УДК 004.056.5
DOI: 10.33764/2618-981X-2019-9-47-53

РАЗРАБОТКА МЕТОДИКИ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ МОБИЛЬНЫХ И ВЕБ-ПРИЛОЖЕНИЙ

Анастасия Евгеньевна Мельникова
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, обучающийся, тел. (999)463-88-33, e-mail: knock1e@yandex.ru

Игорь Николаевич Карманов
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, кандидат технических наук, доцент, зав. кафедрой физики, тел. (903)937-24-90, e-mail: i.n.karmanov@ssga.ru

Актуальность темы работы обусловлена тем, что тестирование на проникновение (тесты на преодоление защиты, penetration testing, pentest, пентест) является популярной во всем мире услугой в области информационной безопасности (ИБ). Суть таких работ заключается в санкционированной попытке обойти существующий комплекс средств защиты информационной системы. В ходе тестирования аудитор выполняет роль злоумышленника, мотивированного на нарушение ИБ сети заказчика. В работе подробно изучены особенности проведения тестирования на проникновение, выполнен детальный анализ существующих зарубежных решений в области тестирования на проникновение, разработана собственная методика и предложены рекомендации по улучшению имеющихся методик.

Ключевые слова: тестирование на проникновение, разработка методики, информационная безопасность, мобильные приложения, веб-приложения, уязвимость, аудит.

DEVELOPMENT OF THE METHODOLOGY FOR PENETRATION TESTING OF MOBILE AND WEB APPLICATIONS

Anastasia E. Melnikova
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Student, phone: (999)463-88-33, e-mail: knock1e@yandex.ru

Igor N. Karmanov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Ph. D., Associate Professor, Head of Department of Phisics, phone: (903)937-24-90, e-mail: i.n.karmanov@ssga.ru

The relevance of the topic is due to the fact that penetration testing (tests to overcome protection, penetration testing, pentest) is a worldwide popular service in the field of information security. The essence of such work is an authorized attempt to circumvent the existing set of protection means of information system. During testing, the auditor performs the role of an attacker motivated to violate the information security of customer's network. In article, features of penetration testing are thoroughly studied, a detail analysis of existing foreign solutions in the field of penetration testing is performed, a proprietary technique is developed and recommendations for improving the existing techniques are proposed.

Key words: penetration testing, methodology development, information security, mobile applications, web applications, vulnerability, audit.

Введение

Тестирование на проникновение (тесты на преодоление защиты, penetration testing, pentest, пентест) является чрезвычайно популярной во всем мире услугой в области ИБ. Суть таких работ заключается в санкционированной попытке обойти существующий комплекс средств защиты информационной системы. В ходе тестирования аудитор выполняет роль злоумышленника, мотивированного на нарушение ИБ сети заказчика.

Целью работы является разработка, апробация и выработка рекомендаций по совершенствованию методики тестирования на проникновение мобильных и веб-приложений.

Методы и методики

Тестирование на проникновение не ограничивается простым обнаружением способов, которыми преступник может получить несанкционированный доступ к конфиденциальным данным или захватить системы в злонамеренных целях. Тестирование также имитирует атаку в реальных условиях, чтобы определить возможную величину ущерба и необходимые средства обеспечения защиты информации [1].

Комплексное тестирование на проникновение включает несколько областей:

– тестирование на проникновение в приложения – выявляет недостатки прикладного уровня (подделка межсайтовых запросов, межсайтовое выполнение сценариев, дефекты внедрения уязвимого программного кода, управление слабыми сеансами, небезопасные прямые ссылки на объекты и т.д.) [2];

– тестирование на проникновение в сеть – выявление уязвимостей на уровне сети и системы (неверные конфигурации, уязвимости для конкретного продукта, уязвимости беспроводной сети, мошеннические службы, слабые пароли и протоколы);

– тестирование на физическое проникновение (вторжение) – взлом физических барьеров (замки, датчики, камеры и т.д.);

– IoT (тестирование проникновения в устройства Интернета вещей) – выявление аппаратных и программных недостатков (слабые пароли, небезопасные протоколы, программный интерфейс приложения (API) или каналы связи, неверные конфигурации и т.д.) [3].

Рассмотрим несколько популярных методологий для проведения тестирования на проникновение (табл. 1).

Первая методология, «Technical Guide to Information Security Testingand Assessment», создана и поддерживается подразделением NIST(National Institute of Standards and Technology) – Computer Security Resource Center, центром по компьютерной безопасности, объединяющим специалистов федеральных служб, университетов, крупнейших ИТ-компаний США [4–5]. Последняя вер-

сия данной методологии выпущена в 2008 году и используется до сих пор, несмотря на то, что данные в ней устарели и нуждаются в детальной доработке [6].

Таблица 1

Сравнительная таблица актуальности методологий

Разработчик	Наименование	Год выпуска
National Institute of Standards and Technology	Technical Guide to Information Security Testing and Assessment	2008
Institute for Security and Open Methodologies	Open Source Security Testing Methodology Manual 3	2010
Open Web Application Security Project	Testing Guide	2014

Ассоциация ISECOM (Institute for Security and Open Methodologies) опубликовала методологию «Open Source Security Testing Methodology Manual» (OSSTMM) – «Руководство по методологии тестирования безопасности с открытым исходным кодом» версии №3 в 2010 году. Это достаточно формализованный и хорошо структурированный документ, по настоящее время используемый в некоторых компаниях, предоставляющих услуги по ИБ [7–10]. С версии 3 OSSTMM охватывает тесты по всем каналам утечки информации – человеческий, физический, беспроводной, телекоммуникационный и сети передачи данных. Разработка OSSTMMv4 ведется в данный момент, но пока точных сроков публикации не назначено.

Open Web Application Security Project (OWASP) – открытый проект обеспечения безопасности веб-приложений. Последняя версия «TestingGuide» датируется 2014 годом, что также является совершенно недопустимым в современных реалиях [11–12]. Разработка новой версии активно ведется на сервисе хранения исходного кода Github, но даже примерные даты релиза отсутствуют [13–14].

Таким образом, как бы ни были хороши существующие решения, с их актуальностью имеются большие проблемы. Все рассмотренные методологии тестирования на проникновения очень сильно устарели. Следовательно, предприятию, которое оказывает услуги тестирования на проникновение, необходимо разработать собственную методику, используя в качестве базы существующие наработки.

Результаты

При внешней и внутренней проверке безопасности исполнитель изучает возможные пути доступа в систему. Исполнитель будет использовать интерактивные методы тестирования [15].

Исполнитель проверяет согласованные с заказчиком IP-адреса и, в частности, предлагаемые на них сервисы в шесть этапов. Порядок проведения проверки показан на рисунке. Исполнитель проводит тестирование в информационной среде заказчика [16].

Этапы анализа защищенности

В итоге, предлагаемая методика включает следующие этапы:

- сбор информации – на первом этапе проводится сбор максимального количества информации из общедоступных баз данных (DNS, Whois, и т.д.), а также других источников (веб-сайт Заказчика, поисковые системы и т.д.), чтобы узнать о том, как можно эффективно атаковать конкретную организацию;
- сканирование портов – подлежащая проверке система подвергается процессу автоматического сканирования портов;
- анализ сервисов – сервисы, выявленные в ходе предыдущего этапа, подлежат изучению Исполнителем на предмет наличия уязвимостей в системе обеспечения безопасности заказчика. Тестирование охватывает как стандартные продукты (Microsoft IIS, ApacheWebserver, и т.д.), так и программное обеспечение, разработанное самим заказчиком или третьими лицами;
- уязвимости протокола канального уровня – проблемы безопасности в пределах второго уровня OSI-модели [17–18];
- уязвимости протоколов сетевого и транспортного уровней – проблемы безопасности в пределах третьего, четвертого и пятого уровней OSI-модели;
- проблемы межсетевого экрана (firewall) – проблемы безопасности, связанные с конфигурацией сетевого устройства защиты;
- конфигурация сервера – эта категория охватывает ошибки конфигурации для всех видов серверного программного обеспечения. Возможно использование известных уязвимостей, даже при наличии доступных обновлений;
- проблемы аутентификации и авторизации – приложение не обеспечивает достаточные средства аутентификации и/или авторизации для защиты своих ресурсов. Неавторизованный или не имеющий привилегий пользователь может получить доступ к ресурсам, которые защищены или должны быть защищены;
- проблемы бизнес-логики – злоумышленник может нарушить бизнес-логику приложения. Конкретные схемы попыток нарушения защиты зависят от конкретного приложения [19];
- раскрытие информации – злоумышленник может собирать информацию о внутреннем содержании приложения или конфигурации серверов;
- организация атак со стороны клиента (веб-браузер) – эта категория уязвимостей связана с сетью Интернет. Она охватывает атаки, нацеленные на веб-браузер;
- проблемы внедрения интерпретаторов/проверки вводимых значений – Приложение пропускает непроверенные параметры входящего потока в базу данных, ИПП операционной системы или другие интерпретаторы [20];

- проблемы управления соединением и небезопасное управление доверительными данными – переменные, участвующие в формировании соединения, могут быть использованы нецелевым образом. Злоумышленник может манипулировать доверительными данными или внутренними данными приложения;
- использование недокументированного или небезопасного функционала приложений, небезопасные алгоритмы – использование данных приложений изначально являются небезопасным. Использование небезопасных алгоритмов подвергает риску конфиденциальные данные;
- уязвимость к атакам на отказ в обслуживании – в результате атаки сервис может стать временно недоступным для использования;
- вторжение в сервисы из сети Интернет – выявленные уязвимости используются с целью получения доступа к системе. Анализ найденных уязвимостей позволяет исключить ложные опасности/аспекты, не представляющие реальной проблемы;
- оценка рисков – на основании результатов предыдущего этапа, сначала с использованием шкалы оценки риска определяется уровень риска каждой отдельной уязвимости и далее – общий риск, которому подвергается система.

По окончании оказания услуг заказчику в бумажном виде предоставляются консультационные и рекомендационные материалы по оптимизации настройки программных и аппаратных комплексов с целью устранения выявленных уязвимостей и общего повышения уровня безопасности информационных систем клиентов. Для каждого класса исследуемых уязвимостей необходимо составить таблицу, в которой будут отражены все виды уязвимостей. Обязательно требуется указать те уязвимости, на которые эксперт по ИБ проводил тестирование и те, которые в конечном итоге получилось успешно проэксплуатировать. Пример оформления приведен в табл. 2.

Таблица 2

Демонстрация исследованных и проэксплуатированных уязвимостей

	Проблемы с интерпретатором / проверкой ввода	
	Приложение передает входные параметры в базу данных, API операционной системы или другие интерпретаторы без надлежащей проверки	
Наименование уязвимости	Протестировано	Проэксплуатировано
Accessing the file system	ДА	НЕТ
Code injection	ДА	ДА
Command injection	ДА	НЕТ
Format string injection	ДА	НЕТ
IMAP/SMTP injection	НЕТ	ДА
LDAP injection	НЕТ	НЕТ
ORM injection	НЕТ	НЕТ
Overflowing character buffers	ДА	ДА
Path traversal	ДА	НЕТ
SQL injection	ДА	ДА
SSI injection	ДА	НЕТ
XML injection	ДА	ДА
XPath injection	ДА	НЕТ

Разработанная методика тестирования на проникновение была применена на реальных проектах по аудиту информационной безопасности зарубежной организации. В связи с соглашением о неразглашении, данные, раскрывающие информацию о клиенте, не приводятся.

Выводы

Предложены следующие рекомендации по улучшению существующих методик проведения тестирования на проникновение:

- стабильное обновление методики раз в квартал – информационные технологии развиваются стремительно, необходимо всегда следовать актуальным трендам в области защиты информации;
- немедленное обновление методики при обнародовании новой уязвимости;
- постоянное информирование сотрудников о новых уязвимостях в виде статей на внутреннем ресурсе компании – исследователям требуется каждый день повышать свою квалификацию, а также делиться знаниями между собой;
- назначение ряда ответственных лиц – в компании следует уделять повышенное внимание вопросу актуальности используемой методики;
- регулярные обсуждения внутри компании на предмет актуальности используемой методики, исключение устаревших или добавление недавно опубликованных уязвимостей;
- анализ проведенной работы, доработка шаблонов и написание документации для новых сотрудников.

Заключение

В работе изучены особенности проведения тестирования на проникновение, проведен сравнительный анализ существующих методик тестирования на проникновение, разработана методика тестирования на проникновение мобильных и веб-приложений, и предложены рекомендации по улучшению качества существующих методик тестирования на проникновение.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Pentest (penetrationtesting) [Электронный ресурс] / отдел «Penetrationtesting». – Электрон. дан. – СФ., 2018. – Режимдоступа: https://searchsecurity.techtarget.com/definition/penetration-testing. – Загл. с экрана.

2. Importance Of Information Security In Organizations Information Technology Essay [Электронный ресурс] / отдел « Information Technology». – Электрон. дан. – К., 2011. – Режим доступа: https://www.uniassignment.com/essay-samples/information-technology/. – Загл. сэкрана.

3. Introduction: Intelligence Gathering & Its Relationship to the Penetration Testing Process [Электронный ресурс] / отдел «Penetration testing». – Электрон. дан. – НЙ., 2016. – Режим доступа: https://resources.infosecinstitute.com/penetration-testing-intelligence-gathering/. – Загл. сэкрана.

4. Technical Guideto Information Security Testingand Assessment [Электронный ресурс] / отдел «Publications». – Электрон. дан. – МД., 2008. – Режим доступа: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf. – Загл. с экрана.

5. Introduction to Penetration Testing and Kali Linux. [Электронный ресурс] / отдел «Security» – Электрон. дан. – Б, 2015. – Режим доступа: https://hub.packtpub.com/introduction-penetration-testing-and-kali-linux/. – Загл. с экрана.

6. Exploit database. Exploits for web applications. [Электронный ресурс] / отдел «Exploits» – Электрон. дан. – НЙ, 2016. – Режим доступа: https://www.exploit-db.com/webapps. – Загл. с экрана.

7. Payment application data security standard. Requirements and security assessment procedures. Version 3.1. Payment Card Industry (PCI). [Электронный ресурс] / отдел «Стандарты PCI-DSS» – Электрон. дан. – НЙ, 2017. – Режим доступа: https://www.pcisecuritystandards.org/documents/PADSS_v3-1.pdf. – Загл. с экрана.

8. TheOpen Source Security Testing Methodology Manual [Электронныйресурс] / отдел «Research». – Электрон. дан. – НЙ., 2010. – Режим доступа: http://www.isecom.org/mirror/OSSTMM.3.pdf. – Загл. с экрана.

9. Mitnick, Kevin. Unauthorized Access: Physical Penetration Testing for IT Security Teams [Текст] – НЙ.: John Wiley & Sons, 2009. – 287 с.

10. MobileTop 10 2016-Top 10 [Электронный ресурс] / отдел «Projects». – Электрон. дан. – ЛА., 2016. – Режим доступа: https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10. – Загл. с экрана.

11. OWASP Mobile Security Testing Guide [Электронный ресурс] / отдел «Projects». – Электрон. дан. – ЛА., 2018. – Режим доступа: https://www.owasp.org/index.php/OWASP_Mobile_Security_Testing_Guide. – Загл. с экрана.

12. OWASP Testing Guide v4 [Электронный ресурс] / отдел «Publications». – Электрон. дан. – ЛА., 2014. – Режим доступа: https://www.owasp.org/images/1/19/OTGv4.pdf. – Загл. с экрана.

13. OWASP Top Ten Project [Электронный ресурс] / отдел «Projects». – Электрон. дан. – ЛА., 2017. – Режим доступа: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project. – Загл. с экрана.

14. Testing Guide Introduction [Электронный ресурс] / отдел «Projects». – Электрон.дан. – ЛА., 2014. – Режим доступа: https://www.owasp.org/index.php/Testing_Guide_Introduction. – Загл. с экрана.

15. Vacca, John R. Computer and Information Security Handbook [Текст] – ЛА.: Elsevier, 2017. – 1280 с.

16. Black box, grey box, white box testing: what differences? [Электронный ресурс] / отдел «Blog». – Электрон. дан. – П., 2016. – Режим доступа: https://nbs-system.com/en/blog/black-box-grey-box-white-box-testing-what-differences/. – Загл. с экрана.

17. ARP Spoofing [Электронный ресурс] / отдел «Security». – Электрон. дан. – НЙ., 2016. – Режим доступа: https://www.veracode.com/security/arp-spoofing/. – Загл. с экрана.

18. What is MAC Flooding? How to prevent it? [Электронный ресурс] / отдел «KB». – Электрон.дан. – ЛА., 2015. – Режим доступа: https://www.interserver.net/tips/kb/mac-flooding-prevent/. – Загл. с экрана.

19. Microsoft Security Development Lifecycle. [Электронный ресурс] / отдел «Безопасный цикл разработки Microsoft» – Электрон.дан. – СФ, 2016. – Режим доступа: http://www.microsoft.com/security/sdl/default.aspx. – Загл. с экрана.

20. XPathinjection. [Электронный ресурс] / отдел «IssueDefinitions» – Электрон.дан. – ЛА, 2018. – Режим доступа: https://portswigger.net/kb/issues/00100600_xpath-injection. – Загл. с экрана.