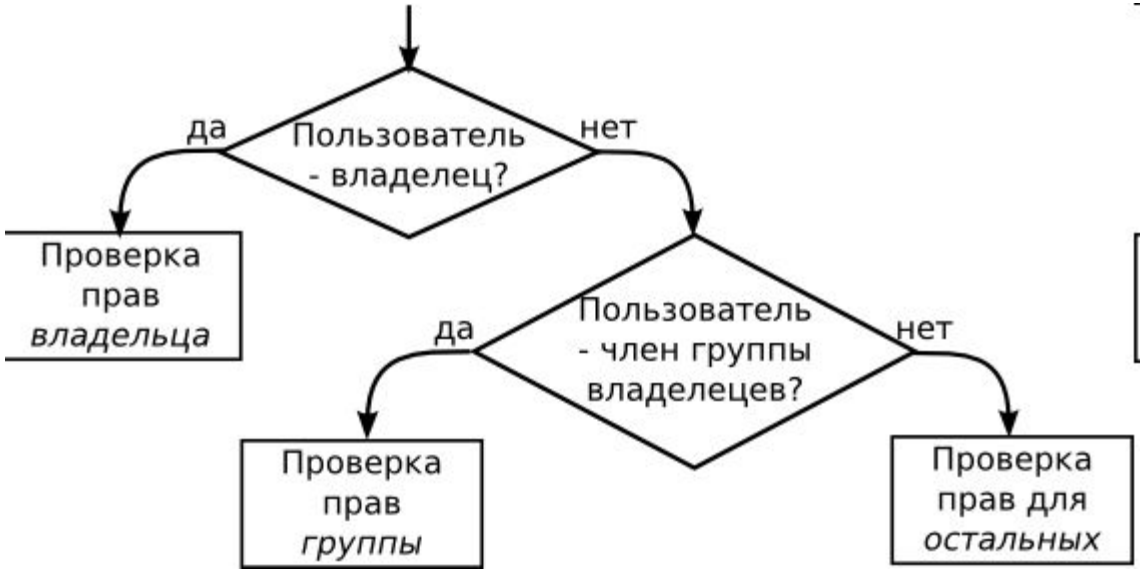
Безопасность Unix

Безопасность ФС. Базовые права доступа

Безопасность Unix

Безопасность ФС. Последовательнось проверки прав доступа в UNIX



Безопасность Unix

Безопасность ФС.
ACL (Access Control List)

ACL для доступа — это список управления доступом для заданного файла или каталога

Стандартная 9 битовая система прав Unix проста, предсказуема но недостаточно гибкая

Система ACL является частью POSIX спецификации

Поддержка ACL есть в большинстве ФС

Использовать следует осторожно, так как усложняет поддержку системы

Безопасность Unix

Безопасность ФС.
ACL (Access Control List)

Активация ACL – монтирование раздела с опцией acl

mount -t ext3 -o acl <device-name> <partition>

Разные ФС поддерживают разный размер ACL

Списки ACL можно настроить:

1. На уровне пользователей
2. На уровне групп
3. С помощью маски эффективных прав
4. Для пользователей, не включённых в группу данного файла

Безопасность Unix

Безопасность ФС. Использование ACL

Установка прав

setfacl -m rules files

 # setfacl -m u:andrius:rw /project/somefile

Удаление прав

setfacl -x rules files

 # setfacl -x u:500 /project/somefile

Установка прав по умолчанию (только для директорий)

 # setfacl -m d:o:rx /share # установка прав rx для всех, кроме владельца и группы (индивидуальные установки ACL для файлов переопределяют установки прав по умолчанию)

Безопасность Unix

Безопасность ФС. Использование ACL

Просмотр прав

```
# getfacl home/john/picture.png
# file: home/john/picture.png
# owner: john
# group: john
user::rw-
user:barry:r--
group::r--
mask::r--
other::r--
default:user::rwx
default:user:john:rwx
default:group::r-x
default:mask::rwx
default:other::r-x
```

Безопасность Unix

Лимиты системы /etc/security/limits.conf

В файле limits.conf определяются ограничения ресурсов системы для пользователя или группы пользователей. Формат файла такой:

<domain> <type> <item> <value>

Первое поле (domain) может содержать:

1. Имя пользователя
2. Имя группы. Перед именем группы нужно указать символ «@»
3. Символ «*». Данное ограничение будет ограничением по умолчанию.

Безопасность Unix

Лимиты системы /etc/security/limits.conf

Второе поле – это тип ограничения: мягкое (soft) или жесткое (hard). Мягкое ограничение определяет число системных ресурсов, которое пользователь все еще может превысить, жесткое ограничение превысить невозможно. При попытке сделать это, пользователь получит сообщение об ошибке.

Элементом ограничения (item) может быть:

1. core – ограничение размера файла core (Кб)
2. data – максимальный размер данных (Кб)
3. fsize – максимальный размер файла (Кб)
4. memlock – максимальное заблокированное адресное пространство (Кб)
5. nofile – максимальное число открытых файлов
6. stack – максимальный размер стека (Кб)
7. cpu – максимальное время процессора (минуты)
8. nproc – максимальное число процессов
9. as – ограничение адресного пространства
10. maxlogins – максимальное число одновременных регистраций в системе
11. locks – максимальное число файлов блокировки

Безопасность Unix

Лимиты системы /etc/security/limits.conf

Пример файла

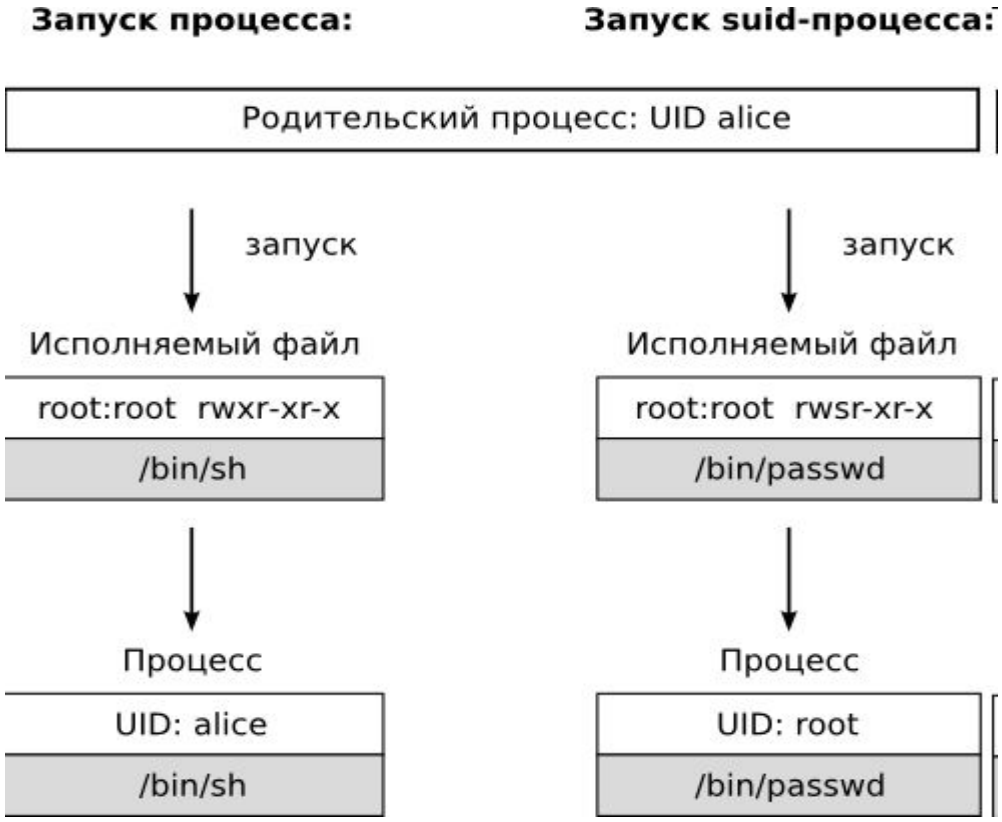
user soft nproc 50

user hard nproc 60

Первая строка определяет мягкое ограничение (равное 50), а вторая – жесткое на максимальное число процессов для пользователя user

Безопасность Unix

Повышение привилегий.SUID бит



Безопасность Unix

Повышение привилегий. Команда su

Команда Unix-подобных операционных систем, позволяющая пользователю войти в систему под другим именем, не завершая текущий сеанс или выполнить команду от имени другого пользователя.

su [-] [имя_пользователя [аргумент ...]]

Безопасность Unix

Повышение привилегий. Команда sudo

Программа для системного администрирования UNIX-систем, позволяющая делегировать те или иные привилегированные ресурсы пользователям с ведением протокола работы. Основная идея — дать пользователям как можно меньше прав, при этом достаточных для решения поставленных задач

Файл конфигурации **/etc/sudoers**

<user> <host> = <user to alias> <password required> < command to run>

Примеры использования: Вид файла конфигурации

user1 ALL = (user2) NOPASSWD: /home/dbinst4/adm/db2start

Примеры использования: Вид команд запуска

sudo -u user2 /home/dbinst4/adm/db2start

Безопасность Unix

Повышение привилегий. Команда sudo

Примеры использования

Примеры использования: Вид файла конфигурации

user1 ALL = (ALL) NOPASSWD: ALL

Примеры использования: Получение командой строки суперпользователя без пароля

sudo –s

sudo su –

Примеры использования: Вид файла конфигурации

user1 ALL = (ALL) ALL

Примеры использования: Получение командой строки суперпользователя на основе пароля пользователя

sudo –s

sudo su –

Безопасность Unix

Role-based access control (RBAC)

RBAC позволяет создавать роли для администрирования системы и делегирования задач по администрированию какому-либо из группы защищенных пользователей системы.

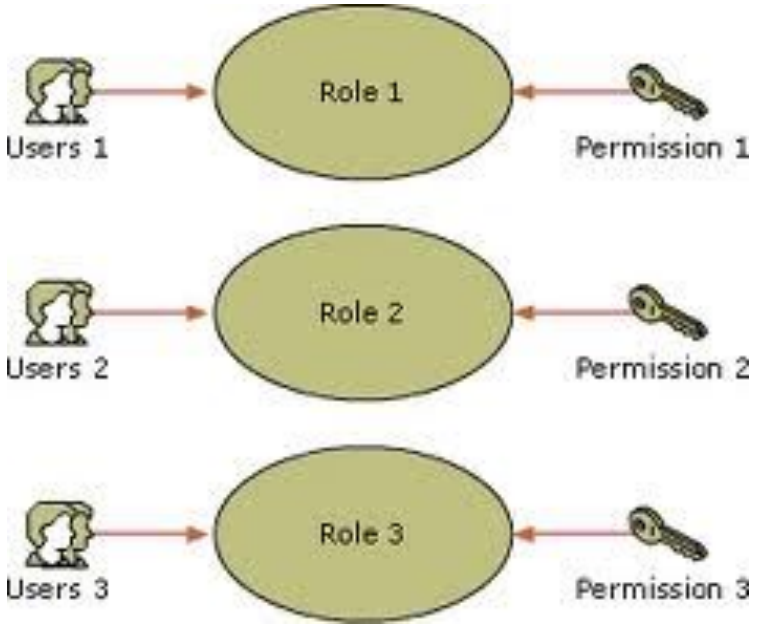
Реализация в ОС Linux

SELinux

AppArmor

Grsecurity

RSBAC



Безопасность Unix

HIDS (Host-based intrusion detection system)

Хостовая система обнаружения вторжений

Хостовая система обнаружения вторжений— это система обнаружения вторжений, которая ведет наблюдение и анализ событий, происходящих внутри системы

Следит за текущей информацией:

В памяти

На дисках

В системных журналах

Безопасность Unix

Аудит системы

- Найдите файлы загрузки и определите, какие приложения запускаются при загрузке системы
- Определите требования для входа через корневую учетную запись.
- Проверьте систему на наличие неиспользуемых учетных записей.
- Установите в системе соответствующие обновления.
- Убедитесь в том, что в системе ведется журнал подозрительной активности, и что файл syslog.conf настроен соответствующим образом.
- Произведите в системе поиск скрытых файлов.
- Произведите поиск файлов SUID и SGID.
- Проверьте систему на предмет прослушиваемых (активных) портов.
- Проверьте таблицу процессов в системе и определите, выполняются ли какие-либо несоответствующие процессы.