Тестирование на проникновение: демонстрация одной уязвимости или объективная оценка защищенности?

В последнее время специалисты по информационной безопасности очень бурно обсуждают полезность такого вида аудита информационной безопасности, как тестирование на проникновение. Одни утверждают, что с его помощью можно выявить все недостатки системы обеспечения информационной безопасности в организации, другие же видят в нем только способ наглядно продемонстрировать руководству необходимость увеличить бюджет на закупку средств защиты. Давайте разберемся, каким образом можно получить максимальную пользу от подобного аудита.

А. Дорофеев, *CISA, CISSP*

Начнем с определения понятия «тестирование на проникновение». Так называется тестирование защищенности, в ходе которого используются приемы и инструменты, применяемые настоящими злоумышленниками. Самих аудиторов в этом случае часто называют «этичными хакерами».

В зависимости от того, какие цели преследуют заказчики и исполнители тестирования, оно может принимать различные формы. Заказчик может желать получить подтверждение уязвимости системы защиты (например, для убеждения руководства выделить дополнительные деньги на информационную безопасность) или, наоборот, подтверждение защищенности (например, для отчета перед руководством) или максимальное количество уязвимостей и объективную оценку защищенности (для улучшения системы защиты информации). Исполнитель, в свою очередь, может преследовать следующие цели: максимальное качество тестирования, минимизацию затрат на выполнение проекта, желание продать заказчику дополнительные услуги и программное обеспечение.

Рассмотрим два наиболее распространенных варианта:

1. Клиент хочет получить демонстрацию незащищенности, а исполнитель хочет провести тестирование с минимальными затратами и поучаствовать в освоении бюджета, который выделят по результатам проекта.

2. Клиент хочет получить максимально объективную оценку защищенности систем, а исполнитель провести максимально качественное тестирование и заработать хорошую репутацию.

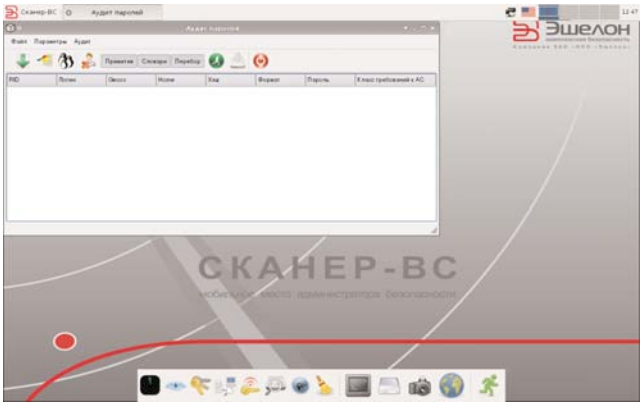
В первом случае тестирование, скорее всего, пойдет по следующему сценарию.

Этичные хакеры, используя какой-нибудь отработанный прием (например, отправку генеральному директору руткита по электронной почте) демонстрируют, что они смогли получить доступ к самой сокровенной информации, которая хранилась на компьютере топ-менеджера (например, к приватным персональным данным). Подобный аудит можно провести в очень сжатые сроки, так как специалисты ищут всего несколько уязвимостей для демонстрации. После того как генеральный директор осознает незащищенность компании и выделяет деньги на информационную безопасность, компания-исполнитель продает ей и внедряет разнообразные средства защиты информации.

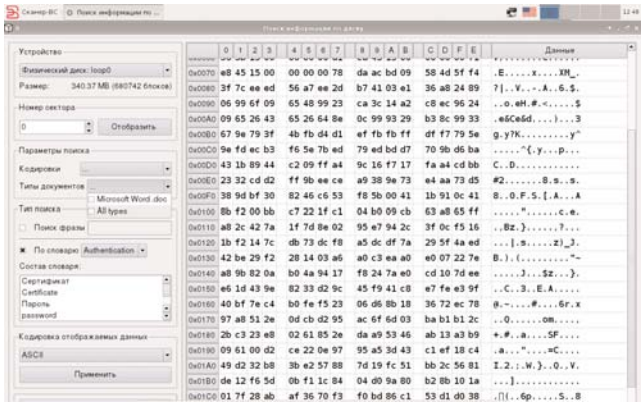
Особый случай, если компания-исполнитель наиболее значимую прибыль получает за счет продаж средств анализа защищенности (например, если компания является производителем подобного программного обеспечения или эксклюзивным дистрибьютором). В этом случае уязвимости для демонстрации будут найдены именно этим программным средством, а заказчика постараются убедить в том, что, купив данное средство, он сможет тестировать свою защищенность самостоятельно.

В случае, когда обе стороны заинтересованы в качественной работе, все намного интереснее.

Перед исполнителем стоит довольно серьезная задача – провести комплексный технический аудит и найти максимальное количество уязвимостей. В этом варианте применить пару отработанных сценариев или один сканер уязвимостей – уже недостаточно. Необходимо использовать целый набор программных средств, которые состоят на вооружении реальных злоумышленников.



Подрисуночная подпись 1



Подрисуночная подпись 2

Что касается методики тестирования, то, как правило, она подразумевает следующие этапы:

- идентификация целей;
- поиск уязвимостей;
- эксплуатация уязвимостей;
- расширение привилегий.

Рассмотрим каждый из этапов на примере внутреннего тестирования на проникновение, когда этичный хакер имеет физический доступ к корпоративной сети.

В ходе идентификации целей аудитор сканирует сеть с помощью специального сканера сети, который позволяет определить, какие узлы доступны, какие службы запущены, а также их версии. В итоге специалист, проводящий тестирование, знает, что скрывается в сети за определенным IP-адресом: сервер базы данных, web-сервер, контроллер домена, сервер приложений или рабочая станция.

После согласования с заказчиком перечня узлов, попадающих в рамки тестирования, проводится сканирование на наличие уязвимостей. Стоит отметить, что особо критичные серверы, например, серверы автоматизированной банковской системы, как правило, исключаются из рамок тестирования и проверяются по проверочным листам, содержащим описание настроек безопасности.

Получив сводный перечень уязвимостей, этичный хакер проводит эксплуатацию части уязвимостей. Особый упор делается на подбор паролей к различным сетевым сервисам, проведению атак типа «человек посередине» для перехвата паролей пользователей.

После получения доступа к какой-либо системе аудитор, как и настоящий взломщик, пытается максимально расширить свои привилегии и получить доступ к другим системам, а также скомпрометировать максимальное количество учетных записей пользователей. Так, например, «раскручивают» хэши паролей пользователей домена с помощью средств локального аудита стойкости паролей.

Большое внимание уделяется анализу стойкости паролей, так как «легко угадываемый пароль» является базовой уязвимостью, ведущей к полной компрометации системы. Наши пользователи до сих пор любят простые пароли:

- имена, которые могут быть дополнены цифрами: «alexandr», «lolita17»;
- номера мобильных телефонов: «89101234567»;
- даты (рождения, свадьбы и т.п.): «23051986»;
- клавиатурные пароли: «qwerty», «qazwsxedc»;
- всевозможные последовательности цифр: «123456789», «1111111»
- слова на русском языке, набранные в английской раскладке клавиатуры: «gfhjkm» («пароль»).

Современные средства аудита паролей включают не только словари, содержащие наиболее распространенные пароли, но и реализуют различные алгоритмы их генерации.

Таким образом, заказчик, выбирая исполнителя и его подход, может получить совершенно различные результаты на выходе проекта: эффектную демонстрацию собственной незащищенности или отчет, содержащий максимально возможное количество уязвимостей, устранение которых позволит серьезно повысить уровень информационной безопасности компании.

Проведение подобного комплексного тестирования невозможно без использования специального программного обеспечения, представляющего собой именно целый комплекс средств, установленных в некой доверенной среде, загружаемой с компакт-диска или USB-накопителя.

В качестве примера здесь можно рекомендовать современное сертифицированное средство анализа защищенности – «Сканер-ВС», разработанное российской компанией ЗАО «НПО «Эшелон». Система «Сканер-ВС» представляет собой Live CD, включающий комплекс программных средств для сканирования на наличие уязвимостей, локального и удаленного анализа стойкости паролей (поддерживаются версии Linux, Windows, а также более двадцати сетевых протоколов), перехвата и анализа сетевого трафика, инвентаризации сетевых сервисов, инвентаризации локальных ресурсов, поиска остаточной информации на локальном диске компьютера. Важно, что данное средство, поддерживающее самые современные технологии анализа защищенности, можно использовать и в госструктурах, так как оно сертифицировано во ФСТЭК России и Минобороны России.

В любом случае, при привлечении сторонней организации либо при организации собственного рабочего места администратора безопасности без сертифицированной системы анализа защищенности решить задачу объективной оценки уровня безопасности ресурсов практически невозможно.