Защищаем ноутбуки с Linux. Шифрование, аутентификация по фингеру и возврат украденного

Алексей Кокин, Системный администратор, ЛК ГАЗ — Сергей Сокольников

Содержание статьи

- Физический доступ
- Шифрование диска
- Аутентификация по отпечатку пальца
  - Теория
  - Практика
- Настройка sudo
- Настройка ssh-agent на ssh
- Выводы

Первая, вполне логичная угроза для ноутбука — украдут. Вторая, не менее логичная — украдут, но не сразу, а сначала вскроют, чтобы посмотреть что в нем есть. Для борьбы с первой угрозой есть замки, для борьбы с второй — шифрование. Мы расскажем о том, что мы добавили к Linux, чтобы все наиболее ценное на наших ноутбуках было зашифровано, а также о том, как мы сделали, чтобы украденный ноутбук обнаружил, куда обратиться, и от кого прощения. Как и украсть такие украденные ноутбуки?

Читайте дальше, если вас это интересует.

Физический доступ

Начнем, как обычно с азов, а именно с того, что нужно выкрасить. Вы, прежде всего, должны, чтобы злоумышленник даже рядом не мог ноутбук использовать. Значит, прежде чем вскрывать ноутбук, злоумышленник должен сначала украсть ноутбук. Для борьбы с кражей ноутбуков мы используем замки с тросиком. Вариантов использования замков, чтобы привязать ноутбук к чему-нибудь — достаточно большое количество вариантов.

Существует такой очень распространенный. Злоумышленник приходит, он то, что интересует — видит, ноутбук, который к чему-то привязан, ему приходится с ним что-то делать, чтобы ноутбук украсть. Злоумышленник, даже обладающий определенной силой, ему это не нравится — он уходит. Но, к сожалению, не всегда. Бывает, что злоумышленник, обладающий определенной силой, ему это нравится, и он ноутбук все-таки украдет — приходит, берет замок, бросает, бросает, бросает, бросает, бросает, и ноутбук все-таки украдет.

Вторая линия защиты — мониторинг. Если замок злоумышленника украсть не смог, мы пытаемся его вычислить. Для этого мы используем такую вещь, как Prey. Prey — это такая программа, которая умеет определять, где ноутбук находится, и сообщать о нем. Prey умеет делать скриншоты, умеет определять координаты по wifi сетям, и если по координатам определяется, что ноутбук не в нашей зоне, то Prey начинает делать скриншоты, определять координаты и сообщать о ноутбуке.

Prey — это, к сожалению, не бесплатная вещь. Prey — это платная вещь. Prey — это платная вещь, которая стоит 9 долларов в месяц. Но, к сожалению, бесплатных аналогов, которые умеют делать то же самое, к сожалению, не существует. Prey — это, к сожалению, единственная вещь, которая умеет делать то, что мы хотим