ТЕХНИЧЕСКИЕ НАУКИ

TECHNICAL SCIENCES

УДК 004.056
ББК 32.973
К 38

Киздермишов А.А.
Кандидат физико-математических наук доцент кафедра 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 построении модели нарушителя правил разграничения доступа к пользовательским информационном ресурсам

(Рецензирована)

Аннотация. *Рассматриваются вопросы, связанные с отсутствием единого подхода к построению модели нарушителя, положения нормативно-правовых актов в области защиты информации. Предложенная неформальная модель нарушителя позволяет создать или провести корректировку перечня актуальных угроз для пользовательских информационных ресурсов с учетом характеристик нарушителя.*

Ключевые слова: *информационная безопасность, модель нарушителя, «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 model creation for the breaker of rules of access to user information resources

Abstract. *The paper explores the lack of uniform approach to model creation of the computer trespasser and the provisions of normative legal acts in the field of information security. The offered informal model of the computer trespasser makes it possible to create or carry out updating of the list of actual threats to the user information resources taking into account characteristics of the computer trespasser.*

Keywords: *information security, model of the computer trespasser, «a black box», network scanner, pentest, CVE.*

В настоящее время значительный объем информации, являющейся предметом собственности и подлежащей защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации, обрабатывается на персональных рабочих станциях физических лиц (в т.ч. мобильные средства вычислительной техники), подключенных к сети Интернет (далее пользовательские информационные ресурсы). При этом ущерб от возможной утечки такой информации и (или) несанкционированного и непреднамеренного воздействия на информацию (разглашения) существенно ниже стоимости построения профессиональной комплексной системы сетевой защиты и соответствует стоимости встроенных механизмов защиты операционной системы и антивирусного программного обеспечения.

Хорошо известно, что построение адекватной защиты информационных ресурсов возможно только при наличии верно описанной модели нарушителя. В [1] рассмотрена неформализованная модель нарушителя, на основе которой предложены меры по защите пользовательских информационных ресурсов от сетевых атак злоумышленника-самоучки, не имеющего навыков по применению средств пентеста, но обладающего достаточной настойчивостью для их самостоятельного изучения. В продолжение [1] с

целью конкретизации возможных способов реализации угроз безопасности информации, в [2] было проведено исследование, в результате которого определены девять сетевых сканеров, demo и trial версии которых доступны для рассматриваемой модели нарушителя в качестве средств реализации атаки. Можно предположить, что модель нарушителя необходима только в случае, если применяются криптографические средства защиты информации, во всех остальных случаях достаточно разработать модель угроз безопасности информации. Однако детальная модель угроз безопасности информации должна содержать описание не только угроз безопасности информации, но и описание возможностей нарушителей (модель нарушителя). Таким образом, для рассматриваемой в статье задачи описание модели нарушителя является важным этапом построения системы защиты информации. Настоящая статья является продолжением работ [1, 2] и посвящена проблеме обеспечения пользовательских информационных ресурсов. Далее предложена уточненная (детализированная) модель нарушителя, учитывающая результаты, полученные в работах [1, 2].

Следует отметить, что не существует единого подхода к построению модели нарушителя, общим является только то, что все авторы и регуляторы (ФСБ России и ФСТЭК России) изначально делят всех нарушителей на внешних и внутренних. Несмотря на то, что в нашем случае речь идет о пользовательских ресурсах, для которых требования регуляторов носят рекомендательный характер, интересно рассмотреть, к какой категории (типу) нарушителя относится пентестер-самоучка, согласно классификации ФСТЭК России (табл. 1). Так как криптосредства не применяются, то классификация ФСБ России не рассматривается. В таблице 1 так же представлены типы нарушителей, разработанные другими авторами по собственным методикам.

Таблица 1

Классификация нарушителей
в соответствии с нормативными документами ФСТЭК России

Категория (тип)	Краткое описание	Источник
Первый уровень	Самый низкий уровень возможностей ведения диалога в автоматизированных системах (АС) – запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации.	[4]
Первая категория – лица, не имеющие права доступа в контролируемую зону ИСПДн	Атаки на информационную систему обработки персональных данных (ИСПДн) путем реализации угроз удаленного доступа.	[5]
Первый тип	Нарушители, не имеющие доступа к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена.	[6]
OutH2	Лица, не имеющие санкционированный доступ в периметр защиты: гость (незарегистрированный пользователь), хакеры-самоучки и т.д.	[3]
Категория 7	Могут воздействовать на все уровни с целью хищения информации, самоутверждения, а также вывода из строя АС. При этом используют методы и средства активного воздействия (модификация и подключение дополнительных технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ).	[7]

Следует отметить, что во всех рассмотренных методиках построения модели нарушителя описана категория (тип) нарушителя, схожая с требуемой. Совместив методики, приведенные в таблице 1, получим следующие характеристики нарушителя (далее модель нарушителя типа H0):

1. Внешний нарушитель, не имеющий доступа к пользовательским информационным ресурсам, реализующий угрозы запуска задач (программ) из фиксированного набора функций по обработке информации, реализованных в системе, или угрозы удаленного доступа из внешних сетей связи общего пользования и (или) сетей международного информационного обмена.

2. Целями атаки могут быть хищение или искажение пользовательских информационных ресурсов:

– личные фотографии и видеофильмы;

– изображение с вебкамеры и звук с микрофона;

– личная переписка, пороли и коды доступа к аккаунтам;

– сведения, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, и т.п.

3. В качестве нарушителей могут выступать следующие лица, изначально не имеющие знаний и навыков по применению средств пентеста:

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

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

– представители преступных организаций.

4. Мотивация нарушителя:

– желание самоутвердиться;

– вандализм;

– месть;

– корыстные интересы.

5. Уровень знаний нарушителя:

– начальные знания о структуре вычислительных систем, стеке протокола IP;

– навыки применения стандартного набора программ;

– не способен, используя средства виртуализации, самостоятельно собирать реалистичные стенды и отрабатывать на них практическое применение методов и средств пентеста;

– способен самостоятельно изучить и применять методы пентеста, используя специализированные сайты и программное обеспечение, так называемые «головоломки для хакеров»;

– способен самостоятельно освоить стандарт выполнения тестов на проникновение (Penetration Testing Execution Standard – PTES), разрабатываемого сообществом пентестеров [9, 10];

– начальные знания о применении метода «черного ящика»;

– обладает достаточной степенью настойчивости для самообучения.

6. Время и место проведения атаки: нарушитель будет атаковать, используя собственное средство вычислительной техники, преимущественно в нерабочее время, удаленно с использованием перехвата информации, передающейся по каналам передачи данных, или без ее использования.

7. Используемые для подготовки и проведения инструменты: описание уязвимостей в каталоге CVE [8] и demo/trial средств пентеста, результаты сканирования которых содержат ссылки на номера уязвимостей в каталоге CVE (табл. 2).

8. Типовой сценарий возможных действий нарушителя:

Шаг 1. Приобретение (бесплатное скачивание с сайта разработчика) demo/trial средств пентеста (табл. 2).

Шаг 2. Изучение работы приобретенного средства пенстеста по публикациям в сети Интернет и легальной среды для обучения пентесту, так называемые «головоломки для хакеров» [2].

Таблица 2

Средства пентеста

№ п/п	Разработчик	Наименование
1.	AdventNet, Inc.	ManageEngine Security Manager Plus
2.	Beyond Security Ltd.	AVDS
3.	GFI Software Ltd.	GFI LANguard Network Security Scanner
4.	LANDesk Software Inc.	LANDesk Security Suite
5.	Rsam	Rsam
6.	Security-Database	Security Database Website
7.	Skybox Security Inc.	Skybox View Enterprise Suite
8.	Tenable Network Security Inc.	Security Center. Passive Vulnerability Scanner
9.	Tripwire, Inc.	Tripwire IP360

Шаг 3. Выбор объекта атаки: случайный, поиск по общедоступным сведениям. По этическим соображениям в статье не рассматриваются методы поиска исходных данных для атаки.

Шаг 4. Сетевое сканирование объекта атаки (атака типа «Сетевая разведка», которая проводится в форме запросов DNS, эхо-тестирования, сканирования портов и мн.др.).

Шаг 5. Интерпретация полученных результатов сканирования (анализ возможности использования обнаруженных уязвимостей для проведения атаки). Интерпретация проводится нарушителем самостоятельно с использованием каталога CVE и может продолжаться несколько дней.

Шаг 6. Подготовка атаки, реализующей угрозы запуска задач (программ) из фиксированного набора функций по обработке информации, реализованных в системе, или угрозы удаленного доступа.

Шаг 7. Проведение атаки «напрямую» или через один «анонимный PROXY» (рис. 1).

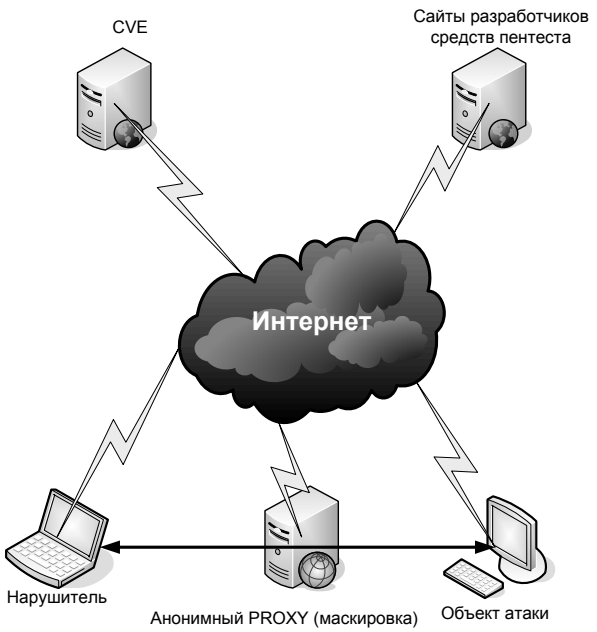

Рис. 1. Атака на пользовательские ресурсы

Рисунок 1 наглядно иллюстрирует минимальность средств, необходимых нарушителю типа H0 для подготовки и проведения атак. При этом возможны атаки следующих типов:

– «Несанкционированный доступ»;
– «Атаки на уровне приложений»;
– «Парольная атака»;
– все виды спуфинга.

На этом построение неформализованной модели нарушителя типа H0 завершено.

В заключение отметим, что описанная выше неформальная модель нарушителя позволяет создать или провести корректировку перечня актуальных угроз для пользовательских информационных ресурсов с учетом характеристик нарушителя. Определению перечня актуальных угроз для пользовательских информационных ресурсов будет посвещена следующая статья.

Примечания:

1. Киздермишов А.А. К вопросу о применении CVE-совместимых сетевых сканеров // Вестник Адыгейского государственного университета. Сер. Естественно-математические и технические науки. 2015. Вып. 1 (154). С. 136-140. URL: http://vestnik.adygnet.ru
2. 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
3. Ершов В.Н., Смирнова П.Л. Информационная защита персональных данных: доминирующий источник угрозы // Бизнес-Информатика. 2012. № 2 (20). С. 71-76. URL: http://ecsocman.hse.ru/mags/bi/
4. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации: Руководящий документ. М.: Гостехкомиссия России, 1992.
5. 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.
6. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных: утв. заместителем директора ФСТЭК России 14 февраля 2008 г.
7. Жуков В.Г., Жукова М.Н., Стефаров А.П. Модель нарушителя прав доступа в автоматизированной системе // Программные продукты и системы. 2012. № 2 (98). С. 75-78.
8. CVE-Compatible Products and Services. URL: http://cve.mitre.org/compatible

References:

1. Kizdermishov A.A. On application of CVE-compatible network scanners // The Bulletin of the Adyghe State University. Ser. Natural-Mathematical and Technical Sciences. 2015. Iss. 1 (154). P. 136-140. URL: http://vestnik.adygnet.ru
2. 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
3. Ershov V.N., Smirnova P.L. Information protection of personal data: the threat dominant source // Business Informatics. 2012. No. 2 (20). P. 71-76. URL: http://ecsocman.hse.ru/mags/bi/
4. The concept of protection of computer aids and the automated systems from unauthorized access to information: a guideline. M.: Gostekhkomissiya Rossii, 1992.
5. 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.
6. Technique of definition of actual threats of safety of personal data at their processing in information systems of personal information: approved by the Deputy director of FSTEC of Russia on February 14, 2008.
7. Zhukov V.G., Zhukova M.N., Stefarov A.P. Model of the violator of access rights in the automated system // Software Products and Systems. 2012. No. 2 (98). P. 75-78.
8. CVE-Compatible Products and Services. URL: http://cve.mitre.org/compatible