Документация, содержащая описание функциональных характеристик программного обеспечения

Программное обеспечение: «Платформа Autopentest iSTEM 2.0»

Правообладатель: Общество с ограниченной ответственностью «АВТОПЕНТЕСТ ЛАБ»

1. Общие сведения

1.1. Настоящий документ разработан в рамках исполнения требований Постановления Правительства РФ от 16 ноября 2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» (с изменениями и дополнениями) и содержит описание функциональных характеристик программного обеспечения «Платформа Autopentest iSTEM 2.0» (далее – «ПО»), правообладателем которого является Общество с ограниченной ответственностью «АВТОПЕНТЕСТ ЛАБ», ОГРН 1265000041976 (далее – «Правообладатель»).

1.2. ПО предназначено для автоматизированного тестирования защищённости ИТ-инфраструктуры и безопасного моделирования действий злоумышленника в контролируемых условиях. Система формирует цепочки этичных атак, проверяет выявленные слабости на практике и создаёт доказательную базу для приоритизации устранения рисков.

2. Функциональные характеристики

Функциональные возможности ПО включают:

2.1. Универсальная модель этичной атаки

Платформа моделирует цепочки атак в анализируемой инфраструктуре с помощью универсальной и расширяемой объектной модели. Её основной принцип – разделение хода атаки на базовые элементы – «факты» и «действия»:

- **«Факт»** – структурированный фрагмент данных об анализируемом ИТ-окружении. Факты поступают в систему либо от пользователя, либо становятся известными или подтверждаются действиями системы.
- **«Действие»** – автоматическая операция системы, выполняемая с целью поиска новых фактов. Одни действия используют известные факты в качестве входных параметров, другие могут выполняться без входных фактов.

2.2. Автоматизированное выявление слабых мест

Система анализирует ИТ-окружение и выявляет небезопасные конфигурации, уязвимости программного обеспечения, слабые учётные данные и иные факторы, способствующие развитию этичной атаки.

2.3. Моделирование действий злоумышленника

Платформа автоматически выполняет последовательность проверок и действий, направленных на развитие этичной атаки от исходной точки до заданной цели. Сценарии действий формируются с учётом известных данных об инфраструктуре и результатов ранее выполненных действий.

2.4. Этичная эксплуатация выявленных слабостей

Система проверяет возможность практической эксплуатации выявленной слабости в условиях конкретного ИТ-окружения, фиксирует полученные результаты и подтверждённые взаимосвязи между объектами инфраструктуры.

2.5. Классификация встроенных техник и тактик согласно матрице MITRE ATT&CK

В платформе используются техники, относящиеся к основным тактикам развития атаки в рамках внутреннего пентеста, включая Discovery, Credential Access, Lateral Movement, Privilege Escalation, Execution и другие.

2.6. Автоматическое построение интерактивных цепочек атак

Система формирует единый граф цепочки атаки (Kill Chain), отражающий причинно-следственные связи между фактами и действиями. Граф может строиться автоматически или пользователем вручную, начиная от любых фактов и действий в рамках конкретного проекта, с возможностью построения цепочки атаки как в ретроспективу, так и в перспективу на любую доступную глубину.

2.7. Поддержка режимов «Чёрный ящик» и «Серый ящик»

Платформа позволяет проводить тестирование с различным объёмом исходных данных об окружении, используя сведения, полученные в ходе анализа, а также данные, добавленные пользователем из внешних источников.

2.8. Управление и контроль

В системе доступна настройка исходных параметров и целей анализа, управление составом выполняемых действий, ручное подтверждение отдельных операций, а также остановка анализа оператором.

2.9. Безопасность применения

Платформа функционирует в изолированном контуре без доступа в интернет. Встроенные техники адаптированы для безопасного выполнения в рабочей инфраструктуре и не включают операции, направленные на утечку, порчу или удаление данных.

2.10. Взгляд на сеть глазами хакера

Платформа формирует интерактивную модель инфраструктуры на основе фактов, полученных в ходе тестирования или из внешних источников. Модель включает сведения об обнаруженных объектах, их свойствах и взаимосвязях, значимых с точки зрения развития атаки. Это позволяет анализировать инфраструктуру с позиции атакующего и оценивать возможности доступа и перемещения между объектами инфраструктуры.

2.11. Многоуровневая интерактивная отчётность

Система формирует детализированные отчёты для специалистов по информационной безопасности, агрегированную статистику и сводные представления для руководителей, а также рекомендации по устранению выявленных слабостей для ИТ-подразделений.

2.12. API-интерфейс и интеграционные возможности

API-first архитектура платформы позволяет получать через API-интерфейс исходные данные (любые типы фактов) из внешних источников, запускать и останавливать целые сценарии или отдельные действия, а также передавать результаты анализа во внешние системы и средства автоматизации.

2.13. Безагентная архитектура

Платформа не требует установки агентов на анализируемые хосты, что снижает требования к изменению анализируемой инфраструктуры и упрощает внедрение.

2.14. Масштабируемость

Система рассчитана на работу с инфраструктурами от сотен до тысяч узлов благодаря структурированной объектной модели, реляционному хранилищу данных и другим технологиям и подходам, применённым в ходе разработки ядра системы.

3. Заключительные положения

Настоящее описание функциональных характеристик отражает актуальный состав функций ПО. Сведения, изложенные в документе, могут использоваться для целей идентификации ПО, подтверждения его функциональной самостоятельности и соответствия требованиям, предъявляемым к российскому программному обеспечению.