Тема 1. Физическая безопасность сервера на базе ОС Linux

План

- 1. Сброс пароля в Linux:
  - single-user mode
  - Внедрение в ход загрузки ОС
  - Загрузка с Live CD – редактирование конфигурационных файлов
- 2. Методы защиты от сброса пароля:
  - Установка пароля суперпользователя root
  - Установка пароля загрузчика Grub
  - Установка пароля EFI
  - Использование прозрачного полнодискового шифрования (Full Disk Encryption)
- 3. Подсистема полнодискового шифрования: dm-crypt и Linux Unified Key Setup

Сброс пароля: Single-user и rescue mode

- Помимо штатного режима загрузки ОС Linux существуют служебные режимы:
  i. **Single-User Mode** (Runlevel 1)
  ii. **Rescue Mode**
- Нормальный режим работы ОС Linux подразумевает загрузку

  …

  linux /boot/vmlinuz-3.13.0-170-generic … ro quiet splash **single**

  …
- Также можно использовать:
  - **S**
  - **s**
  - **systemd.unit=rescue.target**
  - **rescue**
  - **recovery**
  - …

Сброс пароля: Single-user mode

- В старых системах по умолчанию при загрузке в single user mode запускался командный интерпретатор sushell
- Оболочка sushell не требует ввода пароля пользователя **root**
- Исправить подобное поведение можно, выбрав в качестве запускаемой оболочки **sulogin** или аналогичный командный интерпретатор
- CentOS 6
  - # vi **/etc/sysconfig/init**

    …

    SINGLE=**/sbin/sushell** # нужно заменить на SINGLE=**/sbin/sulogin**
- Ubuntu 14.04
  - # nano **/etc/init/rcS.conf**

    …

    exec **/sbin/sulogin**
- Ubuntu 16.04 и старше (systemd-based)
  - # nano **/lib/systemd/system/rescue.service**

    …

    ExecStart=-/usr/lib/systemd/systemd-sulogin-shell rescue

    …
  - # nano **/lib/systemd/system/emergency.service**

    …

    ExecStart=-/usr/lib/systemd/systemd-sulogin-shell emergency

Сброс пароля: Замена init-system на /bin/bash

- Непустой пароль пользователя root и /sbin/sulogin в качестве оболочки для Single user mode приводят к тому, что перед запуском шелла пароль выполняется проверка пароля root
- Однако необязательно пользоваться режимом Single user mode штатной системы инициализации, можно в принципе её (init) не запускать!
- Заменить процесс init можно в параметрах grub:

  …

  linux /boot/vmlinuz-3.13.0-170-generic … ro quiet splash **init=/bin/bash**

  …

Установка пароля на GRUB

- Решение обозначенных проблем – запаролить grub!
- Для этого в конфигурационных файлах прописывают имя пользователя (может быть любым – не привязано к пользователям ОС) и пароль или (лучше) хэш пароля
- Например, в Ubuntu 24.04:
  - # nano /etc/grub.d/40_custom

    …
    set superusers="groot"
    password groot groot
  - лучше вместо пароля в открытом виде указать хэш:

    # grub-mkpasswd-pbkdf2
    Enter password:
    Reenter password:
    PBKDF2 hash of your password is grub.pbkdf2.sha512.10000.C12230…
    # nano /etc/grub.d/40-custom

    …
    set superusers="groot"
    password_pbkdf2 groot grub.pbkdf2.sha512.10000.C12230…
  - после редактирования пересобрать конфиг:

    # update-grub
  - чтобы пароль не запрашивался при загрузке необходимо в файле /etc/grub.d/10_linux добавить *--unrestricted* в переменную CLASS в начале скрипта

Сброс пароля: Загрузка с помощью LiveCD

- Запароленный grub не проблема – можно загрузиться с LiveCD!
- Ставим CD/USB с Live-системой -> Reboot -> жмём <F2> -> выбираем CD/USB
- Далее – монтируем диск с системой, генерируем новый хэш пароля и перезаписываем в **/etc/shadow**:

```
# fdisk –l
Disk /dev/sda: 50 GiB, 53687091200 bytes, 104857600 sectors
…
# mkdir /tmp/disk
# mount /dev/sda2 /tmp/disk
# openssl passwd -6 42
$6$JbluFr0BjGDA6kjw$O0r8h7clHhlgkdIWPIFACOyOQAigp496cC5002yzMVvccmGijPUI1X9rYPBFdRg64pjA4VgceKQHz5MCcydNq0
# nano / tmp/disk/etc/shadow
…
x:$6$JbluFr0BjGDA6kjw$O0r8h7clHhlgkdIWPIFACOyOQAigp496cC5002yzMVvccmGijPUI1X9rYPBFdRg64pjA4VgceKQHz5MCcydNq0 :20002:0:99999:7:::
```

- Изменяем пароль в grub:

```
# mount /dev/sda2 /mnt
# mount /dev/sda1 /mnt/boot/efi
# for i in /dev /dev/pts /proc /sys /run; do mount -B $i /mnt$i; done
#
# chroot /mnt
# grub-install /dev/sda
# nano /etc/grub.d/40-custom
# … - comment out “set superusers” and “password”
# update-grub
# exit
# for i in /run /sys /proc /dev/pts /dev; do umount /mnt$i; done
# umount /mnt/boot/efi
# umount /mnt
```

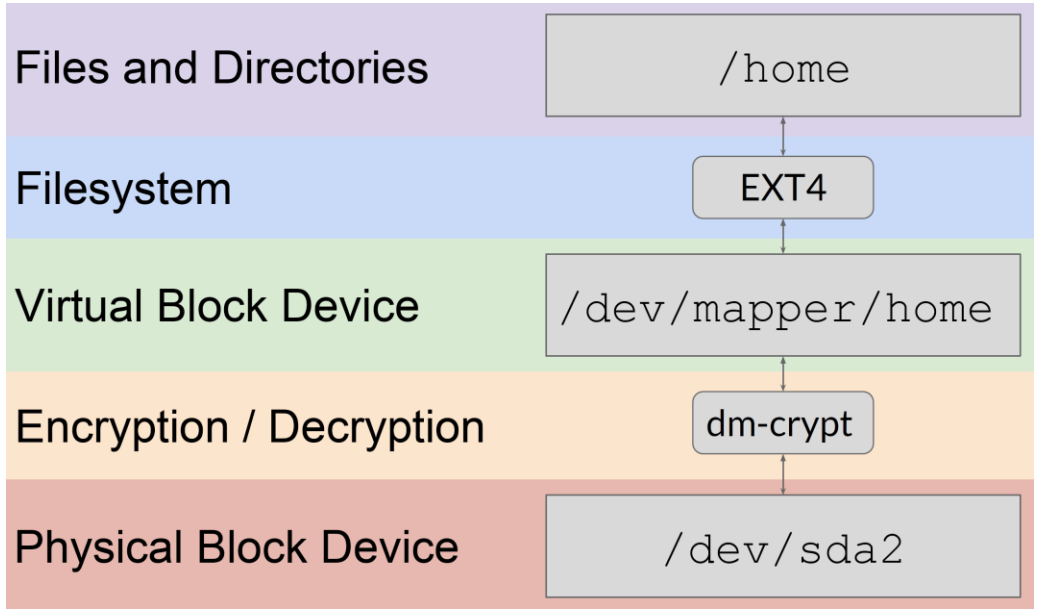
- И перезагружаемся в целевую ОС

Установка пароля на EFI

- Выставление пароля на EFI не даёт возможность загрузиться с диска
- Однако диск всё ещё можно вытащить из машины
- Подключая диск к другой машине, изменяем хэш пароля и (при необходимости) конфиг grub
- Также возможно сбросить настройки (U)EFI машины

Шифрование диска: dm-crypt и LUKS

- Выход – использовать шифрование дисков!
- В Linux прозрачное шифрование дисков выполняется средствами Linux Unified Key Setup, LUKS
- LUKS является фронтендом к службе dm-crypt ядра Linux
- LUKS позволяет создать шифрованный раздел при установке ОС
- Также можно работать с дисками и файлами-контейнерами напрямую



Шифрование диска: dm-crypt и LUKS

- Пример: шифрование нового **диска**

```
# cryptsetup -y -v luksFormat /dev/sdb
# cryptsetup luksOpen /dev/sdb vault
# ls -l /dev/mapper/vault
# cryptsetup -v status vault
# cryptsetup luksDump /dev/sda
#
# dd if=/dev/zero of=/dev/mapper/vault
# mkfs.ext4 /dev/mapper/vault
#
# mkdir /mnt/vault
# mount /dev/mapper/vault /mnt/vault
#
# nano /mnt/vault/secret
#
# umount /mnt/vault
# cryptsetup luksClose vault
```

Шифрование файла-контейнера

- Пример: создание шифрованного файла-контейнера

```
# mkdir –p  /tmp/disk && cd /tmp/disk
# dd if=/dev/urandom of=container.bin bs=1M count=256
# losetup -f --show container.bin
# cryptsetup luksFormat /dev/loop X
# cryptsetup luksDump /dev/loop X
#
# cryptsetup luksOpen /dev/loop X container
# mkfs.ext4 /dev/mapper/container
# cryptsetup luksClose container
```

- Использовать

```
# cryptsetup luksOpen /dev/loop X container
# mount /dev/mapper/container /mnt
# echo "Hello, LUKS!" > /mnt/secret.txt
# umount /mnt
# cryptsetup luksClose container
```

Источники

Сброс пароля пользователя в ОС Linux

1. Performing Linux Password Resets

Защита GRUB паролем и сброс пароля GRUB

2. GRUB set password boot protection
3. Загрузка ОС без ввода пароля GRUB
4. Reinstall the GRUB boot loader to Ubuntu installation in EFI mode
5. How to Install or Repair GRUB 2 with Ubuntu Live CD/Flash

Шифрование дисков с помощью LUKS

6. dm-crypt: Linux kernel device-mapper crypto target
7. [wikipedia.org] Linux Unified Key Setup
8. [xakep.ru] LUKS good! Ставим Linux на шифрованный раздел и делаем удобной работу с ним
9. 10+ losetup command examples in Linux
10. [redhat.com] Encrypting block devices using LUKS security hardening

Разное

11. https://www.cyberciti.biz/faq/understanding-etcpasswd-file-format/
12. https://www.cyberciti.biz/faq/understanding-etcshadow-file/