В. С. Горбатов, А. А. Мещеряков

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СРЕДСТВ КОНТРОЛЯ ЗАЩИЩЕННОСТИ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

Введение

В настоящее время очевидным фактором обеспечения устойчивости деятельности многих организаций, в частности непрерывности бизнеса, стало состояние информационной безопасности их систем управления. Используемые современные вычислительные сети организаций содержат множество критичных узлов и сервисов, нарушение доступности и целостности которых может привести к нанесению значительного ущерба. Поэтому высокая защищенность сетей от угроз информационной безопасности приобретает все большую актуальность и требует для практической реализации все большее количество ресурсов.

В итоге непременным компонентом системы обеспечения информационной безопасности является подсистема выявления уязвимостей, представляющая собой комплекс организационно-технических мероприятий и предназначенная для контроля защищенности вычислительной сети и устранения обнаруженных уязвимостей [1].

Современный период развития инструментальных средств контроля защищенности вычислительных сетей характеризуется стремительным переходом от ручных процедур измерений к специализированным автоматизированным процедурам. На рынке уже предлагается достаточно много таких средств контроля защищенности, что ставит непростую задачу обоснования выбора того или иного варианта.

В статье приведены результаты исследований, являющихся логическим продолжением работ [2, 3] с учетом современного состояния развития средств контроля защищенности вычислительных сетей.

В ходе исследований проведен анализ сущности современного процесса контроля защищенности вычислительных сетей и соответствующей нормативной базы, на основании которого выполнено инструментальное тестирование ряда предлагаемых на рынке средств.

1. Методология контроля защищенности вычислительных сетей

1.1. Понятие защищенности

Одним из вариантов определения защищенности является обоснование степени адекватности реализованных механизмов защиты информации в сопоставлении с существующими в данной среде угрозами безопасности информации и соответствующими рисками их реализации. Под обобщенными угрозами безопасности информации традиционно понимается возможность нарушения таких свойств информации, как конфиденциальность, целостность и доступность. Иными словами, защищенность вычислительной сети — это совокупность ее состояний, в которых обеспечивается безопасность информационных активов системы управления организации, т. е. их конфиденциальность, целостность и доступность.

Контроль состояния защищенности относится к категории так называемых превентивных защитных механизмов. Его главное назначение — своевременно «заметить» слабость (уязвимость) в защищаемой системе управления, обеспечить ее устранение и тем самым предотвратить возможные атаки с ее использованием.

Таким образом, оценка защищенности предполагает поиск «дыр» в системе безопасности, проверку устойчивости вычислительной сети к атакам и т. д. Под средствами контроля защищенности будем понимать подсистему поиска уязвимостей, возникающих при проектировании, практической реализации и в ходе эксплуатации вычислительной сети, выполняющую предупредительный поиск

уязвимых мест путем анализа настроек аппаратного и программного обеспечения сети (пассивный поиск) и имитацией сетевых атак (активный поиск) [4].

1.2. Нормативная база анализа защищенности

Наиболее значимыми нормативными документами в области информационной безопасности, определяющими критерии для оценки защищенности и требования, предъявляемые к механизмам защиты, по-прежнему остаются Руководящие документы (РД) Гостехкомиссии России [5] наряду с современными стандартами [6, 7].

РД составляют основу нормативной базы в области защиты от НСД к информации и определяют наиболее значимые критерии для оценки защищенности автоматизированных систем и средств вычислительной техники. Практические правила управления информационной безопасностью [6] могут использоваться в качестве критериев для оценки механизмов безопасности организационного уровня, включая административные, процедурные и физические меры защиты. Так называемые «Общие критерии» [7] определяют функциональные требования безопасности и требования к адекватности реализации функций безопасности.

1.2. Типовая методика анализа защищенности

На данный момент существует ряд международных методик проведения анализа защищенности, указанных в следующих документах: Open Source Security Testing Methodology Manual (OSSTMM) [8], NIST SP800-15 [9], The Information System Security Assessment Framework (ISSAF) [10], PCI DSS [11].

Проводя их обобщение, можно заключить, что типовая методика анализа защищенности должна включать следующие этапы:

1. Изучение исходных данных о тестируемой сети;
2. Анализ состава, структуры и конфигурации критических элементов сетевой инфраструктуры;
3. Сканирование внешних сетевых адресов тестируемой сети из сети Интернет;
4. Внутреннее сканирование ресурсов сети;
5. Анализ конфигурации сети, серверов и рабочих станций сети при помощи специализированных средств контроля защищенности;
6. Обработка полученных результатов тестирования.

Средства контроля защищенности используются при тестировании как сети, так и системы ее защиты. В ходе тестирования проверяются используемые механизмы защиты, их устойчивость в отношении возможных атак, проводится поиск уязвимостей.

Типовая схема тестирования защищенности сети включает в себя этапы планирования, сбора информации, идентификации уязвимостей, проведения тестовых атак на систему, документирования.

В процессе планирования определяются цели и задачи тестирования. На этапе сбора информации происходит идентификация доступных сетевых устройств, топологии сети, открытых портов и т. д. Далее производится сопоставление собранных данных о сервисах, их версиях с информацией об известных уязвимостях. На этапе подтверждения уязвимостей иллюстрируется возможность получения несанкционированного доступа к системе.

2. Методика сравнительного анализа средств контроля защищенности вычислительной сети

Современное средство контроля защищенности вычислительных сетей должно предоставлять надежный инструментарий, способный эффективно обеспечить сложный процесс мониторинга сетевой безопасности при минимальном вмешательстве специалиста в рутинные задачи сканирования.

За основу для сравнительного анализа средств контроля защищенности вычислительных сетей можно принять методики, описанные в [2, 3] с некоторой модификацией для получения более адекватной оценки их эффективности.

В качестве среды (испытательного стенда) тестирования средств контроля защищенности выбирается типовая сеть некоторого объекта информатизации, включающая подсеть класса С с рабочими станциями, функционирующими под управлением распространенных операционных систем: Microsoft Windows XP SP1, Microsoft Windows XP SP2, Microsoft Windows 2003 Server, Slackware Linux. Помимо их стандартных сервисов целесообразно дополнительно использовать веб-сервер Apache, серверы баз данных MySQL, Postgres, ftp-сервер TFTPD, VNC Server, веб-сервер IIS. Установка всех средств и систем выполняется в режимах по умолчанию.

Схема испытательного стенда среды представлена на рис. 1.

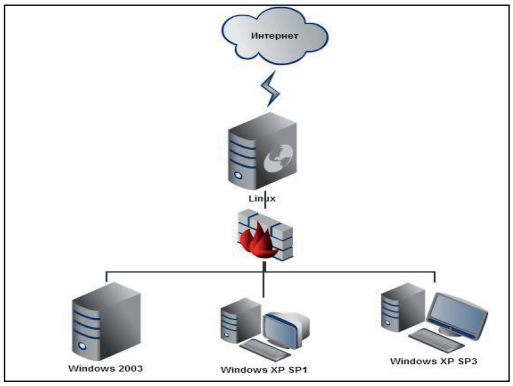

Рис. 1. Схема испытательного стенда среды

Средства контроля защищенности устанавливаются внутри периметра сети, что обеспечивает доступ ко всем компьютерам сети и тем самым позволяет получить наиболее полный отчет о состоянии их защищенности.

В ходе сравнительного анализа проводятся оценки качества идентификации сервисов, приложений, уязвимостей, анализ удобства интерфейса и полноты формирования отчетов. Оценка качества идентификации сервисов и приложений включает в себя совокупность следующих проверок: сканирование портов, идентификация ОС, идентификация сервисов и приложений.

Таблица 1. Критерии оценки средств контроля защищенности вычислительной сети

Критерий	**Количество баллов**
Сканирование портов	
Правильно определенный открытый порт	+1
Ошибочно определенное состояние порта	-1
Идентификация ОС	
Точная идентификация ОС	+3
Правильная идентификация семейства ОС	+1
Выдача списка возможных семейств, в котором содержится правильный ответ	0
Неправильная идентификация ОС	-1
Идентификация сервисов	
Точная идентификация сервиса	+3

Точная идентификация семейства сервиса	+1
Неидентифицированный сервис	-1
Ошибочно идентифицированный сервис	-3
Идентификация уязвимостей	
Точно идентифицированная уязвимость	+2
Ложное срабатывание	-1
Существующая, но неидентифицированная уязвимость	-2

Удобство работы оценивалось с учетом следующих факторов:

- наличие планировщика;
- возможность создания профилей проверок;
- возможность пересканирования отдельных сервисов;
- качество предоставленного отчета;
- наличие дополнительных функций по оценке защищенности.

3. Сравнительный анализ средств контроля защищенности

Средство «Сканер-ВС»

Отечественный программный комплекс «Средство анализа защищенности "Сканер-ВС"» предназначен для поиска уязвимостей сетей, исследования топологии сети и инвентаризации сетевых сервисов, сетевого и локального аудита паролей, поиска остаточной информации и анализа сетевого трафика.

Комплекс состоит из таких компонентов, как сканер сети, сканер безопасности, средство локального аудита паролей, средство сетевого аудита паролей, системный аудитор, сетевой анализатор, средство поиска по диску.

Программную основу «Сканер-ВС» составляют такие средства, как OpenVAS, Nmap, John The Ripper, Hydra, Ettercap.

«Сканер-ВС» сертифицирован Минобороны России (сертификат № 631) и ФСТЭК России (сертификат № 2204).

Стоимость лицензии на 1 год зависит от ограничения на количество одновременных целей для сканирования (IP-адресов) и варьируется от 5000 рублей для 1 IP-адреса до 150000 рублей для версии без ограничений.

Сетевой сканер безопасности XSpider

Сетевой сканер безопасности XSpider позволяет выполнять сканирование, сбор данных, их обработку, сохранение в БД и выпуск отчетов. Сканер XSpider включает в себя графический интерфейс администратора. В состав сканера XSpider включены база знаний, содержащая информацию о проверках и уязвимостях, модуль управления и сканирующее ядро. Данные сканирования хранятся во встроенной базе данных.

Сканер XSpider сертифицирован ФСТЭК России (сертификат № 2530) и Минобороны России (сертификат № 2034).

Стоимость лицензии на 1 год зависит от ограничения на количество одновременных целей для сканирования (IP-адресов) и варьируется от 9000 рублей для 4 IP-адресов до 1000000 рублей для версии на 10000 IP-адресов.

Средство BackTrack

BackTrack – это Linux-платформа, основанная на дистрибутиве Ubuntu, предназначенная для аудита безопасности компьютерных систем и сетей. Поставляется в виде LiveUSB и liveCD с возможностью установки системы на жесткий диск.

В комплект BackTrack входит коллекция эксплойтов и более 300 специализированных утилит для проверки безопасности, таких как Metasploit, RFMON, Aircrack-ng, Gerix Wifi Cracker, Kismet, Nmap, OpenVAS, Ophcrack, Ettercap, Wireshark, BeEF (Browser Exploitation Framework), Hydra, OWASP Mantra Security Framework, Cisco OCS Mass Scanner. Из приведенного списка видно, что в основе средств «Сканер-ВС» и BackTrack лежат схожие утилиты проверки безопасности, но в BackTrack список таких утилит существенно шире.

Все оригинальные наработки, созданные в рамках дистрибутива, распространяются под лицензией GPL. Однако BackTrack не имеет необходимых сертификатов и приводится в данном исследовании в качестве примера некоммерческих разработок.

Результаты тестирования

С TCP-сканированием все проверенные средства контроля защищенности справились отлично. Однако результаты сканирования UDP-портов оказались неудовлетворительными, что объясняется сложностью сканирования UDP-портов из-за отсутствия механизма установки соединения.

При идентификации ОС средства контроля защищенности показали хороший результат, определив все семейства ОС. При идентификации сервисов лидером стал XSpider 7.8. Средства «Сканер-ВС» и BackTrack показали несколько худшие результаты, определив меньшее количество TCP-сервисов.

При идентификации уязвимостей все средства контроля защищенности показали достаточно высокие результаты. Меньше ложных срабатываний отмечено у XSpider, однако «Сканер-ВС» и BackTrack определили большее количество уязвимостей.

Сравнительный анализ удобства работы показал, что все представленные средства удобны в работе, хотя качество отчетов, предоставляемых BackTrack, признано ниже, чем у отечественных средств контроля защищенности, так как имеется только англоязычный вариант. Наличие дополнительных функций для оценки защищенности является существенным преимуществом средств «Сканер-ВС» и BackTrack перед XSpider, реализующим только функции сканера безопасности.

Таким образом, все средства, протестированные в представленном исследовании, достаточно хорошо справляются с задачей контроля защищенности типовой вычислительной сети. Во многом схожие результаты тестирования «Сканер-ВС» и BackTrack объясняются тем, что оба средства контроля защищенности используют сканер безопасности OpenVAS.

Графической иллюстрацией полученных результатов является рис. 2, на котором представлена соответствующая диаграмма.

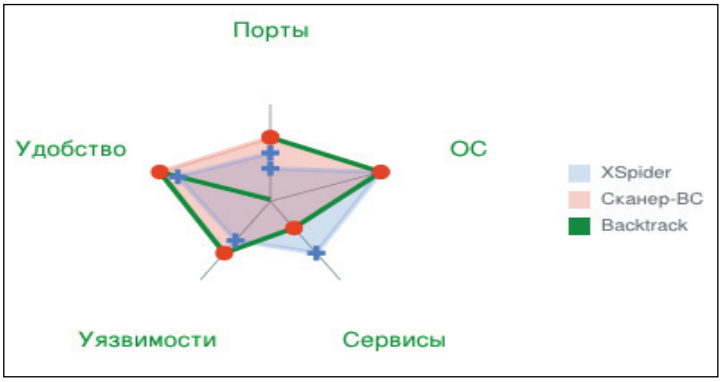

Рис. 2. Диаграмма результатов сравнительного тестирования

С практической точки зрения особо важным преимуществом любого средства защиты информации является наличие сертификата уполномоченного органа государственной власти. Среди таких решений небольшое преимущество имеет средство контроля защищенности «Сканер-ВС»

за счет более точной идентификации уязвимостей, а также благодаря наличию широкого арсенала дополнительных средств для оценки защищенности. В то же время XSpider 7.8 показал лучшие результаты при решении задачи инвентаризации сервисов и приложений вычислительной сети.

В итоге определяющим фактором выбора того или иного инструментального средства оказывается его цена. Если этот критерий взять за основной, то лидером среди сертифицированных решений является «Сканер-ВС». Для приведенной выше типовой вычислительной сети, включающей до 256 хостов, стоимость годовой лицензии «Сканер-ВС» составляет 30000 рублей, что более чем 2 раза меньше, чем стоимость годовой лицензии XSpider 7.8 (78000 рублей). Продление лицензии для «Сканер-ВС» составляет 7500 рублей, тогда как для XSpider продление лицензии будет составлять 31000 рублей. Стоимость максимальной версии «Сканер-ВС» также существенно ниже, чем у XSpider, и составляет 150 тысяч рублей для неограниченной версии «Сканер-ВС» и 1 миллион рублей для версии XSpider на 10000 хостов.

При этом средство анализа защищенности «Сканер-ВС» имеет большую базу данных уязвимостей, что позволяет достаточно точно проводить их идентификацию, русскоязычный интерфейс, обладает возможностью планирования проверок и создания профилей проверок, поддерживает обновления баз уязвимостей, характеризуется наличием дополнительных встроенных средств контроля защищенности.

К недостаткам этого средства можно отнести отсутствие специализированных средств контроля защищенности автоматизированных систем управления технологическим процессом (АСУ ТП), а также систем управления бизнесом (ERP-систем).

Дальнейшее направление описанных исследований связано с совершенствованием приведенных методик контроля защищенности вычислительных сетей, ориентированных на применение средства «Сканер-ВС», а также его интеграцией специализированными средствами контроля защищенности и разработкой дополнительных модулей, предназначенных для анализа защищенности специальных систем (таких как АСУ ТП, ERP-системы и т. д.).

СПИСОК ЛИТЕРАТУРЫ:

1. *Курило А. П., Милославская Н. Г., Сенаторов М. Ю., Толстой А. И.* Основы управления информационной безопасностью. М.: Горячая линия — Телеком, 2012. — 244 с.

2. *Макаров А. С., Миронов С. В., Цирлов В. Л.* Опыт тестирования сетевых сканеров уязвимостей // Информационное противодействие угрозам терроризма. 2005. № 5. С. 109–122.

3. Применение сканеров для анализа защищенности компьютерных сетей: Материалы курса. М.: Учебный центр «Информзащита», 2006.

4. Информационная безопасность открытых систем: Учебник для вузов. В 2-х томах. Том 2 — Средства защиты в сетях / С. В. Запечников, Н. Г. Милославская, А. И. Толстой, Д. В. Ушаков. М.: Горячая линия — Телеком, 2008. — 558 с.

5. ФСТЭК России [Электронный ресурс]. URL: http://fstec.ru (дата обращения: 12.02.2013).

6. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью. М.: Стандартинформ, 2006. — 55 с.

7. ГОСТ Р ИСО/МЭК 15408-1-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности технологий. Часть 1. Введение и общая модель. М.: Стандартинформ, 2009. — 36 с.

8. Open Source Security Testing Methodology Manual (OSSTMM) [Электронный ресурс]. URL: http://www.isecom.org/research/osstmm.html (дата обращения 12.02.2013).

9. Information Systems Security Assessment Framework (ISSAF) [Электронный ресурс]. URL: www.oissg.org/issaf (дата обращения: 12.02.2013).

10. National Institute of Standards and Technology [Электронный ресурс]. URL: http://csrc.nist.gov/publications/PubsSPs.html (дата обращения: 12.02.2013).

11. Data Security Standard: Information Supplement: Requirement 11.3 Penetration Testing [Электронный ресурс]. URL: https://www.pcisecuritystandards.org/pdfs/infosupp_11_3_penetration_testing.pdf (дата обращения 12.02.2013).