УДК 004.056.53
ББК 32.973.202-018.2
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

Анализ возможности использования свободно распространяемых сетевых сканеров

(Рецензирована)

Аннотация. *Рассмотрена задача применения свободно распространяемых сетевых сканеров для обеспечения «минимального уровня» защиты пользовательских информационных ресурсов в части предотвращения атак, основанных на сборе исходных данных об объекте защиты методом «черного ящика».*

Ключевые слова: *защита информации, «черный ящик», сетевой сканер.*

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

The analysis of the possibility to use the freeware network scanners

Abstract. *The paper discusses the problem related to the application of open-source network scanners to provide a «minimum level» of protection of user information resources to prevent attacks based on the collection of baseline data on the subject of protection by the «black box» method.*

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

Число произошедших в последнее время инцидентов, связанных с утечкой информации, обстоятельства которых широко освещены в средствах массовой информации [1-3], свидетельствуют о следующих фактах:

1) в современном мире не существует систем защиты информации, применение которых полностью гарантировало бы защищенность данных, обрабатываемых в информационных системах;

2) задача по защите огромного объема информации, обрабатываемой персональными компьютерами по всему миру, с каждым годом становится все более актуальной.

Именно этими обстоятельствами обусловлен растущий интерес владельцев информационных ресурсов не только к построению систем защиты информации, но и к системам оценки защищенности (средствам контроля защищенности) автоматизированных информационных систем [4-5]. Кроме того в современных условиях, например, для критичных узлов и сервисов вычислительной (компьютерной) сети, оценка защищенности не может проводиться, как это было в конце прошлого века, с периодичностью в несколько лет силами узкого числа специалистов, приглашаемых владельцем информационного ресурса для проведения этой работы, требует проведения мероприятий по анализу защищенности от самих владельцев информационных ресурсов.

Таким образом, перед разработчиками средств защиты информации, кроме традиционной задачи по созданию профессиональных средств контроля защищенности, возникла задача по существенному совершенствованию средств, предназначенных для владельцев информационных ресурсов, самостоятельно обеспечивающих защиту информации пользовательских информационных ресурсов. Такие средства позволяют провести аудит безопасности или пентест, как принято называть метод оценки безопасности компьютерных систем или сетей средствами моделирования атаки злоумышленника. Сложившаяся ситуация привела к появлению довольно эффективных сетевых

сканеров, поддерживающих режимы аудита безопасности и пентеста. По состоянию на сегодняшний день, сетевые сканеры являются наиболее доступными и широко используемыми средствами анализа защищенности, что однозначно способствует росту эффективности защиты информации. Однако, тот факт, что с сайтов разработчиков этих сканеров любой пользователь сети Интернет может скачать бета-версии, полноценные версии с условно-бесплатной лицензией (*trial*) или лицензией свободного (*free software*) программного обеспечения (далее свободно распространяемые сетевые сканеры), в случае возникновения условий, когда этим сканером сможет воспользоваться злоумышленник, приводит к возникновению угрозы безопасности информации. Складывается ситуация, в которой результатом защиты информации, достигаемым в том числе применением свободно распространяемых сетевых сканеров, должно быть предотвращение ущерба обладателю информации (цель защиты информации) из-за возможной утечки информации и (или) несанкционированного и непреднамеренного воздействия на информацию, которые могут возникнуть в результате применения злоумышленником тех же средств сканирования. В нашей статье мы намерены провести анализ этой ситуации, мы ограничимся рассмотрением вопросов контроля защищенности сетевых узлов вычислительных (компьютерных) сетей в части применения результатов сканирования свободно распространяемыми сетевыми сканерами для обеспечения «минимального уровня» защиты. Под «минимальным уровнем» защиты будем понимать уровень защиты, способный блокировать атаку нарушителя, предпринятую исключительно на основе анализа защищенности, проведенного средствами свободно распространяемых сетевых сканеров.

В рассматриваемом нами случае модель объекта защиты – это информационный ресурс, являющийся предметом собственности и подлежащий защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации, ущерб от возможной утечки информации и (или) несанкционированного и непреднамеренного воздействия на информацию (разглашения) которых существенно ниже стоимости построения профессиональной комплексной системы сетевой защиты и соответствует стоимости встроенных механизмов защиты операционной системы и антивирусного программного обеспечения, что соответствует персональной рабочей станции физического лица (в том числе мобильные средства вычислительной техники), подключенной к сети Интернет [6]. Структура информации объекта защиты, которая подлежит защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником, в рамках рассматриваемой модели, описана в таблице 1 [7].

«Персоналом» объекта защиты является сам владелец информационного ресурса – «продвинутый пользователь», способный самостоятельно настраивать системное и прикладное программное обеспечение. Применяются встроенные в операционную систему средства сетевой защиты и установленные антивирусные средства, а так же свободно распространяемые сетевые сканеры (для оценки контроля защищенности системы). Все средства сетевой защиты настроены по умолчанию, либо по предопределенном разработчиком шаблону настройки. Предполагается, что для доступа в Интернет не используются прокси-сервер и межсетевой экран, а так же то, что провайдер не оказывает услуг по защите от сетевых атак.

В рамках нашей модели рассматривается один возможный канал утечки информации – это несанкционированный доступ по компьютерной сети. Предполагается, что программное обеспечение свободно распространяемых сканеров скачивалось с официальных сайтов разработчиков и не содержит недекларированных возможностей. Обзорам сетевых сканеров, рекомендациям по выбору сетевых сканеров посвящено множество работ [8, 9], в которых сканеры сопоставляются по таким, безусловно, важным ха-

рактеристикам, как цена, количество ложных срабатываний, удобство интерфейсов и т.п., однако, мы не нашли обзора, в котором сетевые сканеры сравнивались по таким параметрам, как наличие возможности сканирования в режиме пентеста и аудита безопасности с генерацией отчета, содержащего описание уязвимости со ссылками по каталогу CVE, несмотря на то, что такие свободно распространяемые сканеры встречаются во всех без исключения обзорах. Наличие описания уязвимости со ссылками по каталогу CVE является важным преимуществом, например, в рамках описанной в нашей статье модели, так как 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. В продолжение этой статьи мы намерены подготовить такой обзор.

Таблица 1

Пользовательские информационные ресурсы

№ п/п	Описание информации	Наименование тайны	В соответствии с каким документом подлежит защите
1.	Личная переписка, пароли и коды доступа к аккаунтам	Личная тайна и семейная тайна, персональные данные	«Конституция Российской Федерации» (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ), Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 23.07.2013) «О персональных данных»
2.	Личные фотографии и видеофильмы, изображение с вебкамеры и звук с микрофона	Личная тайна и семейная тайна, персональные данные	Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 23.07.2013) «О персональных данных», «Гражданский кодекс Российской Федерации (часть первая)» от 30.11.1994 № 51-ФЗ (ред. от 02.11.2013)
3.	Сведения, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам	Коммерческая тайна	Федеральный закон от 29.07.2004 № 98-ФЗ (ред. от 11.07.2011) «О коммерческой тайне»

Очевидно, что в качестве атакуемого объекта может выступать любой информационный ресурс, но нами выбран именно этот объект защиты, так как нарушитель, атакующий исключительно на основе анализа защищенности, проведенного средствами свободно распространяемых сетевых сканеров, обладает довольно низким потенциалом нападения и, очевидно, не является источником угрозы информационной безопасности для объектов защиты с уровнем защиты выше «минимального». Будем считать, что ценность содержащейся на машинных носителях объекта защиты коммерческой информации представляется незначительной, тогда на первый план, безусловно, выходит задача по защите личной и семейной тайны, а так же персональных данных. Как известно, утечка персональных данных может привести к существенному ущербу в случае, если они содержат специальные категории персональных данных и биометрические персональные данные. Следует отметить, что решение подобных задач для случая любых информационных ресурсов, кроме пользовательских, потребовало бы от оператора существенных финансовых затрат, направленных на приведение автоматизированной системы в соответствие с требованиями приказов Федеральной службы по техническому и экспортному контролю России [10, 11].

С точки зрения наличия права доступа к объекту защиты нарушитель является лицом, не имеющим права доступа, так называемым внешним нарушителем. В связи с чем модель нарушителя близка к типу Н1 или категории I, определенных в соответствии с [12, 13]. Однако возможности нарушителя ниже, чем у вышеупомянутых типовых

моделей. В целом, потенциал нападения нарушителя можно считать низким. Предполагается, что нарушитель имеет все доступные (свободно распространяемые) средства для подготовки и проведения атак на защищаемые информационные ресурсы.

В отношении объекта защиты в качестве внешнего нарушителями могут выступать следующие лица:

– бывшие друзья, члены семьи, знакомые и т.п.;

– посторонние лица, пытающиеся получить доступ к объекту защиты в инициативном порядке;

– представители преступных организаций.

Нарушитель может осуществлять следующие действия:

– атаки на объект защиты путем реализации угроз удаленного доступа;

– нахождение методом «черного ящика» уязвимостей информационной системы, подразумевается, что нарушитель способен сопоставить результаты пентеста соответствующим результатам аудита безопасности, который он провел заранее на модельной информационной системе, и на основе этого сопоставления верно предположить наличие обнаруженных при аудите безопасности модельной информационной системы уязвимостей так же и у объекта защиты.

Таким образом, для достижения «минимального уровня» защиты мы рекомендуем выполнять несколько несложных правил:

1. Отказаться от настройки элементов средств сетевой защиты по умолчанию, либо по предопределенному разработчиком шаблону, так как это может позволить нарушителю создать модельную информационную систему и применить метод «черного ящика» для получения исходных данных об объекте защиты. Имея исходные данные, нарушитель сможет провести эффективную атаку, используя описания уязвимостей, в том числе из каталога CVE.

2. Использовать свободно распространяемые сетевые сканеры для выявления угроз информационной безопасности, в том числе угроз, возникающих как следствие описанной выше возможности нарушителя использовать метод «черного ящика» для подготовки атаки. В этих целях после каждого обновления операционной системы и антивирусного программного обеспечения необходимо осуществлять поиск уязвимостей средствами нескольких свободно распространяемых сетевых сканеров. По результатам сканирования необходимо принимать меры по устроению уязвимостей, связанных с настройкой программного обеспечения или рекомендуемой дополнительной установкой обновлений. В случаях, если в результате сканирования обнаружены неустранимые уязвимости, следует обращать внимание на признаки реализации угроз, связанных с этими уязвимостями, либо отключить объект защиты от компьютерной сети до нахождения решения по устранению уязвимости. Таким образом возможно блокировать атаку нарушителя, устранив уязвимости, о которых ему известно.

3. Так как владелец информации является непосредственным исполнителем мероприятий по обеспечению информационной безопасности, он обязан знать об изменениях в законах, нормативных и руководящих документах в части, касающейся обрабатываемой им информации. Так же необходимо владеть информацией о гражданском законодательстве в части положений о нематериальных благах и их защите. Следует отметить, что единственным эффективным гражданско-правовым способом защиты этих прав, без «хождения по судам», является самозащита гражданских прав, однако в условиях своеобразной российской уголовной правоприменительной практики использование данного способа путем ответной DoS атаки на сетевой узел нарушителя может быть классифицировано как уголовно наказуемое деяние, несмотря на то, что согласно уголовному праву в этом случае имеет место необходимая оборона.

Примечания:

1. Горковская М., Являнский И. О чем Сноуден написал канцлеру ФРГ // Izvestiia. 2013. № 208. С. 1.
2. Абдуллин Р., Тюкова Д., Субботин И. Сноуден уехал из «Шереметьево» на такси // Moskovskii komsomolets. 2013. № 164. С. 1.
3. Являнский И., Хурсандов Т. Сноуден заставил ЦРУ задуматься о секретности // Izvestiia. 2013. № 116. С. 7.
4. Барабанов А.В., Марков А.С., Цирлов В.Л. Методический аппарат оценки соответствия автоматизированных систем требованиям безопасности информации // Спецтехника и связь. 2011. № 3. С. 48-52.
5. Зензин И.И. Методики управления рисками информационной безопасности в автоматизированных системах // Безопасность информационных технологий. 2011. № 4. С. 113-116.
6. Аудит информационной безопасности органов исполнительной власти / В. Аверченков [и др.]. Litres, 2013. С. 101.
7. Конев А.А., Давыдова Е.М. Подход к описанию структуры системы защиты информации // Доклады ТУСУРа. 2013. Т. 28, № 2. С. 107-111.
8. Марков А.С., Миронов С.В., Цирлов В.Л. Опыт тестирования сетевых сканеров уязвимостей // Информационное противодействие угрозам терроризма. 2007. № 5. С. 109-122.
9. Сравнение сканеров безопасности. Ч. 1. Тест на проникновение. Информзащита, 2008. С. 50.
10. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: приказ ФСТЭК РФ от 18 февраля 2013 г. № 21. URL: http://fstec.ru/normotvorcheskaya/akty
11. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: приказ ФСТЭК РФ от 11 февраля 2013 г. № 17. URL: http://fstec.ru/normotvorcheskaya/akty
12. 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 // СПС «КонсультантПлюс». М., 2014.
13. 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. URL: minsvyaz.ru›common/upload/publication

References:

1. Gorkovskaya M., Yavlyanskiy I. What Snowden wrote to the German chancellor // Izvestiya. 2013. No. 208. P. 1.
2. Abdullin R., Tyukova D., Subbotin I. Snowden left «Sheremetyevo» by taxi // Moskovsky Komsomolets. 2013. No. 164. P. 1.
3. Yavlyanskiy I., Khursandov T. Snowden made CIA think of security // Izvestiya. 2013. No. 116. P. 7.
4. Barabanov A.V., Markov A.S., Tsirlov V.L. Methodological device of assessment of compliance of the automated systems to the requirements of information safety // Special equipment and communication. 2011. No. 3. P. 48-52.
5. Zenzin I.I. Techniques of risk control of information security in automated systems // Safety of information technologies. 2011. No. 4. P. 113-116.
6. Audit of information security of executive authorities / V. Averchenkov [etc.]. Litres, 2013. P. 101.
7. Konev A.A., Davydova E.M. Approach to the description of the structure of system of information security // Reports of TUSUR. 2013. Vol. 28, No. 2. P. 107-111.
8. Markov A.S., Mironov S.V., Tsirlov V.L. Experience of testing the network scanners of vulnerabilities // Information counteraction to terrorism threats. 2007. No. 5. P. 109-122.
9. Comparison of scanners of security. Pt. 1. Penetration test. Information protection, 2008. P. 50.
10. On the statement of the structure and maintenance of organizational and technical measures for safety of personal information at their processing in information systems of personal information: the order of FSTEK of the RF of February 18, 2013 No. 21. URL: http://fstec.ru/normotvorcheskaya/akty
11. On the approval of requirements on the protection of information which is not the state secret, containing in the state information systems: the order of FSTEK of the RF of February 11, 2013 No. 17. URL: http://fstec.ru/normotvorcheskaya/akty
12. Methodological recommendations on the providing by means of cryptosecurity aids of personal information at their processing in information systems of personal data usuing the automation equipment: approved by RF FSB on February 21, 2008 No. 149/54-144 // SPS «ConsultantPlus». M., 2014.
13. Model of threats and the violator of safety of the personal information processed in standard information systems of personal information of the branch: approved by Scientific and technical council of the Ministry of Telecom and Mass Communications of the RF on April 21, 2010. No. 2. URL: minsvyaz.ru›common/upload/publication