Защищенные информационные системы на основе Linux

РусКрипто'2008
6 апреля 2008

Алексей Васюков, RHCE
Консультант / VDEL
www.vdel.ru

План

- Способы контроля доступа и защиты от НСД
  - ✓ Дискреционный и мандатный контроль доступа
  - ✓ Защита данных при физическом доступе
- Управление большой инфраструктурой. Средства централизации управления.
- Сертификации Red Hat Enterprise Linux (RHEL) в области ИБ.

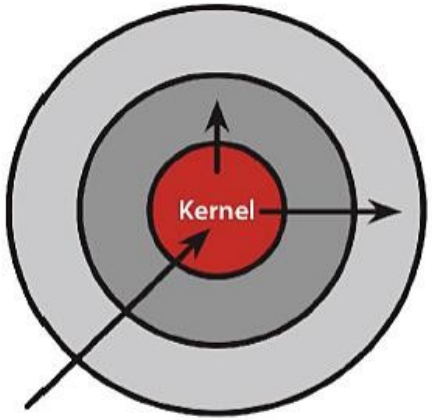
Способы контроля доступа и защиты от НСД

Контроль доступа в Linux

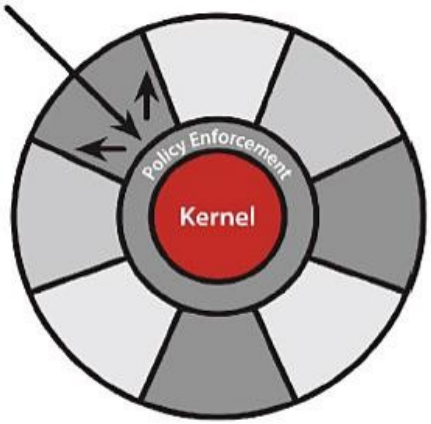
- Стандартная модель основана на дискреционном контроле доступа (DAC) и следует традициям UNIX
  - ✓ Права доступа к файлам устанавливаются для пользователей и групп
  - ✓ Привилегированные операции требуют полномочий администратора
  - ✓ Изоляция процессов в стиле UNIX
- Достаточна ли стандартная модель?
  - ✓ Гибкость ограничена контролем пользователя / группы. Все процессы одного пользователя имеют равные полномочия.
  - ✓ Права доступа к файлам задаются их владельцем. Невозможно ограничить риск ошибки или преднамеренных враждебных действий пользователя.
  - ✓ Администратор имеет полный доступ к системе. Успешная атака на приложение, исполняющееся с правами администратора, приводит к захвату контроля над всей системой

Мандатный контроль доступа

- Реализуется с помощью SELinux
  - ✓ SELinux — подсистема в стандартном ядре Linux, это не отдельная версия Linux.
  - ✓ Дополнение к DAC, не замена.
  - ✓ Приложения не требуют модификации.
- Основа SELinux — политика: целевая на основе MCS, строгая на основе MCS, строгая на основе MLS



Дискреционный контроль доступа
Атакующий, получивший привилегии, имеет полный доступ к системе.



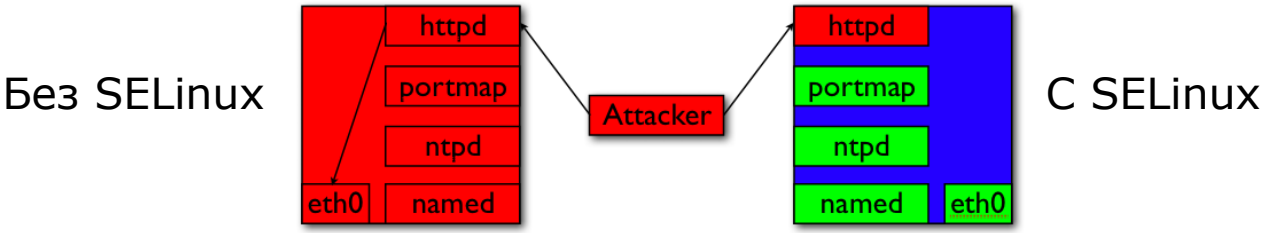
Мандатный контроль доступа
Приложения изолированы. Атакующий ограничен в своих действиях.

Мандатный контроль доступа

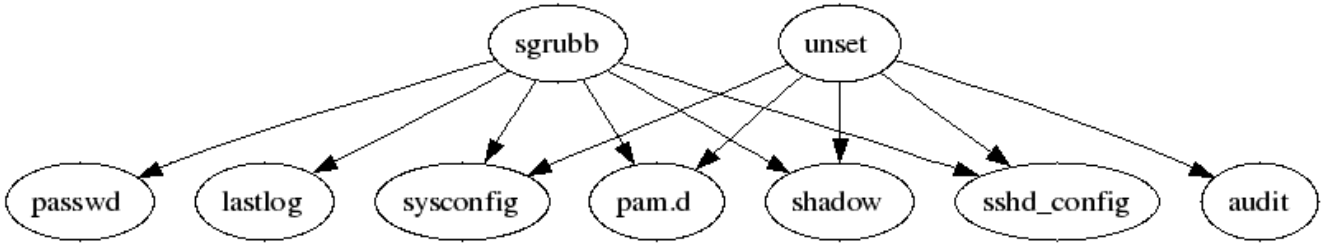
- Разграничение доступа, заданное политикой безопасности, не может быть обойдено
  - ✓ Устраняет последствия ошибок или враждебных действий пользователя — невозможно разрешить то, что запрещено политикой.
  - ✓ Ограничивает последствия некорректной настройки сервисов или наличия в них уязвимостей — невозможно получить доступ к тем частям системы, к которым не имел доступа атакованный сервис.
  - ✓ Ограничивается роль «всесильного администратора системы». Возможно наличие нескольких администраторов, имеющих разные полномочия, в том числе на доступ к данным.
- Ограничение возможных последствий сбоев приложений и других средств защиты
- Централизация политики безопасности

Контроль и аудит

- SELinux – реализация мандатного контроля доступа
  - ✓ Ограничивает последствия ошибок пользователей
  - ✓ Ограничивает последствия уязвимостей в сервисах
  - ✓ Позволяет значительно строже разграничить доступ к данным



- Audit – отслеживание и анализ всех событий в системе
  - ✓ Использование программ пользователями, системные вызовы программ, обращение к файлам и т.д



Защита данных при физическом доступе

- Ноутбуки, флеш-диски, украденный жесткий диск — системы разграничения доступа бесполезны
- LUKS — открытый стандарт в области шифрования дисков
  - ✓ Работает через device-mapper
  - ✓ Полностью прозрачен для приложений
  - ✓ Позволяет шифровать разделы данных, системный раздел, своп-разделы, тома LVM
  - ✓ Ключи могут как вводиться с клавиатуры, так и храниться, например, на флеш-диске или генерироваться во время старта системы (SWAP)
  - ✓ За счет низкоуровневой реализации потери производительность минимальны по сравнению с аналогами, работающими в пространстве пользователя (userspace)
- Изначально LUKS ориентирован на Linux, но существует реализация под Windows

Управление большой инфраструктурой
Средства централизации управления

Централизация управления

- Централизация управления пользователями – LDAP
  - ✓ Единое хранилище для всей информации о пользователях
  - ✓ Интеграция с Active Directory, возможна синхронизация в обе стороны (в некоторых реализациях)
- Централизация управления инфраструктурой
  - ✓ Linux — изначально сетевая ОС, рассчитанная на централизованное администрирование
  - ✓ Система штатными средствами позволяет:
    - Централизованное ведение системных журналов (логов) всех машин сети и централизованный аудит
    - Централизованное задание и применение настроек системы и всех приложений
    - Мониторинг распределенной структуры (SNMP)

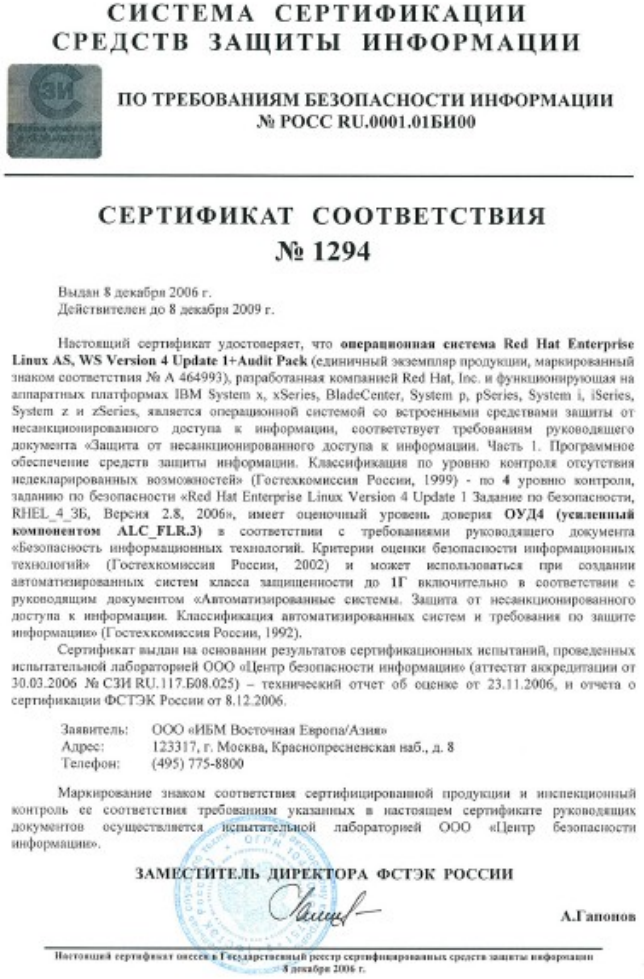
Сертификации RHEL в области ИБ

Сертификации RHEL

- Сертифицированы RHEL4 AS и RHEL4 WS на всех аппаратных платформах IBM.

- Международная сертификация
  - ✓ CAPP/EAL4+
- Российская сертификация (ФСТЭК)
  - ✓ ОУД4 (усиленный) / НДВ4

- Жизненный цикл сертификата:
  - ✓ RHEL4 Update 1 + Audit Pack — до 11 апреля 2010 года
  - ✓ RHEL4 Update 4 — в процессе сертификации в настоящее время



СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 1294

Выдан 8 декабря 2006 г.
Действителен до 8 декабря 2009 г.

Настоящий сертификат удостоверяет, что **операционная система Red Hat Enterprise Linux AS, WS Version 4 Update 1+Audit Pack** (единичный экземпляр продукции, маркированный знаком соответствия № А 464993), разработанная компанией Red Hat, Inc. и функционирующая на аппаратных платформах IBM System x, xSeries, BladeCenter, System p, pSeries, System i, iSeries, System z и zSeries, является операционной системой со встроенными средствами защиты от несанкционированного доступа к информации, соответствует требованиям руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) - по **4** уровню контроля, заданию по безопасности «Red Hat Enterprise Linux Version 4 Update 1 Задание по безопасности, RHEL_4_ЗБ, Версия 2.8, 2006», имеет оценочный уровень доверия **ОУД4 (усиленный компонентом ALC_FLR.3)** в соответствии с требованиями руководящего документа «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» (Гостехкомиссия России, 2002) и может использоваться при создании автоматизированных систем класса защищенности до **1Г** включительно в соответствии с руководящим документом «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (Гостехкомиссия России, 1992).

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ООО «Центр безопасности информации» (аттестат аккредитации от 30.03.2006 № СЗИ RU.117.Б08.025) – технический отчет об оценке от 23.11.2006, и отчета о сертификации ФСТЭК России от 8.12.2006.

Заявитель: ООО «ИБМ Восточная Европа/Азия»
Адрес: 123317, г. Москва, Краснопресненская наб., д. 8
Телефон: (495) 775-8800

Маркирование знаком соответствия сертифицированной продукции и инспекционный контроль ее соответствия требованиям указанных в настоящем сертификате руководящих документов осуществляется испытательной лабораторией ООО «Центр безопасности информации».

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ А.Гапонов

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации 8 декабря 2006 г.

Спасибо за внимание!

www.vdel.ru
www.redhat.com

Вопросы?

Алексей Васюков
vasyukov@vdel.ru