СРЕДСТВА АНАЛИЗА ЗАЩИЩЕННОСТИ КОРПОРАТИВНЫХ СЕТЕЙ

Д. А. Набатчиков
Самарский государственный университет путей сообщения, г. Самара

В России сейчас наблюдается бум на системы аудита защищенности. Некоторые из них предназначены только для одной операционной системы (как правило UNIX), другие требуют очень глубоких знаний архитектуры сети и ОС (например, бесплатно распространяемый продукт SATAN), третьи предназначены для тестирования только одной из уязвимостей сети (например, Crack) [3]. Поэтому наибольший практический интерес представляют продукты нового поколения, к которым относятся сканеры безопасности

Если раньше у нас были известны только западные решения – Internet Scanner, Retina, LAN Guard и т.п., то сейчас интерес к разработке этого класса средств защиты проснулся и у российских производителей: РНТ со своим «Стилетом», ЦБИ с «Ревизором Сети», Элвис+ с «Заставой-Инспектором».

«Сканеры безопасности» (security scanners), появившиеся в результате совершенствования таких средств, как SATAN, анализируют данные о настройке системы безопасности, а затем, используя собственный алгоритм проверки, определяют имеющиеся «дыры» в системе безопасности или недостатки ее конфигурации.

Существует два основных механизма проверки сканером наличия уязвимостей [2]:

- сканирование (scan) – механизм пассивного анализа по косвенным признакам, без фактического подтверждения ее наличия;
- зондирование (probe) - механизм активного анализа путем имитации атаки, использующей проверяемую уязвимость.

Указанные механизмы проверки сканером реализуются следующими методами:

- "Проверка заголовков" (banner check) - вывод об уязвимости делается на основе информации в заголовке ответа на запрос сканера (уточняется версия опрашиваемой программы и на основе этих данных делается вывод о наличии в них уязвимости – прим. неточный метод).
- "Активные зондирующие проверки" (active probing check) – основаны на сравнении фрагмента программного обеспечения со слепком известной уязвимости (по принципу антивирусных систем).
- "Пробные атаки" (exploit check) – против подозрительного сервиса или узла запускаются реальные атаки

Одним из самых популярных анализаторов безопасности является проект Nessus [1]. Nessus обеспечивает проверку на наличие более 300 уязвимостей сетевых компьютеров, работающих под управлением Unix или Windows NT систем,а также маршрутизаторов. Nessus представляет собой бесплатный современный сканер безопасности локальных и удаленных систем. Задачей Nessus является определение работающих сервисов и уязвимых мест, включая самые последние сообщения о дырах wu-ftpd, наличия демонов DDoS, проблемы ipfw FreeBSD и многие другие.

Не менее интересный продукт представен на рынке специалистами фирмы Positive Technologies. Сканер уязвимостей XSpider является средством автоматизированного анализа защищенности и обнаружения уязвимостей информационных систем, обрабатывающих данные, не содержащие сведений, составляющих государственную тайну. XSpider соответствует требованиям технических условий, а также требованиям 2-го уровня контроля отсутствия недекларированных возможностей [1].

В самое ближайшее время будут востребованы услуги, связанные с удаленным анализом защищенности. Не всегда имеется возможность приобрести сканер безопасности для себя (нет денег, нет людей, нет времени), но анализировать защищенность как-то надо. И тут на помощь приходит услуга удаленного сканирования [5]. Ярким примером является сервис «Проверь здоровье своей сети», запущенный компаниями Cisco Systems и Positive Technologies

Таким образом, рассмотренные технологии направлены на решение одной единственной задачи – анализ защищенности информационных ресурсов во всех его аспектах и устранение обнаруженных проблем. Именно подчиненность этой задаче позволяет объединять все эти технологии в единый класс защитных средств – vulnerability management. Они ни в коем случае не заменяют специалистов в области безопасности. Они всего лишь автоматизируют их работу, помогая быстро проверить сотни узлов, в т.ч. и находящихся на других территориях, помогут обнаружить практически все известные уязвимости и порекомендовать меры, их устраняющие.

Список использованных источников

1. Долгин А. А., Хореев П. Б. Разработка сканера уязвимостей компьютерных систем на основе защищенных версий ОС Windows. Труды международной научно-технической конференции «Информационные средства и технологии», том 2, М., 2005.- С. 76-78.

2.Хорев П. Б. Методы и средства защиты информации в компьютерных системах. - М., Издательский центр «Академия», 2005. - 256 с.

3. Зима В. М., Молдовян А. А., Молдовян Н. А., Безопасность глобальных сетевых технологий, СПб.: БХВ-Петербург, 2000. 320 с.

4 Бармен С., Разработка правил информационной безопасности, М., Вильямс, 2002. - 208 с.

5. Левин В.К. Защита информации в информационно-вычислительных системах и сетях / Программирование, 2004.-№5.- С. 5-16.

ПУТИ РЕШЕНИЯ ПРОБЛЕМ ВИБРОИСПЫТАНИЙ ТЕСТОВЫХ БЛОКОВ

А.В. Наседкин
Самарский государственный аэрокосмический университет, г. Самара

Исследование динамики сложных механических систем, подвергающихся действию ударных и вибрационных нагрузок, особенно при создании и разработке образцов ракетно-космической техники, является одной из наиболее быстро развивающихся областей прикладной механики.

Одной из важнейших проблем, связанных с поведением конструкций при динамических воздействиях, является решение задачи моделирования поведения паяного соединения в электронных сборках с поверхностно монтируемыми элементами, при изготовлении которых используется комбинированный метод (пайка свинецсодержащим припоем элементов с бессвинцовым покрытием выводов на печатные платы с бессвинцовым финишным покрытием). Это объясняется тем, что данный вид монтажа в аэрокосмической отрасли в России имеет малый опыт практического применения. Не последнюю роль играет и повышение динамических нагрузок за счет увеличения мощности и расширения диапазона воздействия ракетоносителя.

Одной из областей применения электронных сборок со смешанным монтажом являются системы приема-передачи информации спутников дистанционного зондирования Земли. В процессе вывода на орбиту такого спутника его аппаратура подвергается интенсивным нагрузкам, имеющим сложный, затухающий во времени характер, распределенный в широком диапазоне частот. Эксперименты, проводимые в управляемых условиях, показали, что широкополосное воздействие при испытаниях можно успешно моделировать применяя непериодическую (случайную) вибрацию. Спектры непериодической вибрации определяются как профили спектральной плотности ускорения, которые связывают уровни плотности энергии с определенными полосами частот. Вибрация определяется относительно соответствующего частотного диапазона. Использование среднеквадратичных значений ускорения для описания вибрационных испытаний некорректно, поскольку среднеквадратичное значение ускорения не характеризует конкретный профиль вибрации. Одним среднеквадратичным значением ускорения можно описать бесконечное количество сочетаний частотных полос и спектральных форм. Поэтому при измерении величины и спектрального