УДК 004.056

Г. К. Крючков[1]*

Анализ методик активного исследования безопасности информационных систем

[1] Национальный исследовательский ядерный университет «МИФИ», г. Москва, Российская Федерация
* e-mail: kryuchkovgk@gmail.com

Аннотация. В статье рассматриваются различные методики активного анализа информационных систем, применяемые для обеспечения кибербезопасности в современных организациях. Методы данного вида анализа направлены на выявление с целью последующего устранения потенциальных угроз безопасности информационных систем. Рассматриваются такие подходы как осуществление сетевого сканирования, выявление и эксплуатация конкретных типов уязвимостей, проведение тестирования на проникновение и определение поверхности атаки сетевого периметра организации. В работе отмечается важность проведения анализа информационных систем, подтверждаемая, в том числе, соответствующими указаниями регулирующих государственных органов. Отмечено, что комплексное применение различных методов активного анализа значительно повышает качество проводимых исследований. Главные выводы подчеркивают, что широко ориентированный и гибкий подход к анализу может обеспечить адекватную защиту информационных ресурсов организации в условиях постоянно меняющегося ландшафта киберугроз.

Ключевые слова: информационная безопасность, активный анализ, защита информационных систем, кибербезопасность

G. K. Kryuchkov[1]*

Analysis of Methods for Actively Researching Information Systems Security

[1] National Research Nuclear University MEPhI, Moscow, Russian Federation
* e-mail: kryuchkovgk@gmail.com

Abstract. The article discusses various methods of active analysis of information systems used to ensure cybersecurity in modern organizations. The methods of this type of analysis are aimed at identifying and then eliminating potential threats to the security of information systems. Such approaches as performing network scanning, identifying and exploiting specific types of vulnerabilities, conducting penetration testing and determining the attack surface of the organization's network perimeter are considered. The paper notes the importance of analyzing information systems, confirmed, among other things, by the relevant guidelines of regulatory government agencies. It is noted that the integrated application of various active analysis techniques significantly improves the quality of the research conducted. The main conclusions emphasize that a broadly focused and flexible approach to analysis can ensure adequate protection of an organization's information resources in the ever-changing cyber threat landscape.

Keywords: information security, active analysis, protection of information systems, cybersecurity

Введение

Развитие и широкое распространение информационных систем и связанных с ними киберугроз приводит к постоянному развитию сферы информационной безопасности (ИБ). Практически каждая современная организация обладает как минимум одной информационной системой, в то время как многие владеют целыми сетевыми кластерами. В подобных условиях особенно важно производить систематизацию информации и поиск уязвимостей в инфраструктуре предприятия.

Анализ информационных систем можно разбить на два основных типа: активный и пассивный анализ. Пассивное исследование предполагает получение сведений об исследуемом объекте за счет обработки данных внешних источников без прямого взаимодействия с целью исследования [1]. В то же время активный анализ подразумевает получение сведений посредством воздействия на исследуемый объект. Применение активного анализа позволяет не только собирать информацию о системах организации, но и выявлять различные уязвимости в системе защиты информации.

Существует большое количество различных методов, применяемых в рамках осуществления активного анализа, например: осуществление сканирования с целью поиска уязвимостей, тестирование на проникновение (имитация поведения злоумышленника с целью проверить возможность совершения несанкционированных действий), анализ сетевого трафика, инвентаризация сетевых активов организации.

При этом, с развитием различных систем защиты становится все сложнее производить как пассивный, так и активный анализ в связи с тем, что современные методы [2] и инструменты [3] нацелены на прямое противодействие подобным действиям. В связи с этим происходит постоянное развитие методов анализа информационных систем. В данной статье рассматриваются различные методы активного анализа, такие как сетевое сканирование, тестирование на проникновение, а также инвентаризация сетевых активов.

Методы и материалы

Активный анализ включает в себя разнообразные техники, от сканирования сети до тестирования на проникновение, и применяется для устранения уязвимостей системы до того, как они будут использованы злоумышленниками для совершения несанкционированных операций. Распространенным методом является сетевое сканирование, позволяющее собрать информацию о сетевом узле, например:

– список открытых, закрытых и фильтруемых портов;

– список работающих на сетевом узле сервисов;

– вид и версия применяемого ПО;

– выявленные ошибки конфигурации и наиболее распространенные уязвимости.

Следует отметить, что указанные выше действия могут выполняться как вместе (в комплексе, например [4, 5]), так и по отдельности. При этом эффективность каждого варианта метода зависит от его реализации. Например, при сканировании портов сетей интернета вещей необходимо применение дополнительных техник, позволяющих повысить качество результатов анализа за счет внесения изменений в алгоритм, позволяющих учесть специфичные начальные условия данной области [6]. Важно учитывать, что разрабатываются различные методы и инструменты, которые позволяют выявлять сетевые сканирования [7], что, в свою очередь, повышает необходимость разработки новых методов сетевого сканирования.

Другим методом активного анализа является сканирование с целью выявления и попыток эксплуатации конкретных типов уязвимостей. Данный подход позволяет осуществлять поиск определенного типа уязвимости, например, SQL-инъекции (уязвимости, относящиеся к СУБД, использующими язык SQL – Structured Query Language, связанные с изменением поведения базы данных при взаимодействии с приложением) [8], для чего применяются различные инструменты (в случае поиска SQL-инъекций примером может служить SQLMap [9]). Другим примером автоматизированного поиска уязвимостей служат инструменты OWASP ZAP и Burp Suit, позволяющие автоматически выявлять уязвимости типа Cross Site Scripting (XSS), заключающиеся во внедрении вредоносных клиентских сценариев (в большинстве случаев – JavaScript-код) на веб-страницы, просматриваемые пользователями [10, 11]. Подобные методы анализа предназначены для выявления потенциальных уязвимостей, а также реализации попыток их эксплуатации с целью подтверждения существования недостатков системы защиты.

В случаях, когда требуется комплексный подход к анализу безопасности информационных систем, часто используется тестирование на проникновение. При проведении этого типа анализа специалист по безопасности выполняет различные действия, имитирующие попытки злоумышленника совершить несанкционированные действия, например, получить доступ к закрытой информации из информационной системы, нарушить ее работу, выполнить запрещенные действия или операции с недоступными данными и т. д. [12]. Значимость данного метода подтверждают требования государственных органов, например, Центральный банк России в своем положении обязывает банковские и некоторые другие поднадзорные ему финансовые организации осуществлять проверку на возможность проникновения в инфраструктуру и наличие уязвимостей ежегодно [13]. Важно отметить, что в процессе проведения тестирования на проникновение специалист использует различные автоматизированные инструменты, а также проводит множество проверок вручную, чтобы улучшить покрытие потенциальных уязвимостей.

Крупные организации имеют очень развитую сетевую инфраструктуру, которая за счёт своего масштаба значительно усложняет не только процесс анализа, но и учет отдельных её элементов. В связи с этим возникло направление управления поверхностью атаки (External Attack Surface Management – EASM) [14].

Инструменты данной категории призваны посредством проведения множества различных поисковых операций выявить все сетевые активы организации, потенциально доступные злоумышленникам, в том числе так называемые «теневые» активы [15, 16]. Они находятся и могут быть обнаружены в пределах сетевого периметра организации, однако, по некоторой причине, могут быть не учтены и, соответственно, не контролироваться отделом обеспечения информационной безопасности компании. Данные сетевые узлы или сервисы могут появляться в случае, когда, например, разработчиками без согласования с отделом ИБ создается временный тестовый стенд, который потом по различным причинам не отключается, в результате чего организация получает неучтенный сетевой актив, который при этом может иметь доступ к другим сервисам. Важно отметить, что определение внешней поверхности атаки является самым комплексным из рассмотренных методов. Пример состава применяемых операций представлен на рис. 1, при этом он не является исчерпывающим или ограниченным и зависит от конкретной реализации. Следовательно, инвентаризация сетевых ресурсов путем определения поверхности атаки предприятия имеет большое значение, так как позволяет оценить видимый злоумышленником сетевой периметр и определить набор сетевых узлов, наиболее доступных для проведения атак.

Рис. 1. Примерный набор операций, реализуемых в рамках определения внешней поверхности атаки организации

Таким образом, при проведении активного анализа информационных систем используются различные методы и инструменты, ориентированные на различные аспекты получения информации об исследуемом объекте.

Обсуждение

Активный анализ информационных систем представляет собой класс различных методов, направленных на получение информации о системе путем прямого взаимодействия с ней. Эффективность активного анализа в значительной степени зависит от использования разнообразных методов исследования, вклю-

чая сетевое сканирование, анализ уязвимостей, тестирование на проникновение и другие техники. Применение этих методов в комплексе позволяет не только повысить точность выявления уязвимостей, но и детально оценить уровень безопасности системы.

Комплексное применение методов активного анализа обусловлено необходимостью охвата всех аспектов безопасности информационной системы. Например, сетевое сканирование позволяет идентифицировать активные сетевые устройства, открытые порты и работающие сервисы, которые могут быть потенциальными точками входа для злоумышленников. Однако без дополнительного анализа уязвимостей и тестирования на проникновение невозможно полноценно оценить, как эти сервисы и порты могут быть использованы для атаки. Таким образом, лишь комплексный подход позволяет не только обнаружить потенциальные уязвимости, но и понять контекст их возможной эксплуатации, что является критически важным для разработки эффективных стратегий защиты.

Более того, комплексное использование различных методов активного анализа способствует повышению общей надежности и устойчивости информационной системы к внешним и внутренним угрозам. Так, интеграция результатов сетевого сканирования с данными анализа уязвимостей и тестирования на проникновение позволяет формировать комплексное представление о безопасности системы, а также разрабатывать более точные и адаптированные к конкретной ситуации меры защиты.

Таким образом, только комплексное применение различных методов активного анализа позволяет обеспечить наиболее полное покрытие исследуемого объекта различными проверками.

Заключение

Комплексное применение различных методов активного анализа информационных систем является необходимым условием для достижения высокого уровня защищенности от кибератак. Различные методы анализа, такие как сетевое сканирование, тестирование на проникновение, анализ уязвимостей и инвентаризация сетевых активов при интеграции обеспечивают глубокое исследование угроз и уязвимостей системы. Это позволяет не только выявлять потенциальные угрозы более эффективно, но и предоставляет возможность реагировать на них, разрабатывая эффективные стратегии защиты. Комплексное использование методов активного анализа становится особенно значимым в условиях современного киберпространства, где технологии развиваются стремительно, а методы кибератак становятся всё более изощренными.

Применение комплексного подхода также способствует повышению общей надежности и устойчивости информационных систем к внешним и внутренним угрозам. В контексте постоянно меняющихся условий кибербезопасности, где новые уязвимости и методы атак появляются с удивительной регулярностью, только широко ориентированный и гибкий подход может обеспечить достаточный уровень защиты. Таким образом, активный анализ информационных систем, осуществляемый в комплексе с использованием разнообразных методов, является

ключом к эффективной защите от современных киберугроз и к обеспечению целостности и доступности информационных ресурсов организации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Azevedo R., Medeiros I., Bessani A. PURE: Generating Quality Threat Intelligence by Clustering and Correlating OSINT // 2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE). – 2019.

2. Basinya, E. A. Countermeasure Method Against Unauthorized and Anonymous Information System Data Collection / E. A. Basinya, V. E. Khitsenko, A. A. Rudkovskiy // 13th International IEEE Scientific and Technical Conference Dynamics of Systems, Mechanisms and Machines, Dynamics 2019 - Proceedings, Omsk, 05–07 ноября 2019 года. – Omsk: Institute of Electrical and Electronics Engineers Inc., 2019. – P. 8944715. – DOI 10.1109/Dynamics47113.2019.8944715. – EDN TYGYBF.

3. Свидетельство о государственной регистрации программы для ЭВМ № 2019615756 Российская Федерация. Система автоматического противодействия инструментам несанкционированного активного и пассивного анализа информационных систем и вычислительных сетей : № 2019614319 : заявл. 20.04.2019 : опубл. 07.05.2019 / Е. А. Басыня ; заявитель Общество с ограниченной ответственностью «Научно-исследовательский институт информационно-коммуникационных технологий».

4. Комарова, Ю. А. Nmap как инструмент для изучения хоста/сети / Ю. А. Комарова, В. С. Вечер, М. С. Рублев // Качество продукции: контроль, управление, повышение, планирование : сборник научных трудов 6-й Международной молодежной научно-практической конференции, Курск, 13 ноября 2019 года. – Курск: Юго-Западный государственный университет, 2019. – С. 161-163. – EDN FTSKIN.

5. Поляков, Р. И. Анализ защищенности сегмента сети на основе сканеров защищенности / Р. И. Поляков // 75-я научная конференция студентов и аспирантов Белорусского государственного университета : Материалы конференции. В 3-х частях, Минск, 14–23 мая 2018 года / Редколлегия: В.Г. Сафонов [и др.]. Том Часть 3. – Минск: Белорусский государственный университет, 2018. – С. 552-555. – EDN YZLQUP.

6. Tang F., Kawamoto Y., Kato N., Yano K., Suzuki Y. Probe Delay Based Adaptive Port Scanning for IoT Devices with Private IP Address Behind NAT // IEEE Network. – 2020. – №34.

7. Басыня, Е. А. Метод идентификации киберпреступников, использующих инструменты сетевого анализа информационных систем с применением технологий анонимизации / Е. А. Басыня, В. Е. Хиценко, А. А. Рудковский // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2019. – Т. 22, № 2. – С. 45-51. – DOI 10.21293/1818-0442-2019-22-2-45-51. – EDN GRIZDT.

8. Appelt Dennis,Nguyen Cu D.,Briand Lionel Behind an Application Firewall, Are We Safe from SQL Injection Attacks? // 2015 IEEE 8th International Conference on Software Testing, Verification and Validation (ICST). – 2015.

9. Переспелов, А. В. Проверка безопасности СУБД MySQL при помощи проведения пентестинга на Kalilinux / А. В. Переспелов, К. В. Дубинина, С. А. Матросова // Устойчивое развитие науки и образования. – 2019. – № 10. – С. 168-171. – EDN COCNNN.

10. Савин, И. В. Межсайтовый скриптинг как актуальная угроза для современных вебсистем / И. В. Савин // Наука, техника и образование. – 2017. – № 9(39). – С. 40-43. – EDN ZPDRTF.

11. Garn B., Lang D.S., Leithner M., Kuhn D.R., Kacker R., Simos D.E. Combinatorially XSSing Web Application Firewalls // 2021 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW). – 2021.

12. Макаренко, С. И. Тестирование на проникновение на основе стандарта NIST SP 800-115 / С. И. Макаренко // Вопросы кибербезопасности. – 2022. – № 3(49). – С. 44-57. – DOI 10.21681/2311-3456-2022-3-44-57. – EDN JLCAVG.

13. Положение Банка России от 17.08.2023 N 821-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» (Зарегистрировано в Минюсте России 06.12.2023 N 76286).

14. Свидетельство о государственной регистрации программы для ЭВМ № 2023619366 Российская Федерация. СКИПА - Система Контроля и Информирования о Поверхности Атак : № 2023617827 : заявл. 26.04.2023 : опубл. 10.05.2023 ; заявитель Акционерное общество «Сайбер ОК». – EDN TDZUDG.

15. Everson D., Cheng L. Network attack surface simplification for red and blue teams // IEEE Secure Development (SecDev). – 2020.

16. Huang K., Yang L., Fu R., Zhou S., Hong Z. HASN: A hierarchical attack surface network for system security analysis // China Communications. – 2019. – №16. – С. 137–157.