Vulns.io VM
Управление уязвимостями

фродекс

Что? Где? Когда?

Способы детектирования уязвимостей инфраструктуры в процессе Vulnerability Management

itsec® ИНФОРМАЦИОННАЯ И КИБЕРБЕЗОПАСНОСТЬ РОССИИ

Октябрь 2024

Жизненный цикл управления уязвимостями

Vulns.io™

Инвентаризация активов

Аудит уязвимостей

Критичность по методике ФСТЭК

Метрики CVSS, EPSS, CISA KEV

Наличие эксплойтов

По методике ФСТЭК

По метрикам опасности

Патч-менеджмент

Компенсирующие меры

Отчеты

Динамика уровня защищенности

Детектирование уязвимостей – неотъемлемый этап процесса, на основе которого строится вся последующая работа по управлению уязвимостями

Подходы к детектированию уязвимостей

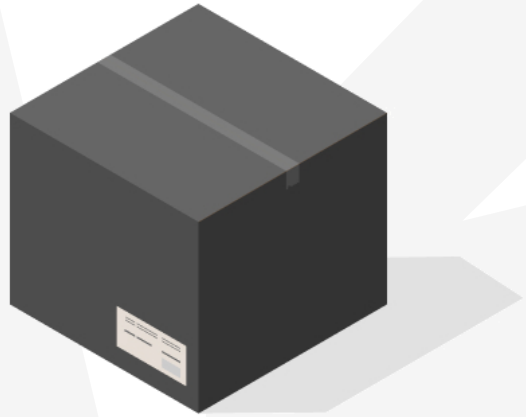
Vulns.io™

Существует два принципиально разных подхода к детектированию уязвимостей инфраструктуры:

Белый ящик

Есть знания о инфраструктуре и ее активах

Черный ящик



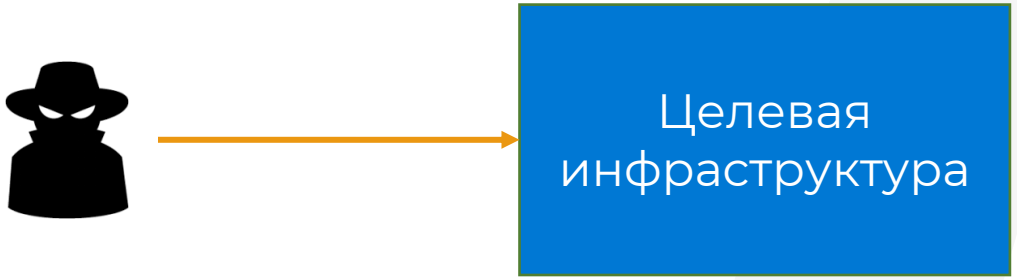
Нет знаний о инфраструктуре и ее активах

Метод «черного ящика»

Vulns.io™

«Черный ящик» - метод анализа системы без предварительного знания о её внутренней структуре.

Этот метод используется для оценки безопасности системы с точки зрения злоумышленника.

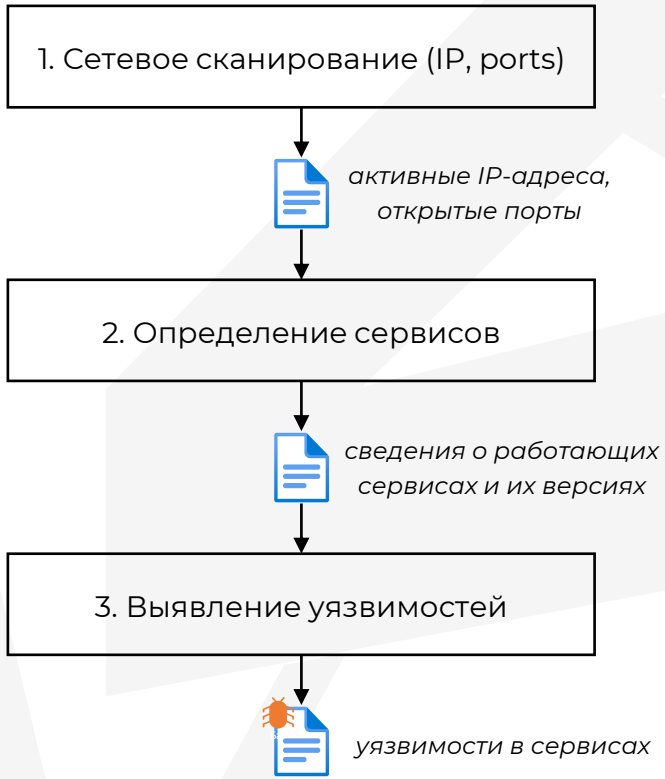


Достоинства

- Знания об уязвимостях, которые «торчат наружу»;

Недостатки

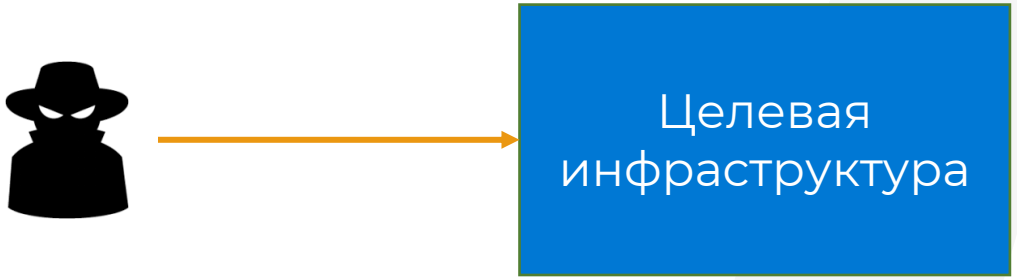
- Невысокая точность результата;
- Долгое время сканирования;
- Подходит только для периметра



Метод «черного ящика» + пентест

Vulns.io™

Пентест, или «проверка на проникновение» - метод активного воздействия на систему путем моделирования атаки.

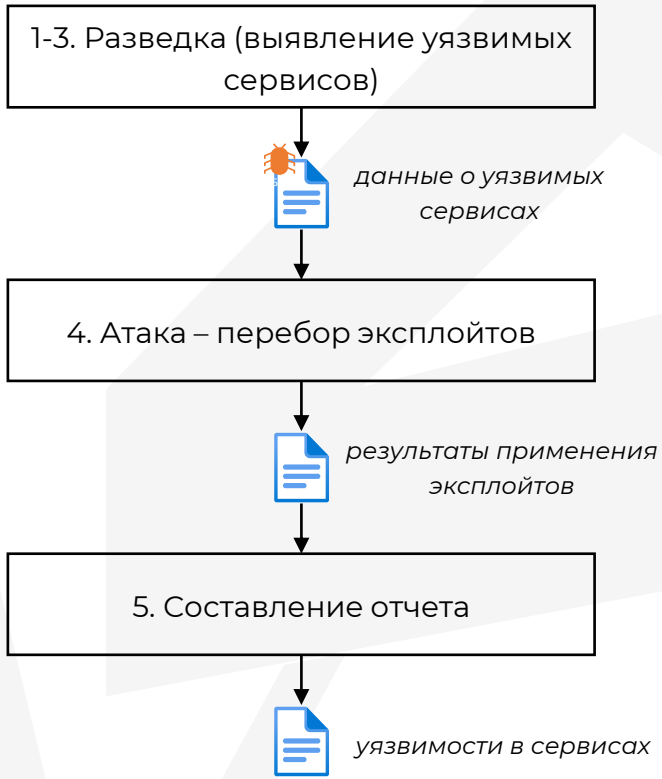


Достоинства

- Можно найти вектора атаки на периметр
- Спектр найденных уязвимостей шире

Недостатки

- Тяжело согласовать условия;
- Долгое время выполнения;
- Можно навредить инфраструктуре в ходе атаки

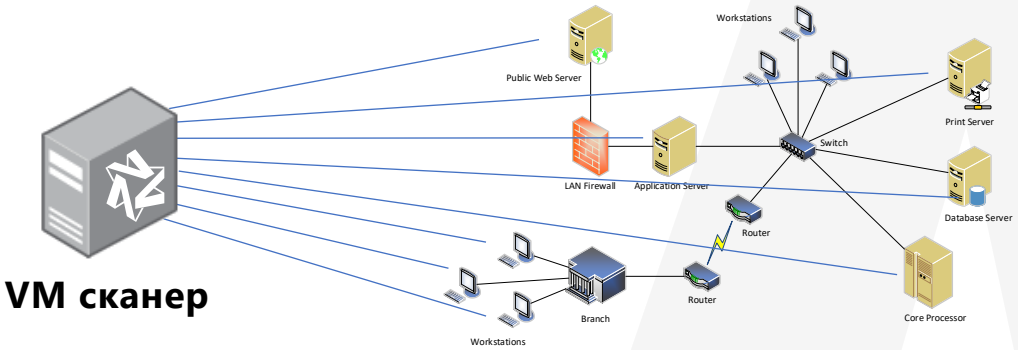


Метод «белого ящика»

Vulns.io VM

«Белый ящик» - метод сканирования системы изнутри.

Уязвимости выявляются на основе данных обо всех компонентах системы и их связях.

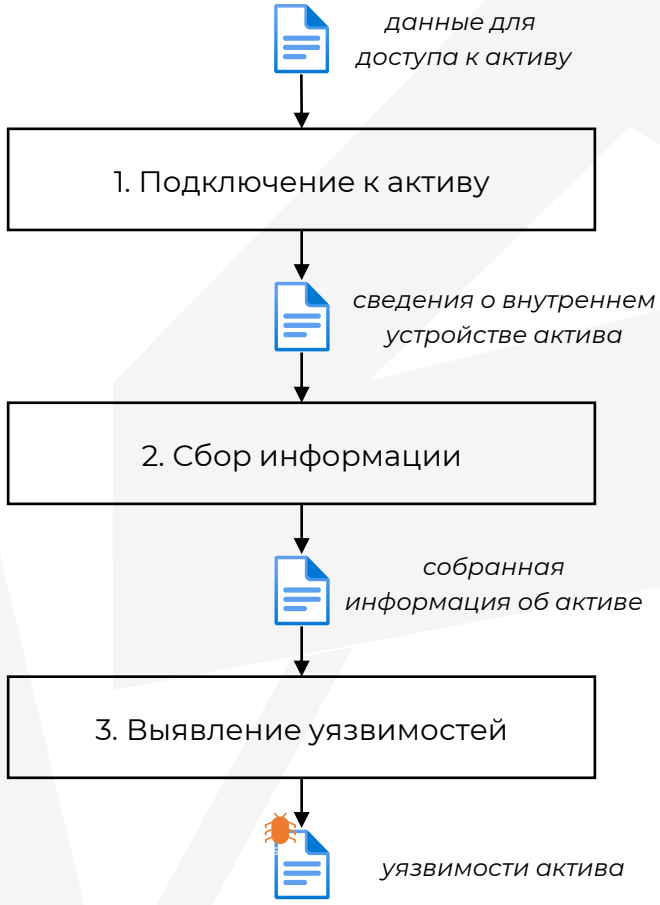


Достоинства

- Более точные и обширные результаты детектирования;
- Процесс проходит быстро;
- Проверить можно все активы инфраструктуры;

Недостатки

- Не имитирует атаку злоумышленника;
- Требуются данные об инфраструктуре и ее активах



Метод «белого ящика»: доступ к активам

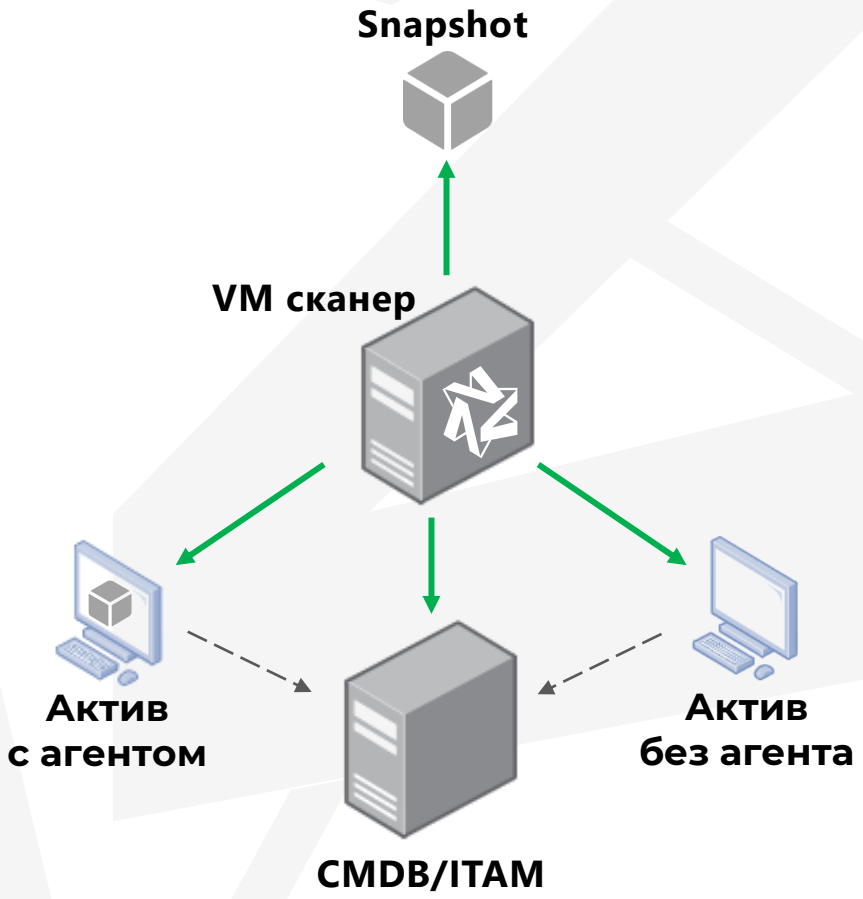
При сборе данных методом «белого ящика», необходимо предоставить сканеру доступ к целевым активам инфраструктуры.

Способы взаимодействия с активами:

- **Агентный** – на актив ставится VM-утилита;
- **Безагентный** – удаленное подключение к активу;
- **Опосредованный** – анализ копии актива (snapshot) или по данным системы инвентаризации

требуется привилегированный доступ к активу

результат зависит от полноты и актуальности данных



Детектирование уязвимостей хостов

Vulns.io VM

При аудите хостов, процесс детектирования уязвимостей может выполняться:

- Непосредственно на целевом активе;
- На VM-сканере.

Детектирование уязвимостей хостов

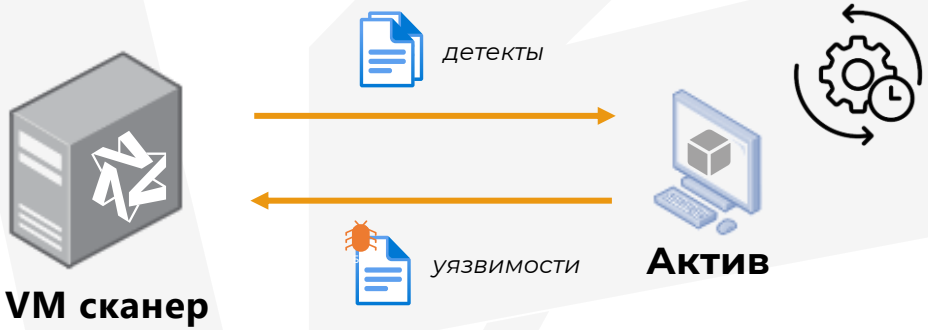
Vulns.io™

Процесс детектирования уязвимостей на целевом активе:

1. VM-сканер по сети передает на актив массив данных – детекты уязвимостей;
2. Детекты проверяются на активе один за другим, выявляя уязвимости;
3. VM-сканер **получает** результат выявленных уязвимостей.

Недостатки:

- Высокая нагрузка на сеть инфраструктуры;
- Высокая нагрузка на целевой актив;
- Долгое и неопределенное время получения результата.



Детектирование уязвимостей хостов

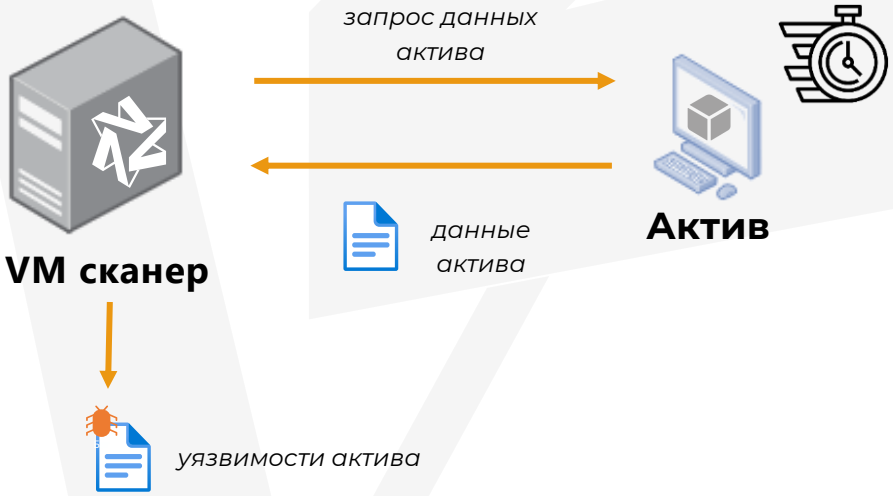
Vulns.io VM

Процесс детектирования уязвимостей на VM-сканере:

1. VM-сканер по сети запрашивает данные актива – собирает сам или через агента;
2. Данные анализируются на уязвимости актива по базе детектов на VM-сканере;
3. VM-сканер **формирует** результат выявленных уязвимостей.

Преимущества:

- Низкая нагрузка на сеть инфраструктуры;
- Нет нагрузки на целевой актив;
- Быстрое и прогнозируемое время получения результата.

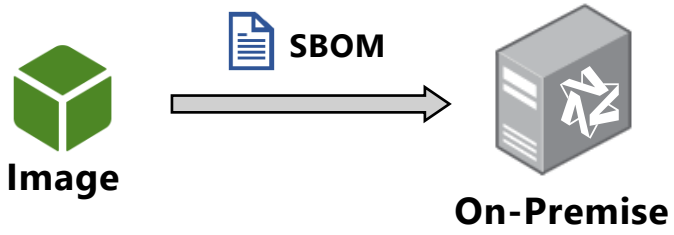


Детектирование уязвимостей образов

Vulns.io™

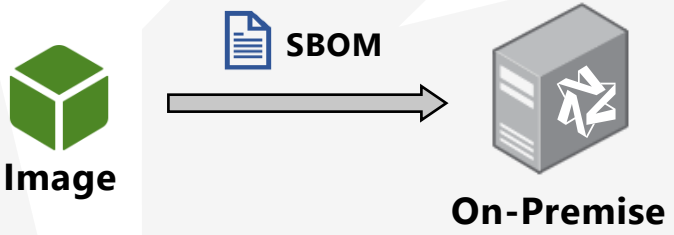
При аудите образов, процесс детектирования уязвимостей может выполняться следующими способами:

Разработанная технология сканирования позволяет проводить аудит образа **без необходимости запуска**.



- ✓ **Быстро:** нет накладных расходов на запуск образа;
- ✓ **Безопасно:** не надо запускать потенциально уязвимый образ.

Разработанная технология сканирования позволяет проводить аудит образа **без необходимости запуска**.



- ✓ **Быстро:** нет накладных расходов на запуск образа;
- ✓ **Безопасно:** не надо запускать потенциально уязвимый образ.

Комбинируем подходы детектирования

Vulns.io™

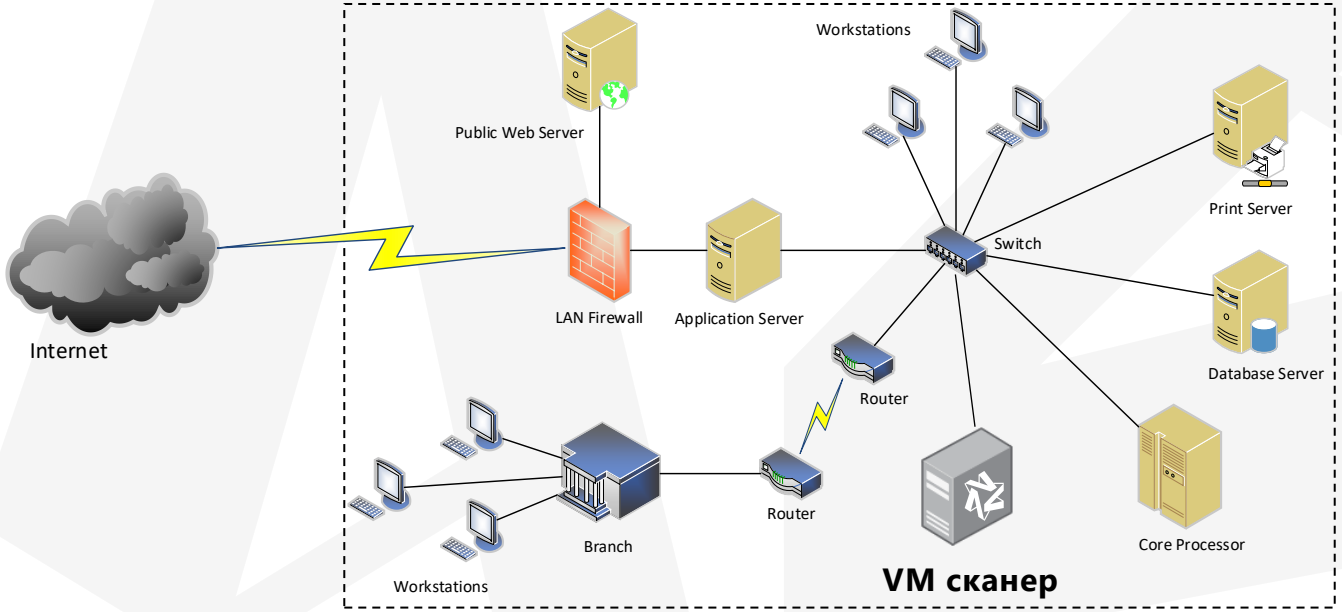
Применение различных подходов выявления уязвимостей даст наиболее полную картину состояния защищенности инфраструктуры.

Черный ящик

Регулярное сканирование периметра для обнаружения рисков безопасности проникновения в инфраструктуру

Белый ящик

Постоянное сканирование активов для определения комплексного уровня защищенности инфраструктуры и обнаружения уязвимостей на раннем этапе



фродекс

Vulns.io VM
Управление уязвимостями

Андрей Никонов
Главный инженер-программист
ООО «Фродекс»

a.nikonov@frodex.ru

t.me/mordron

frodex.ru

Техническая поддержка:
support@frodex.ru

Офис:
г.Уфа, ул.Пархоменко, 133/1

Спасибо за внимание!