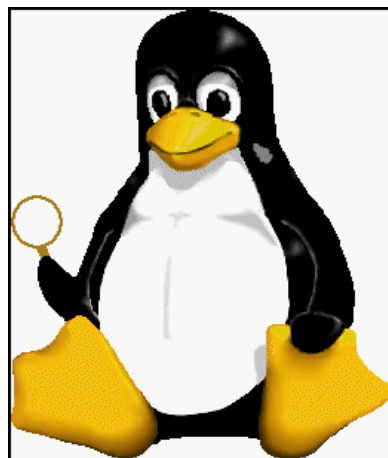


# Особенности применения ОС Linux при расследовании компьютерных инцидентов



Докладчик: Суханов Максим  
ITDefence

# Почему Linux?

---

Ключевые преимущества:

- Открытый исходный код и свободные лицензии;
- Большое количество бесплатного специализированного ПО;
- Возможность программной блокировки записи на любые носители информации.

# Решаемые задачи

---

- Клонирование содержимого компьютерных носителей информации;
- Предварительное исследование содержимого компьютерных носителей информации;
- Полное исследование содержимого компьютерных носителей информации.

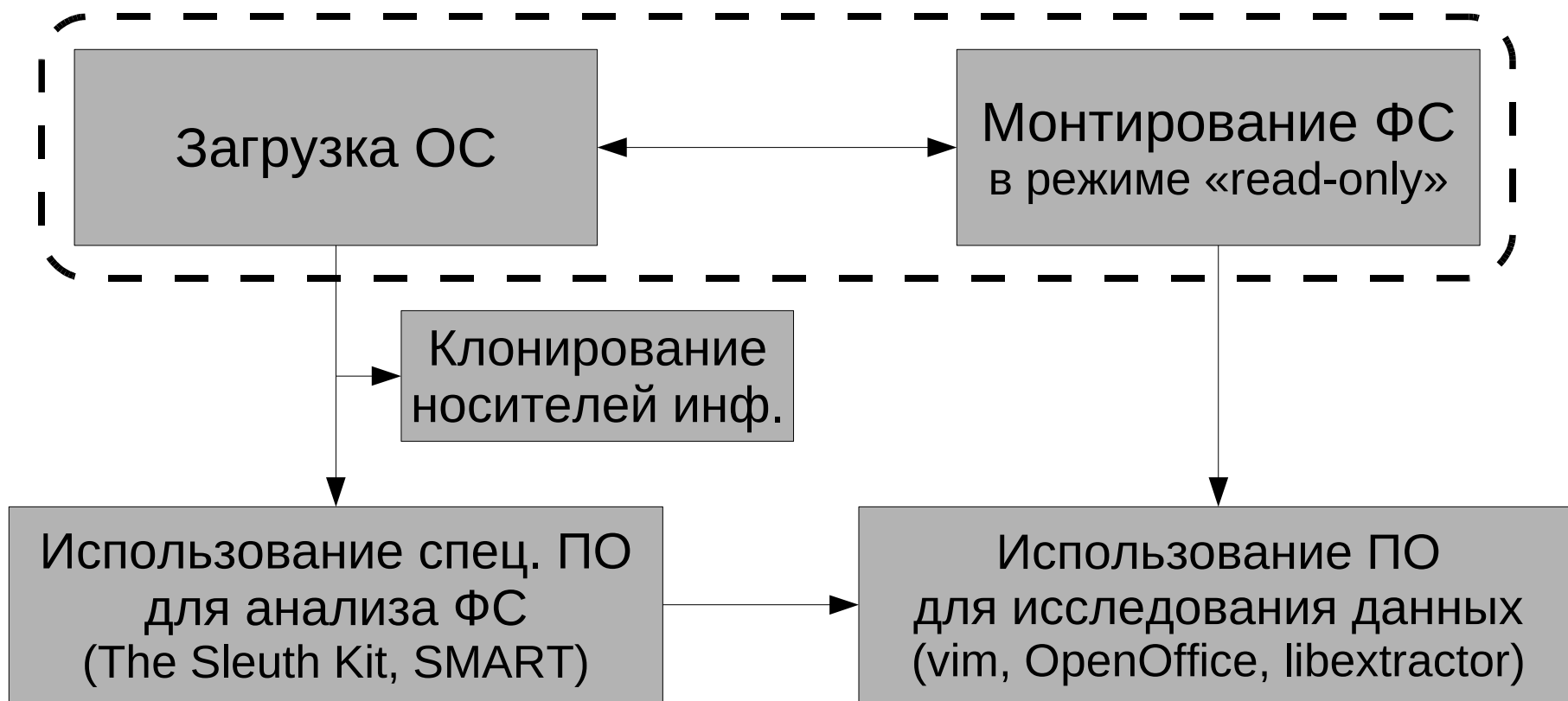
# Судебные дистрибутивы Linux

---

Наиболее популярные:

- Helix3 и Helix3 Pro (<http://e-fense.com>);
- DEFT Linux (<http://deftlinux.net>);
- CAINE (<http://caine-live.net>);
- grml (<http://grml.org>);
- Raptor (<http://www.raptorforensics.com>);
- SMART Linux (<http://asrdata.com>);
- И другие: SPADA, BackTrack, LinEn Boot CD, FCCU GNU/Linux Forensic Boot CD, The FBCD.

# Проблемы судебных дистрибутивов Linux: модель



# Наиболее распространенные проблемы судебных дистрибутивов Linux

---



- Некорректный метод монтирования исследуемых ФС;
- Подмена корневой ФС в процессе загрузки (выполнение произвольного кода);
- Активация пространства подкачки (swap space);
- Некорректные политики монтирования
  - а) HAL;
  - б) Скрипт: scanpartitions.

# Методы монтирования файловых систем с блокировкой записи

---

~~0. mount -o ro /dev/sda1 /mnt/sda1~~

1. Блочные устройства в режиме «только чтение»:

blockdev --setro /dev/sda1 или hdparm -r1 /dev/sda1

Далее: mount /dev/sda1 /mnt/sda1

2. Устройства обратной связи в режиме «только чтение»:

mount -o ro,loop /dev/sda1 /mnt/sda1

3. Различные «трюки»:

mount -t ext2 -o ro /dev/sda1 /mnt/sda1 (для Ext3 и Ext4)

# Проверка перечисленных методов

---

- Способ #1: ATA over Ethernet

Суть способа: перехват команд ATA с помощью Wireshark;

- Способ #2: отладка I/O

Команда: `sysctl vm.block_dump=1`

Все команды чтения и записи добавляются в лог (dmesg).

# Результаты проверки

---

- Блочные устройства в режиме «только чтение»: метод работает, но драйвер ФС может отправлять команды записи (например, при размонтировании XFS);
- Устройства обратной связи в режиме «только чтение»: метод работает.

# Наиболее распространенные проблемы судебных дистрибутивов Linux

---

- Некорректный метод монтирования исследуемых ФС;
- ➔ • Подмена корневой ФС в процессе загрузки (выполнение произвольного кода);
- Активация пространства подкачки (swap space);
- Некорректные политики монтирования
  - а) HAL;
  - б) Скрипт: scanpartitions.

# Подмена корневой ФС в процессе загрузки

---

Процесс загрузки ОС Linux с CD/DVD/USB Flash:

*BIOS → загрузчик → initrd → код на корневой ФС → ...*

Скрипты `initrd` «не знают» адрес устройства с корневой ФС!

# Подмена корневой ФС в процессе загрузки

---

Особенности скриптов Casper (используются в Ubuntu; клон — live-initramfs для Debian):

- Поиск корневой ФС производится по всем доступным устройствам по заданной маске («\*.squashfs») с необязательной сверкой UUID:
  - Монтирование только с опцией «-o ro»;
  - Нет проверки подлинности обнаруженной ФС.

# Подмена корневой ФС в процессе загрузки

---

## Особенности скриптов Casper:

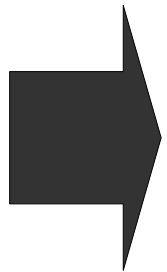
- «Грязный хак»: если `udev` не распознает выбранное устройство как устройство `USB/IDE/SCSI` и на нем нет таблицы разделов, то ФС монтируется в качестве корневой без каких-либо проверок.

# Подмена корневой ФС в процессе загрузки

---

Проверка подлинности корневой ФС отсутствует в загрузочных скриптах KNOPPIX и Debian Live!

Скрипты initrd могут выбрать для продолжения загрузки образ корневой ФС на исследуемом НЖМД.



Возможность подмены корневой файловой системы присутствует в большинстве судебных дистрибутивов Linux!

# Скриншот

Welcome to



grml.org - Linux for sysadmins and texttool users.

```
* Running grml 2009.10 Release Codename Hello-Wien [2009-10-31]
* Finished early booting sequence. [ ok ]
* Searching for GRML file, this might take a few seconds...
* Setting device /dev/sda to read-only mode: done [ execute "blockdev --setrw /dev/sda " to unlock]
* Setting device /dev/sda1 to read-only mode: done [ execute "blockdev --setrw /dev/sda1" to unlock]
* Setting device /dev/sda2 to read-only mode: done [ execute "blockdev --setrw /dev/sda2" to unlock]
* Setting device /dev/sdb to read-only mode: done [ execute "blockdev --setrw /dev/sdb " to unlock]
* Setting device /dev/sdb1 to read-only mode: done [ execute "blockdev --setrw /dev/sdb1" to unlock]
  -> Mounted live system on /dev/sdb1
mount: mounting /dev/sda1 on /live/image failed: Invalid argument
/scripts/live-bottom/23networking: line 44: can't create /root/etc/network/interfaces: nonexistent directory
EVIL CODE EXECUTED! xD
```

Try another forensic Live CD...

# Наиболее распространенные проблемы судебных дистрибутивов Linux

---

- Некорректный метод монтирования исследуемых ФС;
- Подмена корневой ФС в процессе загрузки (выполнение произвольного кода);
- ➔ • Активация пространства подкачки (swap space);
- Некорректные политики монтирования
  - а) HAL;
  - б) Скрипт: scanpartitions.

# Активация пространства подкачки

---

- Активация в процессе загрузки;
- Блокировка записи через `blockdev` (или `hdparm`) после активации не работает!

Судебные дистрибутивы Linux уже давно не активируют пространство подкачки, но...

- Старые версии Raptor пытались заблокировать запись на активированный `swap`.

# Наиболее распространенные проблемы судебных дистрибутивов Linux

---

- Некорректный метод монтирования исследуемых ФС;
- Подмена корневой ФС в процессе загрузки (выполнение произвольного кода);
- Активация пространства подкачки (swap space);
- Некорректные политики монтирования
  - а) HAL;
  - б) Скрипт: scanpartitions.



# Некорректные политики монтирования

---

- Отсутствуют правила HAL для отключения автомонтирования MMC.

Дистрибутив: Helix3 2009R1;

- Скрипт *scanpartitions* игнорирует устройства MMC (монтирование в режиме «r/w») и другие «экзотические» устройства (/dev/sdad):

- Поиск блочных устройств по некорректным маскам («/dev/?d?», а не «/dev/?d\*»).

Дистрибутивы: Helix3 2009R1, Helix3 Pro 2009R3, CAINE 0.5

---

# Выводы

---

- Судебные дистрибутивы Linux плохо тестируются;
  - Большинство «особенностей» применения ОС Linux в судебной практике держатся в секрете;
  - Заблуждение: «разработчик знает всё».
  
  - Необходимо продолжать исследования: какие есть особенности при работе с Linux RAID и LVM?
  - Необходимо поддерживать архивы данных, предназначенных для тестирования судебного ПО:  
<http://digitalcorpora.org>
-

# Вопросы?

---

Где можно задать вопрос по теме доклада?



- Здесь и сейчас;
- На форуме проекта КТЭ:  
<http://computer-forensics-lab.org>
- [fuf@itdefence.ru](mailto:fuf@itdefence.ru)