УДК 004.056

Н.Н. Еременко, А.Н. Кокоулин

N.N. Eremenko, A.N. Kokoulin

Пермский национальный исследовательский
политехнический университет

Perm National Research Polytechnic University

ИССЛЕДОВАНИЕ МЕТОДОВ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

RESEARCH OF METHODS OF PENETRATION TESTING IN INFORMATION SYSTEMS

Исследованы методы тестирования на проникновение в информационных системах. Установлено, что в случае быстрой оценки системы необходимо использовать тестирование методом WhiteBox. Если нужна симуляция действий злоумышленников, проводится тестирование методом BlackBox. Для комбинированного подхода следует придерживаться метода GreyBox.

Ключевые слова: тестирование на проникновение, уязвимость, атака, сканирование, оценка системы.

Penetration testing methods in information systems are researched. It is determined that if the rapid assessment of the system is needed it is necessary to use the WhiteBox testing method. If a malefactor's actions simulation is needed the BlackBox method research is carried. For the combined approach the GreyBox method should be followed.

Keywords: penetration testing, vulnerability attack, scanning, system evaluation.

При построении системы (и даже для действующей системы) встает вопрос об эффективности принятых мер безопасности для защиты от внешних и внутренних угроз. Для оценки эффективности используется тестирование на проникновение.

Тестирование на проникновение – метод оценки защищенности компьютерной системы или сети, основанный на имитации действий внешнего злоумышленника [1]. Оно позволяет оценить устойчивость к атакам, выявить существующие недостатки, определить пути для улучшения средств защиты.

Для объективности и полноценности проведения тестирования используются методики и рекомендации, в которых указаны цели, методы проверки, особенности и правила. Из актуальных можно выделить следующие [2]:

– Open Source Security Testing Methodology Manual (OSSTMM);

– OWASP Testing Guide;

– Penetration Testing Execution Standard (PTES);

– NIST Special Publication 800-115: Technical Guide to Information Security Testing and Assessment (NIST SP 800-115);

– РС БР ИББС-2.6–2014. Рекомендации Банка России «Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных систем» (прил. 3. Рекомендации по проведению оценки защищенности).

Тестирование производится в несколько этапов (рис. 1), которые позволяют структурированно и комплексно произвести оценку [1, 3].

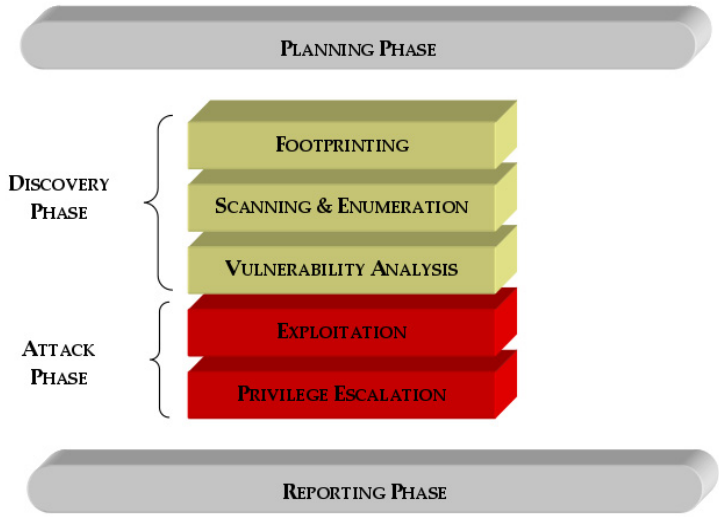

Рис. 1. Стадии тестирования на проникновение

Планирование. На данном этапе с заказчиком согласовываются цели, начальные условия и содержание теста на проникновение.

Первоначально на стадии планирования необходимо утвердить договор, в котором определены границы деятельности, ответственность исполнителя и заказчика. Может быть также подписано соглашение о неразглашении для ограничения распространения информации о системе исследования. Определяются зоны исследования и подход к проведению тестирования на основе исходных сведений о системе (WhiteBox, BlackBox, GreyBox), осведомленности персонала заказчика о проводимых испытаниях и нахождения специалиста, проводящего тесты, относительно сети системы (внешняя, внутренняя).

При оценке методом WhiteBox специалисту предоставляется полная информация о системе и действующих средствах защиты. Плюсы данного метода заключаются в том, что оценка будет произведена качественнее, нежели при проверке методом BlackBox. Недостаток данного метода – в том, что исполнитель тестирования будет находиться в более выгодной позиции, чем злоумышленник в реальной ситуации.

При оценке методом BlackBox информация исполнителю не предоставляется, либо дается необходимый минимум. Плюсы и минусы, соответственно, будут инверсны.

GreyBox – промежуточный вариант между предыдущими двумя методами оценки. Он подразумевает возможность тестирующего запрашивать необходимую информацию о системе для сокращения времени тестирования или повышения эффективности. Данный вариант является в большинстве своем приоритетным, так как позволяет повысить продуктивность исследования за счет снижения времени, затраченного на рутинную работу по поиску начальной информации. Однако проверка данным методом также остается приближенной к моделированию действий злоумышленника.

Если организатором и исполнителем было решено не проводить каких-либо мероприятий по сокрытию действий по тестированию, тестирующий работает в контакте со службой информационной безопасности (ИБ) организации, что позволяет в кратчайшие сроки отреагировать на актуальные уязвимости.

При отсутствии информации о проведении тестирования у персонала задача специалиста более приближена к реальному моделированию атаки злоумышленника. Происходит оценка не только уровня защищенности системы, но и готовности сотрудников службы ИБ организации.

Фаза обнаружения. Данный этап разделяется:

– на получение информации о системе, пользователях (сотрудниках): могут быть применены поисковики, социальные сети, электронная почта, новости;

– сканирование и перечисление: на данном этапе производится сканирование обнаруженных хостов, обнаружение портов, перечисление пользователей и другой важной информации;

– обнаружение и анализ уязвимостей: они могут быть выявлены с помощью специализированных программ, таких как Nessus, Nikto, и методом ручной проверки.

Наиболее распространенные уязвимости систем, характерные при анализе внешней среды, указаны на рис. 2, при анализе внутренней сети – на рис. 3.

Можно сделать вывод, что для большинства систем характерны достаточно простые уязвимости, которых можно избежать, не прибегая к дополнительному обеспечению.

Фаза атаки. Эксплуатация уязвимостей может происходить по техническому и социальному каналам. В первом случае могут использоваться небольшие программы – эксплоиты, которые можно найти в открытых источниках (например, http: //exploit-db.com), а программы для уязвимостей нулевого дня могут продаваться на приватных форумах, сайтах. Во втором случае – это метод несанкционированного доступа к информационным ресурсам, основанный на особенностях психологии человека, называемой социальной

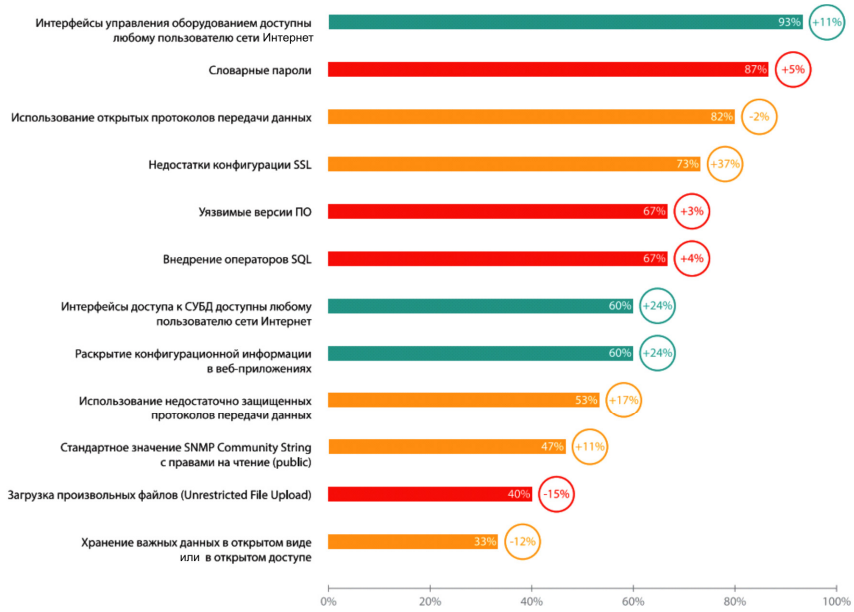

Рис. 2. Наиболее распространенные уязвимости внешней сети [4]

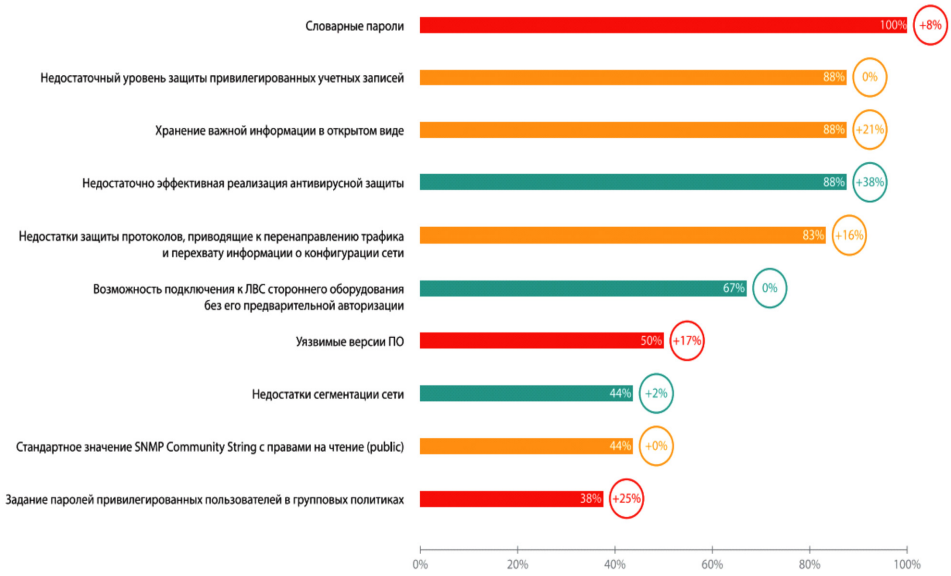

Рис. 3. Наиболее распространенные уязвимости внутренней сети [4]

инженерией. Через социальные сети, электронную почту злоумышленник вступает в контакт с сотрудником организации с целью получения контроля над рабочей станцией и доступа к необходимой информации.

После того как тестирующий закрепился в системе, следующий его шаг – повышение привилегий, что позволит овладеть более ценными данными и может нанести больший урон компании.

Построение отчета. После окончания анализа заказчик получает отчет, в котором указаны проведенные работы, существующие уязвимости, способы их реализации, возможные последствия, ущерб и рекомендации по ликвидации.

В качестве практической части для исследования была взята виртуальная машина Droopy v0.2 с ресурса vulnhub.com, созданная для легальной проверки системы.

В результате сканирования хоста программой nmap было выявлено, что в системе открыт 1 порт – 80, на этом порте находится веб-сайт Apache с CMS Drupal. Версия установленной CMS имела известную уязвимость CVE-2014-3704. Эксплуатация данной уязвимости с помощью Metasploit Framework позволила получить удаленный доступ к системе. Далее с помощью стандартного пароля были получены привилегии суперпользователя, которые позволят злоумышленнику заполучить почти всю информацию в системе и принести огромные убытки компании.

Можно сделать вывод, что своевременное обновление системы и ее составляющих, а также использование достаточно сложных паролей могли бы исключить возможность компрометации системы.

Таким образом, тестирование на проникновение позволит узнать присутствующие угрозы безопасности, оценить последствия реализации уязвимостей и выработать список контрмер. Все методы тестирования имеют свои особенности, поэтому заказчику необходимо совместно с исполнителем выбрать оптимальный вариант для достижения поставленных целей. Если в первую очередь требуется выявить текущие недостатки системы и устранить их, стоит выполнить тестирование методом WhiteBox с привлечением сотрудников ИБ организации. При необходимости симуляции действий злоумышленника проводится BlackBox-изучение системы без привлечения специалистов ИБ. Метод GreyBox актуален, когда необходимо комбинировать подходы для эффективного и ограниченного во времени исследования.

Список литературы

1. Тестирование на проникновение или пентест [Электронный ресурс]. – URL: http: //deflab.ru/blog/metodi-i-sredstva-zashiti/testirovanie-na-proniknovenie-pentest.html (дата обращения: 15.04.2016).

2. Тестирование на проникновение в соответствии с требованиями СТО БР ИББС-1.0–2014 [Электронный ресурс]. – URL: https: //habrahabr.ru/company/pentestit/blog/255113 (дата обращения: 15.04.2016).

3. Этичный хакинг и тестирование на проникновение [Электронный ресурс]. – URL: http: //www.slideshare.net/heirhabarov/publ-57821636 (дата обращения: 15.04.2016).

4. Статистика уязвимостей корпоративных информационных систем 2014 [Электронный ресурс]. – URL: https: //www.ptsecurity.ru/download/PT_Corporate_vulnerability_2015_rus.pdf (дата обращения: 24.04.2016).

Получено 02.09.2016

Еременко Николай Николаевич – студент кафедры «Автоматика и телемеханика», электротехнический факультет, Пермский национальный исследовательский политехнический университет, e-mail: eremenko.nick@gmail.com.

Кокоулин Андрей Николаевич – доцент кафедры «Автоматика и телемеханика», электротехнический факультет, Пермский национальный исследовательский политехнический университет, e-mail: liga_asu@mail.ru.