

# Введение

## 1. Введение

### 1.1 Управление уязвимостями

В области информационной безопасности на поверхность атаки ИТ-инфраструктуры влияет сочетание трёх факторов:

- злоумышленники, обладающие достаточным опытом, оборудованием и финансами для проведения атаки;
- доступ к целевой ИТ-инфраструктуре;
- уязвимости в ИТ-системах, возникающие из-за ошибок в приложениях, операционных системах или неправильных конфигураций.

Когда эти три элемента совпадают, успешная атака на ИТ-инфраструктуру становится вероятной.

Поскольку большинство уязвимостей известны и могут быть устранены, поверхность атаки можно активно сокращать с помощью системы управления уязвимостями. Управление уязвимостями подразумевает анализ инфраструктуры «со стороны» — так, как это сделал бы потенциальный злоумышленник. Цель — выявить все возможные уязвимости в системах.

Система управления уязвимостями позволяет обнаружить слабые места, оценить их потенциальные риски и предложить конкретные меры по устранению. Таким образом, атаки можно предотвращать посредством постоянных профилактических действий. Процесс от выявления до устранения и последующего контроля выполняется непрерывно.



Рис. 1.1 — Процесс управления уязвимостями

## 1.2 OPENVAS SCAN

**OPENVAS SCAN** — это комплексное решение для управления уязвимостями, доступное в виде аппаратных и виртуальных моделей. Оно предназначено для организаций и ведомств, обеспечивая автоматизированную и интегрированную оценку уязвимостей и управление ими.

### 1.2.1 Компоненты и область применения

Решение основано на **НАЙС.ОС**, на которой установлен **OPENVAS Feed**, сервис сканирования, веб-интерфейс, а в случае аппаратного решения — специализированное оборудование. Feed содержит тесты уязвимостей (VT), используемые сервисом сканирования для выявления слабых мест в исследуемой сети.

Поскольку ежедневно обнаруживаются новые уязвимости, набор тестов необходимо регулярно обновлять. Greenbone анализирует уведомления CVE [1] и рекомендации производителей, создавая новые тесты. Обновления выполняются ежедневно, обеспечивая актуальность и полноту проверки.

Гибкость архитектуры позволяет применять OPENVAS SCAN как в крупных организациях, так и в средних и малых компаниях, а также для специальных задач — аудитов и обучения. Благодаря технологии «master-sensor» решение подходит и для высокозащищённых сегментов.

### 1.2.2 Типы сканирования

OPENVAS SCAN позволяет анализировать уязвимости с разных точек зрения потенциального нарушителя:

- **Внешнее сканирование.** Эмулирует внешнюю атаку, выявляя устаревшие или неверно настроенные межсетевые экраны.
- **DMZ (демилитаризованная зона).** Обнаруживает реальные уязвимости, которые могут быть использованы злоумышленниками, получившими доступ через периметр.
- **Внутреннее сканирование.** Позволяет выявить уязвимости внутри корпоративной сети — например, используемые при атаках социальной инженерии или распространении сетевых червей. Из-за потенциального ущерба этот тип сканирования имеет ключевое значение для общей безопасности.

Сканирования DMZ и внутренние могут выполняться в двух режимах — без аутентификации и с аутентификацией. При аутентифицированном сканировании используются учётные данные, что позволяет находить уязвимости в приложениях, не работающих как сервисы (например, веб-браузеры, офисные пакеты, PDF-просмотрщики).

### Сканирование веб-приложений

Сканер OPENVAS SCAN проверяет hosts, указанные по доменному имени или IP-адресу. Однако URL веб-сайта содержит дополнительные элементы (путь, параметры, протокол), которые сканер не анализирует. Поэтому система не является Web Application Security Scanner (WASS) или HTTP-сканером.

Тем не менее, если на целевом хосте запущено веб-приложение, для которого в feed имеется соответствующий тест, уязвимость будет обнаружена.

## 1.2.3 Классификация и устранение уязвимостей

Обнаруженные уязвимости оцениваются по степени критичности с использованием системы CVSS. Эта оценка позволяет определить приоритеты при устранении — первоочередными считаются меры, направленные на защиту от критических рисков.

Существуют два основных подхода к устранению уязвимостей:

- фактическое устранение — обновление программного обеспечения, удаление уязвимого компонента или изменение конфигурации;
- виртуальное устранение — создание компенсирующего правила в межсетевом экране или системе предотвращения вторжений (так называемый виртуальный патч).

Виртуальное исправление лишь маскирует уязвимость, не устраняя её фактически. При сбое компенсирующего механизма злоумышленник может вновь воспользоваться этим дефектом.

Поэтому предпочтительным решением всегда является установка реального патча или обновления программного обеспечения.

## Сноски

[1] Проект **Common Vulnerabilities and Exposures (CVE)** — независимая платформа для идентификации и публикации сведений о новых уязвимостях.