Linux для судебных экспертов: проблемы загрузки доверенной системы

Автор: Суханов Максим

ITDefence.Ru

Введение

Данная работа является продолжением цикла статей «Linux для судебных экспертов» и раскрывает проблемы, возникающие в процессе загрузки некоторых судебных дистрибутивов на основе Ubuntu (Debian).

Процесс загрузки операционных систем на основе Ubuntu

Процесс загрузки дистрибутивов на основе Ubuntu происходит в несколько этапов (на примере загрузки с CD):

1. На начальном этапе загрузки компьютера происходит выполнение кода BIOS с последующей передачей управления загрузчику (например, GRUB);

2. Загрузчик, в свою очередь, передает управление ядру Linux, которое распаковывает образ initrd и передает управление скрипту */init*, который находится в распакованном образе;

3. Скрипт */init* производит запуск различных скриптов Casper, которые производят поиск блочного устройства, на котором расположена корневая файловая система (как правило, в упакованном виде). Для этого скрипты Casper определяют тип файловой системы на выбранном блочном устройстве; в случае, если данный тип файловой системы поддерживается системой инициализации, происходит монтирование ФС в каталог /cdrom; затем производится поиск упакованного файла-образа корневой ФС с опциональной сверкой UUID смонтированной файловой системы;

4. Скрипт */init* монтирует корневую файловую систему в каталог /root и передает управление программе */root/sbin/init*, которая производит дальнейшие операции для завершения загрузки системы (настройка окружения пользователя, запуск скриптов инициализации сервисов и т.п.) и переводит систему на определенный «уровень выполнения».

Аналогичным образом работает система инициализации Live, используемая в дистрибутиве grml (на основе Debian).

Особенности работы скриптов Casper (Live)

Для поиска блочного устройства, на котором расположена корневая файловая система, скрипты Casper (Live) могут производить монтирование файловых систем *на исследуемых носителях информации* с использованием опции «-o ro». В некоторых случаях это может привести к изменению содержимого смонтированных файловых систем (более подробно см. предыдущую работу).

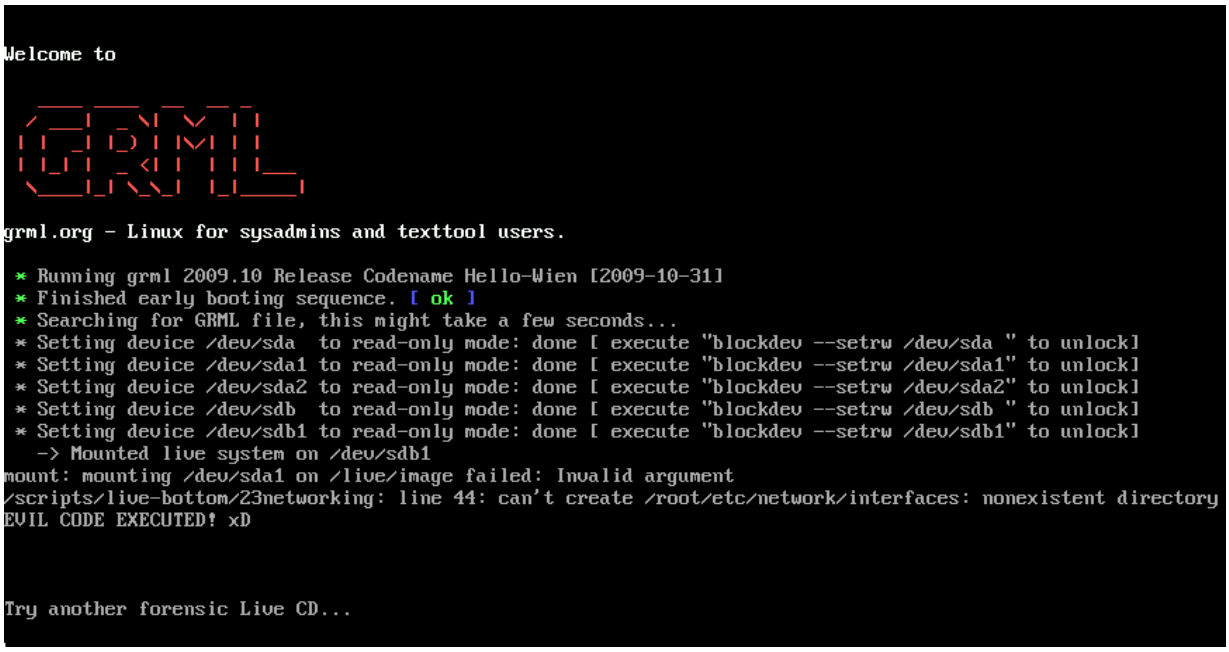
Обнаружение файла-образа корневой ФС происходит путем поиска файлов, имеющих заданную маску (например, «*.squashfs»), в определенной директории (например, «/cdrom/casper»). В случае, если файл с расширением «.squashfs» обнаружен, происходит опциональная сверка значений UUID в файле /cdrom/.disk/casper-uuid-generic (данный файл расположен в смонтированной файловой системе с образом корневой ФС) и /conf/uuid.conf (данный файл расположен в образе initrd).

Далее происходит монтирование корневой файловой системы и передача управления программе *init*.

Подмена загружаемой операционной системы

Отсутствие каких-либо процедур проверки подлинности файла-образа корневой файловой системы (за исключением проверки UUID) создает возможность подмены загружаемой ОС.

К примеру, в процессе загрузки операционной системы скрипты Casper могут смонтировать корневую файловую систему из файла-образа, расположенного на исследуемом носителе информации; данная корневая ФС может содержать в себе программу */sbin/init*, которая перезапишет определенные данные на исследуемых носителях.



Подмена корневой ФС в процессе загрузки grml

(корневая ФС в данном случае расположена не на CD,

а на одном из разделов НЖМД)

Судебные дистрибутивы Linux, в которых отсутствует проверка подлинности корневой ФС

Дистрибутив	Веб-сайт
Helix3 Pro 2009R2	http://www.e-fense.com/helix3pro.php
Helix3 2009R1	http://www.e-fense.com/helix3-download.php
CAINE 1.5	http://www.caine-live.net/
DEFT Linux 5	http://www.deftlinux.net/
Raptor 20091026	http://www.raptorforensics.com/
SMART Linux (Ubuntu) 2009-11-11	http://asrdata2.com/
grml 2009.10	http://grml.org/
BackTrack 4 Pre	http://remote-exploit.org/

Способы устранения возможности подмены ОС

Для устранения возможности подмены корневой файловой системы (и, следовательно, загружаемой операционной системы) можно:

1. Отказаться от использования системы Casper;
2. Сделать проверку UUID обязательной: данное решение оптимально для коммерческих судебных дистрибутивов Linux, т.к. в этом случае фальсификация используемого UUID маловероятна из-за отсутствия подобных дистрибутивов в свободном доступе;
3. Проверять подлинность файла-образа корневой ФС с использованием криптографических хеш-функций (существенно увеличивает длительность загрузки ОС).

Выводы

В ходе тестирования было обнаружено, что все популярные судебные дистрибутивы на основе Ubuntu (Debian) не могут гарантировать возможность успешной загрузки доверенной специализированной среды. Хотя вероятность встретить противодействие криминалистическому исследованию носителей информация подобного рода очень мала, разработчики судебных дистрибутивов Linux должны принять меры для организации проверки подлинности корневой файловой системы в процессе загрузки.