УДК 004.056
ББК 32.973.26–018.2
К 38

Киздермишов А.А.
Кандидат физико-математических наук доцент кафедры автоматизированных систем обработки информации и управления инженерно-физического факультета Адыгейского государственного университета, Майкоп, тел. (8772) 59-39-11, e-mail: Askhad_75@rambler.ru

К вопросу о применении CVE-совместимых сетевых сканеров

(Рецензирована)

Аннотация. *Описывается модель нарушителя, рассматриваются вопросы, связанные с деятельностью сообщества пентестеров. Проводится обзор проектов, связанных со стандартизацией сетевых сканеров и с возможностью генерации отчетов, содержащих описание уязвимостей со ссылками по каталогу CVE.*

Ключевые слова: *информационная безопасность, «черный ящик», сетевой сканер, пентест, CVE.*

Kizdermishov A.A.
Candidate of Physics and Mathematics, Associate Professor of Department of Automated Systems of Processing Information and Control at Engineering-Physics Faculty, Adyghe State University, Maikop, ph. (8772) 59-39-11, e-mail: Askhad_75@rambler.ru

On application of CVE-compatible network scanners

Abstract. *The paper describes a model of the intruder and examines the issues related to the activities of a community of penetration testers. Projects related to standardization of network scanners and the ability to generate reports that contain a description of vulnerabilities with links in the catalog CVE, are reviewed.*

Keywords: *information security, «black box», a network scanner, penetration test, CVE.*

Введение

В статье [1], исходя из предположения, что злоумышленник способен для подготовки атак на пользовательские информационные ресурсы применять метод «черного ящика», при этом основываясь только на результатах сканирования модели сетевого узла средствами свободно распространяемых сканеров, были описаны угрозы, возникающие в связи с этим предположением, и рассмотрены способы их нейтрализации. В том числе было обращено внимание на необходимость изучения возможностей demo-версий сетевых сканеров и их полноценных версий с условно-бесплатной лицензией (trial) или лицензией свободного распространения (free software), в части наличия возможности сканирования в режиме пентеста и аудита безопасности с генерацией отчета, содержащего описание уязвимостей со ссылками по каталогу CVE. В настоящей статье дан обзор именно таких сетевых сканеров.

Требования к сетевым сканерам

Прежде чем приступать к обзору, необходимо определить, какие требования предъявляются к сетевым сканерам. В первую очередь сканер должен обладать таким интерфейсом, чтобы предполагаемый нарушитель был способен самостоятельно научиться применять его для пентеста. В статье [1] дано следующее описание модели предполагаемого нарушителя:

1) с точки зрения наличия права доступа к объекту защиты нарушитель является лицом, не имеющим права доступа, так называем внешним нарушителем;

2) в целом потенциал нападения нарушителя можно считать довольно низким;

3) модель нарушителя близка к типу H1 или категории I, определенных в соответствии с [2, 3], но обладает меньшими возможностями, чем у этих типовых моделей.

Далее будем назвать такого нарушителя нарушитель типа H0.

Исходя из описания нарушителя типа H0 имеет смысл ответить на вопросы: способен ли он освоить любое из свободно распространяемых средств пентеста и какие ограничения на обзор может наложить низкая квалификация нарушителя.

Очевидно, что нарушитель типа H0 неспособен, используя средства виртуализации, самостоятельно собирать реалистичные стенды и отрабатывать на них практическое применение методов и средств пентеста, информацию о которых можно легко найти в Интернете. Однако в последнее время для тех, у кого нет навыков самостоятельно собирать стенды, и для тех, кто желает легально освоить методы пенстета на более высоком профессиональном уровне, появились специализированные сайты, так называемые «головоломки для хакеров». Суть этих ресурсов в том, чтобы предоставить сетевой узел для обучения пентесту. Такие ресурсы могут быть реализованы как непосредственно в сети Интернет, так и в виде специального программного обеспечения, предназначенного для установки на свой собственный веб-сервер, либо распространяются в виде образа виртуальной машины, которую необходимо скачать и запустить. Сравнению и описанию подобных проектов посвящено много работ, например, обзоры [4, 5]. Таким образом создана доступная среда, в которой нарушитель типа H0 может легально получать навыки владения средствами пентеста.

Также целесообразно оценить, насколько разными могут быть навыки нарушителей рассматриваемого типа. Во-первых, согласно статистике по проведению тестов на проникновение, общее количество успешных атак на основе пентестов с каждым годом падает, при этом доля в них успешных тестов с использованием социальной инженерии, которой наш тип злоумышленника не владеет, растет [4]. Таким образом, доля атак, совершаемых нарушителями с низким потенциалом, относительно невелика и со временем уменьшается. Во-вторых, сообщество непрофессиональных и профессиональных пентестеров перестает быть «разношерстным» и стремится к стандартизации [4]. Настоящим прорывом в направлении стандартизации тестирования на проникновение стало создание в 2011 году Стандарта выполнения тестов на проникновение (Penetration Testing Execution Standard – PTES), разрабатываемого сообществом пентестеров [4, 6].

Таким образом, существование нарушителей с заданным потенциалом нападения не вызывает сомнений, при этом в рамках описанной нами задачи они имеют во многом схожие навыки применения средств пентеста, способны изучить и использовать любой свободно распространяемый сетевой сканер. Следуя этому выводу в ходе обзора средств пентеста, не будем применять к ним дополнительных требований, кроме требований о том, что само средство пентеста должно быть бесплатным и отчет выполненного им сканирования должен содержать описание уязвимостей со ссылками по каталогу CVE [7]. Напомним, что наличие в отчете сканирования описания уязвимости со ссылками по каталогу CVE является важным преимуществом, т.к. позволяет и владельцу информационного ресурса, и нарушителю получать информацию об уязвимостях, которую они не имеют возможности (времени, квалификации и т.п.) самостоятельно найти и верно интерпретировать [1]. Сказанное в первую очередь относится именно к результатам работы пентестера с низким потенциалом нападения. По сути, CVE – это «словарь» известных уязвимостей, имеющий строгую характеристику по описательным критериям, что отличает его от Bugtrack-ленты. Текущее состояние CVE публикуется в Национальной Базе Уязвимостей США (NVD) [8] и на официальном сайте CVE [7]. По состоянию на сегодняшний день официально как CVE-совместимые зарегистрированы продукты и сервисы в количестве 146 условных единиц, представленные 79 разработчиками, принимающими участие в проекте CVE [7].

Программные средства сканирования для нарушителя типа H0

Теперь выясним, какими программными средствами предпочтет пользоваться рассматриваемый тип нарушителя. В первую очередь нарушитель типа H0 будет искать

программное обеспечение с дружественным интерфейсом на родном языке. Следует отметить, что в проекте CVE принимают участие две российские компании – ЗАО «АЛТЭКС-СОФТ» и ЗАО «Позитив Технолоджиз» [7, 9], причем доля ЗАО «Позитив Технолоджиз» на российском рынке инструментальных средств анализа защищенности, согласно исследованию, проведенному независимым информационным аналитическим центром, составляет 99% [10]. В отличие от ЗАО «Позитив Технолоджиз», ЗАО «АЛТЭКС-СОФТ» представлен репозиторий языка OVAL (Open Vulnerability and Assessment Language) для разработчиков программного обеспечения. Очевидно, что в рамках рассматриваемой нами задачи программные продукты и сервисы, представленные отечественными разработчиками, не могут быть использованы как свободно распространяемые средства пентеста, т.к. продукты ЗАО «Позитив Технолоджиз» являются коммерческими, а применение репозитария ЗАО «АЛТЭКС-СОФТ» требует навыков программирования.

Особое внимание следует уделить тем средствам пентеста, которые доступны рассматриваемому типу нарушителя. Это программные продукты, на сайтах разработчиков которых выложены для свободного скачивания как demo-версии, так и полноценные версии с условно-бесплатными лицензиями (trial) или лицензиями свободного распространения (free software). Так как по этическим соображениям не рассматривается возможность скачивания взломанного лицензионного программного обеспечения, проведем анализ средств пентеста, выложенных на официальных сайтах разработчиков, которые опубликованы на сайте проекта CVE. Результаты анализа информации, представленной на сайтах разработчиков CVE-совместимого программного обеспечения, показаны на рисунке 1.

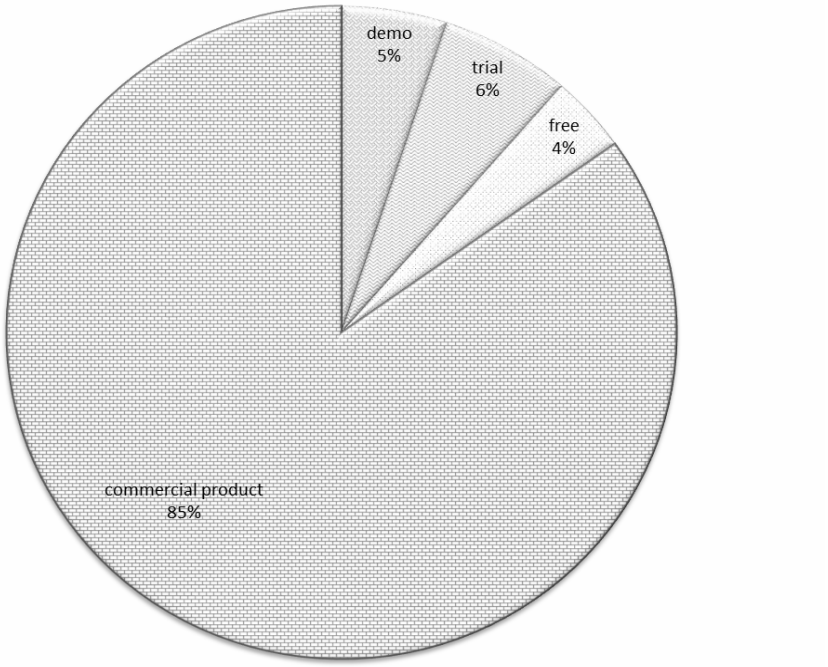

Рис. 1. Распределение долей между demo, trial, free, commercial product средств пентеста, разработанных участниками проекта CVE

Из рисунка 1 следует, что нарушитель типа H0 имеет возможность легально получить средства для пентеста, т.к. суммарная доля доступного ему программного обеспечения составляет порядка 15,2% от общего количества средств пентеста, обладающих заданными характеристиками. Тем не менее современное состояние таково, что общее количество сканеров, которыми нарушитель сможет воспользоваться, не превышает двенадцати [7]. Краткое описание этих сканеров приведено в таблице 1.

Таблица 1

Средства пентеста

№ п/п	Краткое описание	Наименование	Разработчик	Версия
1.	Сетевой сканер, предназначенный для пентеста Web-приложений	DragonSoft Secure Scanner	DragonSoft Security Associates, Inc.	Полная версия (trial)
2.	Классический сканер сетевой безопасности с функциями инвентаризации оборудования и углубленным сканированием по известным уязвимостям, в отчете выдает рекомендации по устранению уязвимостей	AdventNet, Inc.	ManageEngine Security Manager Plus	Demo-версия
		Beyond Security Ltd.	AVDS	Demo-версия
		GFI Software Ltd.	GFI LANguard Network Security Scanner	Полная версия (trial)
		LANDesk Software Inc.	LANDesk Security Suite	Полная версия (trial)
		Rsam	Rsam	Demo-версия
		Security-Database	Security Database Website	Полная версия (free)
		Skybox Security Inc.	Skybox View Enterprise Suite	Полная версия (trial)
		Tenable Network Security Inc.	Security Center. Passive Vulnerability Scanner	Demo-версия
		Tripwire, Inc.	Tripwire IP360	Полная версия (free)
3.	Классические сканеры сетевой безопасности, дополненные возможностью анализа результатов группового сканирования	Beyond Trust	Retina Network Security Scanner	Полная версия (trial)
		Rapid7 LLC	Metasploit Pro	Полная версия (free)

Из таблицы 1 следует, что все CVE-совместимые средства пентеста, которые доступны рассматриваемому типу нарушителя, можно условно разделить на специализированные, предназначенные для пентеста отдельных служб и сервисов, например, Web-приложений, классические сканеры сетевой безопасности и классические сканеры сетевой безопасности, дополненные возможностью анализа результатов группового сканирования. В рамках сформулированной задачи интерес представляет только вторая группа средств пентеста. Очевидно, что нарушителю типа H0 не нужны специализированные сканеры и нет необходимости проводить анализ группового сканирования, т.к. он подготавливает атаку только на один сетевой узел.

Из оставшихся 9 сетевых сканеров следует обратить внимание на те «экзотические» средства пентеста, которые редко или никогда не попадают в обзоры соответствующего программного обеспечения [4, 5, 11-13]. Это ManageEngine Security Manager Plus, LANDesk Security Suite, Rsam, Security Database Website, Skybox View Enterprise Suite, Security Center. Passive Vulnerability Scanner, Tripwire IP360. Особое внимание к возможностям этих сетевых сканеров обусловлено необходимостью исключить неожиданный рост потенциала нападения нарушителя в рамках его типа H0, за счет реализации угрозы наличия в «экзотических» сканерах отдельных более удачных чем у их аналогов технических решений, которые не были широко представлены в обзорах. Тот факт, что из 9 сканеров в русскоязычных обзорах описаны только AVDS и GFI LANguard Network Security Scanner, подтверждает утверждение, сделанное в статье [1], о том, что требуется уделять больше внимания подготовке обзоров, посвященных CVE-совместимым сетевым сканерам.

Заключение

В области обеспечения информационной безопасности компьютерных систем сложилась ситуация, когда успешная сетевая атака может быть проведена злоумышленником-самоучкой, изначально не имеющим никаких навыков по применению средств пентеста, но обладающим достаточной настойчивостью для подготовки атаки. Основным отличием сложившейся ситуации от ситуации прошлых лет является тот факт, что теперь для подготовки сетевой атаки, в том числе для самообучения нарушителя, могут быть использованы абсолютно легальные средства и ресурсы.

Примечания:

1. Киздермишов А.А. Анализ возможности использования свободно распространяемых сетевых сканеров // Вестник Адыгейского государственного университета. Сер. Естественно-математические и технические науки. 2014. Вып. 3 (142). С. 201-205. URL: http://vestnik.adygnet.ru
2. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, утв. ФСБ РФ 21 февраля 2008 г. № 149/54-144.
3. Модель угроз и нарушителя безопасности персональных данных, обрабатываемых в типовых информационных системах персональных данных отрасли, утв. Научно-техническим советом Минкомсвязи РФ от 21 апреля 2010 г. № 2.
4. URL: https://xakep.ru
5. Сравнение сканеров безопасности. Ч. 1. Тест на проникновение // Информзащита. 2008. 50 с.
6. Penetration Testing Execution Standard – PTES. URL: http://www.pentest-standard.org
7. CVE-Compatible Products and Services. URL: http://cve.mitre.org/compatible
8. National Vulnerability Database. URL: http://nvd.nist.gov
9. Официальный сайт ЗАО «Позитив Технолоджиз». URL: http://www.ptsecurity.ru
10. Рынок систем сетевой безопасности, аппаратных средств двухфакторной аутентификации и инструментальных средств анализа защищенности в России // Независимый информационно-аналитический центр. URL: http://www.anti-malware.ru/analytics
11. Марков А.С., Миронов С.В., Цирлов В.Л. Опыт тестирования сетевых сканеров уязвимостей // Информационное противодействие угрозам терроризма. 2007. № 5. С. 109-122.
12. Цирлов В.Л. Выбор сетевого сканера для анализа защищенности сети // PC Week / RE. 2005. № 17 (479).
13. Игра на опережение: обзор сканеров безопасности корпоративных IT-систем. URL: http://servernews.ru/597271

References:

1. Kizdermishov A.A. The analysis of the possibility to use the freeware network scanners // The Bulletin of the Adyghe State University. Ser. Natural-Mathematical and Technical Sciences. 2014. Iss. 3 (142). P. 201-205. URL: http://vestnik.adygnet.ru
2. Methodological recommendations for the security of personally identifiable information by means of cryptomaterial during its processing in information systems of personally identifiable information using automation means, approved by the FSB of the RF on 21 February 2008. No. 149/54-144.
3. The model of threat and security breaker of personally identifiable information processed in the typical information systems of personally identifiable information of the industry, approved by The scientific and technical Council of the RF Ministry of Communications dated by April 21, 2010. No. 2.
4. URL: https://xakep.ru
5. Comparison of security scanners. Pt. 1. The penetration test // Informzaschita, 2008. 50 pp.
6. Penetration Testing Execution Standard – PTES. URL: http://www.pentest-standard.org
7. CVE-Compatible Products and Services. URL: http://cve.mitre.org/compatible
8. National Vulnerability Database. URL: http://nvd.nist.gov
9. The official website of the joint-stock comp. «Positive Technologies». URL: http://www.ptsecurity.ru
10. The market of systems of network security, two-factor authentication hardware and toolkit of analysis of security in Russia // Independent Information-analytical Center. URL: http://www.anti-malware.ru/analytic
11. Markov A.S., Mironov S.V., Tsirlov V.L. Experience in testing the network scanners of vulnerability // Information Counteraction to Terrorism Threats. 2007. No. 5. P. 109-122.
12. Tsirlov V.L. Selecting a network scanner for analyzing network security // PC Week / RE. 2005. No. 17 (479)
13. The outrunning game: a review of scanners of security of corporate IT systems. URL: http://servernews.ru/597271