

# Индивидуальный проект. Этап 4

Использование nikto

---

Щербак Маргарита Романовна

НПИбд-02-21

Студ. билет: 1032216537

2024

RUDN

Научиться использовать nikto.

nikto — базовый сканер безопасности веб-сервера. Он сканирует и обнаруживает уязвимости в веб-приложениях, обычно вызванные неправильной конфигурацией на самом сервере, файлами, установленными по умолчанию, и небезопасными файлами, а также устаревшими серверными приложениями.

# Выполнение лабораторной работы

Nikto можно установить с помощью команды: `sudo apt install nikto` -у. Для сканирования внешнего веб-сервера выполнила команду: `nikto -h http://example.com`.

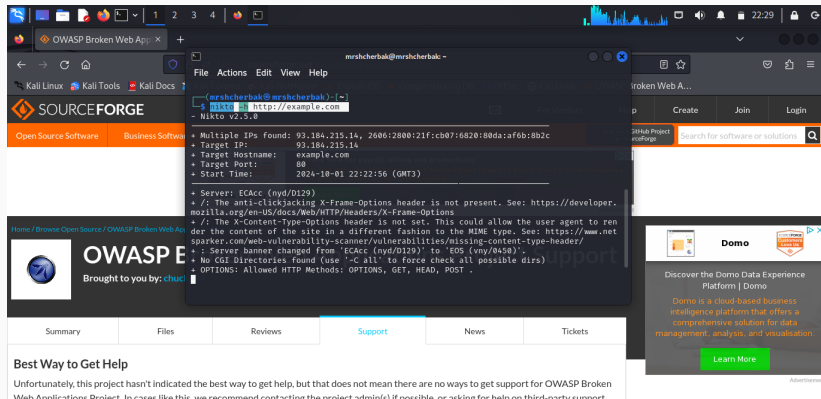


Рис. 1: Сканирование внешнего веб-сервера

# Выполнение лабораторной работы

Для сохранения отчета в файл можно использовать команду: `nikto -h http://127.0.0.1 -output nikto_report.txt`. Для сканирования выбрала локальный сервер.

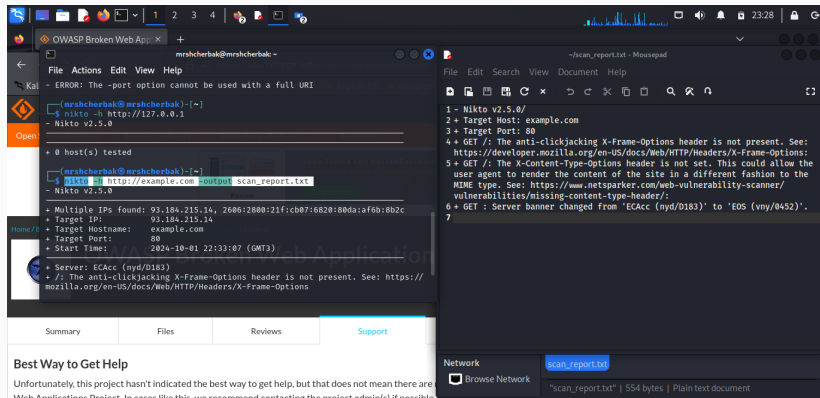


Рис. 2: Сканирование локального веб-сервера и отображение отчета

На основе выявленных уязвимостей можно увидеть возможные проблемы с безопасностью сервера, которые нужно устранить. Например:

- Включить заголовки безопасности (X-Frame-Options, X-Content-Type-Options).
- Закрыть доступ к служебным файлам или интерфейсам администратора.
- Обновить устаревшие версии серверного ПО.

Таким образом, в ходе 4 этапа индивидуального проекта я научилась использовать nikto. Демонстрация Nikto на виртуальной машине Kali Linux позволяет показать, как можно анализировать безопасность веб-сервера и находить потенциальные уязвимости, такие как неправильные настройки серверов, устаревшее ПО или отсутствующие заголовки безопасности.

- Методические материалы курса.
- Rocky Linux Documentation. [Электронный ресурс]. М. URL: Rocky Linux Documentation (Дата обращения: 01.10.2024).