Про сканеры Nikto и OWASP ZAP

Рекогносцировка — это разведка, сбор информации о цели перед атакой. В кибербезопасности это первый этап тестирования. Этим и занимается Никто

Аналогия из военного дела:

- Рекогносцировка (Nikto) → Разведчики фотографируют крепость, считают солдат, изучают стены

- Активное тестирование (ZAP) → Штурм крепости, проверка ворот на прочность, попытка взлома

В веб-безопасности:

- Nikto смотрит: "На сервере стоит Apache 2.2.15 (устаревший), есть файл phpinfo.php, включён directory listing"

- ZAP пробует: "Вставим `<script>alert(1)</script>` в поле поиска и проверим, выполнится ли JavaScript"

Что конкретно делает Nikto? (Ориентация на серверы)

Nikto проверяет конфигурацию сервера, а не логику приложения. Вот что он ищет:

1. Устаревшее ПО и известные CVE

```
# Nikto найдёт:
Apache/2.2.15 (релиз 2010 года) → Уязвим к CVE-2011-3192, CVE-2017-3169
PHP 5.4.16 (не поддерживается) → Известные RCE уязвимости
```

2. Опасные файлы и директории

```
/phpinfo.php        # Выдает системную информацию
/admin/             # Админ-панель по умолчанию
/backup/            # Возможные бэкапы
/config.php.bak     # Резервные копии конфигов
```

3. Небезопасные заголовки и настройки

```
# Сервер возвращает:
Server: Apache/2.2.15 (CentOS)       # Раскрывает версию
X-Powered-By: PHP/5.4.16        # Раскрывает технологию
```

4. Стандартные уязвимости в популярных CMS

```
/wordpress/wp-admin/     # Стандартный путь WordPress
/joomla/administrator/   # Админка Joomla
/drupal/?q=user/login    # Логин Drupal
```

ZAP vs Nikto: детальное сравнение

Аспект	Nikto (Разведчик)	Zap (Штурмовик)
Подход	Пассивный, наблюдает	Активный, воздействует
Цель	Сервер, ОС, сервисы	Веб-приложение, код
Методы	Запросы стандартных, анализ ответов	SQLi, XSS, обход авторизации
Результаты	Информационные сообщение, рекомендации	Конкретные уязвимости с эксплойтами
Время	2-5 минут	10-30 минут
Риск обнаружения	Низкий (похож на обычный браузер)	Высокий (много запросов)

В UI:

Выберите сканер:

OWASP ZAP — глубокое тестирование приложения (15-25 мин)

- XSS, SQL-инъекции, CSRF, авторизация
- Активное воздействие на приложение

Nikto — быстрая разведка сервера (3-5 мин)

- Устаревшее ПО, опасные файлы, заголовки
- Пассивный анализ конфигурации

Пользователь сканирует сайт:

1. Nikto запускается → находит /admin/login.php
2. ZAP запускается → целенаправленно тестирует форму в /admin/login.php
3. ZAP находит SQL-инъекцию в форме логина

Простые аналогии для понимания

Nikto	Zap
Проверяет дверь на наличие таблички «Открыто»	Пробует отпереть дверь отмычками
Смотрит, какие окна открыты	Пытается залезть через окно
Ищет вывешенные на заборе документы	Подделывает подпись в документах