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

Полнодисковое шифрование

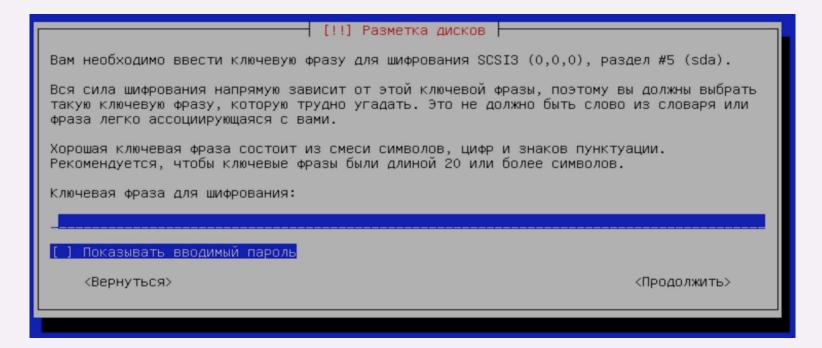
Стирание данных на SCSI3 (0,0,0), раздел #5 (sda)

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



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.