Занятие 2

- Права доступа. Группы. Пользователи.

Безопасность

Linux и вирусы

- По-настоящему безопасной можно считать лишь систему, которая выключена, замурована в бетонный корпус, заперта в помещении со свинцовыми стенами и охраняется вооруженным караулом, но и в этом случае сомнения не оставляют меня"
- © - Юджин Спаффорд

И всё же...

- Open source
- Официальные репозитории
- Уязвимости быстро устраняются
- Права доступа

Пользователи Linux

- /etc/passwd , /etc/shadow
- root пользователь – неограниченный доступ к системе
- Обычный пользователь – ограниченный доступ
- Какие файлы обычный пользователь не может прочитать, изменить, удалить?

Пользователи и группы

- Всё в Linux – это файл. Даже устройства.
- Каждый файл принадлежит хотя бы одному пользователю и хотя бы одной группе.
- У каждого файла может быть три вида прав: 1) запись 2) чтение 3) исполнение
- Новые файлы никогда не имеют прав на исполнение
- Все эти параметры можно изменять

Команда sudo

- sudo позволяет выполнить команду от имени пользователя root.
- Не всякий пользователь может воспользоваться командой sudo
- Неоходимо ввести пароль пользователя (не пароль root !)
- Пользователь должен быть прописан в /etc/sudoers

Группы

- Группа пользователей имеет общие права доступа
- Пользователи одной группы не обязательно имеют одинаковые права доступа
- Зачем нужны группы пользователей?
- Кому принадлежит только что созданный файл?
- К какой группе принадлежит пользователь root?

Особые права доступа

- SUID – права на исполнение с разрешения владельца
- SGID – права на исполнение с разрешения владельца группы
- Sticky bit – не позволяет пользователю удалять файлы, если они созданы не им.

ACL

- Access control list – позволяет наделить пользователя любыми правами для любых файлов в системе
- Когда это может быть полезно?
- Когда это может быть опасно?

Атрибуты файлов

- Immutable
- Append only
- Undeletable
- Compressed
- No copy on write
- ...

Заключение

- Пользователи
- Группы
- Особые права доступа
- ACL