Отчет по этапу №4

Использование nikto

Галацан Николай, НПИбд-01-22

Содержание

# 1 Цель работы

Научиться использовать инструмент для сканирования на уязвимости nikto.

# 2 Выполнение лабораторной работы

**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.

Для сканирования цели необходимо ввести nikto -h <цель> -p <порт>, где <цель> — домен или IP-адрес целевого сайта, а <порт> — порт, на котором запущен сервис [1].

Для получения справки ввожу nikto -h (рис. 1).

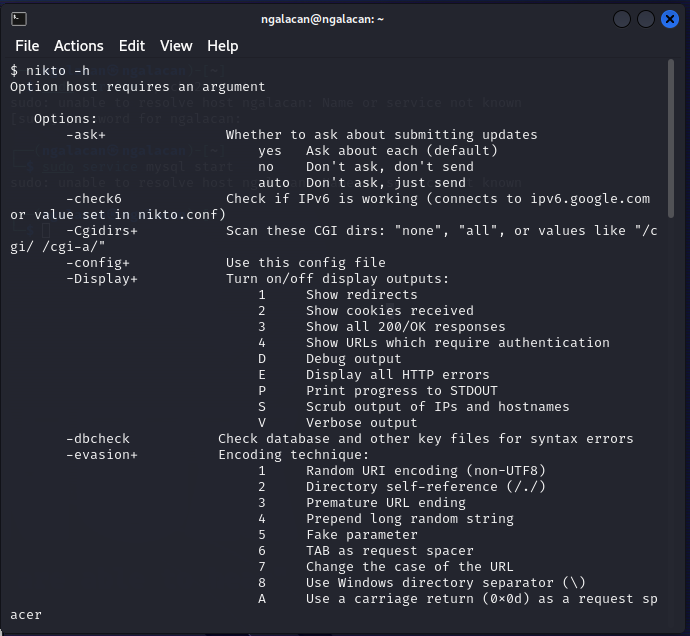


Рис. 1: Справка

Запускаю сканирование для веб-сайта gazel.me. В результате выводятся различные замечания и потенциальные уязвимости (например, уязвимость с кодом CVE-2003-1243) (рис. 2).

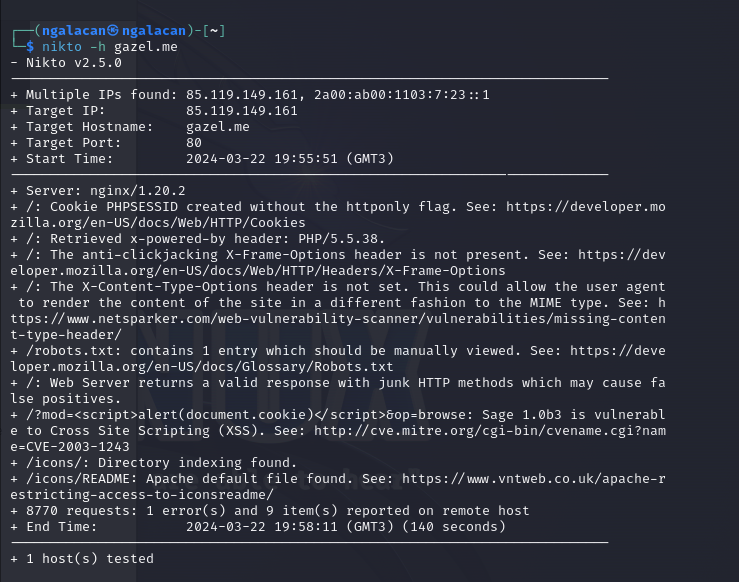


Рис. 2: Сканирование веб-сайта

Запускаю сканирование для локальной сети, введя nikto -h 127.0.0.1. В результате получаю замечаю о работе сервера Apache (рис. 3).

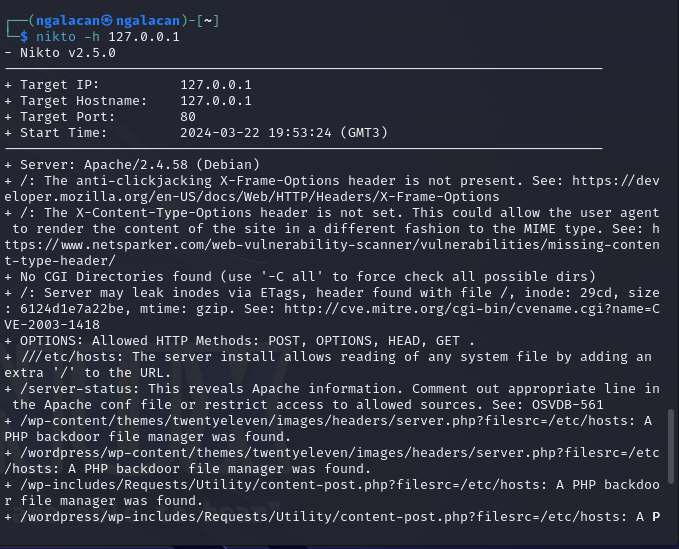


Рис. 3: Сканирование локальной сети

Далее приступаю к сканированию веб-приложения DVWA, запущенном в локальной сети [2] (рис. 4):

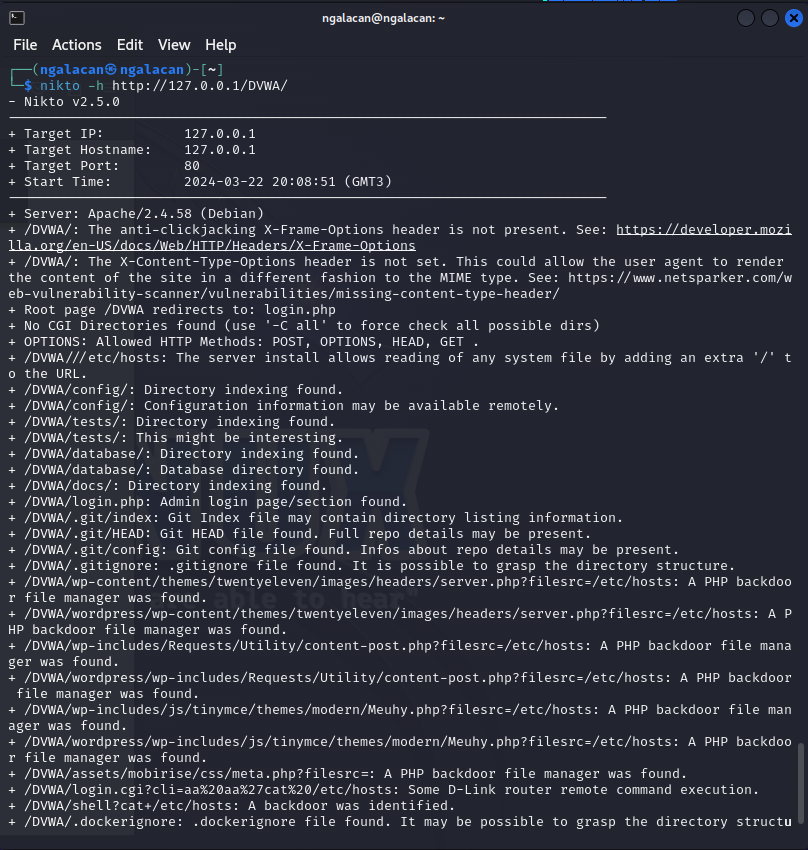


Рис. 4: Сканирование DVWA

nikto выводит информацию о структуре DVWA и находит возможные уязвимости. Среди них, например, PHP backdoor file manager.

# 3 Выводы

Приобретены навыки использования nikto для сканирования веб-серверов на уязвимости. Сканер nikto позволяет идентифицировать уязвимости веб-приложений, такие как раскрытие информации, инъекция (XSS/Script/HTML), удаленный поиск файлов (на уровне сервера), выполнение команд и идентификация программного обеспечения.

# Список литературы

1. Парасрам Ш. и др. Kali Linux: Тестирование на проникновение и безопасность. 4-е изд. Санкт-Петербург: Питер, 2022. 448 с.

2. [Scan for Vulnerabilities on Any Website Using Nikto](https://null-byte.wonderhowto.com/how-to/scan-for-vulnerabilities-any-website-using-nikto-0151729/). [Электронный ресурс].