Безопасность ОС

Безопасность Linux

Файловые операции. Права доступа

Идентификаторы

- *учётное имя* не должно начинаться с цифры, содержать заглавных и русских букв, а также символов типа * # % ^

- под *UID* отводится 4 байта, что достаточно для регистрации более 4 млрд пользователей

Идентификаторы

- первые сотни номеров UID резервируются для *псевдопользователей* `daemon`, `bin`, `sys`, `nobody` и др. компонентов ОС

- учётные записи псевдопользователей не содержат паролей и не позволяют работу с командной строкой

- в некоторых дистрибутивах у суперпользователя тоже нет пароля

Суперпользователь

- можно зарегистрировать более одного суперпользователя с UID = 0 путём редактирования файла с учётными записями
- внимательно вводите команды, напр.

```
rm -rf /home/john

rm -rf /home /john
```

Суперпользователь

- параметры команд позволяют снизить рутину, но это повышает цену ошибки

- злоумышленник может спровоцировать суперпользователя

- администратору следует создать себе учётную запись обычного пользователя

Право исполнения

- двоичные исполняемые файлы имеют специальный формат
- текстовые исполняемый файлы имеют специальную комбинацию символов в начале:

```
#! /bin/bash
```

- для запуска сценария оболочке требуется ещё право на чтение

Создание файла

`touch file` меняет временные метки файла

`echo > file` создаёт пустой файл

`cat > file` позволяет вводить строки до **Ctrl-D**

«Тёмный» каталог

- это каталог с правами w и x

- может служить приёмником в системе файлообмена

Право входа в каталог

```
# chmod 700 /home
```

```
$ cd ..
```

```
$ cd /
```

Смена владельца

обычные пользователи не могут отдавать файлы

- это может быть вредоносная программа
- можно превысить чужую дисковую квоту

Удаление файла

- достаточно прав **w** и **x** для каталога
- не требуется никаких прав на сам файл
- поэтому и появился *sticky bit*
- право **t** обозначается **T**, если нет права **x**
- **s** заменяется на **S**, если у владельца нет права **x**

Эффективные права

- **i** – защита от любых изменений, включая изменение временных меток и создание жёстких ссылок, напр., для защиты конфигурации
- **a** – запрет любых операций, кроме добавления данных, напр., для защиты журналов
- **A** – неизменяемость метки последнего доступа

Копирование файлов

```
cp -arg file1 file2

cp -arg file dir

cp -arg dir dir
```

- `f` – не выдавать запрос на переписывание
- `p` – сохранить метаданные файла, включая права
- `R` – рекурсивное копирование (с вложенными каталогами)
- `a` – создание точной копии каталога

Копирование файла

- необходимо право чтения файла
- нужны права **r** и **x** в каталоге-источнике
- нужны права **w** и **x** в каталоге назначения
- сохранность метаданных определяется соответствием типов файловых систем

Удаление файла

- `rm -arg file`
- `-f` – удаление без запросов и подтверждений
- `-d` – удаление непустого каталога
- `-r` – рекурсивное удаление внутренних каталогов

Жёсткие ссылки

- для создания нужно только право **x** в каталоге с исходным файлом, а также **w** и **x** в каталоге назначения (угрозы?)
- при создании каталога в него записываются две жёсткие ссылки:

  `.` – ссылка на самого себя

  `..` – ссылка на родительский каталог

- создание иных жёстких ссылок на каталог не разрешается даже суперпользователь (петля)

Символические ссылки

- угроза целостности временных файлов в `/tmp`
- если заранее знать имя временного файла
- есть ли угроза конфиденциальности?
- противодействие: случайные имена файлов
- проблема: захламление каталога `/tmp`