Skillbox

Права суперпользователя

Медведик Давид

Ведущий инженер-программист в «Positive Technologies»

Цель урока

Познакомиться с правами суперпользователя, его домашним каталогом, а также изучить новую команду chroot.

В этом уроке мы рассмотрим

- Права суперпользователя
- Домашний каталог суперпользователя
- Команду chroot

Зачем нам нужно это знать?

- Понимать права суперпользователя
- Уметь менять корневой каталог

Права суперпользователя

Права суперпользователя в linux безграничны: он может создавать и удалять любые файлы и каталоги, а также запускать любые программы, в отличие

от обычного пользователя.

Обычный пользователь ограничивается следующим набором прав:

- чтение, запись и изменение любых атрибутов пользовательской папки
- то же самое и для каталога/tmp
- выполнение программ в любом месте, где нет ограничений
- чтение файлов с соответствующим атрибутом для всех пользователей

Домашний каталог суперпользователя

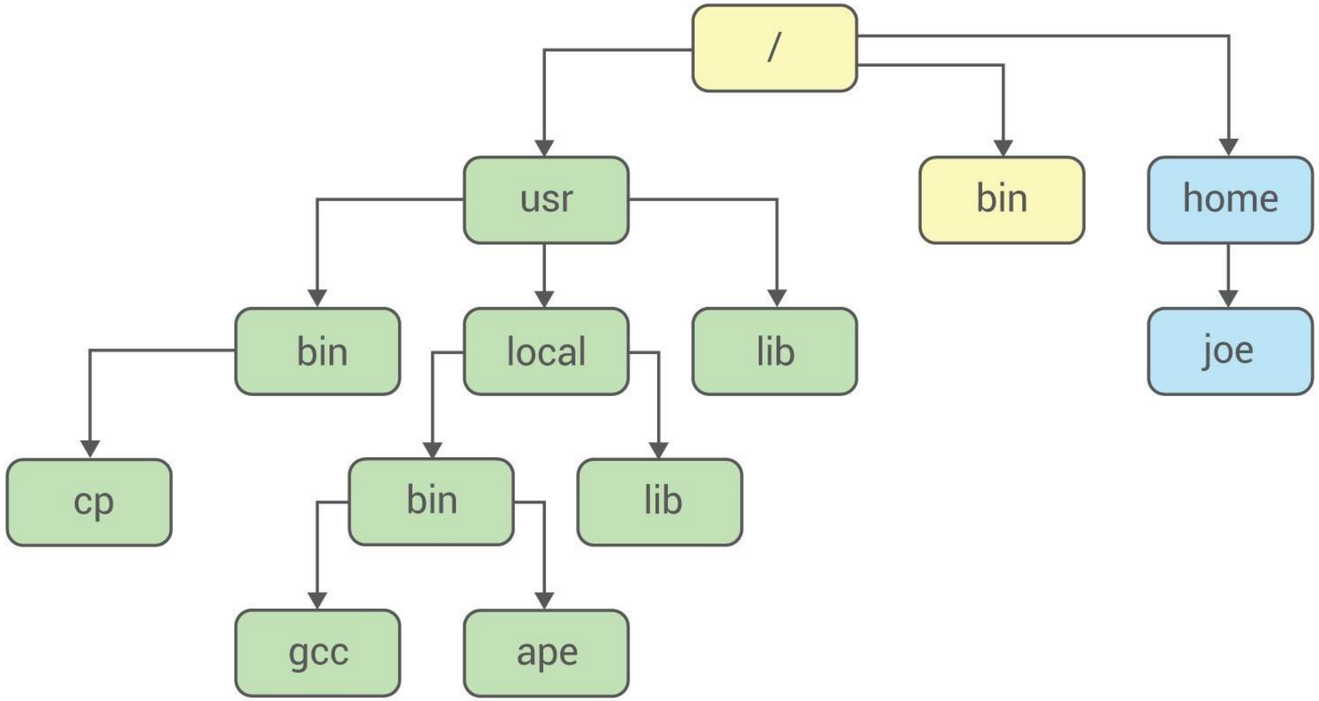
Домашний каталог суперпользователя (root) находится в /root.

Располагается на том же разделе, что и система, отдельно от каталога /home.

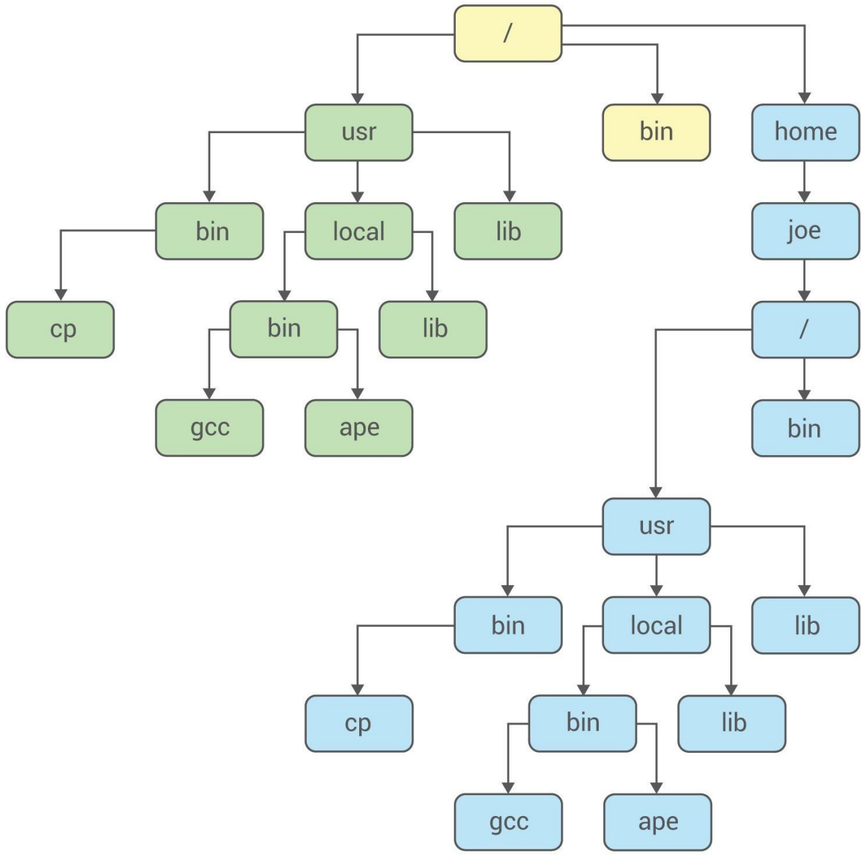
Команда chroot

Chroot — операция изменения корневого каталога в Unix-подобных операционных системах.

Команда chroot



Команда chroot



Команда chroot

Chroot **[OPTION]** NEWROOT [COMMAND [ARG]...]

Опция	Значение
--groups = G_LIST	Задаёт список групп пользователей перечислением в формате g1,g2,…gn.
--userspec = USER:GROUP	Задаёт пользователя и группу в формате ПОЛЬЗОВАТЕЛЬ:ГРУППА
--skip-chdir	Запрещает изменение рабочего каталога на корневой «/».

Использование

- Разделение привилегий
- Изготовление honeypot-ов

Honeypot — ресурс, представляющий собой приманку для злоумышленников.

Недостатки

- Только суперпользователь может выполнять системный вызов chroot
- Сам по себе механизм chroot не полностью безопасен
- Большинство систем Unix не полностью ориентированы на файловую систему и оставляют потенциально разрушительную функциональность
- Механизм chroot сам по себе не умеет осуществлять ограничения на ресурсы

Выводы

Теперь у вас более чёткое представление о суперпользователе и каталоге /root в системе Linux.

Спасибо за внимание!