А. С. Николаев, В. Н. Федосеев
ФГУП «НИИ НПО «Луч», Подольск

РАСШИРЕНИЕ ТРЕБОВАНИЙ БЕЗОПАСНОСТИ В ПРОГРАММНОЙ ПЛАТФОРМЕ ЯНУКС 3.0

В работе представлены результаты разработки расширенных функциональных требований безопасности, связанных с технологией виртуализации, а также усиленных требований доверия к безопасности, направленных на обеспечение процесса устранения недостатков, обнаруживаемых на этапе эксплуатации жизненного цикла программной платформы масштаба предприятия Янукс 3.0.

Вычислительная мощность современных компьютеров быстро растет. Современные многоядерные системы как нельзя лучше позволяют реализовать богатейший потенциал технологии виртуализации, выводя удобство и безопасность обработки информации на качественно новый уровень.

Программная платформа масштаба предприятия Янукс 3.0 представляется собой свободный дистрибутив GNU/Linux, построенный на основе коммерческого продукта RedHat Enterprise Linux 5.1.

Действующие спецификации «Общих критериев» [1] не содержат функциональных требований к подсистеме виртуализации операционной системы. В рамках процесса разработки программной платформы Янукс 3.0 были расширены требования руководящего документа ФСТЭК, описывающего функциональные требования безопасности [2], в отношении разделения доменов виртуальных машин. В задание по безопасности, построенное на основе «Профиля защиты с контролируемым доступом» [3], были добавлены следующие функции безопасности, связанные с виртуализацией:

- поддержка ФБО домена безопасности для выполнения каждой виртуальной машины, защищающей виртуальную машину от вмешательства и воздействия со стороны недоверенных субъектов или субъектов, внешних по отношению к данной виртуальной машине;
- проведение ФБО разделения между доменами безопасности виртуальных машин в пределах ОДФ.

Помимо этого, были усилены требования руководящего документа ФСТЭК, определяющего требования доверия к безопасности [4], связанные с поддержкой жизненного цикла программного обеспечения. Задание по безопасности было усилено компонентом ALC_FLR.1 «Базовое устранение недостатков». Усиление требований направлено на разрешение проблем с устранением недостатков, которые могут быть выявлены в процессе эксплуатации Янукс 3.0. Для обеспечения данного требования разработаны и реализованы процедуры устранения недостатков, включающие в себя:

- поиск и идентификацию недостатков;
- анализ и исправление недостатков;
- распространение информации об исправлениях.

Следует отметить, что расширенные требования безопасности, предъявляемые к Янукс 3.0, позволяют пользователю устанавливать и обновлять состав программного обеспечения программной платформы недоверенными компонентами, если они удовлетворяют следующим условиям:

- не предназначены для запуска от имени суперпользователя;
- не имеют установленных битов SUID/SGID от имени суперпользователя.

Программная платформа масштаба предприятия Янукс 3.0 является первым российским дистрибутивом GNU/Linux, сертифицированным по «Общим критериям». Сертификат ФСТЭК № 1651 от 23.07.2008, уровень сертификации — ОУД3+, уровень контроля отсутствия недекларированных возможностей [5] — 4. Программная платформа Янукс 3.0 может использоваться для создания автоматизированных систем до класса защищенности 1Г включительно.

СПИСОК ЛИТЕРАТУРЫ:

1. ГОСТ Р/ИСО МЭК 15408-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Госстандарт России.
2. Гостехкомиссия России. Руководящий документ. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. 2002 г.
3. Центр безопасности информации. Безопасность информационных технологий. Контролируемый доступ. Профиль защиты (первая редакция). 2002 г.
4. Гостехкомиссия России. Руководящий документ. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. 2002 г.
5. Гостехкомиссия России. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. 1999 г.

В. В. Платонов
Санкт-Петербургский государственный политехнический университет

ЭЛЕМЕНТЫ МЕТОДОЛОГИИ ПОСТРОЕНИЯ СИСТЕМ ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК

Системы обнаружения сетевых атак и вторжений (СОВ) играют важную роль в обеспечении защиты информации в кооперативных сетях, поэтому все большее число публикаций посвящено разработке моделей и подходов к обнаружению злоупотреблений. К системам обнаружения вторжений предъявляются достаточно жесткие требования, в качестве основных из них можно выделить следующие: высокая пропускная способность и минимальные ошибки первого и второго рода.

Исследования показали необходимость использования модульного подхода для повышения качества и производительности СОВ [1]. Данный подход можно назвать «псевдомодульным». В работе предлагается модульный подход, в котором каждый модуль предназначен для обнаружения атак определенного класса. Основные этапы методологии построения СОВ включают в себя:

- определение параметров классов обнаруживаемых сетевых атак;
- выбор состава анализируемых параметров для каждого класса атак;
- выбор моделей обнаружения;
- построение модулей обнаружения на основе выбранных моделей обнаружения;
- проведение тестовых испытаний модулей обнаружения (с учителем или без учителя);
- оценку параметров обнаружения;
- сокращение размерности анализируемых данных без снижения значений параметров обнаружения;
- построение модулей принятия решения.

В качестве примера построения модулей обнаружения рассматриваются методы опорных векторов, которые показали свое превосходство по сравнению с нейронными сетями.

Проведенный анализ позволяет утверждать, что выделение наиболее значимых параметров для обнаружения заданного класса атак позволяет улучшить параметры обнаружения и, в свою очередь, повышает быстродействие системы обнаружения.