ЛАБОРАТОРНАЯ РАБОТА № 8
Шифрование дисков LUKS

Цель работы – Научится выполнять шифрование разделов/дисков, проводить мониторинг жестких дисков.

ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

1 Проверка работоспособности жесткого диска

Утилита smartmontools - предназначена для проверки состояния жестких дисков при помощи SMART (Self-Monitoring Analisys and Reporting Technology - в современных жестких дисках встроенный модуль самоконтроля S. M. A. R. T., который анализирует данные накопителя и помогает определить неисправность на первоначальной стадии). Так же может осуществлять проверку в постоянном режиме и оправлять уведомления по почте.

Smartmontools состоит из двух утилит — smartctl и smartd.

Подробнее о Smartmontools можно узнать на сайте разработчиков https://www.smartmontools.org/wiki/TocDoc

Для работы необходимо установить пакет:

sudo aptitude install smartmontools

Утилита **hdparm** предназначена для установки/получения различных параметров SATA/IDE устройств, к которым относятся жесткие диски. Утилита может установить объём кеш-памяти накопителя, перевести жёсткий диск в спящий режим, управлять питанием и акустикой и изменять настройки DMA. Обычно Hdparm применяется для оптимизации жёсткого диска, для повышения его производительности, активации многорежимности IDE.

Для работы необходимо установить пакет:

sudo aptitude install hdparm

2 Шифрование диска

Методы шифрования:

- шифрование на уровне файловой системы: eCryptfs, ENCfs
- блочное шифрование на уровне устройства: Loop-AES, TrueCrypt, dm-crypt+LUKS (Linux Unified Key Setup)

eCryptfs - это криптографическая файловая система Linux. Она хранит криптографические метаданные для каждого файла в отдельном файле, таким образом, что файлы можно копировать между компьютерами. Файл будет успешно расшифрован, если у вас есть ключ.

2. EncFS - обеспечивает шифрованную файловую систему в пространстве пользователя. Она работает без каких-либо дополнительных привилегий и использует библиотеку fuse и модуль ядра для обеспечения интерфейса файловой

системы. EncFS - это свободное программное обеспечение и она распространяется под лицензией GPL.

Loop-AES - быстрая и прозрачная файловая система, а также пакет для шифрования раздела подкачки в Linux.

TrueCrypt - это бесплатное решение с открытым исходным кодом для шифрования диска

dm-crypt+LUKS - dm-crypt - это прозрачная подсистема для шифрования диска, поддерживается шифрование целых дисков, съемных носителей, разделов, томов RAID, программного обеспечения, логических томов и файлов.

LUKS (Linux Unified Key Setup - протокол шифрования блочного устройства. Чтобы выполнить шифрование диска linux используется модуль ядра dm-crypt. Этот модуль позволяет создавать в каталоге /dev/mapper виртуальное блочное устройство с прозрачным для файловой системы и пользователя шифрованием. Фактически все данные лежат на зашифрованном физическом разделе. Если пользователь пытается записать данные на виртуальное устройство, они на лету шифруются и записываются на диск, при чтении с виртуального устройства, выполняется обратная операция - данные расшифровываются с физического диска и передаются в открытом виде через виртуальный диск пользователю. Обычно для шифрования используется метод AES, потому что под него оптимизированы большинство современных процессоров. Важно заметить, что вы можете шифровать не только разделы и диски, но и обычные файлы, создав в них файловую систему и подключив как loop устройство.

Алгоритм LUKS определяют какие действия и в каком порядке будут выполняться во время работы с шифрованными носителями. Для работы с LUKS и модулем dm-crypt используется утилита Cryptsetup.

Рисунок1 - Формат раздела LUKS

Утилита Cryptsetup предназначена для управления шифрованием дисков, с помощью которой можно:

- создавать шифрованные разделы LUKS;
- открывать/закрывать разделы LUKS;
- управлять слотами ключей;
- делать дамп заголовка LUKS и мастер-ключа.

Установка: sudo apt install cryptsetup

Синтаксис команды:
cryptsetup [опции] [операции] <параметры>

Операции, которые можно сделать с помощью этой утилиты:
luksFormat - создать зашифрованный раздел luks linux;
luksOpen - подключить виртуальное устройство (нужен ключ);
luksClose - закрыть виртуальное устройство luks linux;
luksAddKey - добавить ключ шифрования;

luksRemoveKey - удалить ключ шифрования;
luksUUID - показать UUID раздела;
luksDump - создать резервную копию заголовков LUKS.

В начале выполнения шифрования жесткого диска надо выполнить инициализацию раздела и установку пароля. При этом будет предупреждение об уничтожении данных:

```
administrator@rator:~$ sudo cryptsetup luksFormat /dev/sdd

WARNING!
========
This will overwrite data on /dev/sdd irrevocably.

Are you sure? (Type uppercase yes): YES
Enter passphrase:
Verify passphrase:
```

Далее необходимо открыть LUKS-том:

```
administrator@rator:~$ sudo cryptsetup luksOpen /dev/sdd disk1
Enter passphrase for /dev/sdd:
```

И теперь на разделе можно создать файловую систему и смонтировантъ ее.

Примечание. Один LUKS-раздел может открываться одним из 8 возможных ключей. А также можно использовать единственный ключ в одном слоте. Чтобы узнать состояние всех слотов, применяется команда: cryptsetup luksDump

Для добавления **нового ключа** LUKS на зашифрованный раздел используется команда: cryptsetup luksAddKey

При запросе «Enter any passphrase» требуется ввести один из уже имеющихся паролей для LUKS. Далее нужно ввести новый пароль, который займет новый слот соответственно (слот 1).

Чтобы **удалить** какой-то определенный **ключ** LUKS, надо знать парольную фразу одного из слотов, с помощью: cryptosetup luksKillSlot и проверить с помощью : cryptosetup luksDump.

Можно добавить бинарный ключ или записать пароль в текстовый документ и добавить к ключам (**добавление ключа из файла**). Для этого надо создать 256-битный ключ:

```
administrator@rator:~$ sudo dd if=/dev/random of=/my.key bs=1 count=256
256+0 записей получено
256+0 записей отправлено
256 байт скопировано, 240,125 s, 0,0 kB/s
```

и записать его в один из слотов.

После того, как закончена работа с секретными файлами на зашифрованном устройстве, надо размонтировать файловую систему и полностью закрыть диск.

```
administrator@rator:~$ sudo umount /disk1
administrator@rator:~$ ls /dev/mapper/disk1
/dev/mapper/disk1
administrator@rator:~$ sudo cryptsetup luksClose disk1
```

Обратите внимание, что после размонтирования директории, виртуальное устройство /dev/mapper/disk1 еще присутствует в системе.

Далее, в следующем сеансе работы с зашифрованным разделом, его нужно **открыть** с помощью ключа-пароля или с помощью ключа, записанного в файл.

Чтобы выполнить автоматическое монтирование раздела LUKS пользователь должен ввести пароль во время загрузки. В этом случае в файлы etc/fstab и etc/crypttab добавляется следующая информация:

```
administrator@rator:~$ cat /etc/crypttab
# <target name> <source device>         <key file>      <options>
disk1           /dev/sdd                none            luks

administrator@rator:~$ cat /etc/fstab
UUID=9a332120-6162-49f8-b884-67c78439fda7       /       ext4    errors=remount-ro,
usrquota,grpquota,secdelrnd=6     0  1
UUID=3af25722-abb9-4a4b-a045-51b5ad0f5e14  none  swap  sw  0  0
/dev/sr0  /media/cdrom0  udf,iso9660  user,noauto  0  0
/dev/mapper/disk1       /disk1  ext4    defaults        0 0
```

Так же можно смонтировать раздел с помощью ключа, который надо **хранить на отдельном носителе!** В этом случае в файле etc/crypttab нужно указать путь к ключу.

МЕТОДИКА ВЫПОЛНЕНИЯ

1 Проверка работоспособности жесткого диска

1. Проверить общее состояние диска с помощью smartctl.
2. Посмотреть дополнительную информацию по диску с помощью smartctl.
3. Выполнить расширенный тест диска с помощью smartctl.
4. Распечатать журналы ошибок диска с помощью smartctl.
5. Посмотреть информацию о диске с помощью утилиты hdparm.
6. Посмотреть текущие настройки для различных флагов диска с помощью утилиты hdparm.

2 Шифрование диска

1.Установите cryptsetup-luks
2. Создайте новый раздел на диске (можно использовать весь диск)
3. Отформатируйте раздел (диск) LUKS, например /dev/sdc1.
4. Подключите зашифрованный диск
5. Создайте файловую систему на подключенном диске
6. Создайте директорию для монтирования зашифрованного раздела и смонтируйте зашифрованный раздел в нее
7. Просмотрите список используемых ключей. Сколько свободных слотов для ключей присутствует?
8. Добавьте ключевую фразу к слоту
9. Добавьте ключевой файл
10. Разблокируйте зашифрованный раздел диска при помощи ключевого файла.
11. Удалите один из ключей
12. Чтобы операционная система сама научилась подключать и монтировать нужные криптованные устройства во время загрузки, а затем корректно отключать их во время останова системы, добавьте по одной строке в файлы /etc/crypttab и /etc/fstab:

vi /etc/crypttab

lkfs /dev/sda5 none luks,cipher=aes-cbc-essiv:sha256"
vi /etc/fstab
/dev/mapper/lkfs /mnt/lkfs ext4 defaults 0 0

Теперь во время каждой загрузки ОС будет спрашивать пароль для доступа к криптованному разделу, если он будет указан неправильно – загрузка остановится.

13. Выполните шифрование домашнего каталога.

Шифрование домашнего каталога производится по точно такой же схеме с тем лишь исключением, что перед добавлением новой записи в /etc/fstab следует удалить старую запись, ссылающуюся на /home.

14. Выполните шифрование флешки.

При создании шифрованной флешки специальные записи в /etc/crypttab и /etc/fstab не требуются. Подсистема HAL сама определит наличие на устройстве хранения LUKS-раздела и передаст эту информацию среде рабочего стола (Gnome, KDE, XFCE), которая, в свою очередь, выведет на экран окно с просьбой ввести пароль. Единственное, что необходимо сделать – при первом монтировании изменить права доступа на ее корневой каталог:

$ sudo chown -R student:student /media/usb_name
$ sudo chmod g+s /media/usb_nam

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. В каком файле необходимо указывать путь к ключу для автоматического монтирования зашифрованного раздела/диска?
2. Сколько слотов для хранения ключей содержит LUKS?
3. С помощью какой команды можно получить доступ к зашифрованному разделу/диску (открыть раздел/диск)?
4. Если вы планируете осуществлять мониторинг жестких дисков, какой пакет нужно установить?
5. Какая утилита ориентирована на работу со SCSI устройствами (включая SATA, IEEE1394 и USB)?
6. С помощью какой утилиты можно уменьшить шум от диска?