

Шифрование диска

Анастасия Полякова

Старший инженер безопасности в «Alibaba cloud»

Цели и задачи урока

Цель: рассмотреть функцию шифрования диска при установке с помощью LVM и dm-crypt, определить, для чего нужно использовать шифрование диска.

Зачем применять шифрование

Шифрование данных на устройстве - способ защиты от атак, связанных с доступом к устройству.

dm-crypt

dm-crypt — система ядра Linux, позволяющая создавать блочные устройства, шифрующие данные на лету.

Для работы с устройствами необходим ключ.

Как это выглядит

```
||-----OS-----||
||-Non-LVM-||-----LVM-----||
||  /boot  ||   LV-1 (/)   | LV-2 (swap)| LV 3 (/home) | LV-4 (/tmp)|| Logical Volumes(LV)
||          ||-----||-----||
||          ||           VG 1           |   VG 2   || Volume Groups(VG)
||          ||-----||-----||
||/dev/sda1|| /dev/sda2 |   /dev/sda3   | /dev/sdb2 | /dev/sdd4 || Physical Volumes(PV)
||-----||-----||
```

Полнодисковое шифрование

Стирание данных на SCSI3 (0,0,0), раздел #5 (sda)

0%

Для предотвращения утечки мета-информации шифрованного тома программа установки теперь перезаписывает SCSI3 (0,0,0), раздел #5 (sda) произвольными данными. Данный шаг можно пропустить, отменив действие, хотя это немного снизит стойкость шифрования.

<Отмена>

Ключевая фраза

[!!] Разметка дисков

Вам необходимо ввести ключевую фразу для шифрования SCSI3 (0,0,0), раздел #5 (sda).

Вся сила шифрования напрямую зависит от этой ключевой фразы, поэтому вы должны выбрать такую ключевую фразу, которую трудно угадать. Это не должно быть слово из словаря или фраза легко ассоциирующаяся с вами.

Хорошая ключевая фраза состоит из смеси символов, цифр и знаков пунктуации. Рекомендуется, чтобы ключевые фразы были длиной 20 или более символов.

Ключевая фраза для шифрования:

[] Показывать вводимый пароль

<Вернуться>

<Продолжить>

Полнодисковое шифрование

Стирание данных на SCSI3 (0,0,0), раздел #5 (sda)

0%

Для предотвращения утечки мета-информации шифрованного тома программа установки теперь перезаписывает SCSI3 (0,0,0), раздел #5 (sda) произвольными данными. Данный шаг можно пропустить, отменив действие, хотя это немного снизит стойкость шифрования.

<Отмена>

Выводы

Рассмотрели функцию шифрования диска при установке с помощью LVM и dm-crypt, определили, для чего нужно использовать шифрование диска.