**Инструкция по созданию шифрованной системы на примере Ubuntu**

Понадобятся:

* Установочная флэшка
* LiveCD (LiveUSB, виртуальная машина, другая система на Ubuntu)
* Винт, который будет шифроваться, и на который в итоге будет переноситься наша система
* Флэшка с ключом – флэшка, разбитая на 2 раздела (1ый для ключа и монтирования /boot, 2ой для «видимости» обычного накопителя

1. **Подготовка**

Запускаем LiveCD образ, подключаем флэшку с ключом, в программе Gparted разбиваем её на 2 раздела – первый для ключа на около 100 МБ в фс ext2 (чтобы при подключении в Windows 2ой раздел ощущался единственным), второй всё оставшееся в ntfs или fat32. Соответственно sdc1 и sdc2. Монтируем их в систему.

**sudo su**

**mkdir /mnt/flash /mnt/boot**

**mount /dev/sdc1 /mnt/flash**

**mount /dev/sdc2 /mnt/boot**

далее создаём ключ и копируем его на 1ый раздел

**dd if=/dev/random of=/mnt/boot/mykey bs=1 count=256**

**cp /mnt/boot/mykey /mnt/flash/**

загружаем свой модуль в ядро, проверяем, что он загрузился

**insmod xor.ko**

**lsmod | grep xor # проверяем наличие модуля в ядре**

**cat /proc/crypto #проверяем наличие шифра в списке шифров**

шифруем винт

**sudo cryptsetup -h=sha256 -c=xor -s=128 luksFormat /dev/sdd /mnt/boot/mykey**

сразу расшифровываем и монтируем в блочное устройство

**sudo cryptsetup -d=/mnt/boot/mykey luksOpen /dev/sda drivespace**

с помощью LVM разделим на логические разделы

**pvcreate /dev/mapper/drivespace**

**vgcreate vg /dev/mapper/drivespace**

**lvcreate -L1G -nswap vg**

**lvcreate -L6G -nroot vg**

**lvcreate -l 100%FREE -nhome vg**

форматируем в нужны ФС

**mkswap /dev/mapper/vg-swap**

**mkfs.ext4 /dev/mapper/vg-root**

**mkfs.ext4 /dev/mapper/vg-home**

для последующего переноса нам понадобится UUID sdc1 (раздел с ключом флэшки с ключом) и sdd (винт)

**ls -l /dev/disk/by-uuid >/mnt/flash/uuid.txt**

1. **Настройка системы**

Загружаемся с установочной флэшки и ставим систему туда, куда удобно обычными способами. Единственное убедиться, чтобы на раздел с ключом флэшки с ключом был смонтирован /boot раздел, grub поставлен на саму флэшку с ключом и присутствовал EFI system partition на этой флэшке.

Сразу загружаемся в ОС, нам надо подготовить и настроить её для переноса на шифрованный винт. Установим нужные пакеты и модули (нужен интернет).

**sudo su**

**apt-get -y install cryptsetup lvm2**

**insmod xor.ko**

**lsmod | grep xor # проверяем наличие модуля в ядре**

**cat /proc/crypto #проверяем наличие шифра в списке шифров**

правим **/boot/grub/grub.cfg**. Вместо

linux /vmlinuz-2.6.31-14-server root=UUID=9a651089-88fa-46d6-b547-38d3e10d4e67 ro quiet splash

пишем

linux /vmlinuz-2.6.31-14-server root=/dev/mapper/vg-root ro quiet splash

Правим **/etc/fstab**. Для /boot точку монтирования указать UUID раздела с ключом флэшки с ключом (берём из файла uuid.txt)

proc /proc proc defaults 0 0

UUID=eb7f5e37-b957-43dd-8af6-3c8983670df5 /boot ext2 defaults 0 2

/dev/mapper/vg-root / ext4 errors=remount-ro 0 1

/dev/mapper/vg-home /home ext4 defaults 0 1

/dev/mapper/vg-swap none swap sw 0 0

Правим **/etc/crypttab**. Вставить UUID шифрованного винта

drivespace UUID=090d14c1-e3c8-48e7-b123-6d9b8b2e502b /boot/mykey luks,cipher=xor

Далее надо подготовить initrd для работы с шифрованием. В файле **/etc/initramfs-tools/modules** добавляем:

dm\_mod

dm\_crypt

sha256

xor

Создаем файл **/etc/initramfs-tools/hooks/cryptokeys** с таким скриптом:

PREREQ=""

prereqs()

{

echo "$PREREQ"

}

case $1 in

prereqs)

prereqs

exit 0

;;

esac

if [ ! -x /sbin/cryptsetup ]; then

exit 0

fi

. /usr/share/initramfs-tools/hook-functions

mkdir ${DESTDIR}/etc/console

cp /boot/mykey ${DESTDIR}/etc/console

copy\_exec /sbin/cryptsetup /sbin

Создаем файл **/etc/initramfs-tools/scripts/local-top/cryptokeys** со скриптом:

PREREQ="udev"

prereqs()

{

echo "$PREREQ"

}

case $1 in *# get pre-requisites*

prereqs)

prereqs

exit 0

;;

esac

modprobe -b dm\_crypt

modprobe -b xor

modprobe -b sha256

while ! /sbin/cryptsetup -d=/etc/console/mykey luksOpen /dev/disk/by-uuid/090d14c1-e3c8-48e7-b123-6d9b8b2e502b drivespace; do

echo "Try again..."

done

Он выполнится в процессе загрузки initrd, загрузит нужные модули ядра и будет пытаться открыть наш зашифрованный винт с UUID=090d14c1-e3c8-48e7-b123-6d9b8b2e502b. Вам нужно вписать сюда свой UUID от зашифрованного винта.

Далее даём права на выполнения этим файлам и обновляем initramfs

**sudo chmod +x /etc/initramfs-tools/hooks/cryptokeys**

**sudo chmod +x /etc/initramfs-tools/scripts/local-top/cryptokeys**

**sudo update-initramfs -u -k all**

Смонтируем наш раздел с корневой фс в отдельную папку и упакуем на второй раздел флешки:

**mkdir /mnt/root && mount /dev/sda1 /mnt/root && cd /mnt/root**

**tar cfjv /mnt/flash/systembackup.tar.bz2 . *#НЕ ПРОПУСТИТЕ ТОЧКУ В КОНЦЕ СТРОКИ***

1. **Перенос системы**

Загружаемся с LiveCD, подключаем шифрованный винт, расшифровываем (может понадобится vgscan и vgmknodes, чтобы система увидела разделы), монтируем их и распаковываем архив с системой.

**sudo su**

**mkdir /mnt/flash**

**mount /dev/sdc2 /mnt/flash**

**cryptsetup -d=/mnt/flash/mykey luksOpen /dev/disk/by-uuid/090d14c1-e3c8-48e7-b123-6d9b8b2e502b drivespace**

**apt-get install lvm2**

***#vgscan && vgchange -a y && vgmknodes vg #Выполняем если система не увидела виртуальные разделы***

**mkdir /mnt/root**

**mount /dev/mapper/vg-root /mnt/root**

**mkdir /mnt/root/home**

**mount /dev/mapper/vg-home /mnt/root/home**

**cp /mnt/flash/systembackup.tar.bz2 /mnt/root && cd /mnt/root**

***#переносим архив на винт, для ускорения распаковки***

**tar xfvj systembackup.tar.bz2**

Всё готово