl.conf.
В последнем случае загрузить весь файл можно командой sysctl --load.

	Группа
Название	**SSH**

	Параметр
Название	**Небезопасные права доступа**
Описание	

Значение по умолчанию:
- sshd_config -- конфигурация sshd, доступ только для root,
- ssh_config -- конфигурация ssh, доступ для всех,
- ssh_host_*key -- приватные ключи, доступ только для root,
- ssh_host_*key.pub -- публичные ключи, доступ для всех.

Рекомендуемое значение: по умолчанию

Область действия: вся система

Подробнее: для установления соединения ssh использует схему Диффи-Хеллмана, для чего при инсталляции создаёт пары ключей (в данном случае типы ключей rsa, dsa и ecdsa). Пара ключей состоит из двух компонентов -- приватный ключ (который необходимо держать в секрете) и публичный ключ (который доступен всем). Конфигурацию ssh желательно тоже держать в секрете, чтобы усложнить потенциальному злоумышленнику работу по компрометации системы.

	Параметр
Название	**Запрещение X11Forwarding**
Описание	

Значение по умолчанию: запрещено.

Рекомендуемое значение: запретить.

Область действия: вся система

Подробнее: OpenSSH может перенаправлять X11 траффик от клиента до локального сервера, для этого он может открывать дополнительные порты, и может быт подвержен атаке. Рекомендуется, если нет необходимости в работе с X11, то запретить данную опцию.

	Параметр
Название	**Запрещение пользовательских .rhosts/.shosts файлов**
Описание	

Значение по умолчанию: разрешено.

Рекомендуемое значение: запретить.

Область действия: вся система

Подробнее: OpenSSH поддерживает rhosts-based аутентификацию, которая позволяет вести список доверенных (trusted) хостов, для которых возможен вход без пароля. Список таких хостов может храниться как в /etc/hosts.equiv и /etc/ssh/shosts.equiv, так и в ~/.shosts и ~/.rhosts. Атакующий, узнав данный список, может попытаться подменить dns-адрес для своего хоста и атаковать систему. Если необходимо использовать данный метод для старых сервисов, то надежнее использовать первые два файла, запретив к ним доступ всех, кроме root'а. Надёжнее совсем запретить доступ по rhosts, и перейти на key-based аутентификацию.

	Параметр
Название	**Проверка ip/dns-адреса клиента**
Описание	

Значение по умолчанию: разрешено.

Рекомендуемое значение: зависит от политики сервера.

Область действия: вся система

Подробнее: разрешив данную опцию сервер будет производить дополнительную проверку адреса, с которого происходит запрос соединения: сначала попытается определить dns адрес из ip адреса, а затем из dns адреса определить ip адрес, а затем сравнить их. В случае, если они не совпадают, то будет сгенерировано предупреждение в log-файле о данном инциденте. Если используется rhosts-based аутентификация (см. предидущую главу) то данная опция обязательна. в остальных случаях она в основном бесполезна, только для последующих разборов инцидентов. К отрицательным сторонам данного механизма относится повышенная нагрузка на систему при “обратном резолвинге” ip-адреса (когда для ip адреса пытаются найти соответствующий dns-адрес), часто администраторы не заводят для своих хостов обратные зоны.

	Параметр
Название	**Запретить беспарольный доступ в систему**
Описание	

Значение по умолчанию: запрещено.

Рекомендуемое значение: запретить.

Область действия: вся система

Подробнее: данная опция разрешает вход без пароля, если разрешена аутентификация по паролю. Настоятельно рекомендуется запретить данную возможность.

	Параметр
Название	**Использование HashKnownHosts**
Описание	

Значение по умолчанию: no.

Рекомендуемое значение: зависит от политики системы.

Область действия: ssh-клиент и sshd-сервер

Подробнее: файл ~/.ssh/known_hosts содержие в себе список имён хостов и соотвтствующих им публичных ключей (когда мы коннектимся к серверу, мы можем сравить локальный ключ из этого файла и ключ, полученный от сервера, и если они не идентичны, то вполне вероятно, что мы либо коннектимся не туда, либо мы под mitm-атакой, либо на сервере сменились ключи sshd-сервера, во всяком случае необходимо проконсультироваться по независимому каналу с администратором сервера). Сам файл выглядит примерно так:

```
# head -2 .ssh/known_hosts
malin,192.168.0.1 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABA...
192.168.0.106 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABA...
```

Данная команда разрешает “хешировать” имена хостов (первое поле записи), чтобы при случайной потере данного файла злоумышленник не смог узнать, куда вы ходили.

	Параметр
Название	**Отсутствие ограничений на доступ к серверу**
Описание	

Значение по умолчанию: нет

Рекомендуемое значение: ограничить каким-либо способом доступ в систему.

Область действия: вся система

Подробнее: ssh является основной целью для атаки "перебор по словарю", когда атакующий пытается угадать имя пользователя в системе и подобрать его пароль. Для усложнения его задачи рекомендуется ограничить количество пользователей, которые могут входить в систему через ssh. В sshd_config можно указать опции:
● AllowUsers -- разрешить только указанным пользователям,
● AllowGroups -- разрешить только указанным группам,
● DenyUsers -- запретить указанным пользователям,
● DenyGroups -- запретить указанным группам.
Таким образом можно значительно уменьшить возможность подбора паролей. Для AllowUsers/DenyUsers можно указывать шаблон вида user@host, где user может содержать символы шаблонов ‘*’ -- набор символов любой длины и ‘?’ -- ровно один символ. Те же самые правила можно применять к host -- имя удалённого хоста или его ip-адрес, например: user*@192.168.0.? совпадает с любым локальным пользователем, имя которого начинается с user, и ip-адрес лыбой из набора 192.168.0.{1,9}. Использование имени хоста может быть сопряжено с опастностью его подмены.

	Параметр
Название	**Доступ для root**
Описание	

Значение по умолчанию: PermitRootLogin yes

Рекомендуемое значение: PermitRootLogin no

Область действия: вся система

Подробнее: пользователь root является наиболее частой целью атаки “перебор по словарю”, поэтому рекомендуется запретить ему доступ в систему по ssh, а для выполнения привилегированных команд использовать sudo или su. Если же необходим прямой доступ для root, то предлагается использовать доступ по ключам и указать опцию PermitRootLogin forced-commands-only.

	Параметр
Название	**Работа сервера на порту по умолчанию**
Описание	

Значение по умолчанию: 22

Рекомендуемое значение: зависит от политики сервера.

Область действия: ssh

Подробнее: Одним из рекомендуемых действий по противодействиям атаки “перебор по словарю” является назначение другого порта для ssh-сервера, например 22022. Для этого надо записать в конфигурационный файл строку Port 22022, а для установления соединения использовать команду # ssh -p 22022 server.address

	Параметр
Название	**Включена аутентификация по ключу**
Описание	

Значение по умолчанию: PasswordAuthentication yes, RSAAuthentication yes

Рекомендуемое значение: зависит от политики сервера

Область действия: ssh

Подробнее: так как пароль относительно легко подобрать или скомпрометировать, предлагается рассмотреть возможность запрета аутентификации по паролю. Рекомендуемым способом является аутентификация по ключу. Рекомендуемая конфигурация, таким образом, будет следующей:

PasswordAuthentication no
RSAAuthentication yes

В этом случае пользователи должны создать собственные ключевые пары и прислать публичные ключи администратору.

	Параметр
Название	**Ограничение попыток неуспешного доступа**
Описание	

Значение по умолчанию: MaxAuthTries обычно 6

Рекомендуемое значение: уменьшить до 3-4, в зависимости от политики сервера.

Область действия: SSH

Подробнее: данный параметр задает sshd, сколько раз пользователь может неуспешно ввести пароль, после чего в систему учёта будет направлено сообщение он инциденте. Данная опция помогает своевременно реагировать на атаки “перебор по словарю” - в более короткий срок можно принять меры против атакующего (например, заблокировать его IP адрес).

	Параметр
Название	**DNS SSHFP запись**
Описание	

Значение по умолчанию: нет

Рекомендуемое значение: завести данную запись в DNS.

Область действия: вся система.

Подробнее: против ssh существует тип атаки -- подстановка ложного узла, когда вместо целевого узла соединение происходит с “поддельным”. При установлении соединения по протоколу Диффи-Хеллмана сервер посылает клиенту свой идентификатор -- ключ, по которому клиент может опознать сервер (обычно клиент хранит ассоциацию имя сервера -- ключ). Указанная настройка решает проблему первого подключения к серверу, когда отпечаток сервера должен в теории передаваться по доверенному каналу. Одно из практичных решений данной проблемы -- поместить отпечаток ключа в запись DNS SSHFP, ассоциированную с данным узлом. Заведение данных записей осуществляется следующим образом:

ssh-keygen -r host.name
host.name IN SSHFP 1 1 ee67ba4280cd8ad1c92d6da87a452a1efc691aa5
host.name IN SSHFP 1 2 129241cebf3bb68965941f8534ad14eeca7f57f408b206678352eec149526442
host.name IN SSHFP 2 1 cc28465ac6b0a844b8b3a130720c620d997bbbee
host.name IN SSHFP 2 2 1c08918a3ce8a9c97c3084ae287df390f82c0133f09d8640e59b7b7d5865bb56
host.name IN SSHFP 3 1 84c2e1ffc29f3c2f755ecf176424a6e8ad976842
host.name IN SSHFP 3 2 84d3c21e5da0129beb42c27b0c1eb5873d820495a3cb06422b97708f8dda881b

Данная команда сгенерирует набор SSHFP записей для DNS, которые необходимо поместить в соответствующую зону. Для проверки наличия данной записи для клиента надо поместить директиву VerifyHostKeyDNS yes в конфигурационный файл клиента, либо напрямую использовать команду следующего вида # ssh -o VerifyHostKeyDNS=yes test.net

Описание: RFC 4255: Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints.

	Параметр	
	Название	**Отсутствие защиты от перебора паролей по сети fail2ban**
	Описание	

Значение по умолчанию: зависит от системы, обычно нет

Рекомендуемое значение: инсталлировать fail2ban и настроить

Подробнее: данная программа отслеживает логи программ и реагирует на события, описанные в конфигурационных файлах. События -- ошибки доступа (для sshd -- неудачные попытки входа, для httpd -- неудачные попытки аутентификации, попытки сканирования). Реакция -- блокирование доступа по протоколу и порту или блокирование удалённого хоста по адресу через iptables. Программа ведёт внутреннюю базу заблокированных узлов, а после определённого времени освобождают их.
Последняя версия 0.9.0. Конфигурационные файлы находятся в каталоге /etc/fail2ban, основные для конфигурации fail2ban.conf, jail.conf и jali.local все имеют формат ini-конфигурации):
● fail2ban.conf общие опции для всей системы:
○ socket - сокет для взаимодействия с демоном;
○ loglevel, logtarget - куда посылать сообщения о работе fail2ban, и какой уровень сообщений;
○ dbfile - где данные должны храниться (нигде, в памяти, в SQLite базе);
○ dbpurge - сколько времени информация о бане должна храниться в базе
● jail.conf описания сервисов, за которыми следим, разделы INCLUDES (список файлов, которые будут включены в конфигурацию, обычно пути до лог-файлов специфические для конкретного дистрибутива), DEFAULT (значения по умолчанию для сервисов (jails), которые потом можно заменить в конкретном блоке jail, и, в конце, сами блоки сервисов (в квадратных скобках -- имя сервиса):
○ port - список портов, котрые надо блокировать в случае наступления события;
○ logpath - путь до лог-файла для данного сервиса, который надо сканировать для определения событий;
○ maxretry - сколько событий должно появиться в лог-файле для “забанивания” данного хоста (3);
○ findtime - в течении какого времени (секунды) maxretry событий должно наступить (600);
○ ignoreip - список сетей/хостов, которые не должны учитываться при наступлении события (рекомендуются локальная сеть либо сеть/хосты для администраторов, чтобы случайно не закрыть себе доступ);
○ enabled - разрешить/запретить данный сервис (рекомендуется false в DEFAULT и разрешать индивидуально);
○ filter - имя фильтра для поиска событий в лог-файле (%(__name__)s - имя сервиса). Само определения фильтра лежит в подкаталоге filter.d/name.conf, представляет собой список python-регулярных выражений, применяемых к строке лог-файла, и, если совпадает, то должно отдавать имя хоста, например:

^%(__prefix_line)s[iI](?:llegal|nvalid) user .* from <HOST>\s*$

1. %(__prefix_line)s - старндарный префикс из log-файла, например “Sep 1 05:58:06 dev sshd[4042]:”
2. [iI](?:llegal|nvalid) user .* from <HOST> - должно совпадать со строками “Illegal user name from host” и “Invalid user name from host”, и host должен попасть в <HOST> и дальнейшие манипуляции будут происходить с данным адресом. Желательно сконфигурировать программу, которая генерит данные в лог-файле, чтобы она не пыталась определять имя хоста из ip-адреса.

● usedns - как поступать, если в лог-файле встретится имя хоста, а не его ip-адрес:
○ yes - получить ip-адрес;
○ warn - получить ip-адрес, но предупредить (по умолчанию);
○ no - не использовать для бана .
● destmail - адрес, куда слать извещения о банах
● sender - что проставлять в поле “From:” письма
● jail.local - локальный конфиг, где можно конфигурировать отдельные сервисы (в основном конфиге указать, что по умолчанию ничего не загружается, и только тут указать, какие именно сервисы будут отслеживаться). Формат такой же, что и в jail.conf.

По умолчанию ничего не разрешено, надо разрешать индивидуально, пример jail.local:

[DEFAULT]

bantime = 3600
ignoreip = 127.0.0.1/8 192.168.0.0/16
destemail = root@localhost
action = %(action_mwl)s

[sshd]
enabled = true
maxretry = 3

По умолчанию время бана установлено в 1 час, игнорируются локальные хост и сеть, рапорт по блокировкам отправляются root’у, действие по умолчанию - забанить и отпрваить письмо с данными whois для данного ip и отрывками из лог-файла, относящемуся к данному хосту. Сервис sshd разрешён, после 3 попыток войти или просканировать блокируется ip.

	Параметр
Название	**Использование устаревшей версии протокола**
Описание	

Значение по умолчанию: зависит от системы, обычно 2

Рекомендуемое значение: 2

Область действия: вся система

Подробнее: ssh поддерживает два протокола работы: первый, устаревший и рассматриваемый сейчас как подверженный атакам, и второй - современный и более защищенный. Рекомендуется использовать только протокол версии 2, а первую версию использовать только в случае крайней необходимости (старые клиенты, которых невозможно заменить).

	Группа
Название	**Remote Access**

	Параметр
Название	**Использование устаревших сервисов (telnet, rsh, rcp, etc)**

Описание

Значение по умолчанию: нет

Рекомендуемое значение: не использовать данные сервисы. (tcp порты для этих сервисов 23 и 514)

Область действия: вся система.

Подробнее: устаревшие сервисы, которые успешно заменены ssh u scp, опасны тем, что передают всю информацию в назашифрованном виде (имена пользователей, пароли, данные). Если данные сервисы необходимы, то настоятельно рекомендуется использовать их через криптотуннели (ipsec, openvpn), а сами сервисы закрыть от доступа из сети с помощью iptables, оставив их открытыми только локально.

	Параметр
Название	**Политика доступа по tcp/udp/ip (порты/приложения): Постоянные приложения**
Описание	

Значение по умолчанию: зависит от системы/дистрибутива и политики сервера.

Рекомендуемое значение: разрешить только необходимые сервисы

Область действия: вся система

Подробнее: выполнив из под root'а команды: "# netstat -plna -t" и "# netstat -plna -u"
Первая команда показывает сервисы присоединённые к портам tcp, вторая к udp. Значения колонок:
1. протокол (udp, tcp etc);
2. запросов в очереди на подключение;
3. данных в очереди на отправку;
4. локальный адрес и порт (адрес на интерфейсе, список интерфейсов и их адресов можно посмотреть командой ifconfig);
5. если соединение установлено, то адрес удалённой стороны, если соединение не установлено, то строка 0.0.0.0:*;
6. состояние сокета (только для tcp; для udp, как протокола без состояния, не определено); для tcp интересно состояние LISTEN, когда сокет в состоянии ожидания принятия запроса на соединение;
7. PID и имя программы, владеющей этим сокетом.
Администратору необходимо проанализировать данный список и определить, какие программы необходимы, а какие нет. Если по имени программы невозможно определить, какой сервис она предоставляет, можно воспользоваться следующей командой:

```
# grep -E "\\b123/" /etc/services
ntp 123/tcp
ntp 123/udp # Network Time Protocol
```

На порту 123 по протоколам tcp и udp работает ntp -- протокол сетевого времени.

Затем администратор должен решить, какой доступ должен быть обеспечен для данного сервиса (например раздавать точное время только в локальной сети) и настроить с помощью iptables политику доступа. Подозрительными могут считаться случаи, когда открыт порт, но к нему не привязана никакая программа, либо программа привязана к порту, но он не находится в таблице iptables.

	Параметр
Название	**Политика доступа по tcp/udp/ip (порты/приложения): inetd приложения**
Описание	

Значение по умолчанию: не определено, зависит от дистрибутива.

Рекомендуемое значение: разрешить только необходимые.

Подробнее: как и в предыдущей секции, сложно автоматически определить политику сервера, лучше предоставить право решения администратору. Как определить, какие сервисы разрешены в конфигурационном файле inetd.conf:
grep -E “^[[:alnum:]]+” /etc/inetd.conf
покажет сервисы, которые обслуживает inetd. Формат:
finger stream tcp nowait/3/10 nobody /usr/libexec/fingerd fingerd -s
1. service-name -- имя сервиса, предоставляемого конкретным демоном. Оно должно соответствовать сервису, указанному в файле /etc/services.
2. socket-type -- stream, dgram, raw или seqpacket.
3. protocol -- tcp или udp
4. wait/nowait + опции -- описание, как работает вызываемая программа, через собственный сокет или через inetd.
5. имя пользователя, из под которого будет запущена программа.
6. путь до программы (если данный сервис предоставляется самой программой inetd, то internal).
7. аргументы, с которыми будет выполнена программа (имя программы -- тоже аргумент).

Для xinetd:

```
# perl -0777 -lne 's/#.*$//gm; s/\n+/\n/gsm;
print if (m#disable\s+=\s+no#sm)' /etc/xinetd.d/*
service echo
{
disable = no
id = echo-dgram
type = INTERNAL
wait = yes
socket_type = dgram
}
service echo
{
disable = no
id = echo-stream
type = INTERNAL
wait = no
socket_type = stream
}
```

Команда покажет разрешённые сервисы (в данном случае “echo”, для обоих протоколов, tcp и udp, выполняются оба самим мультиплексором xinetd).

	Параметр	
	Название	**Политика фильтрации iptables**
	Описание	

Значение по умолчанию: не определено, зависит от дистрибутива.

Рекомендуемое значение: разрешить только необходимые порты и протоколы.

Подробнее: для работы с сетью в linux используется система iptables, с помощью которой можно, в том числе, фильтровать трафик. В простейшем случае можно либо пропускать пакеты, либо отвергать их. Для безопасной работы в сети предлагается использовать схему “запрещено всё, что не разрешено”, как показано в примере. Т. е. в данном случае разрешены только порты 22, 25 и 80, и icmp пакеты.
В iptables есть несколько таблиц, через которые проходят пакеты, но нас будет интересовать таблица filter, остальные таблицы могут понадобиться в более сложных случаях, возможно они будут рассмотрены в других главах. Таблица filter содержит цепочки INPUT, OUTPUT и FORWARD через которые проходят соответственно “входящие”, “исходящие” и “передаваемые” пакеты (последний термин означает пакеты, которые приходят на сервер и передаются дальше, т.е. пакеты, у которых адрес источника и адрес назначения не совпадает ни с одним адресом на сетевых интерфейсах сервера). Рекомендуется оставить только протоколы и порты, которые необходимы в системе для ее штатной работы (в данном случае разрешен только доступ к ssh, почте и httpd серверу). Более подробно правила можно посмотреть следующей командой (мы будем рассматривать только таблицу filter):

```
# iptables-save -T filter
# Generated by iptables-save v1.4.19.1 on Tue Jul 8 22:09:51 2014
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp -m conntrack --ctstate NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m conntrack --ctstate NEW -m tcp --dport 80 -j ACCEPT
-A INPUT -p tcp -m conntrack --ctstate NEW -m tcp --dport 25 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
# Completed on Tue Jul 8 22:09:51 2014
```

Команды читаются системой сверху вниз, нас будет интересовать только таблица *filter (комментарии начинаются с символа “#”), в ней обрабатываются только входящие пакеты (цепочка INPUT). Первая строка (*filter) означает, что рассматривается таблица filter. Три последующих строки означают счётчики, и нас не интересуют. Пятая строка означает, что пакеты, которые были зарегистрированы (--ctstate RELATED,ESTABLISHED) в подсистеме iptables conntrack (-m conntrack), принимаются (-j ACCEPT) без обработки. Все icmp пакеты принимаются (строка 6), и пакеты с локального интерфейса lo (строка 7). TCP (-p tcp) пакеты на порты 22, 80 и 25 (--dport) принимаются (-j ACCEPT), обрабатываются как tcp (-m tcp) и регистрируются в conntrack (-m conntrack --ctstate NEW). Предпоследняя строчка говорит, что все пакеты, которые остались непринятыми и дошли до этого места отвергаются с icmp кодом “host prohibited”. Последняя команда означает конец списка команд для данной цепочки. Необходимо убедиться, что все цепочки, через которые входят пакеты в систему, оканчиваются правилом -j REJECT либо -j DROP (последняя цель означает что пакет будет просто уничтожен без отправления icmp пакета с ошибкой), либо изначально политика по умлочанию содержит правило DROP или REJECT (пример ниже). Администратору необходимо показать, какие порты открыты, и какие сетевые приложения запущены (смотри главы “Политика доступа по tcp/udp/ip” и “Мультиплексор xinetd/inetd”).

Расположение конфигурационных файлов:
Для старых RH-based дистрибутивов, на которых используется “чистый” iptables (без firewalld и shorewall) -- /etc/sysconfig/iptables и /etc/sysconfig/ip6tables, пример рекомендованной простейшей конфигурации:

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
-A INPUT -i lo -j ACCEPT
-A INPUT -m tcp -p tcp --dport 22 -j ACCEPT
-A OUTPUT -m tcp -p tcp --sport 22 -j ACCEPT
COMMIT
```

запрещено всё, кроме локального интерфейса (lo), входящих на ssh порт и исходящих из него пакетов. В дальнейшем можно добавлять в него разрешения для других сервисов. Загрузить правила из данного файла можно командой # iptables-restore < /etc/sysconfig/iptables, сохранить существующие командой # iptables-save > /etc/sysconfig/iptables

Для Debian-based дистрибутивов не существует единого места хранения правил для iptables, рекомендуется создать свою собственную систему: например, /etc/iptables.conf использовать для хранения правил, и создать скрипт /etc/network/if-pre-up.d/iptables:

```
#!/bin/sh
/sbin/iptables-restore < /etc/iptables.conf
```

который будет загружать правила при поднятии сети/интерфейсов.

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

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

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

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

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

Описание

Директория `/var/log/audit` используется для хранения логов аудита. Необходимо убедиться во время установки, что она располагается на отдельном разделе или логическом томе, либо перенести её позднее, используя LVM. Необходимо быть абсолютно уверенным, что её размер достаточен для хранения всех логов аудита, создаваемых службой аудита.

Параметр

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 `yum` используется для установки и обновления ПО.

Параметр

Название	Параметр gpgcheck должен быть включён для всех yum репозиториев

Описание

Чтобы убедиться, что проверка цифровых подписей не отключена ни для каких репозиториев, необходимо удалить строки
`gpgcheck=0`
из всех файлов из директории `/etc/yum.repos.d` или заменить на строку
`gpgcheck=1`

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

Название **Добавление nodev опции для некорневых локальных 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 четвёртый столбец файла `/etc/fstab` для строки, которая отвечает за монтирование различных некорневых локальных разделов.

Параметр

Название **Добавление опции nodev для подключаемых 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 различных подключаемых разделов.

Параметр

Название **Добавление опции noexec для подключаемых медиа разделов**

Описание

Опция монтированния `noexec` предотвращает выполнение бинарных файлов на смонтированной файловой системе. Пользователям не должно быть позволено запускать бинарные файлы, из смонтированных разделов носителей, таких как, например, USB. Опция `noexec` препятствует выполнению кода непосредственно с самого носителя и может обеспечить дополнительную линию защиты против некоторых видов червей и вредоносных кодов. Необходимо добавить опцию `noexec` в четвёртую колонку файла `/etc/fstab` для строки, которая отвечает за монтирование подключаемых медиа разделов.

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 локальных 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
Название	**Проверка владельца shadow файла**

Описание

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

	Параметр
Название	**Проверка группы владельца файла shadow**

Описание

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

	Параметр
Название	**Проверка прав доступа файла shadow**

Описание

Для правильного задания прав доступа к файлу `/etc/shadow`, необходимо выполнить команду:
```
# chmod 000 /etc/shadow
```

	Параметр
Название	**Проверка владельца файла group**

Описание

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

	Параметр
Название	**Проверка группы владельца файла group**

Описание

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

	Параметр
Название	**Проверка прав доступа к файлу group**

Описание

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

```
# chmod 644 /etc/group
```

Параметр

Название **Проверка владельца файла gshadow**

Описание

Для правильной установки владельца файла `/etc/gshadow` необходимо выполнить команду:

```
# chown root /etc/gshadow
```

Параметр

Название **Проверка группы владельца файла gshadow**

Описание

Для правильной установки группы владельца файла `/etc/gshadow`, необходимо выполнить команду:

```
# chgrp root /etc/gshadow
```

Параметр

Название **Проверка прав доступа к файлу gshadow**

Описание

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

```
# chmod 0000 /etc/gshadow
```

Параметр

Название **Проверка владельца файла passwd**

Описание

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

```
# chown root /etc/passwd
```

Параметр

Название **Проверка группы владельца файла passwd**

Описание

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

```
# chgrp root /etc/passwd
```

Параметр

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	
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	
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	
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
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
```

	Группа
Название	**Ограничение программ от возможного опасного поведения**
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
Название	**Включение рандомизированного расположения виртуального адресного пространства**
Описание	

Для установки runtime-статуса параметра ядра `kernel.randomize_va_space`, необходимо выполнить следующую команду:
```
# sysctl -w kernel.randomize_va_space=2
```
Если это не значение системы по умолчанию, необходимо добавить следующую строку в `/etc/sysctl.conf`:
```
kernel.randomize_va_space = 2
```

	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..

	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	
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	
Название	**Ограничение входа суперпользователя через последовательный порт**
Описание	

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

```
ttyS0
ttyS1
```

Параметр	
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 /sbin/nologin
                имя учетной записи
```

Параметр	
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	
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/system-auth`, чтобы запретить вход по пустым паролям.

Параметр	
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	
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:

```
PASS_MIN_DAYS
                7
```

Параметр	
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:

```
PASS_MAX_DAYS
                90
```

Параметр	
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/system-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 службы аутентификации.

	Параметр
Название	**Установка минимальной длины пароля**
Описание	

По умолчанию PAM модуль `pam_passwdqc` обеспечивает возможность соблюдения строгих требований к стойкости пароля.

min = N0, N1, N2, N3, N4 [min = disabled, 24,11,8,7]
enforce=everyone

Используемые типы паролей по классам символов (алфавит, число, спецсимвол, верхний и нижний регистр) определяются следующим образом:
- тип N0 используется для паролей, состоящих из символов только одного класса;
- тип N1 используется для паролей, состоящих из символов двух классов;
- тип N2 используется для парольных фраз, кроме этого требования длины, парольная фраза должна также состоять из достаточного количества слов;
- типы N3 и N4 используются для паролей, состоящих из символов трех и четырех классов, соответственно.
Ключевое слово «disabled» используется для запрета паролей выбранного типа N0-N4 независимо от их длины.

Примечание: каждое следующее число в настройке «min» должно быть не больше, чем предыдущее.

Параметр «enforce=everyone» задает ограничение задания паролей в passwd и на пользователей, и на суперпользователя root.

При расчете количества классов символов, заглавные буквы, используемые в качестве первого символа и цифр, используемых в качестве последнего символа пароля, не учитываются.

Далее приводится пример задания следующих значений в файле в файле /etc/passwdqc.conf:
min=disabled,24,11,8,7
enforce=everyone

В указанном примере пользователям, включая суперпользователя root, будет невозможно задать пароли:
- типа N0 (символы одного класса) – запрет;
- типа N1 (символы двух классов) – длиной меньше 24 символа;
- типа N2 (парольные фразы) – длиной меньше 11 символов;
- типа N3 (символы трех классов) – длиной меньше 8 символов;
- типа N4 (символы четырех классов) – длиной меньше 7 символов.

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

Описание

Чтобы настроить систему на блокировку учетной записи после нескольких неверных попыток входа, необходимо отредактировать файл `/etc/pam.d/login`, добавив следующую строку:

```
auth required pam_tally2.so deny=3 even_deny_root
```

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

Название **Проверка прав доступа к файлам конфигурации загрузчика**

Описание

Права доступа к файлам конфигурации загрузчика должны быть установлены в 600. Владельцем файлов должен быть пользователь `root` в группе `root`.

Для правильной установки разрешений загрузчика GRUB, необходимо выполнить команды:

```
# chmod 600 /etc/default/grub; chmod 600 /etc/grub.cfg; chmod 600 /boot/grub/grub.cfg
```

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
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
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
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` или `/etc/net/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
Название	**Отключение параметра ядра для принятия Source-Routed пакетов для всех интерфейсов**
Описание	

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

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

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

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

	Параметр
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
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
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
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
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
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
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
Название	**Включение параметра ядра для игнорирования Bogus ICMP сообщений об ошибках**
Описание	

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

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

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

```
net.ipv4.icmp_ignore_bogus_error_responses = 1
```

	Параметр
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

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

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.

Параметр

Название	**Отключение Беспроводных сетевых интерфейсов**

Описание

Отключение беспроводных сетевых интерфейсов должно препятствовать нормальному использованию беспроводной связи.

Во-первых, интерфейсы определяются с помощью команды:

```
# ifconfig -a
```

Кроме того, следующие команды могут быть использованы для определения беспроводной поддержки ('расширенных') включённых для определенного интерфейса, хотя это не всегда может быть ясно видно:

```
# iwconfig
```

После идентификации любых беспроводных интерфейсов (которые могут иметь имена, такие как `wlan0`, `ath0`, `wifi0`, `em1` или `eth0`), необходимо деактивировать интерфейс с помощью команды:

```
# ifdown
              interface
```

Эти изменения будут активны только до следующей перезагрузки. Чтобы отключить интерфейс для полностью, необходимо удалить файл соответствующего интерфейса из `/etc/sysconfig/network-scripts`:

```
# rm /etc/sysconfig/network-scripts/ifcfg-
              interface
```

Группа	
Название	**Брандмауэр**
Описание	

Просмотреть на данный момент правила можно, выполнив команду:
```
# efw show
```
Если правила брандмауэра не отображаются (Firewall is disabled), необходимо сброс настроек до значений по умолчанию, выполнив следующую команду:
```
# alterator-net-iptables reset
```

Параметр	
Название	**Найстройка брандмауэра**
Описание	

Найстройте брандмауэр в минимально необходимой конфигурации для работы.

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

Параметр	
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/openssh/sshd_config`:
```
IgnoreRhosts yes
```

Параметр	
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/openssh/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.

	Параметр
Название	**Установка SSH Client Alive Count**
Описание	

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

```
ClientAliveCountMax 0
```

	Параметр
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/openssh/sshd_config`:

```
HostbasedAuthentication no
```

	Параметр
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/openssh/sshd_config`:

```
PermitRootLogin no
```

	Параметр
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/openssh/sshd_config`:

```
PermitEmptyPasswords no
```

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

	Параметр
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/openssh/sshd_config`:

```
Banner /etc/issue
```

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

	Параметр
Название	**Не разрешать SSH переменные окружения**
Описание	

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

```
PermitUserEnvironment no
```

	Параметр
Название	**Разрешить только SSH Protocol 2**
Описание	

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

```
Protocol 2
```

	Параметр
Название	**Выключение в SSH RhostsRSAAuthentication**
Описание	

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

```
RhostsRSAAuthentication no
```

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

Служба аудита обеспечивает существенные возможности для записи деятельности системы.

	Параметр
Название	**Включение службы auditd**
Описание	

Служба `auditd` является важным компонентом пользовательской части системного аудита Linux, так как он отвечает за запись контрольных записей на диск. Служба `auditd` может быть запущена командой:

```
# systemctl enable auditd.service && systemctl start auditd.service
```

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

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

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

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
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
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	
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 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	
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 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
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
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 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
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
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
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
Название	**Журналы аудита системы должны иметь права 0640 или менее разрешающие**
Описание	

Изменить права файла журналов аудита можно командой:

```
# chmod 0640
              audit_file
```

	Параметр
Название	**Журналы аудита системы должны принадлежать суперпользователю**
Описание	

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

```
# chown root /var/log
```

	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=b64 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
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
```

Если система 64-разрядная, то эти строки должны быть продублированы и arch=b32 заменить на arch=b64 следующим:

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

	Параметр
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
```

Если система 64-разрядная, то эти строки должны быть продублированы и arch=b32 заменить на arch=b64 следующим:

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

	Параметр
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
```

Если система 64-разрядная, то эти строки должны быть продублированы и arch=b32 заменить на arch=b64 следующим:

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

	Параметр
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
```

Если система 64-разрядная, то эти строки должны быть продублированы и arch=b32 заменить на arch=b64 следующим:

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

	Параметр
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
```

Если система 64-разрядная, то эти строки должны быть продублированы и arch=b32 заменить на arch=b64 следующим:

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

	Параметр
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
```

Если система 64-разрядная, то эти строки должны быть продублированы и arch=b32 заменить на arch=b64 следующим:

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

	Параметр
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
```

Если система 64-разрядная, то эти строки должны быть продублированы и arch=b32 заменить на arch=b64 следующим:

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

	Параметр
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
```

Если система 64-разрядная, то эти строки должны быть продублированы и arch=b32 заменить на arch=b64 следующим:

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

	Параметр
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
```

Если система 64-разрядная, то эти строки должны быть продублированы и arch=b32 заменить на arch=b64 следующим:

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

	Параметр
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
```

Если система 64-разрядная, то эти строки должны быть продублированы и arch=b32 заменить на arch=b64 следующим:

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

	Параметр
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
```

Если система 64-разрядная, то эти строки должны быть продублированы и arch=b32 заменить на arch=b64 следующим:

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

	Параметр
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
```

Если система 64-разрядная, то эти строки должны быть продублированы и arch=b32 заменить на arch=b64 следующим:

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

	Параметр
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
```

Если система 64-разрядная, то эти строки должны быть продублированы и arch=b32 заменить на arch=b64 следующим:

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

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

Как минимум, система аудита должна записывать информацию о не 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
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
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
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
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
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
```

	Параметр
Название	**Сделать конфигурацию auditd неизменяемой**
Описание	

Необходимо добавить следующее в `/etc/audit/audit.rules` для того, чтобы сделать конфигурацию неизменяемой:
`-e 2`
Для этой установки, необходимо перезагрузка для внесения изменений в правила аудита.