УДК 004.056.5 Вестник УрФО № 1(55) / 2025, с. 55–61

Цуканов А. С., Соколов А. Н. DOI: 10.14529/secur250106

ОЦЕНКА ПОЛНОТЫ ПРИМЕНЯЕМЫХ МЕТОДОВ ПРИ ВНЕШНЕМ ТЕСТИРОВАНИИ НА ПРОНИКНОВЕНИЕ С УЧЕТОМ ВОЗМОЖНОСТЕЙ НАРУШИТЕЛЯ

Рассмотрены проблемы полноты и качества применяемых методов при проведении работ по тестированию на проникновение. Показано, что основным фактором, определяющим перечень таких работ, является техническое задание, которое, как правило, предлагается Исполнителем и составляется из соображений снижения его трудозатрат. При этом Заказчику, как правило, трудно оценить полноту, и, как следствие, качество таких работ. В статье предложен новый инструмент для оценки полноты и качества применяемых методов проведения работ по тестированию на проникновение, сформулирована проблематика выбора методов тестирования на проникновение с учетом возможностей нарушителя. Представлена модель оценки полноты применяемых методов при внешнем тестировании на проникновение на основе многодольного графа. На приведенном примере продемонстрирована эффективность представленной модели для выявления работ, не учтенных Исполнителем в предложенном техническом задании на проведение работ.

Ключевые слова: *вектор атаки, информационная безопасность, тестирование на проникновение, кибербезопасность, нарушитель, многодольный граф.*

ASSESSMENT OF THE COMPLETENESS OF THE METHODS USED IN EXTERNAL PENETRATION TESTING

The problems of completeness and quality of the methods used in conducting penetration testing are considered. It is shown that the main factor determining the list of such works is the terms of reference, which, as a rule, is proposed by the Contractor and is compiled from proposals to reduce his labor costs. At the same time, it is usually difficult for the Customer to assess the completeness and, as a result, the quality of such work. The article proposes a new tool for assessing the completeness and quality of the methods used for conducting penetration testing, and formulates the problems of choosing methods for penetration testing, taking into account the capabilities of the intruder. A model for assessing the completeness of the methods used in external penetration testing based on a multipole graph is presented. The given example demonstrates the effectiveness of the presented model for identifying works that were not taken into account by the Contractor in the proposed terms of reference for the work.

Keywords: *attack vector, information security, penetration testing, cyberse-curity, intruder, multipole graph.*

Введение. Важной частью работ в обеспечении кибербезопасности явля-ется моделирование атак реальных злоумышленников. Организации, которые проводят для своих заказчиков работы по внешнему тестированию на проникновение (далее – Исполнители) зачастую проводят работы исключительно по техническому заданию, при этом используя не все возможные методы проведения тестирования на проникновение и оценивая не все слабые места инфраструктуры заказчиков [1].

Работы по тестированию на проникновение проходят на договорной основе и в качестве перечня проверок выступает техническое задание на проведение работ. Как правило, технические задания согласует Заказчик работ, но предлагает его Исполнитель работ. Исполнители зачастую разрабатывают свои технические задания на проведение тестирования на проникновение из расчета наименьших трудозатрат. С таким подходом очень сложно понять, действительно ли были проверены все ресурсы заказчика или Исполнитель нашел только один успешный вектор атаки [2].

Необходимо отметить важность дополнительных проверок инфраструктур Заказчика после внедрения им средств защиты информации, основываясь на рекомендациях Исполнителя. Зачастую возникают ситуации, когда Исполнители проверяют только те вектора атак, которые ранее были успешны, не взяв в расчет то, что внедренные средства информационной безопасности также требуют проверки на возможность взлома [3].

В момент окончания работ возможно два результата: инфраструктура скомпрометирована или нет. В случае, если результат работ: инфраструктура не взломана, необходимо ответить на два вопроса:

1. Охватывает ли техническое задание, используемое Исполнителем, все задействованные ИТ-технологии заказчика?

2. Использованы ли все возможные тактики и техники реализации атак?

Рассмотрим пример проведения тестирования на проникновение с применением оценки применяемых тактик и техник нарушителя.

Пример. Злоумышленник взламывает личные кабинеты пользователей интернет-магазина и получает данные привязанных банковских карт.

Вектором атаки в этом случае является следующая последовательность действий:

1. Направленное сканирование при помощи специализированного программного обеспечения подключенных к сети устройств с целью идентификации сетевых сервисов, типов и версий программного обеспечения этих сервисов, а также с целью получения конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений [4].

2. Эксплуатация уязвимостей сетевого оборудования и средств защиты вычислительных сетей для получения доступа к компонентам систем и сетей при удаленной атаке [4].

Для оценки качества выполненных работ по тестированию на проникно-вение введем следующие определения: *полнота работ по тестированию на проникновение* (далее – *полнота*) – это состояние работ, при котором реализуемые проверки затрагивают все используемые технологии и средства обработки информации. В свою очередь, *полнота применяемых методов при внешнем тестировании на проникновение* (далее – *полнота применяемых методов*) – это состояние работ, при котором реализуемые проверки (с использованием и без использования специально программного обеспечения) затрагивают все используемые технологии и средства обработки информации.

Вполне вероятной может оказаться ситуация, при которой рассмотрены все возможные технические векторы атак, но не учтены возможные ошибки, связанные с человеческим фактором. Для исключения этих ошибок рассмотрим модель оценки полноты работ по внешнему тестированию на проникновение на основе многодольного графа с учетом тактик и техник возможных вредоносных воздействий потенциальных злоумышленников (нарушителя).

Рассматриваемая модель имеет следующие ограничения:

1. Анализируются действия только внешнего нарушителя – злоумышленника, который не знает о внутреннем устройстве организации и действует со стороны сети «Интернет».

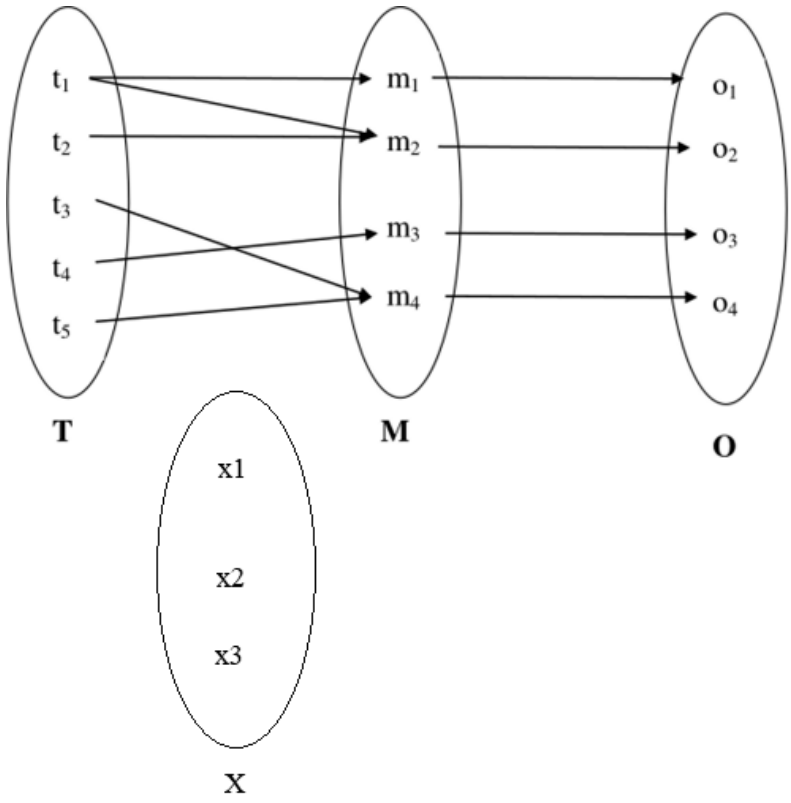

Рис. 1. Частный случай четырехдольного графа, описывающего полноту применяемых методов при внешнем тестировании на проникновение

2. Не рассматриваются технологии защиты информации, используемые организацией.

Модель реализуется на основе четырехдольного графа [5] (рис. 1), в котором:

1. Первая доля (M) — это используемые ИТ-технологии, которые проверяются в ходе работ (например, веб-сайты, JWT-токены и т.д.) [6, 7].

2. Вторая доля (T) — это всевозможные методы проверки при тестировании на проникновение, например, атака перебором (bruteforce) пароля и т.д. [8].

3. Третья доля (O) — потенциал нарушителя, который реализует угрозы безопасности информации. В качестве примера рассмотрим нарушителя с низким потенциалом, который используют только бесплатные инструменты для атаки.

4. Четвертая доля (X) — тактики и техники, реализуемые без использование специального программного обеспечения, которые не могут быть перекрыты средствами защиты информации.

5. Ребра, которые соединяют доли — это взаимосвязи между компонен-тами M, T, O и X. Например, если в первой доле (M) есть веб-сайт с личным кабинетом, то ему, как минимум, из второй доли (T) будет соответствовать атака по перебору паролей, а в третьей доле (O) будет указан низкий потенциал нарушителя, а в четвертой доле будет поиск логинов и паролей пользователей в публичных утечках.

Заметим, что не все вершины из доли T могут быть связаны с вершинами доли M по причине не совместимости используемой технологии и метода проверки. Примером такого исключения может быть метод проверки bruteforce пароля к используемой технологии «реализация https соединения».

Таким образом, для того, чтобы оценить полноту применяемых методов при внешнем тестировании на проникновение со стороны исполнителя, необ-ходимо выяснить: все ли вершины из первой доли (M), которые соединены с вершинами из третьей доли (O), были связаны с вершинами из второй (T) и четвертой (X) долей.

Рассмотрим представленный выше пример для оценки полноты приме-няемых методов технического задания Исполнителя, в котором отсутствует сценарий компрометации

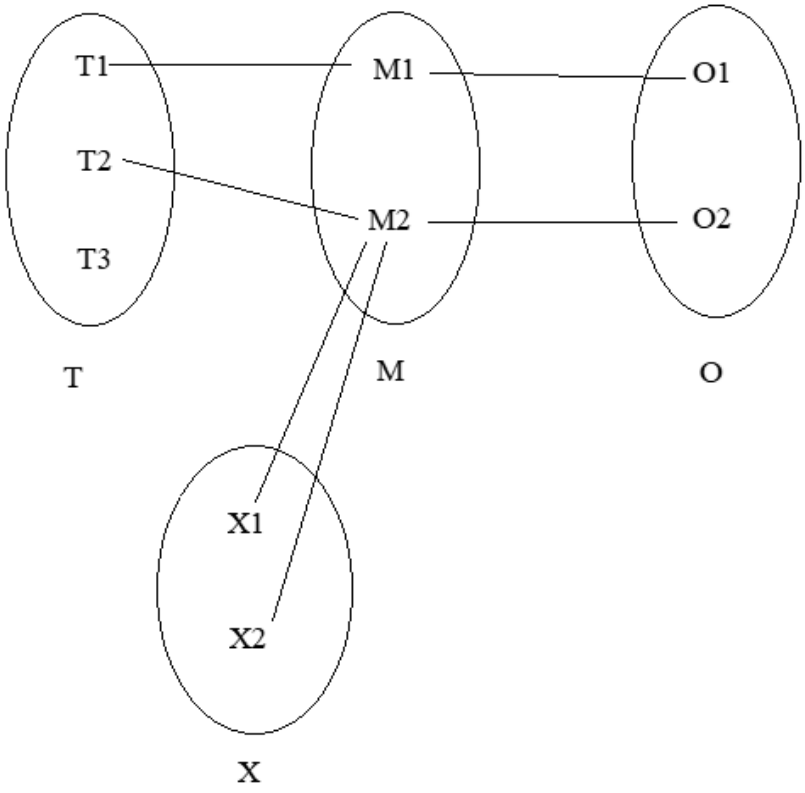

Рис. 2. Четырёхдольный граф, описывающий пример для оценки полноты применяемых методов при внешнем тестировании на проникновение на основе модели нарушителя

инфраструктуры без использования специального программного обеспечения: поиск информации в открытых источниках с использованием графа (рис. 2):

1. Определим доли графа:

1.1. M – форма для ввода данных (M1), форма для ввода логина и пароля (M2).

1.2. T – sql-инъекции (T1), bruteforce (T2), модификация сетевого тра-фика (T3).

1.3. O – потенциал нарушителя низкий (может выполнить атаки на формы M1 и M2, используя проверки/атаки T1 и T2).

1.4. X – поиск информации в открытых источниках (X1), поиск инфор-мации в darknet (X2).

2. Технологии M1 соответствует проверка T1, технологии M2 соответствует проверка T2 и техники X1 и X2.

3. Сверим ребра M1 – T1, M2 – T2, M2 – X1 и M2 – X2 с техническим заданием на проведение работ и видим, что поиск информации в открытых источниках и сети darknet не произведен.

4. Делаем вывод, что работы по тестированию на проникновение выполнены не в полном объеме, проверяемый ресурс находится под угрозой. Требуется актуализация технического задания на проведение работ.

Но, представленный таким образом граф, описывающий полноту применяемых методов при внешнем тестировании на проникновение на основе технического задания на проведение работ, не позволяет оценить их избыточность с целью экономии ресурсов.

С целью повышения качества работы модели по оценке полноты применяемых методов при внешнем тестировании на проникновение необходимо:

1. Рассмотреть варианты расширения модели за счет увеличения количество долей в исследуемом графе, например, путем учета средств защиты информации, добавления вероятностей атак для злоумышленника и т.д.

2. Использовать алгоритмы обхода графов [10] для минимизации количества проверок, которые необходимо пройти, для охвата всех используемых технологий обработки информации.

Таким образом, в работе сформулировано определение применяемых методов при внешнем тестировании на проникновение и рассмотрена ее модель на основе многодольного графа. В представленном примере на основе анализа модели продемонстрирован способ выявления работ, не учитываемых Исполнителем в техническом задании на проведение работ. Приведены варианты развития модели, позволяющие повысить качество оценки полноты работ по тестированию на проникновение.

Литература

1. Иванов, А. В. Вопросы оценки эффективности аудита информационной безопасности / А. В. Иванов, И. А. Огнев, В. В. Селифанов // Вестник УрФО. Безопасность в информационной сфере. – 2024. – № 4(54). – С. 37-48. – DOI 10.14529/secur240405. – EDN MGIOHA.

2. Макарова, О. С. Разработка методики прогнозирования динамики изменения вектора компьютерной атаки с точки зрения нарушителя: специальность 05.13.19 «Методы и системы защиты информации, информационная безопасность»: диссертация на соискание ученой степени кандидата технических наук / Макарова Ольга Сергеевна, 2021. – 218 с. – EDN AEEOAG.

3. Сергеев, С. С. Методика построения графа атак для объектов критической информационной инфраструктуры / С. С. Сергеев, И. И. Баранкова // Вестник УрФО. Безопасность в информационной сфере. – 2022. – № 3(45). – С. 47-53. – DOI 10.14529/secur220305. – EDN SWZHQP.

4. Методика оценки угроз безопасности информации. Режим доступа: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (дата обращения: 20.03.2025).

5. Алексеев В.Е, Захарова Д.В. ТЕОРИЯ ГРАФОВ: Учебное пособие. – Нижний Новгород: Нижегородский госуниверситет, 2017. –119 с.

6. Кинтонова А. Ж., Баенова Г. М., Урынбасарова А. Ж. Вопросы безопасности веб приложений // Colloquium-journal. 2020. №13 (65). Режим доступа: https://cyberleninka.ru/article/n/voprosy-bezopasnosti-veb-prilozheniy (дата обращения: 20.03.2025).

7. WebApplicationFirewall. Режим доступа: https://habr.com/ru/companies/otus/articles/733142/ (дата обращения: 20.03.2025).

8. OWASPtop 10. Режим доступа: https://owasp.org/www-project-top-ten/ (дата обращения: 20.03.2025).

9. Матрица атак MITRE ATT&CK. Режим доступа: https://mitre.ptsecurity.com/ru-RU (дата обращения: 20.03.2025).

10. Дольников, В. Л. Основные алгоритмы на графах: текст лекций / В. Л. Дольников, О. П. Якимова; Яросл. гос.ун-т им. П. Г. Демидова. – Ярославль: ЯрГУ, 2011. – 80 с.

References

11. Ivanov, A. V. Voprosy ocenki jeffektivnosti audita informacionnoj bezo-pasnosti / A. V. Ivanov, I. A. Ognev, V. V. Selifanov // Vest-nik UrFO. Bezopasnost' v informacionnoj sfere. – 2024. – № 4(54). – S. 37-48. – DOI 10.14529/secur240405. – EDN MGIOHA.

12. Makarova, O. S. Razrabotka metodiki prognozirovanija dinamiki izmenenija vektora komp'juternoj ataki s tochki zrenija narushitelja: special'nost' 05.13.19 "Metody i sistemy zashhity informacii, informacionnaja bezopasnost'": dissertacija na soiskanie uchenoj stepeni kandida-ta tehnicheskih nauk / Makarova Ol'ga Sergeevna, 2021. – 218 s. – EDN AEEOAG.

13. Sergeev, S. S. Metodika postroenija grafa atak dlja ob#ektov kri-ticheskoj informacionnoj infrastruktury / S. S. Sergeev, I. I. Barankova // Vestnik UrFO. Be-zopasnost' v informacionnoj sfere. – 2022. – № 3(45). – S. 47-53. – DOI 10.14529/secur220305. – EDN SWZHQP.

14. Metodika ocenki ugroz bezopasnosti informacii. Rezhim dostupa: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (data obrashhenija: 20.03.2025).

15. Alekseev V.E, Zaharova D.V. TEORIJa GRAFOV: Uchebnoe posobie. – Nizhnij Novgorod: Nizhegorodskij gosuniversitet, 2017. –119 s.

16. Kintonova A. Zh., Baenova G. M., Urynbasarova A. Zh. Voprosy bezopasnosti veb prilozhenij // Colloquium-journal. 2020. №13 (65). Rezhim dostupa: https://cyberleninka.ru/article/n/voprosy-bezopasnosti-veb-prilozheniy (data obrashhenija: 20.03.2025).

17. WebApplicationFirewall. Rezhim dostupa: https://habr.com/ru/companies/otus/articles/733142/ (data obrashhenija: 20.03.2025).

18. OWASPtop 10. Rezhim dostupa: https://owasp.org/www-project-top-ten/ (data obrashhenija: 20.03.2025).

19. Matrica atak MITRE ATT&CK. Rezhim dostupa: https://mitre.ptsecurity.com/ru-RU (data obrashhenija: 20.03.2025).

20. Dol'nikov, V. L. Osnovnye algoritmy na grafah: tekst lekcij / V. L. Dol'nikov, O. P. Jakimova; Jarosl. gos. un-t im. P. G. Demidova. – Jaroslavl': JarGU, 2011. – 80 s.

ЦУКАНОВ Александр Сергеевич, аспирант кафедры защиты информации ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: tsukanovas@susu.ru

СОКОЛОВ Александр Николаевич, кандидат технических наук, доцент, заведующий кафедрой защиты информации ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: sokolovan@susu.ru

TSUKANOV Aleksandr Sergeevich, post-graduate student of the Information Security, Federal State Autonomous Educational Institution of Higher Education "South Ural State University (national research university)". 454080, Chelyabinsk, Lenina Avenue, 76. E-mail: tsukanovas@susu.ru

SOKOLOV Alexander Nikolayevich, Candidate of Technical Sciences, Associate Professor, Head of Department of Information Security, Federal State Autonomous Educational Institution of Higher Education "South Ural State University (national research university)". 454080, Chelyabinsk, Lenina avenue, 76. E-mail: sokolovan@susu.ru.