Сергей БАСАРАБ

г. Москва

ТЕСТИРОВАНИЕ СЕТЕВОЙ БЕЗОПАСНОСТИ

Abstract: *In the article there are considered recommendations and network security testing methods of National Institute of Standards and Technology of America. They should be used while initialization of network security testing projects to lighten the search and identification of network testing requests and determine priorities of testing in the conditions of enterprise resource limits.*

Начиная с 80-х годов прошлого столетия, концепция качества продуктов информационных технологий, а также самих технологий бурно обсуждалась и развивалась. В результате чего появились международные стандарты ISO/IEC, американские стандарты ANSI/IEEE и др.

В данной статье будут рассмотрены рекомендации и методики тестирования сетевой безопасности американского Национального Института Стандартизации и Технологий.

В НИСТ разработали набор правил, которыми следует руководствоваться при инициировании проектов по тестированию сетевой безопасности, чтобы облегчить поиск и идентификацию требований к тестированию сети, а также определить приоритеты тестирования в условиях ограниченных ресурсов предприятий. Данные правила носят консультативный характер, что дает возможность при проведении работ по тестированию использовать наиболее подходящие элементы методики в соответствии со спецификой предприятия и предметной областью.

Тем не менее, этот обобщенный подход к тестированию сетевой безопасности применим ко всем сетевым системам, включающим в себя следующие элементы:

1. Брандмауэры;
2. Маршрутизаторы и коммутаторы;
3. Связанный сетевой периметр систем безопасности, таких как системы обнаружения вторжения;
4. Web сервер, почтовый сервер и другие сервера приложений;
5. DNS сервера или файл-сервера (NFS, FTP и др.).

Приведенные выше элементы больше относятся к классу классических сетей, которые используют передачу данных по сетевому кабелю. В таких сетях можно организовать физическую

охрану сетевого оборудования и кабельной инфраструктуры, что не в полной мере относится к беспроводным сетям Wi-Fi, которые используют общую среду передачи данных. Несмотря на это, даже в проводных сетях одной только физической защиты недостаточно. Все эти доводы ведут к тому, что для снижения критичности работы сетевой системы требуется систематическая проверка ее узлов и интерфейсов на возможные уязвимости, которые могут привести к несанкционированному доступу и использованию ее ресурсов.

Задачи, связанные с такими проверками, во многом решаются путем тестирования сетевой безопасности.

Методика тестирования безопасности в соответствии с рекомендациями НИСТ предполагает несколько различных типов тестирования сетевой безопасности:

- Сканирование сети
- Сканирование уязвимостей
- Взлом паролей
- Анализ протоколов (логов)
- Контроль целостности файлов
- Идентификация вирусов War Dialing (“Боевой набор номера”)
- Тестирование беспроводных сетей Wi-Fi (“War Driving” – “Боевое вождение”)
- Тест на проникновение

Зачастую описанные выше типы тестирования комплексной используются оценки в ансамбле состояния чтобы повысить точность общего (совместно), безопасности сети.

Распределение ролей и ответственности в процессе тестирования является важной задачей, которую нужно будет решить. Потребуется определить состав людей, которые будут заниматься тестированием, такими могут быть сетевые администраторы или специально привлеченные специалисты, возможно даже по контракту. Необходимо будет также принять регламент проведения тестирования, формы отчетности по каждому проведенному тесту; уведомлять, в случае необходимости, заинтересованные стороны, задействованные в производстве, о начале и окончании тестирования, чтобы избежать неприятных казусов, конфликтных ситуаций, а также не допустить разглашения конфиденциальной информации.

После проведения тестирования по каждой обнаруженной проблеме в безопасности сети требуется принять адекватное решение по ее устранению либо если это невозможно, смягчению последствий в случае использования ее злоумышленниками для организации атак на сеть.

В целом, как уже было отмечено выше, методика носит консультативный характер, т.е. предлагает обобщенные методики, но при этом достаточно гибкие, для адаптации их под реальные проекты по тестированию сетевой безопасности на предприятиях.

Также данные методики могут дополняться новыми решениями, таким образом, они будут максимально эффективны в условиях быстрого развития информационных технологий и, как следствие, появления новых видов угроз сетевой безопасности.

Литература:

1. “Guideline on Network Security Testing” Recommendation of the National Institute of Standards and Technology. Jon Wack, Miles Tracy, Murugiah Souppaya. Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899-8930, October 2003.
2. “Анализ безопасности беспроводных сетей”, Поваляев И. Г.
3. “Пять неуважительных причин не иметь тестировщиков”, Джоэл Сполски http://russian.joelonsoftware.com/Articles/TopFiveReasonsYouDontHave.html